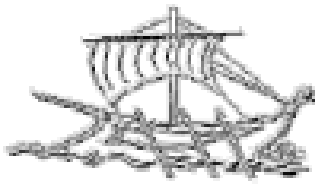


ΑΕΙ ΠΕΙΡΑΙΑ Τ.Τ.

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Δοκιμές και Έλεγχος Διείσδυσης για Διάγνωση και Ανίχνευση Ευπαθειών σε Ασύρματα Δίκτυα Δεδομένων

Ευάγγελος Δ. Κατσαδούρος

Εισηγητής: Δρ Χαράλαμπος Πατρικάκης, Αναπληρωτής Καθηγητής

ΑΘΗΝΑ

ΜΑΡΤΙΟΣ 2017

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Δοκιμές και Έλεγχος Διείσδυσης για Διάγνωση και Ανίχνευση Ευπαθειών σε Ασύρματα Δίκτυα Δεδομένων

Ευάγγελος Δ. Κατσαδούρος

Α.Μ. 43024

Εισηγητής:

Δρ Χαράλαμπος Πατρικάκης, Αναπληρωτής Καθηγητής

Εξεταστική Επιτροπή:

Ημερομηνία εξέτασης

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος, **Κατσαδούρος Ευάγγελος**

του **Δημητρίου**, με αριθμό μητρώου **43024** φοιτητής του Τμήματος Μηχανικών Η/Υ Συστημάτων Τ.Ε. του Α.Ε.Ι. Πειραιά Τ.Τ. πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασης της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Π.Ε. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα προβλεπόμενα στο άρθρο 18, παρ. 5 του ισχύοντος Εσωτερικού Κανονισμού.»

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα πτυχιακή εργασία ολοκληρώθηκε μετά από επίμονες προσπάθειες, σε ένα ενδιαφέρον γνωστικό αντικείμενο, όπως αυτό της δοκιμής διείσδυσης σε ασύρματα δίκτυα δεδομένων. Την προσπάθειά μου αυτή υποστήριξε ο επιβλέπων καθηγητής μου Χαράλαμπος Πατρικάκης, τον οποίο θα ήθελα να ευχαριστήσω.

Ακόμα θα ήθελα να ευχαριστήσω την οικογένειά μου για την δύναμη και την εμψύχωση που μου έδινε καθ' όλη τη διάρκεια των σπουδών μου.

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή αποτελείται από έξι ενότητες, οι οποίες παρουσιάζονται συνοπτικά στη συνέχεια. Στη 1η ενότητα γίνεται εισαγωγή στο αντικείμενο της πτυχιακής, Δοκιμή Διείσδυσης για Διάγνωση και Ανίχνευση Ευπαθειών σε Ασύρματα Δίκτυα Δεδομένων και ιστορική αναδρομή πάνω σε αυτό. Στη συνέχεια στη 2η ενότητα γίνεται παρουσίαση ασυρμάτων τεχνολογιών δικτύωσης αναλύοντας την αρχιτεκτονική τους, τον τρόπο λειτουργίας τους και την ασφάλειά τους. Η τρίτη ενότητα ασχολείται με τους εισβολείς (hackers) και τις επιθέσεις (attacks) τις οποίες προσπαθεί να αντιμετωπίσει και να περιορίσει ο τομέας της ασφάλειας δικτύων. Αναφέρονται και εξηγούνται βασικές επιθέσεις σε ασύρματα δίκτυα δεδομένων και αναλύονται όλοι οι τύποι εισβολών που υπάρχουν. Στην 4η ενότητα, Διάγνωση Ευπαθειών, γίνεται ανάλυση του όρου Ευπάθεια, των διαφορών ανάμεσα σε μια απλή αναζήτηση ευπαθειών και στη δοκιμή διείσδυσης σε ασύρματα δίκτυα δεδομένων, στην μεθοδολογία της δοκιμής διείσδυσης, στους τύπους αυτής και στα εργαλεία τα οποία μπορούμε να χρησιμοποιήσουμε. Στη 5η ενότητα υπάρχει σενάριο δοκιμής διείσδυσης σε ασύρματο δίκτυο δεδομένων με πραγματικά δεδομένα και περνώντας από όλες τις φάσεις της μεθοδολογίας. Στην 6η ενότητα, η οποία αποτελεί τη τελευταία ενότητα της πτυχιακής αυτής, γίνεται σχολιασμός της πτυχιακής και αναφέρονται όλα τα συμπεράσματα που εξήχθησαν κατά την έρευνα για την εγγραφή της πτυχιακής αλλά και προτάσεις για την αντιμετώπιση προβλημάτων ασφάλειας.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: ασύρματα δίκτυα δεδομένων, δοκιμή διείσδυσης, επίθεση σε δίκτυα υπολογιστών, πρωτόκολλα επικοινωνίας, πρωτόκολλα ασφάλειας

ABSTRACT

The present thesis consists of six modules, which are summarized below. In the first section, the introduction to the subject of thesis Penetration Testing for Vulnerability Diagnosis and Detection in Wireless Data Networks and its history. In the second section we present various wireless networking technologies by analyzing their architecture, the way they are work and their security. The third section deals with hackers and attacks which are issues that the security is called upon to solve. Explanations regarding basic attacks to wireless data networks and all types of hackers are also provided.. In the fourth section, Vulnerability Diagnosis, we analyze the term vulnerability, the differences between a simple vulnerability search and penetration testing on wireless data networks, penetration testing methodology, the types of this and the tools that can be used for a penetration test. The fifth section consists of a penetration test scenario to a wireless data network with real data and utilizing all the phases of the methodology. In the sixth section which is the last, there are some comments on the thesis and all the findings which came up during the research for registration of said thesis are listed. Finally some proposals to deal with security problems are being provided.

SCIENTIFIC AREA: NETWORK SECURITY

KEYWORDS: wireless data networks, penetration testing, computer networks attacks, communication protocols, security protocols

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

WLAN Wireless Local Area Network

WPAN Wireless Personal Area Network

AP Access Point

MAC Media Access Control Address

LLC Logical Link Control

MIMO Multiple-Input and Multiple-Output

WEP Wired Equivalent Privacy

TKIP Temporal Key Integrity Protocol

CCMP Counter Mode Cipher Block Chaining Message Authentication CODE PRO-TOCOL

WPA WI-FI Protected Access

WPA2 WI-FI Protected Access II

HCI Host Controller Interface

ACL Asynchronous Connection-Less

TCS Telephony Control Protocol

SDP Service Discovery Protocol

SoF Start of Frame

EoF End of Frame

AES Advanced Encryption Standard

DoS Denial of Service

PSK Phase-Shift Keying

GPU Graphics Processing Unit

1 Εισαγωγή

1.1 Περιγραφή του αντικειμένου της πτυχιακής εργασίας

Τα τελευταία χρόνια ο τομέας των δικτύων πολιορκείται από εισβολείς (Hackers) οι οποίοι με διάφορες τεχνικές χτυπούν την ασφάλεια των δικτύων με σκοπό να βγάλουν χρήματα, να αποκτήσουν φήμη κ.α. Καθημερινά χρήστες και επιχειρήσεις πέφτουν θύματα των επιθέσεων αυτών και πολλές φορές οι ζημιές είναι ανυπολόγιστες, αν σκεφτεί κανείς ότι μπορεί να βλάψουν την εικόνα ενός ανθρώπου προς τη κοινωνία, κάτι το οποίο μπορεί να τον στιγματίσει για όλη τη ζωή του. Τέτοια θέματα είναι που κάνουν επιτακτική την ανάγκη για καλύτερη θωράκιση της ασφάλειας των δικτύων και των υπολογιστών.

Αναπτύσσονται συνεχώς καινούριες επιθέσεις και οι ήδη υπάρχουσες εξελίσσονται συνεχώς κάτι το οποίο κάνει αναγκαίο το συνεχή έλεγχο της ασφάλειας σε δίκτυα και υπολογιστές. Πολλές επιθέσεις έχουν την ικανότητα να αποκτήσουν κωδικούς πρόσβασης, ονόματα χρηστών να δώσουν δικαιώματα λογαριασμών σε υπολογιστές κ.α. Αρκεί να φανταστούμε όλα αυτά να γίνονται σε μια επιχείρηση, τότε θα καταλάβουμε ότι το κόστος για το συνεχή έλεγχο της ασφάλειας είναι πολύ μικρό απέναντι στο κόστος τέτοιων μεγάλων ζημιών.

Για να θωρακιστεί η ασφάλεια σε δίκτυα και υπολογιστές, οι ειδικοί στο τομέα της ασφάλειας των δικτύων εκτελούν δοκιμές οι οποίες ονομάζονται Δοκιμές Διείσδυσης(Penetration Testing) προκειμένου να αξιολογήσουν την ασφάλεια σε δίκτυα και υπολογιστές. Είναι σημαντικό να γίνονται οι δοκιμές αυτές από επιχειρήσεις καθώς μπορούν να κρατήσουν μακριά αρκετούς επιτιθέμενους και με αυτό τον τρόπο να μειώσουν πάρα πολύ τις πιθανότητες κάποιας επίθεσης η οποία θα μπορούσε να προκαλέσει τεράστια ζημιά τόσο στα οικονομικά της επιχείρησης όσο και στη φήμη της στην αγορά. Μια ζημιά στη φήμη μιας εταιρίας μπορεί να καταστρέψει την εμπιστοσύνη της αγοράς στην επιχείρηση με πιθανό αποτέλεσμα την οικονομική κατάρρευση της εταιρείας. Οπότε καταλαβαίνουμε ότι οι Δοκιμές Διείσδυσης είναι αναγκαίες σήμερα και δεν πρέπει να παραλείπονται αλλά ούτε να περνάνε σε δεύτερη μοίρα.

Στα πλαίσια αυτής της πτυχιακής θα ασχοληθώ με τον τομέα της ασφάλειας δικτύων και πιο συγκεκριμένα με τις Δοκιμές και τον Έλεγχο Διείσδυσης για Διάγνωση και Ανίχνευση Ευπαθειών σε Ασύρματα Δίκτυα Δεδομένων. Θα αναλύσω τεχνολογίες ασυρμάτων δικτύων δεδομένων και θα παρουσιάσω τους κινδύνους τους οποίους έχει να αντιμετωπίσει μια εταιρία όπως οι hackers και οι επιθέσεις οι οποίες πραγματοποιούν σε ασύρματα δίκτυα δεδομένων. Στη συνέχεια θα παρουσιάσω τον τρόπο με τον οποίο αντιμετωπίζει του κινδύνους αυτούς ο τομέας της ασφάλειας, τόσο σε θεωρητικό βαθμό όσο και σε πρακτικό μέσα από ένα σενάριο Penetration Testing με πραγματικά δεδομένα.

1.2 Ιστορική Αναδρομή

Σύμφωνα με το installCore (2015) η πρώτη αναφορά στη Δοκιμή Διείσδυσης(Penetration Test) έγινε το 1960. Το 1971 δημιουργείται η πρώτη ομάδα για Pentest και ονομάζεται “Tiger team”. Η πολεμική αεροπορία τότε προσλαμβάνει τον James Anderson και εκτελεί δοκιμές σε χρόνο-μοιραζόμενα συστήματα και το 1974 ηγείται ένα από τα πρώτα “Ethical Hack” προκειμένου να δοκιμάσει την ασφάλεια σε πολλαπλά λειτουργικά συστήματα. Το 1995 οι Dan Farmer και Wietse Venema φτιάχνουν το SATAN(Security Administrator Tool for Analyzing Networks) το οποίο ήταν πρόγραμμα ικανό να βρίσκει αυτόματα μέσα από μια αναζήτηση ευπάθειες σε συστήματα. Το SATAN είναι γνωστό μέχρι και σήμερα και τρέχει σε λειτουργικό Unix. Από τότε και μετά ο τομέας της ασφάλειας αρχίζει και διαδίδεται και γίνεται όλο και πιο αναγκαίος. Έτσι το 2003 ανακοινώνεται ο πρώτος οργανισμός ασφάλειας ο οποίος ονομάζεται OWASP(Open Web Application Security Project). Αποτελεί μια ελεύθερη προς όλους κοινότητα η οποία δημιουργεί άρθρα, μεθοδολογίες, εργαλεία κ.α. γύρω από το τομέα της ασφάλειας. Το 2009 δημιουργείται το πρώτο standard στο Penetration Test με όνομα “The Penetration Testing Execution Standard”, το οποίο αποτελεί οδηγό για τους τεχνικούς ασφάλειας. Το 2014 εκτιμάται ότι δαπανήθηκαν περίπου 71 δισεκατομμύρια δολάρια για θέματα ασφάλειας. Πλέον έχει γίνει αναγκαία η ασφάλεια στο κόσμο της πληροφορίας, χρήστες, επιχειρήσεις και κυβερνήσεις χρειάζονται την ασφάλεια η οποία έχει γίνει

μια από τις πιο αναπτυσσόμενες επιστήμες στο τομέα της πληροφορικής και των δικτύων.

2 Ασύρματα Δίκτυα Δεδομένων

2.1 Εισαγωγή

Στα πλαίσια του κεφαλαίου αυτού θα ασχοληθώ με τις ασύρματες τεχνολογίες δικτύωσης WLAN, WPAN και ZWave. Επέλεξα αυτές καθώς η τεχνολογία WLAN αποτελεί την πιο διαδεδομένη τεχνολογία ασύρματης δικτύωσης μέχρι σήμερα και χρησιμοποιείται σε πάρα πολλούς τομείς. Το Bluetooth το επέλεξα καθώς χρησιμοποιείται αρκετά στα κινητά τηλέφωνα για τη μεταφορά δεδομένων αλλά και για το χειρισμό συσκευών, παρουσιάζοντας έτσι μεγάλο ενδιαφέρον στην ασφάλειά του. Η ZWave τεχνολογία είναι από τις πιο πρόσφατες ασύρματες τεχνολογίες δικτύωσης και χρησιμοποιείται κυρίως στον αυτοματισμό σε σπίτια, οπότε θα ήταν ενδιαφέρον να δούμε πόσο ασφαλές είναι κάτι τέτοιο και πώς αυτό μπορεί να εξελιχθεί. Στις επόμενες υποενότητες θα γίνει παρουσίαση των αρχιτεκτονικών αυτών των τεχνολογιών και της ασφάλειάς τους.

2.2 Wi-Fi

Η τεχνολογία ασύρματης δικτύωσης Wi-Fi αποτελεί αν όχι τη δημοφιλέστερη, μια από τις δημοφιλέστερες τεχνολογίες ασύρματης δικτύωσης καθώς καθημερινά χρήστες απ' όλο τον κόσμο τη χρησιμοποιούν για την σύνδεση τους στο διαδίκτυο. Το Wi-Fi προέρχεται από τα ακρωνύμια των δύο λέξεων, Wireless Fidelity το οποίο σημαίνει ασύρματη πιστότητα. Το Wi-Fi βασίζεται στην προδιαγραφή IEEE 802.11 b/g/n και εκπέμπει στα 2.4 GHz.

Για τη τεχνολογία Wi-Fi όλα ξεκίνησαν το 1985 όταν η Ομοσπονδιακή Επιτροπή Επικοινωνιών (FCC) έδωσε για χρήση στον τομέα των επικοινωνιών τις συχνότητες 900 MHz, 2.4 GHz και 5.8 GHz. Έτσι το 1988 συστάθηκε μια επιτροπή από την IEEE η οποία ονομαζόταν 802.11, με πρόεδρο τον Victor Hayes, η οποία και δούλεψε για τη δημιουργία πρωτοκόλλου ασύρματης δικτύωσης Wi-Fi. Το 1997 ανακοινώθηκε το πρότυπο 802.11 και το 1999 το 802.11 b το οποίο και πήρε την ονομασία Wi-Fi. Το 1999 όμως ανακοινώθηκε και το 802.11 a το οποίο όμως δεν είχε ανάλογη επιτυχία. Το 2003 ανακοινώνεται το 802.11 g το οποίο και θα αντικαταστήσει την έκδοση του 1999 802.11 b, με το 802.11 g να γνωρίζει και αυτό τεράστια επιτυχία και να

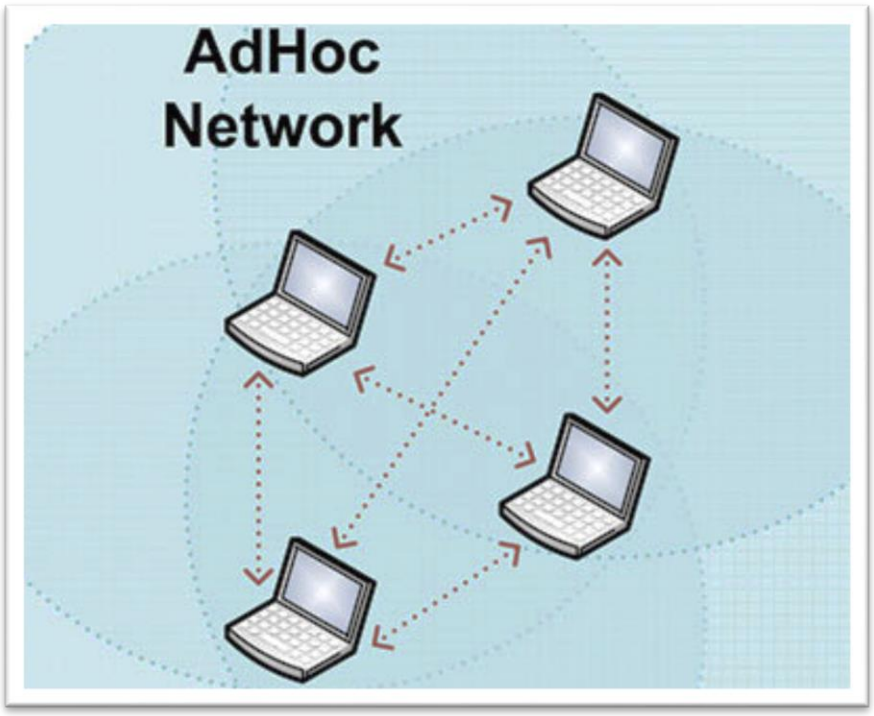
χρησιμοποιείται μέχρι και σήμερα. Από τότε έχουν μελετηθεί και ανακοινωθεί και άλλες εκδόσεις όπως η 802.11 n [1, 2].

2.2.1 Το Πρότυπο 802.11

Για να καταλάβουμε το Wi-Fi θα πρέπει πρώτα να κατανοήσουμε τη λειτουργία του 802.11. Το πρότυπο 802.11 έχει δύο καταστάσεις λειτουργίας, η πρώτη είναι η κατάσταση υποδομής και η δεύτερη η κατάσταση ειδικού σκοπού. Η πρώτη αποτελεί το Wi-Fi με το οποίο θα ασχοληθούμε και είναι η πιο συνηθισμένη στην οποία κάθε χρήστης συνδέεται σε ένα σημείο πρόσβασης (access point) το οποίο αναλαμβάνει την μετάβαση της πληροφορίας από το δίκτυο στο χρήστη μέσω του αέρα με ραδιοκύματα όπως φαίνεται στην εικόνα 2.2 [3].

Η δεύτερη κατάσταση η οποία είναι λιγότερο συνηθισμένη, αφορά δίκτυα Ad-Hoc τα οποία αποτελούνται από ένα σύνολο υπολογιστών συνδεδεμένων μεταξύ τους με σκοπό την απευθείας αποστολή πακέτων μεταξύ τους. Ένα δίκτυο Ad Hoc φαίνεται στην εικόνα 2.3. Το AP σε αυτή την κατάσταση δεν υφίσταται [3].

Εικόνα 2.2: Wi-Fi - Infrastructure Mode [22]



Εικόνα 2.3: Ad Hoc Δίκτυο [23]

Η στοίβα πρωτοκόλλων του 802.11 είναι ίδια για τους πελάτες και για τα σημεία πρόσβασης. Το φυσικό επίπεδο αντιστοιχεί με το φυσικό επίπεδο του OSI, δεν ισχύει το ίδιο όμως και για το επίπεδο συνδέσμου μετάδοσης δεδομένων το οποίο διαιρείται σε δύο υποεπίπεδα, το MAC υποεπίπεδο το οποίο ορίζει ποιος θα μεταδώσει στη συνέχεια και το LLC το οποίο κρύβει τις διαφορές που υπάρχουν ανάμεσα στις παραλλαγές του 802. Οι τεχνικές μετάδοσης διαφέρουν σε κάθε έκδοση του 802.11 όπως φαίνεται στο πίνακα 2.1, με το 802.11 a και 802.11 g να χρησιμοποιούν διαμόρφωση OFDM το 802.11 b να χρησιμοποιεί εξάπλωση φάσματος και η έκδοση 802.11 n του 2009 να έχει αναπτύξει μια νέα μέθοδο MIMO πολλαπλής εξόδου και εισόδου για την επίτευξη μεγαλύτερων ταχυτήτων [3].

2.2.2 Πως Λειτουργεί Το Wi-Fi

Για να καταλάβουμε τον τρόπο λειτουργίας του Wi-Fi πρέπει πρώτα να δούμε από τι αποτελείται. Σε κάθε Wi-Fi δίκτυο υπάρχει τουλάχιστον ένα σημείο πρόσβασης (Access Point - AP) το οποίο αποτελείται από το SSID το οποίο είναι το όνομα του Wi-Fi δικτύου μας (π.χ. vangelis-Wi-Fi), το BSSID το οποίο αποτελεί τη MAC διεύθυνση του δικτύου μας, η οποία αναγνωρίζει μοναδικά τη κάρτα δικτύου μας. Το

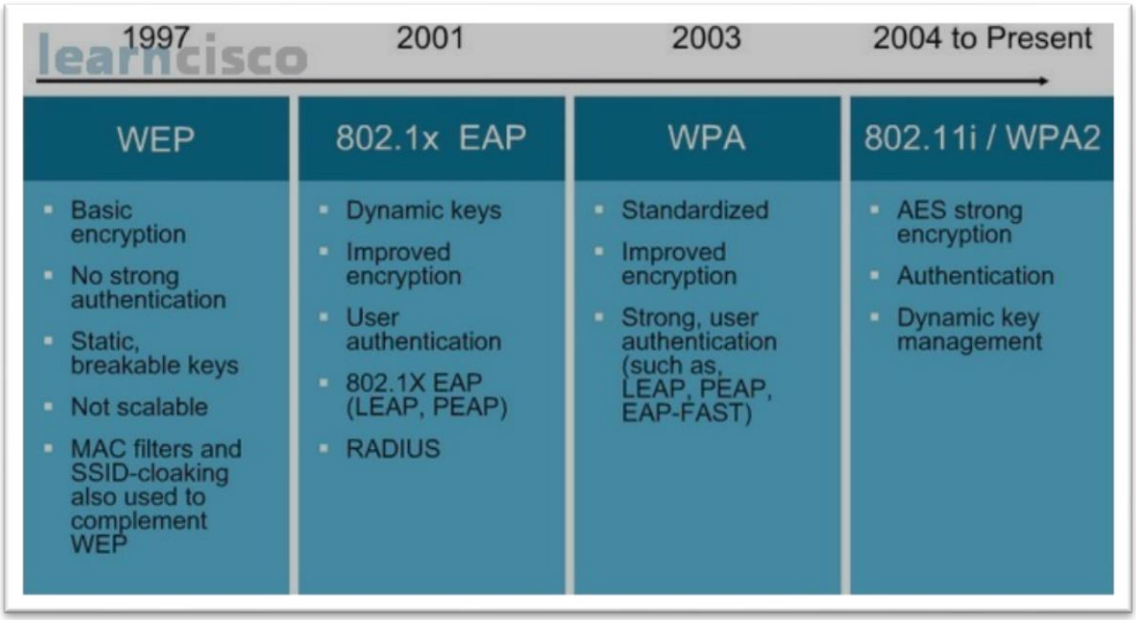
Wi-Fi αποτελείται επίσης από το τύπο ασφάλειας που έχει το δίκτυο μας και από τα beacons τα οποία είναι μικρά πακέτα τα οποία στέλνει το δίκτυο μας προκειμένου να γίνεται ορατό στους χρήστες.

