ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

Πτυχιακή Εργασία

«ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ»

της φοιτήτριας

Σερέφα Ευαγγελίας-Δήμητρας

Α.Μ.11671

Επιβλέπων: Στεργίου Ελευθέριου

ΑΡΤΑ 2016

ΕΥΧΑΡΙΣΤΙΕΣ

Επιθυμώ να εκφράσω όλο μου το σεβασμό και την ευγνωμοσύνη στον επιβλέποντα καθηγητή μου κ.Στεργίου Ελευθέριο, ο οποίος με εμπιστεύθηκε και με καθοδήγησε καθ' όλη τη διάρκεια εκπόνησης της πτυχιακής μου εργασίας. Επίσης θα ήθελα να ευχαριστήσω όλους τους καθηγητές του τμήματος Μηχανικών Πληροφορικής Τ.Ε. , για τις γνώσεις που μου παρείχαν όλα τα χρόνια της φοίτησης μου. Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου για την αμέριστη συμπαράσταση και ηθική στήριξη που μου πρόσφερε όλα αυτά τα χρόνια.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Στην παρούσα πτυχιακή εργασία γίνεται μια παρουσίαση των μεθόδων που χρησιμοποιούνται για την ασφάλεια των δεδομένων στα ασύρματα δίκτυα και συνεπώς και στις κινητές επικοινωνίες, αναφέρονται προβλήματα ασφάλειας που αντιμετωπίζουν και απειλές που μπορεί να βλάψουν το δίκτυο. Παρουσιάζονται τεχνολογίες ασφάλειας που χρησιμοποιούνται ως άμυνα σε τυχόν επιθέσεις.

Στο πρώτο κεφάλαιο ,αρχικά, αναφέρονται κάποιες γενικές και ιστορικές πληροφορίες σε σχέση με τα δίκτυα. Στη συνέχεια γίνεται παρουσίαση των χαρακτηριστικών των ασύρματων δικτύων καθώς και κάποια πλεονεκτήματα αλλά και μειονεκτήματα που παρουσιάζουν.

Το δεύτερο κεφάλαιο παρουσιάζει κάποιες τεχνικές που αναπτύχθηκαν για την ασφάλεια των δεδομένων στα δίκτυα των υπολογιστών, αφού πάνω σε αυτές τις μεθόδους βασίστηκαν και οι ασύρματες επικοινωνίες.

Στο τρίτο κεφάλαιο επισημαίνονται επιθέσεις που στοχεύουν σε ασύρματα δίκτυα wi-fi και δημιουργούν αμφιβολίες για την ασφάλεια τους. Παρουσιάζονται οι κατηγορίες και οι τίτλοι επιθέσεων ανά κατηγορία.

Στο τέταρτο κεφάλαιο γίνεται αναφορά στο hacking του διαδικτύου ,ο ορισμός του, παρουσίαση κάποιων γνωστών hacker αλλά και κάποια από τα πιο δημοφιλή εργαλεία που χρησιμοποιούνται ευρέως.

Στο πέμπτο κεφάλαιο παρουσιάζεται ένα από τα πιο γνωστά λειτουργικά των χρηστών το Kali Linux.

Κ Ε Φ Ά Λ Α Ι Ο 1 : Ε Ι Σ Α Γ Ω Γ Ή

1.1 Τι είναι τα ασύρματα δίκτυα

Ως ασύρματο δίκτυο χαρακτηρίζεται το τηλεπικοινωνιακό δίκτυο, συνήθως, τηλεφωνικό ή δίκτυο υπολογιστών, το οποίο χρησιμοποιεί, ραδιοκύματα ως φορείς πληροφορίας. Τα δεδομένα μεταφέρονται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα φέροντος η οποία εξαρτάται κάθε φορά από τον ρυθμό μετάδοσης δεδομένων που απαιτείται να υποστηρίζει το δίκτυο. Η ασύρματη επικοινωνία, σε αντίθεση με την ενσύρματη, δεν χρησιμοποιεί ως μέσο μετάδοσης κάποιον τύπο καλωδίου. Σε παλαιότερες εποχές τα τηλεφωνικά δίκτυα ήταν αναλογικά, αλλά σήμερα όλα τα ασύρματα δίκτυα βασίζονται σε ψηφιακή τεχνολογία και, επομένως, κατά μία έννοια, είναι ουσιαστικώς δίκτυα υπολογιστών.

Στα ασύρματα δίκτυα εντάσσονται τα δίκτυα κινητής τηλεφωνίας, οι δορυφορικές επικοινωνίες, τα ασύρματα δίκτυα ευρείας περιοχής (WWAN), τα ασύρματα μητροπολιτικά δίκτυα (WMAN), τα ασύρματα τοπικά δίκτυα (WLAN) και τα ασύρματα προσωπικά δίκτυα (WPAN). Η τηλεόραση και το ραδιόφωνο αν και ως τηλεπικοινωνιακά μέσα είναι εκ φύσεως ασύρματα στις περισσότερες περιπτώσεις, δεν συμπεριλαμβάνονται στα ασύρματα δίκτυα, καθώς η μετάδοση γίνεται προς πάσα κατεύθυνση χωρίς να υπάρχει κάποιο δομημένο «δίκτυο» τηλεπικοινωνιακών κόμβων (συσκευών) με τη συνήθη έννοια. Επιπλέον, τα μεταφερόμενα δεδομένα συνήθως είναι αναλογικά και, επομένως, δεν μπορούν να θεωρηθούν δίκτυα υπολογιστών.

1.2 Ιστορικά στοιχεία

Η πρώτη μορφή ασύρματης επικοινωνίας που υπήρξε ποτέ ήταν ο ασύρματος τηλέγραφος του Μαρκόνι. Ο Μαρκόνι άρχισε να πειραματίζεται με τον ηλεκτρομαγνητισμό το 1894 και πέτυχε την πρώτη μετάδοση μηνύματος χωρίς την χρήση καλωδίων μέσω κώδικα μορς. Αυτή του η εφεύρεση χρησιμοποιήθηκε στα πλοία και χρησιμοποιούταν μέχρι και πριν από λίγα χρόνια. Συχνά δε, τον ασυρματιστή του πλοίου τον αποκαλούσαν Μαρκόνι.

Τον περασμένο αιώνα έγινε ένα μεγάλο άλμα στις τηλεπικοινωνίες. Η χρήση δορυφόρων ήταν αυτή που επέτρεψε την εύκολη διασύνδεση απομακρυσμένων περιοχών της υδρογείου και κατήργησε την ανάγκη χρήσης συρμάτινων αγωγών τεράστιου μήκους ή την χρήση πολλών και ισχυρών επίγειων

αναμεταδοτών. Ο πρώτος τηλεπικοινωνιακός δορυφόρος εκτοξεύτηκε από τη nasa στις 12 Αυγούστου 1960.

Το 1970 στο Πανεπιστήμιο της Χαβάη, κάτω από την επίβλεψη του Norman Abramson, αναπτύχθηκε η πρώτη, παγκοσμίως, δικτυακή επικοινωνία χρησιμοποιώντας χαμηλού κόστους ερασιτεχνικά (ham-like) ραδιόφωνα, που ονομάστηκε ALOHAnet. Η αμφίδρομη τοπολογία αστέρα του συστήματος περιελάμβανε επτά υπολογιστές διασκορπισμένους σε τέσσερα νησιά, οι οποίοι επικοινωνούσαν με τον κεντρικό υπολογιστή στα νησί Oahu χωρίς τη χρήση τηλεφωνικών γραμμών. Η ασύρματη επικοινωνία χρησιμοποιεί τα ηλεκτρομαγνητικά κύματα τα οποία μεταδίδονται στη γήινη ατμόσφαιρα ή στο διάστημα. Έτσι για παράδειγμα τα ραδιοκύματα (με συχνότητες από 3KHz μέχρι 300MHz), χρησιμοποιούνται στα ασύρματα τηλέφωνα, στην κινητή τηλεφωνία, στη ραδιοεπικοινωνία, τη ραδιοφωνική και τηλεοπτική μετάδοση. Τα μικροκύματα (με συχνότητες από 300MHz μέχρι 300GHz) χρησιμοποιούνται στη ραδιοφωνική και τηλεοπτική μετάδοση και σε διάφορες μικροκυματικές ζεύξεις. Ακόμα και υπέρυθρη ακτινοβολία χρησιμοποιείται για ψηφιακή επικοινωνία σε δίκτυα περιορισμένης γεωγραφικής εμβέλειας. Με την δημιουργία των πρώτων δικτύων ηλεκτρονικών υπολογιστών, παράλληλα με τις μεθόδους που αναπτύχθηκαν για ενσύρματη σύνδεση των κόμβων, είχαμε και την προσπάθεια δημιουργίας ασύρματων τοπικών δικτύων που θα αποδέσμευε την επικοινωνία από τα ενσύρματα μέσα. Σήμερα τα ασύρματα τοπικά δίκτυα υπολογιστών, υλοποιούνται βασισμένα στις προδιαγραφές που ορίζει η οικογένεια πρωτοκόλλων του IEEE 802.11 και που στην ουσία είναι τον πρότυπο ethernet και το csma/ca, δηλαδή το πρωτόκολλο πολλαπλής πρόσβασης με ανίχνευση φέροντος και αποφυγή συγκρούσεων.

Τα πρώτα ασύρματα δίκτυα που εμφανίστηκαν ήταν τα ραδιοδίκτυα δεδομένων (Data) βασισμένα στο πρωτόκολλο TCP/IP. Οι πρώτες τεχνικές μεταγωγής πακέτων αναπτύχθηκαν γύρω στο 1964, ενώ ο όρος Packet" προτάθηκε από τον D. W. Davies του National Physical Laboratory της Μεγάλης Βρετανίας. Οι έρευνες του εργαστηρίου αυτού οδήγησαν στο σημερινό διεθνές δημόσιο δίκτυο μεταγωγής πακέτων X.25, ενώ το ίδιο έτος ο οργανισμός ARPA (Advanced Research Projects Agency) των Η.Π.Α. άρχισε να χρηματοδοτεί τα προγράμματα που οδήγησαν στη δημιουργία του ARPAnet (πυρήνα του σημερινού Internet) το 1969.

Η τεχνολογία των ασυρμάτων δικτύων μετάδοσης πακέτων άρχισε να αναπτύσσεται στην δεκαετία 1970-1980, αν και η μεγάλη ανάπτυξή της συμπίπτει με την διάδοση των μικροϋπολογιστών στην δεκαετία 1980-1990. Λόγω των ιδιαίτερων χαρακτηριστικών του μέσου μεταδόσεως τα ασύρματα δίκτυα χρησιμοποιούν εξειδικευμένα πρωτόκολλα για το υποεπίπεδο πρόσβασης μέσου (Medium Access Control) και το επίπεδο σύνδεσης δεδομένων (Data Link Layer) και συχνά και για ανώτερα επίπεδα (π.χ. δρομολόγηση πακέτων).

