ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Τμημα Πληροφορικης



IONIAN UNIVERSITY

-- Πτυχιακή Εργασία --

Εκπαιδευτικά σενάρια κυβερνοασφάλειας με βάση το παιχνίδι (GBL) και παιχνίδια εναλλακτικής πραγματικότητας (ARG)

Γεώργιος Παπαδόπουλος

Επιβλέπων Καθηγητής: – Εμμανουήλ Μάγκος –

Σεπτέμβριος 2024

Επιβλέπων Καθηγητής

Εμμανουήλ Μάγκος, *Καθηγητής*,
Τμήμα Πληροφορικής

Τριμελής Επιτροπή

Εμμανουήλ Μάγκος, *Καθηγητής*,
Τμήμα Πληροφορικής
Χριστόφορος Νταντογιάν, *Επίκουρος Καθηγητής*,
Τμήμα Πληροφορικής
Αγγελική Τσώχου, *Αναπληρώτρια Καθηγήτρια*,
Τμήμα Πληροφορικής

Περίληψη

Στη σημερινή εποχή, καθώς αναπτύσσεται η τεχνολογία, είναι εξαιρετικά σημαντικό να υπάρχει επαρκής ενημέρωση στον τομέα της κυβερνοασφάλειας. Ωστόσο, λόγω αυτής της ανάπτυξης, οι μέθοδοι με τους οποίους πραγματοποιούμε την εκπαιδευτική διαδικασία πρέπει να εξελιχθούν παράλληλα. Η *Μάθηση με Βάση το Παιχνίδι* (Game-Based Learning - GBL) αποτελεί μία μέθοδος με την οποία έχουμε τη δυνατότητα για μια πιο ανεπτυγμένη προσέγγιση. Συγκεκριμένα, τα ηλεκτρονικά παιχνίδια είναι εξαιρετικά διαδεδομένα, τα οποία αποτελούν χρήσιμο μέσο για αυτό τον σκοπό. Στην εργασία, θα εξετάσουμε κατά πόσο το GBL, και συγκεκριμένα η χρήση σεναρίου προσεγγίζοντας σενάρια *Δοκιμών Διείσδυσης* (Penetration Testing), μπορεί να χρησιμοποιηθεί στη μάθηση της κυβερνοασφάλειας, αναλύοντας την αποτελεσματικότητα της μεθόδου καθώς και πόσο θετική αντίδραση παρουσιάζουν οι εκπαιδευόμενοι προς αυτό. Για αυτό τον σκοπό, δημιουργήσαμε ένα σενάριο κυβερνοασφάλειας στα πλαίσια ενός εμπορικού παιχνιδιού, NITE Team 4, παρουσιάζοντας γρίφους και προκλήσεις για τους παίκτες του σεναρίου. Το σενάριο έχει περαιτέρω εμπλουτιστεί με στοιχεία από *παιχνίδια εναλλακτικής πραγματικότητας* (Alternate Reality Games - ARG). Για την εκτέλεση της έρευνας, επιλέχθηκαν φοιτητές του Ιονίου Πανεπιστημίου, με την πλειοψηφία να μη διαθέτει μεγάλη εξοικείωση στον τομέα της κυβερνοασφάλειας. Οι φοιτητές αρχικά απάντησαν ένα ερωτηματολόγιο, με ερωτήσεις σχετικά με την κυβερνοασφάλεια. Στη συνέχεια, απάντησαν τις ίδιες ερωτήσεις εφόσον έπαιξαν το σενάριο, έτσι ώστε να παρατηρήσουμε κατά πόσο βελτιώθηκαν οι απαντήσεις τους. Οι συμμετέχοντες παρουσίασαν σημαντική αύξηση στην ποιότητα των απαντήσεων τους, δείχνοντας ότι η προσέγγιση μας αποτελεί αποτελεσματική μέθοδο μάθησης. Επιπλέον, το σενάριο αξιολογήθηκε με βάση το μοντέλο ARCS, παρουσιάζοντας πολύ θετικά αποτελέσματα στις περισσότερες κατηγορίες, με την πλειοψηφία των συμμετεχόντων να είναι πρόθυμοι να μάθουν με παρόμοιο τρόπο στο μέλλον.

Πρόλογος και Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή Εμμανουήλ Μάγκο για την επίβλεψη του προς την εργασία, καθώς και τον Δρ. Στέλιο Καραγιάννη για την καθοδήγηση και συνεισφορά του στην ολοκλήρωση της εργασίας. Θα ήθελα επίσης να ευχαριστήσω το προσωπικό του Ιονίου Πανεπιστήμιου για την καθοδήγηση που πρόσφεραν κατά τη διάρκεια της φοίτησης μου. Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου για τη συμπαράσταση τους σε όλες τις πτυχές της ζωής μου.

Κέρκυρα, Αύγουστος 2024
Γεώργιος Παπαδόπουλος

Περιεχόμενα

A Εισαγωγή 1

A.1 Συνεισφορα . . . 3

A.2 Μεθοδολογια . . . 4

A.3 Παρομοιες Εργασιες . . . 6

A.4 Ενδεικτικη Δομη . . . 7

B Μάθηση με Βάση το Παιχνίδι 8

B.1 Διαφορες Game Based Learning και *Παιχνιδοποίησης* (Gamification) . . . 11

B.2 Alternate Reality Games στη μαθηση . . . 13

B.3 Παιχνιδια με θεματικη την Κυβερνοασφαλεια . . . 15

B.3.1 NITE Team 4 . . . 15

B.3.2 Hacknet . . . 16

B.4 Παιχνιδοποιηση . . . 18

B.4.1 Hack The Box . . . 18

B.4.2 TryHackMe . . . 20

B.4.3 CyberDefenders . . . 22

Γ Παρουσίαση του NITE Team 4 24

Γ.1 Παρουσιαση του *UI/UX* (Σχεδιασμος διεπαφης και εμπειριας χρηστη) στο NITE TEAM 4 . . . 24

Γ.1.1 Information Gathering . . . 27

Γ.1.2 Network Intrusion . . . 29

Γ.1.3 Data Forensic . . . 32

Γ.1.4 Advanced Tools 35
Γ.1.5 Λοιπά στοιχεία UI/UX 36
Γ.2 Οι αποστολες του NITE Team 4 39
Γ.2.1 Academy 40
Γ.2.2 Story Mode 41
Γ.2.3 Open World 42
Γ.2.4 Bounties 43
Γ.2.5 Hivemind Network 44

Δ Δημιουργία σεναρίων στο NITE Team 4 46
Δ.1 Παρουσιαση πλατφορμας για τη δημιουργια σεναριων 46
Δ.2 Παρουσιαση σχεδιασης σεναριου στο NITE Team 4 51
Δ.3 Συνοψη σεναριου στα πλαισια της εργασιας 56
Δ.4 Συνδεση με σεναριο Vulnhub 58
Δ.5 Δοκιμαστικο σταδιο σεναριου 59

E Πειραματικό στάδιο 63
E.1 Μεθοδολογια ερευνας - Ερωτηματολογια 63
E.2 Αποτελεσματα ερευνας 64
E.3 Συζητηση στα αποτελεσματα 72

Z Συμπεράσματα 80
Z.1 Μελλοντικες Εργασιες - Βελτιωσεις 81

Συντμήσεις 88

Γλωσσάρι Ξενικών Όρων 90

Ευρετήριο 94

Κατάλογος Σχημάτων

Α.1 Διαγραμματική απεικόνιση της μεθοδολογίας που ακολούθησε η εργασία . . . 4

Β.2 Η πλατφόρμα του Stinger OS με ανοιχτό το εργαλείο DNS & VHOST Mapping 15
Β.3 Το Network Administrator και η τοπολογία δικτύου του σεναρίου της εργασίας 17
Β.4 Το κύριο μενού χρήστη για το Hack the Box Academy 19
Β.5 Το κύριο μενού χρήστη για το εκπαιδευτικό τμήμα της πλατφόρμας TryHackMe 21
Β.6 Το κύριο μενού χρήστη για το εκπαιδευτικό τμήμα της πλατφόρμας CyberDefenders 23

Γ.7 Η κεντρική διεπαφή του Stinger OS 24
Γ.8 Ένα τμήμα του προφίλ του χρήστη στο Stinger OS 25
Γ.9 Το Stinger OS με διαφορετικό χρώμα και φόντο 26
Γ.10 Τα εργαλεία της κατηγορίας Information Gathering 27
Γ.11 Η χρήση της εντολής sfuzzer μέσα στο εργαλείο DNS & VHost Mapping . . 28
Γ.12 Τα εργαλεία της κατηγορίας Network Intrusion 30
Γ.13 Η διεπαφή του CID Phone Backdoor με περιεχόμενο στα πλαίσια του σεναρίου της έρευνας 32
Γ.14 Τα εργαλεία της κατηγορίας Data Forensic 33
Γ.15 Το εργαλείο XKeyscore, με δεδομένα από το σενάριο της εργασίας 34
Γ.16 Τα εργαλεία της κατηγορίας Advanced Tools 35
Γ.17 Το εργαλείο Turbine C2 Registry, με δύο κάρτες πρόσβασης 36
Γ.18 Οι ρυθμίσεις του Stinger OS 37
Γ.19 Το εργαλείο Goliath-7 37
Γ.20 Όταν η F.A.Y επικοινωνεί με τον παίκτη, αντιπροσωπεύεται και οπτικά στο κάτω δεξιά τμήμα της οθόνης 38
Γ.21 Το κύριο μενού αποστολών 39

Γ.22 Οι αποστολές του τμήματος Basic Terminal Operations στην κατηγορία Academy 40
Γ.23 Το μενού επιλογής αποστολών στην κατηγορία Story Mode 41
Γ.24 Το μενού επιλογής αποστολών στην κατηγορία Open World 42
Γ.25 Το μενού επιλογής αποστολών στην κατηγορία Bounties με μία επιλεγμένη αποστολή 43
Γ.26 Το μενού επιλογής αποστολών στο Hivemind Network 44
Γ.27 Επιλεγμένη αποστολή στο Hivemind Network 45

Δ.28 Το κύριο μενού του χρήστη στο Hivemind Network Administrator 47
Δ.29 Παράδειγμα των κόμβων που είναι διαθέσιμοι στο Hivemind Mapping. Στην περίπτωση ενός WMI κόμβου, έχουμε τη δυνατότητα να προσθέσουμε ports, αντίστοιχα file systems, ένα Trading Outpost, και κάποιο λογαριασμό/άτομο που να αντιστοιχεί στον WMI κόμβο. 48
Δ.30 Η λίστα XKeyscore Entities 49
Δ.31 Η λίστα XKeyscore Documents 50
Δ.32 Η λίστα με τα άτομα τα οποία βρίσκονται στο δίκτυο του σεναρίου 50
Δ.33 Η πρώτη σελίδα του αρχείου Operation: Clear Water 51
Δ.34 Παράδειγμα του επιπρόσθετου περιεχομένου που δημιουργήθηκε για το σενάριο. Εμπλουτίζει τον κόσμο του παιχνιδιού ενώ ταυτόχρονα αποτελεί σημαντικό στοιχείο που βοηθάει τον παίκτη να εξερευνήσει περαιτέρω το δίκτυο 52
Δ.35 Παράδειγμα του επιπρόσθετου περιεχομένου που δημιουργήθηκε για το σενάριο. Έχει τη μορφή ενός email το οποίο ο παίκτης εντοπίζει στα πλαίσια της αποστολής του 53
Δ.36 Τμήμα του γρίφου στην πλατφόρμα X/Twitter 54
Δ.37 Ένα από τα στοιχεία σχεδίασης που χρησιμοποιήθηκαν για την υλοποίηση του σεναρίου. Στο σχήμα απεικονίζεται η δομή ενός συστήματος φακέλων 55
Δ.38 Τα αποτελέσματα της εντολής netscan στο δίκτυο (άνω τμήμα) και τα αποτελέσματα της εντολής dig στο active directory (κάτω τμήμα) 56
Δ.39 Τμήμα του δικτύου που αναπαριστά το active directory του σεναρίου 57
Δ.40 Η περιγραφή του σεναρίου Thales: 1 στο Vulnhub 58
Δ.41 Τμήμα του επιπρόσθετου κεφαλαίου του αρχείου Operation: Clear Water σχετικά με τη λειτουργία των εργαλείων που θα χρειαστεί ο παίκτης. Προστέθηκε κατά το πρώτο δοκιμαστικό στάδιο του σεναρίου 60

Δ.42 Το επιπρόσθετο κεφάλαιο του αρχείου Operation: Clear Water, προσφέροντας μία βοηθητική εισαγωγή για το Stinger OS. Προστέθηκε κατά το δεύτερο δοκιμαστικό στάδιο του σεναρίου 61

E.43 Διάγραμμα με τα ποσοστά των σωστών απαντήσεων πριν και μετά τη συμμετοχή των παικτών στην έρευνα, καθώς και ο μέσος όρος αυτών 72

E.44 Διάγραμμα με τις βαθμολογίες των παικτών στο ερωτηματολόγιο των ερωτήσεων βασισμένο στο μοντέλο ARCS και την επιπρόσθετη παράμετρο, το Perceived Learning 73

Κατάλογος Πινάκων

Β.1 Διαφορές μεταξύ GBL και Gamification [35]. 13

Γ.*1 Τα πιο χρήσιμα εργαλεία και οι εντολές των εργαλείων στην κατηγορία Information Gathering.* 29
Γ.*2 Τα πιο χρήσιμα εργαλεία στην κατηγορία Network Intrusion.* 32
Γ.*3 Τα πιο χρήσιμα εργαλεία στην κατηγορία Data Forensic.* 34
Γ.*4 Τα πιο χρήσιμα εργαλεία στην κατηγορία Advanced Tools.* 36

Ε.1 Απαντήσεις στην ερώτηση "Τι είναι το port scanning;" 64
Ε.2 Απαντήσεις στην ερώτηση "Ποια είναι η σύνηθες τεχνολογία συνδεδεμένη στο port 443;" 65
Ε.3 Απαντήσεις στην ερώτηση "Ποια είναι η σύνηθες τεχνολογία συνδεδεμένη στο port 80;" 65
Ε.4 Απαντήσεις στην ερώτηση "Ποια είναι η χρήση της εντολής search στο metasploit (Searchsploit);" 66
Ε.5 Απαντήσεις στην ερώτηση "Τι είναι το CVE;" 66
Ε.6 Απαντήσεις στην ερώτηση "Τι είναι το Active Directory;" 67
Ε.7 Απαντήσεις στην ερώτηση "Ποια είναι η χρήση του John the Ripper;" . . . 68
Ε.8 Απαντήσεις στην ερώτηση "Τι είναι το salami slicing attack;" 68
Ε.9 Απαντήσεις στην ερώτηση "Τι είναι το XKeyscore;" 69
Ε.10 Απαντήσεις στην ερώτηση "Σε ποιο από τα παρακάτω παραδείγματα φαίνεται ένα subdomain;" 70
Ε.11 Απαντήσεις στην ερώτηση "Ποια είναι η χρήση της εντολής airodump-ng (airodump);" 70
Ε.12 Απαντήσεις στην ερώτηση "Τι είναι ένα password hash;" 71

Ε.13 Απαντήσεις στην ερώτηση "Ποιο από τα παρακάτω είναι σετ πρωτοκόλλων επικοινωνίας;" 71
Ε.14 Απαντήσεις στην ερώτηση ανοικτού τύπου "Εξήγησε συνοπτικά τι έμαθες μέσω του παιχνιδιού" 75
Ε.15 Απαντήσεις στην ερώτηση ανοικτού τύπου "Περιέγραψε τη λειτουργία ή ανάφερε εντολές που χρησιμοποίησες στο παιχνίδι." 76
Ε.16 Απαντήσεις στην ερώτηση ανοικτού τύπου "Πιστεύεις ότι υπάρχουν πλεονεκτήματα σε σχέση με το αληθινό περιβάλλον; Αν ναι, ποια;" 77
Ε.17 Απαντήσεις στην ερώτηση ανοικτού τύπου "Τι θα ήθελες να είναι διαφορετικό για να γίνει πιο αποδοτική η εκμάθηση μέσω του παιχνιδιού;" 78

Κεφάλαιο A

Εισαγωγή

Η ραγδαία τεχνολογική ανάπτυξη και η διείσδυση του διαδικτύου στην καθημερινή ζωή έχουν καταστήσει την κυβερνοασφάλεια ένα από τα πιο κρίσιμα ζητήματα της σύγχρονης εποχής. Το διαδίκτυο δεν παρέχει μόνο αυτό όμως, είναι ένας χώρος γεμάτος με ψυχαγωγία [1], μάθηση και εκπαίδευση [2]. Πλέον δεν είναι μόνο ένα δίκτυο διαμοιρασμού πληροφοριών από ένα άτομο σε ένα άλλο, αλλά ενώνει συσκευές, ιατρικό εξοπλισμό, ακόμα και οχήματα μεταξύ τους [3]. Λόγω της τεράστιας σημασίας που έχει το διαδίκτυο για εμάς, είναι αναγκαία η ύπαρξη καλής προστασίας και του ίδιου του δικτύου, αλλά και των χρηστών. Με τις επιχειρήσεις, τους οργανισμούς και τους ιδιώτες να βασίζονται όλο και περισσότερο στην ψηφιακή τεχνολογία, η ανάγκη για εξειδικευμένο προσωπικό στον τομέα της κυβερνοασφάλειας γίνεται επιτακτική[1]. Ωστόσο, η έλλειψη δεξιοτήτων σε αυτόν τον τομέα αποτελεί ένα σοβαρό πρόβλημα, που απειλεί την ασφάλεια των πληροφοριακών συστημάτων παγκοσμίως. Η υιοθέτηση κατάλληλων μεθόδων εκπαίδευσης για την καλλιέργεια αυτών των δεξιοτήτων είναι ζωτικής σημασίας.

Το βασικό πρόβλημα που αντιμετωπίζεται είναι η έλλειψη ανθρώπινου δυναμικού με τις κατάλληλες δεξιότητες στην κυβερνοασφάλεια [4]. Ειδικά στον τομέα της πληροφορικής, οι φοιτητές και το προσωπικό συχνά δυσκολεύονται να εξοικειωθούν με τις τεχνικές πτυχές της κυβερνοασφάλειας. Αυτό το κενό γνώσεων και δεξιοτήτων αυξάνει τους κινδύνους κυβερνοεπιθέσεων, καθώς δεν υπάρχει επαρκής προετοιμασία για την αντιμετώπιση αυτών των απειλών. Οι πιο συντηρητικές εκτιμήσεις δείχνουν ότι υπάρχει έλλειψη 1.8 εκατομμυρίων ατόμων τα τελευταία χρόνια, ενώ ενδεχομένως ο αριθμός να ανέρχεται έως και 4 εκατομ-

[1] https://digital-strategy.ec.europa.eu/el/activities/cybersecurity-digital-programme

μύρια [5]. Στην Ευρώπη μόνο για το 2022, το ζητούμενο εργατικό δυναμικό ανέρχεται σε 883.000, με την έλλειψη να είναι μεταξύ 260.000 και 500.000 άτομα, επιδεικνύοντας την ανάγκη για αύξηση προσωπικού[2]. Ακόμη, η κυβερνοασφάλεια διαθέτει διάφορες πτυχές και κατηγορίες, δημιουργώντας ένα πιο δύσκολο περιβάλλον για κάποιον που δε διαθέτει μεγάλη εξοικείωση. Σύμφωνα με τον *Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια*[3], μπορούμε να κατηγοριοποιήσουμε τους ρόλους της κυβερνοασφάλειας σε 12 κατηγορίες, με την κάθε κατηγορία να αναλύεται στις αντίστοιχες ικανότητες, ευθύνες, συνεργασίες και άλλα. Αποτελεί χρήσιμη κατηγοριοποίηση αλλά ο μεγάλος αριθμός αυτού ενδεχομένως να υπάρξει εμπόδιο προς άτομα τα οποία επιθυμούν να μάθουν πιο βασικά στοιχεία λόγω της πολυπλοκότητας που υπάρχει. Συνεπώς, υπάρχει αναγκαιότητα για την καλλιέργεια των δεξιοτήτων προς την κυβερνοασφάλεια και η ανάπτυξη ενδιαφέροντος του τομέα αυτού στους μαθητές με προσιτό τρόπο.

Η παραδοσιακή εκπαίδευση συχνά δεν προσφέρει επαρκή εφόδια για την ανάπτυξη απαραίτητων τεχνικών δεξιοτήτων στην κυβερνοασφάλεια. Επιπλέον, είναι χρήσιμο οι υφιστάμενες μέθοδοι διδασκαλίας να περιλαμβάνουν ρεαλιστικά σενάρια εκπαίδευσης[6]. Ωστόσο, αυτό δεν είναι εφικτό για όλες τις περιπτώσεις, καθιστώντας δύσκολη την εφαρμογή των γνώσεων σε πραγματικές καταστάσεις. Παρόλο που η μάθηση μέσω παιχνιδιού (Game-Based Learning - GBL) έχει αναδειχθεί ως μια αποτελεσματική προσέγγιση με πολλαπλά πλεονεκτήματα, συχνά αποτυγχάνει να ενσωματώσει αληθινά σενάρια που απαιτούν τεχνικές δεξιότητες [7]. Ωστόσο, για να είναι επιτυχημένη αυτή η προσέγγιση, το εκπαιδευτικό σενάριο πρέπει να είναι ρεαλιστικό. Η ιστορία και το σενάριο που παρουσιάζεται μέσω του παιχνιδιού πρέπει να αντιπροσωπεύουν πραγματικές καταστάσεις και προκλήσεις της κυβερνοασφάλειας. Μόνο έτσι μπορεί να εξασφαλιστεί ότι οι εκπαιδευόμενοι θα αναπτύξουν τις δεξιότητες που απαιτούνται για να ανταποκριθούν στις απαιτήσεις της εργασίας τους.

Με βάση τα παραπάνω, προτείνεται η δημιουργία ενός εκπαιδευτικού σεναρίου στο πλαίσιο του παιχνιδιού NITE Team 4[4], το οποίο είναι ένα γνωστό παιχνίδι προσομοίωσης που επικεντρώνεται στην κυβερνοασφάλεια. Το σενάριο αυτό θα βασιστεί σε υπάρχουσες ασκήσεις κυβερνοασφάλειας που είναι διαθέσιμες στο διαδίκτυο, όπως προσομοιώσεις penetration testing, ασκήσεις ανίχνευσης απειλών και ανάλυσης κακόβουλου λογισμικού. Η προσαρμογή αυτών των ασκήσεων στο περιβάλλον του παιχνιδιού NITE Team 4 θα επιτρέψει τη δημιουργία

[2]https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

[3]https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu

[4]https://www.niteteam4.com/

ενός εκπαιδευτικού εργαλείου που όχι μόνο θα διδάσκει τις απαραίτητες τεχνικές δεξιότητες αλλά θα το πραγματοποιήσει με έναν τρόπο που είναι ελκυστικός και ρεαλιστικός για τους εκπαιδευόμενους. Το σενάριο και το παιχνίδι θα επιτρέψουν στους συμμετέχοντες να βυθιστούν σε ένα περιβάλλον που προσομοιώνει αληθινές προκλήσεις κυβερνοασφάλειας, ενισχύοντας την εκμάθηση μέσω της πρακτικής εφαρμογής και της ενεργής συμμετοχής.

A.1 Συνεισφορά

Στα πλαίσια της εργασίας, εξετάζεται κατά πόσο το GBL και συγκεκριμένα η *ψηφιακή μάθηση μέσω του παιχνιδιού* (Digital Game Based Learning - DGBL) με τη χρήση σεναρίου κυβερνοασφάλειας, καθώς και διάφορα στοιχεία των παιχνιδιών εναλλακτικής πραγματικότητας (Alternate Reality Games - ARG) μπορούν να βελτιώσουν τη μάθηση και την εκπαίδευση στοιχείων της κυβερνοασφάλειας. Για αυτό τον σκοπό, δημιουργήσαμε ένα εκπαιδευτικό σενάριο στα πλαίσια του παιχνιδιού NITE Team 4. Συνοπτικά η κύρια συνεισφορά συνοψίζεται ως εξής:

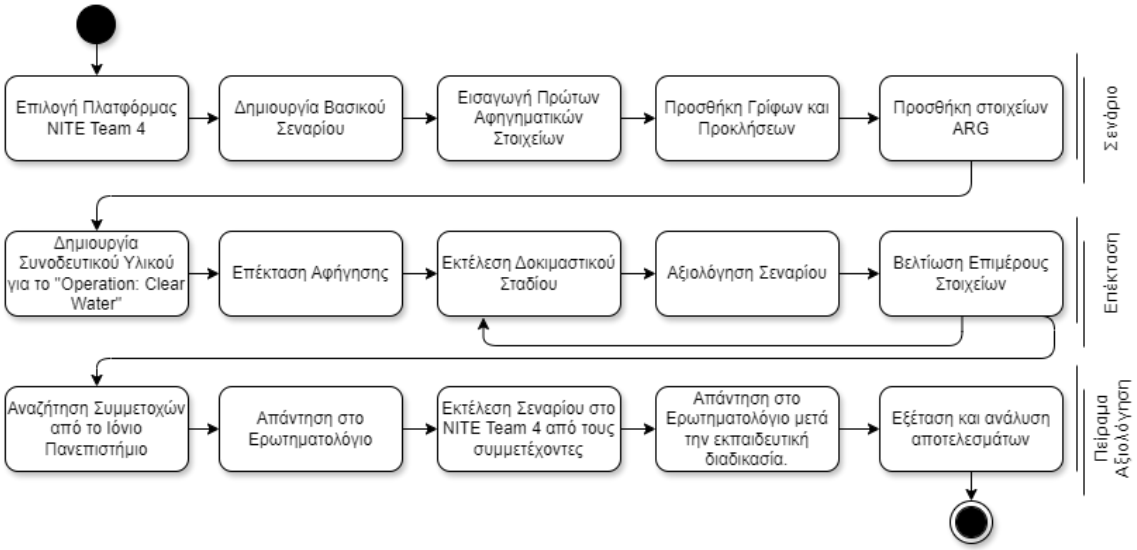
- Εξέταση της αποτελεσματικότητας του Digital Game-Based Learning (DGBL) στην εκπαίδευση κυβερνοασφάλειας.
- Δημιουργία εκπαιδευτικού σεναρίου μέσα στο παιχνίδι NITE Team 4.
- Ανάπτυξη επιπρόσθετου περιεχομένου εκτός του παιχνιδιού για την ενίσχυση της εμβύθισης και την κατανόηση της κυβερνοασφάλειας.
- Παρουσίαση εννοιών κυβερνοασφάλειας μέσω του σεναρίου, με τις οποίες ο παίκτης πρέπει να αλληλεπιδράσει.
- Αξιολόγηση της αποτελεσματικότητας του DGBL μέσω του ARCS μοντέλου και συλλογή εμπειρικών δεδομένων από συμμετέχοντες.

Για την καλύτερη διατύπωση του σεναρίου, δημιουργήσαμε επιπρόσθετο περιεχόμενο εκτός του παιχνιδιού, που έχει ως σκοπό την εμβύθιση του παίκτη στον κόσμο του σεναρίου, καθώς διατυπώνει πληροφορίες για όρους της κυβερνοασφάλειας και τις λειτουργίες του NITE Team 4. Στα πλαίσια του σεναρίου, παρουσιάζονται έννοιες της κυβερνοασφάλειας με τις οποίες ο παίκτης πρέπει να αλληλεπιδράσει.

Μέσω του σεναρίου και της ίδιας της εργασίας, σκοπεύουμε να παρουσιάσουμε εμπειρικά δεδομένα για την αποτελεσματικότητα του DGBL στην κυβερνοασφάλεια, την οποία αξιολογούμε με βάση αποτελεσμάτων του ARCS μοντέλου, καθώς και τη συλλογή απαντήσεων των συμμετεχόντων της έρευνας, σχετικά με τις γνώσεις τους στην κυβερνοασφάλεια πριν και μετά τη συμμετοχή τους. Συμπεραίνουμε ότι το σενάριο ήταν αποτελεσματικό στη μάθηση των συμμετεχόντων, με πολλούς από αυτούς να εκφράζουν το ενδιαφέρον προς παρόμοιες μορφές μάθησης. Οι παίκτες προτίμησαν το εκπαιδευτικό σενάριο συγκριτικά με πιο παραδοσιακούς τρόπους βίωσης σεναρίων κυβερνοασφάλειας.

A.2 Μεθοδολογία

Για την υλοποίηση της εργασίας, επιλέχθηκε η πλατφόρμα Hivemind Network Administrator[5] στο NITE Team 4. Μέσω των εργαλείων δημιουργίας που παρέχει, είναι εφικτή η δημιουργία σεναρίων που να ανταπεξέρχονται στους επιθυμητούς σκοπούς μας, ενώ ακολουθεί τη δομή και τη διασκέδαση που παρέχει το ίδιο το περιεχόμενο του παιχνιδιού. Έμφαση τοποθετήθηκε στην ύπαρξη αφήγησης στα πλαίσια του σεναρίου, ως στοιχείο ενίσχυσης της εμβύθισης και δημιουργία σημείων ενδιαφέροντος.



Σχήμα *A.1*: *Διαγραμματική απεικόνιση της μεθοδολογίας που ακολούθησε η εργασία*

[5]https://store.steampowered.com/app/971750/NITE_Team_4_Network_Administrator/

Στο σενάριο οι συμμετέχοντες έχουν την ευκαιρία να ακολουθήσουν την αφήγηση η οποία λειτουργεί με υποστηρικτικό τρόπο και προσδίδει επιπλέον στοιχεία αυξάνοντας την αλληλεπίδραση και ενισχύοντας το ενδιαφέρον των εκπαιδευομένων. Το σενάριο διαθέτει διάφορες δοκιμασίες και γρίφους προς επίλυση, με την κάθε πρόκληση να απαιτεί είτε τη χρήση κάποιου εργαλείου του παιχνιδιού, είτε την αξιοποίηση κριτικής σκέψης. Επιπλέον, τα στοιχεία ARG τοποθετήθηκαν στο σενάριο, με στόχο την αξιοποίηση της αφήγησης για τη μεγαλύτερη αλληλεπίδραση των χρηστών με το υλικό, καθώς και υλικό το οποίο προστέθηκε έξω από τα πλαίσια του σεναρίου (πχ. σε κοινωνικά δίκτυα).

Για την επιπρόσθετη υποστήριξη του σεναρίου, δημιουργήθηκε το αρχείο Operation: Clear Water εκτός των πλαισίων του παιχνιδιού. Το αρχείο αυτό αποτελεί την αρχή του σεναρίου, και δίνει στο παίκτη πληροφορίες για το περιεχόμενο που θα αντιμετωπίσει. Είναι δομημένο με τέτοιο τρόπο ώστε να περιέχει τον ARG χαρακτήρα του παιχνιδιού, ενώ ταυτόχρονα παρέχει βοηθητικά στοιχεία για την αφήγηση, τα εργαλεία του παιχνιδιού αλλά και τους αντίστοιχους όρους της κυβερνοασφάλειας.

Πριν την εκτέλεση του πειράματος της εργασίας, υπήρχαν δυο δοκιμαστικά στάδια, στα οποία εξετάστηκε το σενάριο. Μέσω αυτού, λάβαμε σημειώσεις και σχόλια για βελτιώσεις στο σενάριο, πραγματοποιώντας αλλαγές για να γίνει πιο προσιτό και βελτιώνοντας τη ροή και το είδος βοήθειας που προσφέρει το επιπρόσθετο αρχείο. Εφόσον πραγματοποιήσαμε τις βελτιώσεις, συνεχίσαμε στην εκτέλεση του πειράματος. Για τη διεξαγωγή του πειράματος 10 φοιτητές από το Τμήμα Πληροφορικής του Ιονίου Πανεπιστήμιου κλίθηκαν να παίξουν το σενάριο. Η πλειοψηφία των φοιτητών που συμμετείχαν στην έρευνα δε διέθεταν ιδιαίτερες γνώσεις στον τομέα της κυβερνοασφάλειας. Οι φοιτητές πριν παίξουν το σενάριο, ολοκλήρωσαν το ερωτηματολόγιο σχετικά με ερωτήσεις κυβερνοασφάλειας, έτσι ώστε να γνωρίζουμε τις γνώσεις που διαθέτουν ήδη. Στη συνέχεια, εφόσον ολοκλήρωσαν το σενάριο, απάντησαν το ίδιο ερωτηματολόγιο και πραγματοποιήσαμε μία σύγκριση μεταξύ των αποτελεσμάτων. Επιπλέον, οι συμμετέχοντες αξιολόγησαν το σενάριο απαντώντας ερωτήσεις στα πλαίσια των εξής παραμέτρων με βάση το μοντέλο ARCS [8] το οποίο απότελείται από τις εξής κατηγορίες: *Προσοχή* (Attention), *Σχετικότητα* (Relevance), *Αυτοπεποίθηση* (Confidence), *Ευχαρίστηση* (Satisfaction). Το μοντέλο ARCS παρέχει κατευθυντήριες γραμμές και στρατηγικές για κάθε παράμετρο, καθώς και μεθόδους για την αξιολόγηση του παρακινητικού αντίκτυπου ενός μαθησιακού περιβάλλοντος. Επιπρόσθετα αξιοποιείται η παράμετρος της *Αντιληπτής Μάθησης* (Perceived Learning) για την αξιολόγηση του μαθησιακού αντίκτυπου. Η αντιληπτή μάθηση αναφέρεται στο μέτρο της μαθησιακής επιτυχίας στο τέλος των μαθησι-

ακών εμπειριών του μαθητή. Η αντιληπτή μάθηση και η μετρική της ικανοποίησης έχουν στο παρελθόν ερευνηθεί για την αλληλεπίδραση τους [9].

A.3 Παρόμοιες Εργασίες

Διάφορες εργασίες παρουσιάζουν παρόμοια μεθοδολογία με τη δική μας, ωστόσο με σημαντικές διαφορές. Τρεις παρόμοιες εργασίες θα εξεταστούν παρακάτω. Στην πρώτη εργασία [10], οι συγγραφείς εξετάζουν την αποτελεσματικότητα που έχει το GBL και συγκεκριμένα τα ηλεκτρονικά παιχνίδια στη μάθηση βασικών γνώσεων στον τομέα της κυβερνοασφάλειας. Για την υλοποίηση της έρευνας, εξετάστηκαν διάφορα παιχνίδια και πλατφόρμες, με το NITE Team 4 να είναι εκείνο που επιλέχθηκε. Οι συγγραφείς εστίασαν στην ποικιλία περιεχομένου που παρέχει το NITE Team 4 για να αξιολογήσουν την ποιότητα της μάθησης. Αυτό διαφέρει με τη δική μας προσέγγιση, στην οποία οι παίκτες εξερευνούν περιεχόμενο το οποίο είναι σχεδιασμένο στα πλαίσια της εργασίας και όχι περιεχόμενο που έχει δημιουργηθεί ήδη από το παιχνίδι ή από άλλους παίκτες, παρουσιάζοντας έμφαση στην ύπαρξη επιμελημένης εμπειρίας. Για την αξιολόγηση των αποτελεσμάτων, χρησιμοποιήθηκε το ARCS μοντέλο, δείχνοντας αποτελέσματα υπέρ της μάθησης μέσω ηλεκτρονικών παιχνιδιών.

Στα πλαίσια της δεύτερης εργασίας [11], δημιουργήθηκε μία πλατφόρμα μάθησης προς την κυβερνοασφάλεια, το CyberAware. Η συγκεκριμένη πλατφόρμα έχει μαθητές δημοτικού ως κύριο εκπαιδευτικό κοινό, με έμφαση στον παιδαγωγικό του χαρακτήρα, ο οποίος στην έρευνα αξιολογείται με τη χρήσης του ARCS μοντέλου. Η πλατφόρμα χωρίζεται σε δύο τμήματα, το διαδικτυακό τμήμα το οποίο παρέχει το εκπαιδευτικό υλικό, και την εφαρμογή για κινητές συσκευές στην οποία βρίσκονται τα παιχνίδια. Τα παιχνίδια είναι γρήγορα προς την ολοκλήρωση τους, με τον παίκτη να έχει την επιλογή αν θέλει να είναι συνδεδεμένος στον διαδικτυακό χώρο ή όχι. Ο τρόπος με τον οποίο αξιοποιείται η πλατφόρμα αποτελεί και την κύρια διαφορά μεταξύ αυτή την εργασία και τη δική μας. Το σενάριο κυβερνοασφάλειας που δημιουργήσαμε κατά μέσο όρο απαιτεί 1-2 ώρες για την ολοκλήρωση. Επίσης, λόγω της μεγαλύτερης διάρκειας του σεναρίου, η αξιοποίηση της ιστορίας και χαρακτήρων που δημιουργήσαμε καθιστά την προσέγγιση πιο προσιτή, προσθέτοντας διαφοροποίηση στο περιεχόμενο με αφηγηματικό τρόπο. Η εργασία κατέληξε ότι με τη χρήση της πλατφόρμας, οι χρήστες βελτίωσαν την επίδοση τους κατά ένα μέσο όρο 20%.