Για να συνδεθεί ένας χρήστης σε ένα δίκτυο Wi-Fi επιλέγει το AP που θέλει πατάει πάνω σε αυτό για σύνδεση, βάζει κωδικό εάν το δίκτυο χρησιμοποιεί κάποια ασφάλεια και αν γίνει δεκτός αποκτά πρόσβαση στο δίκτυο. Αυτή είναι μια απλή εξήγηση για τον τρόπο με τον οποίο αποκτάμε πρόσβαση σε ένα δίκτυο Wi-Fi. Ας δούμε αυτή τη διαδικασία πιο αναλυτικά και επιστημονικά. Για να γίνει η σύνδεση θα πρέπει πρώτα ο χρήστης να στείλει ένα αίτημα ανίχνευσης (probe request) στο AP που θέλει να συνδεθεί προκειμένου αυτό να του γνωστοποιήσει όλες τις πληροφορίες που πρέπει να έχει ο χρήστης όπως το όνομα του AP το τύπο κρυπτογραφίας που έχει κ.α. Μόλις το AP λάβει το Probe Request θα απαντήσει με μια απάντηση ανίχνευσης (Probe Response) με το οποίο θα στείλει όλες τις πληροφορίες που χρειάζεται. Στη συνέχεια για να αποκτήσει πρόσβαση ο χρήστης θα στείλει ένα πλαίσιο πιστοποίησης (Authentication packet) το οποίο θα περιλαμβάνει το κωδικό πρόσβασης και μόλις λάβει αυτό το πακέτο το AP θα ελέγξει το κωδικό. Αν ο κωδικός είναι σωστός τότε θα στείλει πίσω στο χρήστη ένα Authentication packet με το οποίο θα γνωστοποιεί ότι ο κωδικός του έγινε δεκτός. Στη συνέχεια η μεριά του χρήστη στέλνει ένα αίτημα σύνδεσης (Association Request) προκειμένου να γίνει η σύνδεση και το AP απαντάει με μια απάντηση σύνδεσης (Association Response) το οποίο σημαίνει τη σύνδεση μεταξύ χρήστη και AP. Με τη πραγματοποίηση της σύνδεσης όλα τα πακέτα που φεύγουν από το χρήστη περνάνε πρώτα από το AP και μετά στο δίκτυο. Όλα αυτά γίνονται αν ο κωδικός που βάζει ο χρήστης είναι σωστός. Σε περίπτωση που ο κωδικός όμως δεν ήταν σωστός τότε το Authentication Request δε θα γινόταν δεκτό και η διαδικασία θα σταματούσε εκεί.

2.2.3 Ασφάλεια Wi-Fi

Στο Wi-Fi προκειμένου να αντιμετωπίσουμε τις διάφορες απειλές οι οποίες υπάρχουν στο κόσμο της πληροφορίας και των δικτύων χρησιμοποιούμε διάφορους τύπους ασφάλειας. Η ασφάλεια στο Wi-Fi έχει κυρίως να κάνει με το πώς θα αποτρέψει τη πρόσβαση σε μη εξουσιοδοτημένους χρήστες, και για να το πετύχει αυτό βάζει κωδικό στο δίκτυο ώστε να το κλειδώσει και να μην είναι ελεύθερο για όλους.

Η ασφάλεια όμως του Wi-Fi δε σταματάει εκεί καθώς το βασικότερο στοιχείο της είναι ότι κρυπτογραφεί με διάφορες τεχνικές το κωδικό αυτό για να αποτρέψει κάποιο hacker όχι να τον κλέψει αλλά να μπορέσει να τον διαβάσει! Η λιγότερο αξιόπιστη τεχνική είναι η WEP η οποία αποτελεί κρυπτογράφηση προ-κοινόχρηστου κλειδιού και η πιστοποίηση ταυτότητας γίνεται πριν τη συσχέτιση [3]. Η χρήση του WEP ως μέτρο ασφαλείας στο Wi-Fi δεν συνίσταται λόγω διαφόρων κενών ασφαλείας σε αυτό [4]. Λόγω των κενών αυτών σχεδιάστηκε από τη Wi-Fi alliance το WPA το οποίο ήταν πολύ ανώτερο του WEP καθώς με την χρήση του TKIP γίνεται μια δυναμική κατανομή κλειδιών των 128-bit για κάθε πακέτο με αποτέλεσμα να αποτρέπονται επιθέσεις που υπήρχαν στο WEP στο οποίο το κλειδί έμενε σταθερό [4, 5]. Εκτός από το TKIP το WPA περιλαμβάνει επίσης ένα έλεγχο ακεραιότητας μηνύματος ο οποίος αποτρέπει την αλλοίωση ή την αλλαγή του αρχικού μηνύματος [4]. Μετά το WPA ήρθε το WPA2 το οποίο αποτελεί ακόμα πιο ισχυρή ασφάλεια για το Wi-Fi καθώς υποστηρίζει CCMP μια λειτουργία η οποία βασίζεται σε κρυπτογράφηση AES ενώ ταυτόχρονα περιέχει ένα ακόμα πιο ισχυρό έλεγχο δεδομένων απ' ότι το WPA [4]. Αυτά είναι τα στοιχεία που καθιστούν το WPA2 σήμερα τη πιο ισχυρή ασφάλεια στη τεχνολογία Wi-Fi. Στην εικόνα 2.4 φαίνονται όλες οι τεχνικές κρυπτογράφησης με τα βασικά τους χαρακτηριστικά.



Εικόνα 2.4 Τεχνικές κρυπτογράφησης στο Wi-Fi [24]

Εκτός όμως από την εισαγωγή κωδικού και κρυπτογράφησης αυτού υπάρχουν και άλλες τεχνικές οι οποίες συμβάλουν στην ασφάλεια του Wi-Fi. Τέτοιες τεχνικές είναι

το φιλτράρισμα των MAC διευθύνσεων (οι συσκευές που συνδέονται στο AP) το οποίο επιτρέπει μόνο συγκεκριμένες συσκευές να συνδέονται στο δίκτυο και το “κρύψιμο” του SSID. Άλλο ένα μέτρο ασφάλειας είναι η αλλαγή των εργοστασιακών ssids και των κωδικών πρόσβασης με πιο ισχυρούς. Τέλος σημαντικό είναι η μείωση του σήματος του AP προκειμένου να μην γίνεται ορατό σε χρήστες που δε θέλουμε.

2.3 Bluetooth

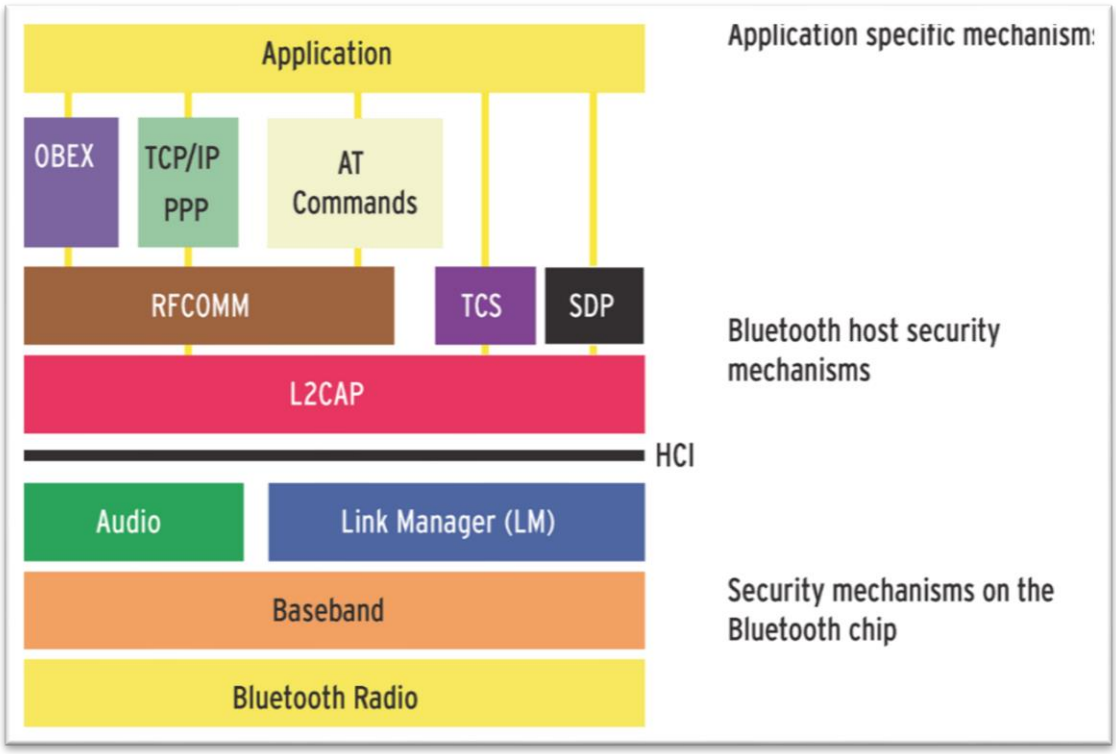
Το Bluetooth αποτελεί και αυτό μια τεχνολογία ασύρματης δικτύωσης η οποία είναι ευρέως γνωστή καθώς εκατομμύρια χρήστες τη χρησιμοποιούν για τη μεταφορά δεδομένων και για έλεγχο συσκευών. Επίσης στις περισσότερες φορητές συσκευές υπάρχει εγκατεστημένη. Η ιστορία της τεχνολογίας Bluetooth ξεκινάει το 1998 όταν η σουηδική εταιρία τηλεπικοινωνιών Ericsson άρχισε να ερευνά με ποιο τρόπο θα μπορούσε να συνδέσει τα κινητά της τηλέφωνα ασύρματα με άλλες συσκευές όπως ο υπολογιστής. Τελικά τον Ιούλιο του 1999 δημοσιεύτηκε η πρώτη έκδοση Bluetooth, με το Bluetooth να γνωρίζει τεράστια επιτυχία και να μην σταματά στη πρώτη έκδοση. Το πρότυπο αυτό υιοθέτησε η IEEE ως 802.15 για τα ασύρματα προσωπικά δίκτυα. Η τεχνολογία αυτή όμως δε σταμάτησε εκεί καθώς το 2004 ανακοινώθηκε η έκδοση Bluetooth 2.0 την οποία ακολούθησε το 2009 η έκδοση 3.0 με χαρακτηριστικό γνώρισμα της η ικανότητα να συνδυαστεί με την 802.11 για τη μεταφορά δεδομένων. Το 2009 δημοσιεύτηκε και η έκδοση 4.0 η οποία σχεδιάστηκε για λειτουργία χαμηλής κατανάλωσης [3,7].

2.3.1 Η τεχνολογία Bluetooth

Η τεχνολογία Bluetooth όπως προαναφέρθηκε είναι για την ασύρματη σύνδεση μεταξύ συσκευών. Ας δούμε τη δομή και την αρχιτεκτονική αυτής της τεχνολογίας για να την κατανοήσουμε καλύτερα. Στην εικόνα 2.5 φαίνεται η στοίβα πρωτοκόλλων του 802.15 και μπορούμε να παρατηρήσουμε ότι δε μοιάζει με το OSI, το tcp/ip η κάποιο άλλο πρωτόκολλο της οικογένειας 802. Στη τεχνολογία Bluetooth έχουμε δύο είδη δικτύου το piconet και το scattemet. Στο piconet υπάρχει ένας κόμβος master και μέχρι εφτά κόμβοι slave, ενώ το δίκτυο scattemet έχει να κάνει με ένα σύνολο από συνδεδεμένα Piconets [3].

Στη τεχνολογία Bluetooth υπάρχει και ένα σύνολο πρωτοκόλλων ή αλλιώς μια στοίβα πρωτοκόλλων τα οποία συνεργάζονται για να πετύχουν το σκοπό του Bluetooth. Η στοίβα αυτή των πρωτοκόλλων φαίνεται στην εικόνα 2.5. Βλέπουμε ότι

ξεκινάει από κάτω με το Bluetooth radio το οποίο αποτελεί τη διεπαφή φυσικής διασύνδεσης, επόμενο είναι το Baseband μετά είναι το Audio και το Link Manager απ' τα οποία το πρώτο είναι για τη μεταφορά εντολών ελέγχου ήχου πάνω από το κανάλι L2CAP και το δεύτερο για τον έλεγχο του επιπέδου Radio των δύο συσκευών. Το L2CAP υπάρχει για τη μεταφορά των πακέτων από το HCI στο ACL και το αντίθετο, έχοντας ως λειτουργίες τη τμηματοποίηση, τη πολυπλεξία και την επανασύνδεση. Πάνω από το L2CAP βρίσκονται τα RFCOMM, TCS και SDP στα οποία το πρώτο είναι για μεταφορά δεδομένων, το δεύτερο είναι για τη διαχείριση τηλεφωνικών κλήσεων ανάμεσα σε συσκευές Bluetooth και το τρίτο είναι για παροχή πληροφοριών που έχουν να κάνουν με τις παραμέτρους που πρέπει να χρησιμοποιηθούν για τη σύνδεση, για τις λειτουργίες που προσφέρει κάθε συσκευή κ.α. Τέλος το Application ορίζει τη κατάσταση του Bluetooth που μπορεί να είναι για τη μεταφορά ενός αντικειμένου ανάμεσα σε δύο συσκευές (OBEX) ή για να θέσεις το Bluetooth σε λειτουργία χαμηλής κατανάλωσης (ATT) κ.α [8].



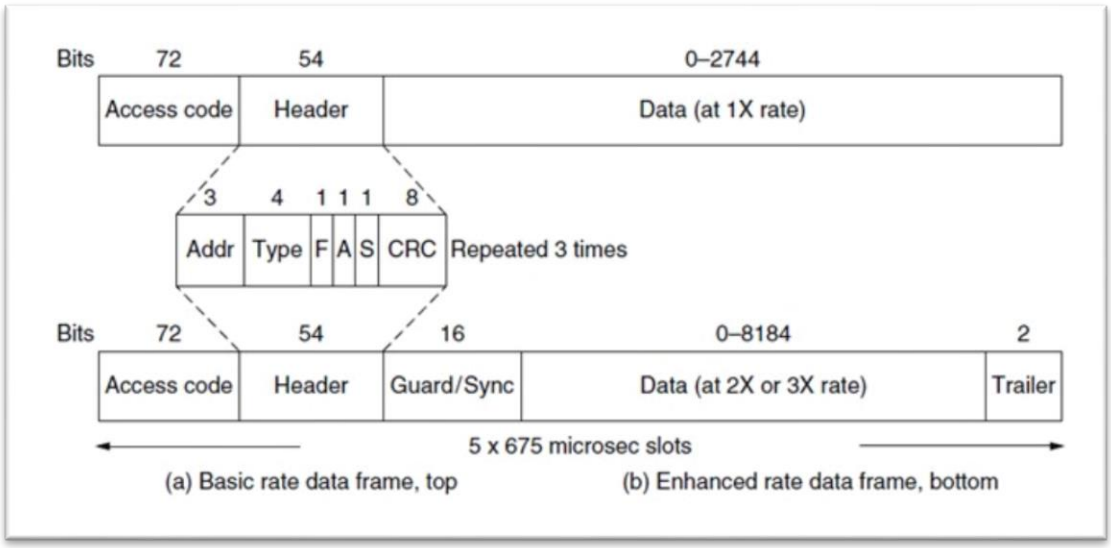
Εικόνα 2.5: Στοίβα πρωτοκόλλων Bluetooth [25]

Η τεχνολογία Bluetooth όμως δε θα μπορούσε να λειτουργήσει αν δεν υπήρχαν τα πακέτα στα οποία μπαίνει όλη η πληροφορία για να μεταδοθεί από τη μια συσκευή στην άλλη. Η μορφή του πακέτου που χρησιμοποιεί το Bluetooth φαίνεται στην

εικόνα 2.6. Βλέπουμε ότι ξεκινάει με 72 bit τα οποία είναι ο κωδικός πρόσβασης και τα επόμενα 52 bit αφορούν την κεφαλίδα στην οποία βρίσκονται τα βασικά πεδία του υποεπιπέδου MAC. Τέλος έχουμε το πεδίο δεδομένων το οποίο μπορεί να είναι μέχρι 2744 bit. Αυτό είναι το βασικό πακέτο Bluetooth αλλά υπάρχει και μια παραλλαγή αυτού η οποία έχει σχεδιαστεί για μεγαλύτερες ταχύτητες. Οι αλλαγές που υπάρχουν σε αυτό είναι ότι τα δεδομένα πλέον έχουν μέγεθος μέχρι 8184 bit και έχει επίσης άλλα δύο πεδία, ένα προστασίας και συγχρονισμού 16 bit το οποίο βρίσκεται πριν το πεδίο δεδομένων και χρησιμοποιείται για τη εναλλαγή σε μεγαλύτερο ρυθμό στο πεδίο δεδομένων και το δεύτερο ονομάζεται επίμετρο είναι 2 bit και είναι για το τερματισμό του ενισχυμένου ρυθμού. Τα πεδία το οποία βρίσκονται στη κεφαλίδα είναι τα εξής :

- **Διεύθυνση(3 bit)** : Προσδιορίζει τον παραλήπτη του πακέτου
- **Τύπος(4 bit)** : Προσδιορίζει το τύπο του πλαισίου(ACL, SCO, κενό, περιόδευση)
- **Ροή(1 bit)** : Ενεργοποιείται σε περίπτωση που γεμίσει η προσωρινή μνήμη
- **Επιβεβαίωση(1 bit)** : Χρησιμοποιείται για την τοποθέτηση εμβόλιμης επιβεβαίωσης
- **Ακολουθία(1 bit)** : Χρησιμοποιείται για την αρίθμηση των πλαισίων
- **Άθροισμα ελέγχου(8 bit)** : Ελέγχει το άθροισμα της κεφαλίδας

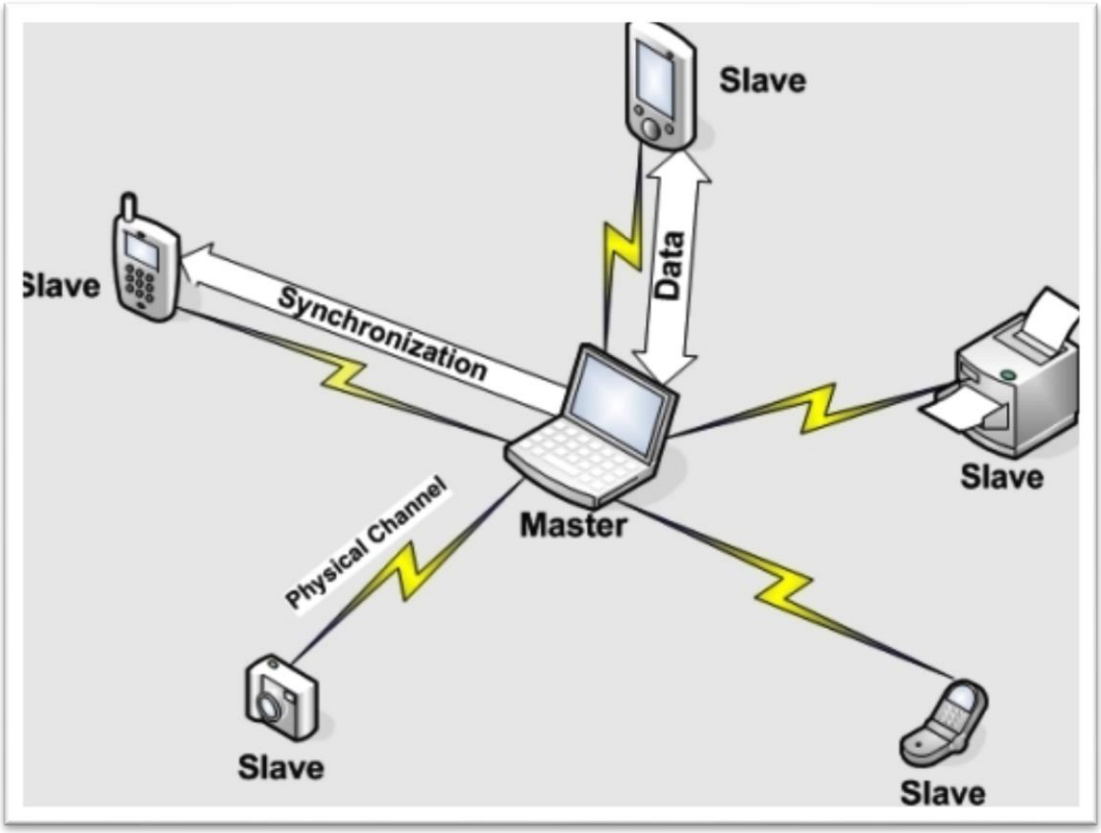
Παρατηρούμε ότι το άθροισμα τους είναι 18 bits και είπαμε ότι η κεφαλίδα είναι 54 bits, έτσι η διαδικασία της κεφαλίδας επαναλαμβάνεται τρείς φορές ώστε να σχηματιστεί. Ο παραλήπτης μετά κοιτά αν και τα τρία αντίγραφα είναι ίδια και αν ναι δέχεται το πακέτο [3].



Εικόνα 2.6: Δομή Πακέτου Bluetooth [26]

2.3.2 Πώς Λειτουργεί το Bluetooth

Για να υπάρξει λειτουργία στο Bluetooth θα πρέπει τουλάχιστον δύο συσκευές να συνδεθούν μεταξύ τους και αυτό γίνεται όταν μία από τις δύο είναι εμφανή προς τις άλλες συσκευές. Έτσι μία συσκευή κάνει αναζήτηση για συσκευές Bluetooth και βρίσκει αυτή που θέλει. Προκειμένου να συνδεθεί μαζί της, στέλνει ένα αίτημα σύνδεσης και η συσκευή slave απαντά σε αυτό. Αμέσως αν υπάρχει ασφάλεια η master συσκευή στέλνει ένα αίτημα πιστοποίησης με το κωδικό και αν είναι σωστός η slave συσκευή απαντά αντίστοιχα με κάποιο μήνυμα υποδοχής. Τέλος γίνεται η σύνδεση μεταξύ τους και δημιουργείται ένα δίκτυο piconet. Με τη δημιουργία αυτού αρχίζουν να ανταλλάσσουν δεδομένα με τη χρήση των πακέτων που είδαμε παραπάνω μέσω του αέρα. Στην εικόνα 2.7 φαίνεται ένα piconet με μια συσκευή master και εφτά συσκευές slave συνδεδεμένες σε αυτή.



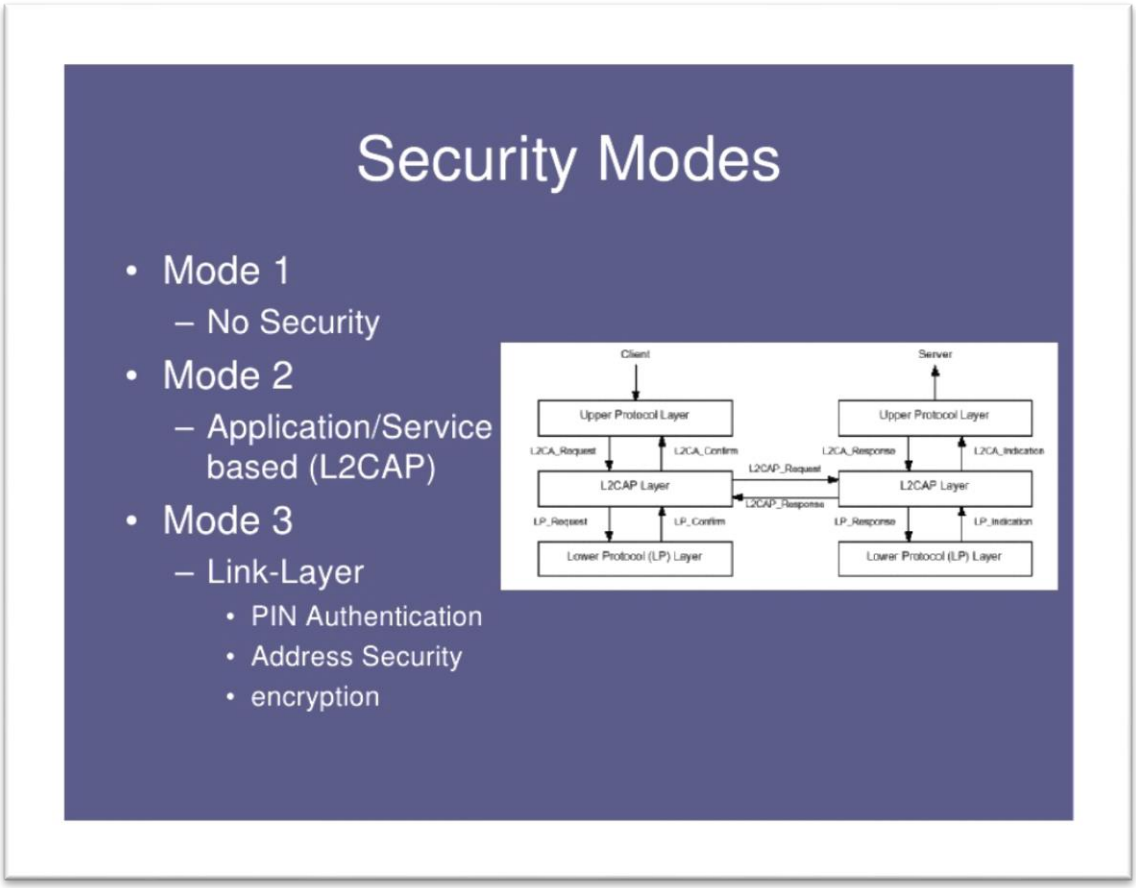
Εικόνα 2.7: Piconet [27]

2.3.4 Ασφάλεια Bluetooth

Γενικά η τεχνολογία Bluetooth προσφέρει τρία διαφορετικά επίπεδα ασφάλειας, όπως φαίνεται στην εικόνα 2.8 τα οποία διαφέρουν ανάλογα με τις υπηρεσίες ασφάλειας που προσφέρει το καθένα.