Υπάρχουν πολλά ανταγωνιστικά πρότυπα για ασύρματη δικτύωση σήμερα. Τα πιο δημοφιλή βέβαια (και τα οποία χρησιμοποιούνται πιο πολύ στο εμπόριο) είναι οι διάφορες εκδόσεις του πρότυπου IEEE 802.11. Αυτά είναι για παράδειγμα το 802.11b, το 802.11g (επέκταση του 802.11b),το 802.11a.. Το 802.11g είναι το πιο διαδεδομένο πρότυπο φυσικού επιπέδου σήμερα. Είναι για ασύρματα τοπικά δίκτυα στη μπάντα των 2,4GHz. Αποτελείται από τρία διαθέσιμα μη-επικαλυπτόμενα ασύρματα κανάλια, τα οποία έχουν ρυθμό μετάδοσης έως 54 Mbps το καθένα με χρήση OFDM. Νέα τεχνολογία είναι το 802.11i: Είναι ένα συμπληρωματικό πρότυπο για βελτίωση της ασφάλειας του συστήματος. Παρέχει έναν εναλλακτικό μηχανισμό του κλασσικού Wired Equivalent Privacy – WEP με καινούριες μεθόδους κρυπτογράφησης και πιστοποίησης.

Ο όρος WiFi (Wireless Fidelity, κατά την ορολογία High Fidelity η οποία αφορά την εγγραφή ήχου) χρησιμοποιείται για να προσδιορίσει τις συσκευές που βασίζονται στην προδιαγραφή IEEE 802.11 b/g/n και εκπέμπουν σε συχνότητες 2.4GHz. Το πρότυπο 802.11 γενικά το διαχειρίζεται η Wi-Fi Alliance, γνωστή πιο παλιά ως WECA, ένας μη κερδοσκοπικός οργανισμός που σχηματίστηκε το 1999 για να πιστοποιήσει την διαλειτουργικότητα των προϊόντων ασύρματης τοπικής δικτύωσης.

1.3 Πλεονεκτήματα Ασύρματης Δικτύωσης

Τα πλεονεκτήματα ασύρματων δικτύων είναι βραχυπρόθεσμα και μακροπρόθεσμα. Ενδεικτικά αναφέρονται τα ακόλουθα:

- Ευκολία χρήσης: Σήμερα, όλοι οι φορητοί υπολογιστές και πολλά κινητά τηλέφωνα είναι εξοπλισμένα με τεχνολογία WiFi που απαιτείται για απευθείας σύνδεση σε ένα ασύρματο δίκτυο LAN. Οι εργαζόμενοι μπορούν να συνδέονται

με ασφάλεια στους πόρους του δικτύου σας από οπουδήποτε εντός της εμβέλειας κάλυψης του δικτύου. Η περιοχή κάλυψης είναι κατά κανόνα οι εγκαταστάσεις της επιχείρησής σας, ωστόσο μπορεί να επεκτείνεται και σε περισσότερα κτήρια.

- Φορητότητα: Οι εργαζόμενοι μπορούν να παραμένουν συνδεδεμένοι στο δίκτυο, ακόμα και όταν δεν βρίσκονται στο γραφείο τους. Οι συμμετέχοντες σε συσκέψεις μπορούν να έχουν πρόσβαση σε έγγραφα και εφαρμογές. Οι πωλητές μπορούν να εντοπίζουν στο δίκτυο σημαντικές λεπτομέρειες από οποιαδήποτε τοποθεσία.
- Παραγωγικότητα: Η πρόσβαση στις πληροφορίες και στις βασικές εφαρμογές της εταιρείας σας υποστηρίζει το προσωπικό κατά τη διεκπεραίωση των εργασιών και ενθαρρύνει τη συνεργασία. Οι επισκέπτες (όπως πελάτες, συνεργάτες ή προμηθευτές) μπορούν να έχουν πρόσβαση υψηλής ασφαλείας στο Internet και στα επιχειρηματικά δεδομένα τους.
- Εύκολη ρύθμιση: Εφόσον δεν απαιτείται η τοποθέτηση καλωδίων σε ένα χώρο, η εγκατάσταση μπορεί να ολοκληρωθεί γρήγορα και οικονομικά. Τα ασύρματα δίκτυα LAN διευκολύνουν επίσης τη συνδεσιμότητα δικτύου σε δυσπρόσιτους χώρους, όπως οι αποθήκες ή οι εγκαταστάσεις εργοστασιακής παραγωγής.
- Δυνατότητα κλιμάκωσης: Καθώς οι επιχειρηματικές δραστηριότητές σας αναπτύσσονται, ενδεχομένως να απαιτείται άμεση επέκταση του δικτύου σας. Τα ασύρματα δίκτυα μπορούν κατά κανόνα να επεκταθούν με τον υπάρχοντα εξοπλισμό, ενώ ένα ενσύρματο δίκτυο ενδέχεται να απαιτεί επιπλέον καλωδίωση.
- Ασφάλεια: Ο έλεγχος και η διαχείριση της πρόσβασης στο ασύρματο δίκτυό σας είναι μέγιστης σημασίας για την επιτυχία του. Οι εξελιγμένες δυνατότητες της τεχνολογίας WiFi προσφέρουν ισχυρή προστασία, ώστε τα δεδομένα σας να είναι εύκολα προσβάσιμα μόνο από τους χρήστες στους οποίους επιτρέπετε την πρόσβαση.
- Κόστος: Μπορεί να αποδειχθεί οικονομικότερη η λειτουργία ενός ασύρματου δικτύου LAN, το οποίο εξαλείφει ή μειώνει το κόστος καλωδίωσης σε περιπτώσεις μετακόμισης, αναδιάταξης ή επέκτασης γραφείων.

1.4 Μειονεκτήματα Ασύρματης Δικτύωσης

Παρόλα τα θετικά που υπάρχουν από τη χρήση των ηλεκτρομαγνητικών κυμάτων, ραδιοκυμάτων και υπέρυθρης ακτινοβολίας, για την μεταφορά πληροφορίας, υπάρχουν και κάποια αρνητικά στοιχεία, όπως για παράδειγμα το γεγονός ότι τα ασύρματα δίκτυα προσβάλλονται πιο εύκολα από φαινόμενα παρεμβολής, τα οποία συχνά αλλοιώνουν την επικοινωνία των χρηστών. Αυτά τα μειονεκτήματα παρουσιάζονται σε αυτή την ενότητα:

- Παρεμβολή λόγω πολλαπλών διαδρομών: Αυτό το φαινόμενο οφείλεται στην πιθανότητα που υπάρχει τα σήματα που μεταδίδονται να συνδυαστούν με άλλα ανακλώμενα από επιφάνειες ή εμπόδια σήματα, τα οποία βρίσκονται στην ευθεία μετάδοσης του σήματος.
- Path loss: Ονομάζονται οι απώλειες που μπορεί να έχουμε σε μια ασύρματη επικοινωνία και εξαρτώνται άμεσα από την ύπαρξη ή μη οπτικής επαφής (LOS: Line Of Sight)
- Παρεμβολές ραδιοσημάτων: Οι παρεμβολές από ραδιοσήματα (Radio Signal Interference) διαχωρίζονται σε Εσωτερικές (inward) και Εξωτερικές (outward).
- Διαχείριση ενέργειας: Καλό είναι να επιλέγονται προϊόντα για σωστή διαχείριση ενέργειας, ώστε να μεγιστοποιείται η αυτονομία του δικτύου.
- Ασυμβατότητα συστημάτων: Για την εγκατάσταση ενός WLAN θα πρέπει να λάβουμε υπόψη και την ασυμβατότητα μεταξύ προϊόντων διαφορετικών κατασκευαστών.
- Προστασία της υγείας των χρηστών: Τα ασύρματα δίκτυα που χρησιμοποιούν την τεχνική μετάδοσης με υπέρυθρες ακτίνες, θα πρέπει να περιορίζουν την ισχύ του εκπεμπόμενου σήματος στο ανώτερο όριο των 2 Watts, για να αποφευχθούν προβλήματα υγείας.
- Το πρόβλημα του κρυμμένου κόμβου: Το φαινόμενο αυτό παρατηρείται όταν υπάρχει ένας σταθμός ο οποίος δεν μπορεί να ανιχνεύσει την δραστηριότητα ενός άλλου σταθμού ώστε να αναγνωρίσει ότι το μέσο χρησιμοποιείται.
- Ασφάλεια δικτύου: Η συνολική λειτουργία ενός ασύρματου δικτύου εμπεριέχεται στα χαμηλότερα επίπεδα της αρχιτεκτονικής ενός δικτύου και δεν ενυπάρχει με άλλες λειτουργίες όπως εγκατάσταση σύνδεσης ή άλλες υπηρεσίες (π.χ. login) που προσφέρουν τα ανώτερα στρώματα. Έτσι το μόνο θέμα που σχετίζεται με την ασφάλεια και τα ασύρματα δίκτυα είναι τα θέματα

ασφαλείας των χαμηλότερων στρωμάτων, π.χ. κρυπτογράφηση (encryption) δεδομένων. Συνεπώς, έχουν δημιουργηθεί διάφορες τεχνικές κωδικοποίησης οι οποίες καθιστούν δύσκολη την υποκλοπή της πληροφορίας που μεταδίδεται. Τέτοιες τεχνικές είναι η εξάπλωση φάσματος (spread spectrum), ενώ εάν απαιτείται μεγαλύτερη ασφάλεια, καθορίζεται η χρήση της κωδικοποίησης WEP (Wired Equivalent Privacy).

1.5 Δομικά στοιχεία ασύρματων δικτύων

Για την ανάπτυξη ενός ασύρματου τοπικού δικτύου είναι απαραίτητη κάποια υλικοτεχνική υποδομή, δηλαδή τα διάφορα στοιχεία (components) τα οποία συντονίζουν την μετάδοση, λήψη και επεξεργασία του σήματος μεταξύ των χρηστών. Η δομή αυτή περιλαμβάνει τόσο το λογισμικό (software) όσο και τον ανάλογο υλικό εξοπλισμό (hardware).