Στην τρίτη εργασία [7], οι συγγραφείς δημιούργησαν μία πλατφόρμα μάθησης, η οποία παρέχει πληροφορίες, παιχνίδια, οδηγίες και προκλήσεις για διάφορους τομείς της κυβερνοασφάλειας.

Παρομοίως με τη δικιά μας και τις άλλες δύο εργασίες που αναφέρθηκαν, χρησιμοποιείται ένα ARCS μοντέλο για την αξιολόγηση των αποτελεσμάτων και της επίδοσης της έρευνας. Ωστόσο, η εργασία διαφέρει στον τρόπο με το οποίο πραγματοποιείται η μάθηση, καθώς ο εκπαιδευτικός χαρακτήρα διαμορφώνεται μέσω προκλήσεων, μικρών παιχνιδιών και επιμορφωτικού υλικού. Η πλατφόρμα υποστηρίζεται διαδικτυακά, χρησιμοποιώντας το Docker για τον διαμοιρασμό των διάφορων προκλήσεων. Οι εκπαιδευόμενοι αξιοποιούν αυτή την πλατφόρμα για να αποκτήσουν πρόσβαση στο υλικό της. Επιπλέον, περιέχονται εικονικά εργαστήρια, με τα οποία οι χρήστες μπορούν να εξασκηθούν. Συνολικά, 120 φοιτητές κλίθηκαν να δοκιμάσουν την πλατφόρμα σε δύο ομάδες, παρουσιάζοντας διαφορετικούς διαγωνισμούς για την κάθε μία. Οι περισσότεροι φοιτητές έδειξαν ενδιαφέρον σχετικά με τη μάθηση μέσω παιχνιδιών, ενώ υπήρξε βελτίωση των αποτελεσμάτων και των γνώσεών τους.

A.4 Ενδεικτική Δομή

Στο κεφάλαιο Β διατυπώνονται βασικές έννοιες και πληροφορίες σχετικά με τις έννοιες οι οποίες είναι σημαντικές για την κατανόηση του ρόλου της εργασίας. Το κεφάλαιο Γ αναλύει τη διεπαφή και το περιεχόμενο του παιχνιδιού NITE Team 4. Στο κεφάλαιο Δ, πραγματοποιείται ανάλυση στον σχεδιασμό του σεναρίου που δημιουργήσαμε. Στο κεφάλαιο Ε παρουσιάζεται η μεθοδολογία και τα αποτελέσματα της εργασίας. Στο κεφάλαιο Ζ παρουσιάζονται τα αποτελέσματα της έρευνας καθώς γίνεται πρόταση για μελλοντικές βελτιώσεις.

Κεφάλαιο B

Μάθηση με Βάση το Παιχνίδι

Το GBL αποτελεί μία από τις αρχαιότερες και πιο χρήσιμες μορφές μάθησης, η οποία έχει χρησιμοποιηθεί εκτενώς σε κάθε χρονική περίοδο [12]. Ειδικά πρόσφατα, υπάρχει μία ανάπτυξη μοντέλων μάθησης με βάση το παιχνίδι, καθώς αυτά τα μοντέλα προσφέρουν στους μαθητές την ικανότητα να αλληλεπιδρούν με το περιεχόμενο αλλά και να εστιάσουν και να αλληλεπιδράσουν με εμβαθυμένους τρόπους σε σχέση με πιο παραδοσιακά μοντέλα [13]. Επιπλέον, ακόμη και τα ίδια τα παιχνίδια μπορούν να καλλιεργήσουν επιπρόσθετες ικανότητες. Οι μαθητές έχουν τη δυνατότητα να χρησιμοποιήσουν τις γνώσεις τους και τις δεξιότητές τους για να αποφασίσουν σωστά στα πλαίσια του παιχνιδιού ενώ μπορούν να παρατηρήσουν τις επιπτώσεις των αποφάσεών τους. Στη συνέχεια, μπορούν να επικοινωνήσουν με άλλους μαθητές για το παιχνίδι και να συζητήσουν σχετικά με τις κινήσεις μέσα σε αυτό, αυξάνοντας τον συντονισμό μεταξύ τους και εν τέλει τις κοινωνικές τους δεξιότητες. Οι μαθητές μέσω αυτού, παρουσιάζουν μεγαλύτερο ενδιαφέρον προς το περιεχόμενο, καθώς συνδυάζεται με κάτι ευχάριστο και διασκεδαστικό, και έχουν μεγαλύτερη θέληση να μάθουν [14].

Τα οφέλη του GBL είναι πολλά, αλλά σε αυτή την εργασία θα εστιάσουμε στον τομέα της μάθησης και εκπαίδευσης στην κυβερνοασφάλεια. Διάφορα μοντέλα έχουν δημιουργηθεί και δοκιμαστεί για την προσέγγιση τέτοιου στόχου, όπως η οντολογία COFELET [15]. Στα πλαίσια του, υπάρχει καθοδήγηση και κανόνες με την οποία ένα παιχνίδι μάθησης κυβερνοασφάλειας μπορεί να διατυπωθεί. Στην εργασία μας, σκοπός είναι να εξετάσουμε τα οφέλη του GBL στη μάθηση της κυβερνοασφάλειας, δημιουργώντας ένα φανταστικό σενάριο κυβερνοασφάλειας, το οποίο παρομοιάζει σενάρια penetration testing, που θα περιέχει στοιχεία από

ARG. Τα ARG είναι παιχνίδια στα οποία ο παίκτης βρίσκει στοιχεία και λύνει διάφορους γρίφους και παζλ για να προχωρήσει στο παιχνίδι. Έχουν την ιδιαιτερότητα ότι αυτά τα παιχνίδια αλληλεπιδρούν με την πραγματικότητα και συχνά το παιχνίδι παραδίδει την ψευδαίσθηση ότι είναι αληθινό [16, 17], και όχι μόνο ένα παιχνίδι. Τα ARG ήδη έχουν χρησιμοποιηθεί στη διδασκαλία και εμφανίζουν θετικά αποτελέσματα, καθώς οι παίκτες είναι πιο αφοσιωμένοι προς το παιχνίδι, δίνοντας τους μεγαλύτερο κίνητρο να συνεχίσουν το παιχνίδι και να μάθουν μέσω αυτού [18].

Διάφορες έρευνες έχουν πραγματοποιηθεί στο χώρο του GBL, με διάφορες μεθόδους και μεθοδολογίες. Για παράδειγμα, στην έρευνα του Hakulinen [19], κύριος σκοπός είναι η ανάπτυξη της μάθησης μέσω της πληροφορικής εξετάζοντας δύο μεθόδους, τη χρήση επιβραβευτικών μεταλλίων και τη χρήση ARG. Στην πρώτη μέθοδο, μελέτησαν τη χρήση τους σε ένα μάθημα σχετικά με το θέμα "Δομές Δεδομένων και Αλγορίθμους", και παρατήρησαν ότι οι μαθητές είναι πιο πρόθυμοι να αξιοποιήσουν τον χρόνο τους στο να μάθουν στα πλαίσια του διαδικτυακού εκπαιδευτικού περιβάλλοντος, ενώ η συμμετοχή τους ήταν πιο συχνή. Επιπρόσθετη ανάλυση έγινε σχετικά με τη σχέση της αποτελεσματικότητας των μεταλλίων και τον προσανατολισμό που είχαν οι μαθητές σε σχέση με τους στόχους τους. Στη δεύτερη μέθοδο, ο συγγραφέας δημιούργησε ένα ARG με στόχο να αξιολογήσει κατά πόσο οι μαθητές έμαθαν έννοιες της πληροφορικής μέσα αυτό. Παρουσίασαν θετικά αποτελέσματα, με τους συμμετέχοντες να μαθαίνουν τεχνολογικούς όρους. Στην εργασία επίσης αξιολογούν πως διάφορα δομικά στοιχεία ενός παιχνιδιού χρησιμοποιήθηκαν στον σχεδιασμό του παιχνιδιού. Τέλος, παρουσιάζουν τους τρόπους με τους οποίους αυτές οι δύο μέθοδοι μπορούν να χρησιμοποιηθούν στην εκπαίδευση.

Ο Hartt [13] εξηγεί ότι στόχος της έρευνας είναι η εξέταση των αποτελεσμάτων που έχει το GBL στη μάθηση, συνεργασία με άλλα άτομα και ενδιαφέρον των μαθητών. Δύο διαλέξεις πραγματοποιήθηκαν στα πλαίσια ενός μαθήματος, το πρώτο με ένα παραδοσιακό τρόπο μάθησης και το δεύτερο να αξιοποιεί GBL. Στα πλαίσια του GBL, δημιουργήθηκε ένα παιχνίδι, το Game of a Lifetime, συγκεκριμένα για τη διάλεξη. Οι μαθητές χωρίστηκαν σε ομάδες, αλλά ο καθένας προχωρούσε στο παιχνίδι μόνος του, με τους μαθητές να δηλώνουν τις απόψεις του σχετικά με τις διαλέξεις μέσω ερωτηματολογίων και διαλέξεων. Με τα αποτελέσματα που απέκτησε ο συγγραφέας, συμπεραίνει ότι οι μαθητές προτίμησαν και έδειξαν μεγάλο ενδιαφέρον προς το GBL, παρουσιάζοντας υποσχόμενα στοιχεία για τη χρήση του στη μάθηση.

Ο Mohanty [20], αναλύει τη δημιουργία του λογισμικού Measure Your Intelligence, εξηγώντας τα στάδια και τη νοοτροπία σχετικά με αυτή. Η εφαρμογή προορίζεται για κινητές εφαρ-

μογές, και χωρίζεται σε 5 παιχνίδια. Το κάθε παιχνίδι αντιστοιχεί στην εκπαίδευση κάποιας ικανότητας (μαθηματική γνώση, παρατηρητικότητα, συγκέντρωση, λογική σκέψη και οπτικοκινητικός συντονισμός), με τα παιχνίδια να είναι βασισμένα σε παιχνίδια που είναι διαθέσιμα σε κινητές συσκευές. Με την ολοκλήρωση κάθε παιχνιδιού, υπάρχει μία βαθμολογία, προωθώντας την ύπαρξη φιλικού ανταγωνισμού μεταξύ των παικτών. Σκοπός της εφαρμογής είναι η παροχή μιας πλατφόρμας για μάθηση και εκπαίδευση ενώ διατηρεί στοιχεία ψυχαγωγίας και διασκέδασης, δημιουργικότητας, ικανοποίησης, κοινωνικής αλληλεπίδρασης και άλλα. Ο συγγραφέας συμπεραίνει ότι η χρήση της εφαρμογής μπορεί να είναι μία χρήσιμη προσθήκη στα πλαίσια της εκπαίδευσης σε σχολεία, δείχνοντας θετικά αποτελέσματα.

Ήδη έχουν παρατηρηθεί θετικά αποτελέσματα μέσω του GBL, με πολύ συχνό τομέα εκπαίδευσης να αποτελεί η μάθηση μαθηματικών και η μάθηση κάποιας νέας γλώσσας [21]. Ειδικά στη δεύτερη περίπτωση, το παιχνίδι εύκολα έχει τη δυνατότητα να συσχετίσει μια εικόνα ή ένα γεγονός με την αντίστοιχη λέξη π.χ. ένα χιονισμένο βουνό ίσως να χαρακτηριστεί ως "snowy mountain" στα πλαίσια του παιχνιδιού. Έπειτα, ο παίκτης μπορεί να καταλήξει στο συμπέρασμα ότι η λέξη "snowy" χρησιμοποιείται για τον χαρακτηρισμό "χιονισμένο", ειδικά αν είναι ήδη γνώριμος με τη σημασία της λέξης "mountain".

Η πιο διαδεδομένη μορφή GBL, ειδικά στις μέρες μας, είναι η μάθηση μέσω ηλεκτρονικών παιχνιδιών. Σύμφωνα με τον Plass [22], υπάρχει μεγαλύτερη αποδοχή των ηλεκτρονικών παιχνιδιών ως μέσο ψυχαγωγίας τα τελευταία χρόνια, που οδηγεί στους ερευνητές να δείξουν μεγαλύτερο ενδιαφέρον για τη δυνατότητα να χρησιμοποιούνται αυτά τα παιχνίδια ως μέσο εκπαίδευσης. Αυτό το ενδιαφέρον έχει μεγαλύτερη αξία καθώς οι ίδιοι οι νέοι αφιερώνουν εκτεταμένο χρόνο σε ηλεκτρονικά παιχνίδια. Παρόλο που υπάρχει εμφανής διαφορά και μεταξύ το είδος παιχνιδιών που προτιμούν τα αγόρια και τα κορίτσια αλλά και στη συχνότητα που παίζουν παιχνίδια, δεν παρατηρείται η ίδια διαφορά στο ενδιαφέρον που δείχνουν οι νέοι προς τις GBL δραστηριότητες. Παρόλο που το GBL πλέον είναι πιο συχνό αντικείμενο έρευνας, χρειάζονται περαιτέρω εμπειρικές έρευνες για να κατανοηθεί καθαρά η διαθεσιμότητα των μαθητών αλλά ακόμα και των καθηγητών προς αυτή τη μορφή μάθησης [23].

Συγκεκριμένα για τη μάθηση μέσω ηλεκτρονικών παιχνιδιών, είναι σημαντικό να υπάρξει ο διαχωρισμός μεταξύ παιχνίδια που έχουν δημιουργηθεί με κύριο σκοπό να ψυχαγωγήσουν και παιχνίδια με κύριο σκοπό να προσφέρουν εκπαίδευση και γνώση. Η Tay [24] εξηγεί ότι παρόλο που στοιχεία όπως η ιστορία του παιχνιδιού και η αισθητική διαμόρφωση του χαρακτήρα του παίκτη προτρέπουν τον παίκτη να αλληλεπιδράσει περισσότερο και για μεγαλύτερο χρονικό διάστημα, αυτά τα ίδια στοιχεία ίσως να μη βοηθήσουν τον παίκτη στον τομέα της μάθησης,

ειδικά αν δεν υπάρχει άμεση σύνδεση με τη μάθηση του παίκτη. Η χρονική διάρκεια του παιχνιδιού καθώς και η συχνότητα με την οποία παρουσιάζεται το εκπαιδευτικό υλικό αλλά και πότε μέσα στο παιχνίδι φαίνεται αυτό το υλικό αποτελεί κάτι που πρέπει να αξιολογηθεί εκτενώς όσο το παιχνίδι δημιουργείται. Ένα παιχνίδι για να παρουσιάσει καλό εκπαιδευτικό χαρακτήρα θα χρειαστεί να μην έχει προβλήματα, γρίφους ή δοκιμασίες οι οποίες απαιτούν υπερβολικά μεγάλο χρονικό διάστημα για την επίλυσή τους. Η υπερ-πολυπλοκότητα καθώς και η αστάθεια του παιχνιδιού και τεχνικά αλλά και μηχανικά ενδεχομένως να αποτρέψει τον παίκτη από το να ευχαριστηθεί το παιχνίδι. Αντιθέτως, η ύπαρξη μιας οριοθετημένης δοκιμασίας ενδεικτικά να αυξήσει την προσοχή και το ενδιαφέρον που έχει ο παίκτης προς το παιχνίδι, προσφέροντας θετικά ερεθίσματα με την επίτευξη του κατορθώματος [25]. Ακόμη, υπάρχουν και άλλα στοιχεία, όπως η ύπαρξη ή μην κάποιου βραβείου ή ανταμοιβής μέσα στο παιχνίδι, που πρέπει να αναλογιστεί. Μπορεί να προσφέρει μεγαλύτερο κίνητρο για τον παίκτη, αλλά συχνά μπορεί να περιορίσει τον τρόπο με τον οποίο γίνεται η εκπαίδευση μέσω του παιχνιδιού. Μέσω αυτού, καταλαβαίνουμε τη σημασία που έχει η σωστή δημιουργία ενός παιχνιδιού που είναι προορισμένο για GBL χρήση, ειδικά επειδή συχνά η ποιότητα του παιχνιδιού του οποίου χρησιμοποιείται δε λαμβάνεται ως μεταβλητή για τα αποτελέσματα των ερευνών [26].

Το κίνητρο και το ενδιαφέρον του μαθητή αποτελεί και αυτό έναν εξαιρετικά σημαντικό παράγοντα για την απόδοση του GBL. Μπορούμε να το θεωρήσουμε αυτό το κίνητρο και το ενδιαφέρον του παίκτη ως το σύνολο του ελέγχου και το σύνολο των στοιχείων που προτρέπει τον ίδιο να συνεχίζει να παίζει [27, 28]. Ο παίκτης θέλει κατά τη διάρκεια του παιχνιδιού να έχει αρκετό έλεγχο για να λάβει τις αποφάσεις που θέλει και να προχωρήσει στο παιχνίδι με αυτό τον τρόπο, αλλά και κατά τη διάρκεια του παιχνιδιού ή στο τέλος, να υπάρχει κάποιο ικανοποιητικό κέρδος προς αυτόν. Το αυξημένο ενδιαφέρον του παίκτη προς το παιχνίδι τον ωθεί να αλληλεπιδράσει και να αφοσιωθεί περισσότερο στο παιχνίδι, προσφέροντας του το κίνητρο να συγκεντρωθεί στο περιεχόμενο του. Στην περίπτωση των εκπαιδευτικών παιχνιδιών, ο παίκτης εν τέλει αφομοιώνει ευκολότερα τα εκπαιδευτικό υλικό.

B.1 Διαφορές Game Based Learning και *Παιχνιδοποίησης* (Gamification)

Το gamification είναι μια παρόμοια έννοια με το GBL, ωστόσο, οι δύο υπάρχουν ως διακριτές έννοιες. Συγκεκριμένα χαρακτηριστικά τα διαφοροποιούν, παρόλο που συχνά οι ειδικοί δεν είναι σίγουροι για το πόσο αυτές οι δύο έννοιες επικαλύπτουν η μία την άλλη [29]. Συγ-

κεκριμένα, το gamification είναι η προσθήκη στοιχείων παιχνιδιού σε ένα περιβάλλον το οποίο δε συσχετίζεται με το παιχνίδι. Αυτά τα στοιχεία για παράδειγμα, μπορεί να έχουν τη μορφή πόντων, επιπέδων ή κατατάξεων, με τα οποία το άτομο που αλληλεπιδρά με το συγκεκριμένο περιβάλλον, μπορεί να αλληλεπιδράσει περαιτέρω με τα στοιχεία που προσφέρει το gamification [12, 30]. Το gamification δεν είναι περιορισμένο μόνο στη μάθηση, αλλά μπορεί να βρεθεί σε πολλές πτυχές της ανθρώπινης ζωής όπως για παράδειγμα η συλλογή πόντων σε ένα κατάστημα με στόχο την απόκτηση κάποιας έκπτωσης.

Αντίθετα, το GBL είναι η μέθοδος με την οποία τα ίδια τα παιχνίδια χρησιμοποιούνται με σκοπό την εκπαίδευση αντί για αποκλειστικά την ψυχαγωγία [31]. Και στις δύο περιπτώσεις ωστόσο, στόχος παραμένει η ύπαρξη αυτού του σοβαρού σκοπού, όπως η εκπαίδευση σε αυτή την περίπτωση. Οι δύο έννοιες έχουν ερευνηθεί αρκετά και κυρίως τα τελευταία χρόνια, αλλά ειδικά στην περίπτωση του gamification, δε διαθέτουμε μία απόλυτη κατανόηση με τον ακριβές τρόπο με τον οποίο βοηθούνε εκπαιδευτικά. Διάφορες έρευνες τοποθετούν απόψεις και αποτελέσματα που διχάζουν, ειδικά με την πληθώρα θεωριών και μοντέλων που υπάρχουν γύρω από τον τρόπο με τον οποίο το gamification βελτιώνει την εκπαίδευση [32]. Ωστόσο, παρατηρούμε ότι και τα δύο μοντέλα έχουν ανάπτυξη στη χρήση τους, με το gamification να χρησιμοποιείται σε εταιρικά πλαίσια και να εξετάζεται η απόδοσή του σχετικά με την εκμάθηση και τη βελτίωση της ψυχικής κατάστασης των υπαλλήλων, καθώς και τη σημασία του στην απόδοση των εργασιών στη δουλειά [33, 34].

Πίνακας *B*.**1:** *Διαφορές μεταξύ GBL και Gamification [35].*

Στοιχεία προς σύγκριση	**Game-based Learning**	**Gamification**
Βασικός ορισμός	Η μέθοδος με την οποία ένα άτομο μαθαίνει μέσω του παιχνιδιού	Η χρήση στοιχείων παιχνιδιού σε περιβάλλον που δε συσχετίζεται με το παιχνίδι
Σκοπός	Εκμάθηση του παίκτη	Συχνά αυξάνει το κίνητρο προς το θέμα ενώ προσθέτει την αίσθηση παιχνιδιού
Λόγος για τη χρήση του	Βελτίωση του τρόπου και της αποδοτικότητας της μάθησης	Ανάλογα την περίπτωση, μπορεί να συσχετίζεται με πολλαπλούς λόγους
Ερώτηση κλειδί	Μαθαίνω αυτά που θα έπρεπε να μαθαίνω;	Εργασία: Βελτιώνει τα κέρδη; Εκπαίδευση: Είναι αποτελεσματικό;
Εστίαση	Μαθησιακοί στόχοι (τι και πως)	Εμπειρία χρήστη (πως)
Προϋπολογισμός	Συνήθως προέρχεται από τον προϋπολογισμό κάποιου ιδρύματος	Κυμαίνεται, συνήθως μπορεί να αποτελεί πολύ μικρό πόσο μέχρι δεκάδες χιλιάδες
Χρηματοοικονομικό μοντέλο	Πληρώνει το ίδρυμα	Πληρώνει ο παραγωγός
Εννοιολογική σημασία	Το παιχνίδι είναι το μάθημα ή μέρος του μαθήματος	Στον τομέα της μάθησης, επηρεάζει τον τρόπο μάθησης παρά το περιεχόμενο μάθησης
Πιστότητα	Πιστότητα στο μήνυμα που παραδίδεται	Δεν υπάρχει, καθώς οποιοδήποτε στοιχείο αφήγησης που ενδεχομένως να υπάρχει δεν είναι αποκλειστικά συνδεδεμένο με το παιχνιδοποιημένο περιεχόμενο

B.2 Alternate Reality Games στη μάθηση

Τα ARGs αποτελούν μία μορφή παιχνιδιών που τα τελευταία χρόνια έχει παρουσιάσει μεγαλύτερο ενδιαφέρον, ξεκινώντας από το 2012 [36]. Ως ARGs ορίζουμε παιχνίδια τα οποία χρησιμοποιούν τον πραγματικό κόσμο ως την πλατφόρμα στην οποία υπάρχει το παιχνίδι, συχνά με τη βοήθεια του διαδικτύου. Επίσης συχνά, πολλά ARGs θολώνουν και κρύβουν τη σχέση πραγματικότητας και παιχνιδιού, προσπαθώντας να παρουσιάσουν μια αληθινή κατάσταση, δημιουργώντας μία αίσθηση αυξημένης εμβύθισης για τον παίκτη. Τα ARG παρουσιάζουν και άλλα στοιχεία, όπως η ύπαρξη μίας ιστορίας με συνοχή, η ύπαρξη πολυμέσων και γρίφων και δοκιμασιών ενώ προωθούν μία αίσθηση συνεργασίας και ομαδικότητας μεταξύ των παικτών [37]. Ωστόσο, πιο πρόσφατα ARGs, παρόλο που ενθαρρύνουν αυτά στοιχεία, η ύπαρξη τους

δεν είναι υποχρεωτική για την εμπειρία. Για παράδειγμα, το ARG "The Black Watchmen" παρόλο που τοποθετεί έμφαση στην ομαδικότητα με άλλους παίκτες, ο παίκτης μπορεί να βιώσει την εμπειρία μόνος του αν επιθυμεί.

Στα πλαίσια ενός ARG υπάρχει ο *μαριονετίστας* (puppet master), ο οποίος χειρίζεται το ARG πίσω από τη σκηνή και οδηγεί τους παίκτες σε διαφορετικά μονοπάτια. Ο puppet master είτε έχει τον ρόλο ενός βοηθού προς τον παίκτη και τον καθοδηγεί προς τον στόχο του, είτε αποτελεί αντίπαλος και προσπαθεί να εμποδίσει τον παίκτη από το να πραγματοποιήσει πρόοδο [38]. Παρών είναι και η έννοια της *λαγουδότρυπας* (rabbit hole), με την οποία αναφέρεται η πρώτη επαφή του παίκτη με το ARG και εκείνο το στοιχείο το οποίο τον προτρέπει να εξερευνήσει το παιχνίδι [38].

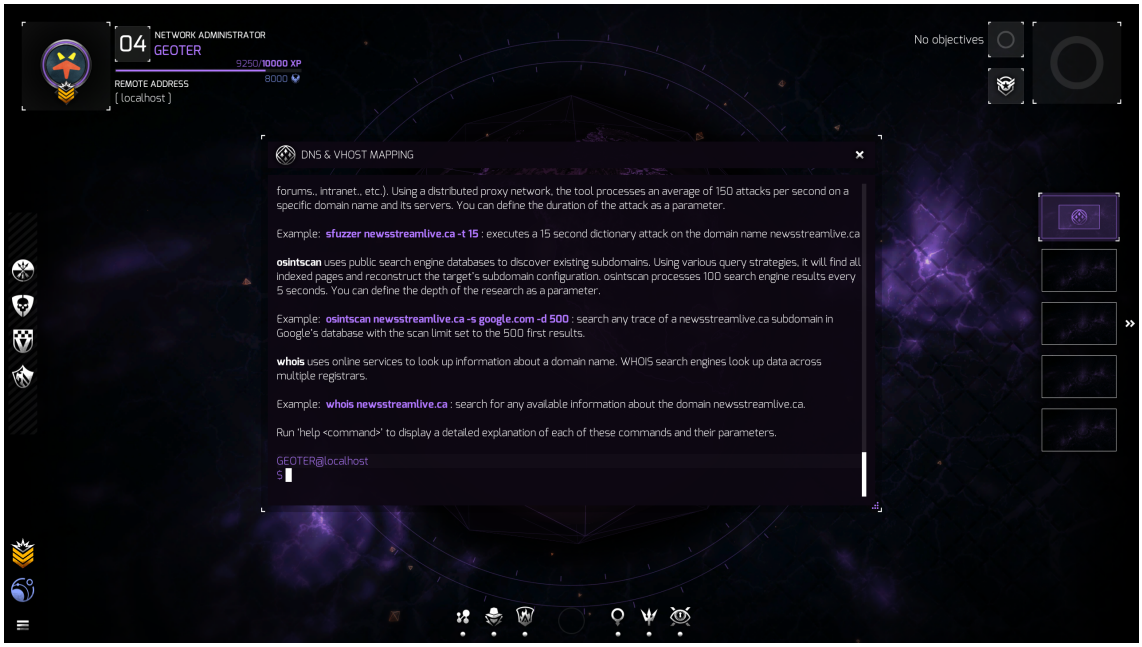
Τα ARG παρουσιάζουν παρόμοια πλεονεκτήματα με άλλα παιχνίδια, ωστόσο λόγω του είδους του παιχνιδιού και τον τρόπο με τον οποίο είναι διατυπωμένα, υπάρχουν στοιχεία που αναδεικνύονται για καλή χρήση στα πλαίσια της παιδαγώγησης. Συγκεκριμένα [36, 38, 39]:

- Λόγω των προκλήσεων και γρίφων, καλλιεργεί σε μεγάλο βαθμό κριτική σκέψη και την ικανότητα επίλυσης προβλημάτων.
- Μέσω της ιστορίας και των χαρακτήρων που περιέχει τα ARG, ο παίκτης έχει μεγαλύτερο κίνητρο και ενδιαφέρον προς τους σκοπούς του. Αυτό επικρατεί ακόμη περισσότερο καθώς το παιχνίδι αλληλεπιδρά με την πραγματικότητα του παίκτη, αυξάνοντας σε μεγάλο βαθμό το επίπεδο εμβύθισης του παίκτη.
- Ο παίκτης μέσω των πράξεων του διαμορφώνει το μονοπάτι που ακολουθεί, προσφέροντας ένα επιπλέον επίπεδο κριτικής σκέψης.
- Υπάρχει ξεκάθαρη πρόοδο από τον παίκτη καθώς συνεχίζει και λύνει όλο και περισσότερα προβλήματα, παρέχοντας μία μέθοδο παρακολούθησης της προόδου.
- Ο παίκτης λύνει προβλήματα σε πραγματικό χρόνο ενώ πρέπει στη συνέχεια να αντιμετωπίσει επιπλέον προκλήσεις, προσφέροντας μία σταθερή ροή από ενδιαφέρον περιεχόμενο.
- Υπάρχει δυνατότητα οικοδόμησης μιας ενεργής κοινότητας γύρω από το παιχνίδι, προωθώντας την κοινωνικότητα και τη συνεργασία μεταξύ παικτών.
- Συνήθως απλές μορφές τεχνολογίας όπως το διαδίκτυο, ήχους, εικόνες κτλ. τα οποία είναι πιο προσιτές και κατανοητές σε μεγαλύτερο πλήθος.

B.3 Παιχνίδια με θεματική την Κυβερνοασφάλεια

B.3.1 NITE Team 4

Το NITE Team 4 είναι ένα παιχνίδι στρατηγικής που προσομοιώνει σενάρια κυβερνοασφάλειας και *hacking* (Ηλεκτρονική παρείσφρηση), από την εταιρεία Alice & Smith και ημερομηνία κυκλοφορίας τις 27 Φεβρουαρίου 2019. Ο παίκτης έχει τον ρόλο ενός νεοσύλλεκτου *χάκερ* (hacker) στην τέταρτη ομάδα για "Network Intelligence & Technical Evaluation", από το οποίο προκύπτει το όνομα NITE Team 4. Σε αυτόν τον ρόλο, συνεργάζεται με την Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ αλλά και με άλλες μυστικές υπηρεσίες που άλλες χώρες διαθέτουν. Το παιχνίδι προσφέρει το δικό του σύστημα εμπνευσμένο από συστήματα όπως το Kali Linux, με την ονομασία Stinger OS, όπως φαίνεται στο σχήμα *B*.2, στο οποίο ο παίκτης μπορεί να πραγματοποιήσει διάφορες ενέργειες οι οποίες είναι βασισμένες πάνω σε αυτές τις αληθινές πλατφόρμες.



Σχήμα *B*.2: *Η πλατφόρμα του Stinger OS με ανοιχτό το εργαλείο DNS & VHOST Mapping*

Στο Stinger OS, ο παίκτης μπορεί να χρησιμοποιήσει τα εργαλεία και τις εντολές που του δίνονται για να επιτεύξει τον σκοπό του, από την εισχώρηση σε ένα εκτεθειμένο δίκτυο μέχρι την απόκτηση πληροφοριών για κάποιο φανταστικό άτομο μέσα στο παιχνίδι. Η σωστή χρήση

του Stinger OS είναι πολύ σημαντική καθώς είναι ο κύριος μηχανισμός του παιχνιδιού. Για τη σωστή εκμάθηση του, το παιχνίδι έχει το Academy, το οποίο έχει διάφορες μικρές αποστολές και δοκιμασίες έτσι ώστε ο παίκτης να εξοικειωθεί με τη χρήση του. Καθώς όμως το παιχνίδι προσομοιώνει συστήματα όπως το Kali Linux, ένας έμπειρος χρήστης μπορεί πιο εύκολα να χρησιμοποιήσει την πλατφόρμα με λιγότερη καθοδήγηση από το παιχνίδι.

Ο παίκτης έχει τη δυνατότητα μέσω του NITE Team 4[1] να παίξει την κεντρική ιστορία, ακολουθώντας αποστολές όπου η μία ενώνει την άλλη και δημιουργεί την υπόθεση και πλοκή. Εκτός από αυτό, υπάρχουν ειδικές αποστολές που είναι ξεχωριστές από την ιστορία του παιχνιδιού. Το Open World, το οποίο έχει στοιχεία από ARG, στο οποίο ο παίκτης θα πρέπει να αλληλεπιδράσει με στοιχεία εκτός του παιχνιδιού, συχνά αναζήτηση στο διαδίκτυο, για να εντοπίσει πληροφορίες και να χρησιμοποιήσει τα ευρήματα του μέσα στο παιχνίδι. Τα Bounties, είναι αποστολές οι οποίες εμφανίζονται κατά τακτά χρονικά διαστήματα, με τον φορέα των αποστολών να είναι κάποια από τις μυστικές υπηρεσίες, τις οποίες μπορεί να βοηθήσει ο παίκτης για να βελτιώσει τις σχέσεις του. Και αυτές οι δύο κατηγορίες αποστολών προσφέρουν μετάλλια, εικονίδια, τίτλους και άλλα στοιχεία προσαρμογής, τα οποία χρησιμοποιούνται για τη διαμόρφωση του προφίλ του παίκτη στο Stinger OS (Σχήμα *Β*.2).

Τέλος, υπάρχει το Hivemind Network, στο οποίο μπορεί ο παίκτης να παίξει σενάρια και αποστολές που έχουν δημιουργηθεί από άλλους παίκτες. Αυτό είναι εφικτό μέσω επιπλέον περιεχόμενο επί πληρωμή που προσφέρει το παιχνίδι, το Network Administrator. Το Network Administrator δίνει πρόσβαση στους παίκτες στα εργαλεία που χρησιμοποιούν οι δημιουργοί του NITE Team 4, για να έχει την ικανότητα ο χρήστης να προσεγγίσει τη δομή των αποστολών του παιχνιδιού. Το Network Administrator, καθώς αποτελεί τον κύριο τρόπο υλοποίησης της εργασίας, θα αναλυθεί περαιτέρω στο κεφάλαιο Δ.

Β.3.2 Hacknet

Το Hacknet[2] αποτελεί ένα άλλο διάσημο παιχνίδι προσομοίωσης hacking, με δημιουργό την Team Fractal Alligator και ημερομηνία κυκλοφορίας τις 13 Αυγούστου 2015. Στο επίκεντρο της πλοκής του παιχνιδιού, είναι ο hacker με το όνομα Bit, ο οποίος είχε ένα απροσδόκητο θάνατο. Ο Bit, δημιουργός του Hacknet-OS, επιθυμεί να το κρατήσει μακριά από επικίνδυνα χέρια καθώς θεωρείται εξαιρετικά δυνατό σύστημα παραβίασης. Για αυτόν τον σκοπό, έχει

[1] https://store.steampowered.com/app/544390/NITE_Team_4__Military_Hacking_Division/

[2] https://store.steampowered.com/app/365450/Hacknet/



Σχήμα *B*.3: *Το Network Administrator και η τοπολογία δικτύου του σεναρίου της εργασίας*

ετοιμάσει αυτοματοποιημένα μηνύματα προς τον παίκτη, έτσι ώστε να μπορεί να τον καθοδηγεί παρά τον θάνατο του. Στόχος του παίκτη είναι να προστατεύσει το Hacknet-OS αλλά και να ανακαλύψει τα μυστικά που κρύβονται πίσω από τον θάνατό του ενώ περιηγείται τον υπόκοσμο των hackers.

Μία μεγάλη διαφορά που έχει το Hacknet σε σχέση με το NITE Team 4 είναι ότι το Hacknet χρησιμοποιεί αποκλειστικά τον χώρο του *τερματικό* (terminal). Το NITE Team 4 αντίθετα, παρόλο που εστιάζει κυρίως στο terminal, περιέχει στοιχεία που δεν πραγματοποιούνται με τη χρήση εντολών, ωστόσο αποτελούν σημαντικά στοιχεία για τη διαδικασία της εισχώρησης ή τη συλλογή πληροφοριών. Έμφαση υπάρχει και στο επίπεδο εμβύθισης του παίκτη καθώς το Hacknet δεν έχει συγκεκριμένα επίπεδα. Η καθοδήγηση που έχει ο παίκτης για να προχωρήσει το παιχνίδι είναι τα μηνύματα του Bit, που είναι δομημένα με τέτοιο τρόπο ώστε ο παίκτης να μη χαθεί κατά τη διάρκεια του παιχνιδιού ενώ ταυτόχρονα δεν αποσπάται η εμβύθιση.

Δύο χρόνια ύστερα, στις 31 Μαρτίου 2017, κυκλοφόρησε μία επέκταση επί πληρωμή του παιχνιδιού, το "Hacknet - Labyrinths"[3]. Η επέκταση περιέχει νέο περιεχόμενο, καινούριους μηχανισμούς στο παιχνίδι προσφέροντας περισσότερες δυνατότητες στο terminal, αλλά και νέους χαρακτήρες, με συνολική διάρκεια τρεις με τέσσερις ώρες. Στην πλοκή του παιχνιδιού,

[3]https://store.steampowered.com/app/521840/Hacknet__Labyrinths/

ένας μυστηριώδης hacker, ο Kaguya, δημιουργεί μία ομάδα από hackers με σκοπό να εντοπίσει ισχυρά προγράμματα και λογισμικό, στην οποία προσκαλεί τον παίκτη. Χρονολογικά, αυτά τα γεγονότα λαμβάνουν χώρο λίγο πριν το τέλος του παιχνιδιού, παρόλο που ο παίκτης μπορεί να παίξει το περιεχόμενο αυτό ακόμη και αν έχει τερματίσει το παιχνίδι.