Στο πρώτο στάδιο ασφάλειας η συσκευή Bluetooth βρίσκεται σε promiscuous mode και οποιαδήποτε άλλη συσκευή Bluetooth μπορεί να συνδεθεί σε αυτή, χωρίς να υπάρχει καμία ασφάλεια. Από άποψη ασφάλειας είναι το χειρότερο καθώς μπορεί να συνδεθεί και να έχει πρόσβαση στη συσκευή ο καθένας χωρίς κανένα έλεγχ. Στο δεύτερο επίπεδο ασφάλειας Bluetooth η ασφάλεια προσδιορίζεται αφού γίνει σύνδεση στο L2CA. Την ασφάλεια την προσδιορίζει το επίπεδο εφαρμογής, δηλαδή η κάθε εφαρμογή που τρέχει στη Bluetooth συσκευή μπορεί να ορίσει ευέλικτα την ασφάλεια που θέλει. Θεωρείται το καλύτερο επίπεδο ασφάλειας καθώς είναι ευέλικτο και δίνει τη δυνατότητα στην εφαρμογή να αποφασίσει αν χρειάζεται ασφάλεια στην

επικοινωνία ή όχι. Το τρίτο επίπεδο ασφάλειας είναι και το πιο αυστηρό από τα άλλα δύο καθώς απαιτεί ασφάλεια όπως ταυτοποίηση και κρυπτογράφηση από το χαμηλότερο επίπεδο Baseband δηλαδή πριν καν δημιουργηθεί η σύνδεση μεταξύ των δύο συσκευών. Η κρυπτογράφηση η οποία δημιουργείται πριν τη σύνδεση διατηρείται και κατά την επικοινωνία των συσκευών μετά τη σύνδεσή τους [9, 10].



Εικόνα 2.8: Επίπεδα Ασφαλείας Bluetooth [28]

Όλες οι προδιαγραφές ασφάλειας που αναφέραμε πιο πάνω ισχύουν για τις εκδόσεις Bluetooth μέχρι 2.1. Οι προδιαγραφές ασφάλειας για την έκδοση Bluetooth χαμηλής ενέργειας (4.0 Bluetooth Low Energy) διαφέρουν λίγο με αυτές των προηγούμενων εκδόσεων. Στην έκδοση χαμηλής ενέργειας έχουμε 2 τρόπους ασφαλείας. Στο πρώτο τρόπο υπάρχουν διάφορα επίπεδα που έχουν να κάνουν με τη κρυπτογράφηση. Στο πρώτο επίπεδο δεν υπάρχει καθόλου ασφάλεια, στο δεύτερο επίπεδο δεν υπάρχει πιστοποίηση σύνδεσης αλλά υπάρχει κρυπτογράφηση. Στο τρίτο και τελευταίο επίπεδο απαιτείται και πιστοποίηση σύνδεσης και κρυπτογράφηση. Ο δεύτερος τρόπος ασφάλειας που προσφέρει το Bluetooth 4.0 έχει να κάνει με τη υπογραφή δεδομένων (data signing) και αποτελείται

από δύο επίπεδα. Στο πρώτο επίπεδο δεν υπάρχει πιστοποίηση σύνδεσης αλλά υπάρχει υπογραφή δεδομένων. Στο δεύτερο επίπεδο υπάρχει πιστοποίηση σύνδεσης και υπογραφή δεδομένων [11].

2.4 Home Automation ZWave

Το Zwave αποτελεί μια τεχνολογία ασύρματης δικτύωσης η οποία χρησιμοποιείται για αυτοματισμό στο σπίτι. Το Zwave σχεδιάστηκε από μια δανέζικη εταιρία τη Zen-Sys. Από το 2005 υπολογίζεται ότι έχουν πουληθεί πάνω από 35 εκατομμύρια συσκευές. Μεγαλύτερη επιτυχία φαίνεται να έχει στην Αμερική, όμως τα τελευταία χρόνια αναπτύσσεται και στην Ευρώπη. Το Zwave όμως δεν είναι η μοναδική τεχνολογία για αυτοματισμό στο σπίτι καθώς υπάρχει και η ZigBee η οποία και αποτελεί το βασικό ανταγωνιστή της Zwave.

2.4.1 Η Τεχνολογία ZWave

Το ZWave αποτελεί ένα πρωτόκολλο ασύρματης επικοινωνίας μεταξύ συσκευών για λόγους αυτοματισμού σε σπίτια, γραφεία κ.α. Προσφέρει αξιόπιστη μεταφορά δεδομένων, απλότητα και ευελιξία. Δουλεύει με ραδιοσυχνότητες χρησιμοποιώντας διαμόρφωση μετατόπισης συχνότητας (frequency-shift keying). Η ρυθμοαπόδοση του είναι στα 40 Kb/Sec η οποία είναι κατάλληλη για εφαρμογές αισθητήρων. Η ζώνη συχνοτήτων ποικίλει ανάλογα με τη κάθε ήπειρο όπως φαίνεται στο πίνακα 2.1 [12].

Πίνακας 2.1: Συχνότητες ZWave ανά χώρα

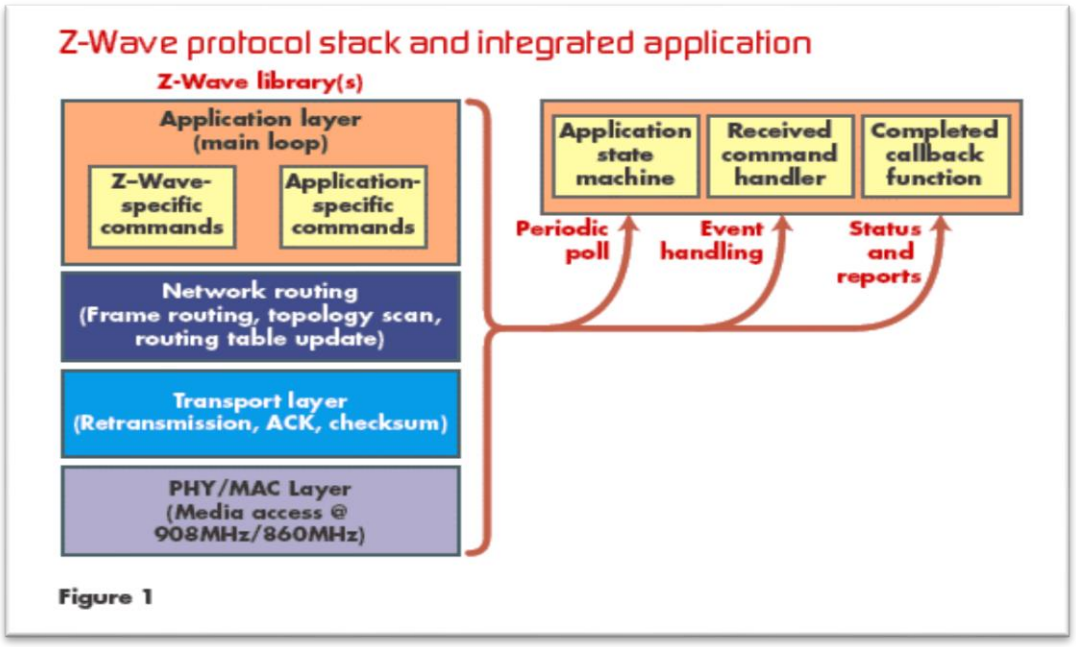
Χώρα	Συχνότητα
Αμερική/ Καναδάς	908.4 MHz
Αυστραλία	921.4 MHz
Βραζιλία	921.4 MHz
Ηνωμένα Αραβικά Εμιράτα	868.4 MHZ
Ιαπωνία	922-926 MHz
Ινδία	865.2 MHz
Κίνα	868.4 MHz
Μαλαισία	868.1 MHz

Μεξικό	908.4 MHz
Νέα Ζηλανδία	921.4 MHz
Νότια Αφρική	868.4MHz
Ρωσία	869.0 MHz
Σιγκαπούρη	868.4 MHz
Χονγκ Κονγκ	919.8 MHz
Χώρες Ευρωπαϊκής Ένωσης (CEPT)	868.4 MHz

Όπως βλέπουμε στο πίνακα η Ελλάδα ανήκει στην Ευρωπαϊκή Ένωση και γι' αυτό το ZWave δουλεύει στα 868.4 MHZ. Επίσης πολύ σημαντικό για τη τεχνολογία ZWave είναι ότι δουλεύει σε χαμηλή κατανάλωση και αυτό το χαρακτηριστικό είναι που την κάνει ιδανική για εφαρμογές αυτοματισμού.

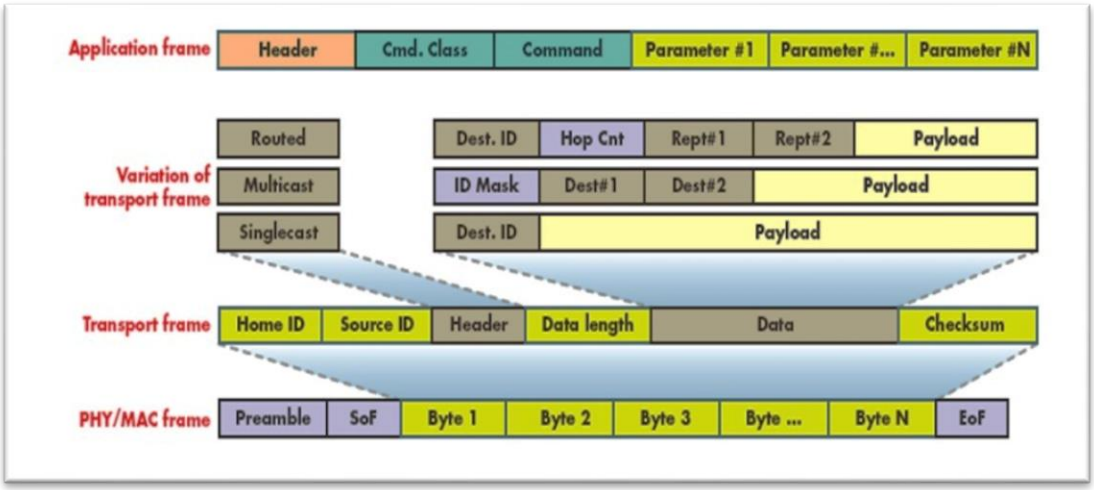
2.4.2 Στοίβα Πρωτοκόλλου ZWave

Η τεχνολογία ZWave έχει το δικό της πρωτόκολλο επικοινωνίας το οποίο φτιάχτηκε από τη Zen-Sys και μάλιστα θα μπορούσαμε να πούμε ότι αποτελεί ένα πάρα πολύ καλό πρωτόκολλο. Το πρωτόκολλο αυτό μπορούμε να πούμε ότι μοιάζει με αυτό του tcp/ip αλλά δεν είναι ίδια! Όπως φαίνεται στην εικόνα 2.9 η στοίβα πρωτοκόλλου ZWave αποτελείται από το επίπεδο PHY/MAC το οποίο διαχειρίζεται το μέσο ραδιοσυχνότητας, το επίπεδο Μεταφοράς το οποίο διαχειρίζεται την ακεραιότητα των πακέτων που μεταφέρονται και το επίπεδο δικτύου το οποίο διαχειρίζεται όλη τη δρομολόγηση αλλά και τη διεπαφή εφαρμογών [12].



Εικόνα 2.9: Στοίβα πρωτοκόλλου ZWave [29]

Η δομή των πακέτων φαίνεται στην εικόνα 2.10 και ξεκινάει με το πλαίσιο PHY/MAC το οποίο ξεκινάει με το Synchronization Preamble το οποίο υπάρχει για λόγους συγχρονισμού, το SoF(Start of Frame) το οποίο είναι δείκτης αρχής πλαισίου ακολουθούν τα δεδομένα και στο τέλος είναι το EoF(End of Frame) το οποίο είναι δείκτης τέλους πλαισίου. Το μέγιστο μέγεθος των δεδομένων δηλαδή του



Εικόνα 2.10: Δομή Πακέτου ZWave [30]

payload μπορεί να είναι 64 bytes [12].

Στο επίπεδο Μεταφοράς το οποίο διαχειρίζεται τη μεταφορά των δεδομένων μεταξύ δύο συσκευών ZWave περιλαμβάνοντας αναμετάδοση, checksum check το οποίο συμβάλει στην ακεραιότητα των δεδομένων και acknowledgements τα οποία όλα μαζί συμβάλουν στην ποιότητα της επικοινωνίας. Το επίπεδο Μεταφοράς περιλαμβάνει τέσσερεις διαφορετικούς τύπους πλαισίου για την μεταφορά εντολών στο δίκτυο. Οι τέσσερεις αυτοί τύποι πλαισίου χρησιμοποιούν την ίδια διάταξη πλαισίου. Οι τύποι είναι οι εξής:

- **Singlecast Frame Type** στο οποίο γίνεται μετάδοση προς μια συγκεκριμένη συσκευή και γίνεται χρήση acknowledgement ώστε ο μεταδότης να ξέρει ότι το πακέτο έφτασε. Σε περίπτωση φθοράς του πακέτου ή μη αποστολής, τότε το πακέτο αναμεταδίδεται από το μεταδότη.
- **Transfer Acknowledge Frame Type** το οποίο είναι ίδιο με το Singlecast Frame Type με τη διαφορά ότι το πεδίο μεγέθους δεδομένων είναι μηδέν.
- **Multicast Frame Type** σε αυτό το τύπο γίνεται μετάδοση προς πολλές συσκευές και όχι αποκλειστικά σε μια. Μπορεί να στείλει μέχρι και σε 232 συσκευές καθώς τόσες είναι οι μέγιστες συσκευές που μπορεί να έχει ένα δίκτυο. Σε αυτό το τύπο δεν έχουμε acknowledgement κατά τη μετάδοση των δεδομένων.
- **Broadcast Frame Type** στο οποία τα πακέτα τα οποίο μεταδίδονται λαμβάνονται από όλες τις συσκευές του δικτύου. Και σε αυτό το τύπο δεν υπάρχει acknowledgement κατά τη μετάδοση των πακέτων.

Γενικά στους τύπους στους οποίους δεν έχουμε acknowledgement η ποιότητα στην επικοινωνία μειώνεται καθώς η μεταφορά των πακέτων παύει να είναι αξιόπιστη [13].

Το επίπεδο Network Routing αναλαμβάνει τη δρομολόγηση ανάμεσα στις συσκευές ZWave αλλά και ελέγχει αν η δρομολόγηση έγινε σε όλες τις συσκευές. Το επίπεδο δρομολόγησης έχει δύο διαφορετικά πλαίσια που χρησιμοποιούνται όταν η επανάληψη των πλαισίων είναι απαραίτητη.

- **Routed Singlecast Frame Type** είναι το ένα από τα δύο πλαίσια το οποίο έχει σαν προορισμό μια μόνο συσκευή και μεταδίδει επαναλαμβανόμενη πληροφορία. Το πλαίσιο επαναλαμβάνεται από τον ένα παραλήπτη στον άλλο μέχρι να φτάσει στο προορισμό του.

- **Routed Acknowledge Frame Type** είναι το δεύτερο πλαίσιο το οποίο δεν περιέχει payload πληροφορία και υπάρχει για να ενημερώνει τον controller ότι το πακέτο έφτασε στο προορισμό του [13].

Τέλος το επίπεδο Εφαρμογής είναι υπεύθυνο για την αποκωδικοποίηση και εκτέλεση των εντολών ZWave. Το πλαίσιο του όπως φαίνεται στην εικόνα έχει το Application command class στο οποίο προσδιορίζεται η κλάση εντολών στην οποία ανήκει μια εντολή και προσδιορίζεται με έναν δεκαεξαδικό αριθμό από 00 έως FF. Στην συνέχεια είναι το Application command στο οποίο προσδιορίζεται η εντολή ή ενέργεια προς εκτέλεση και τα Command parameters τα οποία προσδιορίζουν τις παραμέτρους οι οποίες θα εκτελεστούν μαζί με την εντολή [13].

2.4.3 Ασφάλεια ZWave

Στη τεχνολογία ZWave δε συναντάμε τόσο μεγάλη ασφάλεια όπως στο Wi-Fi και Bluetooth και αυτό γιατί δεν είναι τόσο εξελιγμένη. Η ασφάλεια του περιορίζεται στην κρυπτογράφηση των πακέτων η οποία υπάρχει μόνο στη σειρά 500 των συσκευών ZWave και στο Application level sample code. Η κρυπτογράφηση που χρησιμοποιείται είναι AES-128 bit και το Application level sample code αποτελεί ένα μηχανισμό για την εύρεση και διόρθωση ευπαθειών στο κώδικα εφαρμογών ZWave. Όπως βλέπουμε η τεχνολογία Zwave αποτελεί μια τεχνολογία πολύ πιο ευπαθή σε επιθέσεις απ’ ότι οι προηγούμενες δύο που είδαμε.

3 Εισβολείς και Επιθέσεις

3.1 Εισαγωγή

Όσο τα χρόνια περνάνε τόσο πιο επιτακτική γίνεται η ανάγκη για ασφάλεια στο τομέα της πληροφορικής και δικτύων, καθώς κάθε μέρα που περνάει οι απειλές που υπάρχουν είναι όλο και περισσότερες. Κάθε μέρα πολλές επιχειρήσεις αλλά και απλοί χρήστες πέφτουν θύματα επιθέσεων από Hackers οι οποίοι έχουν ως σκοπό είτε το χρήμα είτε να κάνουν κακό στην εικόνα μιας εταιρίας η και να βλάψουν σε προσωπικό επίπεδο κάποιόν με τον οποίο έχουν προσωπικές διαμάχες. Για αυτό το λόγο κάθε μέρα γίνεται προσπάθεια από τους ειδικούς του αντικειμένου για την ανάπτυξη καλύτερης ασφάλειας τόσο στο διαδίκτυο όσο και στις συσκευές στις οποίες χρησιμοποιούμε.

3.2 Hackers

Ο τομέας της ασφάλειας δικτύων είναι σε συνεχή αγώνα προκειμένου να κρατήσει ασφαλή χρήστες και επιχειρήσεις από τους hackers. Τους hackers μπορούμε να τους χωρίσουμε σε 7 κατηγορίες:

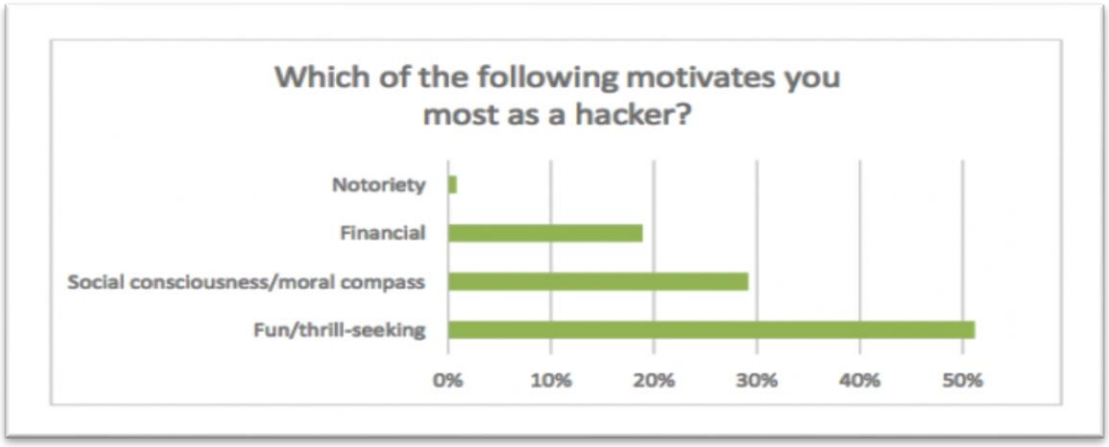
- **White Hat Hackers:** Άνθρωποι οι οποίοι δουλεύουν για να εξασφαλίσουν τη μεγαλύτερη δυνατή ασφάλεια σε δίκτυα και υπολογιστές. Είναι επαγγελματίες οι οποίοι δουλεύουν στο τομέα της ασφάλειας και εκτελούν Penetration Test σε επιχειρήσεις οι οποίες θέλουν να δοκιμάσουν την ασφάλεια τους και να τη θωρακίσουν ακόμα περισσότερο. Αποκαλούνται και Ηθικοί Εισβολείς (Ethical Hackers) [14].
- **Black Hat Hackers:** Οι γνωστοί εισβολείς οι οποίοι κάνουν κακό στους υπολογιστές μας, στις επιχειρήσεις, στις κυβερνήσεις κ.α. Σε αντίθεση με τους White Hat Hackers κάνουν κακό και δεν έχουν σκοπό να βοηθήσουν καθώς είναι εγκληματίες που πίσω από το hacking υπάρχει προσωπικό κέρδος. Είναι έξυπνοι και συνηθίζουν να δουλεύουν σε ομάδες χτυπώντας μεγάλους στόχους (κυβερνήσεις, μεγάλες εταιρίες κ.α.). Είναι οι hackers που καλείται να αντιμετωπίσει ο τομέας της ασφάλειας. Όταν αυτοί οι εισβολείς συλληφθούν, οι κυβερνήσεις συνηθίζουν να τους παίρνουν με το μέρος τους μετατρέποντας τους σε Red Hat Hackers [21, 14].

- **Script Kiddie:** Μια κατηγορία ανθρώπων τους οποίους δε μπορείς να χαρακτηρίσεις ως εισβολείς. Δεν τους ενδιαφέρει το hacking απλά αντιγράφουν κώδικα τον οποίο βρίσκουν ελεύθερο στο διαδίκτυο και κάνουν συνηθισμένες επιθέσεις όπως για παράδειγμα άρνηση υπηρεσιών (DoS attack) [14] .
- **Gray Hat Hackers:** Εισβολείς οι οποίοι δε κάνουν ούτε καλό αλλά ούτε και κακό. Πολλές φορές μπορεί να προκαλέσουν μικρές ζημιές χωρίς όμως να έχουν εγκληματικές διαθέσεις. Μπορούμε να πούμε ότι βλέπουν το hacking σαν δραστηριότητα. Δε βοηθούν στην επιστήμη της ασφάλειας και αποτελούν το μεγαλύτερο ποσοστό των hackers [14].
- **Green Hat Hackers:** Ερασιτέχνες εισβολείς οι οποίοι μόλις έχουν αρχίσει την εξάσκηση τους πάνω στο hacking. Συχνά του αποκαλούν «Newbs» και έχουν τη τάση να θέλουν να μάθουν και να ακούσουν πιο έμπειρους εισβολείς. Γενικά σε αυτή τη κατηγορία υπάρχει ενδιαφέρον για το hacking σε αντίθεση με τους Blue Hat Hackers και τους Script Kiddies [20].
- **Red Hat Hackers:** Εισβολείς οι οποίοι θα μπορούσαμε να πούμε ότι ανήκουν στο ίδιο στρατόπεδο με τους White Hat Hackers δίνουν όμως διαφορετική μάχη [14]. Οι White Hat εκτελούν δοκιμές διείσδυσης και στο τέλος γράφουν μια αναφορά ενώ οι Red Hat δεν μένουν στην ανίχνευση και στην αναφορά κάποιου εισβολέα, αντιθέτως τον βρίσουν και του επιτίθονται προκειμένου να τον σταματήσουν [14]. Πολλές φορές σε αυτή τη κατηγορία βλέπουμε black hat hackers οι οποίοι συνελήφθηκαν από τις αρχές και έγιναν red hat hackers για λογαριασμό των κυβερνήσεων [20].
- **Blue Hat Hacker:** Εισβολείς οι οποίοι κάνουν hacking για λόγους εκδίκησης είτε προς μια εταιρία είτε προς κάποιο άτομο. Γενικά δεν τους ενδιαφέρει το hacking παρά μόνο ο σκοπός τους και γι’ αυτό οι κοινότητα των hackers συνηθίζει να τους λέει «noobs» [20].