Συσκευές χρηστών (End-user devices) :

Η επικοινωνία μεταξύ των χρηστών σε ένα ασύρματο δίκτυο γίνεται μέσω συγκεκριμένων συσκευών όπως:

- Σταθεροί Υπολογιστές (Desktops)
- Φορητοί Υπολογιστές (Laptops)
- Υπολογιστής παλάμης (Palmtop)
- Υπολογιστής Χειρός και εκτυπωτές (Handheld PCs and printers)
- IP Phones
- IP Cameras
- Projectors
- Printers

➢ Λογισμικό δικτύου (Network Software) :

Ένα ασύρματο δίκτυο είναι σχεδιασμένο σύμφωνα με το κατάλληλο λογισμικό που βρίσκεται σε διάφορα μέρη του δικτύου. Ένα σύστημα διαχείρισης δικτύου (NOS: Network Operating System), όπως είναι για παράδειγμα το Microsoft NT Server, παρέχει διαφόρων ειδών υπηρεσίες, όπως μεταφορά δεδομένων, εκτύπωση κ.ά. Αυτά τα συστήματα στηρίζονται στην ύπαρξη ενός εξυπηρετητή (server), ο οποίος διαθέτει τις βάσεις δεδομένων στις οποίες μπορούν να έχουν πρόσβαση οι διάφορες συσκευές

τις οποίες ελέγχει ο χρήστης. Οι τελευταίες «τρέχουν» το δικό τους λογισμικό (client software), το οποίο κατευθύνει τις εντολές του χρήστη στον server.

- Ασύρματες κάρτες δικτύου (Wireless NICs) :

Η ασύρματη κάρτα δικτύου (Wireless Network Interface Card) χρησιμοποιείται για την μετάδοση του σήματος ενός υπολογιστή σε έναν άλλο υπολογιστή. Σε αυτή τη διαδικασία συμπεριλαμβάνεται η διαμόρφωση και η ενίσχυση του σήματος. Αυτή η κάρτα είναι σαν μία τυπική κάρτα δικτύου απλά διαθέτει μία μικρή κεραία. Μερικές εταιρίες παράγουν κάρτες οι οποίες συνδέονται με τον υπολογιστή μέσω μιας RS-232 σειριακής ή παράλληλης θύρας. Η διασύνδεση της ασύρματης κάρτας με την συσκευή του χρήστη συμπεριλαμβάνει και έναν οδηγό λογισμικού (software driver) που συνδέει το λογισμικό του NOC στην κάρτα.

- Σημεία πρόσβασης (access points): Το σημείο πρόσβασης είναι μια κεντρική συσκευή σε ένα ασύρματο δίκτυο που παρέχει το εύρος για την ασύρματη επικοινωνία με τους άλλους σταθμούς σε ένα δίκτυο. Συνήθως συνδέεται σε ένα ενσύρματο δίκτυο και έτσι παρέχει μια γέφυρα ανάμεσα στο ενσύρματο δίκτυο και τις ασύρματες συσκευές. Τα σημεία πρόσβασης περιλαμβάνουν χαρακτηριστικά ασφάλειας όπως επικύρωση και κρυπτογράφηση, έλεγχο πρόσβασης που βασίζεται σε λίστες ή φίλτρα καθώς και πολλά άλλα τα οποία συνήθως απαιτούν τη ρύθμιση τους από τον χρήστη σύμφωνα με τις προτιμήσεις του, συνήθως χρησιμοποιώντας μια διεπαφή βασισμένη στο διαδίκτυο. Πολλά σημεία πρόσβασης περιλαμβάνουν επιπρόσθετα χαρακτηριστικά δικτύωσης όπως πύλες διαδικτύου, κόμβους μεταγωγής, ασύρματες γέφυρες ή επαναλήπτες.
- Ασύρματες Τοπικές Γέφυρες (Wireless Local Bridges):

Οι ασύρματες τοπικές γέφυρες είναι βασικό κομμάτι στην τοπολογία ενός δικτύου αφού συνδέουν πολλά τοπικά δίκτυα μεταξύ ώστε να αναπτυχθεί ένα πιο λειτουργικό δίκτυο. Οι γέφυρες χωρίζονται σε δύο κατηγορίες: Local bridges, δημιουργία σύνδεσης ανάμεσα σε κοντινά τοπικά δίκτυα και Remote bridges, δημιουργία σύνδεσης ανάμεσα δίκτυα που χωρίζονται από αποστάσεις μεγαλύτερες από αυτές που μπορούν να υποστηρίξουν τα πρωτόκολλα των τοπικών δικτύων. Συνήθως οι γέφυρες, οι οποίες είναι συσκευές που χρησιμεύουν στην διασύνδεση ασύρματου με ενσύρματου δικτύου, αλλά και τη διασύνδεση πολλών WLAN μεταξύ τους, αναφέρονται ως APs (Access Points).

- Κεραίες (Antennas):

Οι κεραίες είναι υπεύθυνες για την εκπομπή του διαμορφωμένου σήματος στον αέρα και μπορούν να διακριθούν σε πολλές κατηγορίες και βασικά τους χαρακτηριστικά είναι η ισχύς μετάδοσης (Transmit power), το εύρος ζώνης (Bandwidth), το μοντέλο διάδοσης (propagation pattern) που χρησιμοποιούν και το κέρδος (Gain). Ο τρόπος που μεταδίδει το σήμα μια κεραία καθορίζει επίσης και την περιοχή κάλυψης της. Για την μετάδοση του σήματος στα ασύρματα δίκτυα χρησιμοποιούνται κυρίως δύο είδη κεραιών η πολυκατευθυντική (omnidirectional) κεραία, όπου πρόκειται για κεραίες που διοχετεύουν την ισχύ τους προς κάθε κατεύθυνση και αθροιστικά έχουν την ίδια ενίσχυση προς κάθε κατεύθυνση. Το πρότυπο εκπομπής τους είναι τέτοιο, ώστε να δημιουργούν γύρω τους ένα πεδίο που μοιάζει με «ιπτάμενο δίσκο». Η δεύτερη κατηγορία περιλαμβάνει την μονοκατευθυντική (directional) κεραία η οποία συγκεντρώνει το μεγαλύτερο μέρος της ισχύος της σε μία μόνο κατεύθυνση.

1.5.1Εξοπλισμός ασύρματου δικτύου

Η επιλογή του κατάλληλου εξοπλισμού είναι βασικό στάδιο για τη δημιουργία του δικτύου. Θα πρέπει να πληρεί τους κανονισμούς, να ανταποκρίνεται στις ανάγκες της υλοποίησης, να τηρεί κάποιες προδιαγραφές, και να έχει ένα λογικό κόστος.

Ένα ασύρματο σύστημα αποτελείται από την ασύρματη συσκευή και το αντίστοιχο κεραιοσύστημα. Η ποικιλία συσκευών και κεραιών διαφόρων τύπων με διαφορετικές προδιαγραφές, ποιότητα κατασκευής και κόστος, είναι μεγάλη, η σωστή επιλογή ανάμεσα τους απαιτεί στοιχειώδη τουλάχιστον γνώση των χαρακτηριστικών τους.

Ένα απλό λειτουργικό ασύρματο συστήματος λειτουργεί ως εξής :

Το ηλεκτρομαγνητικό κύμα συλλαμβάνεται από την κεραία, και μετατρέπεται σε ηλεκτρικό και μέσω κατάλληλου καλωδίου μεταφέρεται στο δέκτη. Εκεί ενισχύεται, το σήμα, φιλτράρεται για να απορριφθούν τα γειτονικά κανάλια και αποδιαμορφώνεται.

Το ψηφιακό σήμα που ανακτάται οδηγείται μέσω κατάλληλης διεπαφής προς τον υπολογιστή.

Κατά την εκπομπή το σήμα πληροφορίας μεταφέρεται στην ασύρματη συσκευή, διαμορφώνεται στο κατάλληλο RF σήμα και οδηγείται στην κεραία, όπου και εκπέμπεται με τη μορφή ηλεκτρομαγνητικών κυμάτων στο χώρο.

Κεραία

Χρησιμοποιείται για να μετατρέπει τα ηλεκτρικά σήματα σε ραδιοκύματα στην περίπτωση της εκπομπής και το αντίστροφο στην περίπτωση της λήψης.

Τύπος κεραίας

Για μικρές αποστάσεις ή εσωτερικούς χώρους, η κεραία είναι ενσωματωμένη στην συσκευή.

Σε πολλές συσκευές υπάρχουν δύο τέτοιες κεραίες για να αντιμετωπίζεται το φαινόμενο των ανακλάσεων που υφίσταται σε εσωτερικούς χώρους. Αντίθετα, σε εξωτερικούς χώρους ή όταν θέλουμε να αυξήσουμε την εμβέλεια χρησιμοποιούμε εξωτερικές κεραίες. Αυτές συγκεντρώνουν την ακτινοβολία σε συγκεκριμένες κατευθύνσεις. Πρέπει να προσέξουμε ότι προσθέτοντας εξωτερική κεραία σε μια συσκευή, αλλάζουμε τα χαρακτηριστικά εκπομπής της, και αναιρούμε την πιστοποίηση καταλληλότητας. Συνεπώς, αυτό θα πρέπει να γίνεται σε εξοπλισμό που προβλέπει την προσθήκη εξωτερικής κεραίας και να λαμβάνουμε υπόψη το ρυθμιστικό πλαίσιο, αλλά και τους κανόνες καλής σχεδίασης. Διαφορετικά, παραβαίνουμε τον κανόνα χρήσης της ζώνης συχνοτήτων ISM.

Με βάση το εύρος γωνιών στο οποίο εκπέμπουν οι κεραίες, χωρίζονται σε κάποιους βασικούς τύπους. Η κατευθυντική κεραία συγκεντρώνει την εκπομπή της σε μια κατεύθυνση, οπότε το εύρος του κύριου λοβού ακτινοβολίας είναι λίγες μοίρες, και παρέχει έτσι μεγάλο κέρδος και πραγματοποιούνται ζεύξεις μεγάλων αποστάσεων. Η ομοιοκατευθυντική κεραία, εκπέμπει σε εύρος 360 μοιρών (προς όλες της κατευθύνσεις). Οι κεραίες αυτές προκαλούν μεγάλο θόρυβο, οπότε καλό θα ήταν να αποφεύγονται. Ακόμη, υπάρχουν και οι κεραίες τομέα με γωνία οριζόντιας κάλυψης από 40 έως 180 μοίρες.

Ένα βασικό χαρακτηριστικό της κεραίας, είναι το κέρδος. Το κέρδος το μετράμε σε μονάδες dBi και εκφράζει την ενίσχυση της εκπομπής μιας κεραίας προς μια κατεύθυνση σε σχέση με την περίπτωση που η ισχύς σκορπίζονταν ομοιόμορφα προς όλες τις κατευθύνσεις. Έτσι, πρώτα ελέγχουμε τον τύπο της κεραίας και το κέρδος της ανάλογα με την περιοχή που θέλουμε να καλύψουμε και την εμβέλεια που θέλουμε να έχουμε.