B.4 Παιχνιδοποίηση

Η παιχνιδοποίηση στην κυβερνοασφάλεια είναι ένα φαινόμενο το οποίο ήδη έχει αναγνωριστεί αλλά και συνεχίζεται να αναπτύσσεται. Συχνά παρουσιάζεται η έννοια του διαγωνισμού "*Πιάσε τη σημαία*" (Capture the Flag - CTF) σε αυτά τα πλαίσια. Τα CTF είναι παιχνιδοποιημένοι διαγωνισμοί ή προκλήσεις στις οποίες ένα άτομο ή μία ομάδα ατόμων πρέπει να πλοηγηθούν σε κάποιο δίκτυο πραγματοποιώντας hacking, με στόχο να εντοπίσουν μία *σημαία* (flag), συχνά στη μορφή ενός αρχείου με τίτλο flag.txt [40]. Το άτομο ή η ομάδα που εντοπίζει πρώτη το flag λαμβάνει πόντους, με νικητή το άτομο ή την ομάδα με τους περισσότερους πόντους, προσφέροντας έτσι ανταγωνιστική και παιχνιδοποιημένη αξία [41].

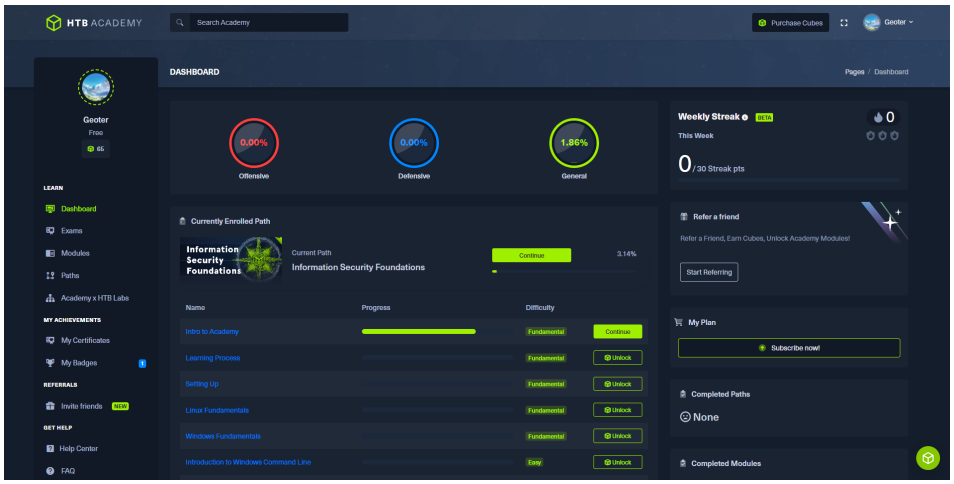
Πλέον, πολλά CTF χρησιμοποιούνται και για τον εκπαιδευτικό τους χαρακτήρα. Αυτά μπορεί να είναι είτε στη μορφή κάποιου μικρού διαγωνισμού ή εργαστηρίου στα πλαίσια μια τάξης [42], είτε διαδικτυακά μέσω των πλατφορμών οι οποίες είναι διαθέσιμες. Σε ορισμένες περιπτώσεις, CTF διαγωνισμοί δημιουργούνται και από οργανισμούς ή επιχειρήσεις, καθώς είναι ένας καλός τρόπος να εξερευνήσουν τις ικανότητες υποψήφιων υπαλλήλων [43]. Διαδικτυακά υπάρχει μία πληθώρα πλατφορμών για CTF, όπως το Facebook CTF, το CTFd, το Mellivora και το Root the Box [43]. Άλλες πλατφόρμες αποτελούν το *Hack The Box* (HTB), το TryHackMe και το CyberDefenders.

B.4.1 Hack The Box

Το Hack The Box[4] είναι μία διαδικτυακή πλατφόρμα που προσφέρει περιεχόμενο gamification, με το κοινό τους να είναι επιχειρήσεις, πανεπιστήμια, κρατικά ινστιτούτα αλλά και μεμονωμένα άτομα που δεν είναι μέρος κάποιου γκρουπ. Τα τελευταία χρόνια έχει παρατηρήσει ραγδαία ανάπτυξη, με πάνω από 2 εκατομμύριους χρήστες το 2023. Η πλατφόρμα είναι επίσης αξιοσημείωτη καθώς έχει από τις μεγαλύτερες κοινότητες στον τομέα του gamification και του hacking, με την πλειοψηφία του προσωπικού να βρίσκεται στην Ελλάδα.

[4]https://www.hackthebox.com/

Το HTB κυρίως παρέχει τέσσερις υπηρεσίες. Το HTB Academy (σχήμα *B.4*) προσφέρει στους χρήστες γνώσεις σχετικά με την κυβερνοασφάλεια στη μορφή μαθημάτων σε μορφή κειμένου. Κατά τη διάρκεια των μαθημάτων, ο χρήστης μπορεί να εξεταστεί στις γνώσεις που απέκτησε ενώ έχει τη δυνατότητα να επιλέξει ο ίδιος τη σειρά με την οποία παρακολουθεί τα μαθήματα. Ωστόσο, υπάρχει μια προτεινόμενη σειρά για την ολοκλήρωση των μαθημάτων. Το HTB Academy επιπλέον διαθέτει διάφορα πεδία και κατευθύνσεις για να τον χρήστη να εξερευνήσει. Επιπλέον, στα μαθήματα υπάρχουν στοιχεία παιχνιδοποίησης, με τη λήψη πόντων με σωστές απαντήσεις και την ύπαρξη ενός εβδομαδιαίου σερί σωστών απαντήσεων, προτρέποντας τον χρήστη να πραγματοποιήσει πρόοδο σε τακτά χρονικά διαστήματα.



Σχήμα *B.4*: *Το κύριο μενού χρήστη για το Hack the Box Academy*

Το HTB Labs παρέχει μία πιο πρακτική προσέγγιση, παρουσιάζοντας σενάρια και μαθήματα στη μορφή εργαστηρίων. Τα μαθήματα συνοδεύονται με ερωτήσεις τις οποίες ο χρήστης πρέπει να απαντήσει κατά τη διάρκεια του εργαστηρίου. Σε αυτά τα εργαστήρια, ο χρήστης συχνά πρέπει να πραγματοποιήσει χρήση του terminal για να ολοκληρώσει τα ζητούμενα. Εκτός από εκπαιδευτικό υλικό, το HTB Labs παρέχει και διάφορα εργαστήρια με σκοπό οι χρήστες να δοκιμάσουν τις ικανότητες τους. Εβδομαδιαία παρουσιάζεται ένα εκτεθειμένο μηχάνημα με τη μορφή CTF, με τους χρήστες να διαγωνίζονται για πόντους, με την ύπαρξη παγκόσμιας κατάταξης. Υπάρχει ακόμη και πιο εξειδικευμένο περιεχόμενο με διάφορες κατηγορίες. Αυτό το περιεχόμενο ενδεχομένως να προορίζεται για συγκεκριμένες ομάδες ή άτομα τα οποία θέλουν να δοκιμαστούν σε συγκεκριμένα σενάρια, ή ακόμα περιεχόμενο προορισμένο για εξαιρετικά ικανούς χρήστες, προσφέροντας μία γιγάντια πρόκληση.

Το HTB Business παρέχει σενάρια προς την εκπαίδευση μιας ομάδας προσωπικού για τον συνεργαζόμενο οργανισμό ή επιχείρηση. Υπάρχει ιδιαίτερη έμφαση στην παροχή ρεαλιστικών σεναρίων κυβερνοασφάλειας που είναι πιθανό να προκύψουν στα πλαίσια της εταιρείας. Στο πρόγραμμα υπάρχουν διάφορα εργαλεία για τους εργαζόμενους αλλά και τον αρχηγό της ομάδας να χρησιμοποιήσει. Κύριος στόχος είναι η εκπαίδευση των εργαζομένων μέσω των στοιχείων παιχνιδοποίησης που παρουσιάζεται μέσω των σεναρίων

Τέλος, υπάρχει το HTB CTF, στο οποίο οι χρήστες μπορούν να συμμετάσχουν ή να δημιουργήσουν CTF προκλήσεις. Συγκεκριμένα για τη δημιουργία CTF, το HTB προσφέρει πακέτα τα οποία περιέχουν έτοιμες επιλογές και προτάσεις για τη δομή του CTF, με τη δυνατότητα ο διοργανωτής να τροποποιήσει το περιεχόμενο. Στην περίπτωση που κανένα από τα πακέτα δεν τον εξυπηρετεί, μπορεί να επικοινωνήσει με την ομάδα του CTF για τη δημιουργία ενός πιο προσαρμοσμένου CTF.

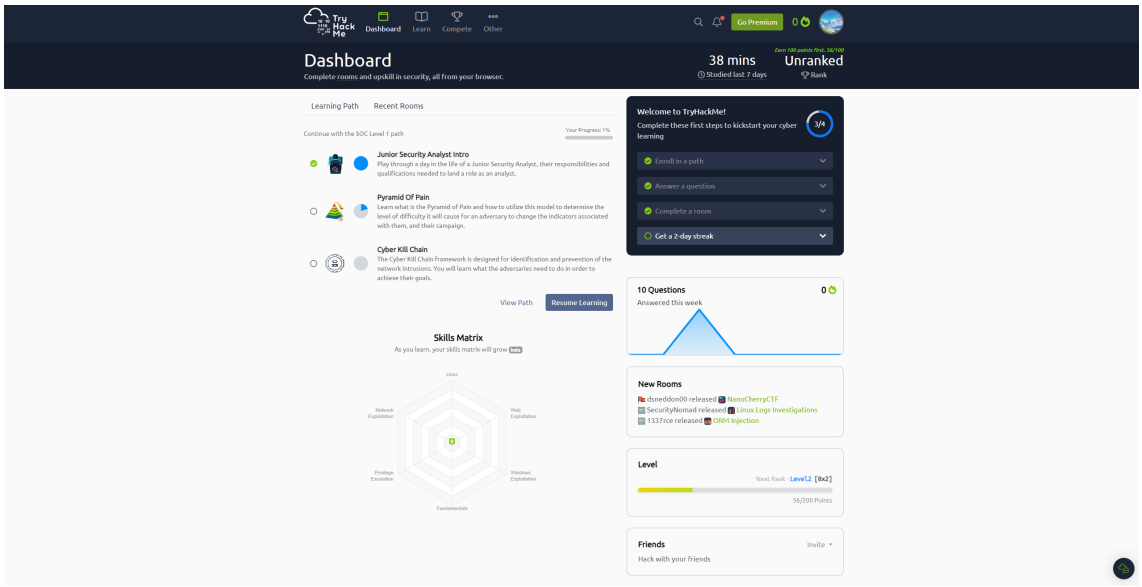
Β.4.2 TryHackMe

Το TryHackMe[5] είναι μία εξίσου μεγάλη διαδικτυακή πλατφόρμα, εξειδικευμένη στην εκμάθηση κυβερνοασφάλειας μέσω gamification. Όπως το HTB, το TryHackMe έχει ως κύριο κοινό άτομα που θέλουν να μάθουν ή να εξασκηθούν στο κομμάτι της κυβερνοασφάλειας, καθώς και επιχειρήσεις και εκπαιδευτικά ινστιτούτα ή σχολεία. Σύμφωνα με τους ιδρυτές της πλατφόρμας, παρατήρησαν ότι δεν υπήρχε κάποιος εύκολος τρόπος ενημέρωσης προς τον τομέα, δείχνοντας μεγάλη δυσκολία για κάποιον να εισαχθεί ή να αναβαθμίσει τις ικανότητες του, με αποτέλεσμα τη δημιουργία της πλατφόρμας.

Η πλατφόρμα προσφέρει την πλειοψηφία του περιεχομένου της δωρεάν, αλλά υπάρχει επιλογή για συνδρομητικό πακέτο που παρέχει στον χρήστη καλύτερες λειτουργίες και περισσότερο περιεχόμενο. Το περιεχόμενο είναι δομημένο σε μαθήματα, από τα βασικά της κρυπτογραφίας μέχρι πιο εξειδικευμένα θέματα όπως ανάλυση κακόβουλου λογισμικού και επιθέσεις χρησιμοποιώντας αδυναμίες στην ασφάλεια ενός συστήματος. Το TryHackMe επίσης παρέχει μικρότερα μαθήματα σε τύπου εργαστηρίου, τα οποία ονομάζει *μονάδες* (module). Αυτά συνήθως επικεντρώνονται σε πιο στοχευμένα θέματα αντί για ένα μεγάλο σύνολο θεμάτων, όπως η χρήση του εργαλείου Nmap ή Metasploit, εισαγωγικές γνώσεις για τη χρήση του λογισμικού Linux και άλλα. Τέλος, υπάρχουν μαθήματα τα οποία είναι βασισμένα σε κάποιο συγκεκριμένο δίκτυο που παρέχει το TryHackMe. Ο χρήστης μπορεί να αποκτήσει πιο πρακ-

[5]https://tryhackme.com/

τικές γνώσεις μέσω αυτών, καθώς συχνά πρέπει να περιηγηθεί μέσα στο αντίστοιχο δίκτυο, αντί να υπάρχει μόνο ένα στοχευμένο σύστημα ή να υπάρχει έμφαση σε θεωρητικές γνώσεις.



Σχήμα *B.5: Το κύριο μενού χρήστη για το εκπαιδευτικό τμήμα της πλατφόρμας TryHackMe*

Το TryHackMe περιέχει πολλά στοιχεία από gamification, που φαίνεται ακόμη και στο προφίλ του χρήστη. Μέσω του μενού, ο χρήστης μπορεί να δει τα επόμενα εργαστήρια και σε πιο ποσοστό έχει απαντήσεις τις ερωτήσεις. Υπάρχουν επίσης διάφοροι μηχανισμοί, όπως ένα σερί πόντων και ένα γράφημα με την ποσότητα σωστών ερωτήσεων ανά εβδομάδα, προτρέποντας τον χρήστη στο να αλληλεπιδράσει περισσότερο με τα μαθήματα της πλατφόρμας. Υπάρχει επιπλέον γράφημα το οποίο αναπτύσσεται όσο βελτιώνεται και ο χρήστης, παρέχοντας μια εικόνα της προόδους του. Τέλος, το επίπεδο του χρήστη ανεβαίνει με το ποσό των σωστών απαντήσεων και αποτελεί ένα περαιτέρω κίνητρο ενώ η λίστα φίλων προωθεί την ύπαρξη κοινότητας μεταξύ των χρηστών, βελτιώνοντας τις κοινωνικές ικανότητες του χρήστη.

Εκτός από περιεχόμενο στοχευμένο στη μάθηση, υπάρχει και ένα μεγάλος αριθμός περιεχομένου με σκοπό ο χρήστης να εξασκηθεί πάνω στις γνώσεις που ίσως να γνωρίζει ήδη ή στις γνώσεις που έχει αποκτήσει μέσω των μαθημάτων. Το υλικό, συνήθως της μορφής CTF, συχνά συνοδεύεται και με μία μορφή εισαγωγής για να τοποθετήσει το σενάριο σε μία είδους πλοκή. Με αυτό τον τρόπο, αυξάνεται η εμβύθιση του χρήστη προς το σενάριο καθώς έχει ένα σκοπό και έναν λόγο για τον οποίο αλληλεπιδρά με το ζητούμενο μηχάνημα. Το υλικό

συνοδεύεται επίσης με ερωτήσεις τις οποίες πρέπει να απαντήσει, με τη λύση να κρύβεται μέσα στο σενάριο. Ακόμη, υπάρχουν και σειρές από παιχνιδοποιημένο υλικό, όπου είτε το κάθε σενάριο έχει κάποια είδους συνοχή και ροή με τα υπόλοιπα σενάρια της σειράς λόγω της ιστορίας και της πλοκής που υπάρχει, είτε το θέμα του σεναρίου είναι τέτοιο ώστε να επιτρέπει την καλή τμηματοποίηση του περιεχομένου.

Η πλατφόρμα εστιάζει και στην ύπαρξη ανταγωνιστικών στοιχείων, όπως με την παροχή μιας κατάταξης μεταξύ των χρηστών. Με την ολοκλήρωση σεναρίων ανεξαρτήτους περιεχομένου, οι χρήστες αποκτούν πόντους, με τους πρώτους 50 να φαίνονται στην κατάταξη. Ανταγωνισμός υπάρχει και στη μορφή ενός παιχνιδιού, του King of the Hill. Σε αυτό, μέχρι δέκα άτομα εισάγονται σε ένα ψηφιακό δωμάτιο, με τον κάθε παίκτη να έχει πρόσβαση στο στοχευμένο μηχάνημα. Το μηχάνημα που θα επιλεχθεί είναι τυχαίο από τα μηχανήματα που έχει το TryHackMe για αυτό τον σκοπό. Στη συνέχεια, οι παίκτες πρέπει να αποκτήσουν πρόσβαση στο μηχάνημα. Το άτομο το οποίο αποκτά πρώτος πρόσβαση, πρέπει να εισάγει το όνομα χρήστη του στο αρχείο /root/king.txt. Στη συνέχεια, σκοπός του είναι να εμποδίσει τους άλλους παίκτες από τον να αποκτήσουν πρόσβαση στον μηχάνημα επιδιορθώνοντας οποιαδήποτε κενά ασφάλειας έχει το σύστημα. Το άτομο κερδίζει 10 πόντους για κάθε λεπτό που το όνομα χρήστη του βρίσκεται στο αρχείο, με τον νικητή να είναι το άτομο με τους περισσότερους πόντους μετά από μία ώρα. Όμως, μέσα στο μηχάνημα υπάρχουν διάφορα flags, που η εύρεση τους δίνει επιπλέον πόντους. Το παιχνίδι, εκτός από την ψυχαγωγική του αξία, εστιάζει και σε μορφές επιθετικού hacking, αλλά και στην άμυνα ενός συστήματος και στη διόρθωση σφαλμάτων. Ακόμη, το παιχνίδι επιβραβεύει παίκτες που εξερευνούν το δίκτυο μέσω των flags. Ο συνδυασμός αυτών των στοιχείων δημιουργεί ένα διασκεδαστικό παιχνίδι με καθοριστικό θετικό αντίκτυπο στις δεξιότητες αλλά και την αντιπαραβολή με τις ικανότητες των συμμετοχών, προσφέροντας ένα σημαντικό εκπαιδευτικό χαρακτήρα.

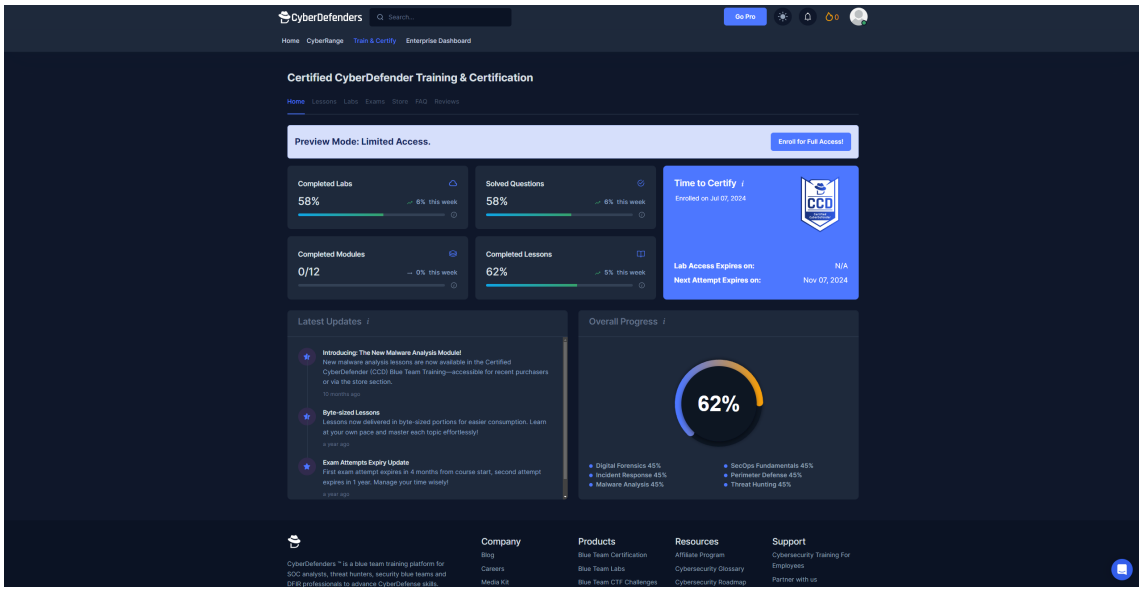
Β.4.3 CyberDefenders

Το CyberDefenders[6], σε αντίθεση με τις δύο προηγούμενες πλατφόρμες, εξειδικεύεται αποκλειστικά στην ασφάλεια και προστασία των συστημάτων. Παρόλο που δεν έχει τόσο μεγάλη έμφαση στο gamification, το CyberDefenders παρέχει CTFs καθώς και λοιπά στοιχεία gamification, όπως μετάλλια, τίτλους και κατατάξεις. Η πλειοψηφία του περιεχόμενου του είναι επί πληρωμή, αλλά υπάρχουν δοκιμαστικά εργαστήρια για κάποιον χρήστη να δοκιμάσει την

[6]https://cyberdefenders.org/

πλατφόρμα.

Τα CTF που διαθέτει έχουν παρόμοια δομή με τα CTF εργαστήρια των άλλων δύο πλατφορμών, παρέχοντας το ανάλογο μηχάνημα και ερωτήσεις με βάση αυτό που ο χρήστης χρειάζεται να απαντήσει. Το CyberDefenders παρουσιάζει επιπλέον πληροφορίες για κάθε ερώτηση όμως, όπως τον αριθμό ατόμων που έχουν απαντήσει σωστά καθώς και τον μέσο όρο χρόνου απάντησης. Η πλατφόρμα επίσης προτείνει στους ικανούς χρήστες να συμμετέχουν και αυτοί στη δημιουργία περιεχομένου μέσω φόρμας, στην οποία ο χρήστης εξηγεί το σενάριο του. Με αυτόν τον τρόπο, καλλιεργείται και το είδος του περιεχομένου αλλά και η ίδια η κοινωνία των χρηστών γύρω από την πλατφόρμα.



Σχήμα *B*.**6:** *Το κύριο μενού χρήστη για το εκπαιδευτικό τμήμα της πλατφόρμας CyberDefenders*

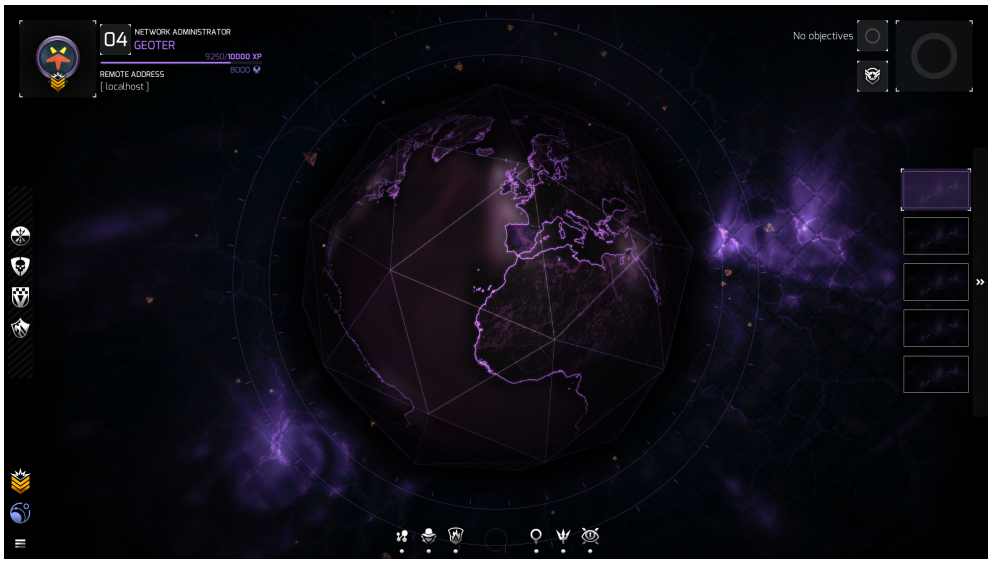
Παρόλο που υπάρχει λιγότερη έμφαση στο τμήμα της παιχνιδοποίησης, τα εκπαιδευτικά εργαστήρια και μαθήματα που διαθέτουν παρουσιάζουν αναλυτικά το υλικό. Όπως φαίνεται στο σχήμα *B*.6, η πλατφόρμα καταγράφει την πρόοδο του χρήστη και του παρέχει στατιστικά προς αυτόν τον σκοπό. Ταυτόχρονα, από το κεντρικό μενού, ο χρήστης μπορεί να εξερευνήσει τα διαθέσιμα μαθήματα και επιπλέον εργαστήρια. Επιπλέον, υπάρχει η επιλογή να εξεταστεί ο χρήστης με ένα πιο παραδοσιακό τρόπο εξέτασης, για να δοκιμάσει τις ικανότητες του αλλά και ένα τμήμα συχνών ερωτήσεων για την πλατφόρμα και τις λειτουργίες της, αυξάνοντας την ευχρηστία.

Κεφάλαιο Γ

Παρουσίαση του NITE Team 4

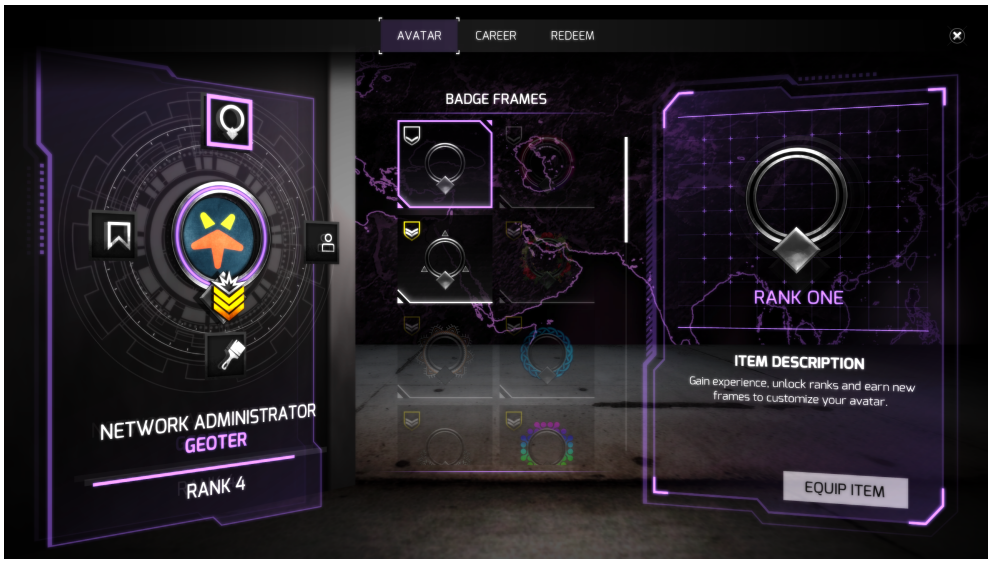
Κύριο παράγοντα της εργασίας αποτελεί το NITE Team 4. Σε αυτό το κεφάλαιο, το περιβάλλον καθώς και στοιχεία της λειτουργικότητας θα επεξηγηθούν περαιτέρω ως συνέχεια του κεφαλαίου Β.2.1.

Γ.1 Παρουσίαση του *UI/UX* (Σχεδιασμός διεπαφής και εμπειρίας χρήστη) στο NITE TEAM 4



Σχήμα Γ.7: *Η κεντρική διεπαφή του Stinger OS*

Η κύρια διεπαφή του μενού είναι το Stinger OS, όπως απεικονίζεται στο σχήμα Γ.7. Ξεκινώντας από την πάνω αριστερή πλευρά, όπου εμφανίζονται το εικονίδιο του χρήστη, το επίπεδο του, το όνομα του, πόσους πόντους εμπειρίας χρειάζεται για να αυξήσει ο χρήστης το επίπεδό του, τον τίτλο του καθώς και σε ποιο δίκτυο είναι συνδεδεμένος στο παιχνίδι. Πατώντας πάνω στο εικονίδιο του, ο χρήστης μπορεί να διαμορφώσει το προφίλ του, όπως φαίνεται στη σελίδα "AVATAR" (Σχήμα Γ.8). Εκεί ο χρήστης μπορεί να αλλάξει το εικονίδιο και το πλαίσιο του εικονιδίου, αλλά και τον τίτλο του. Ιδιαίτερη είναι και η επιλογή σχετικά με τα χρώματα της διεπαφής. Ο χρήστης με διάφορους τρόπους μπορεί να ξεκλειδώσει συνδυασμούς χρωμάτων για να χρησιμοποιήσει, όπως φαίνεται στο σχήμα Γ.9.



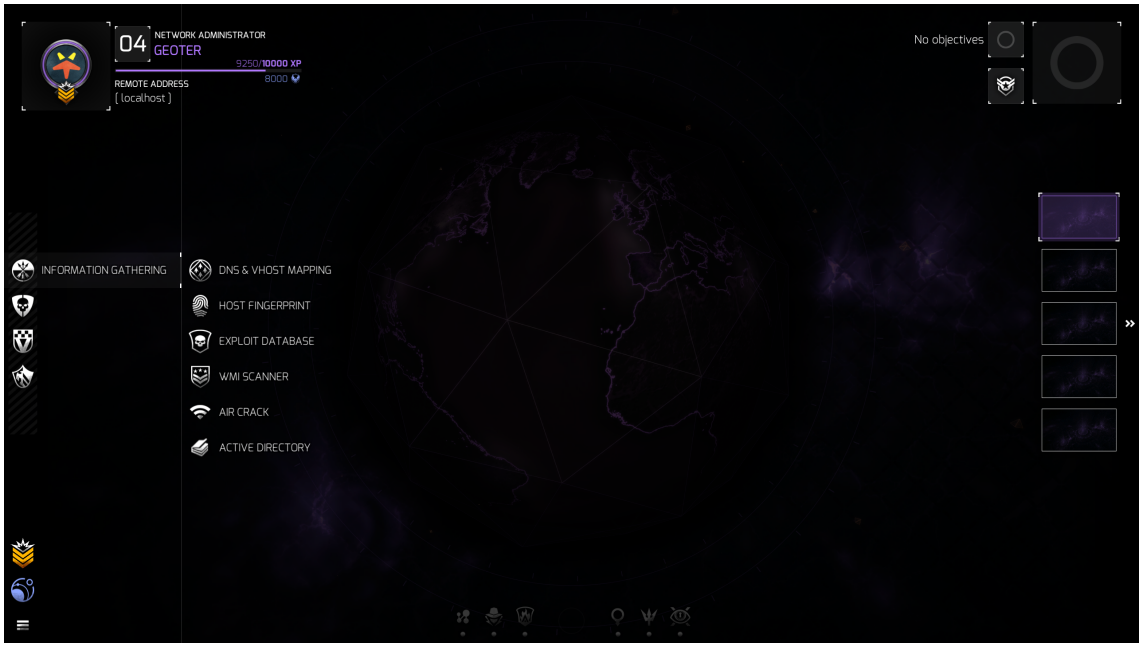
Σχήμα Γ.8: *Ένα τμήμα του προφίλ του χρήστη στο Stinger OS*



Σχήμα Γ.9: *Το Stinger OS με διαφορετικό χρώμα και φόντο*

Αριστερά της οθόνης βρίσκονται τα κύρια εργαλεία που ο παίκτης θα χρησιμοποιήσει. Τα εργαλεία είναι χωρισμένα στις εξής κατηγορίες: Information Gathering (Συλλογή Πληροφοριών), Network Intrusion (Διάρρηξη Δικτύου), Data Forensic (Εγκληματολογία Δεδομένων) και Advanced Tools (Προχωρημένα Εργαλεία). Στους αντίστοιχους πίνακες παρακάτω, μόνο τα εργαλεία στην κατηγορία Information Gathering χρησιμοποιούν εντολές με τη συνηθισμένη έννοια στα πλαίσια ενός terminal και της *γραμμής εντολών* (command line). Υπάρχουν και άλλα εργαλεία που αξιοποιούν εντολές, αλλά είτε χρησιμοποιούνται πολύ σπάνια και δεν αναφέρονται στους πίνακες (Hydra Terminal, SIRPNet), είτε οι εντολές έχουν τον ρόλο ενός μενού (Social Engineering Toolkit). Επιπλέον, όλα τα εργαλεία με τη δυνατότητα εντολών με εξαίρεση το Social Engineering Toolkit, έχουν πρόσβαση στις εντολές help, exit και purge. Η πρώτη αναφέρει τις εντολές ενός εργαλείου και δίνει πληροφορίες για κάποια άλλη επιλεγμένη εντολή, η δεύτερη κλείνει το παράθυρο του εργαλείου και η τρίτη κλείνει όλα τα παράθυρα.

Γ.1.1 Information Gathering

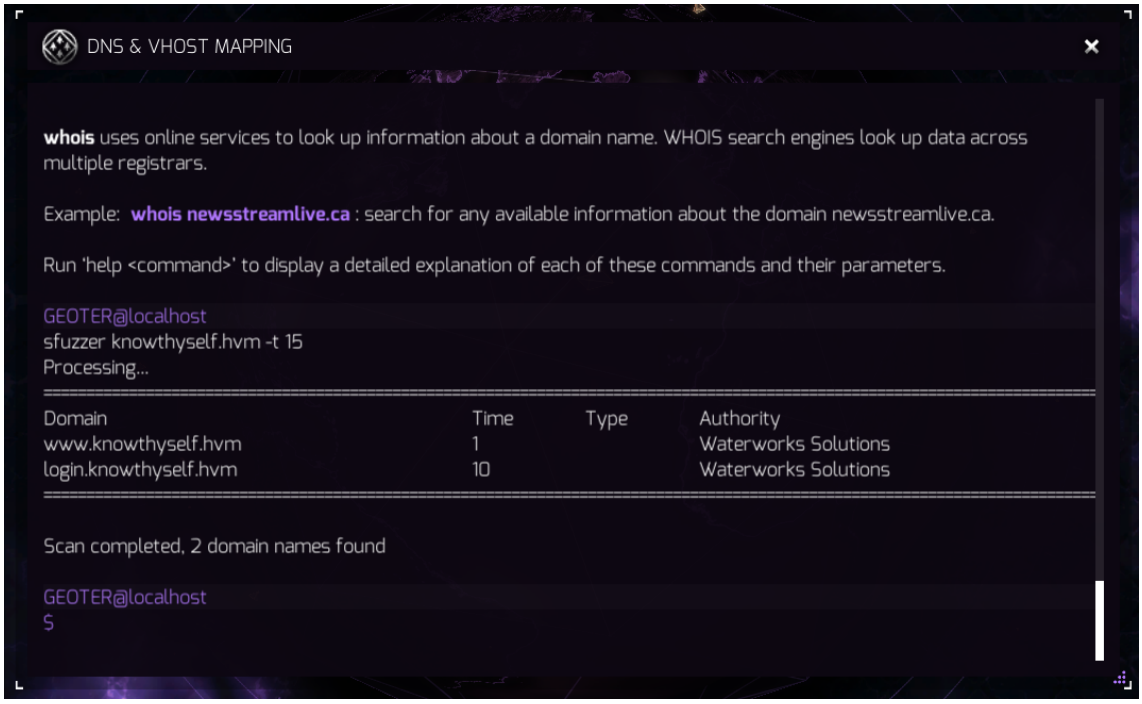


Σχήμα Γ.10: *Τα εργαλεία της κατηγορίας Information Gathering*

Στην κατηγορία του Information Gathering βρίσκονται εργαλεία με κύριο σκοπό την αναζήτηση πληροφοριών σχετικά με το σύστημα. Το DNS & VHost Mapping έχει ως λειτουργία την εντόπιση *ηλεκτρονικού υποχώρου* (subdomain) για την ιστοσελίδα η οποία είναι ο στόχος και συχνά αποτελεί ένα από τα πρώτα εργαλεία με τα οποία ο χρήστης πρέπει να εξοικειωθεί. Στη συνέχεια υπάρχει το Host Fingerprint, το οποίο δημιουργεί μια σειρά επιθέσεων έτσι ώστε να αναγνωρίσει την τεχνολογία στην οποία είναι βασισμένο κάποιο συγκεκριμένο subdomain. Το εργαλείο επίσης εμφανίζει τη *θύρα* (port) στο οποίο βρίσκεται το subdomain, καθώς και αν η συγκεκριμένη έκδοση του λογισμικού που χρησιμοποιεί είναι ευάλωτη ή όχι. Και τα δύο αυτά εργαλεία έχουν ομοιότητες με το αληθινό εργαλείο Nmap[1], το οποίο διαθέτει αυτές τις δυνατότητες. Στην περίπτωση που βρεθεί κάποιο κενό ασφάλειας, ο χρήστης θα συνεχίσει στο επόμενο εργαλείο σε αυτή την κατηγορία, το Exploit Database. Το Exploit Database εμφανίζει τα *Common Vulnerabilities and Exposures* (CVE) της τεχνολογίας στην περίπτωση που αντιστοιχεί σε κάποιο αληθινό παράδειγμα, ενώ παρέχει πληροφορίες σχετικά με τις αδυναμίες που ο χρήστης θα πρέπει να εκμεταλλευτεί. Παρόμοια λειτουργία έχει η

[1]https://nmap.org/

εντολή search του εργαλείου Metasploit[2]. Το τέταρτο εργαλείο είναι το *Windows Management Instrumentation* (WMI) Scanner. Σε αντίθεση με τα προηγούμενα εργαλεία, το WMI Scanner λειτουργεί μόνο για εσωτερικά δίκτυα που χρησιμοποιούν το WMI. Σκοπός του είναι η εύρεση των *καταλόγων αρχείων* (directories) και των *μονοπατιών* (path) μέσα σε ένα δίκτυο. Ταυτόχρονα, έχει τη δυνατότητα να ερευνήσει πιο βαθιά το δίκτυο, εντοπίζοντας στοιχεία για κάποιο στοχευμένο directory, όπως το port, την τεχνολογία πίσω από αυτό, αν είναι ενεργό ή όχι καθώς και αν είναι ευάλωτο σε επιθέσεις. Το προτελευταίο εργαλείο είναι το Air Crack. Έχει τη δυνατότητα να πραγματοποιήσει *σάρωση* (scan) για σημεία Wi-Fi που είναι κοντά στην εκτεθειμένη συσκευή και στη συνέχεια, να κατεβάσει τα αρχεία καταγραφής που αντιστοιχούν. Παρόμοιο εργαλείο είναι το Aircrack-ng[3]. Τέλος, το εργαλείο Active Directory δίνει στον παίκτη πρόσβαση στο Active Directory που είναι συνδεδεμένο με το εκτεθειμένο δίκτυο. Το εργαλείο έχει διεπαφή παρόμοια με ένα συνηθισμένο *σύστημα αρχειοθέτησης* (file management system), στο οποίο ο παίκτης μπορεί να δει τα αρχεία, των οποίων το περιεχόμενο είναι περιορισμένο στα πλαίσια του παιχνιδιού.