Από της παραπάνω κατηγορίες των Hackers είδαμε ότι δεν είναι όλοι εγκληματίες όπως πιστεύει το μεγαλύτερο ποσοστό του κόσμου. Αυτοί όμως οι οποίοι είναι εγκληματίες, έχουν κάποια βασικά κίνητρα που τους οδηγούν στο έγκλημα:

1. Οικονομικοί (κέρδος)

2. Φήμη
3. Κοινωνικοί
4. Ευχαρίστηση



Εικόνα 3.1: Τα κίνητρα των hackers σε ποσοστά [31]

Στην εικόνα 3.1 βλέπουμε σε ποσοστά τα κίνητρα των hackers. Το μεγαλύτερο ποσοστό ανήκει στην Ευχαρίστηση το οποίο επιβεβαιώνει ότι το μεγαλύτερο ποσοστό των hackers ανήκει στην κατηγορία Gray Hat Hackers [15].

3.3 Επιθέσεις

Οι hackers λοιπόν με διάφορους τρόπους προσπαθούν όπως είπαμε να βλάψουν χρήστες και επιχειρήσεις. Θα δούμε μερικές από τις πιο συχνές επιθέσεις σε δίκτυα δεδομένων Wi-Fi, Bluetooth και ZWave. Ξεκινώντας από τη τεχνολογία Wi-Fi οι πιο συχνές επιθέσεις είναι οι εξής :

- **Wep Key cracking:** Ο επιτιθέμενος μέσω διάφορων πακέτων που πιάνει από το δίκτυό μας προσπαθεί να σπάσει το κωδικό πρόσβασης με διάφορα εργαλεία. Όπως είπαμε το Wep είναι ξεπερασμένη ασφάλεια και σπάει πολύ εύκολα.
- **Evil Twin attack:** Ο επιτιθέμενος μετατρέπει ή αλλιώς κλωνοποιεί ένα AP με σκοπό να τραβήξει πάνω του τους χρήστες που είχαν σύνδεση σε άλλο δίκτυο, χωρίς όμως αυτοί να το καταλάβουν.
- **DoS attack:** DoS ή Denial of Service σημαίνει άρνηση υπηρεσιών δηλαδή ο επιτιθέμενος με διάφορες τεχνικές βγάζει “εκτός υπηρεσιών” ένα δίκτυο.

- **MITM attack:** MITM ή Man in the Middle είναι η επίθεση στην οποία ο επιτιθέμενος με διάφορες τεχνικές καταφέρνει να μπει ανάμεσα σε μια επικοινωνία καταφέρνοντας έτσι να κλέψει και να τροποποιήσει τα πακέτα που μεταφέρονται.
- **PSK Cracking:** Στη συγκεκριμένη επίθεση γίνεται σπάσιμο του κωδικού πρόσβασης WPA/WPA2 με dictionary attack.

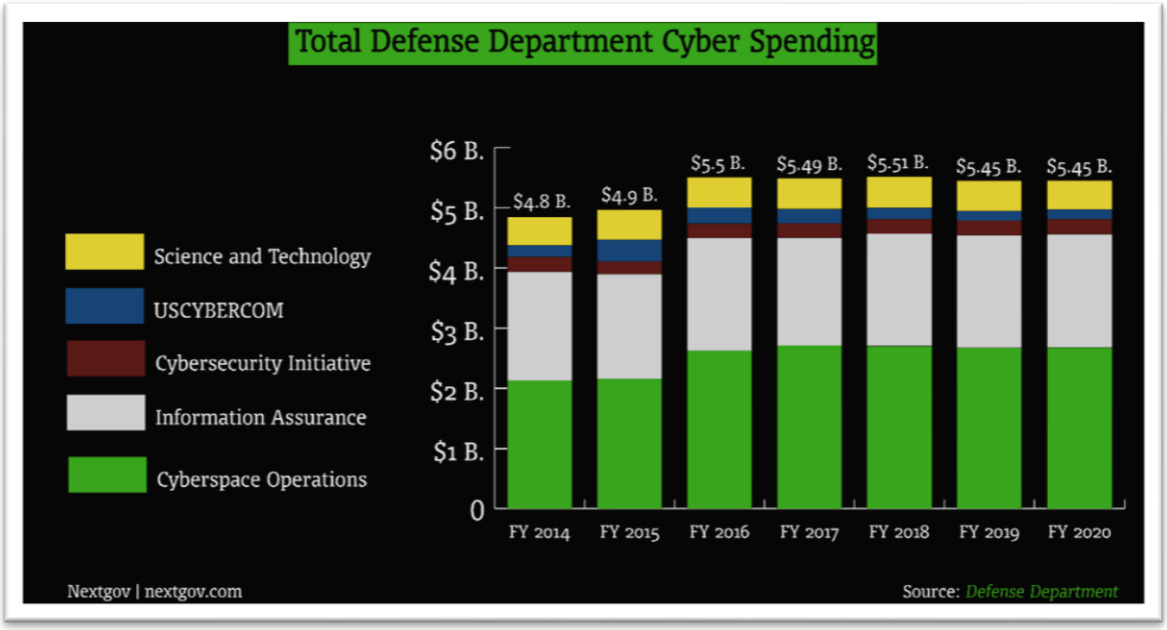
Αυτές είναι μερικές από τις πιο συνηθισμένες επιθέσεις σε Wi-Fi δίκτυα, ας δούμε μερικές ενδιαφέρουσες περιπτώσεις επιθέσεων για τη τεχνολογία Bluetooth:

- **Bluesnarfing:** Με την επίθεση αυτή ο επιτιθέμενος έχει ως σκοπό να αποκτήσει πρόσβαση σε μια συσκευή Bluetooth και να κλέψει πληροφορίες μέσα από αυτή. Αυτή την επίθεση την βλέπουμε περισσότερο στα κινητά τηλέφωνα, με την οποία οι επιτιθέμενοι έκαναν μεγάλη ζημιά στους χρήστες καθώς έκλεβαν διάφορα προσωπικά τους δεδομένα όπως μηνύματα, διευθύνσεις, αριθμούς τηλεφώνων κ.α [16].
- **Bluejacking:** Είναι μια επίθεση με την οποία ο επιτιθέμενος μπορεί να στείλει ανώνυμα μηνύματα σε κάποια συσκευή Bluetooth χωρίς αυτή να ξέρει από ποια συσκευή είναι [16].
- **Bluebagging:** Είναι μια επίθεση με την οποία ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε μια συσκευή Bluetooth όπως για παράδειγμα ένα Smartphone και με τη χρήση εντολών αυτής της συσκευής να πάρεις τον έλεγχο αυτής [16].
- **DoS attack:** Όπως και στο Wi-Fi έτσι και στο Bluetooth κάποιος επιτιθέμενος μπορεί να κάνει DoS επίθεση σε κάποια Bluetooth συσκευή.

Στη τεχνολογία ZWave όμως δεν έχουμε τόσες πολλές επιθέσεις καθώς όπως είπαμε είναι μια καινούρια τεχνολογία που έχει αρχίσει να εφαρμόζεται τα τελευταία δυο χρόνια, έτσι οι επιθέσεις οι οποίες έχουν παρουσιαστεί στα BlackHat αφορούν κυρίως το sniffing των πακέτων και τον έλεγχο διαφόρων συσκευών ZWave.

4 Ανίχνευση Ευπαθειών

Όλα αυτά τα οποία αναφέραμε στη προηγούμενη ενότητα συνιστούν το κύριο λόγο για τον οποίο υπάρχει η ανίχνευση ευπαθειών. Η ανίχνευση ευπαθειών είναι περισσότερο γνωστή ως Penetration Test ή Ethical Hack και όπως είπαμε ο λόγος για τον οποίο το κάνουμε είναι για να θωρακίσουμε όσο γίνεται περισσότερο το σύστημα μας ή το δίκτυο μας απέναντι στις απειλές που υπάρχουν στο κόσμο της πληροφορίας. Ειδικότερα οι επιχειρήσεις δαπανούν αρκετά χρήματα σε ειδικούς ασφάλειας προκειμένου να θωρακίσουν το δίκτυο τους και τα συστήματα τους με το καλύτερο δυνατό τρόπο. Για να καταλάβουμε τη χρησιμότητα της ασφάλειας και της ανίχνευσης ευπαθειών, αρκεί να ρίξουμε μια ματιά στην εικόνα 4.1 στην οποία μπορούμε να δούμε τα ποσά που δαπανά το τμήμα άμυνας της Αμερικής για το Cyber Security, τα οποία φτάνουν στα 5 και 6 δισεκατομμύρια!



Εικόνα 4.1: Δαπάνες Τμήματος Άμυνας Αμερικής [32]

4.1 Ευπάθειες

Οι ευπάθειες είναι ο λόγος για τον οποίο κάνουμε δοκιμή διείσδυσης. Στόχος είναι η εύρεση αυτών για να κάνουμε ένα δίκτυο πιο ασφαλές. Ευπάθεια είναι ένα τρωτό σημείο του δικτύου μας το οποίο μπορεί να γίνει αιτία ώστε ένας hacker να πατήσει πάνω σε αυτό και να σπάσει το δίκτυό μας ώστε να έχει πρόσβαση. Για να κατανοήσουμε καλύτερα την έννοια της ευπάθειας αρκεί να τη δούμε στην καθημερινότητά μας. Μια ευπάθεια λοιπόν θα μπορούσε να είναι το κλείσιμο της πόρτας εισόδου του σπιτιού μας αλλά όχι το κλείδωμα της. Αμέσως το σπίτι μας γίνεται ευπαθές προς τους διαρρήκτες καθώς θα μπορούσαν να το διαρρήξουν πολύ πιο εύκολα απ' ότι αν ήταν κλειδωμένο. Έτσι και στο κόσμο των δικτύων δημιουργούνται ανάλογες ευπάθειες όπως για παράδειγμα η έλλειψη κωδικού πρόσβασης σε ένα δίκτυο.

Στο κόσμο των δικτύων υπάρχουν πάρα πολλές διαφορετικές ευπάθειες, απ' τις οποίες η κάθε μια ξεχωριστά μπορεί να δώσει και ένα διαφορετικό πάτημα στον επιτιθέμενο προκειμένου να σπάσει ένα δίκτυο. Παρακάτω αναγράφονται μερικές από τις κυριότερες ευπάθειες οι οποίες εμφανίζονται σε ασύρματα δίκτυα δεδομένων Wi-Fi, Bluetooth και ZWave.

Ευπάθειες Wi-Fi:

- **Εργοστασιακές ρυθμίσεις:** Μια από τις σημαντικότερες ευπάθειες είναι η μη αλλαγή των εργοστασιακών ρυθμίσεων του router.
- **Έλλειψη κωδικού πρόσβασης:** Η έλλειψη κωδικού πρόσβασης αποτελεί σημαντική ευπάθεια καθώς ο χρήστης μπορεί να έχει ελεύθερη πρόσβαση στο δίκτυο.
- **Αδύναμος κωδικός πρόσβασης:** Πολλές φορές η εφαρμογή κωδικού πρόσβασης στο δίκτυο μας δεν είναι αρκετό. Οι αδύναμοι κωδικοί πρόσβασης αποτελούν ευπάθεια στα ασύρματα δίκτυα Wi-Fi. Ένας αδύναμος κωδικός είναι μικρός σε μήκος και μη συνδυαστικός.
- **Ασφάλεια Wep:** Η ασφάλεια Wep αποτελεί ευπάθεια καθώς θεωρείται πλέον ξεπερασμένη και είναι πάρα πολύ εύκολο να παραβιαστεί.

Οι παραπάνω ευπάθειες αποτελούν μερικές από τις πιο συχνές του Wi-Fi. Παρόμοιες ευπάθειες έχουμε και στο Bluetooth αλλά όχι τόσες πολλές. Μερικές από αυτές είναι οι εξής:

- **Η συσκευή να είναι πάντα ανιχνεύσιμη**
- **Το ελεύθερο ζευγάρωμα συσκευών (Bluetooth pairing)**
- **Τύπος κρυπτογράφησης**

Η τεχνολογία ZWave είναι μια καινούρια τεχνολογία όπως είπαμε και πιο πάνω, η οποία έχει αρχίσει και εξελίσσεται τη τελευταία τριετία. Γι' αυτό το λόγο η ευπάθειες της θα μπορούσαμε να πούμε ότι είναι δύο :

- **Έλλειψη κρυπτογράφησης στα δεδομένα**
- **Έλλειψη κωδικού κατά το ζευγάρωμα συσκευών**

4.2 Δοκιμή Διείσδυσης και Αναζήτηση Ευπαθειών

Για την ασφάλεια των υπολογιστικών συστημάτων και δικτύων μπορούμε να βρούμε πολλά λογισμικά τα οποία κάνουν αναζήτηση ευπαθειών και τις εμφανίζουν στο χρήστη με το πάτημα ενός κουμπιού, γι' αυτό γεννάται το ερώτημα γιατί να κάνω Penetration Test και όχι απλά μια αναζήτηση ευπαθειών με ένα απλό λογισμικό; Η απάντηση είναι πως μια ολοκληρωμένη και σωστή διαδικασία είναι αυτή του Penetration Test καθώς στο Penetration Test υπάρχει και η αναζήτηση ευπαθειών. Για την ακρίβεια η αναζήτηση ευπαθειών κάνοντας χρήση ενός απλού λογισμικού αποτελεί δομικό στοιχείο του Penetration Test.

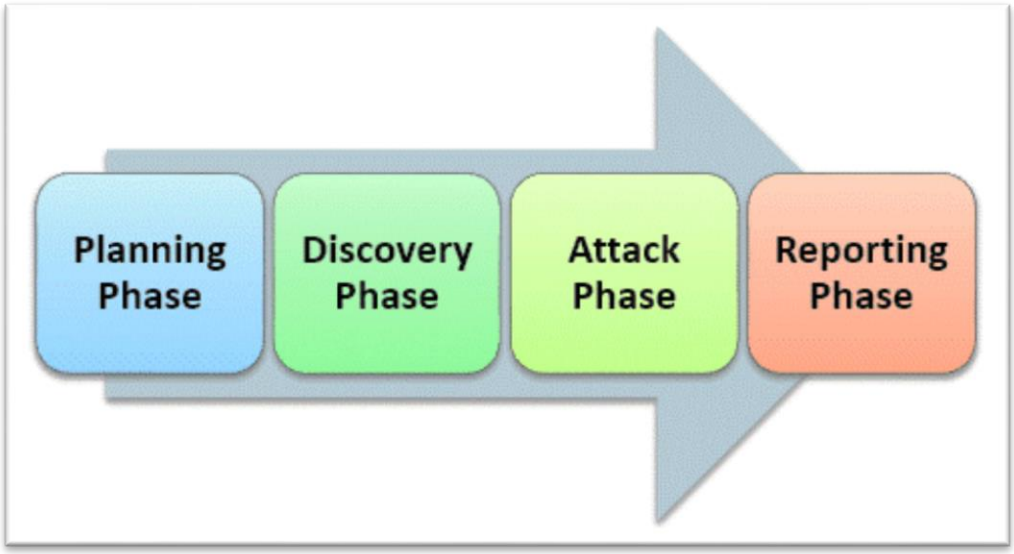
Η αναζήτηση ευπαθειών μπερδεύεται πολλές φορές με το Penetration Test. Όπως αναφέρεται πιο πάνω η αναζήτηση ευπαθειών αποτελεί δομικό στοιχείο του Penetration Test και η λειτουργία της περιορίζεται στο να βρει τις ευπάθειες χωρίς όμως να δώσει στο χρήστη μια εικόνα του τι πραγματικά σημαίνει η ύπαρξη αυτής της ευπάθειας.

Το Penetration Test αποτελεί ένα πιο τελειοποιημένο μηχανισμό αναζήτησης ευπαθειών καθώς δε περιορίζεται μόνο στην εύρεση των ευπαθειών. Το Penetration Test μας δίνει τη δυνατότητα να καταλάβουμε το πραγματικό κίνδυνο ύπαρξης μίας ευπάθειας. Αυτό γίνεται γιατί μόλις ανακαλύψουμε τις ευπάθειες ενός δικτύου ή υπολογιστικού συστήματος παίρνουμε τη θέση του επιτιθέμενου και κάνοντας συγκεκριμένες επιθέσεις μπορούμε να δούμε τη ζημιά που μπορεί να γίνει πατώντας πάνω σε αυτές τις ευπάθειες. Μπορούμε λοιπόν να συμπεράνουμε ότι μια σωστή αναζήτηση και ανίχνευση ευπαθειών δε περιορίζεται στη χρήση ενός Vulnerability

Scanner αλλά στη πραγματοποίηση ενός Penetration Test ώστε να βγάλουμε σαφή συμπεράσματα για την επικινδυνότητα των ευπαθειών που υπάρχουν.

4.3 Μεθοδολογία Δοκιμής Διείσδυσης

Για να έχουμε μια επιτυχημένη δοκιμή διείσδυσης θα πρέπει να ακολουθήσουμε πιστά και αμετάκλητα τη μεθοδολογία της. Η μεθοδολογία μιας δοκιμής διείσδυσης μπορεί να χωριστεί σε 4 διαφορετικά βήματα όπως φαίνεται στην εικόνα 4.2. Τα τέσσερα αυτά βήματα ονομάζονται Σχεδιασμός, Ανίχνευση, Διείσδυση – Επίθεση και Αναφορά [17].



Εικόνα 4.2: Φάσεις Δοκιμής Διείσδυσης [33]

1η Φάση: Το πρώτο βήμα κατά την εκτέλεση μιας δοκιμής διείσδυσης είναι ο Σχεδιασμός. Στο σχεδιασμό θα πρέπει να γίνει ένα αναλυτικό πλάνο το οποίο θα αφορά την εκτέλεση μιας Δοκιμής Διείσδυσης. Κατά το σχεδιασμό γίνονται όλες οι απαραίτητες συζητήσεις με ανθρώπους της επιχείρησης προκειμένου να καταγράψουμε το τύπο δοκιμής διείσδυσης, σε τι θα πραγματοποιηθεί δοκιμή διείσδυσης(ασύρματα δίκτυα δεδομένων, βάσεις δεδομένων κ.λπ.) υπό ποιες προϋποθέσεις θα γίνει, από ποιους και τι ώρα. Όλα αυτά βέβαια πρέπει να συμφωνηθούν γιατί οι ειδικοί της Ασφάλειας Δεδομένων δουλεύουν μέσα στα πλαίσια του νόμου σε αντίθεση με κάποιο εγκληματία Hacker ο οποίος δε χρειάζεται να λάβει υπόψη τίποτα από όλα αυτά, καθώς απλά θα επιτεθεί με σκοπό να σπάσει την ασφάλεια μας για διάφορους προσωπικούς του λόγους αλλά και κέρδος. Αφού

συμφωνηθούν και καταγραφούν όλα τα απαραίτητα θα πρέπει οι ειδικοί να σχεδιάσουν το τρόπο με τον οποίο θα εκτελέσουν την όλη διαδικασία. Επομένως οι τρεις βασικοί περιορισμοί που ξεχωρίζουν έναν ειδικό ασφάλειας από έναν εγκληματία είναι:

- Νόμος
- Δικαιώματα
- Χρόνος

Αυτούς τους περιορισμούς είναι που θα πρέπει να ληφθούν σοβαρά υπόψη κατά την εκτέλεση της δοκιμής έτσι ώστε να μην υπάρξουν σοβαρά προβλήματα από το νόμο[17].

2η Φάση: Στη δεύτερη φάση Ανίχνευση περνάμε αφού ολοκληρωθεί η πρώτη. Στη φάση της ανίχνευσης ξεκινάει το πρακτικό κομμάτι της δοκιμής. Σε αυτή τη φάση συλλέγονται όλες οι απαραίτητες πληροφορίες για το στόχο. Η ανίχνευση περιλαμβάνει τις φάσεις:

- Footprint
- Σάρωση και Απαρίθμηση (Scan and Enumeration)
- Ανάλυση Ευπαθειών (Vulnerability Analysis)

Στη φάση **Footprint** γίνεται αναζήτηση στο internet για διάφορα στοιχεία που μπορεί να αφορούν την επιχείρηση. Τέτοια στοιχεία μπορεί να είναι email τα οποία μπορεί να υπάρχουν στο internet πρόσωπα της εταιρείας usernames αλλά και passwords! Είναι αρκετά σημαντική διαδικασία αν σκεφτεί κανείς τι μπορεί να βρεθεί σε βάσεις δεδομένων στο διαδίκτυο. Το Footprint μπορεί να γίνει με χρήση διαφόρων εργαλείων (whois κ.α) [17].

Στη φάση **Scan and Enumeration** συλλέγουμε διάφορες τεχνικές πληροφορίες γύρω από το στόχο. Τέτοιες πληροφορίες μπορεί να είναι ονόματα δικτύων, υπολογιστών, πόρτες οι οποίες είναι ανοιχτές, εφαρμογές και υπηρεσίες οι οποίες τρέχουν σε αυτές, πληροφορίες δικτύων, πληροφορίες λειτουργικού κ.α. Όλη αυτή η αναζήτηση γίνεται κάνοντας χρήση ειδικών εργαλείων από τα οποία κάποια μπορεί να είναι ανοιχτά λογισμικά και άλλα όχι. Μετά την ολοκλήρωση της αναζήτησης

πρέπει να επαληθεύσουμε αν όντως τρέχουν στο σύστημα όλα αυτά που βρέθηκαν [17].

Στη φάση **Vulnerability Analysis** αφού έχουμε συγκεντρώσει όλες τις πληροφορίες από τα προηγούμενα βήματα, εξετάζουμε πλέον την ύπαρξη ευπαθειών στο σύστημα. Αυτό μπορεί να γίνει με τις γνώσεις που έχει ένας ειδικός στις υπάρχουσες ευπάθειες ή κάνοντας χρήση εργαλείων ικανών στην εύρεση ευπαθειών. Γενικά τις ευπάθειες που υπάρχουν τις 'μαρτυρούν' οι πληροφορίες οι οποίες έχουμε συγκεντρώσει, γι' αυτό και θα πρέπει να εξετάζονται όλες πάρα πολύ προσεκτικά [17].

Οι ειδικοί στην ασφάλεια θα πρέπει να είναι συνεχώς ενημερωμένοι για τις τελευταίες εξελίξεις στο χώρο της ασφάλειας και ειδικότερα για τις ευπάθειες οι οποίες εμφανίζονται!

3η Φάση: Στη τρίτη φάση Επίθεση αξιοποιούμε τις ευπάθειες που βρήκαμε στη δεύτερη φάση. Η αξιοποίηση αυτών των ευπαθειών μας δίνει τη δυνατότητα να κατανοήσουμε την επικινδυνότητα ύπαρξης των ευπαθειών. Επίσης μας δίνει ρεαλιστικά αποτελέσματα χρησιμοποίησης αυτών. Η αξιοποίηση αυτών των ευπαθειών γίνεται πραγματοποιώντας επιθέσεις στο στόχο που έχει τεθεί. Οι επιθέσεις μπορούν να επιτευχθούν κάνοντας χρήση κάποιον exploits τα οποία είναι προγράμματα, δηλαδή γραμμές κώδικα ή και μια απλή εντολή τα οποία όμως εκμεταλλεύονται μια ευπάθεια του συστήματος ώστε να δώσει στον επιτιθέμενο αποτελέσματα τα οποία μπορούν να θέσουν σε κίνδυνο μια επιχείρηση ή κάποιο χρήστη. Exploits μπορούν να βρεθούν έτοιμα στο διαδίκτυο ή μπορούν να γραφτούν από ειδικούς οι οποίοι έχουν πολύ καλές γνώσεις στους τομείς δικτύων, λειτουργικών και φυσικά στο προγραμματισμό. Εκτός όμως από τα exploits μπορεί να γίνει και χρήση έτοιμων εργαλείων τα οποία δέχονται για είσοδο πληροφορίες που έχουμε συλλέξει και πραγματοποιούν την επίθεση [17] .