Άλλοι παράγοντες που πρέπει να λάβουμε υπόψη, κατά την επιλογή μας:

- ***Εγκατάσταση***

Ανάλογα με τις συνθήκες εγκατάστασης, μπορεί να αγοράσουμε μία κεραία από τις μη ενδεδειγμένες.

- ***Ποιότητα κατασκευής***

Ποιότητα κατασκευής εκτός, από την αντοχή, σημαίνει επίσης καλά ηλεκτρικά χαρακτηριστικά. Δηλαδή, να έχει καλό διάγραμμα ακτινοβολίας, για να μην επηρεάζεται από παρεμβολές και να παρεμβάλλει όσο το δυνατό λιγότερο.

- ***Διακριτικότητα***

Κυρίως για λόγους αισθητικής, σε εσωτερικούς χώρους, χρησιμοποιούμε όσο το δυνατό πιο μικρές και διακριτικές κεραίες.

- ***Διασύνδεση κεραίας - συσκευής***

Στις μη ενσωματωμένες κεραίες μεταφέρουμε το σήμα μέσω ομοαξονικού καλωδίου και συνδετήρων κατάλληλων προδιαγραφών.

- ***Ασύρματη συσκευή***

Πρότυπο

Υπάρχουν συσκευές για κάθε ένα από τα πρότυπα 802.1 lb, 802.11g, 802.1 la, καθώς και συσκευές που υλοποιούν περισσότερα του ενός πρότυπα (b/g, a/b, a/g, b/g/a).

Τύπος

Οι συσκευές μπορεί να είναι με μορφή κάρτας ή αυτόνομες συσκευές. Οι αυτόνομες συνδέονται με το υπόλοιπο δίκτυο με μια τυποποιημένη διεπαφή Ethernet ή USB. Αυτές μπορούν να εκτελούν κάποιες επιπλέον λειτουργίες όπως να ενσωματώνουν ένα switch ή ένα ADSL modem ή να υλοποιούν πρωτόκολλα όπως το DHCP ή το NAT.

- ***Κόστος***

Ένα Access Point κυμαίνεται από 100 ως 1000 ευρώ. Η τιμή μιας απλής ασύρματης κάρτας μπορεί να είναι από 50 ως 150 ευρώ.

1.6 Πρότυπο IEEE 802.11

Το πρώτο πρότυπο ασύρματων τοπικών δικτύων είναι το IEEE 802.11 και όπως προαναφέραμε είναι υπεύθυνο για τον έλεγχο πρόσβασης στα ασύρματα δίκτυα και υιοθετήθηκε το 1997. (IEEE 802.11 WG)

- Οικογένεια: Στα τέλη του 1999 η IEEE γνωστοποίησε δύο νέα συμπληρωματικά πρότυπα για WLANs, τα 802.11a, 802.11b, 802.11g και 802.11y.
    - Το 802.11a μπορεί να υποστηρίζει ρυθμούς δεδομένων έως και 54 Mbps, ονομαστικός ρυθμός μετάδοσης, με συνήθη ρυθμό μετάδοσης 23 Mbits/s, εμβέλεια εσωτερικού χώρου έως και 35 m και χρήση της τεχνικής διαμόρφωσης OFDM (Orthogonal Frequency Division Multiplexing) στην μπάντα των 5,7 GHz.
    - Το 802.11b είναι ουσιαστικά ο αντικαταστάτης του αρχικού 802.11 αφού υποστηρίζει ρυθμούς δεδομένων έως και 11 Mbps, με εμβέλεια εσωτερικού χώρου έως και 35 m ενώ χρησιμοποιεί ως διαμόρφωση την τεχνική DSSS (direct-sequence spread spectrum) στα 2.4 GHz.
    - Το 2003, η IEEE κοινοποίησε το πρότυπο 802.11g, το οποίο υποστηρίζει ρυθμούς δεδομένων έως και 54 Mbps, με συνήθη ρυθμό μετάδοσης 19 Mbits/s, εμβέλεια εσωτερικού χώρου έως και 38 m με την τεχνική OFDM στα 2.4 GHz.
    - Για το 2008, προτάθηκε από την IEEE το πρότυπο 802.11y, το οποίο χρησιμοποιεί την τεχνική MIMO (Multiple – Input Multiple - Output) με συχνότητα 3,7 GHz, ρυθμό μετάδοσης 54Mbits/s και εμβέλεια 5000 m.

Εκτός των παραπάνω εκδόσεων έχουν προταθεί και κάποιες άλλες επεκτάσεις τους, οι οποίες όμως δεν έχουν υλοποιηθεί σε εμπορικά προϊόντα και έχουν περισσότερο ακαδημαϊκό ενδιαφέρον. (IEEE 802.11 WG)

- 802.11e ή QoS: προσπαθεί να εξασφαλίζει ικανοποιητική ποιότητα υπηρεσιών για εφαρμογές πραγματικού χρόνου που εκτελούνται πάνω σε ένα WLAN ελαχιστοποιώντας ή μεγιστοποιώντας ένα από τα παρακάτω κριτήρια: μέση καθυστέρηση από άκρο σε άκρο, μέση μεταβολή της καθυστέρησης ή μέσο ποσοστό επιτυχούς παράδοσης πλαισίων.
- 802.11n, το οποίο με χρήση πολλαπλών κεραιών (μέθοδος γνωστή ως MIMO, εκ του Multiple Input Multiple Output) παρέχει ονομαστικό ρυθμό μετάδοσης τουλάχιστον 108 Mbps. Το πρότυπο οριστικοποιήθηκε το 2009.

1.6.1 Χαρακτηριστικά του IEEE 802.11

Η ζώνη συχνοτήτων των 2.4 GHz σήμερα είναι ιδιαίτερα δημοφιλής, διότι είναι μία ελεύθερη ζώνη με συγκεκριμένα χαρακτηριστικά που επιτυγχάνουν την επικοινωνία σε μεγάλες αποστάσεις. Στη συνέχεια θα παρουσιάσουμε τα πιο σημαντικά:

- Εμβέλεια

Η εμβέλεια ενός τοπικού ασύρματου δικτύου σε εσωτερικούς χώρους κυμαίνεται από 20 έως 38 μέτρα. Τα ραδιοκύματα όμως πρέπει να διαπεράσουν τοίχους και οροφές, οπότε έχουμε σημαντικές απώλειες του σήματος. Επιπλέον το σήμα υπόκειται και σε άλλους μηχανισμούς διάδοσης όπως είναι η ανάκλαση σε προσπίπτουσες επιφάνειες ή η διάχυση. Σε περιβάλλον όμως με οπτική επαφή (Line Of Sight) μεταξύ των χρηστών, σε εξωτερικό χώρο, η εμβέλεια του ασύρματου δικτύου είναι μεγαλύτερη και εξαρτάται από διάφορους παράγοντες που σχετίζονται με τις συσκευές όπως την ευαισθησία του δέκτη, την ποιότητα των κεραιών, το επίπεδο παρεμβολών και θορύβου.

- Ρυθμός μετάδοσης

Ο ρυθμός μετάδοσης του σήματος εξαρτάται από διάφορους παράγοντες όπως η απόσταση, οι ανακλάσεις, η απορρόφηση και η σκέδαση, αλλά και ο αριθμός των χρηστών.

- Ποιότητα επικοινωνίας

Ύστερα από την πάροδο ετών χρήσης και εκατοντάδων εμπορικών και στρατιωτικών εφαρμογών, οι τεχνολογίες ασύρματης μετάδοσης έχουν γίνει πολύ αξιόπιστες.

- Συμβατότητα με το υπάρχον δίκτυο

Τα πιο πολλά ασύρματα δίκτυα έχουν συγκεκριμένο τρόπο διασύνδεσης με τα ενσύρματα δίκτυα, επομένως η προσάρτηση ασύρματης δικτύωσης, σε υπάρχουσες δομές δικτύων, μπορεί να γίνει με εύκολο τρόπο.

- Παρεμβολές

Το ασύρματο τοπικό δίκτυο μπορεί να δεχτεί και να προκαλέσει παρεμβολές σε άλλες συσκευές που λειτουργούν στα 2.4GHz όπως άλλα ασύρματα δίκτυα, ασύρματα τηλέφωνα, φούρνοι μικροκυμάτων και συσκευές Bluetooth. Σημαντικότερες όμως είναι οι παρεμβολές που προκύπτουν από την κακή σχεδίαση ενός ασύρματου δικτύου.

- Διαλειτουργικότητα

Οι περιπτώσεις κατά τις οποίες οι συσκευές δε συνεργάζονται μεταξύ τους είναι λόγω διαφορετικής τεχνολογίας, λόγω διαφορετικής συχνότητας, ή λόγω διαφορετικών υλοποιήσεων

- Η Τοπολογία του 802.11

Η τοπολογία του 802.11 αποτελείται από στοιχεία που αλληλεπιδρούν ώστε να παρέχουν ένα ασύρματο τοπικό δίκτυο το οποίο παρέχει τη δυνατότητα μετακίνησης των σταθμών χωρίς να γίνεται αντιληπτή στα ανώτερα στρώματα, όπως το LLC (Logical Link Control). Ένας σταθμός (station) είναι κάθε συσκευή η οποία εμπεριέχει τις λειτουργίες του 802.11. Οι λειτουργίες του 802.11 ενυπάρχουν (reside) σε μια ασύρματη κάρτα δικτύου NIC (Network Interface Card), το λογισμικό διασύνδεσης που οδηγεί την κάρτα NIC και τον σταθμό βάσης ή AP (Access Point).

Κ Ε Φ Ά Λ Α Ι Ο 2 : ΑΣΦΑΛΕΙΑ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΥΠΟΛΟΓΙΣΤΩΝ

2.1 Εισαγωγή

Κατά τις πρώτες δεκαετίες της ύπαρξης τους, τα δίκτυα υπολογιστών χρησιμοποιούνταν κυρίως από τους πανεπιστημιακούς ερευνητές για αποστολή ηλεκτρονικού ταχυδρομείου και από τους υπαλλήλους των εταιρειών για κοινή χρήση των εκτυπωτών. Υπό αυτές τις συνθήκες, δεν δινόταν και πολύ σημασία στην ασφάλεια. Στις μέρες μας, όμως, που εκατομμύρια απλοί άνθρωποι χρησιμοποιούν τα δίκτυα για τραπεζικές συναλλαγές, αγορές, υποβολή φορολογικών δηλώσεων κ πολλών άλλων προσωπικών χρήσεων, και όπου ανακαλύπτεται η μία αδυναμία μετά την άλλη, η ασφάλεια των δικτύων προβάλλει στον ορίζοντα ως ένα δυνητικά τεράστιο πρόβλημα.