Σχήμα Γ.11: *Η χρήση της εντολής sfuzzer μέσα στο εργαλείο DNS & VHost Mapping*

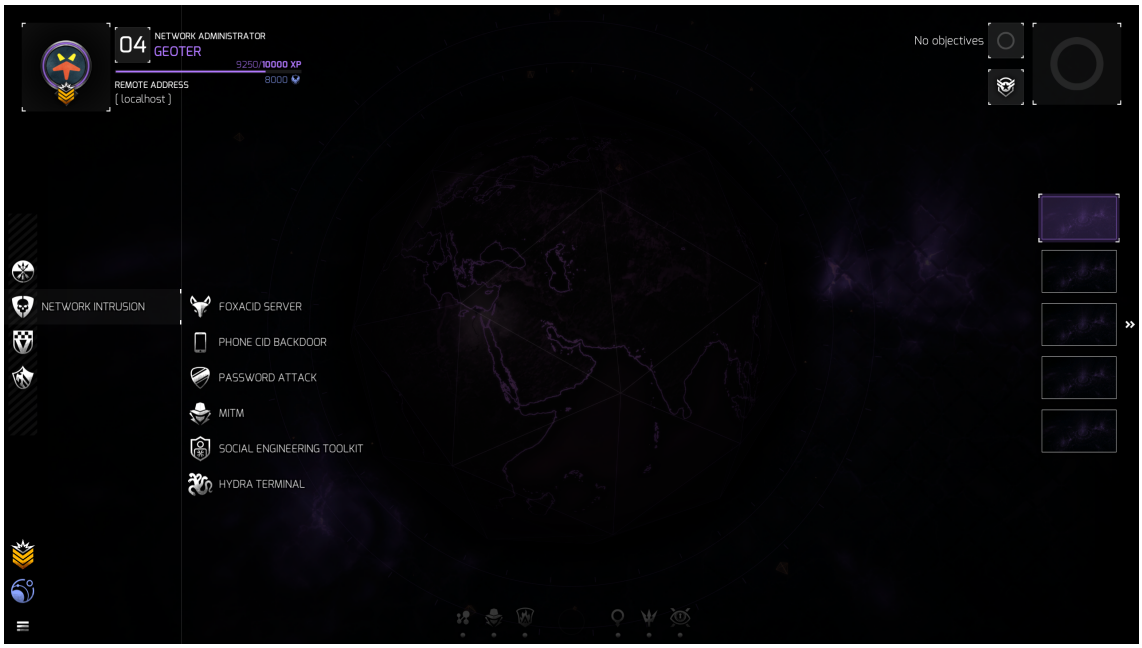
[2]https://www.metasploit.com/
[3]https://www.aircrack-ng.org/

Πίνακας Γ.1: *Τα πιο χρήσιμα εργαλεία και οι εντολές των εργαλείων στην κατηγορία Information Gathering.*

Εργαλείο	**Χρήσιμες εντολές**	**Χρήση εργαλείου**
DNS & VHost Mapping	sfuzzer, osintscan, whois	Εντοπίζει τα subdomains για το στοχευμένο *ηλεκτρονικό χώρο*(domain)
Host Fingerprint	fingerprint	Εντοπίζει τα ports και τις αντίστοιχες τεχνολογίες/λογισμικό του στοχευμένου subdomain
Exploit Database	searchsploit	Βρίσκει πιθανούς τρόπους εκμετάλλευσης των αδυναμιών μιας τεχνολογίας/λογισμικού
WMI Scanner	netscan, dig	Ανιχνεύει το εσωτερικό ενός δικτύου, βρίσκοντας τα μονοπάτια που υπάρχουν, τα ports και τις τεχνολογίες/λογισμικό που χρησιμοποιούν
Air Crack	airodump, handshake	Εντοπίζει τα δίκτυα Wi-Fi και κατεβάζει τα αρχεία καταγραφής στο Stinger OS
Active Directory	-	Σύστημα για την οργάνωση πληροφοριών για τους πόρους και τους χρήστες ενός συστήματος

Γ.1.2 Network Intrusion

Στο Network Intrusion εμφανίζονται τα εργαλεία που επιτρέπουν στον χρήστη να αποκτήσει πρόσβαση είτε στο ίδιο το δίκτυο είτε σε διάφορα στοιχεία του δικτύου. Συγκεκριμένα, το Foxacid Server είναι μια απλοποιημένη εκδοχή των διαφόρων πραγματικών εργαλείων που χρησιμοποιούνται για να εκμεταλλευτούν αδυναμίες σε ένα δίκτυο. Μέσω του γραφικού του περιβάλλον, ο χρήστης μπορεί να διαλέξει την τεχνολογία με την οποία θα εκτελέσει την επίθεση, καθώς και τον τρόπο με τον οποίο θα εκμεταλλευτεί τις αδυναμίες. Ο παίκτης θα έχει αποκτήσει τις πληροφορίες για το τι θα χρειαστεί να χρησιμοποιήσει με τη χρήση του Exploit Database που αναφέρεται στο κεφάλαιο Γ.1.1. Στη συνέχεια, το Phone CID Backdoor επιτρέπει στον παίκτη να αποκτήσει πρόσβαση σε συγκεκριμένες κινητές συσκευές. Η διαδικασία της διάρρηξης είναι εξίσου απλοποιημένη καθώς ο παίκτης χρειάζεται μόνο τη *διεύθυνση MAC* (Media Access Control Address - MAC Address) του κινητού τηλεφώνου καθώς και το όνομα της εταιρείας η οποία κατασκευάζει το συγκεκριμένο είδος τηλεφώνου. Με την εισαγωγή των σωστών στοιχείων, ο χρήστης έχει πλήρης πρόσβαση στο κινητό και μπορεί να παρακολουθήσει αποθηκευμένα δεδομένα όπως μηνύματα, κλήσεις, *ηλεκτρονικά*

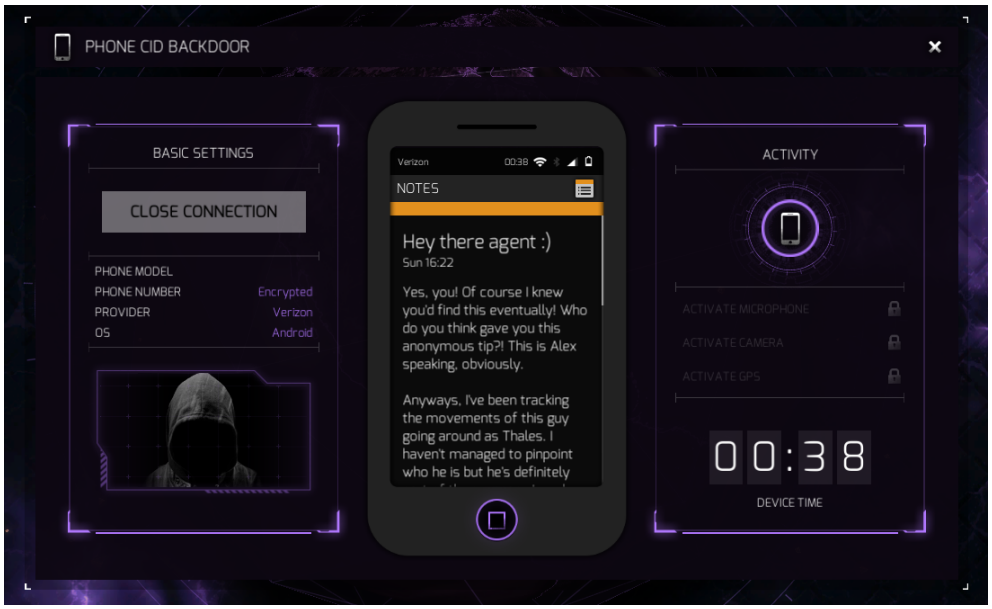


Σχήμα Γ.12: *Τα εργαλεία της κατηγορίας Network Intrusion*

ταχυδρομεία (email) και άλλα. Ωστόσο, το παιχνίδι επιτρέπει στον παίκτη να πραγματοποιήσει μόνο συγκεκριμένες πράξεις. Για παράδειγμα, δεν έχει τη δυνατότητα να δημιουργήσει κλήσεις ή να αποστείλει μηνύματα, αλλά μπορεί να χρησιμοποιήσει το μικρόφωνο του κινητού για να ακούσει ενδεχομένως τον κάτοχο του κινητού ή οποιονδήποτε ήχο γύρω από την τοποθεσία του κινητού. Το εργαλείο Password Attack έχει ως σκοπό την εύρεση και ανάκτηση κωδικών, το όποιο πραγματοποιείται με δύο μεθόδους. Στην πρώτη, ο παίκτης πρέπει να εισάγει το όνομα χρήστη καθώς και το path μέσα στο δίκτυο το οποίο αντιστοιχεί στο όνομα χρήστη. Στη συνέχεια, ο χρήστης μπορεί να πραγματοποιήσει μία *επίθεση λεξικού* (dictionary attack), συνδυάζοντας διάφορες λίστες. Τέλος, ο παίκτης μπορεί να επιταχύνει τον χρόνο που χρειάζεται για να βρεθεί ο κωδικός με την εισαγωγή στοιχείων που συνδέονται με τον χρήστη του οποίου τον κωδικό ψάχνει ο παίκτης. Αυτά τα στοιχεία είναι το όνομα, επίθετο και η ημερομηνία γέννησης του καθώς και έως πέντε επιπλέον στοιχεία τα οποία μπορεί να έχουν διάφορο περιεχόμενο αλλά και πάλι συνδέονται με τον χρήστη, π.χ. το όνομα του καλύτερου του φίλου, το αγαπημένο του φαγητό, ο αγαπημένος του ταξιδιωτικός τόπος, το μέρος γέννησης του κτλ. Αυτή η μέθοδος επιβραβεύει έναν παίκτη που έχει ερευνήσει παραπάνω και έχει βρει σημαντικά στοιχεία, καθώς πολύ συχνά η μείωση του χρόνου είναι σημαντική. Το Password Attack χρησιμοποιεί διάφορους μηχανισμούς για την εύρεση του

κωδικού, όπως το John the Ripper[4], και λεξιλογικές λίστες όπως το rockyou, δεδομένα από πλατφόρμες όπως το LinkedIn και άλλα. Το Man in the Middle (MITM) πραγματοποιεί μία MITM επίθεση, με τον παίκτη να έχει την επιλογή μεταξύ ARP poisoning και LLMNR poisoning. Ο παίκτης έπειτα μπορεί να εντοπίσει τις "συνομιλίες" μεταξύ τα διάφορα *διαδικτυακά πρωτόκολλα* (Internet Protocol - IP) και να διακόψει οποιαδήποτε μηνύματα μεταφέρονται. Το Social Engineering Toolkit επιτρέπει στον παίκτη να πραγματοποιήσει μία επίθεση είδους spear-phishing στον στόχο του. Η διεπαφή βοηθάει τον παίκτη να οργανώσει την επίθεση, προσφέροντας διάφορες δυνατότητες. Μέσω αυτής, έχει τη δυνατότητα να κατασκευάσει τη βάση των email τα οποία θα στοχεύσει, είτε χρησιμοποιώντας έναν *ανιχνευτή ηλεκτρονικού ταχυδρομείου* (email crawler) μέσω διαφόρων φυλλομετρητών, είτε μέσω της χρήσης του LinkedIn για να στοχεύσει ο παίκτης τη συγκεκριμένη εταιρεία και να γίνει κάποια μορφή dictionary attack για να εντοπίσει πιθανά email. Ο παίκτης έχει και την επιλογή να εισάγει ο ίδιος τα email που θέλει να στοχεύσει στην περίπτωση που τα έχει εντοπίσει. Στη συνέχεια, μπορεί να επιλέξει τον τύπο του αρχείου που θα περιέχει το *φορτίο πληροφοριών* (payload), καθώς και τον τύπου του payload. Τέλος, ο παίκτης πρέπει να δομήσει το ίδιο το email που θα αποσταλεί, ακολουθώντας διάφορα κοινά είδη email που θα χρησιμοποιούσε μία εταιρεία, και εισάγοντας το θέμα και τον αποστολέα που αρμόζει με το είδος του email. Εφόσον γίνει η επίθεση, ο παίκτης διαθέτει μια αναλυτική εικόνα από τα δεδομένα σχετικά με την επίθεση, όπως ποιοι έχουν λάβει το email, ποιοι έχουν αλληλεπιδράσει με αυτό και σε ποια συστήματα η επίθεση είναι επιτυχής. Τελευταίο είναι το Hydra Terminal, το οποίο διαφέρει σε αντίθεση με τα άλλα εργαλεία στο Network Intrusion, καθώς δεν έχει κάποια προκαθορισμένη λειτουργία. Αντί αυτού, το εργαλείο έχει τη δυνατότητα να συνδεθεί με διάφορα εξωτερικά δίκτυα και συσκευές, με το κάθε δίκτυο να εμφανίζει μία ξεχωριστή γραφική διεπαφή. Μέσω αυτής της διεπαφής, ο παίκτης μπορεί να αλληλεπιδράσει με το συνδεδεμένο σύστημα. Λόγω της ιδιαιτερότητάς του, το Hydra Terminal δεν μπορεί να χρησιμοποιηθεί στο Network Administrator, και χρησιμοποιείται μόνο σε διάφορα τμήματα της ιστορίας του παιχνιδιού.

[4]https://www.openwall.com/john/



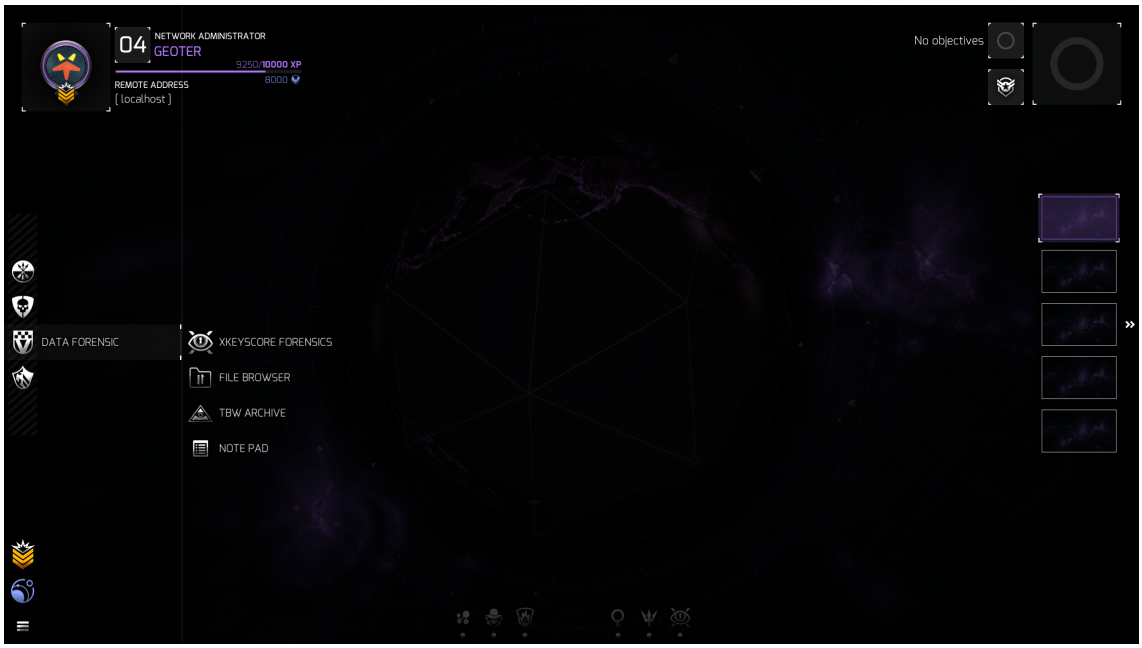
Σχήμα Γ.13: *Η διεπαφή του CID Phone Backdoor με περιεχόμενο στα πλαίσια του σεναρίου της έρευνας*

Πίνακας Γ.2: *Τα πιο χρήσιμα εργαλεία στην κατηγορία Network Intrusion.*

Εργαλείο	**Χρήση εργαλείου**
Foxacid Server	Αξιοποιεί τις αδυναμίες ενός δικτύου ή συστήματος για να αποκτήσει πρόσβαση
Phone CID Backdoor	Χρησιμοποιεί τη MAC Address ενός κινητού τηλεφώνου καθώς και τη μάρκα του για να αποκτήσει πρόσβαση στη συσκευή
Password Attack	Βρίσκει τον κωδικό που αντιστοιχεί σε κάποιο *κατακερματισμένο κωδικό* (password hash) ή εντοπίζει τον κωδικό που αντιστοιχεί σε κάποιο χρήστη
MitM	Πραγματοποιεί επίθεση Man in the Middle μεταξύ δύο *διευθύνσεις διαδικτυακού πρωτοκόλλου* (IP address)
Social Engineering Toolkit	Πραγματοποιεί επίθεση spear-phishing στοχεύοντας συγκεκριμένα email ή τα email που χρησιμοποιεί κάποια εταιρεία

Γ.1.3 Data Forensic

Το Data Forensic έχει λιγότερα εργαλεία σε σχέση με τις άλλες κατηγορίες, προσφέροντας ένα συνδυασμό λειτουργιών. Το XKeyscore Forensics, εμπνευσμένο από το σύστημα XKeyscore που χρησιμοποιεί η Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ, αποτελεί μια γιγαντιαία βάση με πληροφορίες σε συγκεκριμένα άτομα. Κατά τη διάρκεια του παιχνιδιού, το παιχνίδι προσθέτει



Σχήμα Γ.14: *Τα εργαλεία της κατηγορίας Data Forensic*

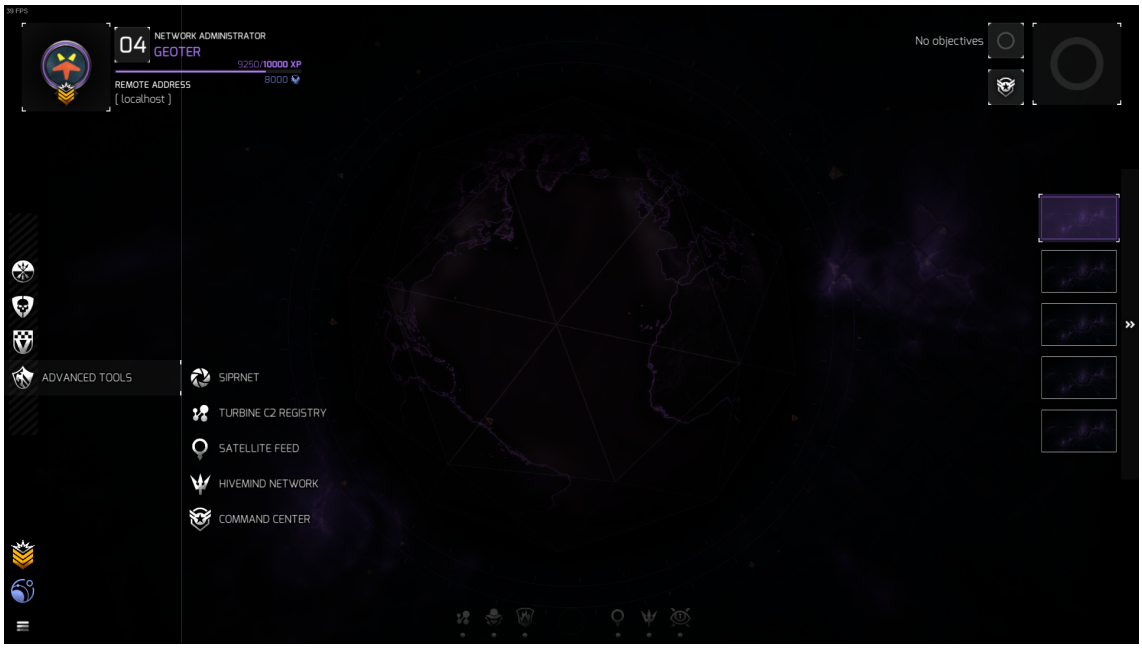
τα ονόματα σημαντικών ατόμων ή οργανισμών στο XKeyscore. Στη συνέχεια, ο παίκτης μπορεί να επιλέξει έως τρία άτομα ή οργανισμούς και να βρει έγγραφα ή συναλλαγές που ενδεχομένως να ταιριάζουν με τα επιλεγμένα άτομα. Αυτό πραγματοποιείται αξιοποιώντας τα φίλτρα που προσφέρει το ίδιο το XKeyscore. Για παράδειγμα, ο παίκτης μπορεί να βρει την ταυτότητα ενός ατόμου, ή να εντοπίσει μία συναλλαγή μεταξύ ένα άτομο και μία επιχείρηση, προσφέροντας σημαντικές πληροφορίες για το άτομο. Το File Browser είναι ο τρόπος με τον οποίο ο παίκτης μπορεί να περιηγηθεί τα directories τα οποία έχει εντοπίσει. Έχει την ίδια γραφική διεπαφή με το Active Directory που αναφέρεται στο κεφάλαιο Γ.1.1. Με το *TBW* (The Black Watchmen) Archive ο παίκτης μπορεί να συνδεθεί με το αρχείο του Black Watchmen. Συχνά το εργαλείο χρησιμοποιείται για το ARG τμήμα των αποστολών για να αποκτήσει πρόσβαση σε πληροφορίες σχετικά με τη συγκεκριμένη αποστολή. Τέλος, το Note Pad δεν έχει κάποια συγκεκριμένη λειτουργία και αποτελεί ένα μέρος για τον παίκτη να σημειώσει ή να καταγράψει στοιχεία που θεωρεί είναι σημαντικά για την πρόοδο του στο παιχνίδι.



Σχήμα Γ.15: *Το εργαλείο XKeyscore, με δεδομένα από το σενάριο της εργασίας*

Πίνακας Γ.3: *Τα πιο χρήσιμα εργαλεία στην κατηγορία Data Forensic.*

Εργαλείο	**Χρήση εργαλείου**
XKeyscore	Εντοπίζει σχετικά αρχεία και πληροφορίες μέσω συναλλαγών και επαφών μεταξύ ατόμων για αυτά τα άτομα
File Browser	Χρησιμοποιείται για την περιήγηση των διαφόρων φακέλων του συστήματος
Note Pad	Χρησιμοποιείται για τη σημείωση στοιχείων από τον παίκτη τα οποία ενδεχομένως να τον βοηθήσουν στο παιχνίδι

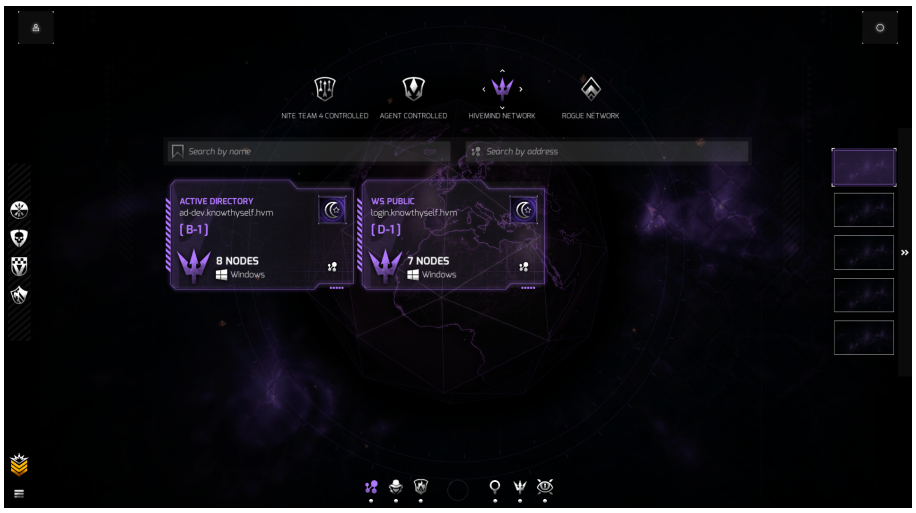


Σχήμα Γ.16: *Τα εργαλεία της κατηγορίας Advanced Tools*

Γ.1.4 Advanced Tools

Τα εργαλεία που βρίσκονται στο Advanced Tools δε χρησιμοποιούνται ιδιαίτερα κατά το παιχνίδι και κατά πλειοψηφία είναι λοιπά εργαλεία σχετικά με τις αποστολές του παιχνιδιού. Το SIPRNet χρησιμοποιείται για να δοθεί στον παίκτη πρόσβαση σε terminals σε συγκεκριμένα ιδιωτικά δίκτυα χωρίς τη χρήση άλλων μεθόδων. Το Turbine C2 Registry καταγράφει τα διάφορα δίκτυα στα οποία ο χρήστης έχει πρόσβαση και τα αποθηκεύει ως κάρτες έτσι ώστε ο παίκτης να έχει άμεση πρόσβαση στην περίπτωση που επιθυμεί να συνδεθεί πάλι σε ένα ευάλωτο δίκτυο. Το Satellite Feed, παρομοίως με το Hydra Terminal, είναι περιορισμένο στη χρήση του και δεν μπορεί να χρησιμοποιηθεί στα πλαίσια του Hivemind Administrator ως εργαλείο. Ο παίκτης μπορεί να εισάγει συντεταγμένες έτσι ώστε να αποκτήσει μία δορυφορική όψη της περιοχής. Στη συνέχεια, ανάλογα την περίπτωση, έχει συγκεκριμένες επιλογές όπως να συνδεθεί απομακρυσμένα σε οποιεσδήποτε έξυπνες συσκευές της περιοχής. Το Hivemind Network είναι η περιοχή στην οποία φαίνονται οι αποστολές που έχουν δημιουργηθεί από άλλους παίκτες. Ο παίκτης μπορεί να διαλέξει από διάφορα φίλτρα και κατηγορίες και να βρει μία αποστολή που να ταιριάζει στις προτιμήσεις του. Καθώς το Hivemind Network είναι συνδεδεμένο με το Hivemind Administrator, το Hivemind Network παρουσιάζει στον παίκτη

και μία πιο απλοποιημένη μορφή του γραφήματος του δικτύου. Τέλος, το Command Center προσφέρει τη δυνατότητα ο παίκτης να συνεργαστεί με άλλους παίκτες για τις αποστολές. Με αυτόν τον τρόπο, όχι μόνο οι παίκτες μπορούν να οργανώσουν καλύτερα τον τρόπο με τον οποίο θα επιτεύξουν τον στόχο τους, έχουν τη δυνατότητα επιπλέον να ανταλλάξουν πληροφορίες μεταξύ τους. Επιπλέον, ο χρήστης κατά τη διάρκεια του παιχνιδιού μπορεί να αποθηκεύσει ορισμένα σημαντικά ευρήματα, τα οποία εμφανίζονται εδώ.



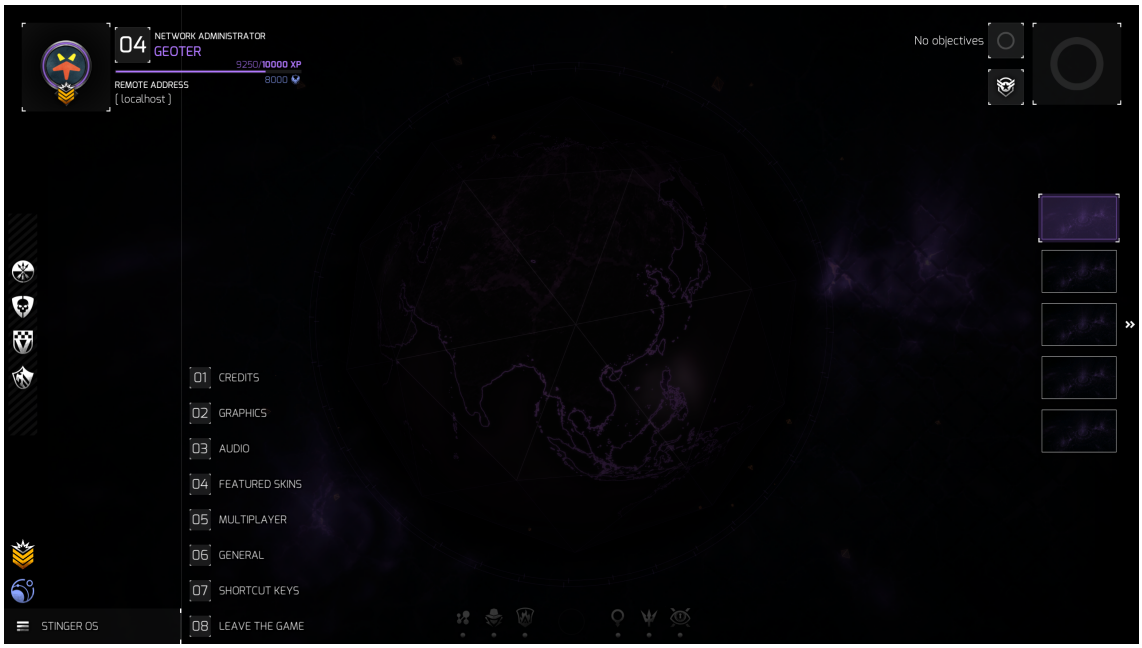
Σχήμα Γ.17: *Το εργαλείο Turbine C2 Registry, με δύο κάρτες πρόσβασης*

Πίνακας Γ.4: *Τα πιο χρήσιμα εργαλεία στην κατηγορία Advanced Tools.*

Εργαλείο	**Χρήση εργαλείου**
Turbine C2 Registry	Με την επιτυχή παραβίαση ενός δικτύου, δημιουργείται μία σύνδεση *εικονικού ιδιωτικού δικτύου* (Virtual Private Network - VPN) και αποθηκεύονται τα στοιχεία του δικτύου ως μία εύκολα προσβάσιμη κάρτα
Hivemind Network	Χρησιμοποιείται για την περιήγηση του περιεχομένου που έχει δημιουργηθεί από άλλους χρήστες στα πλαίσια του Hivemind Network Administrator
Command Center	Παρουσιάζονται τα αποθηκευμένα στοιχεία (αρχεία, φωτογραφίες, γενικά ίχνη κτλ) που έχει βρει ο παίκτης. Επιπλέον, έχει τη λειτουργία οργάνωσης συμμετοχικού περιεχομένου μεταξύ των παικτών

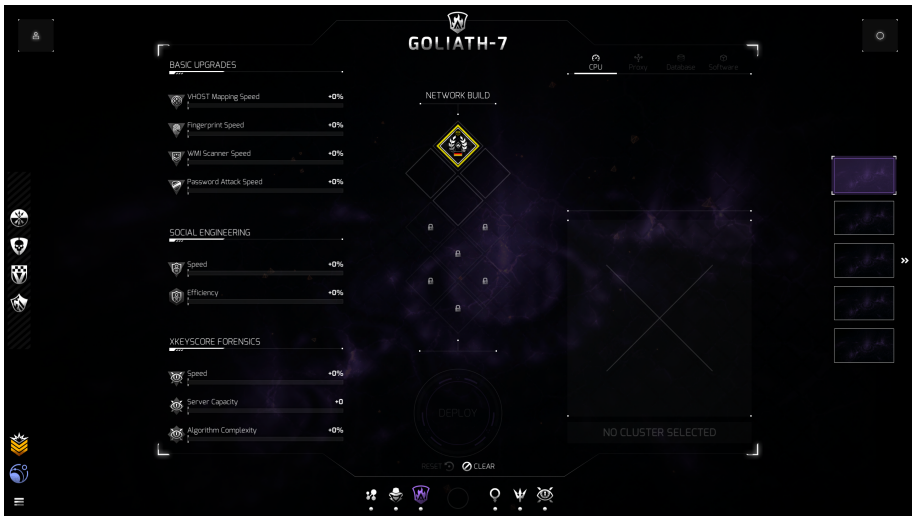
Γ.1.5 Λοιπά στοιχεία UI/UX

Στην κάτω αριστερή πλευρά της οθόνης, φαίνεται το Network Administrator, το οποίο θα αναλυθεί εκτεταμένα στο κεφάλαιο Δ, αλλά και γενικές ρυθμίσεις για το Stinger OS. Ο



Σχήμα Γ.18: *Οι ρυθμίσεις του Stinger OS*

παίκτης μπορεί να ρυθμίσει τις προτιμήσεις του για το παιχνίδι όπως τον ήχο, ποιότητα γραφικών, τη λειτουργία των πλήκτρων και άλλες γενικές ρυθμίσεις.



Σχήμα Γ.19: *Το εργαλείο Goliath-7*

Στο κάτω τμήμα της οθόνης, εμφανίζονται διάφορα από τα εργαλεία που μπορεί να χρησι-

μοποιήσει ο χρήστης για πιο άμεση και εύκολη πρόσβαση. Εξαίρεση αυτών είναι το Goliath-7 εργαλείο, το οποίο δεν εμφανίζεται σε καμία από τις κατηγορίες των εργαλείων και η πρόσβαση του γίνεται μόνο από αυτό το τμήμα. Με το Goliath-7, ο παίκτης μπορεί να αναβαθμίσει το Stinger OS, έτσι ώστε να είναι πιο αποδοτικό και να εκπληρώνει πιο γρήγορα τις διεργασίες. Οι αναβαθμίσεις είναι σε τρεις κύριες κατηγορίες, με την πρώτη να είναι γενικές αυξήσεις αποδοτικότητας, η δεύτερη να είναι σχετικά με την ταχύτητα και αποδοτικότητα του Social Engineering Toolkit και η τρίτη να αυξάνει την ταχύτητα του XKeyscore καθώς βελτιώνει τη χωρητικότητα και την ικανότητα του επεξεργαστή για να μπορεί να πραγματοποιήσει πιο περίπλοκες διεργασίες. Υπάρχουν επίσης επιπρόσθετες αναβαθμίσεις, που προσφέρουν στον παίκτη επιπλέον βελτιώσεις ή ακόμα και νέες λειτουργίες.