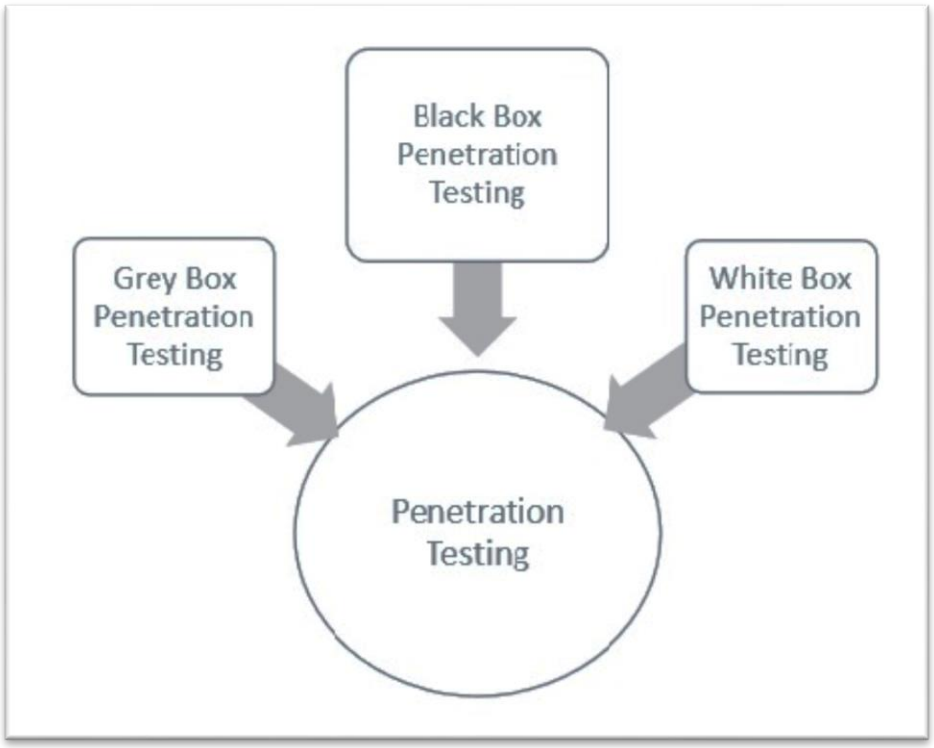
Η 3η φάση θέλει πολύ προσοχή καθώς μπορεί να προκαλέσει ζημιά ή να θέσει σε κίνδυνο μια επιχείρηση ή κάποια άτομα. Επίσης θα πρέπει να τηρούνται στο έπακρο όσα έχουν συμφωνηθεί στη πρώτη φάση. Για λόγους ασφάλειας θα πρέπει να καταγράφεται ότι γίνεται κατά την επίθεση [17].

4η Φάση: Η 4η φάση αποτελεί το τελευταίο βήμα της μεθοδολογίας και θεωρείται πολύ σημαντικό. Στη φάση Αναφορά συγκεντρώνουμε όλη τη δουλειά που έχουμε κάνει, τα αποτελέσματα αυτής και τα συμπεράσματα της. Αφού τα συλλέξουμε αυτά γράφουμε μια αναλυτική αναφορά. Στην αναφορά θα πρέπει να υπάρχουν επίσης αναλυτικά γραφήματα, πίνακες, ανάλυση ρίσκου, αναφορά στις επιπτώσεις και τους κινδύνους που έχουν οι ευπάθειες οι οποίες βρέθηκαν και αναλυτικές πληροφορίες για το έργο αυτό.

Η ολοκλήρωση των τεσσάρων αυτών φάσεων αποτελούν μια Δοκιμή Διείσδυσης. Όσο πιο προσεκτικά και αναλυτικά γίνει η κάθε φάση ξεχωριστά τόσο μεγαλύτερη επιτυχία θα έχει η Δοκιμή Διείσδυσης. Μια Δοκιμή Διείσδυσης θα πρέπει να γίνεται πάντα τηρώντας όσα έχουν συμφωνηθεί με τον υπεύθυνο του συστήματος υπό έλεγχο!

4.4 Τύποι Δοκιμής Διείσδυσης

Υπάρχουν διαφορετικοί τύποι και τομείς Δοκιμής Διείσδυσης. Υπάρχουν τρείς διαφορετικοί τρόποι Δοκιμής Διείσδυσης, οι οποίοι διαφέρουν κυρίως στη πληροφορία την οποία θα έχει ένας ειδικός για το στόχο προς δοκιμή. Οι τρεις αυτοί διαφορετικοί τρόποι ονομάζονται Δοκιμή Μαύρου Κουτιού(Black-box Testing), Δοκιμή Άσπρου Κουτιού(White-box Testing) και Δοκιμή Γκρι Κουτιού (Grey-box Testing) [18].



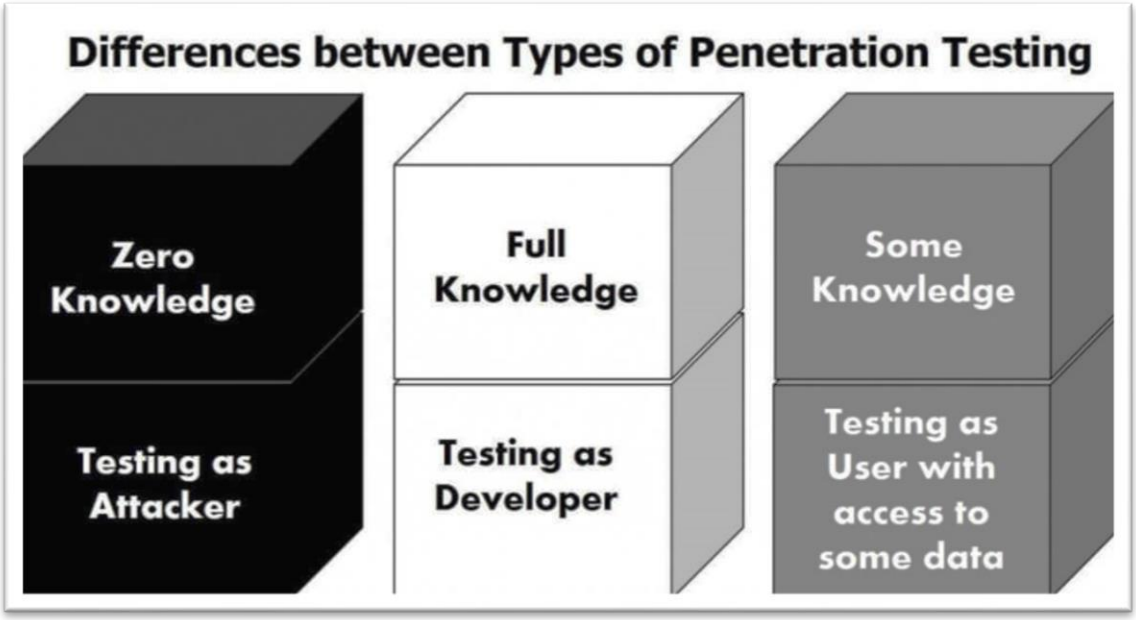
Εικόνα 4.3: Τύποι Penetration Test [34]

Black-box Testing: Στο black-box testing το άτομο που εκτελεί τη δοκιμή δεν γνωρίζει τίποτα απολύτως για το στόχο. Ξεκινάει από την αρχή να συλλέγει πληροφορίες γι' αυτόν με σκοπό να εκτελέσει κάποιες επιθέσεις. Θα μπορούσαμε να πούμε ότι αυτός που εκτελεί τη δοκιμή συμπεριφέρεται σαν ένα cracker που ξεκινάει από το μηδέν για να κάνει μια επίθεση. Βέβαια το άτομο που εκτελεί τη δοκιμή γνωρίζει ποιο θα είναι το αποτέλεσμα αλλά δε γνωρίζει τον τρόπο με τον οποίο θα φτάσει σε αυτό, γι' αυτό το λόγο ξεκινάει συλλέγοντας πληροφορίες για το στόχο [18].

White-box Testing: Στο white-box testing στο άτομο που εκτελεί τη δοκιμή έχουν δοθεί όλες οι πληροφορίες για το στόχο όπως λειτουργικό, ονόματα δικτύων, IP διευθύνσεις κ.α. Το μόνο που χρειάζεται να γίνει είναι οι δοκιμές διείσδυσης με βάση της πληροφορίες που έχουν δοθεί. Στο συγκεκριμένο τρόπο ένα μέρος της φάσης Ανίχνευση($2^{η}$ φάση) δεν υλοποιείται καθώς οι πληροφορίες για το στόχο έχουν δοθεί [18].

Grey-box Testing: Το grey-box testing αποτελεί ένα συνδυασμό των black-box και white-box καθώς το άτομο που εκτελεί την Δοκιμή Διείσδυσης έχει λάβει μερικές

πληροφορίες για το στόχο αλλά όχι λεπτομέρειες όπως στο white-box. Θεωρείται ότι είναι ο πιο συνηθισμένος τρόπος δοκιμής διείσδυσης [18].



Εικόνα 4.4: Διαφορές Ανάμεσα στους τύπους Δοκιμής Διείσδυσης [35]

4.5 Εργαλεία Δοκιμής Διείσδυσης

Για να μπορέσουμε να πετύχουμε μια ανίχνευση ευπαθειών σε κάποιο ασύρματο δίκτυο δεδομένων, χρειαζόμαστε τη βοήθεια ειδικών εργαλείων. Αυτά τα εργαλεία είναι λογισμικά φτιαγμένα έτσι ώστε να κάνουν κάποια αναζήτηση πληροφοριών σε ένα δίκτυο, αναζήτηση ευπαθειών σε κάποιο δίκτυο και κάποια διείσδυση σε ένα δίκτυο ώστε να μπορέσουμε να έχουμε μια σαφή εικόνα της ύπαρξης μιας ευπάθειας. Στο πίνακα 4.1 παρουσιάζονται μερικά από τα πιο δημοφιλή εργαλεία για αναζήτηση ευπαθειών τα οποία μπορούν να μας βοηθήσουν να έχουμε αποτέλεσμα σε κάθε βήμα σε μια τέτοια αναζήτηση.

Πίνακας 4.1: Εργαλεία Δοκιμής Διείσδυσης σε Ασύρματα Δίκτυα

Εργαλείο	Ιδιότητα	Διαθεσιμότητα

Nmap	Σάρωση μηχανημάτων και υπηρεσιών. Εξερεύνηση Δικτύων.	Linux, Windows, και Mac OS X
Aircrack-ng	Σπάει ασφάλειες WEP, WPA, WPA2	Linux, Solaris, Windows, OS X, freeBSD
Airodump-ng	Καταγραφή πακέτων ασυρμάτων δικτύων 802.11	Linux, Solaris, Windows, OS X, freeBSD
Aireplay-ng	Αποστολή μη έγκυρων πακέτων πιστοποίησης (DeAuthentication At-tack).	Linux, Solaris, Windows, OS X, freeBSD
Hashcat	Εργαλείο παραβίασης κωδικών πρόσβασης κάνοντας χρήση τη κάρτα γραφικών (GPU)	Linux, Windows, και Mac OS X
Airbase-ng	Προκαλεί επιθέσεις παραπλάνησης με βάση το AP.	Linux, Solaris, Windows, OS X, freeBSD
Wireshark	Κάνει καταγραφή πακέτων ασυρμάτων δικτύων και κάνει ανάλυση πρωτοκόλλων	Windows, OS X και Linux
Airjack	Πραγματοποιεί επιθέσεις MITM και DoS	Linux
Btscanner	Συλλογή πληροφοριών για Bluetooth συσκευές	Windows XP και Linux
Bluediving	Αποτελεί μια σουίτα δοκιμής διείσδυσης σε Bluetooth συσκευές	Linux και

	πραγματοποιώντας επιθέσεις όπως Bluebag, Bluesnarf, bluesmack κ.α.	freeBSD
Btcrack	Εργαλείο για Bluetooth το οποίο πραγματοποιεί σπάσιμο PIN και LINK-KEY	Linux
ezstumbler	Εξερεύνηση δικτύου zwave	Linux
ezrecon	Συλλογή πληροφοριών γύρω από μια συσκευή όπως όνομα, έκδοση firm-ware, κλάσεις εντολών και ρυθμίσεις	Linux
ezfingerprint	Βρίσκει τη γενιά της συσκευής zwave (π.Χ. $3^{η}$ ή $5^{η}$)	Linux

5 Σενάριο Αναζήτησης Ευπαθειών σε Ασύρματο Δίκτυο Δεδομένων Wi-Fi

Στο κεφάλαιο αυτό γίνεται παρουσίαση μιας Αναζήτησης – Ανίχνευσης Ευπαθειών σε ασύρματο δίκτυο Wi-Fi με πραγματικά δεδομένα, περνώντας απ' όλες τις φάσεις τις διαδικασίας. Σε αυτό το σενάριο δοκιμής διείσδυσης υποθέτουμε ότι κάνουμε δοκιμή στο AP μιας επιχείρησης του οποίου το όνομα είναι TestNet το οποίο θεωρείται εργοστασιακό ssid.

5.1 1η Φάση – Σχεδιασμός

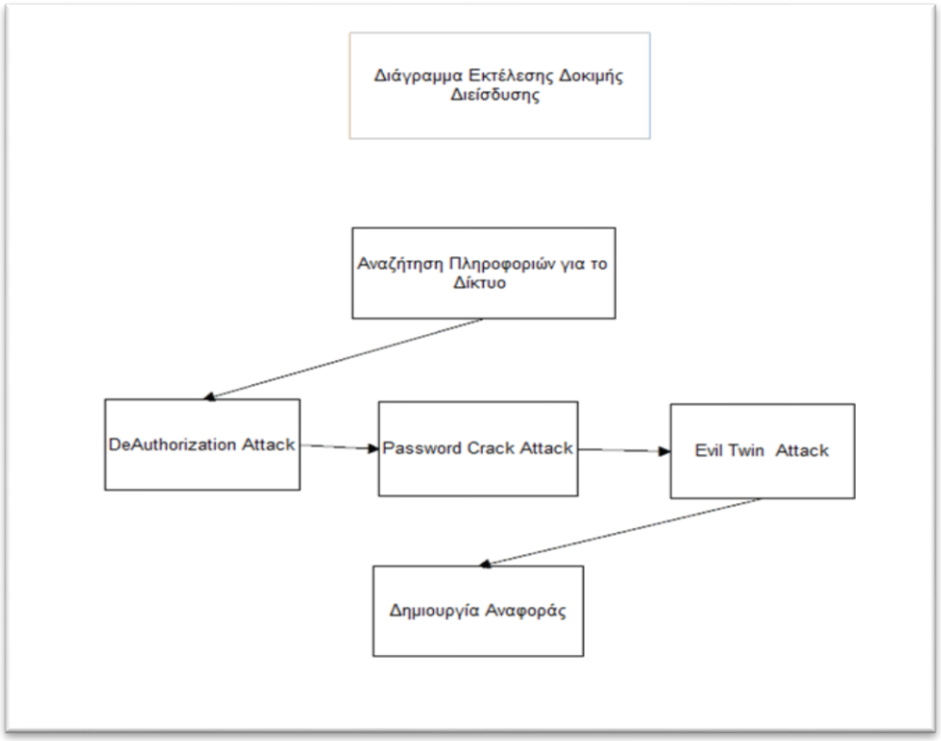
Στη πρώτη φάση σχεδιάζουμε προσεκτικά τι θέλουμε να δοκιμάσουμε στο δίκτυό μας, ποιες επιθέσεις θα πραγματοποιήσουμε καθώς και να ληφθούν υπόψη όλες οι νομικές διατάξεις. Για αυτούς τους λόγους θα κατασκευάσουμε ένα πλάνο με το τι έχει συμφωνηθεί και τι θα κάνουμε. Στο πλαίσιο αυτού του σεναρίου και για τη πτυχιακή θα παρουσιαστούν τρεις επιθέσεις για την εύρεση ευπαθειών. Αυτές οι επιθέσεις θα είναι εύρεση κωδικού πρόσβασης (password crack) στο Wi-Fi δίκτυο, αποστολή μη πιστοποιημένων πακέτων (DeAuthorization) σε αυτό και ένα Evil Twin. Άρα θα πρέπει να φτιαχτεί ένας πίνακας με το τι έχει συμφωνηθεί και με το αν τηρεί τις νομικές διατάξεις.

Πίνακας 5.1: Παράδειγμα Πίνακα Αναζήτησης Ευπαθειών

Πίνακας Σχεδιασμού Αναζήτησης Ευπαθειών σε Δίκτυο Wi-Fi				
Ημερομηνία	**Αριθμός Δοκιμής**	**Δοκιμή**	**Συμφωνία με τον υπεύθυνο του συστήματος υπό έλεγχο**	**Νομική Κάλυψη**
30/6/2016	1	Δοκιμή επίθεσης Password Crack	✓	✓
30/6/2016	2	Δοκιμή επίθεσης DeAuthorization	✓	✓

30/6/2016	3	Δοκιμή Επίθεσης Evil Twin	✓	✓

Αφού έχουμε φτιάξει ένα πίνακα με όσα έχουν συμφωνηθεί για την αναζήτηση ευπαθειών στο ασύρματο δίκτυο ακολουθεί ο σχεδιασμός ενός σχεδιαγράμματος για το πώς θα συνεχιστεί η διαδικασία αυτή.



Εικόνα 5.1: Διάγραμμα εκτέλεσης Αναζήτησης Ευπαθειών σε Wi-Fi

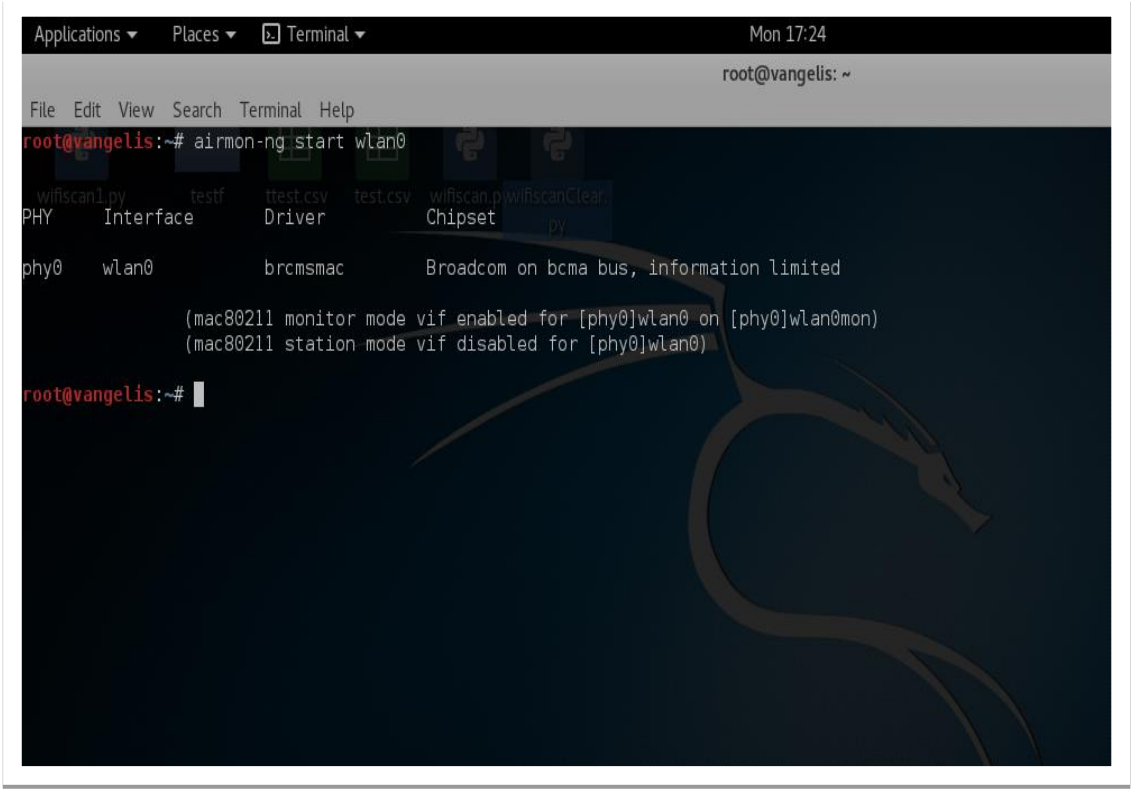
Με την ολοκλήρωση του σχεδιασμού περνάμε στο επόμενο βήμα το οποίο είναι η συγκέντρωση πληροφοριών για το δίκτυο.

5.2 2η Φάση – Ανίχνευση

Σε αυτή τη φάση θα παρουσιαστεί ο τρόπος με τον οποίο θα γίνει συγκέντρωση των πληροφορίων για το δίκτυο τις οποίες χρειαζόμαστε για την αναζήτηση ευπαθειών σε αυτό. Η συγκέντρωση των πληροφοριών θα γίνει με εργαλεία τα οποία έχουν αναφερθεί στο προηγούμενο κεφάλαιο και σε περιβάλλον Kali Linux.

Το πρώτο που κάνουμε είναι να θέσουμε το δίκτυο μας σε monitor mode καθώς σε αυτή τη κατάσταση μας δίνεται η δυνατότητα να λαμβάνουμε όλη τη κίνηση του

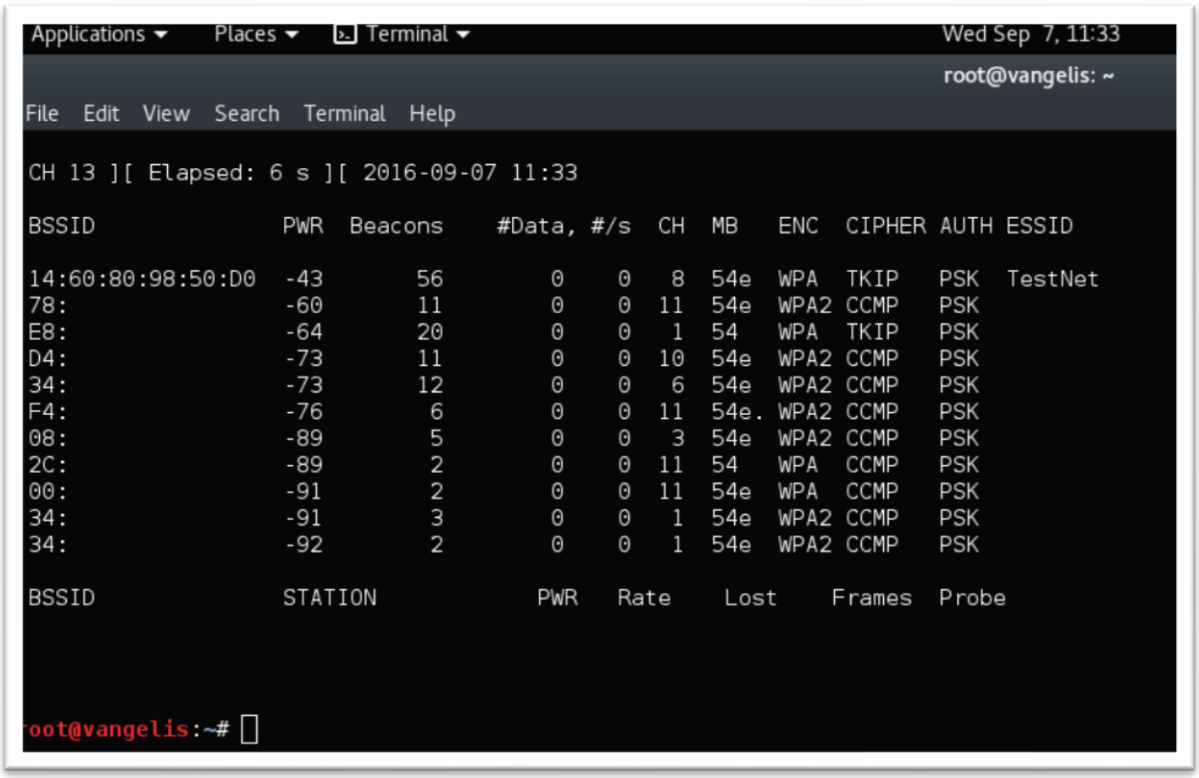
δικτύου. Για να μπορέσουμε να θέσουμε το δίκτυο μας σε monitor mode θα χρησιμοποιήσουμε την εντολή **airmon-ng start wlan0** όπου wlan0 είναι η διεπαφή της κάρτας δικτύου μας.



Εικόνα 5.2: Αλλαγή διεπαφής σε Monitor Mode

Στην οθόνη μας στο τερματικό βλέπουμε το αποτέλεσμα εκτέλεσης αυτής της εντολής το οποίο μας λέει ότι έχει δημιουργήσει μια διεπαφή wlan0mon η οποία αφορά το monitor mode.

Στη συνέχεια εκτελούμε την εντολή **airodump-ng wlan0mon** για τη συγκέντρωση πληροφοριών γύρω από το δίκτυο στόχο.