Η ασφάλεια είναι ένα πλατύ θέμα που περικλείει πολλές αμαρτίες. Στην απλούστερη μορφή της προσπαθεί να εξασφαλίσει ότι οι αδιάκριτοι δεν θα μπορούν να διαβάσουν, ή ακόμη χειρότερα να τροποποιήσουν, χωρίς να γίνουν αντιληπτοί τα μηνύματα που προορίζονται για άλλους παραλήπτες. Ασχολείται επίσης με μεθόδους με τις οποίες μπορούμε να προσδιορίσουμε αν, για παράδειγμα, αυτό το μήνυμα που λάβατε (υποτίθεται) από την εφορία και το οποίο λέει «Πλήρωσε μέχρι την Παρασκευή αλλιώς…» προέρχεται πραγματικά από την εφορία, και όχι από την Μαφία. Η ασφάλεια ασχολείται επίσης με το πρόβλημα της «σύλληψης» και αναπαραγωγής νόμιμων μηνυμάτων, καθώς και με όσους προσπαθούν αργότερα να αρνηθούν ότι έστειλαν ορισμένα μηνύματα.

Τα περισσότερα προβλήματα ασφαλείας προκαλούνται σκόπιμα από κακόβουλα άτομα τα οποία προσπαθούν να αποκομίσουν κάποιο κέρδος, να προσελκύσουν την προσοχή, ή να βλάψουν κάποιον. Ορισμένοι από τους πιο συχνούς δράστες φαίνονται στον παρακάτω πίνακα 1. Θα πρέπει να είναι σαφές από τη λίστα αυτή ότι το να γίνει ένα δίκτυο ασφαλές απαιτεί πολύ περισσότερα πράγματα από το να είναι απλώς απαλλαγμένο από προγραμματιστικά σφάλματα. Απαιτεί να ξεπεράσουμε σε εξυπνάδα αντιπάλους οι οποίοι είναι συχνά έξυπνοι, αφοσιωμένοι στον στόχο τους, και μερικές φορές καλά χρηματοδοτούμενοι. Θα πρέπει να είναι επίσης σαφές ότι τα

μέτρα που θα αποθαρρύνουν τους περιστασιακούς αντιπάλους θα έχουν αντίκτυπο στους πιο σοβαρούς από αυτούς.

Αντίπαλος	**Στόχος**
Φοιτητής	Να διασκεδάσει κρυφοκοιτάζοντας τα email των άλλων
Κράκερ	Να δοκιμάσει το σύστημα ασφαλείας κάποιου, να κλέψει δεδομένα
Επιχείρηση	Να ανακαλύψει τη στρατηγική μάρκετινγκ ενός ανταγωνιστή
Πρώην υπάλληλος	Να εκδικηθεί επειδή τον απέλυσαν
Λογιστής	Να καταχραστεί χρήματα από μια εταιρεία
Χρηματιστής	Να αρνηθεί μια υπόσχεση που έδωσε σε έναν πελάτη μέσω ηλεκτρονικού ταχυδρομείου
Απατεώνας σε πλαστογραφίες	Να κλέψει και να πουλήσει αριθμούς πιστωτικών καρτών

Πίνακας 1 Ορισμένοι άνθρωποι που προκαλούν προβλήματα ασφαλείας, και οι λόγοι για τους οποίους το κάνουν αυτό.

Τα αρχεία της αστυνομίας δείχνουν ότι οι περισσότερες καταστροφικές επιθέσεις δεν προέρχονται από εξωτερικούς παράγοντες που παγιδεύουν μια τηλεφωνική γραμμή, αλλά από άτομα που βρίσκονται μέσα στον οργανισμό και έχουν κάποιο παράπονο. Κατά συνέπεια, τα συστήματα ασφαλείας θα πρέπει να σχεδιάζονται με βάση το γεγονός αυτό.

Τα προβλήματα ασφαλείας δικτύου μπορούν να υποδιαιρεθούν γενικά σε τέσσερις στενά αλληλένδετους τομείς: μυστικότητα, πιστοποίηση ταυτότητας, μη απάρνηση, και έλεγχος ακεραιότητας. Η μυστικότητα (secrecy), η οποία ονομάζεται και εμπιστευτικότητα (confidentiality), προσπαθεί να διατηρήσει τις πληροφορίες μακριά από τα χέρια των μη εξουσιοδοτημένων χρηστών. Αυτό είναι το χαρακτηριστικό που συνήθως έρχεται στο μυαλό των ανθρώπων όταν σκέφτονται την ασφάλεια δικτύων. Η πιστοποίηση ταυτότητας (authentication) ασχολείται με τον προσδιορισμό του συνομιλητή μας πριν αποκαλύψουμε ευαίσθητες πληροφορίες ή πριν κλείσουμε μια επιχειρηματική συμφωνία. Η μη απάρνηση (nonrepudiation) ασχολείται με τις υπογραφές: πώς αποδεικνύεται ότι ένας πελάτης όντως σας έδωσε μια ηλεκτρονική παραγγελία για δέκα εκατομμύρια μπιχλιμπίδια προς 89 λεπτά το καθένα, όταν αργότερα αυτός ισχυρίζεται ότι η τιμή ήταν 69 λεπτά; Ή όταν ίσως ισχυρίζεται ότι δεν έδωσε ποτέ κάποια παραγγελία; Τέλος, ο έλεγχος ακεραιότητας ασχολείται με το πώς μπορεί κανείς να είναι βέβαιος ότι το μήνυμα που έλαβε ήταν

όντως αυτό που στάλθηκε , και όχι κάτι που σκάρωσε ή τροποποίησε στη διαδρομή ένας κακόβουλος αντίπαλος.

Όλα αυτά τα ζητήματα (μυστικότητα, πιστοποίηση ταυτότητας, μη απάρνηση, και έλεγχος ακεραιότητας) εμφανίζονται και στα παραδοσιακά συστήματα, αλλά με ορισμένες σημαντικές διαφορές. Η ακεραιότητα και η μυστικότητα επιτυγχάνονται με χρήση συστημένου ταχυδρομείου και με κλείδωμα εγγραφών. Η ληστελια του ταχυδρομείου είναι δυσκολότερη τώρα, απ' ότι ήταν την εποχή του διάσημου ληστή Jesse James.

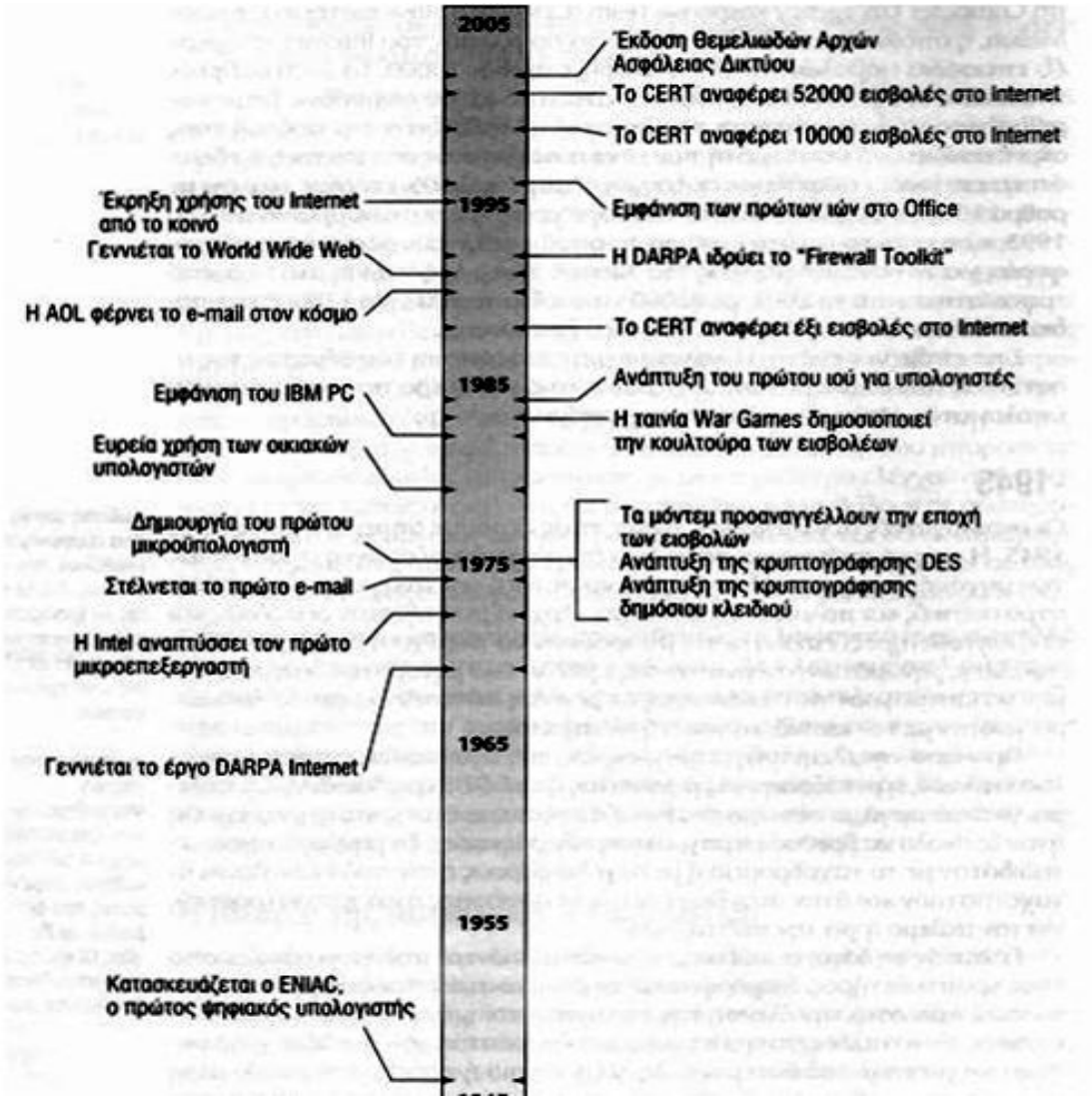
Πιο παλιά, εμφανίζονταν διαρκώς ιστορίες μεγάλων και καταστροφικών εισβολών στους ηλεκτρονικούς υπολογιστές με πιο γνωστή, το 2001 όπου ήταν ένα ιδιαίτερα κακό έτος για την ασφάλεια στο Internet. Τότε ένα «σκουλήκι» με το όνομα Code Red διαχύθηκε χωρίς έλεγχο μέσα στο Internet και αφού διορθώθηκε ο ιός Nimda έκανε ακριβώς το ίδιο πράγμα. Οι ιοί, οι οποίοι είναι υπεύθυνοι για την παραβίαση της ασφάλειας των συστημάτων υπολογιστών, διαχέονται συχνά μέσω e-mail. Όταν η Microsoft εμφάνισε στην αγορά το λειτουργικό σύστημα Windows XP, αποδείχθηκε ότι είχε ένα σφάλμα ασφάλειας, το οποίο ήταν τόσο εμφανές, που οι περισσότεροι εισβολείς θα μπορούσαν να εισβάλουν, σχεδόν, σε κάθε υπολογιστή χωρίς ιδιαίτερη προσπάθεια.