Σχήμα Γ.20: *Όταν η F.A.Y επικοινωνεί με τον παίκτη, αντιπροσωπεύεται και οπτικά στο κάτω δεξιά τμήμα της οθόνης*

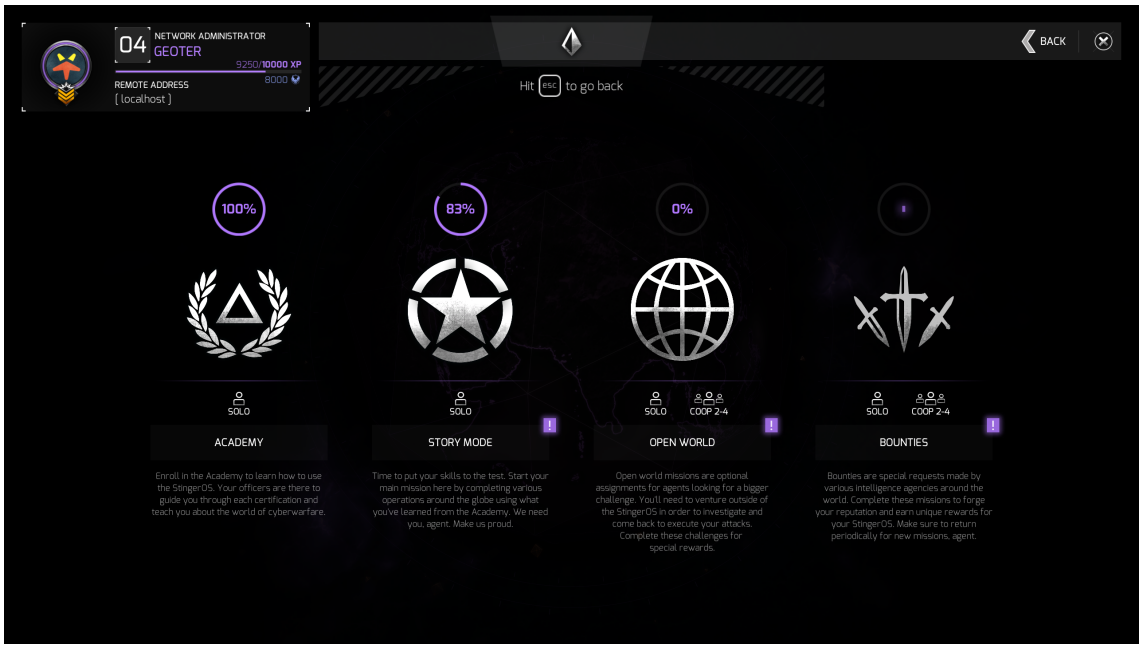
Σημαντικό τμήμα του user experience είναι η ύπαρξη της F.A.Y. Η F.A.Y αποτελεί ένα είδος βοηθού *τεχνητής νοημοσύνης* (Artificial Intelligence - AI), συνοδεύοντας διάφορες πράξεις του παίκτη με κάποιου είδους ηχητική ανάδραση. Συχνά αυτά τα ηχητικά μηνύματα χρησιμοποιούνται με την εκκίνηση κάποιου εργαλείου ή με την εκτέλεση συγκεκριμένων διεργασιών στα πλαίσια του εργαλείου και αναφέρουν πως η αντίστοιχη εκκίνηση ή εκτέλεση έχει πραγματοποιηθεί επιτυχώς ή ανεπιτυχώς. Η ύπαρξη της F.A.Y δεν αποτελεί υποχρεωτικό

στοιχείο του παιχνιδιού καθώς οι πληροφορίες που παρέχει εμφανίζονται και οπτικά στην οθόνη. Ωστόσο, βελτιώνει την εμπειρία του παίκτη προσφέροντας ηχητικά ερεθίσματα για μία πιο πλήρη εμπειρία.

Στα δεξιά της οθόνης, ο παίκτης έχει πρόσβαση σε διαφορές μονάδες του Stinger OS έτσι ώστε να έχει την ικανότητα να οργανωθεί καλύτερα το σύστημα στην περίπτωση που έχουν αξιοποιηθεί πολλά εργαλεία ή θέλει ο χρήστης να τα διαχωρίσει.

Στο πάνω αριστερό τμήμα της οθόνης, υπάρχει μία συντόμευση για το Command Center εργαλείο, στοιχεία για την τωρινή αποστολή του παίκτη, καθώς και το κεντρικό μενού τον αποστολών. Πατώντας το, ο παίκτης μπορεί να παίξει τις διάφορες αποστολές του παιχνιδιού.

Γ.2 Οι αποστολές του NITE Team 4



Σχήμα Γ.21: *Το κύριο μενού αποστολών*

Οι αποστολές του NITE Team 4 χωρίζονται σε τέσσερις κατηγορίες, με την κάθε μια να προσφέρει διαφορετικό είδος περιεχομένου: το Academy, το Story Mode, το Open World και το Bounties. Οι παίκτες κυρίως θα αξιοποιήσουν το Academy στην αρχή του παιχνιδιού και στη συνέχεια μπορούν να προχωρήσουν στο επόμενο περιεχόμενο που προσφέρει το παιχνίδι.

Επιπλέον, εκτός από το περιεχόμενο που προσφέρει το παιχνίδι, υπάρχουν και αποστολές που άλλοι χρήστες έχουν δημιουργήσει. Ο παίκτης μπορεί να εξερευνήσει το περιεχόμενο στο εργαλείο Hivemind Network όπως αναφέρεται στο κεφάλαιο Γ.1.4. Συγκεκριμένα, για τις αποστολές στις κατηγορίες Open World, Bounties και Hivemind Network, ο παίκτης μπορεί να συνεργαστεί με άλλους παίκτες για να ολοκληρώσουν την αποστολή.

Γ.2.1 Academy



Σχήμα Γ.22: *Οι αποστολές του τμήματος Basic Terminal Operations στην κατηγορία Academy*

Οι αποστολές του Academy έχουν ένα κύριο σκοπό, να βοηθήσει τον παίκτη να κατανοήσει το Stinger OS και τις δυνατότητες του. Πριν αρχίσει καν ο παίκτης τις άλλες αποστολές, πρέπει πρώτα να παίξει τις αποστολές που υπάρχουν στο Basic Terminal Operations. Σε αυτές τις αποστολές, ο παίκτης μαθαίνει τη γενική νοοτροπία του πως να κάνει scan ένα δίκτυο, να εντοπίζει αδυναμίες και έπειτα ανάλογα με τις αδυναμίες που υπάρχουν να πραγματοποιήσει την ανάλογη επίθεση. Για επαυξημένη διάδραση, υπάρχουν διάφορα ηχητικά μηνύματα από χαρακτήρες του παιχνιδιού έτσι ώστε να καθοδηγήσουν τον παίκτη, προσφέροντας μία σύνοψη της αποστολής και μετά προσφέροντας συμβουλές ή βοήθεια κατά την εκτέλεση της αποστολής. Οι δύο πιο συχνοί χαρακτήρες είναι η λοχίας Wheeler, η οποία συνήθως προσφέρει

τη σύνοψη και την εισαγωγή για μία αποστολή, εξηγώντας τα γεγονότα, και ο πράκτορας Dylan, ο οποίος είναι πράκτορας της ομάδας όπως και ο παίκτης. Λόγω της εμπειρίας του, κατά τη διάρκεια των αποστολών εξηγεί στον παίκτη διάφορες λειτουργίες ενώ τον καθοδηγεί προς τους στόχους της αποστολής. Η Wheeler και ο Dylan δεν είναι οι μόνοι χαρακτήρες ωστόσο, υπάρχουν και επιπλέον χαρακτήρες με τους αντίστοιχους ρόλους τους. Όταν ο παίκτης ολοκληρώσει το Basic Terminal Operations, έχει πλέον πρόσβαση και στις άλλες τρεις κατηγορίες, ενώ έχει την επιλογή είτε να ξαναπαίξει τις εκπαιδευτικές αποστολές, είτε να δοκιμάσει καινούριες για να τον προετοιμάσουν για τις υπόλοιπες λειτουργίες του Stinger OS.

Γ.2.2 Story Mode



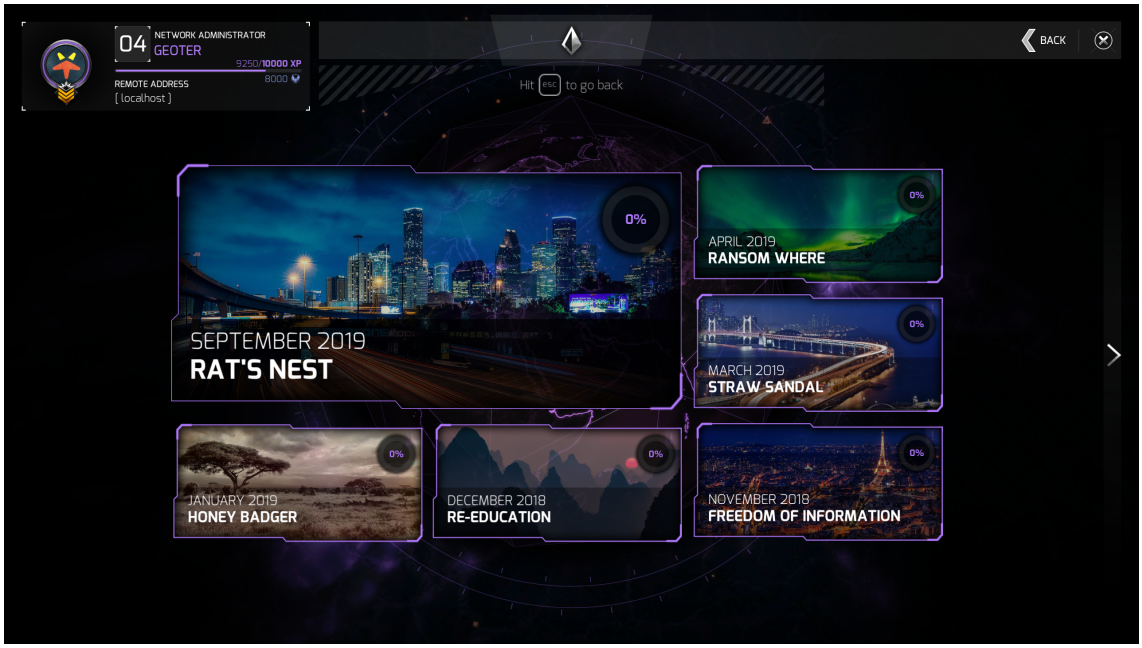
Σχήμα Γ.23: *Το μενού επιλογής αποστολών στην κατηγορία Story Mode*

Στο Story Mode βρίσκεται το κύριο τμήμα του περιεχομένου καθώς και η πλοκή της ιστορίας του παιχνιδιού. Η κύρια ιστορία διαχωρίζεται σε τέσσερις επιχειρήσεις, με την κάθε μια να είναι συνέχεια της προηγούμενης. Όπως και πριν, ο παίκτης είναι πράκτορας του NITE Team 4. Στόχος του είναι να βρει πληροφορίες σχετικά με την κλοπή κακόβουλου λογισμικού που χρησιμοποιεί το ίδιο το NITE Team 4 καθώς μπορεί να προκαλέσει τεράστιες ζημιές στα λάθος χέρια. Όσο ο παίκτης ακολουθεί τα ίχνη που βρίσκει, καταλαβαίνει ότι η κλοπή

αυτή κρύβει πολλά περισσότερα πράγματα από πίσω, στο σημείο όπου ο παίκτης πρέπει να συνεργαστεί και με διάφορες κρατικές υπηρεσίες από όλο τον κόσμο για να βρει το λογισμικό και τον εγκληματία.

Τον Νοέμβριο του 2019, οι Alice & Smith πρόσθεσαν μία καινούρια αποστολή ως περιεχόμενο επί πληρωμή. Με το όνομα Operation Withering Dusk, η αποστολή αφορά μια σημαντική παραβίαση δεδομένων σε μία φανταστική εταιρεία που υπάρχει στα πλαίσια του παιχνιδιού, την Kotok Analytics. Ο παίκτης πρέπει να ερευνήσει την παραβίαση και να βρει τι πραγματικά κρύβεται πίσω από αυτή την επίθεση. Το περιεχόμενο εκτός από την αποστολή που προσθέτει, χωρισμένη σε 5 υπο-αποστολές, προσθέτει επιπλέον λειτουργίες στο Hydra Terminal καθώς δίνει μία επιπλέον μέθοδο επίθεσης στο εργαλείο Phone CID Backdoor. Τέλος, υπάρχει ένα καινούριο εργαλείο, το Uplink51. Σε αυτό το εργαλείο, ο παίκτης μπορεί να χρησιμοποιήσει τη F.A.Y ως AI συνομιλητής. Ο παίκτης μπορεί να επικοινωνήσει μαζί της, καθώς και να χρησιμοποιήσει διάφορες λειτουργίες της όπως η εκτέλεση εργαλείων, να βρει συγκεκριμένα αρχεία με βάση τον αναγνωριστικό κωδικό τους και άλλα.

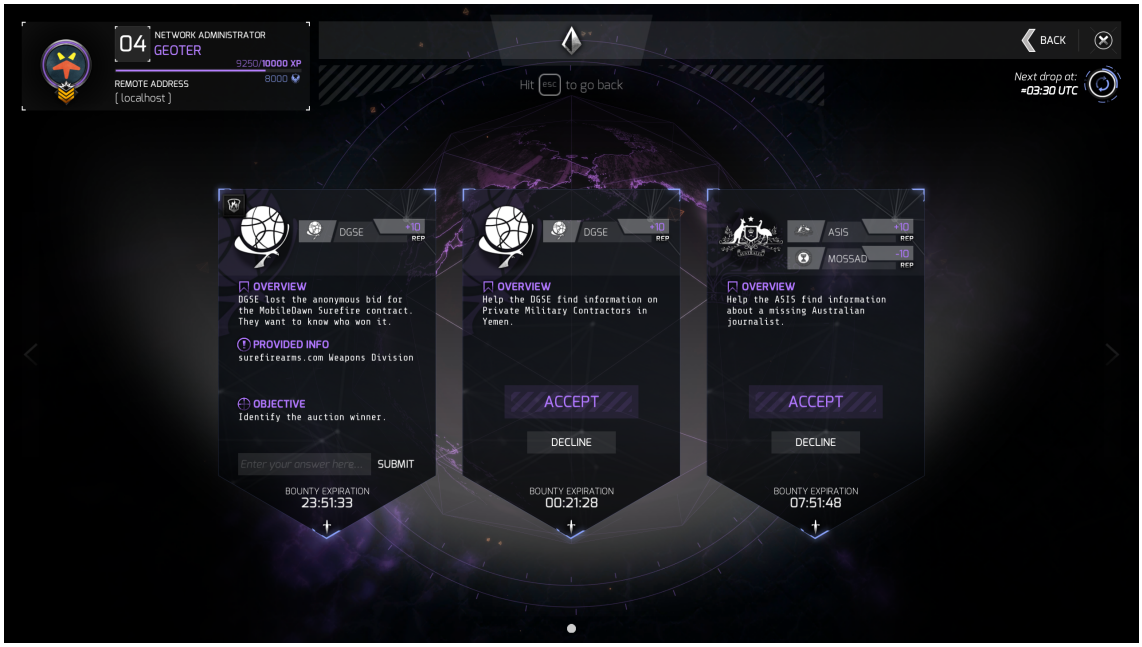
Γ.2.3 Open World



Σχήμα Γ.24: *Το μενού επιλογής αποστολών στην κατηγορία Open World*

Οι αποστολές στο Open World έχουν αρκετά διαφορετικά χαρακτηριστικά που τις κάνουν να διαφέρουν σε σχέση με το Story Mode. Οι αποστολές αυτές είναι ξεχωριστές με την κάθε μία, και δεν υπάρχει κάποια σύνδεση, όμως όλες έχουν κάποιο συγκεκριμένο σενάριο γύρω από την αποστολή. Καθώς δεν είναι κομμάτι της ιστορίας, δεν υπάρχει η παρουσία των χαρακτήρων που υπάρχουν στο Academy και στο Story Mode, δίνοντας πολύ μεγαλύτερη έμφαση στην ίδια την αποστολή. Το πιο ιδιαίτερο κομμάτι όμως, είναι η ύπαρξη ARG στοιχείων. Σε όλες τις διαθέσιμες αποστολές, ο χρήστης θα πρέπει να ψάξει εκτός του Stinger OS, πολύ συχνά με τη χρήση του διαδικτύου έτσι ώστε να βρει στοιχεία προς την αποστολή του. Για να βοηθήσουν τον παίκτη, κάθε σενάριο συνοδεύεται από ένα αρχείο εξηγώντας την κατάσταση, ταυτόχρονα προτείνοντας ένα μέρος για να ξεκινήσει στον ιστό την έρευνα ο παίκτης. Πολύ συχνά υπάρχουν επιπλέον στοιχεία και στα αρχεία του The Black Watchmen. Οι αποστολές χωρίζονται σε τρία μέρη, και η ολοκλήρωση των διαδοχικών τμημάτων δίνει στον παίκτη πόντους εμπειρίας για την αύξηση του επιπέδου του στο παιχνίδι καθώς και καινούρια χαρακτηριστικά για να τροποποιήσει το προφίλ του.

Γ.2.4 Bounties



Σχήμα Γ.25: *Το μενού επιλογής αποστολών στην κατηγορία Bounties με μία επιλεγμένη αποστολή*

Η κατηγορία των Bounties είναι εξίσου διαφορετική συγκριτικά με τις άλλες κατηγορίες αποστολών. Σε αυτή, υπάρχει μία λίστα κατηγοριών, όπου σε τακτά χρονικά διαστήματα, γίνεται διαθέσιμη μία από αυτές τις αποστολές, συνήθως για μία ώρα. Αν ο χρήστης δεν ολοκληρώσει την αποστολή στο χρονικό διάστημα που είναι διαθέσιμη, η αποστολή σταματάει να είναι διαθέσιμη. Ωστόσο, δε χάνεται για πάντα, καθώς μπορεί να γίνει πάλι διαθέσιμη. Επιπλέον, οι συγκεκριμένες αποστολές δεν είναι από την ομάδα του NITE Team 4 που βρίσκεται στο παιχνίδι όπως στις προηγούμενες τρεις κατηγορίες, αλλά παρέχονται από άλλα πρακτορεία από διάφορες χώρες. Με την εκπλήρωση της αποστολής, ο παίκτης κερδίζει μοναδικές επιβραβεύσεις καθώς και πόντους προς το συγκεκριμένο πρακτορείο. Όσο ο παίκτης ολοκληρώνει περισσότερες αποστολές, η λίστα με τις διαθέσιμες αποστολές μεγαλώνει, προσφέροντας καινούριο περιεχόμενο.

Γ.2.5 Hivemind Network



Σχήμα Γ.26: *Το μενού επιλογής αποστολών στο Hivemind Network*



Σχήμα Γ.27: *Επιλεγμένη αποστολή στο Hivemind Network*

Το τελευταίο είδος αποστολών το οποίο ωστόσο δεν εμπεριέχονται στο μενού με τις προηγούμενες αποστολές, είναι το Hivemind Network. Ο παίκτης μπορεί να αποκτήσει πρόσβαση μέσω του ομώνυμου εργαλείου στο Advanced Tools. Εκεί ο παίκτης μπορεί να επιλέξει αποστολές που έχουν δημιουργήσει άλλοι παίκτες μέσω του Hivemind Network. Ο παίκτης μπορεί να επιλέξει την αποστολή που θέλει με βάση το είδος της αποστολής, τον εκτιμώμενο χρόνο ολοκλήρωσης και το επίπεδο δυσκολίας. Επιπλέον, έχει την επιλογή να διαλέξει μεταξύ τις πιο καινούριες αποστολές, αυτές που έχει ολοκληρώσει ήδη, εκείνες που το ίδιο το παιχνίδι προτείνει ή έχει τη δυνατότητα απλά να εισάγει το όνομα της αποστολής εφόσον το γνωρίζει. Όσο ο παίκτης δημιουργεί πρόοδο στην αποστολή, δημιουργείται ένα γράφημα του δικτύου, παρόμοιο με αυτό που φαίνεται στο Network Administrator. Με την ολοκλήρωση της αποστολής, ο παίκτης μπορεί να δώσει κριτική στην αποστολή, βαθμολογώντας τη δυσκολία, την ποιότητα του περιεχομένου, πόσο διασκεδαστικό είναι καθώς και τον χρόνο ολοκλήρωσης.

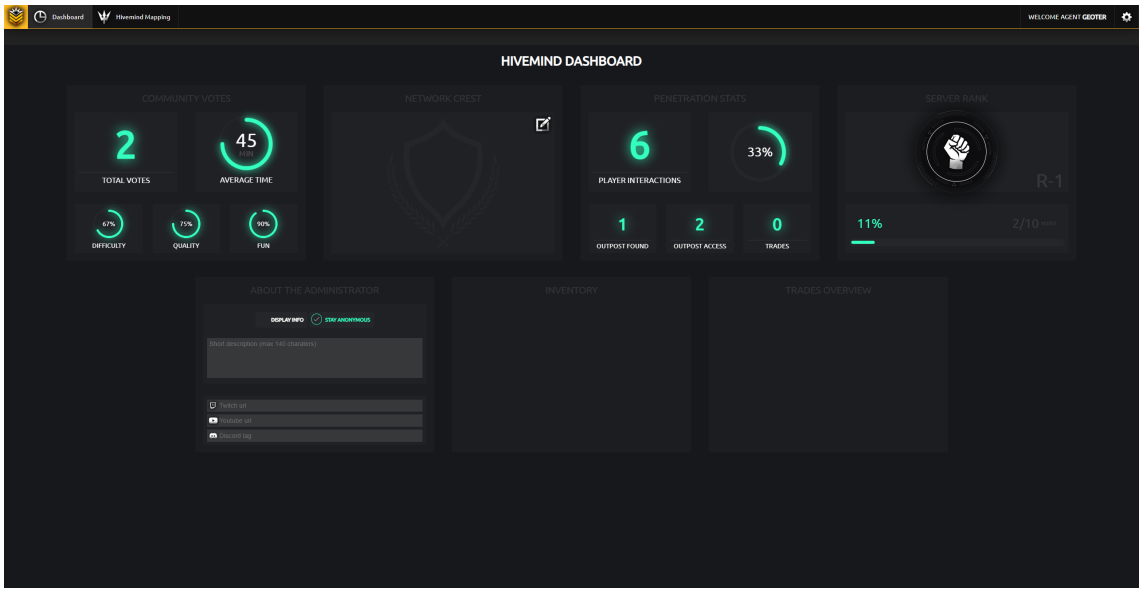
Κεφάλαιο Δ

Δημιουργία σεναρίων στο NITE Team 4

Για την υλοποίηση και τη δημιουργία σεναρίων μέσω του NITE Team 4 από τους παίκτες, απαιτείται η χρήση του επιπρόσθετου περιεχομένου επί πληρωμή, το Hivemind Network Administrator. Με την αγορά του περιεχομένου, ο χρήστης έχει πρόσβαση στο Hivemind Network μέσω του παιχνιδιού. Εναλλακτικά, καθώς η πλατφόρμα βρίσκεται στο διαδίκτυο, με τη χρήση φυλλομετρητή ο χρήστης μπορεί απλά να εισάγει τα στοιχεία του στην ανάλογη ιστοσελίδα.

Δ.1 Παρουσίαση πλατφόρμας για τη δημιουργία σεναρίων

Με την είσοδο του χρήστη στην πλατφόρμα, εμφανίζεται το κεντρικό μενού, στο οποίο παρουσιάζονται διάφορα στοιχεία. Ο χρήστης μπορεί να δει τα στατιστικά του σεναρίου του από τα άτομα τα οποία ολοκλήρωσαν και βαθμολόγησαν τον παιχνίδι. Ο χρήστης μπορεί επιπλέον να δει πόσα άτομα ανακάλυψαν το ολοκληρωτικό flag και πόσα άτομα βρήκαν το σωστό όνομα χρήστη και κωδικό για το flag. Ο χρήστης μπορεί επιπλέον να δημιουργήσει ένα εικονίδιο-έμβλημα για το δίκτυο του σεναρίου, καθώς και να γράψει μια περιγραφή για τον ίδιο με την ικανότητα να προβάλλει τους λογαριασμούς κοινωνικής δικτύωσης του. Τέλος, παρουσιάζεται ένα κατάλογος με τα αντικείμενα που έχει συλλέξει ο χρήστης παίζοντας τα σενάρια άλλων παικτών. Με την ολοκλήρωση ενός σεναρίου, ο δημιουργός μπορεί να τοποθετήσει ένα είδος αντικειμένου, το οποίο ο παίκτης μπορεί να ανταλλάξει με άλλους παίκτες.

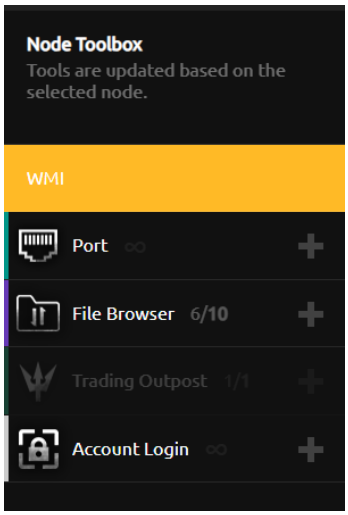


Σχήμα Δ.28: *Το κύριο μενού του χρήστη στο Hivemind Network Administrator*

Ωστόσο, αυτή η λειτουργικότητα δεν αναπτύχθηκε περαιτέρω και δεν προσφέρει κάποιο είδος πλεονέκτημα ή επιβράβευση στον χρήστη παρά την ύπαρξη μια συνοπτικής συλλογής.

Η κύρια λειτουργία του Hivemind Network παρουσιάζεται στο Hivemind Mapping όπως φαίνεται στο σχήμα *B*.3. Εκεί, ο παίκτης διαθέτει την πλήρη λειτουργικότητα της πλατφόρμας για να δημιουργήσει το σενάριο του. Κάθε σενάριο έχει έναν Hivemind Network κόμβο, στον οποίο ρυθμίζεται το όνομα του δικτύου, το domain του καθώς και η κατηγορία στην οποία βρίσκεται. Το domain του δικτύου έχει τη μη αληθινή κατάληξη ".hvm". Επιπλέον, στο δίκτυο πρέπει να υπάρχει ένα public και ένα private *ακραίο σημείο επικοινωνίας* (endpoint), μία κάρτα Turbine C2 για το Turbine C2 Registry εργαλείο, καθώς και το Trading Outpost. Στην περίπτωση του Trading Outpost, λειτουργεί ως το τελευταίο *σημείο ελέγχου* (checkpoint) του σεναρίου, με τον χρήστη να πρέπει να εντοπίσει το όνομα χρήστη και τον κωδικό πρόσβασης που αντιστοιχεί στο Trading Outpost. Στην περίπτωση που δεν υπάρχουν αυτοί οι κόμβοι, ο χρήστης έχει τη δυνατότητα να παίξει το δικό του σενάριο, αλλά μόνο σε τοπικό περιβάλλον. Για να το διαμοιράσει δημοσίως, το σενάριο πρέπει να διαθέτει αυτούς τους κόμβους αλλά και ο χρήστης να αποδεχτεί τους όρους χρήσης.

Μέσα στο δίκτυο υπάρχουν υποδίκτυα χωρισμένα σε *δημόσια* (public) και *ιδιωτικά* (private) *υποδίκτυα* (subnets). Μπορεί να υπάρχουν απεριόριστοι αριθμοί από subnets, ωστόσο το σύνολο των endpoints δεν μπορεί να ξεπερνάει τα 50. Τα public subnets μπορούν να έχουν

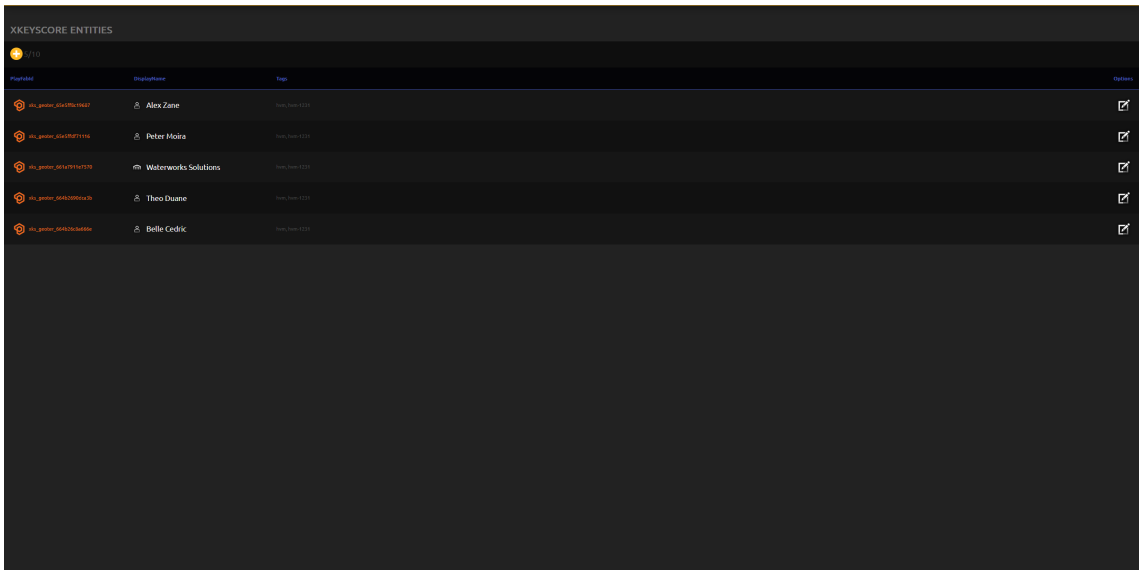


Σχήμα Δ.29: *Παράδειγμα των κόμβων που είναι διαθέσιμοι στο Hivemind Mapping. Στην περίπτωση ενός WMI κόμβου, έχουμε τη δυνατότητα να προσθέσουμε ports, αντίστοιχα file systems, ένα Trading Outpost, και κάποιο λογαριασμό/άτομο που να αντιστοιχεί στον WMI κόμβο.*

μόνο endpoints και τους αντίστοιχους υποκόμβους. Αντιθέτως, τα private subnets είναι συμβατά με κόμβους αφοσιωμένους στα εργαλεία Man in the Middle, WMI Scanner και Air Crack. Με τη χρήση των διαφόρων endpoint και των υπόλοιπων κόμβων, ο χρήστης μπορεί να δημιουργήσει ένα δίκτυο όπως φαίνεται στο σχήμα $B.3$. Ο κάθε κόμβος αντιστοιχεί σε κάποια λειτουργία ή στοιχείο στα πλαίσια του παιχνιδιού, τα οποία ρυθμίζουν τη συμπεριφορά των εργαλείων, την ύπαρξη πληροφοριών, τη διαδρομή που μπορεί να ακολουθήσει ο παίκτης στο σενάριο και άλλα.

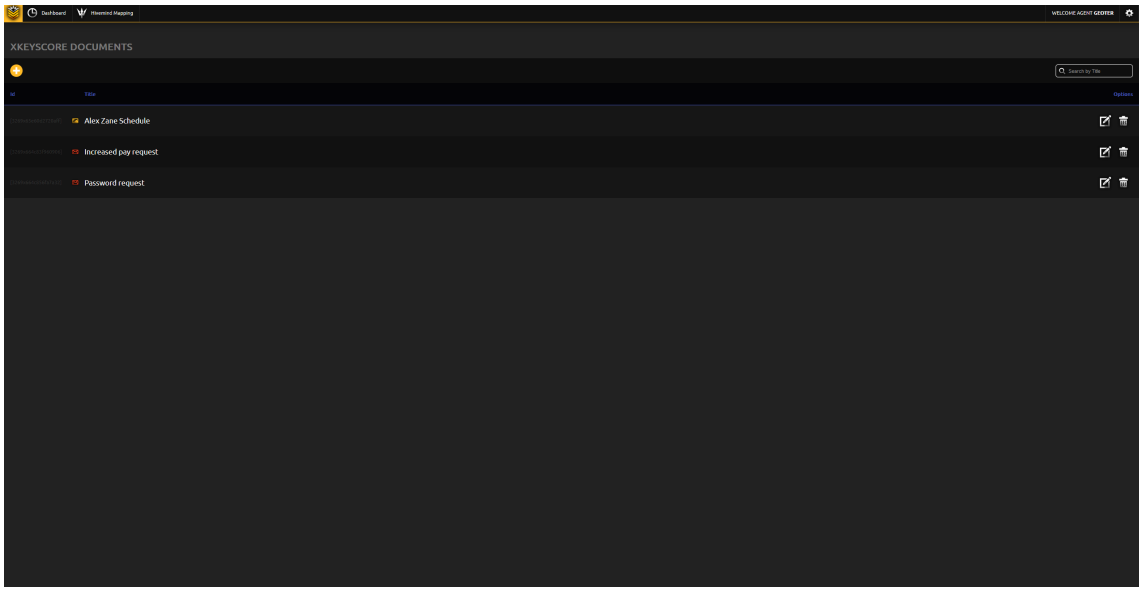
Λόγω της ιδιαιτερότητας του εργαλείου, οι λειτουργίες του XKeyscore ρυθμίζονται από ξεχωριστό τμήμα της πλατφόρμας. Στο XKeyscore Entities παρουσιάζονται οι οντότητες (άτομα ή οργανισμοί) που ανήκουν στο σενάριο. Για κάθε οντότητα υπάρχει ένα αναγνωριστικό, το οποίο ο χρήστης μπορεί να εισάγει στο κόμβο του XKeyscore για να γίνει η αντιστοίχιση με την ανάλογη οντότητα. Στο XKeyscore Documents υπάρχουν τα αρχεία και δεδομένα τα οποία λαμβάνει ο παίκτης με τη σωστή χρήση του XKeyscore. Ο δημιουργός πάλι με τη χρήση του αναγνωριστικού, μπορεί να συσχετίσει διάφορες οντότητες με το ανάλογο τμήμα πληροφορίας. Ως περιεχόμενο, ο δημιουργός μπορεί είτε να εισάγει ένα μήνυμα στη μορφή email, ένα αντίγραφο μιας συνομιλίας ή ανταλλαγής ή μία εικόνα. Στην περίπτωση που το περιεχόμενο που θέλει να εμφανίσει ο δημιουργός δεν ταιριάζει με τα δύο πρώτα είδη, συχνά

πρέπει να το διαμορφώσει στη μορφή εικόνας.



Σχήμα Δ.30: *Η λίστα XKeyscore Entities*

Σε διαφορετικό τμήμα γίνεται και η επεξεργασία των ατόμων που βρίσκονται στο δίκτυο. Τα συγκεκριμένα άτομα ενδεχομένως να μην είναι τα ίδια τα οποία φαίνονται στο XKeyscore καθώς η συσχέτιση τους είναι ανάλογα στη δομή που έχει αξιοποιήσει ο δημιουργός, συχνά ωστόσο υπάρχει επικάλυψη των δύο. Το κάθε άτομο μπορεί να αντιστοιχηθεί με ένα κινητό τηλέφωνο για τη χρήση του εργαλείου Phone CID Backdoor, με ένα όνομα χρήστη και κωδικό πρόσβασης για τη χρήση του εργαλείου Password Attack ή και με τα δύο, όπως φαίνεται στο σχήμα Δ.32. Στη συνέχεια, εφόσον έχουν δημιουργηθεί οι κόμβοι και οι υποκόμβοι του ατόμου, ο δημιουργός μπορεί να εισάγει το άτομο μαζί με τους επιμέρους κόμβους στο ανάλογο σημείο του δικτύου που υποστηρίζει την εισαγωγή ατόμου. Συχνά οι κόμβοι των χρηστών αξιοποιούνται στους κόμβους που αντιστοιχούν στο εργαλείο File Browser, έτσι ώστε να γίνει η συσχέτιση του αντίστοιχου directory με κάποιο άτομο-χρήστη του δικτύου.