Εικόνα 5.3: Συλλογή Πληροφοριών για το δίκτυο με το Airodump-ng

Στην εικόνα 5.3 φαίνεται το δίκτυο το οποίο μας ενδιαφέρει, **TestNet** αλλά και όλες οι πληροφορίες που θέλουμε γι' αυτό όπως η Mac διεύθυνση του, η ασφάλεια η οποία χρησιμοποιεί, η κρυπτογράφηση κλπ. Το ESSID TestNet αποτελεί εργοστασιακό ESSID.

Στην εικόνα 5.3 βλέπουμε όλες τις πληροφορίες τις οποίες χρειαζόμαστε για να προχωρήσουμε στη φάση της επίθεσης. Βλέποντας τη παραπάνω εικόνα μπορούμε να διαπιστώσουμε κάποιες ευπάθειες του δικτύου:

1. Χρησιμοποίηση εργοστασιακού ESSID
2. Χρησιμοποιεί Encryption WPA και όχι WPA2
3. Χρήση Cipher TKIP

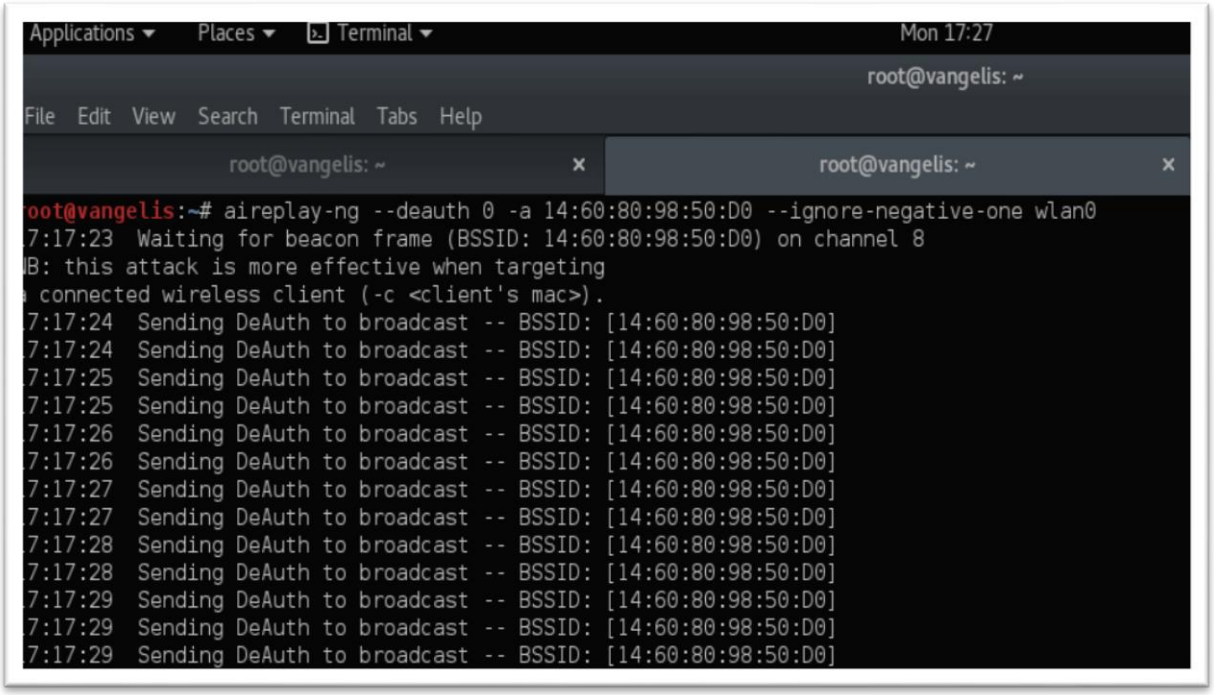
Από τη φάση της ανίχνευσης έχουμε βγάλει ήδη κάποια βασικά συμπεράσματα. Συνεχίζουμε στη φάση της επίθεσης προκειμένου να δούμε την επικινδυνότητα αυτών των ευπαθειών και για την εύρεση περισσότερων κενών ασφαλείας.

5.3 3η Φάση – Επίθεση

Σε αυτή τη φάση εκτελούμε επιθέσεις οι οποίες έχουν συμφωνηθεί στη 1η φάση του Penetration Test για να δούμε τα αποτελέσματα εκμετάλλευσης των ευπαθειών αυτών αλλά και για την ανίχνευση περισσότερων κενών ασφαλείας.

- **1η Επίθεση DeAuthorization Attack**

Η πρώτη επίθεση που θα δοκιμαστεί πάνω στο δίκτυο θα είναι τύπου DoS και θα πραγματοποιηθεί κάνοντας DeAuthorization attack με το εργαλείο aireplay-ng.



Εικόνα 5.4: Επίθεση DeAuthorization (DoS Attack)

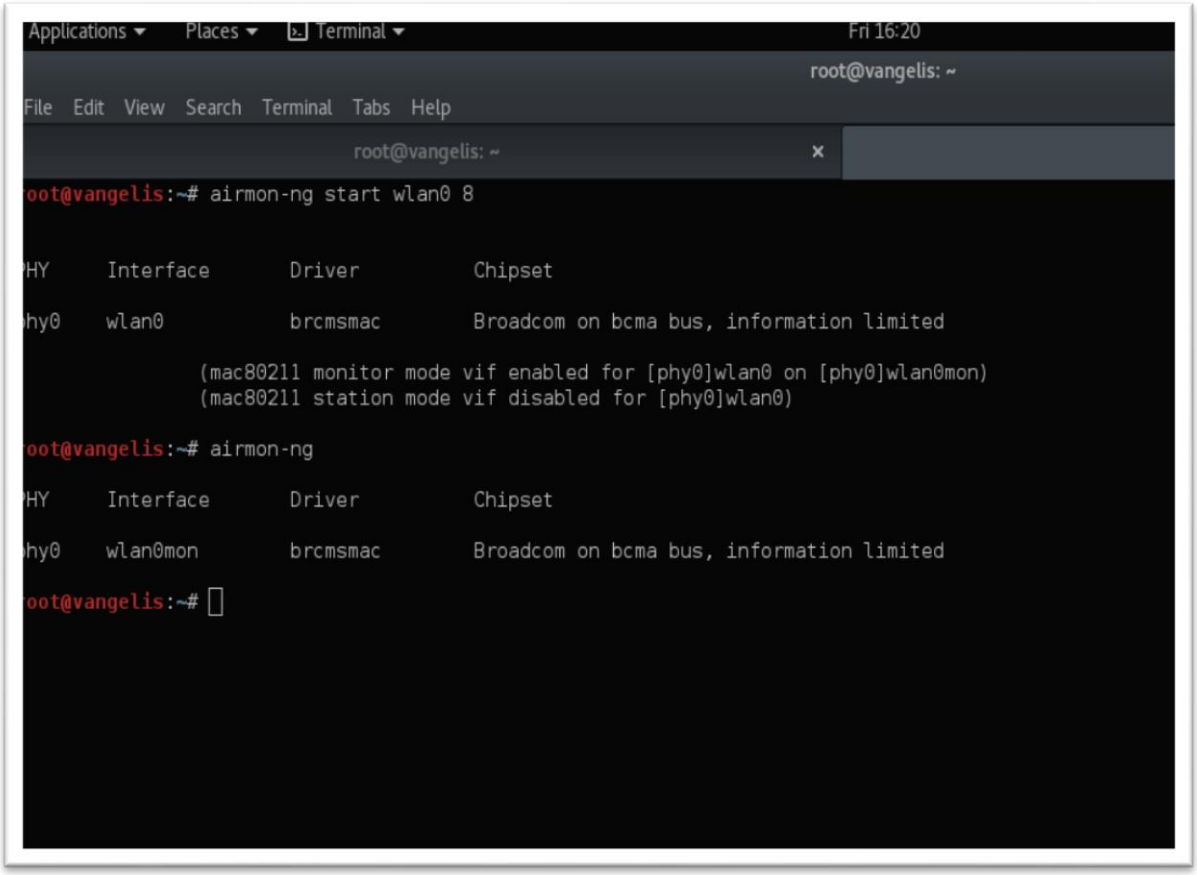
Βλέπουμε ότι χρησιμοποιήσαμε τα στοιχεία που συλλέξαμε από το Information Gathering προκειμένου να πραγματοποιήσουμε αυτή την επίθεση. Η επίθεση έχει γίνει σε όλο το δίκτυο, δηλαδή σε όλους τους χρήστες οι οποίοι είναι συνδεδεμένοι στο AP. Με αυτό το τρόπο καταφέραμε να τους βγάλουμε όλους εκτός υπηρεσιών δικτύου στέλνοντας μη πιστοποιημένα πακέτα. Η συγκεκριμένη επίθεση είχε 100% επιτυχία.

- **2η Επίθεση Wpa Password Crack**

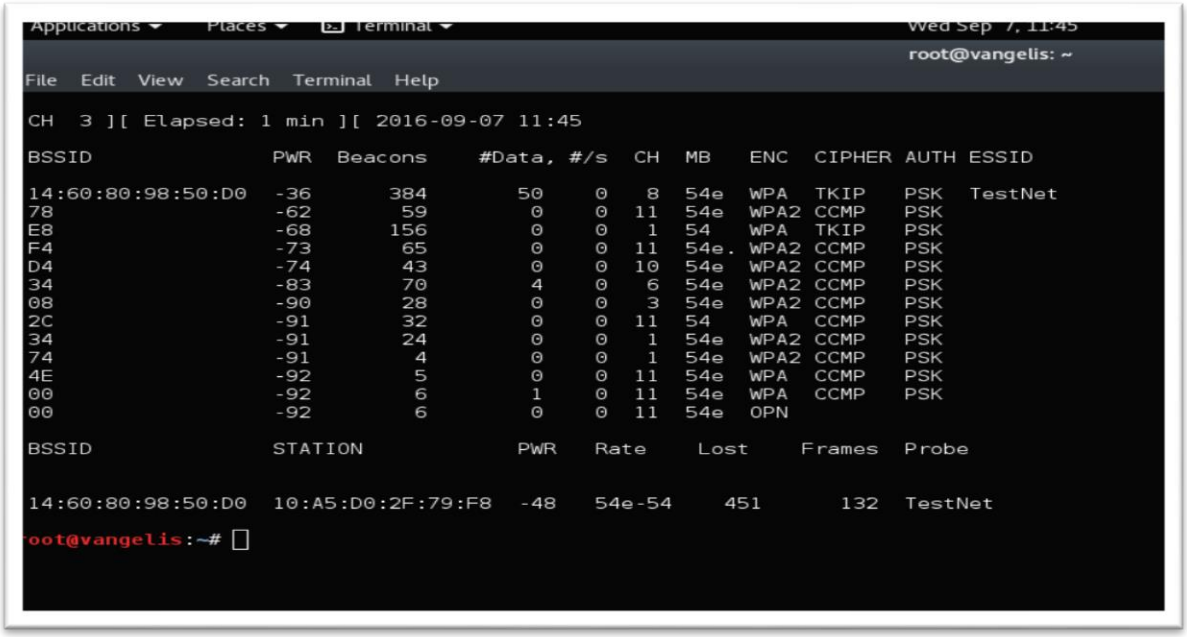
Σε αυτή την επίθεση θέλουμε με βάση τα στοιχεία που έχουμε αλλά και τα πρώτα συμπεράσματα που βγάλαμε για ευπάθειες στο δίκτυο μας, να δούμε πόσο σοβαρή

είναι η ευπάθεια της ασφάλειας WPA και να βρούμε πόσο δυνατός είναι ο κωδικός πρόσβασης που υπάρχει στο δίκτυο μας.

Η επίθεση αυτή ξεκινάει με την εύρεση ενός χρήστη ο οποίος είναι συνδεδεμένος στο δίκτυο. Γι' αυτό ξεκινάμε βάζοντας τη κάρτα δικτύου μας σε monitor mode προκειμένου να πιάνουμε όλη την ασύρματη πληροφορία και εκτελούμε ένα airodump για να βρούμε τους χρήστες οι οποίοι είναι συνδεδεμένοι στο δίκτυο μας.

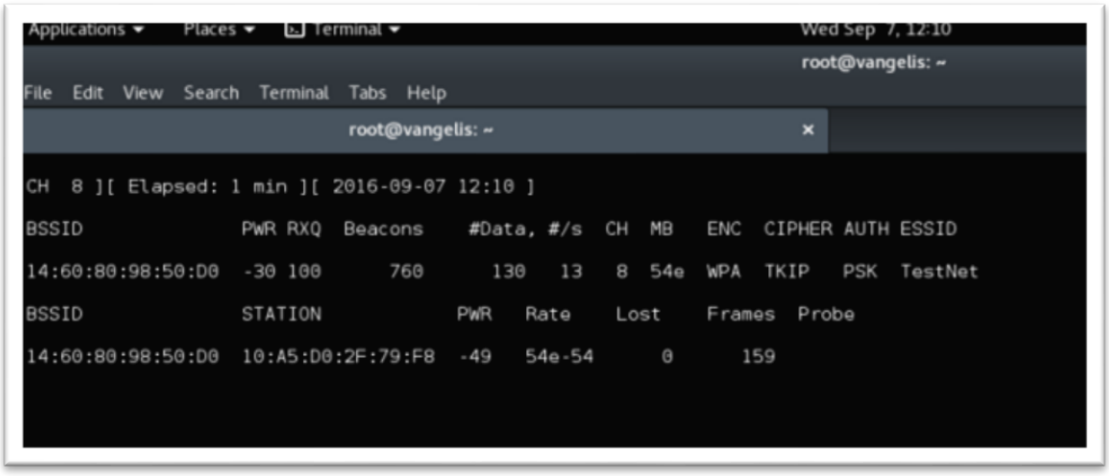


Εικόνα 5.5: Κάρτα Δικτύου σε Monitor Mode

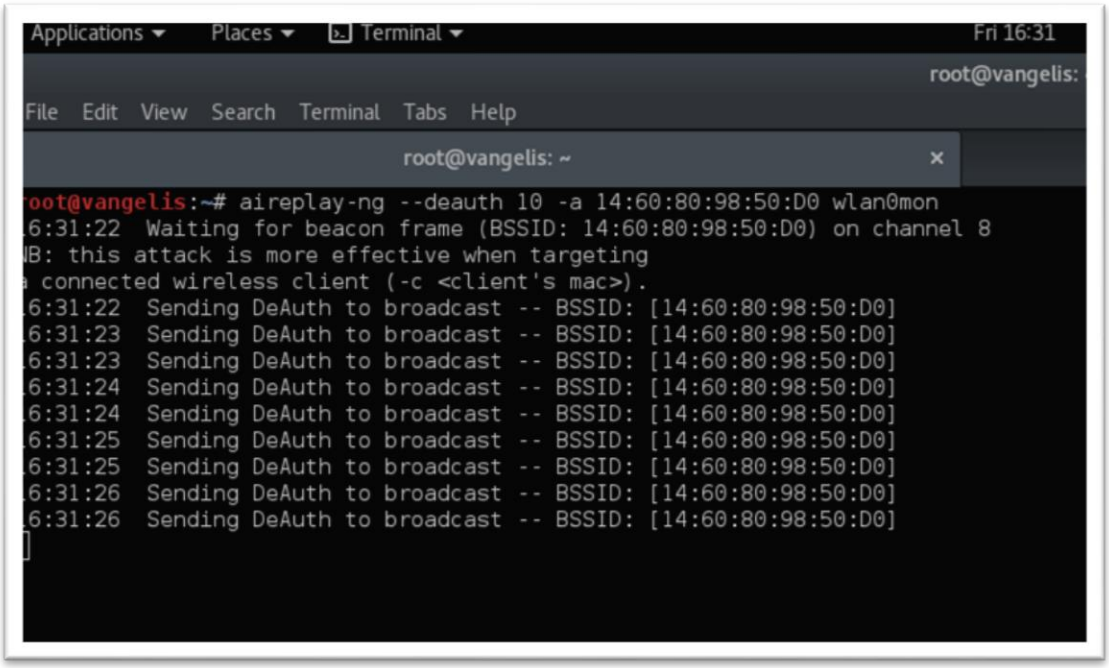


Εικόνα 5.6: Χρήση Airodump-ng για εύρεση συνδεδεμένων συσκευών

Βρήκαμε ότι η συσκευή με Mac διεύθυνση 10:A5:D0:2F:79:F8 είναι συνδεμένη στο δίκτυο μας. Εκμεταλλεύοντας αυτή τη συσκευή πιάνουμε τα πακέτα τα οποία περιέχουν το κωδικό πρόσβασης. Αρχικά αρχίζουμε να καταγράφουμε τα πακέτα τα οποία μεταφέρονται από τη συσκευή αυτή. Στη συνέχεια εκτελούμε μια DeAuthorization επίθεση με σκοπό η συσκευή να βγει εκτός δικτύου με τα μη πιστοποιημένα πακέτα τα οποία στέλνουμε. Έτσι στη συνέχεια μόλις σταματήσουμε την DeAuthorization επίθεση η συσκευή θα ξαναπροσπαθήσει να συνδεθεί στέλνοντας το σωστό κωδικό πρόσβασης, τον οποίο θα πιάσουμε με τη καταγραφή των πακέτων.

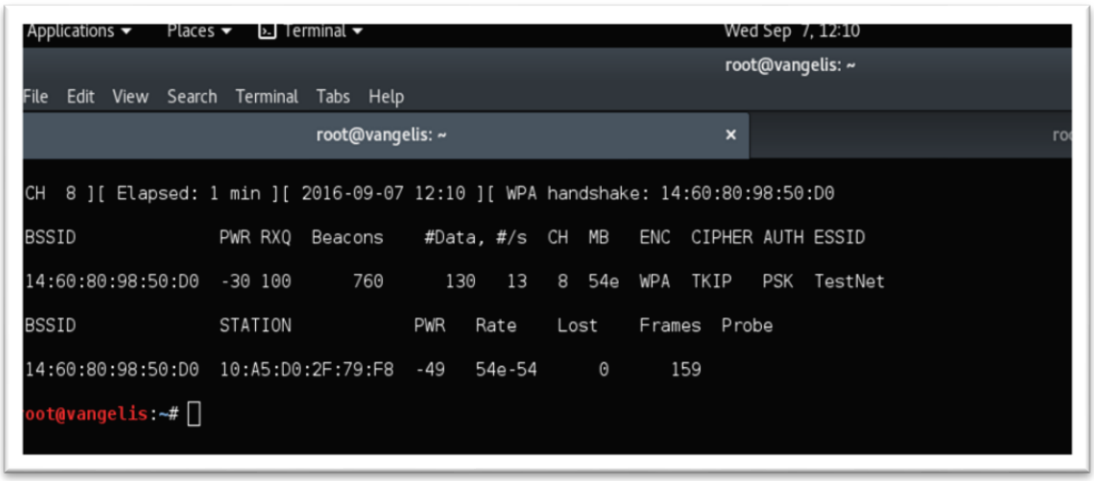


Εικόνα 5.7: Καταγραφή Πακέτων του AP



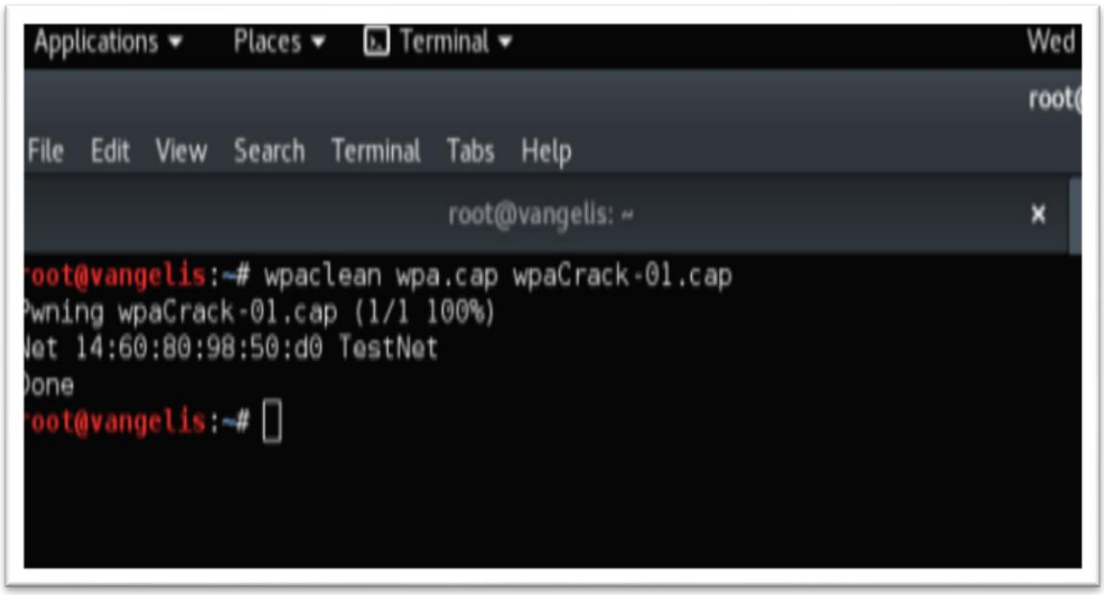
Εικόνα 5.8: Επίθεση DeAuthorization με Aireplay

Μόλις γίνει η καταγραφή των πακέτων χειραψίας δηλαδή των πακέτων τα οποία περιέχουν κρυπτογραφημένο το κωδικό πρόσβασης, το airodump μας εμφανίζει το μήνυμα handshake το οποίο μας γνωστοποιεί ότι έχουμε καταγράψει τα επιθυμητά πακέτα ώστε να σταματήσουμε τη καταγραφή.



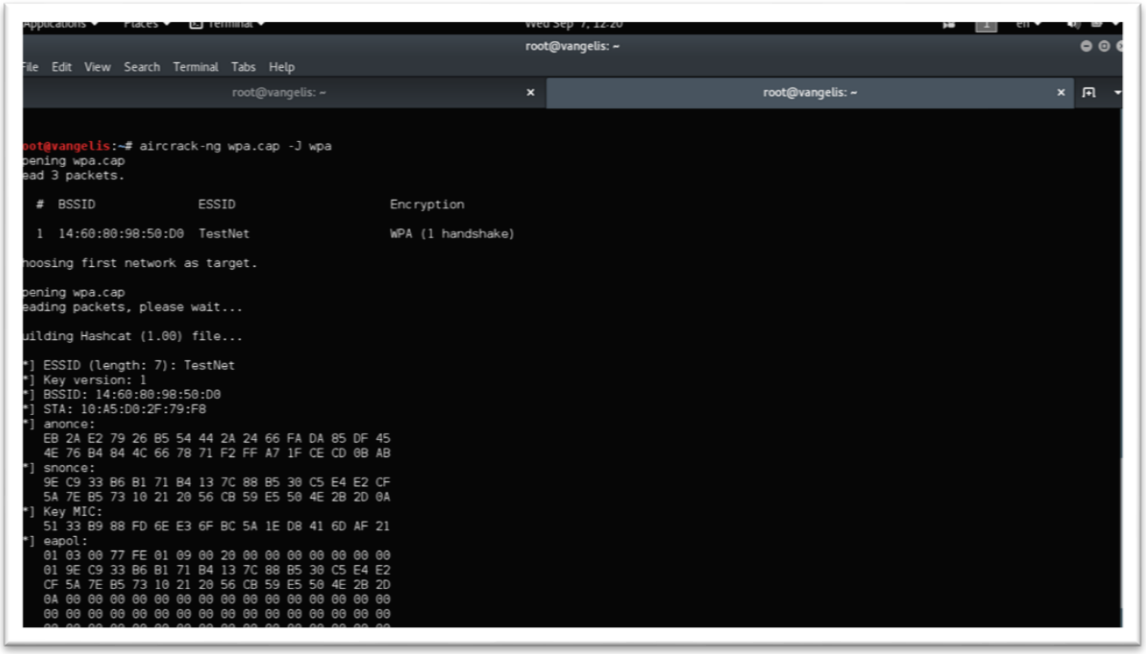
Εικόνα 5.9: Airodump-ng - Ένδειξη Handshake

Στο επόμενο βήμα καθαρίζουμε το αρχείο από την άχρηστη πληροφορία ώστε να μείνει μόνο το Handshake.