Οι πρότυπες υπηρεσίες FTP (File Transfer Protocol) και NDS του Unix υπέστησαν εισβολές, δίνοντας μάλιστα στους εισβολείς την δυνατότητα να εισέλθουν σε ιστοσελίδες και να καταστρέψουν τα περιεχόμενά τους. Μέχρι το 2004, παραλλαγές του Nimda συνέχιζαν να υπάρχουν ακόμη στο Internet, πραγματοποιώντας επιθέσεις σε νέες εγκαταστάσεις, ενώ παρόμοιοι ιοί όπως ο Sasser χρησιμοποιούν το διορθωμένο κώδικα για να υλοποιήσουν νέες επιθέσεις. Οι επιχειρήσεις δαπανούν ολοένα και περισσότερα χρήματα ώστε να εξασφαλίσουν την ασφάλεια των πληροφοριακών τους συστημάτων, αλλά οι εισβολείς βελτιώνουν και αυτοί με τη σειρά τους τα εργαλεία που χρησιμοποιούν για τις παραβιάσεις τους.

Το έτος που άρχισαν να καταγράφονται τα πρώτα προβλήματα λόγω παραβίασης της ασφάλειας είναι το 1988, από την επιτροπή Computer Emergency Response Team (CERT) στο Πανεπιστήμιο Carnegie Mellon, η οποία παρακολουθεί επεισόδια ασφάλειας του Internet και είχε αναφέρει έξι επεισόδια εισβολών. Η ίδια επιτροπή το 1999, ανέφερε σχεδόν 10000 επιθέσεις, το 2000 ανέφερε πάνω από 22000, ενώ το 2001 ανέφερε πάνω από 52000 επεισόδια Αυτοί οι αριθμοί φαίνονται πολύ μεγάλοι,

όμως αν αναλογιστούμε μεμονωμένα τις επιθέσεις που συμβαίνουν σε κάθε υπολογιστή που είναι συνδεδεμένος στο Internet, θα συνειδητοποιήσουμε ότι τα επεισόδια ασφάλειας αυξάνονται με ρυθμό 50% ετησίως και όχι με ρυθμό 100%, που φαίνεται από τους αριθμούς. Ωστόσο από το 2003 και μετά αυτή η αύξηση των επιθέσεων τείνει να μειωθεί.

Στην εικόνα που ακολουθεί φαίνεται συνοπτικά η εξέλιξη των μηχανισμών ασφαλείας στους υπολογιστές.



Εικόνα 1 - Εξέλιξη ασφάλειας υπολογιστών

Το πρόβλημα της ασφάλειας των πληροφοριών είναι ιδιαίτερα σημαντικό στα σύγχρονα δίκτυα υπολογιστών. Η χρησιμοποίηση όλο και πιο προχωρημένων τεχνικών και τεχνολογιών όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων και τα σύγχρονα δίκτυα, προσφέρει αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες, αυξάνει όμως ταυτόχρονα σημαντικά τα προβλήματα τα σχετικά με την προστασία και τη διαθεσιμότητα των πληροφοριών.

Ασφάλεια Ασυρμάτων Δικτύων

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με την ποιότητα και την απόδοση, για την εξασφάλιση της εύρυθμης λειτουργίας μίας επιχείρησης ή ενός οργανισμού. Αυτό είναι ιδιαίτερα σημαντικό στη σημερινή εποχή όπου πλέον το μεγαλύτερο ποσοστό των παρερχομένων υπηρεσιών μιας επιχείρησης στηρίζεται στην πληροφορική.

Η έννοια της ασφάλειας ενός δικτύου υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Επίσης έχει να κάνει με την ικανότητά του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του δικτύου.

Επομένως η ασφάλεια στα δίκτυα υπολογιστών έχει να κάνει με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών του δικτύου καθώς και την λήψη σχετικών μέτρων. Πιο συγκεκριμένα η ασφάλεια στα δίκτυα υπολογιστών σχετίζεται με:

- Πρόληψη (prevention) : Την λήψη δηλαδή μέτρων για να προληφθούν φθορές των μονάδων ενός δικτύου υπολογιστών.
- Ανίχνευση (detection) : Την λήψη μέτρων για την ανίχνευση του πότε, πώς και από ποιον προκλήθηκε φθορά σε μία από τις παραπάνω μονάδες.
- Αντίδραση (reaction) : Την λήψη δηλαδή μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός δικτύου.

Η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών, μπορούν να ορίσουν την ασφάλεια δικτύων και πληροφοριών.

Όμως όταν ένα σύστημα βρίσκεται συνδεδεμένο στο δίκτυο, το κάνει πιο επιρρεπές σε απειλές που προέρχονται και από νόμιμους χρήστες του συστήματος αλλά κυρίως από επίδοξους εισβολείς. Κάθε κόμβος του δικτύου είναι ένα

υπολογιστικό σύστημα με όλα τα γνωστά προβλήματα ασφάλειας. Σε αυτά, έρχεται το δίκτυο να προσθέσει το πρόβλημα της επικοινωνίας μέσω ενός πολύ εκτεθειμένου μέσου και της προσπέλασης από μακρινές τοποθεσίες μέσω πιθανώς μη-έμπιστων υπολογιστικών συστημάτων. Μερικοί λόγοι για τους οποίους αποκτούν ιδιαίτερη σημασία τα θέματα ασφάλειας δικτύων υπολογιστών είναι οι εξής:

- Η αυξημένη περιπλοκότητα η οποία περιορίζει το αίσθημα εμπιστοσύνης για την ασφάλεια των δικτύων.
- Αύξηση στον αριθμό των διαύλων επικοινωνίας επομένως και των πιθανών σημείων επίθεσης, τα οποία πρέπει να οχυρωθούν κατάλληλα.
- Τα ασαφή όρια των δικτύων και οι διακρίσεις μεταξύ των τμημάτων μιας επιχείρησης. Κάθε κόμβος οφείλει να είναι ικανός να αντιδράσει σωστά στη παρουσία ενός νέου και μη-έμπιστου κόμβου. Από την άλλη, κάθε κόμβος μπορεί να ανήκει ταυτόχρονα σε περισσότερα από ένα δίκτυα, με αποτέλεσμα να μην είναι ξεκάθαρη η εικόνα των νομίμων χρηστών του κάθε δικτύου.
- Η δυνατότητα ανωνυμίας ενός χρήστη απαιτεί ισχυρούς μηχανισμούς πιστοποίησης μεταξύ των υπολογιστών, που συνήθως είναι διαφορετικοί από αυτούς που πιστοποιούν τους χρήστες στα υπολογιστικά συστήματα.
- Υπάρχει αδυναμία ελέγχου της δρομολόγησης των δεδομένων που διακινούνται μέσω των δικτύων.

Όπως είναι αναμενόμενο, η λήψη των απαραίτητων μέτρων ασφάλειας δημιουργεί κάποια πρόσθετη επιβάρυνση στην απόδοση και το κόστος λειτουργίας του δικτύου υπολογιστών μιας επιχείρησης. Μάλιστα πολλές φορές το κόστος της ασφάλειας εμφανίζεται και ως κόστος χρόνου και ως κόστος χρήματος επομένως, μπορεί να θεωρηθεί ότι η ασφάλεια βρίσκεται σε σχέση αντιστρόφως ανάλογη με την αποδοτικότητα του δικτύου υπολογιστών μιας επιχείρησης. Αυτό όμως δεν είναι σωστό εφόσον η ασφάλεια είναι κόστος αναγκαίο για την ομαλή και εύρυθμη λειτουργία του.

Το συγκεκριμένο κόστος εξαρτάται και προκύπτει από την εκάστοτε ακολουθούμενη πολιτική ασφάλειας της επιχείρησης. Απαιτείται συνεπώς μια πολιτική ασφαλείας η οποία θα πρέπει να εξισορροπεί το κόστος εισαγωγής ασφάλειας από την μία πλευρά και το κόστος ζημιών από πιθανολογούμενο κίνδυνο από την άλλη. Επίσης, θα πρέπει να δημιουργούνται τέτοιες συνθήκες ασφάλειας ώστε να μη παρεμποδίζεται η ευελιξία και η ανάπτυξη της επιχείρησης.

Η αναγκαία πολιτική ασφάλειας καθορίζεται από μία δυναμική εκτίμηση του κόστους των μέτρων ασφάλειας σε σχέση με τις συνέπειες που θα έχει για τον οργανισμό οποιαδήποτε πρόκληση δυσλειτουργίας. Ο βασικός αυτός κανόνας ισχύει για όλους τους τομείς και όλα τα επίπεδα ασφάλειας. Έτσι, σε κάθε περίπτωση όπου απαιτείται η λήψη κάποιου μέτρου ασφάλειας, πρέπει να εξετάζεται η πιθανότητα να συμβεί κάποιο πρόβλημα ασφάλειας, σε σχέση με τις συνέπειες που αυτό θα δημιουργήσει. Εάν η τιμή των δύο αυτών παραμέτρων είναι υψηλή, τότε πρέπει απαραίτητα να ληφθούν μέτρα, ανεξάρτητα από το κόστος πρόληψης.

Τέλος, πρέπει να σημειωθεί ότι η ασφάλεια χαρακτηρίζεται από την φύση της ως δυναμική παράμετρος και όχι στατική, καθώς η τεχνολογία, ο ανταγωνισμός, η πολυπλοκότητα των πληροφοριακών συστημάτων και η ολοένα βελτιωμένη επιτηδειότητα των ‘επιτιθέμενων’, απαιτούν τη λήψη νέων και συνεχώς αυστηρότερων μέτρων ασφάλειας. Συνεπώς, η ακολουθούμενη πολιτική ασφαλείας θα πρέπει να επανεξετάζεται τακτικά και να διορθώνεται όπου αυτό κρίνεται απαραίτητο.