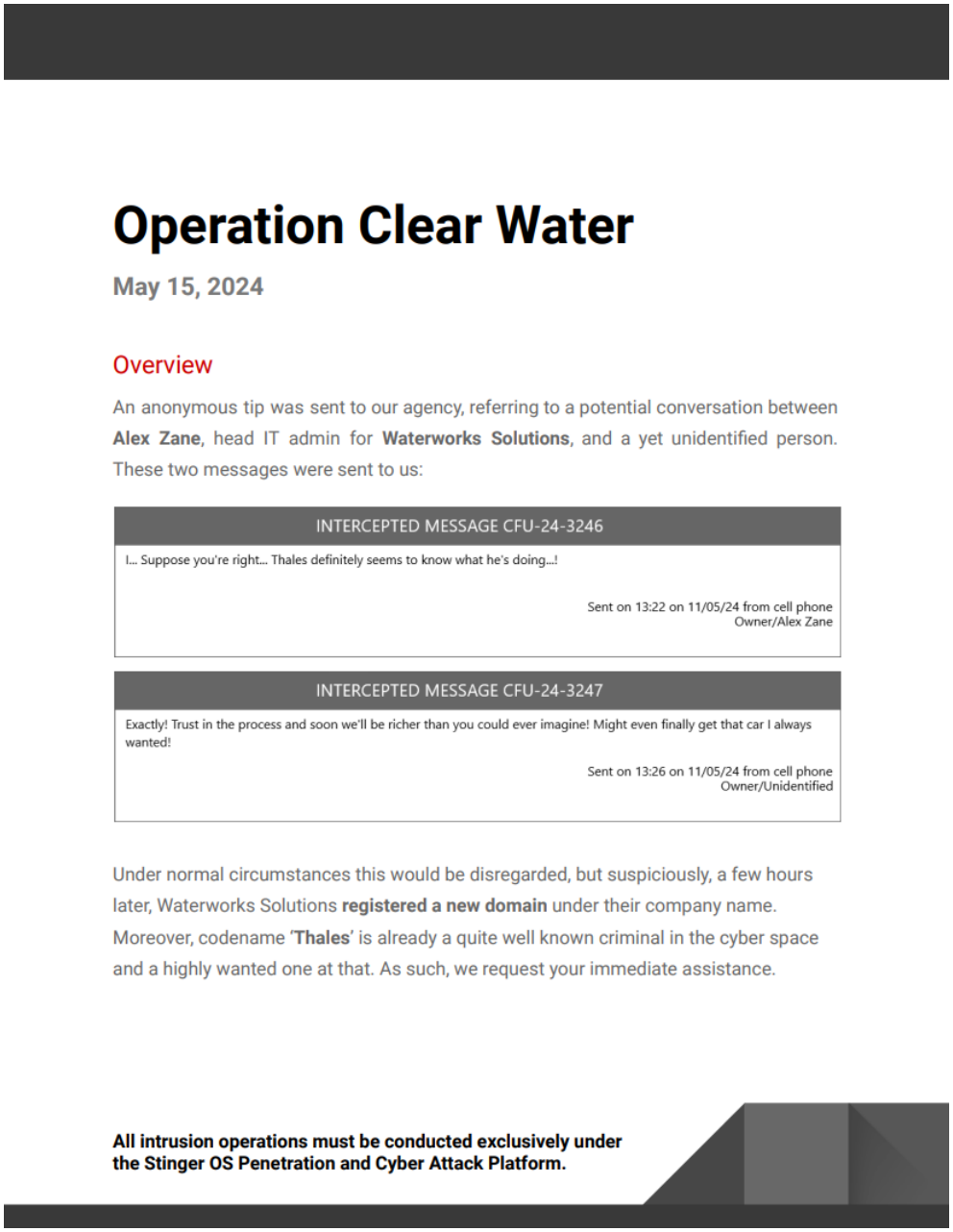


Σχήμα Δ.31: *Η λίστα XKeyscore Documents*



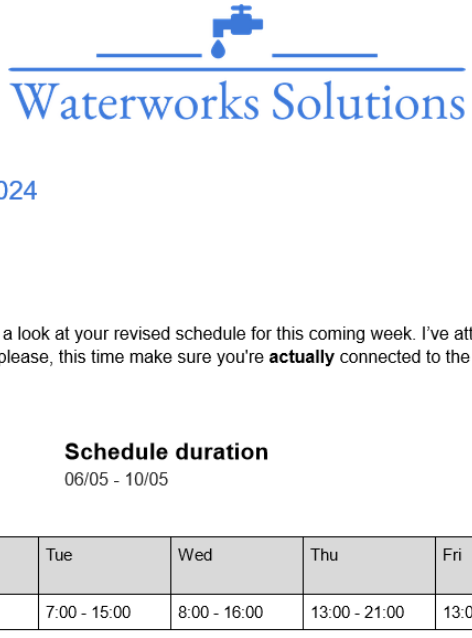
Σχήμα Δ.32: *Η λίστα με τα άτομα τα οποία βρίσκονται στο δίκτυο του σεναρίου*

Δ.2 Παρουσίαση σχεδίασης σεναρίου στο NITE Team 4



Σχήμα Δ.33: *Η πρώτη σελίδα του αρχείου Operation: Clear Water*

Η πλειοψηφία του σεναρίου υλοποιήθηκε στα πλαίσια του Hivemind Network. Για την υποστήριξη του σεναρίου καθώς και για την αύξηση της διαδραστικότητας, δημιουργήθηκαν έγγραφα σε μορφή εικόνας έτσι ώστε να μπορούν να χρησιμοποιηθούν στα πλαίσια του σεναρίου. Δημιουργήθηκε και ένα επιπλέον αρχείο με όνομα Operation: Clear Water, εκτός του παιχνιδιού, που έχει ως σκοπό να αυξήσει περαιτέρω τη διάδραση και να δώσει σημαντικές πληροφορίες στους παίκτες. Το αρχείο χωρίζεται σε τρία τμήματα. Στο πρώτο, αναφέρονται πληροφορίες για την ίδια την αποστολή, καθώς και τον ρόλο του παίκτη στο σενάριο και τους στόχους του. Στο δεύτερο, προσφέρονται επιπρόσθετες πληροφορίες για τα διάφορα εργαλεία του παιχνιδιού έτσι ώστε οι παίκτες να έχουν μία ξεκάθαρη όψη για τη χρησιμότητά της. Σε κάθε περιγραφή, εμπεριέχονται υπερσύνδεσμοι σχετικά με τη λειτουργία του εργαλείου στον πραγματικό κόσμο για τα εργαλεία τα οποία έχουν άμεση ομοιότητα με ένα αληθινό εργαλείο. Τέλος, στο τελευταίο τμήμα υπάρχουν οδηγίες για τη μεθοδολογία που πρέπει να ακολουθήσει ο παίκτης για να αποκτήσει πρόσβαση σε ένα δίκτυο. Καθώς αυτά τα βήματα εμφανίζονται συχνά κατά τη διάρκεια του σεναρίου, η ύπαρξη γραπτών οδηγιών για αυτές τις λειτουργίες είναι χρήσιμες.



Waterworks Solutions

03/05/2024

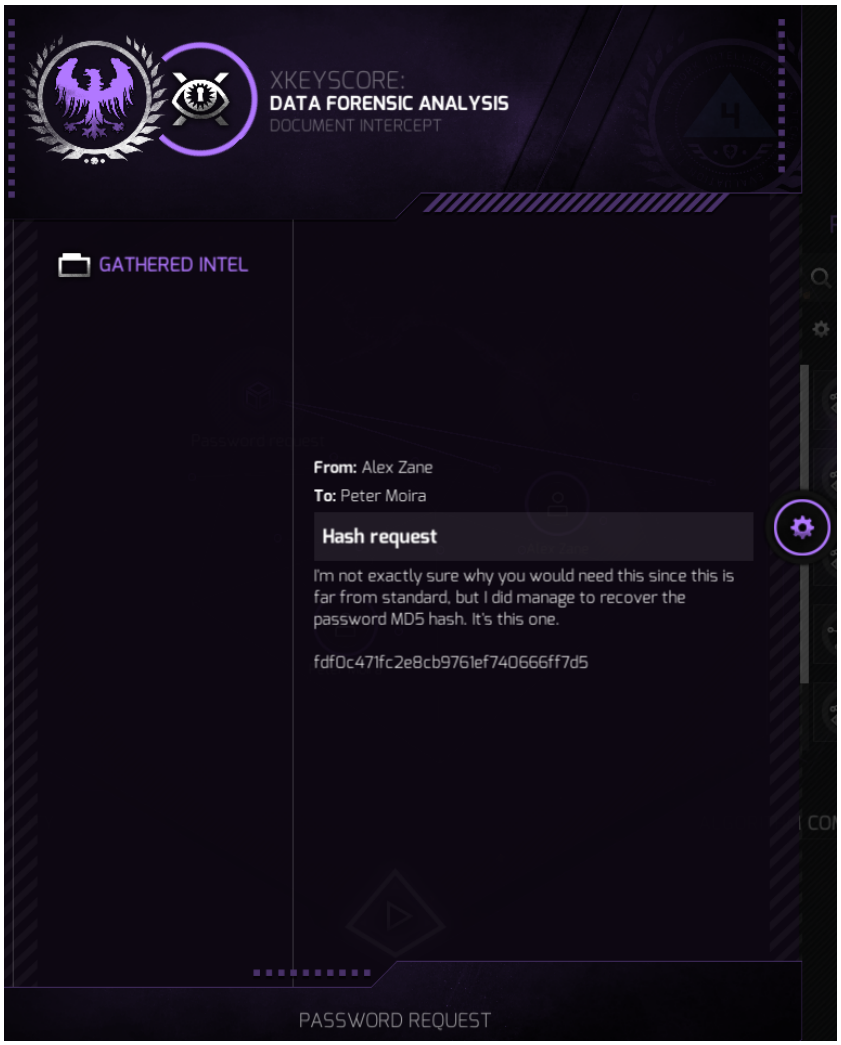
Dear Alex,

Please take a look at your revised schedule for this coming week. I've attached it below. And please, this time make sure you're **actually** connected to the correct WiFi hotspot.

Name	**Schedule duration**
Alex Zane	06/05 - 10/05

Mon	Tue	Wed	Thu	Fri
8:00 - 16:00	7:00 - 15:00	8:00 - 16:00	13:00 - 21:00	13:00 - 21:00

Σχήμα Δ.34: *Παράδειγμα του επιπρόσθετου περιεχομένου που δημιουργήθηκε για το σενάριο. Εμπλουτίζει τον κόσμο του παιχνιδιού ενώ ταυτόχρονα αποτελεί σημαντικό στοιχείο που βοηθάει τον παίκτη να εξερευνήσει περαιτέρω το δίκτυο*



Σχήμα Δ.35: *Παράδειγμα του επιπρόσθετου περιεχομένου που δημιουργήθηκε για το σενάριο. Έχει τη μορφή ενός email το οποίο ο παίκτης εντοπίζει στα πλαίσια της αποστολής του*

Για την υποστήριξη του επιμέρους υλικού που υπάρχει στο σενάριο, δημιουργήθηκε μία πλοκή καθώς και χαρακτήρες γύρω από αυτή. Η πλοκή αποτελεί σημαντικό κομμάτι της εμπειρίας καθώς ο παίκτης έχει κίνητρο για να ακολουθήσει τα στοιχεία που του παρέχονται. Ο παίκτης έχει τη δυνατότητα να εξερευνήσει το δίκτυο περαιτέρω αντί να ακολουθήσει μόνο τις οδηγίες και τους σκοπούς του, προσφέροντας του επιπλέον πληροφορίες σχετικά με την πλοκή και την επίλυση του μυστηρίου γύρω από αυτή. Το περιεχόμενο του παιχνιδιού είναι εμπλουτισμένο με επιπρόσθετο περιεχόμενο, συχνά γραπτής στη μορφή κειμένου. Ο παίκτης ενδεχομένως να

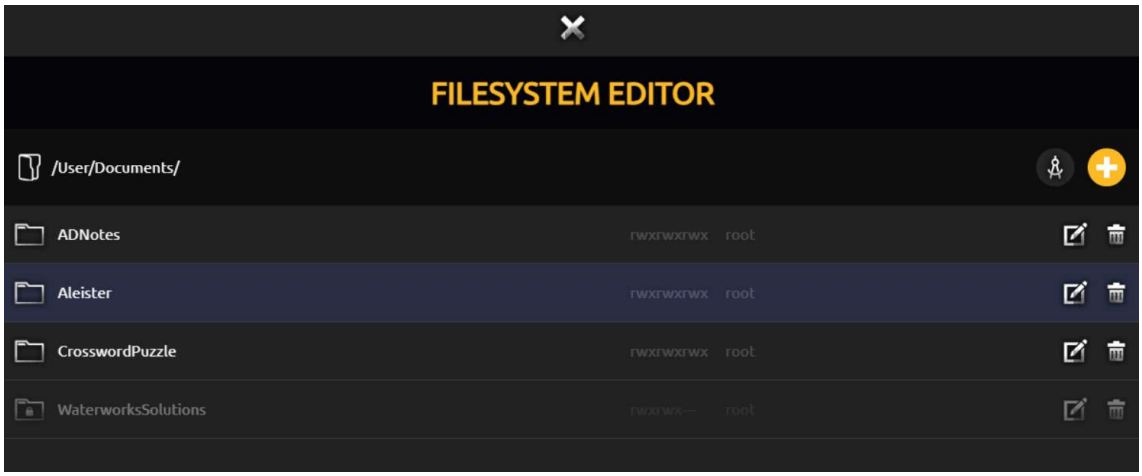
βρει μηνύματα, σημειώσεις ή email μεταξύ χαρακτήρων, βελτιώνοντας τη μορφή διάδρασης του σεναρίου. Αυτά τα στοιχεία βρίσκονται σε διάφορα μέρη του παιχνιδιού, και συχνά αποτελούν μια καθοδήγηση, επεξήγηση της ιστορίας ή απλά εμπλουτίζουν τον κόσμο του παιχνιδιού. Αρκετά από τα εργαλεία που βρίσκονται στο Story Mode για την ενίσχυση της ιστορίας δεν υπάρχουν στο Hivemind Network, οπότε διάφορα τμήματα της ιστορίας είναι δομημένα με τέτοιο τρόπο ώστε η ιστορία να αποτελεί σημαντικό κομμάτι του σεναρίου ακόμη και μέσα στην πλατφόρμα του Stinger OS.



Σχήμα Δ.36: *Τμήμα του γρίφου στην πλατφόρμα X/Twitter*

Το σενάριο επιπλέον διαθέτει διάφορα στοιχεία ενός ARG. Η πλοκή της ιστορίας είναι συνδεδεμένη με μία φανταστική εταιρεία στον χώρο του νησιού της Κέρκυρας, τη Waterworks So-

lutions, και παρόλο που δεν αναφέρεται ξεκάθαρα στα πλαίσια του σεναρίου για να διατηρηθεί απλότητα, υπάρχουν μυστικά στοιχεία που σηματοδοτούν την πιθανή σύνδεση. Το πρώτο αρχείο που λαμβάνει ο παίκτης και τους προσφέρει την εισαγωγή αποτελεί το rabbit hole ενώ εμείς έχουμε τον ρόλο του puppet master, διαθέτοντας ένα συνεργατικό ρόλο μαζί με τους χαρακτήρες που υπάρχουν στο σενάριο.

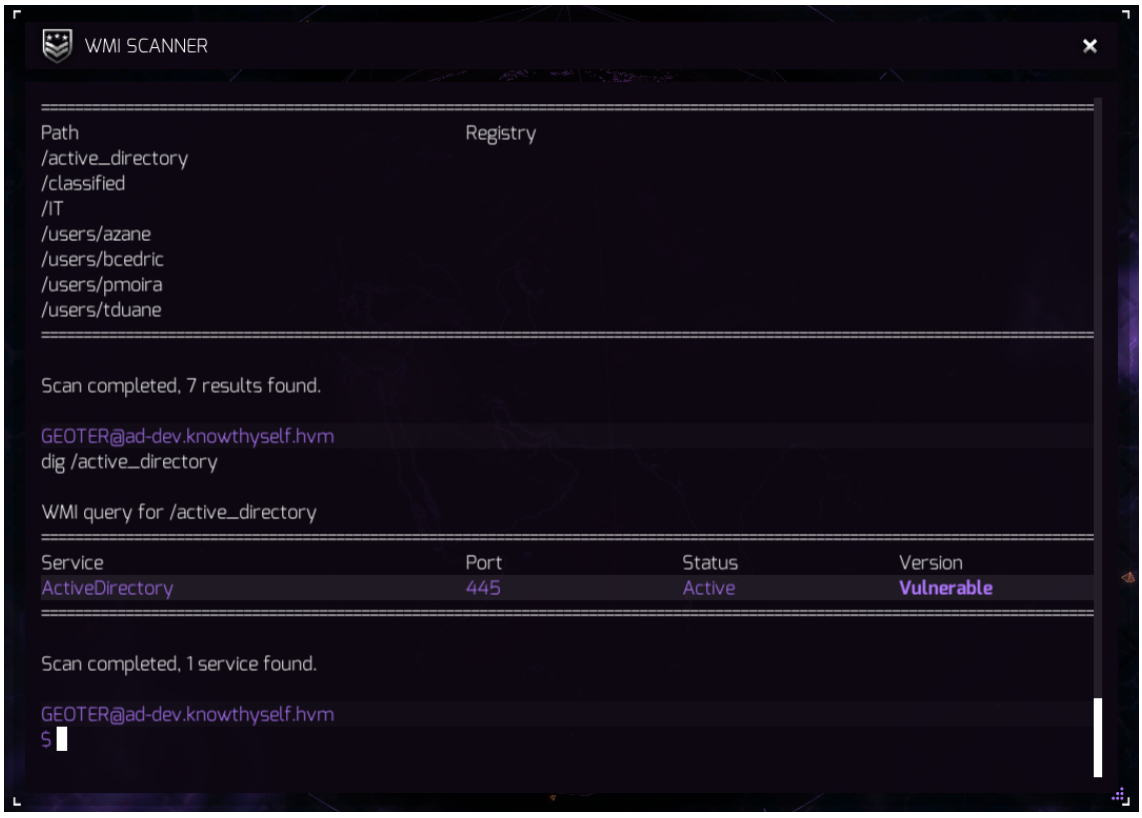


Σχήμα Δ.37: *Ένα από τα στοιχεία σχεδίασης που χρησιμοποιήθηκαν για την υλοποίηση του σεναρίου. Στο σχήμα απεικονίζεται η δομή ενός συστήματος φακέλων*

Ο παίκτης επίσης πρέπει να χρησιμοποιήσει το διαδίκτυο ή φωτογραφίες και αρχεία που εντοπίζει για να λύσει τα προβλήματα που αντιμετωπίζει. Μερικά από τα προβλήματα που παρουσιάζονται βρίσκονται στη μορφή γρίφων ενώ υπάρχει συνοχή και σύνδεση με την ιστορία του σεναρίου. Οι ARG γρίφοι που υπάρχουν στο σενάριο βρίσκονται σε δύο κατηγορίες. Η πρώτη, είναι σχετικά με την παρατηρητικότητα και τη λογική σκέψη. Ένα παράδειγμα αυτού του γρίφου είναι στο σημείο όπου οι παίκτες βρίσκουν έναν υπερσύνδεσμο, ο οποίος του καθοδηγεί σε έναν λογαριασμό στην πλατφόρμα κοινωνικής δικτύωσης του X/Twitter (σχήμα Δ.36). Οι παίκτες στη συνέχεια πρέπει να σκεφτούν με τη βοήθεια στοιχείων που έχουν αποκτήσει και παρατηρώντας μοτίβα ή την απουσία αυτών, τι μήνυμα μπορεί να κρύβεται στις δημοσιεύσεις του χρήστη. Η δεύτερη κατηγορία εξετάζει την ικανότητα του χρήστη να χρησιμοποιεί το διαδίκτυο για να βρει πληροφορίες ενώ ταυτόχρονα πάλι εξετάζεται η λογική κρίση του παίκτη. Παράδειγμα αποτελεί μία σειρά από ερωτήσεις, για τις οποίες ο παίκτης ενδεχομένως να μη γνωρίζει, με τα στοιχεία να τον προτρέπουν να χρησιμοποιήσει το διαδίκτυο. Απαντώντας σωστά τις ερωτήσεις, πρέπει μετά να σκεφτεί την πραγματική σημασία της πρότασης που οι απαντήσεις διαμορφώνουν.

Καθώς το NITE Team 4 παρέχει πολλά εργαλεία και η χρήση και κατανόηση όλων των εργαλείων είναι δύσκολη για κάποιον που δεν είναι εξοικειωμένος με την πλατφόρμα, στο σενάριο δε χρησιμοποιούνται όλα τα εργαλεία. Συγκεκριμένα, από εκείνα διαθέσιμα στο Hivemind Network, δεν αξιοποιούνται τα Man in the Middle και Social Engineering Toolkit. Σχετικά με το πρώτο, παρόλο που συχνά αποτελεί ένα κύριο κομμάτι της εκπαίδευσης της κυβερνοασφάλειας, η πολυπλοκότητα του εμποδίζει τη χρήση του στα πλαίσια της εργασίας. Σχετικά με το Social Engineering Toolkit, κατά το πειραματικό στάδιο της εργασίας υπήρχε η ιδέα της χρήσης του ως εναλλακτική μέθοδος εισχώρησης, αλλά τελικά απορρίφθηκε καθώς υπήρχε ήδη πληθώρα στοιχείων και εργαλείων στο παιχνίδι.

Δ.3 Σύνοψη σεναρίου στα πλαίσια της εργασίας



Σχήμα Δ.38: *Τα αποτελέσματα της εντολής netscan στο δίκτυο (άνω τμήμα) και τα αποτελέσματα της εντολής dig στο active directory (κάτω τμήμα)*



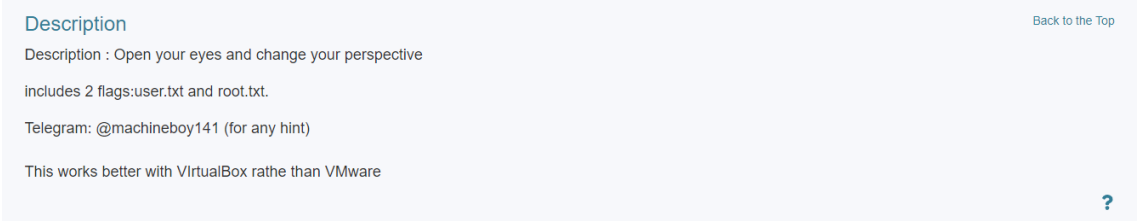
Σχήμα Δ.39: *Τμήμα του δικτύου που αναπαριστά το active directory του σεναρίου*

Η σχεδίαση του δικτύου ακολουθεί παρόμοια δομή με αρκετά από τα σενάρια που έχει ήδη το παιχνίδι. Παρόλο που το Hivemind Network δεν περιορίζει τον δημιουργό στα στοιχεία που θα χρησιμοποιήσει, καθώς το σενάριο έχει εκπαιδευτικό χαρακτήρα, οι τεχνολογίες που χρησιμοποιούνται μέσα στο δίκτυο καθώς και τα ports, τα CVE και λοιπά στοιχεία ταιριάζουν με τα αντίστοιχα στοιχεία στον πραγματικό κόσμο. Ο παίκτης έχει ως κύριο σκοπό να αποκτήσει πρόσβαση στα δίκτυα που του ζητάει η αποστολή, ή σε υποδίκτυα που θα βοηθήσουν τον παίκτη να συνεχίσει προς τον στόχο του, οπότε πολλές από τις διεργασίες που πραγματοποιεί είναι σχετικά με την εισχώρηση σε ένα δίκτυο και χρησιμοποιώντας τις αδυναμίες του δικτύου. Ωστόσο, έμφαση υπάρχει και στη χρήση των διαφορετικών εργαλείων που παρέχει το NITE Team 4, έτσι ώστε οι παίκτες να αποκτήσουν μία πιο ολική εικόνα για τις δυνατότητες της πλατφόρμας, αλλά και τις δυνατότητες ενός πραγματικού συστήματος.

Στο δίκτυο του σεναρίου υπάρχουν τρία υποδίκτυα, ένα public και δύο private. Ο παίκτης κατά τη διάρκεια του σεναρίου, αρχικά πρέπει να χρησιμοποιήσει τα εργαλεία του για να εισχωρήσει στο public υποδίκτυο. Από εκεί, έχει τη δυνατότητα παρακολούθησης των δύο private υποδικτύων αλλά μπορεί να εντοπίσει μόνο τα directories του δικτύου με όνομα "Private". Για να έχει πρόσβαση και στα paths του άλλου υποδικτύου με όνομα Active Directory, θα χρειαστεί να βρει ένα τρόπο να εισχωρήσει σε αυτό το υποδίκτυο. Με την

εξερεύνηση του παίκτη στο πρώτο private υποδίκτυο, εντοπίζει πληροφορίες που του επιτρέπει να αποκτήσει πρόσβαση στο κινητό τηλεφώνου του κύριου ύποπτου. Από εκεί, ο παίκτης ανακαλύπτει ένα από τα κύρια μυστήρια του σεναρίου, και συνεχίζει την εισχώρηση του πιο βαθιά στο δίκτυο, αυτήν τη φορά στο υποδίκτυο του Active Directory. Σε αυτό το σημείο παρουσιάζονται και οι πρώτοι προαιρετικοί στόχοι του παίκτη, με αυτούς τους στόχους να παρέχουν είτε περισσότερες πληροφορίες για την ιστορία είτε ενδεχομένως να διευκολύνουν τον παίκτη να επιτύχει τον κύριο σκοπό του. Με τη βοήθεια πληροφοριών που βρίσκει στο Active Directory και με τη σωστή χρήση των εργαλείων που προσφέρει το Stinger OS, ο παίκτης ανακαλύπτει το άτομο πίσω από τα εγκλήματα και πρέπει πλέον να αποκτήσει πρόσβαση στον φάκελο όπου είναι κρυμμένα τα ενοχοποιητικά στοιχεία. Για την επίλυση της τελευταίας πρόκλησης, ο παίκτης ενδεχομένως να χρειαστεί να χρησιμοποιήσει το διαδίκτυο για βρει τη λύση. Με την παραβίαση του directory, τελειώνει το σενάριο και εφόσον ο παίκτης επιθυμεί, έχει τη δυνατότητα να διαβάσει ο ίδιος τα ενοχοποιητικά στοιχεία που υπάρχουν.

Δ.4 Σύνδεση με σενάριο Vulnhub



Σχήμα Δ.40: *Η περιγραφή του σεναρίου Thales: 1 στο Vulnhub*

Η ιδέα του σεναρίου ξεκίνησε από το σενάριο Thales: 1. Το Vulnhub παρέχει υλικό απάνω σε penetration testing σε πραγματικό υλικό όπως Kali Linux, με το Thales: 1 να αποτελεί ένα απλό σενάριο στα πλαίσια της κυβερνοασφάλειας. Το Thales: 1 αποτελεί έμπνευση για το σενάριο στο NITE Team 4, με το εξής σενάριο να αναπτύσσεται σε οριζόντια και κάθετη κλίμακα γύρω από το Vulnhub σενάριο. Παρόλο που αρκετά στοιχεία διατηρήθηκαν, μια μεγάλη πλειοψηφία αυτών έχουν τροποποιηθεί μεταξύ των σεναρίων έτσι ώστε να παρουσιάζονται καλύτερα στο NITE Team 4 αλλά και για να συσχετίζονται καλύτερα με τον εκπαιδευτικό χαρακτήρα του σεναρίου. Για παράδειγμα, καθώς το Vulnhub σενάριο αξιοποιεί μια ιστοσελίδα με την οποία ο παίκτης ενδεχομένως να αλληλεπιδράσει, και στα πλαίσια του NITE Team 4 δεν είναι εφικτό η υλοποίηση τέτοιου στοιχείου, ο παίκτης χρησιμοποιεί εργαλεία όπως το

Host Fingerprint για να αναγνωρίζει τις αδυναμίες και έπειτα να αποκτήσει πρόσβαση μέσω του εργαλείου Foxacid Server.

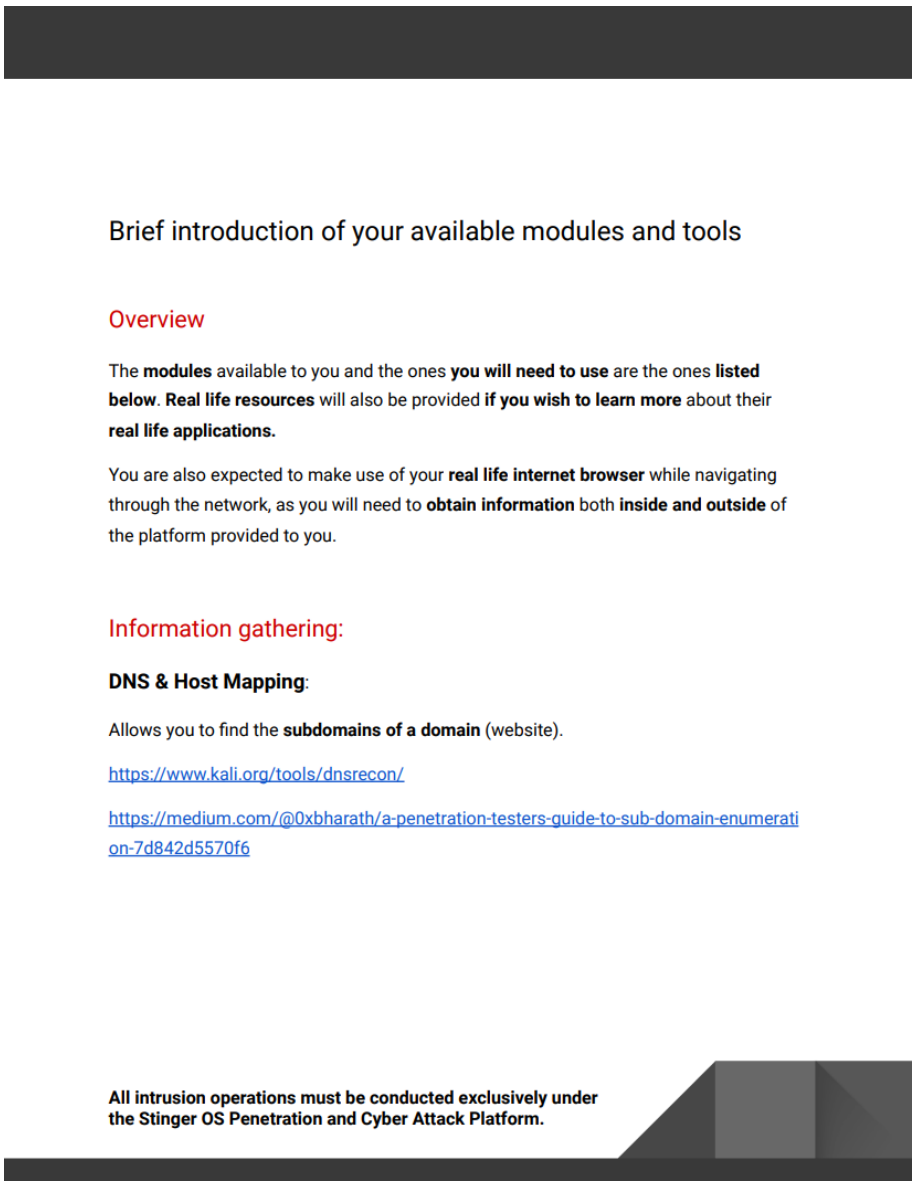
Μία περαιτέρω έμπνευση είναι και το ίδιο το όνομα του σεναρίου. Το Vulnhub σενάριο χρησιμοποιεί τον τίτλο του Thales/Θαλής ως μία απλή ονομασία, αλλά στα πλαίσια της εργασίας ο Θαλής αποτελεί σημαντικό πρόσωπο. Περαιτέρω, στο NITE Team 4 σενάριο έχει γίνει η σύνδεση μεταξύ του ιστορικού Θαλή με τον Thales της ιστορίας του σεναρίου. Η ιστορία έχει εμπλουτιστεί με αναφορές στην αρχαιοελληνική ιστορία, προσθέτοντας μεγαλύτερο βάθος μυστήριο αλλά και γνώσεις καθώς οι παίκτες ανακαλύπτουν στοιχεία για τον Θαλή του παιχνιδιού αλλά και τον ιστορικό φιλόσοφο. Πολλοί από τους γρίφους αναφέρονται στον Θαλή, είτε το πρόσωπο του παιχνιδιού, είτε το ιστορικό πρόσωπο, με την ίδια την ιστορία να είναι γύρω από αυτόν.

Δ.5 Δοκιμαστικό στάδιο σεναρίου

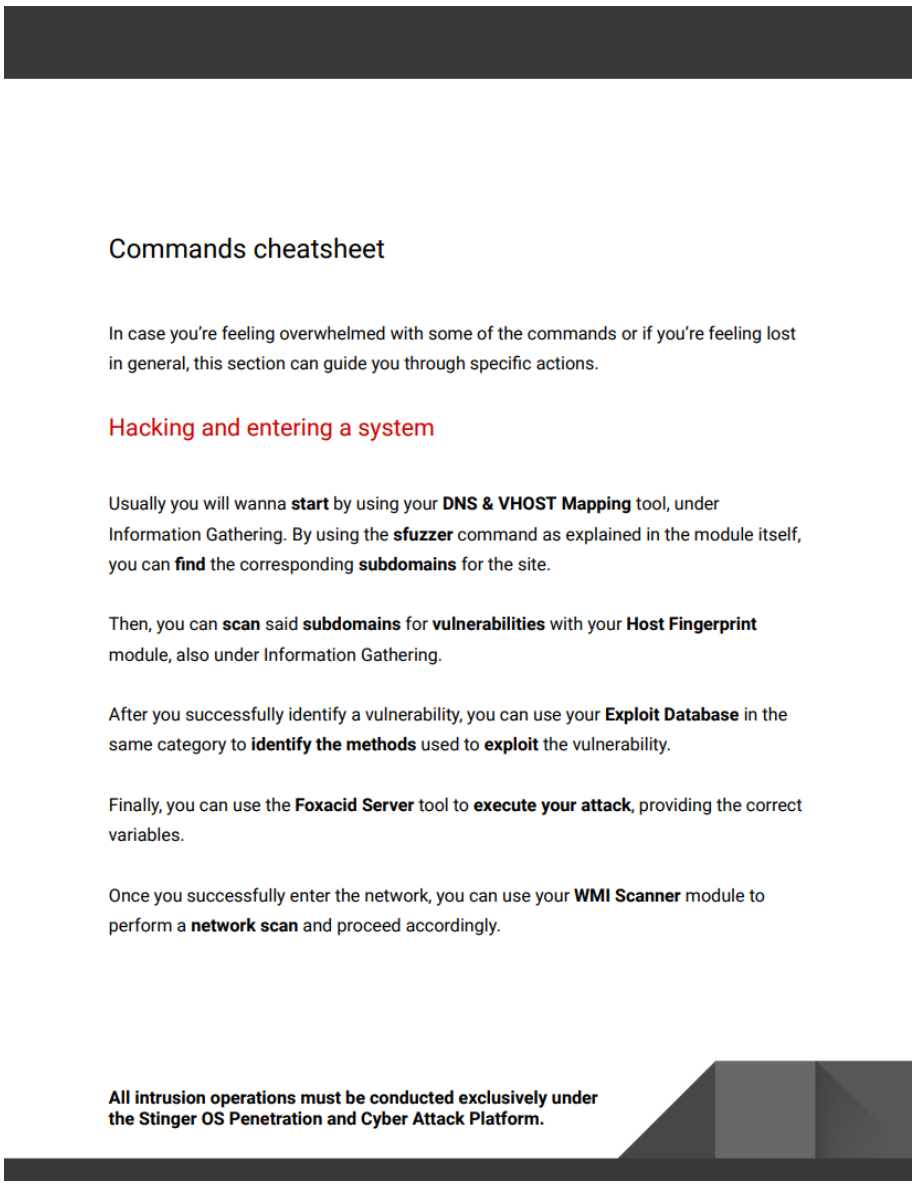
Κατά τη σχεδίαση του σεναρίου, υπήρξε ένα δοκιμαστικό στάδιο στο οποίο το σενάριο διαμοιράστηκε σε συγκεκριμένα άτομα έτσι ώστε να αξιολογήσουν στοιχεία του, όπως δυσκολία, συνάφεια οδηγιών, ευχαρίστηση, ύπαρξη εκπαιδευτικής αξίας και άλλα. Σε αυτό το στάδιο διάφορα τμήματα του σεναρίου διαμορφώθηκαν έτσι ώστε να προσφέρει μία καλύτερη εμπειρία. Κύριο πρόβλημα αποτελούσε η πολυπλοκότητα του παιχνιδιού λόγω τον αριθμό των εργαλείων που παρουσιάζονται στον παίκτη. Για την αντιμετώπιση του προβλήματος, καθώς η ενημερωτική εισαγωγή του παιχνιδιού είναι βοηθητική αλλά χρειάζεται αρκετό χρόνο για την ολοκλήρωση του, προστέθηκε ένα νέο κεφάλαιο στο αρχείο Operation: Clear Water, στο οποίο επεξηγούνται οι βασικές λειτουργίες του κάθε εργαλείου.

Στα πιο περίπλοκα εργαλεία προστέθηκαν πιο εκτεταμένες επεξηγήσεις, δίνοντας περισσότερες πληροφορίες για τη σωστή λειτουργία τους ενώ υπάρχουν υπερσύνδεσμοι σχετικά με το αντίστοιχο εργαλείο στην πραγματική ζωή για όσους παίκτες επιθυμούν να μάθουν περαιτέρω. Εντοπίστηκαν επιπλέον και μικρότερα σφάλματα μέσα στο δίκτυο, με την πλειοψηφία από αυτών να μην επηρεάζουν άμεσα την εμπειρία του παίκτη αλλά η διόρθωση τους να παρουσιάζει βελτίωση της ολικής εμπειρίας.

Με τη διόρθωση των προβλημάτων που παρουσιάστηκαν στο πρώτο στάδιο, πραγματοποιήθηκε και ένα μικρότερο δεύτερο στάδιο για την επίλυση προβλημάτων που ίσως να μην είχαν παρουσιαστεί. Παρόλο που το επιπλέον κεφάλαιο βοήθησε του παίκτες σε μεγάλο βαθμό, υπήρχε



Σχήμα Δ.41: *Τμήμα του επιπρόσθετου κεφαλαίου του αρχείου Operation: Clear Water σχετικά με τη λειτουργία των εργαλείων που θα χρειαστεί ο παίκτης. Προστέθηκε κατά το πρώτο δοκιμαστικό στάδιο του σεναρίου*



Σχήμα Δ.42: *Το επιπρόσθετο κεφάλαιο του αρχείου Operation: Clear Water, προσφέροντας μία βοηθητική εισαγωγή για το Stinger OS. Προστέθηκε κατά το δεύτερο δοκιμαστικό στάδιο του σεναρίου*

και πάλι δυσκολία από μερικούς καθώς ήταν αβέβαιο ποιο εργαλείο να χρησιμοποιήσουν ή πως να προχωρήσουν στο σενάριο. Επιπλέον, παρουσιάστηκε μεγαλύτερη δυσκολία σε μερικούς γρίφους, με μερικούς παίκτες να μην έχουν τη δυνατότητα να τους λύσουν. Ως λύση για το πρώτο πρόβλημα, προστέθηκε ένα τρίτο κεφάλαιο στο αρχείο Operation: Clear Water. Το συγκεκριμένο κεφάλαιο απευθύνεται για τους παίκτες που χρειάζονται μία επιπλέον βοήθεια και εξηγεί μερικά από τα βήματα που πρέπει να ακολουθήσει ο παίκτης για τις πιο κοινές ενέργειες μέσα στο παιχνίδι στην περίπτωση που ο παίκτης δεν είναι σίγουρος για την πορεία του. Επιπλέον, μερικά από τα ευρήματα που ανακαλύπτει ο παίκτης μέσα στο δίκτυο έχουν βελτιωμένο κείμενο, δίνοντας περισσότερη καθοδήγηση και επεξήγηση στον παίκτη. Σχετικά με τους γρίφους, προστέθηκαν επιπλέον στοιχεία συνάφειας έτσι ώστε η επίλυση τους να είναι πιο προσιτή. Συγκεκριμένα, βελτιώθηκε η δομή για γρίφους στους οποίους παρατηρήθηκε ιδιαίτερη δυσκολία. Πλέον αντί να είναι υποχρεωτικό στοιχείο της ιστορίας, μερικοί παρουσιάζονται ως δευτερεύων προαιρετικά στοιχεία. Οι παίκτες προτρέπονται να ολοκληρώσουν αυτούς τους γρίφους καθώς αποκτούν πληροφορίες που τους βοηθάει να ολοκληρώσουν την αποστολή τους και βιώνουν ικανοποίηση ξεπερνώντας τη δοκιμασία, ωστόσο παίκτες οι οποίοι ενδεχομένως να παρουσιάσουν δυσκολία μπορούν ακόμη να ολοκληρώσουν την αποστολή τους.