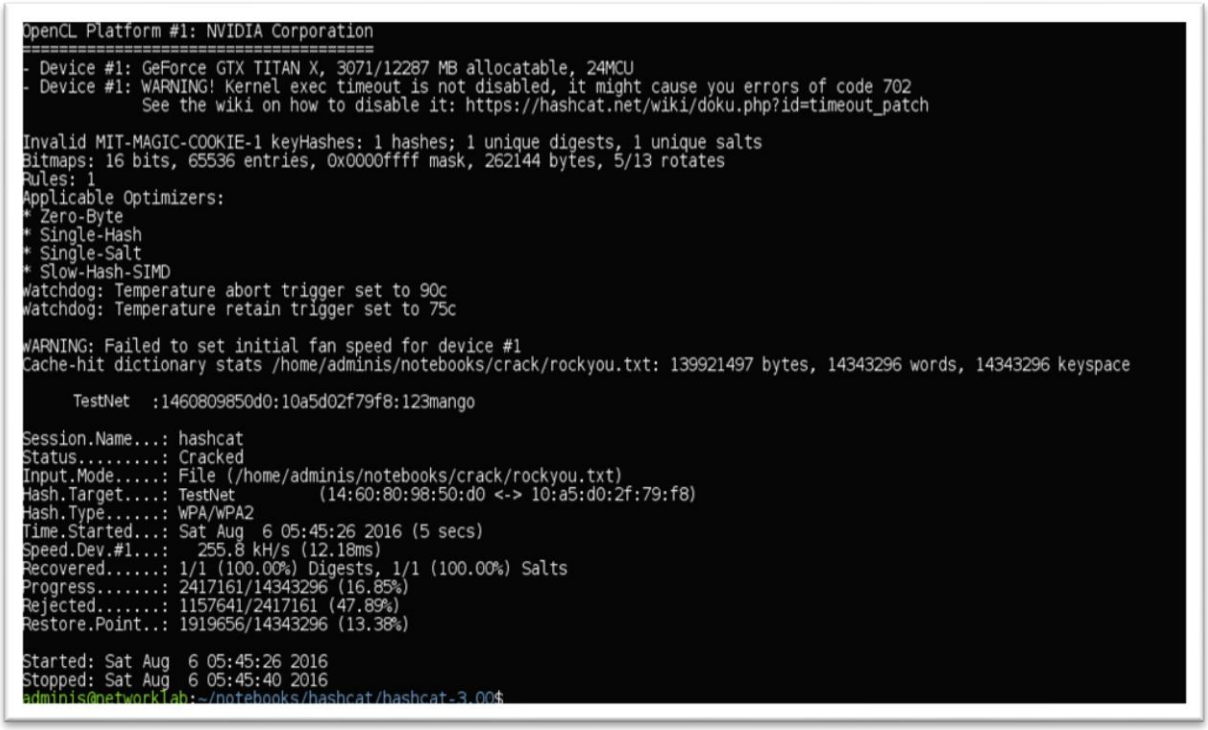
Εικόνα 5.10: Καθαρισμός αρχείου καταγραφής

Στη συνέχεια θα προσπαθήσουμε να σπάσουμε το κωδικό αυτό με το εργαλείο hashcat, χρησιμοποιώντας τη τεχνική dictionary attack. Το hashcat δουλεύει με hccap αρχεία οπότε θα μετατρέψουμε το αρχείο μας σε hccap.



Εικόνα 5.11: Μετατροπή cap αρχείου σε hccap

Εικόνα 5.12: Password Crack με χρήση GPU



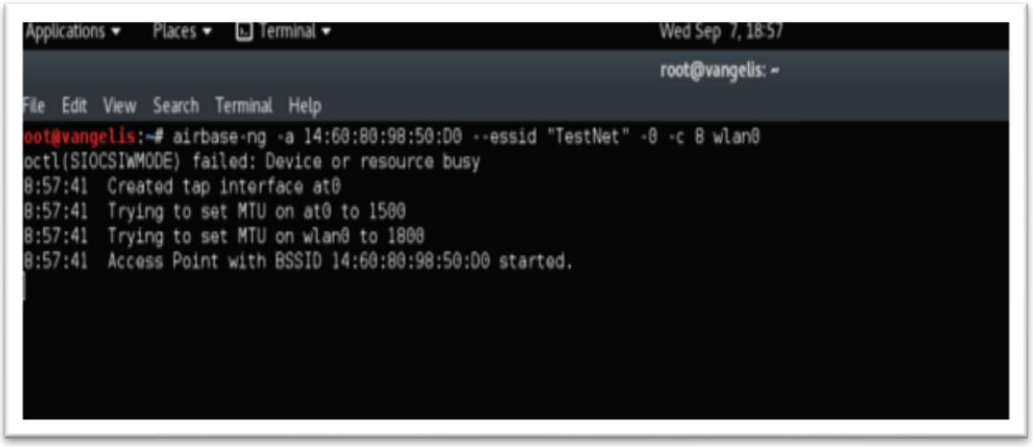
Εικόνα 5.13: Επιτυχία διαδικασίας Crack

Η διαδικασία τελείωσε με επιτυχία και ο κωδικός που βρέθηκε είναι ο **123mango**. Η διαδικασία έγινε με χρήση της GPU καθώς προσφέρει μεγαλύτερη επεξεργαστική ισχύ.

- **3η Επίθεση Evil Twin**

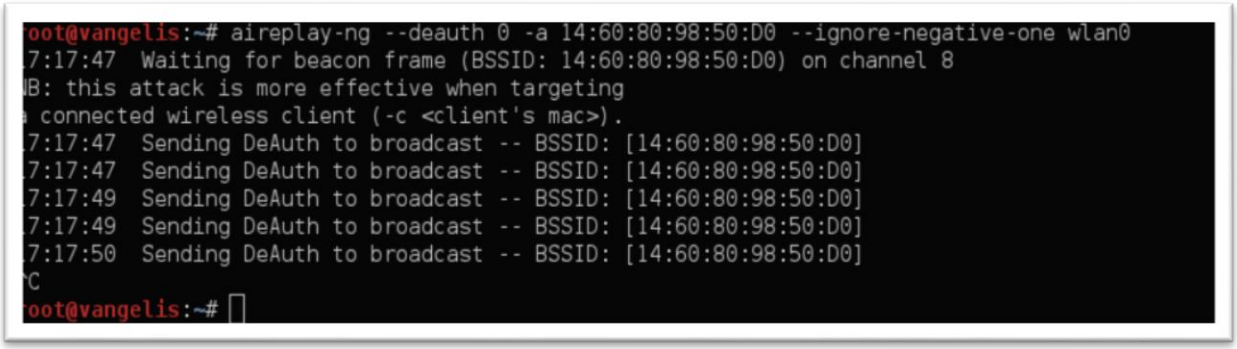
Στη τρίτη επίθεση θα γίνει προσπάθεια για δημιουργία κλώνου του δικτύου ώστε να μπορέσω να εξαπατήσω τους ασύρματα συνδεδεμένους χρήστες να συνδεθούν στο δικό μου δίκτυο και να μπορέσω να παρακολουθώ τις κινήσεις τους στο διαδίκτυο.

Η επίθεση ξεκινάει φτιάχνοντας τον κλώνο δίκτυο με τη βοήθεια με του airbase-ng.



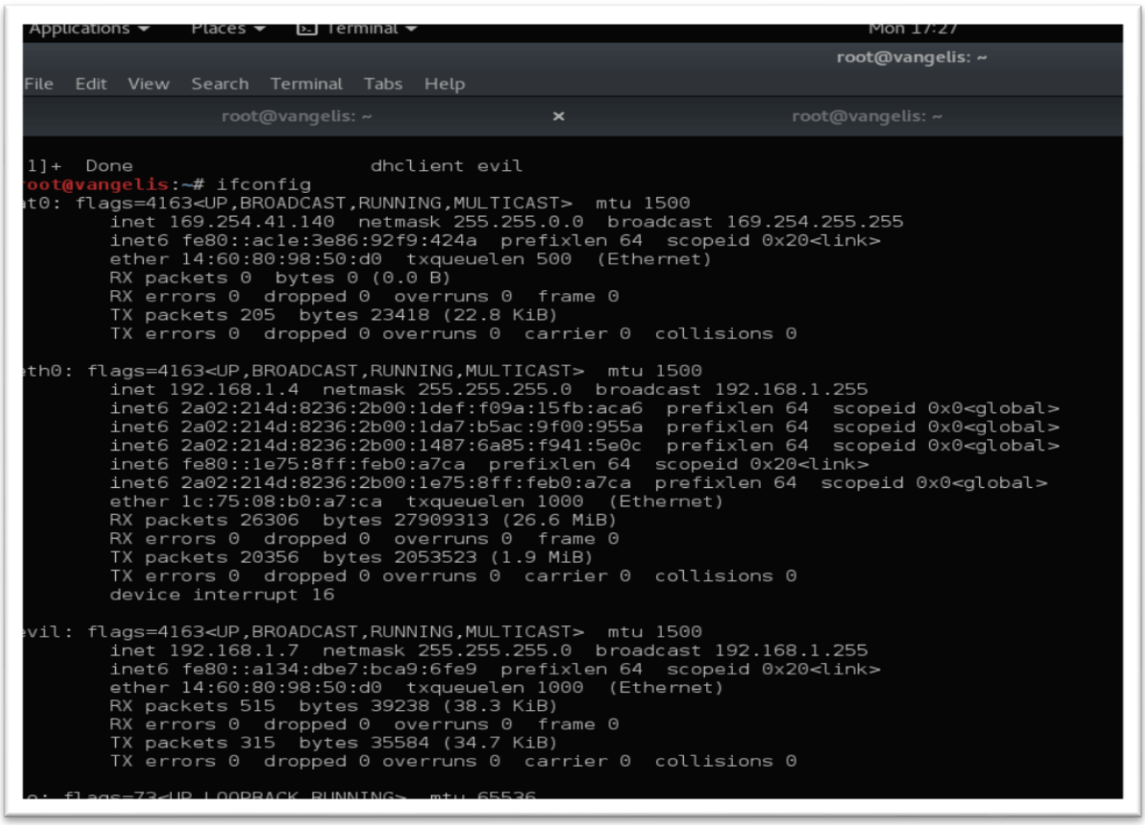
Εικόνα 5.14: Airbase-ng

Το επόμενο βήμα είναι η πραγματοποίηση μιας επίθεσης DeAuthorization στο AP ώστε να βγουν εκτός δικτύου οι χρήστες και να συνδεθούν στο κλώνο δίκτυο.

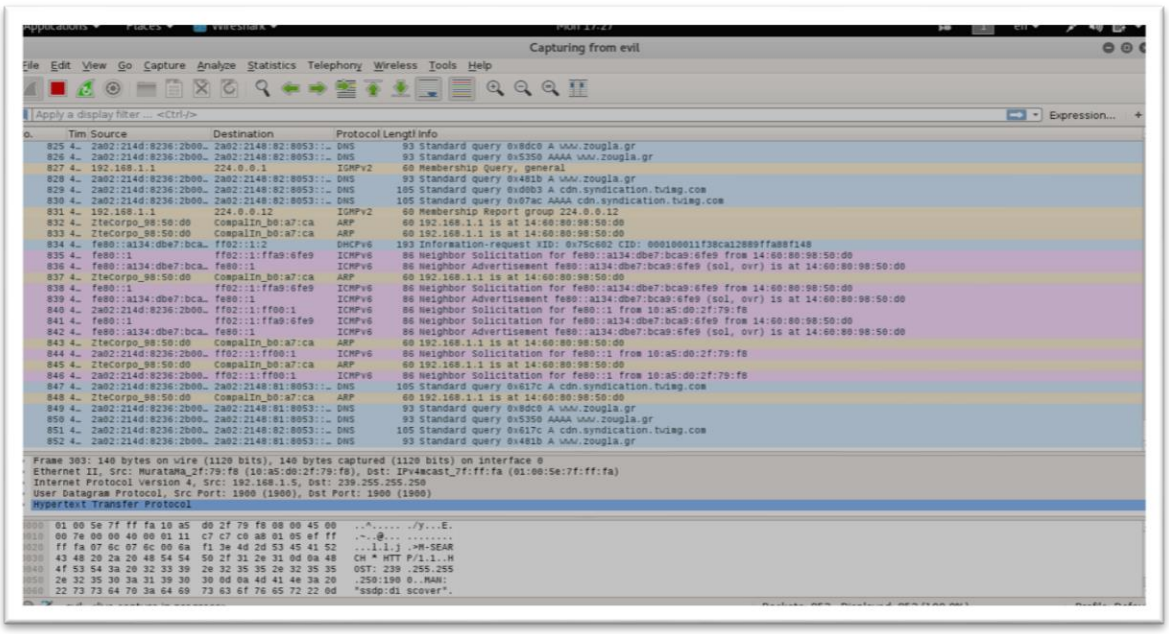


Εικόνα 5.15: Επίθεση DeAuthenticate

Οι συνδεμένοι χρήστες πλέον έχουν πρόσβαση μέσα από μια διεπαφή δικτύου την οποία δημιούργησα με το όνομα evil ώστε να γίνεται η καταγραφή των κινήσεών τους αποκλειστικά από αυτή.



Εικόνα 5.16: Διεπαφή Δικτύου Evil



Εικόνα 5.17: Κινήσεις χρηστών στο δίκτυο κλώνο

5.4 4η Φάση - Αναφορά Δοκιμής Διείσδυσης

Στη 4η φάση, η οποία είναι η τελευταία φάση της μεθοδολογίας της δοκιμής διείσδυσης θα φτιάξω μια αναφορά στην οποία βρίσκεται όλη η δουλειά η οποία έχει γίνει έτσι ώστε ο υπεύθυνος του συστήματος υπό έλεγχο να ξέρει όλες τις δοκιμές που έγιναν στο δίκτυό του. Μέσα σε αυτή την αναφορά υπάρχει πίνακας με όλα τα στοιχεία του εγγράφου, υπάρχει μια περίληψη στην οποία αναφέρεται συνοπτικά η δουλειά η οποία έχει γίνει πάνω στο δίκτυο δοκιμής, στη συνέχεια υπάρχει όλη η μεθοδολογία με την οποία έγινε αυτή η δοκιμή διείσδυσης με εξήγηση στη κάθε φάση και τέλος υπάρχουν τα αναλυτικά αποτελέσματα στα οποία υπάρχει πίνακας με όλες τις πληροφορίες οι οποίες συλλέχθηκαν στη 1η φάση, υπάρχουν επίσης όλες οι ευπάθειες οι οποίες βρέθηκαν αναφέροντας σε αυτές και το βαθμό ρίσκου που έχουν προς την επιχείρηση και τέλος υπάρχουν και όλες οι επιθέσεις οι οποίες έγιναν με σχολιασμό στη κάθε μια ξεχωριστά και με τρόπο αντιμετώπισης. Η δημιουργία μιας τέτοιας αναφοράς αποτελεί πάρα πολύ σημαντικό βήμα καθώς αποτελεί εγγύηση για τη δουλειά την οποία έχουμε κάνει. Επίσης είναι πολύ χρήσιμο για το υπεύθυνο του συστήματος υπό έλεγχο ώστε να έχει μια αναλυτική εικόνα της ασφάλειας του δικτύου του έτσι ώστε να μπορεί να βγάλει συμπεράσματα για τους κινδύνους τους οποίους διατρέχουν την επιχείρηση αλλά και να πάρει σημαντικές αποφάσεις για την εξέλιξη της ασφάλειας στο δίκτυο του.

5.4.1 Παράδειγμα Αναφοράς

ΑΝΑΦΟΡΑ ΔΟΚΙΜΗΣ ΔΙΕΙΣΔΥΣΗΣ ΣΕ ΑΣΥΡΜΑΤΟ ΔΙΚΤΥΟ ΔΕΔΟΜΕΝΩΝ

Black Box Penetration Test

Για: «την επιχείρηση στην οποία γίνεται το Penetration Testing»

V 1.0

20 Ιουλίου 2016

Από: Κατσαδούρος Δ. Ευάγγελος

Στοιχεία Εγγράφου

Πίνακας 5.2: Στοιχεία εγγράφου

Τίτλος	Αναφορά Δοκιμής Διείσδυσης σε Ασύρματο Δίκτυο Δεδομένων
Έκδοση	1.0
Συγγραφέας	Κατσαδούρος Δ. Ευάγγελος
Εκτελεστές Δοκιμής	Κατσαδούρος Δ. Ευάγγελος
Ελέγχθηκε από	« Όνομα Υπευθύνου Ελέγχου»
Εγκρίθηκε από	« Όνομα Υπευθύνου Έγκρισης»
Κατάταξη	Απόρρητο

Πίνακας Έκδοσης

Πίνακας 5.3: Πίνακας Έκδοσης

Έκδοση	Ημερομηνία	Συγγραφέας	Περιγραφή
1.0	20/7/2016	Κατσαδούρος Δ. Ευάγγελος	Τελική Έκδοση

1. ΠΕΡΙΛΗΨΗ

Σκοπός του εγγράφου αυτού είναι η παρουσίαση της δουλειάς που έγινε κατά την εκτέλεση της Δοκιμής Διείσδυσης. Όλη η δοκιμή έγινε υπό τους όρους τους οποίους συμφωνήθηκαν κατά τη φάση του σχεδιασμού. Όλη η δοκιμή εκτελέστηκε με απόλυτη επιτυχία στο ασύρματο δίκτυο δεδομένων **TestNet.** Η εκτέλεση της δοκιμής έγινε στο διάστημα **5 Ιουλίου 2016** μέχρι **18 Ιουλίου 2016.** Κατά την εκτέλεση της δοκιμής έγινε συλλογή πληροφοριών πάνω στο δίκτυο **TestNet** και εκτελέστηκαν επιθέσεις για την αξιολόγηση της ασφάλειας του δικτύου αλλά και την εύρεση ευπαθειών σε αυτό.

2. ΜΕΘΟΔΟΛΟΓΙΑ

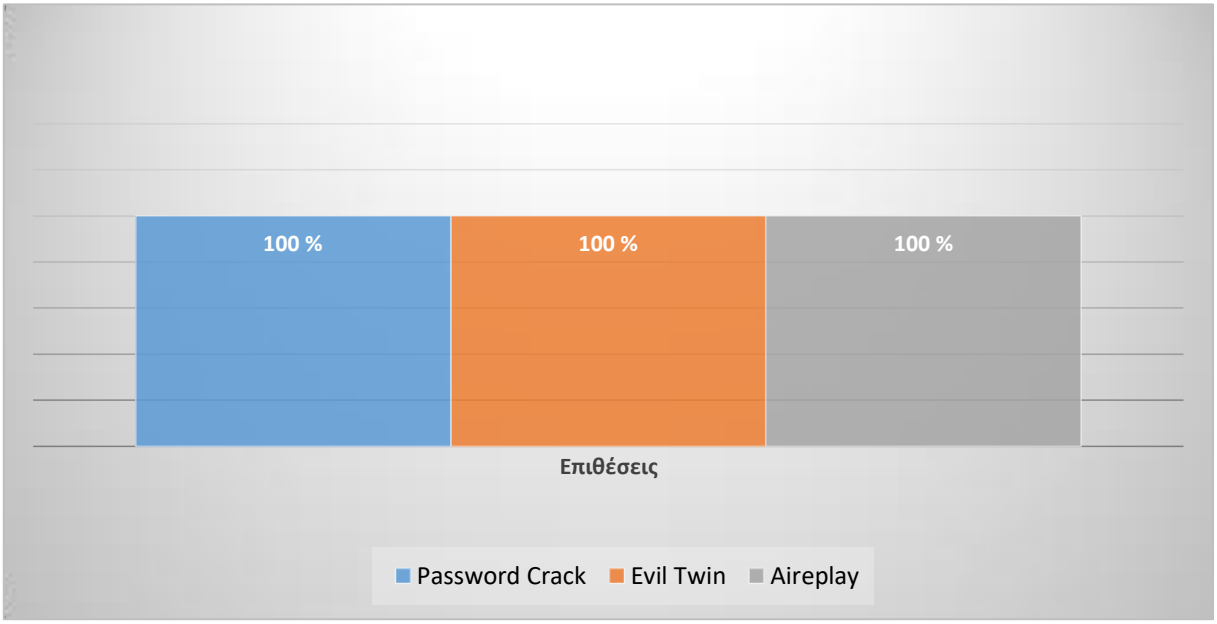
Η μεθοδολογία αυτής της δοκιμής έγινε σε τέσσερις φάσεις η οποίες είναι με τη σειρά οι Σχεδιασμός, Ανίχνευση, Επίθεση και Αναφορά.

1η Φάση - Σχεδιασμός: Σε αυτή τη φάση έγιναν όλες οι απαραίτητες συζητήσεις με τον υπεύθυνο του συστήματος υπό έλεγχο προκειμένου να διευκρινιστούν τα δικαιώματα αυτής της δοκιμής, το πιθανό χρονοδιάγραμμα της δοκιμής αλλά και οι τομείς οι οποίοι θα δοκιμαστούν. Τέλος σε αυτή τη φάση δόθηκαν όλες οι απαραίτητες πληροφορίες για τη δοκιμή αυτή όπως το όνομα του δικτύου στο οποίο έγινε η δοκιμή.

2η Φάση - Ανίχνευση: Σε αυτή τη φάση χρησιμοποιήθηκαν τεχνικές και εργαλεία προκειμένου να γίνει συλλογή πληροφοριών για το δίκτυο προς δοκιμή. Συλλέχθηκαν πληροφορίες για την ασφάλεια του δικτύου αλλά και τεχνικές πληροφορίες αυτού οι οποίες ήταν χρήσιμες για την επόμενη φάση.

3η Φάση - Επίθεση: Σε αυτή τη φάση πραγματοποιήσαμε κάποιες επιθέσεις με βάση της πληροφορίες που συλλέξαμε στο δεύτερο βήμα, προκειμένου να βγάλουμε συμπεράσματα για την ασφάλεια του δικτύου και για να κάνουμε στη συνέχεια μια ανάλυση των ρίσκων στο δίκτυο αυτό. Σε αυτή τη φάση πραγματοποιήθηκαν οι επιθέσεις DeAuthorization, Password Crack και Evil Twin. Και οι τρεις επιθέσεις πραγματοποιήθηκαν με επιτυχία.

Πίνακας 5.4: Ποσοστά επιτυχίας επιθέσεων



4η Φάση - Αναφορά: Στη 4η φάση πραγματοποιήθηκε ανάλυση των ρίσκων και των ευπαθειών και παρουσιάζουμε τα συμπεράσματα της δοκιμής αυτής και όλη τη δουλειά την οποία έχουμε κάνει. Η ανάλυση των ρίσκων έγινε σύμφωνα με το Nist SP 800-30 και ο υπολογισμός γίνεται με βάση τη πιθανότητα και την επίπτωση.

3. ΑΝΑΛΥΤΙΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ ΔΟΚΙΜΗΣ ΔΙΥΣΔΕΙΣΗΣ

Σε αυτό το κεφάλαιο παρουσιάζονται αναλυτικά τα αποτελέσματα των επιθέσεων και τρόποι αντιμετώπισης αυτών, οι ευπάθειες οι οποίες βρέθηκαν με περιγραφή, ανάλυση ρίσκου αυτής για την επιχείρηση και τρόποι αντιμετώπισης.

ΠΛΗΡΟΦΟΡΙΕΣ ΔΙΚΤΥΟΥ

Πίνακας 5.5: Πληροφορίες Δικτύου

Τύπος Δικτύου	Δίκτυο	Πληροφορίες Δικτύου
Ασύρματο Δίκτυο Δεδομένων Wlan	**TestNet**	**BSSID** 14:60:80:98:50:D0
		PWR -63
		Beacon 172
		Data 0
		S 0
		Channel 8
		MB 54e
		Encryption WPA
		Cipher

		TKIP
		Authenticate PSK
		ESSID TestNet

ΕΥΠΑΘΕΙΕΣ

- **ΚΩΔΙΚΟΣ ΠΡΟΣΒΑΣΗΣ**

  Rating: Hight

  Περιγραφή: Ο κωδικός με τον οποίο μπορεί να αποκτήσει κάποιος χρήστης πρόσβαση στο ασύρματο δίκτυο είναι αρκετά ανίσχυρος. Επίσης ο κωδικός αυτός υπάρχει σε αρκετές wordlist.

  Επίπτωση: Οι επιπτώσεις αυτής της ευπάθειας είναι το εύκολο σπάσιμο του κωδικού από hackers με Password Attacks(Brute Force, Dictionary) που έχει ως αποτέλεσμα μια αθέμιτη πρόσβαση στο ασύρματο δίκτυο η οποία μπορεί να οδηγήσει σε άλλες επιθέσεις.