Εικόνα 2 – Ασφαλές Δίκτυο

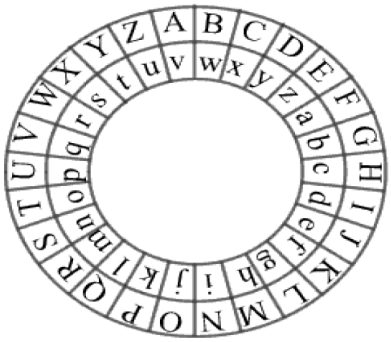
2.2 Κρυπτογραφία

Η λέξη κρυπτογραφία (cryptography) προέρχεται από τις ελληνικές λέξεις «κρυφή γραφή». Γενικά με τον όρο κρυπτογραφία εννοείται η μελέτη μαθηματικών τεχνικών οι οποίες έχουν σαν στόχο να εξασφαλίσουν θέματα που σχετίζονται άμεσα με την ασφάλεια που απαιτείται για τη μετάδοση των πληροφοριών, όπως είναι η εμπιστευτικότητα, η πιστοποίηση ταυτότητας του αποστολέα και να διασφαλισθεί το αδιάβλητο της πληροφορίας. Η κρυπτογραφία πρέπει να εξασφαλίσει την επίτευξη κάποιων βασικών στόχων όπως να φτάσουν τα μηνύματα στον σωστό προορισμό, να

μπορέσει ο παραλήπτης να πιστοποιήσει την ταυτότητα του αποστολέα και η πληροφορία να μην έχει αλλοιωθεί από κάποια μη εξουσιοδοτημένη οντότητα.

Η κρυπτογραφία έχει μεγάλη και εντυπωσιακή ιστορία που φθάνει χιλιάδες χρόνια πίσω, και πιο συγκεκριμένα το πρώτο κρυπτογραφημένο κείμενο χρονολογείται το 1500π.Χ. στη Βαβυλώνα. Η κρυπτογραφία ξεκίνησε με την λογική τα κείμενα που μετέφεραν οι αγγελιοφόροι να μην μπορούν να τα διαβάσουν ούτε αυτοί αλλά ούτε και οι μη εγκεκριμένοι παραλήπτες. Επομένως ο Ιούλιος Καίσαρας επειδή δεν εμπιστευόταν τους αγγελιοφόρους του, εφάρμοσε ένα σύστημα κρυπτογράφησης. Πιο συγκεκριμένα, αναφέρεται ότι αντικαθιστούσε κάθε γράμμα του μηνύματος με ένα άλλο που ήταν τρεις θέσεις μπροστά στο ρωμαϊκό αλφάβητο. Την μέθοδο της κρυπτογραφίας την βλέπουμε και στο Β' Παγκόσμιο Πόλεμο όπου οι Γερμανοί ανέπτυξαν το σύστημα enigma για να μεταδίδουν απόρρητες πληροφορίες. Οι Βρετανοί τότε επιστράτευσαν γνωστούς μαθηματικούς οι οποίοι κατάφεραν να σπάσουν τον κώδικα και να διαβάσουν τα μηνύματα.

Μέχρι την έλευση των υπολογιστών, ένας από τους κύριους περιορισμούς στην κρυπτογραφία ήταν η ικανότητα του υπαλλήλου κώδικα να εκτελεί τους απαιτούμενους μετασχηματισμούς, συχνά στο πεδίο της μάχης και με λίγο εξοπλισμό. Ένας πρόσθετος περιορισμός ήταν η δυσκολία μετάβασης από τη μία κρυπτογραφική μέθοδο σε μία άλλη, αφού κάτι τέτοιο απαιτεί εκ νέου εκπαίδευση μεγάλου πλήθους ανθρώπων. Ωστόσο ο κίνδυνος να συλληφθεί ένας υπάλληλος κώδικα από τον εχθρό ένα κρίσιμη τη δυνατότητα άμεσης αλλαγής της κρυπτογραφικής μεθόδου, όταν χρειαζόταν κάτι τέτοιο.

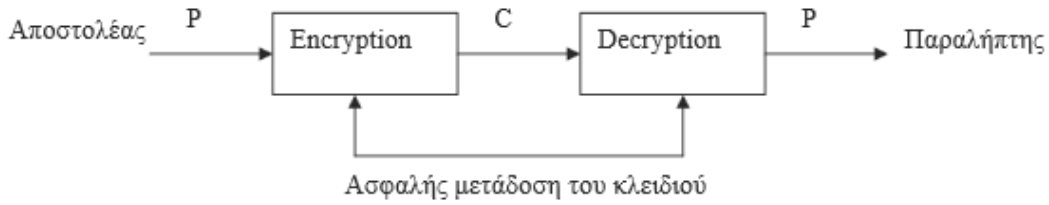


Εικόνα 3 – Αρχαία Μέθοδος Κρυπτογράφησης

2.2.1: Ορισμοί Κρυπτογραφίας

Ακολούθως δίνονται κάποιοι από τους πιο γνωστούς ορισμούς για την κρυπτογραφία:

- Κρυπτογραφία: Η επιστήμη, αλλά και η τέχνη, η οποία έχει ως αντικείμενο την εξεύρεση μεθόδων για το μετασχηματισμό των κειμένων έτσι ώστε να είναι αναγνωρίσιμα μόνο από εξουσιοδοτημένα άτομα.
- Κρυπτογράφηση – Encryption: Η διαδικασία μετατροπής ενός κειμένου από την αρχική του μορφή σε μη αναγνωρίσιμη ή μη επεξεργάσιμη μορφή.
- Αποκρυπτογράφηση – Decryption: Η διαδικασία με την οποία το κρυπτογραφημένο κείμενο μετασχηματίζεται στην αρχική του, αναγνωρίσιμη ή/ και επεξεργάσιμη μορφή
- Αρχικό κείμενο, είναι το κείμενο που θέλουμε να κρυπτογραφήσουμε .
- Κρυπτογραφημένο κείμενο ή κρυπτογράφημα ονομάζεται αυτό που προκύπτει μετά την κρυπτογράφηση.
- Αλγόριθμος κρυπτογράφησης ονομάζεται η μέθοδος που χρησιμοποιείται και μετατρέπει το αρχικό κείμενο σε μυστική μορφή.
- Κλειδί κρυπτογράφησης ονομάζεται η αναλυτική περιγραφή της μεθόδου κρυπτογράφησης, για παράδειγμα είναι η αντιστοιχία των γραμμάτων του αρχικού κειμένου και του κρυπτογραφήματος.



Εικόνα 4 – Μυστικό κλειδί

2.3 Πρωτόκολλα κρυπτογράφησης ασύρματων δικτύων

Από την έρευνα που πραγματοποιήθηκε σε κεντρικές περιοχές της πόλης των Αθηνών, ακόμη και σήμερα, παρατηρήθηκε ότι είναι αρκετά τα δίκτυα που δεν χρησιμοποιούν κανενός είδους κρυπτογράφηση. Σε αυτά τα ανασφάλιστα δίκτυα είναι προφανές ότι δεν μπορεί να υπάρξει καμία προστασία στους χρήστες που είναι συνδεδεμένοι, στην πληροφορία που ανταλλάσουν, καθώς και στα αποθηκευμένα

δεδομένα στο εσωτερικό του δικτύου. Η κρυπτογράφηση των ασύρματων δικτύων μπορεί να χωριστεί σε δύο βασικές κατηγορίες:

- WEP: Χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης RC4, για τον οποίο πλέον υπάρχουν διαδεδομένες τεχνικές εύρεσης του μυστικού κλειδιού. Στην οικογένεια
- WPA/WPA2: Θεωρείται το πιο ασφαλές πρωτόκολλο κρυπτογράφησης. Αντικατέστησε το ανασφαλές WEP και χρησιμοποιεί τον αλγόριθμο CCMP, ο οποίος βασίζεται στον AES.

2.4 Κρυπτογράφηση WEP

Ο τομέας της ασφάλειας των επικοινωνιών θέτει τους ακόλουθους τρεις σημαντικούς στόχους:

- Εμπιστευτικότητα: με τον όρο αυτό περιγράφεται η προστασία των δεδομένων από την πρόσβαση μη εξουσιοδοτημένων χρηστών.
- Ακεραιότητα: η διασφάλιση ότι το στοιχείο δεν έχει τροποποιηθεί.
- Επικύρωση: η υποστήριξη οπουδήποτε μηχανισμού ασφάλειας της αξιοπιστίας των δεδομένων.

Το πρωτόκολλο κρυπτογράφησης WEP παρέχει τις διαδικασίες που βοηθούν στην επιτυχία αυτών των στόχων. Η εμπιστευτικότητα και η ακεραιότητα των δεδομένων στο πρωτόκολλο αυτό εξασφαλίζεται συγχρόνως, χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης RC4 (River Cipher 4), μήκους 64 ή 128 bit. Είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης ακολουθίας, ο οποίος δημιουργεί μία ψευδοτυχαία ακολουθία από bit, που συνδυάζεται με το υπό κρυπτογράφηση κείμενο (cipher text) με τη γνωστή συνάρτηση XOR για να παράξει το κρυπτογραφημένο κείμενο. Το κρυπτογραφημένο κείμενο παράγεται χρησιμοποιώντας τα 24 bit του πίνακα αρχικοποίησης (Initialization Vector) και το κλειδί κρυπτογράφησης (pre-shared key) που εισήγαγε ο χρήστης, μήκους 40 ή 104 bit. Το αποτέλεσμα εισάγεται σε μία πύλη XOR μαζί με το αρχικό κείμενο (plain text) ώστε να δημιουργηθεί το τελικό κρυπτογραφημένο κείμενο.

Το πρωτόκολλο WEP χρησιμοποιεί ένα κλειδί μήκους μόνο 40 bit, λόγω περιορισμών που έθεσε η Αμερικάνικη κυβέρνηση, το οποίο ευνοεί τις brute force

επιθέσεις. Οι συγκεκριμένες επιθέσεις χρησιμοποιούν όλους τους πιθανούς συνδυασμούς κλειδιών μέχρι να βρεθεί το σωστό, με αποτέλεσμα υπολογιστές με μεγάλη υπολογιστική ισχύ να το σπάσουν πολύ γρήγορα. Όταν οι περιορισμοί κάμφθηκαν, όλοι οι κατασκευαστές προσπάθησαν να το διορθώσουν. Επέκτειναν το μήκος του κλειδιού στα 128 bit χρησιμοποιώντας κλειδί κρυπτογράφησης μήκους 104 bit. Αυτό δεν άλλαξε τον τρόπο επίθεσης, αλλά λόγω της μεγάλης υπολογιστικής ισχύς που χρειάζονταν, καθιστά τις brute force επιθέσεις δυσκολότερες.