Κεφάλαιο E

Πειραματικό στάδιο

E.1 Μεθοδολογία έρευνας - Ερωτηματολόγια

Στα πλαίσια της έρευνας, δέκα φοιτητές του Ιονίου Πανεπιστημίου επιλέχθηκαν να παίξουν το σενάριο. Η πλειοψηφία των φοιτητών βρίσκονται στο τμήμα Πληροφορικής του πανεπιστημίου, με όλους τους συμμετέχοντες να μην έχουν ιδιαίτερη ή καμία εξοικείωση με το παιχνίδι. Για την προετοιμασία των φοιτητών για το παιχνίδι, τους δόθηκε πρόσβαση στο εξωτερικό αρχείο Operation: Clear Water στο οποίο υπάρχουν πληροφορίες για τους στόχους τους στο παιχνίδι, τις λειτουργίες των εργαλείων του παιχνιδιού καθώς και μία ενδεικτική εισαγωγή. Οι φοιτητές ταυτόχρονα κλήθηκαν να απαντήσουν σε ερωτήσεις πάνω σε θέματα της κυβερνοασφάλειας με τη μορφή πολλαπλών απαντήσεων. Με την ολοκλήρωση του ερωτηματολογίου, οι συμμετέχοντες κλήθηκαν να παίξουν το παιχνίδι, χρησιμοποιώντας το αρχείο και τα στοιχεία του παιχνιδιού για να γίνει η σωστή καθοδήγηση. Με την ολοκλήρωση του σεναρίου, οι συμμετέχοντες απάντησαν δύο επιπλέον ερωτηματολόγια. Το πρώτο, διαθέτει ερωτήσεις του ARCS μοντέλου απάνω στο κίνητρο του παίκτη, σε 4 κατηγορίες. Επιπλέον, έχουμε αξιοποιήσει μια επιπρόσθετη παράμετρο, το Perceived Learning, για την αξιολόγηση του μαθησιακού αντίκτυπου. Το Attention εξετάζει το ενδιαφέρον των συμμετεχόντων κατά τη διάρκεια του πειράματος, το Relevance εξετάζει τη χρησιμότητα του περιεχόμενου σε σχέση με τον πραγματικό κόσμο, το Confidence εξετάζει την αυτοπεποίθηση των συμμετεχόντων στο να επιτύχουν στη διαδικασία, το Satisfaction εξετάζει την ικανοποίηση προς το περιεχόμενο και τέλος το Perceived Learning εξετάζει κατά πόσο οι συμμετέχοντες θεωρούν ότι έμαθαν μέσω της διαδικασίας. Το δεύτερο έχει τις ίδιες ερωτήσεις

με εκείνες που απάντησαν πριν παίξουν το σενάριο, έτσι ώστε να παρουσιαστούν οι αλλαγές στις γνώσεις τον παικτών μέσω του σεναρίου. Οι απαντήσεις σε όλες τις ερωτήσεις που διατυπώθηκαν σε αυτό το ερωτηματολόγιο παρουσιάζονται στα πλαίσια του παιχνιδιού. Ένας μεγάλος αριθμός από αυτών αφορά πληροφορίες που ο παίκτης πρέπει να επεξεργαστεί μέσα στο παιχνίδι. Ωστόσο, μερικές ερωτήσεις είτε απασχολούν θέματα τα οποία δεν έχουν άμεση σημασία στο παιχνίδι και έτσι δεν είναι τόσο εύκολο να παρατηρηθούν είτε συσχετίζονται με στοιχεία από το προαιρετικό περιεχόμενο. Με αυτόν τον τρόπο, μπορούμε να παρατηρήσουμε αν οι παίκτες απορρόφησαν πληροφορίες από διάφορες πλευρές του παιχνιδιού ή αν κυρίως έχουν μάθει από το κύριο περιεχόμενο.

E.2 Αποτελέσματα έρευνας

Για τα ερωτηματολόγια αξιολόγησης της γνώσης των παικτών, παρουσιάζονται πίνακες για κάθε ερώτηση, στην οποία υπάρχουν τα ποσοστά των απαντήσεων που δόθηκαν από τους παίκτες πριν και μετά το παιχνίδι. Οι σωστές απαντήσεις βρίσκονται με έντονους χαρακτήρες.

Πίνακας *E*.**1:** *Απαντήσεις στην ερώτηση "Τι είναι το port scanning;"*

Απαντήσεις	**% πριν**	**% μετά**
Μέθοδος παράκαμψης της προστασίας ενός port	0%	0%
Μέθοδος ανίχνευσης μόνο των ports που χρησιμοποιούνται σε ένα σύστημα	**0%**	**20%**
Μέθοδος ανίχνευσης όλων των ports ενός συστήματος	60%	70%
Μέθοδος ανίχνευσης των ports τα οποία έχουν κάποια ευπάθεια	10%	10%
Δε γνωρίζω	30%	0%

Για τον πίνακα Ε.1, παρατηρούμε ότι αρχικά το 60% των ατόμων απάντησε ότι είναι "Μέθοδος ανίχνευσης όλων των ports ενός συστήματος" ενώ κανένα άτομο δεν απάντησε σωστά. Μετά το παιχνίδι, 20% των ατόμων έδωσαν τη σωστή απάντηση, με το προηγούμενο ποσοστό του 60% να ανεβαίνει σε 70%. Επιπλέον, αρχικά 30% των συμμετεχόντων απάντησαν ότι δε γνωρίζουν την απάντηση, με αυτό το ποσοστό να μετακινείται στο 0%. Συμπεραίνουμε ότι όλοι οι παίκτες κατά ελάχιστο είχαν περισσότερη αυτοπεποίθηση στις απαντήσεις τους. Παρόλο που αρκετοί δεν έδωσαν την απαραίτητη σημασία για να υποδείξουν τη διαφορά μεταξύ την εύρεση όλων των θυρών τους συστήματος και αυτών που αξιοποιούνται, παρουσιάζεται

αύξηση στο ποσό σωστών απαντήσεων.

Πίνακας *Ε*.2: *Απαντήσεις στην ερώτηση "Ποια είναι η σύνηθες τεχνολογία συνδεδεμένη στο port 443;"*

Απαντήσεις	**% πριν**	**% μετά**
Secure Shell protocol (SSH)	0%	10%
Hypertext Transfer Protocol (HTTP)	30%	10%
Hypertext Transfer Protocol Secure (HTTPS)	**10%**	**10%**
Domain Name System (DNS)	10%	20%
Δε γνωρίζω	50%	50%

Για τον πίνακα Ε.2, δεν παρουσιάζεται ιδιαίτερη διαφορά στις απαντήσεις. Το 50% των συμμετεχόντων δε γνωρίζουν την απάντηση, με το ίδιο ποσοστό να διατηρείται εφόσον έχουν παίξει το παιχνίδι. Το ποσοστό των σωστών απαντήσεων επίσης διατηρήθηκε στο 10%. Καθώς η εξής ερώτηση δε διαθέτει κεντρικό ρόλο στο παιχνίδι και οι παίκτες πρέπει να δείξουν μεγαλύτερο ενδιαφέρον προς αυτή για να την κατανοήσουν πλήρως, συμπεραίνουμε ότι οι παίκτες δεν έδειξαν ενδιαφέρον σχετικά με τη σημασία του συγκεκριμένου port.

Πίνακας *Ε*.3: *Απαντήσεις στην ερώτηση "Ποια είναι η σύνηθες τεχνολογία συνδεδεμένη στο port 80;"*

Απαντήσεις	**% πριν**	**% μετά**
Secure Shell protocol (SSH)	30%	20%
Hypertext Transfer Protocol (HTTP)	**0%**	**30%**
Hypertext Transfer Protocol Secure (HTTPS)	0%	0%
Domain Name System (DNS)	20%	0%
Δε γνωρίζω	50%	50%

Παρόλο που η ερώτηση του πίνακα Ε.3 είναι παρόμοια με την ερώτηση στον πίνακα Ε.2, παρατηρούμε πιο θετικά αποτελέσματα. Το ίδιο ποσοστό των ατόμων δε γνώριζαν την απάντηση πριν και μετά το παιχνίδι, στο 50% των συμμετεχόντων. Ωστόσο, το 30% άλλαξε την απάντηση τους στο σωστό, δείχνοντας μία αύξηση από 0% σε 30%. Καθώς το συγκεκριμένο port χρησιμοποιείται στα πλαίσια του παιχνιδιού από τους παίκτες για τη διάρρηξη του συστήματος, περισσότεροι παρατήρησαν τη σημασία του port σε σχέση με το port 443 στο οποίο δεν υπάρχει τόση μεγάλη αλληλεπίδραση, αναγνωρίζοντας ότι το port 80 δεν

είναι προστατευόμενο.

Πίνακας *Ε.4:* *Απαντήσεις στην ερώτηση "Ποια είναι η χρήση της εντολής search στο metasploit (Searchsploit);"*

Απαντήσεις	**% πριν**	**% μετά**
Προσφέρει πληροφορίες για κάποια τεχνολογία και τις ευπάθειες της	**10%**	**70%**
Εντοπίζει την τεχνολογία που χρησιμοποιεί το αντίστοιχο port και προσφέρει πληροφορίες για αυτή	0%	10%
Βρίσκει τις ευπάθειες που υπάρχουν σε ένα σύστημα	30%	20%
Βρίσκει τα ports που υπάρχουν σε ένα σύστημα	20%	0%
Δε γνωρίζω	40%	0%

Στην ερώτηση του πίνακα Ε.4, 10% των συμμετεχόντων απάντησαν σωστά για τη λειτουργία της εντολής, με ένα επιπλέον 30% να γνωρίζει ότι συσχετίζεται με ευπάθειες. Μετά το παιχνίδι, παρουσιάζεται μεγάλη βελτίωση, παρουσιάζοντας αύξηση κατά 60%, από 10% σε 70% για τη σωστή απάντηση. Το ποσοστό, των ατόμων που δε γνώριζαν τη σωστή απάντηση επίσης έπεσε στο 0%, από 40%. Συμπεραίνουμε ότι οι παίκτες μέσω του παιχνιδιού ήταν εξαιρετικά σίγουροι για ποια είναι η σωστή απάντηση βελτιώνοντας τη γνώση τους στο θέμα, ενώ τουλάχιστον όλοι οι παίκτες είχαν την αυτοπεποίθηση ότι γνώριζαν ποια είναι η σωστή απάντηση.

Πίνακας *Ε.5:* *Απαντήσεις στην ερώτηση "Τι είναι το CVE;"*

Απαντήσεις	**% πριν**	**% μετά**
Σύστημα καταγραφής των σημασιών και τις σύνηθες αντιστοιχίσεις των port	10%	10%
Σύστημα ταξινόμησης ευπαθειών κυβερνοασφάλειας	**20%**	**30%**
Εργαλείο εντόπισης ευπαθειών	10%	30%
Εργαλείο εντόπισης των port και τις τεχνολογίες που αντιστοιχούν στο δίκτυο	0%	0%
Δε γνωρίζω	60%	30%

Στον πίνακα Ε.5, παρατηρούμε ότι για την ερώτηση "Τι είναι το CVE;", υπάρχει μία μικρή αύξηση στο ποσοστό σωστών απαντήσεων από 20% σε 30% ενώ παρουσιάζεται μεγαλύτερη

αύξηση στην απάντηση "Εργαλείο εντόπισης ευπαθειών" παρόλο που δεν έχει τον ρόλο ενός εργαλείου. Ωστόσο, όλοι οι συμμετέχοντες είχαν την αυτοπεποίθηση ότι γνωρίζουν τη σωστή απάντηση. Η συγκεκριμένη ερώτηση σχετίζεται με προαιρετικό περιεχόμενο του παιχνιδιού, οπότε μόνο παίκτες που έχουν ολοκληρώσει αυτό το περιεχόμενο θα γνώριζαν τη σωστή απάντηση, το οποίο εξηγεί το μεγάλο ποσοστό των λανθασμένων απαντήσεων, καθώς οι παίκτες επέλεξαν να μην αλληλεπιδράσουν ιδιαιτέρως με το περιεχόμενο αυτό.

Πίνακας *Ε*.6: *Απαντήσεις στην ερώτηση "Τι είναι το Active Directory;"*

Απαντήσεις	**% πριν**	**% μετά**
Σύστημα της Microsoft για την οργάνωση πληροφοριών για τους πόρους και τους χρήστες ενός συστήματος	**20%**	**60%**
Σύστημα της Microsoft για την οργάνωση των server που διαθέτουν	0%	20%
Σύστημα της Google για την οργάνωση των server που διαθέτουν	0%	0%
Κανένα από τα παραπάνω	30%	20%
Δε γνωρίζω	50%	0%

Στην ερώτηση του πίνακα Ε.6, οι συμμετέχοντες παρουσίασαν μερική εξοικείωση με την ερώτηση, με 20% να απαντάει σωστά. Το υπόλοιπο 30% απάντησε λανθασμένα και το 50% δε γνώριζαν την απάντηση. Έπειτα από το σενάριο, το 60% απάντησε σωστά, με όλους τους συμμετέχοντες να προσφέρουν κάποιου είδους απάντηση εκτός του "Δε γνωρίζω". Επίσης 20% παρόλο που δεν απάντησε σωστά, έδειξε ότι έμαθε πως το active directory σχετίζεται με τη Microsoft. Ως συμπέρασμα, παρατηρούμε ότι οι παίκτες αλληλεπίδρασαν παραπάνω με αυτό το προαιρετικό περιεχόμενο σε σχέση με την ερώτηση του πίνακα Ε.5. Παρόλο που τμήμα του active directory εμφανίζεται στην κύρια ιστορία του παιχνιδιού, οι παίκτες χρειάζονται να δείξουν μεγαλύτερο ενδιαφέρον και κατανόηση προς το περιεχόμενο για να απαντήσουν σωστά, το οποίο έδειξαν.

Πίνακας *Ε.7:* *Απαντήσεις στην ερώτηση "Ποια είναι η χρήση του John the Ripper;"*

Απαντήσεις	**% πριν**	**% μετά**
Να εντοπίζει και να σπάει κωδικούς	**60%**	**100%**
Να χρησιμοποιεί ευπάθειες για να εισχωρήσει ο χρήστης του εργαλείου σε ένα σύστημα	10%	0%
Να διαμοιράζει κακόβουλο κώδικα στις συνδεδεμένες συσκευές	0%	0%
Να παρακολουθεί μηνύματα μεταξύ δύο συσκευών	0%	0%
Δε γνωρίζω	30%	0%

Για την ερώτηση του πίνακα Ε.7, οι παίκτες παρουσίασαν μεγάλη εξοικείωση με το εργαλείο, με 60% να γνωρίζει σωστά τη χρήση του πριν το παιχνίδι. Αυτό το ποσοστό αυξάνεται σε 100%, με όλους τους συμμετέχοντες να απαντούν σωστά την ερώτηση. Το συγκεκριμένο εργαλείο είναι αρκετά γνωστό και από άτομα τα οποία έχουν μικρή εξοικείωση με την κυβερνοασφάλεια, και η χρήση του στο παιχνίδι είναι ενδιαφέρον προς τους παίκτες, παρουσιάζοντας ξεκάθαρα τη χρήση του στα πλαίσια του παιχνιδιού, με τους παίκτες να δίνουν πλήρη σημασία προς αυτό το εργαλείο.

Πίνακας *Ε.8:* *Απαντήσεις στην ερώτηση "Τι είναι το salami slicing attack;"*

Απαντήσεις	**% πριν**	**% μετά**
Είδος εγκλήματος στον κυβερνοχώρο	**30%**	**30%**
Μέθοδος για την εύρεση ενός κωδικού	0%	10%
Μέθοδος διαμοιρασμού ενός συστήματος σε υποσυστήματα για τη διευκόλυνση αναζήτησης συνδέσεων	20%	10%
Ορολογία που χρησιμοποιείται στην εισχώρηση ενός ευπαθούς συστήματος	0%	0%
Δε γνωρίζω	50%	50%

Η ερώτηση του πίνακα Ε.8, αποτελεί επίσης προαιρετικό περιεχόμενο, και υπάρχει ελάχιστη αλλαγή μεταξύ των αποτελεσμάτων πριν και μετά το σενάριο. Ένα 10% άλλαξε την απάντηση του σε μία άλλη λανθασμένη απάντηση, παρουσιάζοντας αβεβαιότητα στις απαντήσεις. Το 50% επίσης δε γνώριζαν την απάντηση πριν και μετά το παιχνίδι, με το ποσοστό σωστών απαντήσεων να παραμένει στατικό στο 30%. Συμπεραίνουμε ότι όπως και με την ερώτηση του πίνακα Ε.5, οι παίκτες δεν αλληλεπίδρασαν ιδιαιτέρως με αυτό το περιεχόμενο. Συγκεκριμένα, η συγκεκριμένη απάντηση βρίσκεται πίσω από ένα γρίφο με μεγαλύτερη δυσκολία σε σχέση

με τους άλλους, με τους παίκτες να χάνουν το ενδιαφέρον τους προς αυτό εφόσον έχουν χρησιμοποιήσει αρκετό χρόνο και δεν έχουν βρει ακόμη τη λύση του γρίφου. Συνεπώς, οι παίκτες δε θα αλληλεπιδράσουν με περιεχόμενο το οποίο δεν είναι υποχρεωτικό αν αυτό το περιεχόμενο είναι πιο δύσκολο από ότι επιθυμούν.

Πίνακας *Ε*.9: *Απαντήσεις στην ερώτηση "Τι είναι το XKeyscore;"*

Απαντήσεις	**% πριν**	**% μετά**
Σύστημα αξιολόγησης ισχύς ενός κωδικού	10%	10%
Σύστημα εισχώρησης με τη χρήση κωδικών-κλειδιά που αντιστοιχούν σε κάποιο άτομο	20%	30%
Σύστημα αναζήτησης, ανάλυσης και καταγραφής δεδομένων απάνω σε άτομα	**0%**	**30%**
Όλα τα παραπάνω	0%	0%
Δε γνωρίζω	70%	30%

Στην ερώτηση του πίνακα Ε.9, 70% των συμμετεχόντων απάντησε ότι δε γνωρίζει την απάντηση, καθώς το XKeyscore αποτελεί πολύ εξειδικευμένο σύστημα για το οποίο πολλά άτομα δε θα γνώριζαν τη χρήση του. Οι υπόλοιποι συμμετέχοντες απάντησαν την ερώτηση λανθασμένα. Έπειτα από τη συμμετοχή τους στο παιχνίδι, το 30% απάντησε σωστά την ερώτηση, με 30% να δηλώνουν ότι δε γνωρίζουν την απάντηση σε σχέση με το προηγούμενο 70&. Συμπερασματικά, καθώς για την πλήρη κατανόηση του εργαλείου οι παίκτες πρέπει να δείξουν μεγαλύτερο ενδιαφέρον, αρκετοί παίκτες όντως έδειξαν το αναγκαίο ποσό ενδιαφέροντος. Ωστόσο, λόγω της φύσης του εργαλείου και ο τρόπος με τον οποίο παρουσιάζεται στο παιχνίδι, παρόλο που οι παίκτες πρέπει να το χρησιμοποιήσουν δύο φορές για να συνεχίσουν στο παιχνίδι, αρκετοί δεν ήταν βέβαιοι για την ακριβής χρήση του καθώς δεν πραγματοποίησαν αυτήν την ανεπτυγμένη αλληλεπίδραση που έδειξαν άλλοι συμμετέχοντες.

Πίνακας Ε.10: *Απαντήσεις στην ερώτηση "Σε ποιο από τα παρακάτω παραδείγματα φαίνεται ένα subdomain;"*

Απαντήσεις	**% πριν**	**% μετά**
google.com/	0%	10%
http://google.com/	0%	0%
https://google.com/	0%	0%
cloud.google.com/	**70%**	**90%**
Δε γνωρίζω	30%	0%

Στην ερώτηση του πίνακα Ε.10, 70% των συμμετεχόντων αναγνώρισε σωστά σε ποιες από τις διευθύνσεις παρουσιάζεται ένα subdomain, παρουσιάζοντας ομοίως με τα αποτελέσματα στον πίνακα Ε.7, τις βασικές γνώσεις των συμμετεχόντων για το θέμα. Το υπόλοιπο 30% απάντησε "Δε γνωρίζω". Το 90% απάντησε σωστά στη συνέχεια, ενώ ένας συμμετέχων άλλαξε την απάντηση του από "Δε γνωρίζω" σε μία λανθασμένη απάντηση. Συμπεραίνουμε ότι η πλειοψηφία των ατόμων ήδη γνώριζε τη μορφή ενός subdomain, με τους υπόλοιπους να μαθαίνουν μέσω του παιχνιδιού.

Πίνακας Ε.11: *Απαντήσεις στην ερώτηση "Ποια είναι η χρήση της εντολής airodump-ng (airodump);"*

Απαντήσεις	**% πριν**	**% μετά**
Εντοπίζει όλα τα δίκτυα που είναι ανιχνεύσιμα από τη στοχευμένη συσκευή	**0%**	**80%**
Μεταφέρει αρχεία από μία συσκευή σε μία άλλη μέσω Wi-FI	10%	0%
Χρησιμοποιεί τις ευπάθειες του δικτύου για να εισχωρήσει σε κάποιο ανιχνεύσιμο Wi-Fi hotspot	0%	10%
Μεταφέρει αρχεία από μία συσκευή σε μία άλλη μέσω NFC	10%	0%
Δε γνωρίζω	80%	10%

Στον πίνακα Ε.11, παρατηρούμε ότι το 80% όλων των συμμετεχόντων δε γνωρίζει τη λειτουργία της εντολής, με το υπόλοιπο 20% να απαντάει λανθασμένα. Η συγκεκριμένη εντολή αποτελεί τμήμα ενός εργαλείου το οποίο ακόμα και σε πλαίσια κυβερνοασφάλειας δεν είναι τόσο συχνό, καθώς είναι αποκλειστικά για πακέτα στα πλαίσια ενός Wi-Fi hotspot. Παρόλα αυτά, στη συνέχεια το 80% των συμμετεχόντων απάντησε σωστά, με μόνο το 10% να μη γνωρίζει τη χρήση της εντολής και 10% να απαντάει λάθος. Συμπεραίνουμε ότι οι παίκτες έμαθαν

πολύ αποτελεσματικά για τη λειτουργία της εντολής, ειδικά λόγω της απλής και κατανοητής λειτουργίας του, ενώ δε συσχετίζεται με ένα περίπλοκο θέμα.

Πίνακας *Ε*.12: *Απαντήσεις στην ερώτηση "Τι είναι ένα password hash;"*

Απαντήσεις	**% πριν**	**% μετά**
Επίσημη ονομασία των κωδικών που χρησιμοποιούμε στην καθημερινή μας χρήση	0%	0%
Κρυπτογραφημένη μορφή κωδικού	**80%**	**90%**
Απλοποιημένη μορφή κωδικού	0%	0%
Ο κύριος κωδικός ενός συστήματος	0%	10%
Δε γνωρίζω	20%	0%

Στην ερώτηση του πίνακα Ε.12, οι παίκτες έδειξαν μεγάλη εξοικείωση, με το 80% να απαντάει σωστά. Το υπόλοιπο 20% απάντησε ότι δε γνωρίζει την απάντηση. Μέσω του παιχνιδιού, το ποσοστό σωστών απαντήσεων αυξήθηκε στα 90%, με το υπόλοιπο 10% να απαντάει λάθος αντί για "Δε γνωρίζω". Συμπερασματικά, η πλειοψηφία των συμμετεχόντων είτε ήδη γνώριζε, είτε έμαθε για τη σημασία της ερώτησης μέσω του σεναρίου.

Πίνακας *Ε*.13: *Απαντήσεις στην ερώτηση "Ποιο από τα παρακάτω είναι σετ πρωτοκόλλων επικοινωνίας;"*

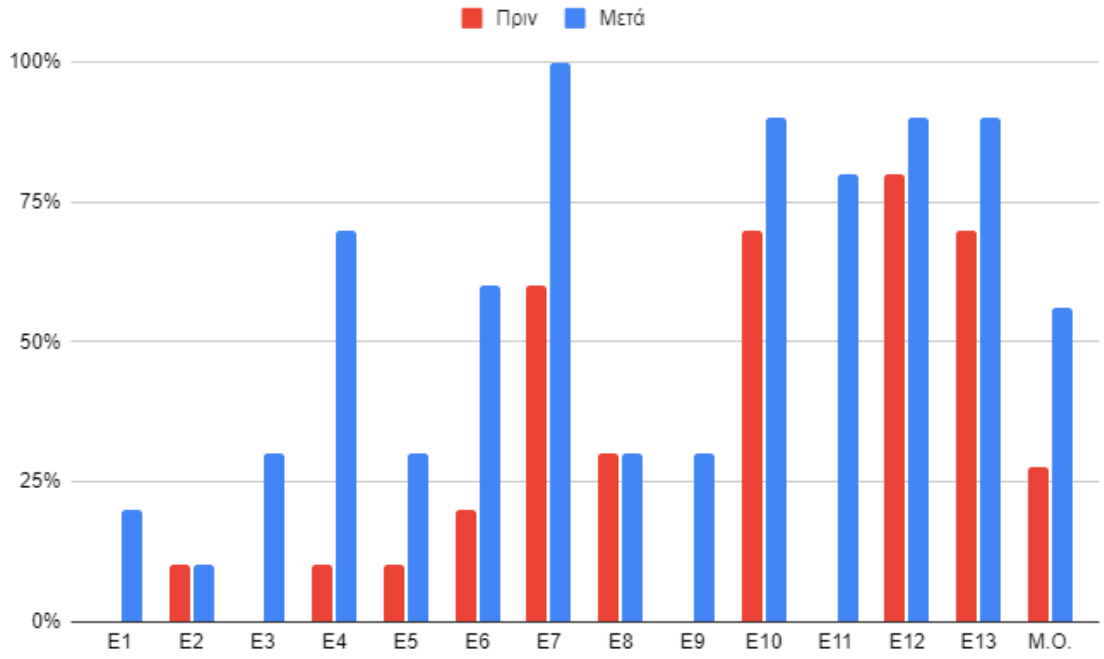
Απαντήσεις	**% πριν**	**% μετά**
TCP/IP	**70%**	**90%**
IP	0%	0%
WPA2	20%	0%
Κανένα από τα παραπάνω	0%	10%
Δεν γνωρίζω	10%	0%

Για την ερώτηση στον πίνακα Ε.13, παρουσιάζεται παρόμοια εξοικείωση από τους παίκτες όπως στον πίνακα Ε.12. 70% απάντησε σωστά πριν το παιχνίδι, με το 20% να δίνει λανθασμένες απαντήσεις. Στη συνέχεια, οι σωστές απαντήσεις αυξήθηκαν σε 90%, ενώ δεν υπήρχε καμία "Δε γνωρίζω" απάντηση. Παρομοίως με άλλα πιο κοινά θέματα της κυβερνοασφάλειας, οι παίκτες ήδη είχαν μεγάλη γνώση επί του θέματος, με κάποιο ποσοστό των ατόμων που δε γνώριζε, πλέον να έχει γνώση προς τη σωστή απάντηση, συμπεραίνοντας πως οι συμμετέχοντες διαθέτουν αυτή τη βασική γνώση, και μέσω του παιχνιδιού, επιπλέον άτομα απέκτησαν

αυτή τη γνώση.

Ε.3 Συζήτηση στα αποτελέσματα

Παρατηρώντας τους πίνακες και το σχήμα *Ε*.43, στις 11 από τις 13 ερωτήσεις υπάρχει είτε βελτίωση είτε το ποσοστό σωστών απαντήσεων παραμένει το ίδιο. Συγκεκριμένα, σημειώνεται αύξηση έως 80% ενώ η μέση αύξηση σημειώνεται σε 28%.

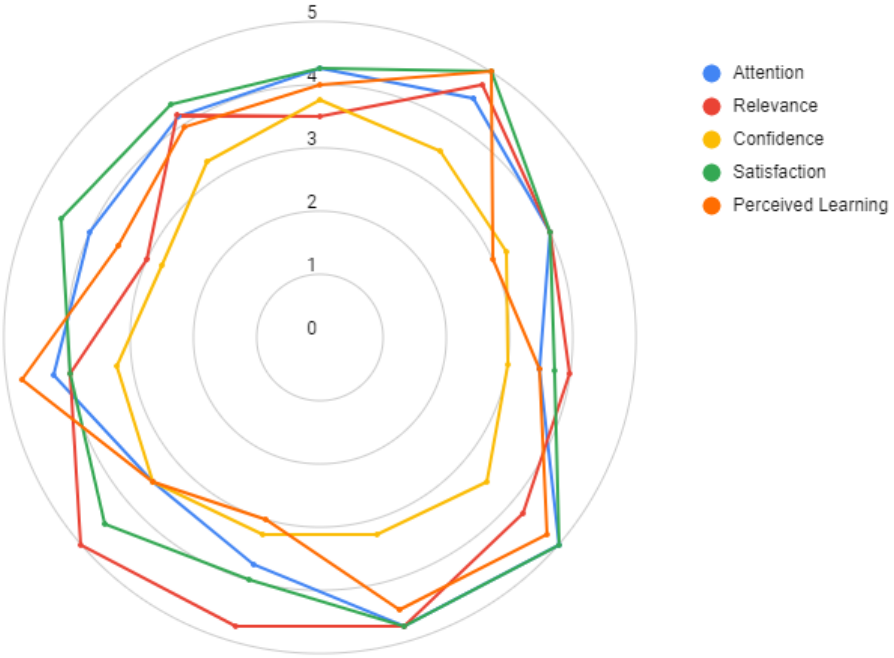


Σχήμα *Ε*.43: *Διάγραμμα με τα ποσοστά των σωστών απαντήσεων πριν και μετά τη συμμετοχή των παικτών στην έρευνα, καθώς και ο μέσος όρος αυτών*

Στις ερωτήσεις οι οποίες χρειάζονται πληροφορίες από το προαιρετικό περιεχόμενο του παιχνιδιού (ερωτήσεις 5, 6 και 8), στις ερωτήσεις 5 και 6 υπήρχε βελτίωση κατά 10% και 40% αντίστοιχα, ενώ στην ερώτηση 8 δεν παρουσιάστηκε βελτίωση. Στις ερωτήσεις 2, 3 και 13 όπου ο παίκτης θα χρειαστεί να δώσει περισσότερο προσοχή για να απαντήσει σωστά, δεν παρουσιάζεται βελτίωση για την ερώτηση 2 ενώ η ερώτηση 3 και 13 έχουν αύξηση κατά 30% και 20% αντίστοιχα, παρουσιάζοντας σημαντική βελτίωση αλλά λιγότερη σε σχέση με άλλες ερωτήσεις. Σημαντικά μεγάλη μείωση υπάρχει και στο πόσο των υποψηφίων που δε γνώριζαν κάποια απάντηση. Σε όλες τις ερωτήσεις αρχικά παρουσιάζεται τουλάχιστον ένας συμμετέχων

ο οποίο δήλωσε ότι δε γνωρίζει τη σωστή απάντηση. Έπειτα, στις 10 από τις 13 σημειώνεται μείωση στο ποσό των "Δε γνωρίζω" απαντήσεων, ενώ σε 7 ερωτήσεις, όλοι οι συμμετέχοντες δηλώσαν κάποια απάντηση που δεν είναι "Δε γνωρίζω".

Επιπλέον, στο σχήμα *Ε*.44 παρουσιάζεται διαγραμματικά οι απαντήσεις των υποψηφίων. Από την κλίμακα 1 έως 5 που παρουσιάζει το ερωτηματολόγιο, ο μέσος όρος του Attention είναι 4.15, 4.2 για το Relevance, 3.3 για το Confidence, 4.375 για το Satisfaction και 3.95 για το Perceived Learning. Οι παίκτες έδωσαν πολύ θετικά αποτελέσματα σε όλες τις κατηγορίες, εκτός από το Confidence το οποίο είχε πιο μεικτές απαντήσεις.



Σχήμα *Ε*.44: *Διάγραμμα με τις βαθμολογίες των παικτών στο ερωτηματολόγιο των ερωτήσεων βασισμένο στο μοντέλο ARCS και την επιπρόσθετη παράμετρο, το Perceived Learning*

Όπως παρουσιάζεται στο σχήμα *Ε*.43, γίνεται προφανές ότι υπάρχει σημαντική βελτίωση στις απαντήσεις των συμμετεχόντων. Αυτή η αύξηση παρατηρήθηκε έως 80% αλλά τα αποτελέσματα παρουσιάζουν μία μέση αύξηση σε 28%. Μεγαλύτερες βελτιώσεις σημειώνονται στις ερωτήσεις στις οποίες οι απαντήσεις παρουσιάζονται ξεκάθαρα μέσα στο σενάριο, είτε σε αυτές που η χρήση τους μέσα στο σενάριο ήταν εύκολη προς κατανόηση. Επίσης μεγάλη

αύξηση παρατηρήθηκε στην αυτοπεποίθηση των συμμετεχόντων προς τη σωστή απάντηση. Πολύ συχνά, οι συμμετέχοντες αρχικά δε γνώριζαν κάποια απάντηση, και μέσω του παιχνιδιού είχαν μεγαλύτερη αυτοπεποίθηση σχετικά με ποια είναι η σωστή απάντηση, παρόλο που μερικές από τις απαντήσεις παραμένουν λάθος. Σε ερωτήσεις απάνω σε βασικούς όρους της κυβερνοασφάλειας, ένα σημαντικά μεγάλο ποσοστό των συμμετεχόντων έδειξαν εξοικείωση προς αυτά. Τμήμα των ατόμων που δεν είχαν την εξοικείωση αυτή, έμαθαν για το θέμα μέσω του σεναρίου. Στις ερωτήσεις που είναι γύρω από το προαιρετικό υλικό του παιχνιδιού ή στο υλικό που χρειάζεται και απαιτεί την πιο βαθιά ενασχόληση με το παιχνίδι, δεν παρατηρήθηκε σημαντική διαφορά στην ποιότητα των απαντήσεων σε σχέση με τις άλλες ερωτήσεις, δείχνοντας ότι οι παίκτες δεν παρουσίασαν πρόβλημα με την αναγνώριση στοιχείων ανεξαρτήτως είδους περιεχομένου.

Σχετικά με τα αποτελέσματα του σχήματος *Ε.44* οι παίκτες παρουσίασαν θετικές απαντήσεις στο Attention, Relevance, Satisfaction και Perceived Learning του παιχνιδιού. Το σενάριο βοήθησε του παίκτες στο να αφοσιωθούν στο περιεχόμενο του σενάριο, καθώς το ίδιο το περιεχόμενο έχει μεγάλο βαθμό συσχέτισης με τον τομέα της κυβερνοασφάλειας. Συγκεκριμένα για το Satisfaction, περιέχει τις πιο θετικές απαντήσεις με 4.375/5, καθώς οι παίκτες θεώρησαν όλη την εμπειρία διασκεδαστική και ικανοποιητική προς αυτούς. Το Relevance επίσης ήταν υψηλό, επιδεικνύοντας τη χρησιμότητα του σεναρίου σε σχέση με στοιχεία της αληθινής ζωής. Το Perceived Learning είναι αρκετά υψηλό με 3.95, με τους παίκτες να αναφέρουν πως η εμπειρία τους ανέπτυξε τις γνώσεις τους προς την κυβερνοασφάλεια. Τέλος, στο Confidence παρατηρούμε το μικρότερο σκορ, με 3.3/5. Οι παίκτες κατά τη διάρκεια του σεναρίου εντόπισαν διάφορες δυσκολίες στο περιεχόμενο του παιχνιδιού, καθώς είχαν μικρή εξοικείωση με το περιβάλλον και τη χρήση των εργαλείων. Συνεπώς, το σενάριο ήταν μια εξαιρετικά θετική εμπειρία για τους παίκτες, καθώς συνδύασε τη διασκέδαση με τη μάθηση θεμάτων της κυβερνοασφάλειας, με τους παίκτες να δείχνουν ενδιαφέρον προς το περιεχόμενο. Ωστόσο, καθώς μερικοί όροι και εργαλεία είναι περίπλοκοι για παίκτες που δε διαθέτουν πολλές γνώσεις παρά πολύ βασικές, μια αρχική εξοικείωση της πλατφόρμας του Stinger OS με πιο αναλυτική εισαγωγή στα εργαλεία θα βοηθούσε τους παίκτες περαιτέρω.