  Τρόπος αντιμετώπισης: Για την αντιμετώπιση αυτής της ευπάθειας θα μπορούσε να αλλαχθεί ο κωδικός με έναν πιο ισχυρό. Γενικά ένας ισχυρός κωδικός θα πρέπει να είναι από 16 ψηφία και πάνω και να περιλαμβάνει γράμματα κεφαλαία και μικρά, αριθμούς και σύμβολα. Σε καμία περίπτωση μέσα στο κωδικό δε πρέπει να υπάρχουν λέξεις τις οποίους βρίσκουμε στο λεξικό. Επίσης θα ενίσχυε την ασφάλεια του δικτύου η συχνή αλλαγή του κωδικού.

- **ΑΣΦΑΛΕΙΑ WPA**

  Rating: Moderate

Περιγραφή: Η ασφάλεια WPA είναι ο τρόπος με τον κωδικοποιείται ο κωδικός πρόσβασης κατά τη μεταφορά από το χρήστη στο AP. Η τεχνολογία WPA θεωρείται πλέον ξεπερασμένη και μπορεί να προσπελασθεί.

Επίπτωση: Η συγκεκριμένη ευπάθεια μπορεί να αξιοποιηθεί από κάποιο hacker και να ¨σπάσει¨ το κωδικό πρόσβασης του ασύρματου δικτύου μας. Η πρόσβαση ενός hacker στο δίκτυο μας μπορεί να οδηγήσει σε άλλες επιθέσεις.

Τρόπος αντιμετώπισης: Για την αντιμετώπιση της ευπάθειας αυτής, θα πρέπει στις ρυθμίσεις ασφάλειας του wlan να αλλάξουμε την ασφάλεια σε WPA2 η οποίο είναι η πιο σύγχρονη και ισχυρή ασφάλεια.

- **ΥΨΗΛΗ ΙΣΧΥ ΣΗΜΑΤΟΣ**

Rating: Low

Περιγραφή: Η ισχύς του σήματος ορίζει το εύρος στο οποίο μπορεί να είναι ορατό το ασύρματο δίκτυο.

Επίπτωση: Η υψηλή ισχύ σήματος μπορεί να κάνω ορατό το ασύρματο δίκτυο σε χρήστες στους οποίους δε θέλουμε. Τέτοιοι χρήστες μπορεί να είναι και οι hackers οι οποίοι μπορούν να το εκμεταλλευτούν και να πραγματοποιήσουν διάφορες επιθέσεις(DeAuthorization Attacks, Evil Twin κ.α).

Τρόπος αντιμετώπισης: Γίνεται να χαμηλώσουμε την ισχύ του σήματος από τις ρυθμίσεις του AP.

ΕΠΙΘΕΣΕΙΣ

- **DeAuthorization Attack**

Περιγραφή Επίθεσης: Στην επίθεση μη πιστοποιημένων πακέτων ο επιτιθέμενος αρχίζει να στέλνει μη πιστοποιημένα πακέτα με τη mac διεύθυνση ενός χρήστη που είναι συνδεδεμένος στο δίκτυο. Ο επιτιθέμενος μπορεί να κρατήσει για όση ώρα θέλει εκτός δικτύου το θύμα στέλνοντας μη πιστοποιημένα πακέτα. Μπορεί να το κάνει αυτό και για όλους τους χρήστες του δικτύου προκαλώντας με αυτό τον τρόπο άρνηση υπηρεσιών.

Αποτέλεσμα: Η δοκιμή αυτή ολοκληρώθηκε με επιτυχία. Έκανα επίθεση μη πιστοποιημένων πακέτων στο δίκτυο βγάζοντας εκτός δικτύου όλους τους συνδεδεμένους χρήστες.

Τρόπος Αντιμετώπισης: Δεν υπάρχει τρόπος αντιμετώπισης αυτής της επίθεσης καθώς τα μη πιστοποιημένα πακέτα είναι μέρος της λειτουργίας των AP. Μπορούμε όμως χαμηλώνοντας την ισχύ του σήματος του AP να δυσκολέψουμε τη πραγματοποίηση των επιθέσεων αυτών.

- **Evil Twin Attack**

Περιγραφή Επίθεσης: Στην επίθεση Evil Twin ο επιτιθέμενος προσπαθεί να δημιουργήσει ένα δίκτυο ίδιο με αυτό του θύματος. Αυτό γίνεται δίνοντας στο δίκτυο κλώνο ίδιο ssid, mac διεύθυνση, και τύπο ασφάλειας. Μόλις ο επιτιθέμενος καταφέρει να δημιουργήσει το δίκτυο κλώνο πραγματοποιεί άρνηση υπηρεσιών στο δίκτυο. Μόλις επιτευχθεί η άρνηση υπηρεσιών θέτει σε λειτουργία το δίκτυο κλώνο, το οποίο έχει ως αποτέλεσμα όλοι οι χρήστες οι οποίοι ήταν συνδεδεμένοι στο δίκτυο του θύματος να συνδεθούν στο δίκτυο του επιτιθέμενου, χωρίς να το καταλάβουν με τον επιτιθέμενο να μπορεί να παρακολουθήσει τη κίνηση στο δίκτυο, να χειραγωγήσει τα πακέτα που φεύγουν από τους χρήστες και να υποκλέψει χρήσιμες πληροφορίες.

Αποτέλεσμα: Η συγκεκριμένη επίθεση ολοκληρώθηκε με επιτυχία. Αφού κλωνοποιήσαμε το δίκτυο TestNet, στη συνέχεια το βγάλαμε εκτός υπηρεσιών με επίθεση μη πιστοποιημένων πακέτων. Μόλις το δίκτυο τέθηκε εκτός υπηρεσιών βάλαμε σε λειτουργία το δίκτυο κλώνο πάνω στο οποίο συνδέθηκαν όλοι οι χρήστες. Με χρήση του Wireshark επιβεβαιώσαμε τις κινήσεις τους στο δίκτυο κλώνο.

Τρόπος Αντιμετώπισης: Η επίθεση Evil Twin θεωρείται επίθεση δύσκολα αντιμετωπίσιμη. Υπάρχουν όμως τρόποι για να περιοριστεί ή για να την αντιμετωπίσουμε. Μια λύση είναι η ενημέρωση των χρηστών ότι σε περίπτωση περίεργης συμπεριφοράς του δικτύου να αποσυνδέονται. Μια τέτοια περίεργη συμπεριφορά είναι η αποσύνδεση και επανασύνδεση στο δίκτυο. Η ισχύς σήματος είναι μια ακόμα λύση. Η μείωση της ισχύς τους σήματος ώστε να πιάνει μόνο στο χώρο τον οποίο θέλουμε αποτρέπει κακόβουλους χρήστες εκτός του

χώρου να πραγματοποιήσουν επίθεση Evil Twin. Τέλος η χρήση VPN σύνδεσης για όλο το δίκτυο προσφέρει ισχυρή ασφάλεια με ισχυρή πιστοποίηση, με αποτέλεσμα να δυσκολεύει αρκετά τη πραγματοποίηση μιας Evil Twin Επίθεσης.

- **WPA Password Crack**

Περιγραφή Επίθεσης: Στη συγκεκριμένη επίθεση ο επιτιθέμενος προσπαθεί να σπάσει το κωδικό πρόσβασης ο οποίος βασίζεται πάνω σε ασφάλεια WPA. Αυτό το καταφέρνει καταγράφοντας τα wlan πακέτα του δικτύου στόχου. Παράλληλα με τη καταγραφή των πακέτων πραγματοποιεί σε κάποιον συνδεδεμένο χρήστη επίθεση μη πιστοποιημένων πακέτων με σκοπό να τον αποσυνδέσει και μόλις σταματήσει την επίθεση να ξανασυνδεθεί. Όταν ξανασυνδεθεί το πρόγραμμα καταγραφής πιάνει το πακέτο χειραψίας (handshake) το οποίο περιέχει το κωδικό πρόσβασης κρυπτογραφημένο. Στη συνέχεια παίρνει το hash από αυτό το πακέτο και το συγκρίνει με μια μεγάλη λίστα πιθανών κωδικών οι οποίοι κρυπτογραφούνται με τα κλειδιά του δικτύου με αποτέλεσμα να πέσει στο κωδικό που έχει το δίκτυο.

Αποτέλεσμα: Η δοκιμή αυτής της επίθεσης ολοκληρώθηκε με επιτυχία καταφέρνοντας να βρούμε τον κωδικό πρόσβασης του ασύρματου δικτύου Test-Net.

Τρόποι Αντιμετώπισης: Για να αντιμετωπισθούν αυτές οι επιθέσεις προτείνω την εφαρμογή των πιο πρόσφατων μεθόδων ασφάλειας. Η πιο πρόσφατη είναι η WPA2. Επίσης η χρήση ισχυρών κωδικών πρόσβασης είναι υποχρεωτική. Ένας ισχυρός κωδικός πρόσβασης χαρακτηρίζεται από το μήκος του και τη πολυπλοκότητα του σε χαρακτήρες. Επομένως ένας ισχυρός κωδικός περιλάμβανει πάνω από 16 χαρακτήρες οι οποίοι πρέπει να είναι γράμματα, πεζά και κεφαλαία, αριθμοί και σύμβολα. Τέλος σαν όνομα δικτύου (SSID) θα πρέπει να χρησιμοποιείται κάποιο το οποίο θα είναι σπάνιο και όχι κάποιο κοινό SSID (myhome, business κλπ), καθώς η κρυπτογράφηση του κωδικού στις ασφάλειες WPA και WPA2 βασίζεται και στο SSID.

ΣΥΝΟΛΙΚΟ ΡΙΣΚΟ

Το συνολικό ρίσκο που υπολογίστηκε με βάση τα αποτελέσματα αυτής της δοκιμής διείσδυσης είναι Moderate.

ΕΠΙΛΟΓΟΣ

Η παρούσα δοκιμή διείσδυσης εκτελέστηκε για την «την επιχείρηση στην οποία γίνεται το Penetration Testing» με απόλυτη επιτυχία. Η δοκιμή διείσδυσης πραγματοποιήθηκε πάνω στο ασύρματο δίκτυο δεδομένων TestNet. Στόχος αυτής της δοκιμής διείσδυσης ήταν

- Η ανακάλυψη των ευπαθειών του ασυρμάτου δικτύου
- Να δοκιμαστεί σε συγκεκριμένες επιθέσεις και
- Η συνολική αξιολόγηση της ασφάλειας του.

Όλοι οι παραπάνω στόχοι πραγματοποιήθηκαν με επιτυχία με αποτέλεσμα την ανακάλυψη αρκετών θεμάτων ασφάλειας του δικτύου τα οποία απαιτούν άμεση αντιμετώπιση. Για κάθε ευπάθεια και κενό ασφάλειας που ανακαλύφθηκε υπάρχει αναλυτική περιγραφή αλλά και πιθανοί τρόποι αντιμετώπισης αυτών. Η δοκιμή διείσδυσης πραγματοποιήθηκε τηρώντας όλους τους όρους που συμφωνήθηκαν, τηρώντας πιστά το χρονοδιάγραμμα το οποίο συμφωνήθηκε.

6 Επίλογος

Στη παρούσα πτυχιακή ασχολήθηκα με τη Δοκιμή Διείσδυσης σε Ασύρματα Δίκτυα Δεδομένων, παρουσιάζοντας ασύρματες τεχνολογίες δικτύωσης Wlan, Wpan και ZWave. Επίσης παρουσίασα διάφορα θέματα που έχουν να κάνουν με την ασφάλεια στις ασύρματες τεχνολογίες δικτύωσης και την διαδικασία που χρειάζεται για την επίτευξη μιας πετυχημένης δοκιμής διείσδυσης.

Μέσα από την έρευνα που έκανα κατά την εγγραφή της πτυχιακής μου έβγαλα χρήσιμα συμπεράσματα για την ασφάλεια στις ασύρματες τεχνολογίες δικτύωσης. Τα συμπεράσματα αυτά είναι:

- Δεν υπάρχει απόλυτη ασφάλεια στα δίκτυα. Οι επιθέσεις αυξάνονται καθημερινά με μεγάλο ρυθμό, όπως και οι hackers οι οποίοι μπορεί να είναι επαγγελματίες ή ερασιτέχνες. Αυτοί οι λόγοι είναι που καθιστούν την ασφάλεια των ασύρματων τεχνολογιών δικτύωσης αβέβαιη απέναντι στους κινδύνους που υπάρχουν. Για να καταλάβουμε το μέγεθος των κινδύνων αυτών αρκεί να δούμε τις δυνατότητες που προσφέρουν τα ελεύθερα λογισμικά επιθέσεων που υπάρχουν στο διαδίκτυο. Μπορούν με πληκτρολόγηση μιας εντολής να σπάσουν κωδικούς ασφαλείας, να βγάλουν τα δίκτυα εκτός υπηρεσιών και να καταργήσουν ασφάλεια η οποία μπορεί να υπάρχει σε αυτά. Επίσης συμπέρανα ατά τη διάρκεια εγγραφής της πτυχιακής μου ότι το κόστος για τη συνεχή παρακολούθηση της ασφάλειας ασυρμάτων δικτύων είναι πολύ μικρό μπροστά στο κόστος πραγματοποίησης μιας επίθεσης. Η ζημιά που μπορεί να προκληθεί από κάποιες επιθέσεις είναι πολύ μεγάλη και πολλές φορές μη αναστρέψιμη Όλοι αυτοί οι λόγοι καθιστούν επιτακτική την ανάγκη για συνεχή παρακολούθηση της ασφάλειας των δικτύων κάνοντας δοκιμές διείσδυσης ανά τακτικά χρονικά διαστήματα.
- Το δεύτερο συμπέρασμα έχει να κάνει με την αξιοποίηση νέων τεχνολογιών ασύρματης δικτύωσης. Οι τεχνολογίες Wi-Fi και Bluetooth έχουν μελετηθεί πάρα πολύ με αποτέλεσμα να υπάρχουν πάρα πολλές επιθέσεις και μάλιστα από άτομα που δεν είναι άριστοι γνώστες του τομέα αυτού, αλλά με τη χρήση αυτοματοποιημένων εργαλείων που υπάρχουν διαθέσιμα στο διαδίκτυο, μπορούν να κάνουν ζημιά. Κατά τη διάρκεια των δοκιμών που έκανα η

αναζήτηση εργαλείων για επιθέσεις σε δίκτυα Wi-Fi και Bluetooth ήταν πάρα πολύ εύκολη καθώς υπάρχουν αρκετά ελεύθερα λογισμικά. Επίσης το μόνο που χρειάζεσαι είναι ένας φορητός υπολογιστής ο οποίος έχει ενσωματωμένη κεραία για Wi-Fi και Bluetooth. Ως αποτέλεσμα η ευκολία για πραγματοποίηση επιθέσεων σε αυτά τα δίκτυα ήταν πάρα πολύ μεγάλη και χωρίς κανένα εμπόδιο. Για την τεχνολογία ZWave η υπόθεση Επίθεση, δεν ήταν τόσο εύκολη. Το πρώτο εμπόδιο για την πραγματοποίηση επίθεσης σε ένα δίκτυο Zwave ήταν η έλλειψη λογισμικών που να πραγματοποιούν επιθέσεις. Το σημαντικότερο εμπόδιο όμως ήταν η ανάγκη για ειδικό υλικό εξοπλισμό. Οι φορητοί υπολογιστές οι οποίοι έχουμε δεν διαθέτουν κεραία για ZWave δίκτυα. Αυτό έχει σαν αποτέλεσμα την ανάγκη για αγορά ειδικού εξοπλισμού ο οποίος ονομάζεται Software Defined Radio (SDR). Το SDR είναι μια συσκευή με την οποία μπορείς να λάβεις και να αναλύσεις πακέτα Zwave αλλά και να στείλεις, με χρήση του κατάλληλου λογισμικού. Το κόστος αυτών των συσκευών όμως κυμαίνεται από 500 έως 2000 ευρώ με αποτέλεσμα να είναι δύσκολη η αγορά του. Αυτό βέβαια αυξάνει την ασφάλεια αυτής της τεχνολογίας καθώς η ανάγκη για χρήση ειδικού υλικού εξοπλισμού του οποίο το κόστος είναι υψηλό σε συνδυασμό με την έλλειψη λογισμικού για επιθέσεις μειώνει αρκετά το ποσοστό των hackers που θα προσπαθούσαν να χτυπήσουν τέτοια δίκτυα. Επομένως πρέπει να γίνει χρήση νέων τεχνολογιών ασύρματης δικτύωσης όπως η ZWave οι οποίες δεν είναι τόσο μελετημένες με αποτέλεσμα να κρύβουν λιγότερους κινδύνους σε σχέση με ήδη υπάρχουσες τεχνολογίες (Wi-Fi, Bluetooth) οι οποίες πλέον κρύβουν πάρα πολλούς κινδύνους.

Με τον συνεχή έλεγχο της ασφάλειας των δικτύων κάνοντας δοκιμές διείσδυσης μπορούν τα κρούσματα τον επιθέσεων να μειωθούν αρκετά στο μέλλον και οι τεράστιες οικονομικές ζημιές επιχειρήσεων από hackers να ελαττωθούν. Ο τομέας της ασφάλειας Ο τομέας της ασφάλειας των δικτύων αποτελεί εγγύηση για το κλάδο των επιχειρήσεων και γενικότερα για τα κόσμο!

Βιβλιογραφία

[1] Βικιπαιδεία, IEEE 802.11 [online], Διαθέσιμο εδώ: < https://el.wikipedia.org/wiki/IEEE_802.11 >

[2] The Economist, 2004. A brief history of Wi-Fi [online], Διαθέσιμο εδώ: < http://www.economist.com/node/2724397 >

[3] Andrew S. Tanenbaum, David J. Wetherall, ¨ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ, ΠΕΜΠΤΗ ΑΜΕΡΙΚΑΝΙΚΗ ΕΚΔΟΣΗ¨, KLIDARITHMOS PUBLICATIONS EPE, 2011

[4] Wikipedia, Wi-Fi Protected Access [online], Διαθέσιμο εδώ: < https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access >

[5] Wikipedia, Temporal Key Integrity Protocol [online], Διαθέσιμο εδώ: < https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol >

[6] Wikipedia, CCMP [online], Διαθέσιμο εδώ: < https://en.wikipedia.org/wiki/CCMP >

[7] Βικιπαιδεία, Bluetooth [online], Διαθέσιμο εδώ: < https://el.wikipedia.org/wiki/Bluetooth >

[8] Wikipedia, List of Bluetooth protocols [online], Διαθέσιμο εδώ: < https://en.wikipedia.org/wiki/List_of_Bluetooth_protocols >

[9] ΑΡΤΕΜΙΟΣ Γ. ΒΟΓΙΑΤΖΗΣ, ΔΗΜΗΤΡΙΟΣ Ν. ΣΕΡΠΑΝΟΣ, 2005. ΑΝΑΛΥΣΗ ΑΣΦΑΛΕΙΑΣ ΕΠΙΠΕΔΟΥ ΣΥΝΔΕΣΗΣ ΔΕΔΟΜΕΝΩΝ ΓΙΑ ΔΙΚΤΥΑ ΤΕΧΝΟΛΟΓΙΑΣ BLUETOOTH [online], Διαθέσιμο εδώ: < http://portal.tee.gr/portal/page/portal/PUBLICATIONS/BYMONTHLY_PUBLICATIONS/diminiaia_2005/proto_tefhos/bluetooth.pdf >

[10] Tom Olzak, 2006. Secure your Bluetooth wireless networks and protect your data [online], Διαθέσιμο εδώ: < http://www.techrepublic.com/article/secure-your-bluetooth-wireless-networks-and-protect-your-data/ >

[11] John Padgette, Karen Scarfone, Lily Chen, 2012. Guide to Bluetooth Security [online], Διαθέσιμο εδώ: < http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-121r1.pdf >

[12] Mikhail T. Galeev, 2006. Catching the Z-Wave [online], Διαθέσιμο εδώ: < http://www.drdobbs.com/embedded-systems/catching-the-z-wave/193104353 >

[13] JFR, 2006. Z-Wave Protocol Overview [online], Διαθέσιμο εδώ: < https://wiki.ase.tut.fi/courseWiki/images/9/94/SDS10243_2_Z_Wave_Protocol_Overview.pdf >

[14] GrayHat4Life, 2015. 7 Types of Hackers You Should Know [online], Διαθέσιμο εδώ: < https://www.cybrary.it/0p3n/types-of-hackers/ >

[15] Jennifer Cowan, 2014. Majority of Hackers Do it for the Thrill, Believe They Won't Be Caught: Survey [online], Διαθέσιμο εδώ: < http://www.sitepronews.com/2014/08/14/majority-hackers-thrill-believe-wont-caught-survey/ >

[16] Carlos A. Soto, 2005. A menu of Bluetooth attacks [online], Διαθέσιμο εδώ: < https://gcn.com/articles/2005/07/20/a-menu-of-bluetooth-attacks.aspx >

[17] Manish S. Saindane, PENETRATION TESTING – A SYSTEMATIC APPROACH [online], Διαθέσιμο εδώ: < http://www.infosecwriters.com/text_resources/pdf/PenTest_MSaindane.pdf >

[18] tutorialspoint, Types of Penetration Testing [online], Διαθέσιμο εδώ: < http://www.tutorialspoint.com/penetration_testing/types_of_penetration_testing.htm >

[19] installCore, 2015. The History of Ethical Hacking and Penetration Testing [online], Διαθέσιμο εδώ: < http://www.slideshare.net/installCore/install-core-history-of-ethical-hacking-and-penetration-testing >

[20] Volimer, 2010. Types of Hackers (part 2/2) [online], Διαθέσιμο εδώ: < http://el.urbandictionary.com/define.php?term=Types%20of%20Hackers >

[21] Volimer, 2010. Types of Hackers (Part 1) [online], Διαθέσιμο εδώ: < http://el.urbandictionary.com/define.php?term=Types%20of%20Hackers&defid=4542209 >

[22] Hanso, 2015. WLAN MANUALLY [online], Διαθέσιμο εδώ: < http://duinorasp.hansotten.com/wlan-manually/ >

[23] Andy Ross, MAKE YOUR TABLETS AND SMART PHONES SMARTER - ADD SERIAL [online], Διαθέσιμο εδώ: < http://www.bb-elec.com/Learning-

Center/All-White-Papers/Serial/%E2%80%A2-Make-Your-Tablets-and-Smart-Phones-Smarter-Add-S.aspx >

[24] Learncisco, Understanding WLAN Security [online], Διαθέσιμο εδώ: < http://www.learncisco.net/courses/icnd-1/wireless-lans/wlan-security.html >

[25] Marcel Holtmann, Christoph Wegener, What your phone vendor didn't tell you about Bluetooth security [online], Διαθέσιμο εδώ: < https://nnc3.com/mags/LM10/Magazine/Archive/2007/80/022-026_BlueSecurity/article.html >

[26] Andrew Tanenbaum, David Wetherall, 2011. Computer Networks, Fifth Edition [online], Διαθέσιμο εδώ: < http://slideplayer.com/slide/7840942/ >

[27] Tom Olzak, 2006. Secure your Bluetooth wireless networks and protect your data [online], Διαθέσιμο εδώ: < https://en.wikipedia.org/wiki/File:Bluetooth_piconet_diagram.svg >

[28] Victor Yee, 2008. Bluetooth Vulnerabilities [online], Διαθέσιμο εδώ: < https://www.slideshare.net/VictorYee/bluetooth-vulnerbilities >

[29] Mikhail T. Galeev, 2006. Catching the Z-Wave [online], Διαθέσιμο εδώ: < http://www.embedded.com/design/connectivity/4025721/Catching-the-Z-Wave >

[30] Mikhail T. Galeev , 2006. Catching the Z-Wave [online], Διαθέσιμο εδώ: < http://www.embedded.com/design/connectivity/4025721/Catching-the-Z-Wave >

[31] Jennifer Cowan, 2014. Majority of Hackers Do it for the Thrill, Believe They Won't Be Caught: Survey [online], Διαθέσιμο εδώ: < http://www.sitepronews.com/2014/08/14/majority-hackers-thrill-believe-wont-caught-survey/ >

[32] Aliya Sternstein, 2015. US MILITARY CYBERSECURITY BY THE NUMBERS [online], Διαθέσιμο εδώ: < http://www.nextgov.com/media/ckeditoruploads/2015/03/17/CyberSpendingNG.png >

[33] Guru99, Penetration Testing Tutorial: Learn Manual & Automated Types PenTest [online], Διαθέσιμο εδώ: < http://www.guru99.com/learn-penetration-testing.html >

[34] tutorialspoint, Types of Penetration Testing [online], Διαθέσιμο εδώ: < https://www.tutorialspoint.com/penetration_testing/types_of_penetration_testing.htm >

[35] Darril, Black Box Testing and More [online], Διαθέσιμο εδώ: < http://blogs.getcertifiedgetahead.com/black-box-testing-and-more/ >