Πίνακας *Ε*.14: *Απαντήσεις στην ερώτηση ανοικτού τύπου "Εξήγησε συνοπτικά τι έμαθες μέσω του παιχνιδιού"*

Απαντήσεις
Από το παιχνίδι έμαθα αρκετά πράγματα. 1) Εξερεύνηση του δικτύου 2) εξερεύνηση subdomain 3) πως πραγματοποιείται είσοδος στο δίκτυο 4) πως γίνεται παραβίαση password ανάλογα με πληροφορίες που γνωρίζουμε από τον χρήση.
Θυμήθηκα κυρίως θέματα σχετικά με το αντικείμενο
Κάποια πρωτόκολλα και εργαλεία που δεν ήξερα τις χρήσεις τους και γενικά κάποιες ενδιαφέρουσες πληροφορίες για τον Θαλή.
Τη διαδικασία και νοοτροπία του hacking.
Σίγουρα το ποσό "εύκολο" ήταν κάποιος να βρει πληροφορίες για εσένα όταν βρίσκεσαι συνδεδεμένος σε κάποιο δίκτυο, καθώς και το πως να αναλύω και να αποκωδικοποιώ καλύτερα συγκεκριμένα στοιχεία έτσι ώστε να βρίσκω περισσότερες πληροφορίες.
Τι είδους exploits μπορούν να χρησιμοποιηθούν στην κυβερνοασφάλεια.
Έμαθα καλύτερα τις λειτουργίες searchsploit, dig και λοιπά.
Το σενάριο μου έδειξε πως θα μπορούσε να γίνει μια επίθεση από το εξωτερικό μιας επιχείρησης προς το εσωτερικό της.
Νιώθω ότι έχω καλύτερη κατανόηση του πως δουλεύουν οι επιθέσεις κατά της κυβερνοασφάλειας.
Εύρεση ευπαθειών και τη χρήση τους για την πρόσβαση σε άλλα μηχανήματα. Τη δομή και λειτουργία των Domain, Subdomain και πως να βρίσκω, μέσα στο Port Scanning κλπ, να βρίσκω εκδόσεις υπηρεσιών και στη συνέχεια αντίστοιχων CVE. Επιπλέον, χρήση εργαλείων για Password Cracking, γενικότερο Information Retrieval!

Τα αποτελέσματα των απαντήσεων (Πίνακας *Ε*.14) δείχνουν ότι οι συμμετέχοντες απέκτησαν σημαντική γνώση σχετικά με βασικές έννοιες και τεχνικές της κυβερνοασφάλειας μέσω του παιχνιδιού. Συγκεκριμένα, αναφέρθηκαν σε πρακτικές διαδικασίες όπως η εξερεύνηση δικτύων και υποτομέων, η παραβίαση κωδικών με βάση πληροφορίες που συλλέγονται από χρήστες, καθώς και η αναγνώριση πρωτοκόλλων και εργαλείων που δεν ήταν προηγουμένως γνωστά. Επίσης, οι συμμετέχοντες εξοικειώθηκαν με τη διαδικασία και τις τεχνικές του ethical hacking, κατανοώντας πώς μπορεί κάποιος να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα μέσα από ευπάθειες των συστημάτων. Οι συμμετέχοντες εξέφρασαν ότι το παιχνίδι τους βοήθησε να κατανοήσουν καλύτερα τον τρόπο λειτουργίας των επιθέσεων κυβερνοασφάλειας και την εύρεση ευπαθειών σε δίκτυα και υπηρεσίες. Έμαθαν επίσης πώς να χρησιμοποιούν εργαλεία για την αναζήτηση ευπαθειών, την ανάλυση δεδομένων και την αποκωδικοποίηση πληροφοριών, με στόχο την εφαρμογή αυτών των γνώσεων σε πραγματικά σενάρια. Η εμπειρία αυτή τους έδωσε μια πιο ολοκληρωμένη κατανόηση της κυβερνοασφάλειας και τους προετοίμασε καλύτερα

για να αντιμετωπίσουν τέτοιες προκλήσεις στο μέλλον.

Πίνακας *Ε*.15: *Απαντήσεις στην ερώτηση ανοικτού τύπου "Περιέγραψε τη λειτουργία ή ανάφερε εντολές που χρησιμοποίησες στο παιχνίδι."*

Απαντήσεις
Αυτή η διαδικασία γινόταν αρκετά συχνά 1) εξερεύνηση των κόμβων στο δίκτυο 2) εύρεση κόμβων που έχουν αδυναμίες 3) εύρεση είδους αδυναμιών και λήψη στοιχείων για αυτές 4) παραβίαση των αδυναμιών βάση των στοιχείων που λάβαμε παραπάνω. 5) εισαγωγή βαθύτερα στο δίκτυο Πέρα από αυτά υπήρχαν ορισμένα σημεία που έπρεπε να βρεις κωδικούς των χρηστών και μέσω αυτών να αποκτήσεις πρόσβαση στους λογαριασμούς τους. Σε αυτά χρειαζόταν να χρησιμοποιήσεις ορισμένου αλγόριθμος προκειμένου να τους σπάσεις καθώς και να συλλέξεις πληροφορίες για τους χρήστες.
dig searchsploit netscan
airodump, searchsploit, netscan, dig, whois, password attack, xkeyscore, active directory, file browser, foxacid, exploit database, fingerprint, nmap
Dig, netscan
Netscan, dig, vulnerabilities, CVE, password attack, airodump, sfuzzer, Foxacid, ports
sfuzzer netscan dig fingerprint purge exit searchsploit
Fingerprint, searchploit, netscan, dig
Στην αρχή, χρησιμοποιώντας τις πληροφορίες που μου δόθηκαν, έψαξα για τα domains της IP που μου δόθηκαν, μετά βρήκα μια αδυναμία και μπήκα πιο βαθιά για να μπορέσω να μαζέψω στοιχεία χρησιμοποιώντας exploits και πληροφορίες οπότε ήταν χρήσιμα για να μπορέσω να λύσω το σενάριο. Με τη βοήθεια χαρακτήρων της ιστορίας κατάφερα να ξεσκεπάσω τον κακό της υπόθεσης και να εισχωρήσω στο σημείο που μου είχε αναθέσει το σενάριο.
Sfuzzer, searchploit, dig, fingerprint, netscan, help, ointscan, who is, aerodump
Searchsploit, Port Scanner, Password Cracker (John the Ripper, MD5 αλγόριθμος κλπ), WiFi hacking, FoxAcid

Οι απαντήσεις στην ερώτηση ανοικτού τύπου σχετικά με τις λειτουργίες και τις εντολές που χρησιμοποιήθηκαν στο παιχνίδι (Πίνακας *Ε*.15) δείχνουν τη μεγάλη ποικιλία εργαλείων και τεχνικών που εφαρμόστηκαν. Οι συμμετέχοντες ανέφεραν ότι η διαδικασία περιλάμβανε εξερεύνηση των κόμβων στο δίκτυο, ανίχνευση αδυναμιών, παραβίαση αυτών των αδυναμιών με βάση τα στοιχεία που συγκεντρώθηκαν και εισαγωγή βαθύτερα στο δίκτυο. Επιπλέον, χρησιμοποιήθηκαν εντολές και εργαλεία, για τη συλλογή και ανάλυση στοιχείων. Η χρήση αυτών των εργαλείων επιβεβαιώνει τη σημασία της συνδυασμένης εφαρμογής τεχνικών και εντολών για την επίλυση του σεναρίου. Οι συμμετέχοντες χρησιμοποίησαν εντολές για να εντοπίσουν ευπάθειες, να αναλύσουν στοιχεία και να επιτεθούν σε διάφορα σημεία του δικτύου. Αυτή η ποικιλία εργαλείων αντανακλά την πολυπλοκότητα των επιθέσεων και τη σημασία της

εξειδίκευσης στην κυβερνοασφάλεια, ενώ οι προσωπικές αναφορές επιβεβαιώνουν την αποτελεσματικότητα των εργαλείων στην επιτυχή ολοκλήρωση των αποστολών του παιχνιδιού.

Πίνακας *Ε*.16: *Απαντήσεις στην ερώτηση ανοικτού τύπου "Πιστεύεις ότι υπάρχουν πλεονεκτήματα σε σχέση με το αληθινό περιβάλλον; Αν ναι, ποια;"*

Απαντήσεις
Ορισμένα πλεονεκτήματα του παιχνιδιού σε σχέση με πραγματικό περιβάλλον είναι τα εξής. 1) Καλύτερο γραφικό περιβάλλον για τον χρήση σε σχέση με μια γραμμή εντολών 2) Σε ορισμένα σημεία, όπως σε αυτά που προσπαθούσες να σπάσεις κωδικούς ασφαλείας το περιβάλλον μου άρεσε οπτικά σε σχέση με την εισαγωγή παραμέτρων σε γραμμή εντολών.
Ναι, είναι πιο εύκολο και οργανωμένο σε σχέση με ένα κανονικό σύστημα Linux
Το UI βοηθάει αρκετά στη διατήρηση της προσοχής μου σε αντίθεση με ένα απλό μαύρο command prompt και κάνει την όλη διαδικασία λίγο πιο ευχάριστη, ειδικά το ότι έχω τη δυνατότητα για πολλαπλές επιφάνειες εργασίας
Ναι το βασικό πλεονέκτημα κατά τη γνώμη μου είναι ότι είναι παιχνίδι και κάνει τη διαδικασία ποιο ελκυστική.
Ίσως. Πιστεύω πως αν δεν είχα καμία καθοδήγηση ενώ έπαιζα το παιχνίδι, δεν θα υπήρχε κάποιο πλεονέκτημα λόγω του ότι δεν είχα ασχοληθεί προηγουμένως με το αντικείμενο.
Υπάρχουν ξεκάθαρα πλεονεκτήματα, όπως η καθοδήγηση και το βοηθητικό UI
Ναι είναι πολύ πιο φιλικό στον χρήστη
Το ui και το qol κάνει την εμπειρία πιο συμβατή προς τον χρήστη.
Σε αληθινό περιβάλλον υπάρχουν αρκετά πιο πολλές επιλογές, το οποίο το κάνει πιο δύσκολο λογικά.
Ευκολία στη χρήση, καλύτερη οργάνωση των εργαλείων, και επεξήγηση του για το τι κάνουν.

Οι απαντήσεις στην ερώτηση ανοικτού τύπου σχετικά με τα πλεονεκτήματα του παιχνιδιού σε σχέση με το πραγματικό περιβάλλον (Πίνακας *Ε*.16) καταδεικνύουν διάφορους τρόπους με τους οποίους η ψηφιακή μάθηση μπορεί να προσφέρει βελτιωμένη εμπειρία. Οι συμμετέχοντες αναγνωρίζουν ότι το παιχνίδι προσφέρει ένα πιο οργανωμένο και φιλικό προς τον χρήστη περιβάλλον σε σύγκριση με τα παραδοσιακά συστήματα Linux και τις γραμμές εντολών. Η γραφική διεπαφή του παιχνιδιού και οι πολλαπλές επιφάνειες εργασίας βοηθούν στη διατήρηση της προσοχής και κάνουν τη διαδικασία πιο ευχάριστη. Επιπλέον, το παιχνίδι προσφέρει καθοδήγηση και έναν βοηθητικό χρήστη διεπαφή (UI) που διευκολύνει τη μάθηση και την κατανόηση των εργαλείων και των διαδικασιών. Αυτά τα χαρακτηριστικά καθιστούν την εμπειρία πιο προσιτή και ελκυστική, σε αντίθεση με τα πιο σύνθετα και λιγότερο φιλικά προς τον χρήστη περιβάλλοντα του πραγματικού κόσμου. Ωστόσο, ορισμένοι συμμετέχοντες σημειώνουν ότι, αν δεν είχαν προηγούμενη εμπειρία με το αντικείμενο, το παιχνίδι μπορεί να μην προσφέρει σημαντικά πλεονεκτήματα χωρίς την κατάλληλη καθοδήγηση.

Πίνακας *Ε*.17: *Απαντήσεις στην ερώτηση ανοικτού τύπου "Τι θα ήθελες να είναι διαφορετικό για να γίνει πιο αποδοτική η εκμάθηση μέσω του παιχνιδιού;"*

Απαντήσεις
Πιο εύκολη διαχείριση των παραθύρων. Πιστεύω αυτό ήταν το μόνο κουραστικό σε όλη τη διαδικασία. Σε κάθε terminal όταν πραγματοποιείς πολλές δοκιμές δεν μπορείς να ανέβεις αρκετά πάνω ώστε να δεις και στη συνέχεια να αλλάξεις 1) τυπογραφικά λάθη που έχεις κάνει 2) παραμέτρους που εισάγεις στις εντολές.
Να βελτιωθεί το UI για να είναι όλα πιο οργανωμένα
Ίσως αν είναι εφικτό, να μιλάει λίγο παραπάνω το AI της φωνής για να εξηγεί το κάθε goal ή να παρέχει tips αντί να γίνεται με τη χρήση του google docs παράλληλα για να είναι πιο immersive. Ή πολύ απλά να παρέχεται το doc μέσα στα αρχεία του παιχνιδιού και να τα βλέπουμε εκεί. Μικρής σημασίας πράγματα γενικά αλλά ίσως να έκαναν πιο γρήγορη και γραμμική τη διαδικασία
Δεν είμαι σίγουρος
Κάποιου είδους tutorial που να παρέχει παράδειγμα χρήσης των κάθε commands. Αλλιώς πιο μικρές και απλοϊκές επεξηγήσεις ή υποδείξεις.
Δεν ξέρω
Όχι
Μερικά στοιχεία που δεν υπάρχουν μέσα στο παιχνίδι να γίνει η εισαγωγή τους μέσα στο περιβάλλον του σενάριο και λίγο καλύτερο qol για μερικά copy paste πράγματα.
Ότι μένει αχρησιμοποίητο από το παιχνίδι για το σενάριο, να κρύβεται Γενικά είναι εύκολο να χαθείς αν δεν οργανώσεις σωστά τα παράθυρα και εργαλεία από μόνος σου.
Γνώση των υπάρχων εργαλείων εντός του παιχνιδιού πριν την εισαγωγή σε ένα σενάριο.

Οι απαντήσεις στην ερώτηση ανοικτού τύπου για τη βελτίωση της εκμάθησης μέσω του παιχνιδιού (Πίνακας *Ε*.17) δείχνουν διάφορες προτάσεις που επικεντρώνονται κυρίως στη βελτίωση της χρηστικότητας και της οργάνωσης του περιβάλλοντος. Πολλοί συμμετέχοντες επισημαίνουν την ανάγκη για καλύτερη διαχείριση των παραθύρων και πιο οργανωμένο UI, καθώς η τρέχουσα διάταξη μπορεί να είναι δυσχέρεια και να προκαλεί σύγχυση κατά τη διάρκεια της εκμάθησης.

Άλλες προτάσεις περιλαμβάνουν την ενσωμάτωση περισσότερων βοηθητικών στοιχείων, όπως αναλυτικές εξηγήσεις ή βοήθεια και υποστήριξη μέσω του AI του παιχνιδιού, αντί της χρήσης εξωτερικών εγγράφων. Επιπλέον, προτείνεται η δημιουργία ενός οδηγού που να εξηγεί τη χρήση των εντολών ή η ενσωμάτωση περισσότερων στοιχείων και εργαλείων στο περιβάλλον του παιχνιδιού για να διευκολυνθεί η διαδικασία. Τέλος, η οργάνωση και η διαχείριση των εργαλείων και παραθύρων, καθώς και η κρυφή εμφάνιση μη χρησιμοποιούμενων στοιχείων, θα μπορούσαν να βελτιώσουν την εμπειρία του χρήστη και να μειώσουν την ακαταστασία.

Στις ερωτήσεις ανοικτού τύπου, όλοι οι συμμετέχοντες ανέφεραν τουλάχιστον ένα στοιχείο που έμαθαν, με τις απαντήσεις να διαφέρουν από άτομο σε άτομο με βάση τι θεώρησαν πιο ενδιαφέρον. Επίσης, σωστά περιέγραψαν τις λειτουργίες που πραγματοποίησαν ή ανέφεραν μερικές από τις εντολές τις οποίες χρησιμοποίησαν. Σχετικά με τα πλεονεκτήματα που προσφέρει η πλατφόρμα του NITE Team 4 σε σχέση με ένα αληθινό σύστημα, πολύ συχνή αναφορά γίνεται στη φιλικότητα προς τον χρήστη και το UI καθώς και στην ποσότητα καθοδήγησης σε σχέση με ένα αληθινό σύστημα. Η διατύπωση της πλατφόρμας και του σεναρίου βοήθησε τους παίκτες στην καλύτερη αντιμετώπιση του ίδιου του σεναρίου. Στις πιθανές βελτιώσεις που ανέφεραν οι παίκτες, πολύ συχνή είναι η αναφορά στην ύπαρξη καλύτερης οργάνωσης των τερματικών παραθύρων στην πλατφόρμα. Συχνή αναφορά υπάρχει και στην ύπαρξη ενός καλύτερου τρόπου να εξοικειωθούν οι παίκτες με τα εργαλεία ή ενδεχομένως να είναι ήδη εξοικειωμένοι πριν την αρχή του σεναρίου.

Κεφάλαιο Z

Συμπεράσματα

Στα πλαίσια της εργασίας, εξετάστηκε η αποτελεσματικότητα της ψηφιακής μάθησης μέσω του DGBL με τη χρήση ενός εκπαιδευτικού σεναρίου βασισμένο στο παιχνίδι NITE Team 4. Αρχικά, έγινε εξέταση της αποτελεσματικότητας του DGBL, ερευνώντας κατά πόσο η ψηφιακή μάθηση μέσω παιχνιδιού μπορεί να βελτιώσει την εκπαίδευση στον τομέα της κυβερνοασφάλειας, προσφέροντας μια εναλλακτική προσέγγιση σε σύγκριση με τις παραδοσιακές μεθόδους. Στη συνέχεια, δημιουργήθηκε ένα εκπαιδευτικό σενάριο στο NITE Team 4, το οποίο σχεδιάστηκε ώστε να προσομοιώνει πραγματικές κυβερνοαπειλές και τεχνικές, παρέχοντας στους συμμετέχοντες μια ρεαλιστική και πρακτική εμπειρία μάθησης. Επιπλέον, αναπτύχθηκε επιπρόσθετο περιεχόμενο εκτός παιχνιδιού που ενίσχυσε την εμβύθιση των παικτών στον κόσμο της κυβερνοασφάλειας, βοηθώντας τους να κατανοήσουν καλύτερα τις σχετικές έννοιες και διαδικασίες. Οι συμμετέχοντες ήρθαν σε επαφή με διάφορες έννοιες και προκλήσεις του τομέα, τις οποίες έπρεπε να αντιμετωπίσουν, ενισχύοντας έτσι την πρακτική τους κατανόηση. Η αποτελεσματικότητα του DGBL αξιολογήθηκε μέσω του ARCS μοντέλου, το οποίο αναλύει την προσοχή, τη συνάφεια, την αυτοπεποίθηση και την ικανοποίηση των συμμετεχόντων. Μέσω ερωτηματολογίων συλλέχθηκαν εμπειρικά δεδομένα και αναλύθηκαν τα αποτελέσματα. Τα ευρήματα της έρευνας έδειξαν ότι το σενάριο ήταν αποτελεσματικό στην ενίσχυση της γνώσης των συμμετεχόντων στον τομέα της κυβερνοασφάλειας.

Οι συμμετέχοντες ανέφεραν ότι η εμπειρία τους βοήθησε να κατανοήσουν καλύτερα τις τεχνικές και τις διαδικασίες του τομέα, εκφράζοντας ταυτόχρονα το ενδιαφέρον τους για παρόμοιες μορφές μάθησης στο μέλλον. Τέλος, προτίμησαν αυτή τη διαδραστική προσέγ-

γιση έναντι των παραδοσιακών μεθόδων εκπαίδευσης. Συμπερασματικά, το DGBL και η ενσωμάτωση σεναρίων κυβερνοασφάλειας μπορούν να αποτελέσουν μια αποτελεσματική εναλλακτική για την εκπαίδευση στον τομέα αυτό, προσελκύοντας το ενδιαφέρον των μαθητών και ενισχύοντας τη μάθησή τους μέσω ενεργής συμμετοχής και εμβύθισης.

Τα θετικά στοιχεία του σεναρίου φαίνονται και στις απαντήσεις των παικτών, με όλους τους συμμετέχοντες να νιώθουν ευχαρίστηση και ικανοποίηση. Όλοι οι συμμετέχοντες επίσης αξιολόγησαν το περιεχόμενο ως χρήσιμο, με την πλειοψηφία να επιθυμεί να μάθει με έναν παρόμοιο τρόπο. Το σενάριο επίσης έδωσε επιπλέον ενδιαφέρον στους συμμετέχοντες σχετικά με την κυβερνοασφάλεια και σε μικρότερο βαθμό με γενικά διάφορους τομείς τεχνολογίας. Παρόλο που οι συμμετέχοντες έδειξαν και εξέφρασαν ικανοποίηση και με το σενάριο αλλά και με τις γνώσεις που έλαβαν, υπάρχει χώρος για βελτίωση, και συγκεκριμένα η ύπαρξη μιας πιο ομαλής εισαγωγής στα εργαλεία του παιχνιδιού. Συγκεκριμένα για το NITE Team 4 και το Stinger OS, η πλειοψηφία των παικτών επιθυμεί μια βελτίωση των UI στοιχείων, καθώς η διαχείριση των τερματικών είναι άβολη στην περίπτωση που πρέπει να χρησιμοποιηθούν πολλαπλά εργαλεία ταυτόχρονα. Ωστόσο, παρόλο που συγκεκριμένα στοιχεία ίσως να ήταν πιο δύσχρηστα, οι συμμετέχοντες ανέφεραν ότι είναι πιο φιλικά σε σχέση με τις πραγματικές εναλλακτικές που διαθέτουμε όπως συστήματα UNIX / LINUX. Μέσω αυτών, θεωρούμε ότι η χρήση εκπαιδευτικών σεναρίων GBL στην εκπαίδευση της κυβερνοασφάλειας θα βελτιώσει το ποσό ενδιαφέροντος αλλά και την ποιότητα γνώσης την οποία αποκτούν οι μαθητές, παρουσιάζοντας μια πιο μοντέρνα μέθοδο μάθησης η οποία ανταποκρίνεται στις ανάγκες των μαθητών και στο τρόπο με τον οποίο επιθυμούν να μάθουν. Τα αποτελέσματα μας υποστηρίζουν ότι η ύπαρξη σεναρίων κυβερνοασφάλειας μέσω παιχνιδιών ενισχύει την εκπαιδευτική διαδικασία.

Z.1 Μελλοντικές Εργασίες - Βελτιώσεις

Λόγω του μικρού αριθμού των συμμετεχόντων, θεωρούμε ότι μελλοντικά θα ήταν χρήσιμη η εκτέλεση παρόμοιου πειράματος σε μεγαλύτερο πλήθος ατόμων και χρησιμοποιώντας μια μεγαλύτερη ομάδα ερωτήσεων. Το σενάριο και ο τρόπος με τον όποιο οι παίκτες εξοικειώνονται με το παιχνίδι έχει περιθώριο να βελτιωθεί, οπότε ενδεχομένως να υπάρχουν καλύτερα αποτελέσματα με τη βελτίωση αυτού. Καθώς η εργασία εξέτασε τις γνώσεις που αποκτούν οι συμμετέχοντες βραχυπρόθεσμα, και στην εκπαιδευτική διαδικασία είναι επίσης σημαντικό να εξεταστεί κατά πόσο υπάρχει εμπέδωση του περιεχομένου, χρήσιμη θα είναι και η εξέ-

ταση των γνώσεων των παικτών μετά από κάποιο διάστημα χρόνου. Ενδιαφέρον είναι και η εξέταση του συγκεκριμένου περιεχομένου το οποίο μαθαίνουν οι παίκτες, και αν υπάρχει κάποιο συγκεκριμένο είδος το οποίο είναι πιο προσιτό στο GBL, ωστόσο μία τέτοια προσέγγιση θα χρειαστεί εκτενή έρευνα. Τέλος, παρόλο που το σενάριο παρουσιάζει στοιχεία ARG, μελλοντικά θα ήταν καλό να εξεταστεί και τα κοινωνικά οφέλη των ARG στα πλαίσια εκπαιδευτικών αλλά και μη σεναρίων, όπως στην πιθανή ανάπτυξη του λογαριασμού X/Twitter που χρησιμοποιήθηκε στα πλαίσια της εργασίας.

Βιβλιογραφία

[1] Magdalena Kowal et al. "Gaming your mental health: a narrative review on mitigating symptoms of depression and anxiety using commercial video games". In: *JMIR Serious Games* 9.2 (2021), e26575.

[2] Abdul Azis Wahab, Purnama Syae Purrohman, Evy Segarawati Ampry, et al. "Internet user behavior and social media in learning". In: *4th International Conference on Research of Educational Administration and Management (ICREAM 2020)*. Atlantis Press. 2021, pp. 50–55.

[3] Laura DeNardis. *The Internet in everything*. Yale University Press, 2020.

[4] Giddeon N Angafor, Iryna Yevseyeva, and Ying He. "Bridging the cyber security skills gap: Using tabletop exercises to solve the CSSG crisis". In: *Joint International Conference on Serious Games*. Springer. 2020, pp. 117–131.

[5] Steven Furnell. "The cybersecurity workforce and skills". In: *Computers & Security* 100 (2021), p. 102080.

[6] Razvan Beuran et al. "Cybersecurity education and training support system: CyRIS". In: *IEICE TRANSACTIONS on Information and Systems* 101.3 (2018), pp. 740–749.

[7] Manzoor Ahmed Khan et al. "Game-based learning platform to enhance cybersecurity education". In: *Education and Information Technologies* (2022), pp. 1–25.

[8] John M Keller. "Development and use of the ARCS model of instructional design". In: *Journal of instructional development* 10.3 (1987), pp. 2–10.

[9] Gary R Pike. "The relationship between perceived learning and satisfaction with college: An alternative view". In: *Research in Higher Education* 34 (1993), pp. 23–40.

[10] Stylianos Karagiannis and Emmanouil Magkos. "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: Papers in Honor of Professor Nikolaos Alexandris* (2021), pp. 55–81.

[11] Filippos Giannakas et al. "A comprehensive cybersecurity learning platform for elementary education". In: *Information Security Journal: A Global Perspective* 28.3 (2019), pp. 81–106.

[12] Zi-Yu Liu, Zaffar Ahmed Shaikh, and Farida Gazizova. "Using the Concept of Game-Based Learning in Education." In: *International Journal of Emerging Technologies in Learning* (2020).

[13] Maxwell Hartt, Hadi Hosseini, and Mehrnaz Mostafapour. "Game on: Exploring the effectiveness of game-based learning". In: *Planning Practice & Research* 35.5 (2020), pp. 589–604.

[14] Surattana Adipat et al. "Engaging students in the learning process with game-based learning: The fundamental concepts." In: *International Journal of Technology in Education* 4.3 (2021), pp. 542–552.

[15] Menelaos N Katsantonis, Ioannis Mavridis, and Dimitris Gritzalis. "Design and evaluation of cofelet-based approaches for cyber security learning and training". In: *Computers & Security* 105 (2021), p. 102263.

[16] Sandra Elsom, Colleen Stieler-Hunt, and Margaret Marshman. "Supporting learning in higher education with a curriculum-embedded alternate reality game". In: *Interactive Learning Environments* (2023), pp. 1–12.

[17] Vlasios Kasapakis and Damianos Gavalas. "Pervasive gaming: Status, trends and design principles". In: *Journal of Network and Computer Applications* 55 (2015), pp. 213–236.

[18] Huei-Tse Hou, Ying-Sang Fang, and Joni Tzuchen Tang. "Designing an alternate reality board game with augmented reality and multi-dimensional scaffolding for promoting spatial and logical ability". In: *Interactive Learning Environments* 31.7 (2023), pp. 4346–4366.

[19] Lasse Hakulinen et al. "Gameful approaches for computer science education: from gamification to alternate reality games". In: (2015).

[20] Atasi Mohanty et al. “Design and development of digital game-based learning software for incorporation into school syllabus and curriculum transaction”. In: *Design Engineering* 8 (2021), pp. 4864–4900.

[21] Berna Karakoç et al. “The effect of game-based learning on student achievement: A meta-analysis study”. In: *Technology, Knowledge and Learning* 27.1 (2022), pp. 207–222.

[22] Jan L Plass, Bruce D Homer, and Charles K Kinzer. “Foundations of game-based learning”. In: *Educational psychologist* 50.4 (2015), pp. 258–283.

[23] Georgios Lampropoulos. “Educational benefits of digital game-based learning: K-12 teachers’ perspectives and attitudes”. In: *Advances in Mobile Learning Educational Research* 3.2 (2023), pp. 805–817.

[24] Juliana Tay et al. “Designing digital game-based learning for professional upskilling: A systematic literature review”. In: *Computers & Education* 184 (2022), p. 104518.

[25] Elina Jääskä et al. “Game-based learning and students’ motivation in project management education”. In: *Project Leadership and Society* 3 (2022), p. 100055.

[26] Anissa All, Elena Nunez Patricia Castellar, and Jan Van Looy. “Digital Game-Based Learning effectiveness assessment: Reflections on study design”. In: *Computers & Education* 167 (2021), p. 104160.

[27] Andrew Emerson et al. “Multimodal learning analytics for game-based learning”. In: *British Journal of Educational Technology* 51.5 (2020), pp. 1505–1526.

[28] Richard E Mayer. “Computer games in education”. In: *Annual review of psychology* 70 (2019), pp. 531–549.

[29] Mohadeseh Zohari et al. “Comparison of gamification, game-based learning, and serious games in medical education: a scientometrics analysis”. In: *Journal of Advances in Medical Education & Professionalism* 11.1 (2023), p. 50.

[30] E Jääskä and K Aaltonen. *Teachers’ experiences of using game-based learning methods in project management higher education. Project Leadership and Society, 3, 100041.* 2022.

[31] Qi Zhang and Zhonggen Yu. "Investigating and Comparing the Effects on Learning Achievement and Motivation for Gamification and Game-Based Learning: A Quantitative Study Employing Kahoot". In: *Education Research International* 2022.1 (2022), p. 9855328.

[32] Jeanine Krath, Linda Schürmann, and Harald FO Von Korflesch. "Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning". In: *Computers in Human Behavior* 125 (2021), p. 106963.

[33] Fazlida Dahalan, Norlidah Alias, and Mohd Shahril Nizam Shaharom. "Gamification and game based learning for vocational education and training: A systematic literature review". In: *Education and Information Technologies* 29.2 (2024), pp. 1279–1317.

[34] Nibu John Thomas, Rupashree Baral, and Oliver S Crocco. "Gamification for HRD: Systematic review and future research directions". In: *Human Resource Development Review* 21.2 (2022), pp. 198–224.

[35] Katrin Becker. "What's the difference between gamification, serious games, educational games, and game-based learning". In: *Academia Letters* 209.2 (2021).

[36] Xiao Hu, Hongzhi Zhang, and Zane Ma Rhea. "Alternate reality game in education: a literature review". In: *AARE* (2016), pp. 1–16.

[37] Ronan Lynch, Bride Mallon, and Cornelia Connolly. "The pedagogical application of alternate reality games: Using game-based learning to revisit history". In: *International Journal of Game-Based Learning (IJGBL)* 5.2 (2015), pp. 18–38.

[38] Thomas M Connolly, Mark Stansfield, and Thomas Hainey. "An alternate reality game for language learning: ARGuing for multilingual motivation". In: *Computers & Education* 57.1 (2011), pp. 1389–1415.

[39] Alex Moseley. "An alternate reality for education?: Lessons to be learned from online immersive games". In: *International Journal of Game-Based Learning (IJGBL)* 2.3 (2012), pp. 32–50.

[40] Valdemar Švábenskỳ et al. "Cybersecurity knowledge and skills taught in capture the flag challenges". In: *Computers & Security* 102 (2021), p. 102154.

[41] Stela Kucek and Maria Leitner. "An empirical survey of functions and configurations of open-source capture the flag (ctf) environments". In: *Journal of Network and Computer Applications* 151 (2020), p. 102470.

[42] Jan Vykopal, Valdemar Švábenskỳ, and Ee-Chien Chang. "Benefits and pitfalls of using capture the flag games in university courses". In: *Proceedings of the 51st ACM Technical symposium on computer science education*. 2020, pp. 752–758.

[43] Stylianos Karagiannis, Elpidoforos Maragkos-Belmpas, and Emmanouil Magkos. "An analysis and evaluation of open source capture the flag platforms as cybersecurity e-learning tools". In: *IFIP World Conference on Information Security Education*. Springer. 2020, pp. 61–77.

Συντμήσεις

AI	Artificial Intelligence
ARG	Alternate Reality Games
CTF	Capture the Flag
CVE	Common Vulnerabilities and Exposures
DGBL	Digital Game Based Learning
GBL	Game-Based Learning
HTB	Hack The Box
IP	Internet Protocol
MAC	Media Access Control
TBW	The Black Watchmen
VPN	Virtual Private Network

`WMI`	Windows Management Instrumentation
`UI/UX`	User Interface / User Experience

Γλωσσάρι Ξενικών Όρων

Advanced Tools	Προχωρημένα Εργαλεία
Alternate Reality Game	Παιχνίδι Εναλλακτικής Πραγματικότητας
Artificial Intelligence	Τεχνητή Νοημοσύνη
Attention	Προσοχή
Cyberbullying	Διαδικτυακός Εκφοβισμός
Capture the Flag	Πίασε την Σημαία
Checkpoint	Σημείο Ελέγχου
Command Line	Γραμμή Εντολών
Confidence	Αυτοπεποίθηση
Data Forensic	Εγκληματολογία Δεδομένων
Dictionary Attack	Επίθεση Λεξικού

Digital Game Based Learning	Ψηφιακή Μάθηση Μέσω του Παιχνιδιού
Directory	Κατάλογος Αρχείων
Domain	Ηλεκτρονικός Χώρος
Email	Ηλεκτρονικό Ταχυδρομείο
Email Crawler	Ανιχνευτής Ηλεκτρονικού Ταχυδρομείου
Endpoint	Ακραίο Σημείο Επικοινωνίας
File Management System	Σύστημα Αρχειοθέτησης
Flag	Σημαία
Game-Based Learning	Μάθηση με Βάση το Παιχνίδι
Gamification	Παιχνιδοποίηση
Hacker	Χάκερ
Hacking	Ηλεκτρονική Παρείσφρηση
Information Gathering	Συλλογή Πληροφοριών
Internet Protocol	Διαδικτυακό Πρωτόκολλο

`Internet Protocol Address`	Διεύθυνση Διαδικτυακού Πρωτοκόλλου
`MAC Address`	Διεύθυνση MAC
`Module`	Μονάδα
`Network Intrusion`	Διάρρηξη Δικτύου
`Password Hash`	Κατακερματισμένος Κωδικός
`Payload`	Φορτίο Πληροφοριών
`Path`	Μονοπάτι
`Penetration Testing`	Δοκιμή Διείσδυσης
`Perceived Learning`	Αντιληπτή Μάθηση
`Port`	Θύρα
`Private`	Ιδιωτικός
`Public`	Δημόσιος
`Puppet Master`	Μαριονετίστας
`Rabbit Hole`	Λαγουδότρυπα
`Relevance`	Σχετικότητα

Satisfaction	Ευχαρίστηση
Scan	Σάρωση
Smart Home	Έξυπνο Σπίτι
Smart City	Έξυπνη Πόλη
Subdomain	Ηλεκτρονικός Υπο-χώρος
Subnet	Υποδίκτυο
Terminal	Τερματικό
User Interface / User Experience	Διεπαφή και Εμπειρία Χρήστη
Virtual Private Network	Εικονικό Ιδιωτικό Δίκτυο

Ευρετήριο

A

Active Directory 28, 59, 60

AI 38, 42

Aircrack-ng 28

ARCS 4-6

ARG 2-3, 13-15, 43, 57

C

CTF 17-19, 21-22

CVE 27, 59

CyberDefenders 22-23

G

Gamification 11-12, 17-22

GBL 1-5, 9-12

H

Hacknet 16-17

Hack The Box 18-19

Hivemind Network 15-16, 36, 45-46

Hivemind Network Administrator 15-16, 47-52

J

John the Ripper 31

M

Metasploit 28

MitM 31

N

NITE Team 4 4, 14-16, 24-52, 57-60

Nmap 27

O

Operation: Clear Water 6, 53-54, 62-65

P

Penetration Testing 61

S

Stinger OS 14-15, 26-39

T

TryHackMe 19-22

U

UI/UX NITE Team 4 24-39

V

Vulnhub 61

W

WMI 28, 49

X

XKeyscore 34, 50-51

Δ

Διαφορές GBL-Gamification 11-12

Θ

Θαλής 61

Σ

Σχεδίαση σεναρίου NITE Team 4 53-65