Η επικύρωση εξασφαλίζεται μέσω του ελέγχου των πακέτων. Ο αλγόριθμος CRC32 αναπτύχθηκε για να εντοπίζει, να επισημαίνει και πολλές φορές να διορθώνει τα λάθη κατά τη μετάδοση των πακέτων.

2.4.1 Ασφάλεια στο WEP

Η κρυπτογράφηση του πρωτοκόλλου WEP έχει μειωμένα επίπεδα ασφαλείας, γεγονός που το κάνει ιδιαίτερα ευάλωτο σε επιθέσεις. Το μήκος του IV είναι μόλις 24 bit, τα οποία θεωρούνται λίγα για να εξασφαλιστεί η εμπιστευτικότητα των δεδομένων. Η τιμή ελέγχου ακεραιότητας (ICV) δεν παρέχει την απαιτούμενη ασφάλεια και δεν αποτρέπει την τροποποίηση των μηνυμάτων από κάποιον εισβολέα. Επιπλέον, το WEP συνδυάζει το κλειδί της κρυπτογράφησης με το IV, με τέτοιο τρόπο ώστε ο οποιοσδήποτε μπορεί να αποκτήσει το κλειδί της κρυπτογράφησης χρησιμοποιώντας μερικά εκατομμύρια κρυπτογραφημένα πακέτα. Επιπλέον δεν παρέχεται προστασία της ακεραιότητας των διευθύνσεων του αποστολέα και του παραλήπτη.

Οι επιθέσεις στοχεύουν στον πίνακα αρχικοποίησης (IV), ο οποίος εκπέμπεται συνεχώς μαζί με τα πακέτα. Τη στιγμή που θα επανεκπεμφθεί ο ίδιος πίνακας σε δύο διαφορετικά πακέτα, μπορούμε μέσω της XOR να βρούμε κομμάτια του αρχικού κειμένου. Τμηματικά θα αποκαλυφθεί όλο το μη-κωδικοποιημένο κομμάτι του μηνύματος. Επειδή ο χρόνος εκπομπής του πίνακα αρχικοποίησης δεν είναι ίδιος, έχουν αναπτυχθεί διάφορες τεχνικές για την επιτάχυνση της. Η πιο συνηθισμένη τεχνική είναι ο εξαναγκασμός του σταθμού να εκπέμψει πάλι το πακέτο είτε λόγω απώλειας, είτε απόρριψης, είτε στέλνοντας πακέτα NACK. Με αυτή τη τεχνική, ο σταθμός αναγκάζεται να εκπέμπει συνεχώς, μειώνοντας έτσι ταχύτατα το διαθέσιμο εύρος τιμών του, με αποτέλεσμα σε σύντομο χρονικό διάστημα να επανεκπεμφθεί ο ίδιος πίνακας.

Η ακεραιότητα των δεδομένων δεν είναι καλά προστατευμένη στο WEP, διότι ο αλγόριθμος CRC προστατεύει μόνο από τυχαία λάθη που συμβαίνουν κατά τη μετάδοση. Γι αυτό το λόγο τα κρυπτογραφημένα πακέτα μπορούν να αλλοιωθούν ή να υποκλαπούν. Οι εταιρείες αναγκάστηκαν να προβούν σε διορθώσεις του πρωτοκόλλου. Νέες εκδόσεις αναπτύχθηκαν για να εξαλειφθούν τα ελαττώματα του. Η πρώτη αναβάθμιση έγινε με την έκδοση WEP2 η οποία αύξησε το μέγεθος του πίνακα αρχικοποίηση στα 128 bit. Ως αποτέλεσμα, αυξήθηκε ο χρόνος επανεκπομπής του ίδιου πίνακα αρχικοποίησης. Στη συνέχεια ακολούθησαν ακόμα δύο αναβαθμίσεις, το WEPplus (WEP+) και το Dynamic WEP.

2.5 WPA(Wi-Fi Protected Access)

Το 2004 το πρότυπο IEEE με την έκδοση 802.11i ανέπτυξε ένα καινούργιο πρωτόκολλο ασφάλειας για ασύρματη προστατευμένη πρόσβαση, το WPA (Wi-Fi Protected Access). Ουσιαστικά είναι ο αντικαταστάτης του WEP, διότι υπήρχε η ανάγκη στις ασύρματες μεταδόσεις για περισσότερη ασφάλεια. Αποτέλεσε μία ενδιάμεση λύση έως την πλήρη ανάπτυξη της έκδοσης 802.11i με το πρωτόκολλο WPA2. Η WPA κρυπτογράφηση βελτιώνει την WEP και προσθέτει έναν ισχυρό μηχανισμό αυθεντικοποίησης. Η αυθεντικοποίηση των χρηστών γίνεται με δύο τρόπους λειτουργίας:

- Μέσω της WPA-Personal ή WPA-PSK ο χρήστης συνδέεται σε ένα Access Point και η αυθεντικοποίηση γίνεται μέσω προ-μοιρασμένων κλειδιών (Pre-Shared keys). Επακόλουθο είναι ότι για την καλύτερη ασφάλεια των συνδέσεων παίζει ρόλο το μήκος και η πολυπλοκότητα του κλειδιού.
- Η ασφαλέστερη λειτουργία εκτελείται με την υλοποίηση WPA-Enterprise, η οποία προϋποθέτει την ύπαρξη ενός 802.1x server, μέσω του οποίου ανά τακτά χρονικά διαστήματα, γίνεται ο διαμοιρασμός διαφορετικών κλειδιών για κάθε υπολογιστή, με αποτέλεσμα το σύστημα να είναι πιο ασφαλές, πιο πολύπλοκο και με μεγαλύτερο κόστος.

Εικόνα 5 – Ασφαλές Δίκτυο Wi-Fi

2.5.1 Ασφάλεια στο WPA

Το WPA χρησιμοποιεί τον RC4 αλγόριθμο, ο οποίος αποτελείται από τον πίνακα αρχικοποίησης μήκους 48 bit και ένα κλειδί χρονικής κρυπτογράφησης μήκους 128 bit. Η ύπαρξη του RC4 και στην καινούργια έκδοση εξασφαλίζει συμβατότητα με τις προηγούμενες εκδόσεις προϊόντων ασύρματης δικτύωσης. Επιπλέον, το WPA εισάγει ένα νέο πρωτόκολλο χρονικής ακεραιότητας κλειδιού, το TKIP (Temporal Key Integrity Protocol), το οποίο αναλαμβάνει δυναμικά την ανανέωση των κλειδιών κατά τη διάρκεια της σύνδεσης. Για να μειωθεί το ποσοστό επανάληψης του ίδιου κλειδιού, χρησιμοποιείται ανά εκπεμπόμενο πακέτο μία ακολουθία αριθμών, το pre-shared key και η εκπεμπόμενη MAC address.

Στο νέο κλειδί που δημιουργείται προστίθεται ο πίνακας αρχικοποίησης και παράγεται μία νέα ακολουθία κλειδιού (keystream). Για την ενίσχυση της ακεραιότητας των πακέτων έχει προστεθεί ένα πεδίο ελέγχου της ακεραιότητας των δεδομένων, το MIC (Message Integration Check). Η τιμή του MIC υπολογίζεται από τον κρυπτογραφικό αλγόριθμο Michael και προστατεύονται το μήνυμα και οι διευθύνσεις του αποστολέα και παραλήπτη. Ένα επιπλέον χαρακτηριστικό είναι ότι υποστηρίζει έναν ειδικό μηχανισμό, ο οποίος ανιχνεύει οποιαδήποτε προσπάθεια παραβίασης του TKIP, με αποτέλεσμα το μπλοκάρισμα της επικοινωνίας.

2.5.2 Αυθεντικοποίηση στο WPA

Αυθεντικοποίηση στο WPA Η αυθεντικοποίηση στο πρωτόκολλο κρυπτογράφησης WPA-Personal ή WPA- PSK έχει σχεδιαστεί για επαγγελματική και οικιακή χρήση. Με αυτή τη μέθοδο η αυθεντικοποίηση των χρηστών γίνεται μέσω του Access Point χρησιμοποιώντας μία φράση 8 έως 63 ASCII χαρακτήρες. Όταν επιλεγούν οι ASCII χαρακτήρες, μία hash function αναλαμβάνει τη μείωση από τα 504 bit (63characters * 8bit) στα 256 bit. Ακολούθως το σημείο πρόσβασης παρέχει στο σταθμό ένα προσωρινό κλειδί το οποίο ανανεώνεται σε τακτά χρονικά διαστήματα. Το 256 bit κλειδί υπολογίζεται χρησιμοποιώντας τη hash συνάρτηση PBKDF2 χρησιμοποιώντας τον αρχικό κωδικό ως κλειδί.

2.6 WEP vs. WPA

Τα πρωτόκολλα κρυπτογράφησης WPA και WEP χρησιμοποιούν τον αλγόριθμο RC4 για κρυπτογράφηση. Ωστόσο, το WEP χρησιμοποιεί πίνακα αρχικοποίησης μήκους 24 bit με κλειδί κρυπτογράφησης μήκους 40 ή 104 bit, σε αντίθεση με το WPA που χρησιμοποιεί 48 bit IV με 128 bit κλειδί κρυπτογράφησης. Το WEP είναι ανεπαρκές για ασφάλεια, διότι οι επιθέσεις στοχεύουν στον πίνακα αρχικοποίησης και στις αλλοιώσεις των πακέτων. Στο WPA έχουν ελαχιστοποιηθεί τέτοιου είδους επιθέσεις εξαιτίας του συνδυασμού του πρωτοκόλλου TKIP, του MIC και του μεγαλύτερου μήκους πίνακα αρχικοποίησης. Το κλειδί TKIP χρησιμοποιεί περίπου 300 τρισεκατομμύρια πιθανά κλειδιά για την κρυπτογράφηση του πακέτου. Συνδυάζοντας το με τον 48 bit πίνακα αρχικοποίησης, το TKIP συμβάλλει στην αποτελεσματική ασφάλεια του δικτύου στις επιθέσεις ανάκτησης κλειδιού. Επίσης, το MIC βάζει ένα τέλος στην υποκλοπή πακέτων.

Το WPA-Enterprise και η WPA-PSK κρυπτογράφηση παρέχουν έναν ισχυρό μηχανισμό ασφάλειας, ο οποίος έλειπε από το WEP. Στο WEP η αυθεντικοποίηση του χρήστη γινόταν με τον διαμοιρασμό ενός κοινού κλειδιού. Στο WPA η αυθεντικοποίηση και η κρυπτογράφηση είναι ξεχωριστές λειτουργίες. Η αυθεντικοποίηση στον 802.1x server γίνεται με credentials, και τα κλειδιά διανέμονται αυτόματα.

2.7 WPA2 (Wi-Fi Protected Access Version 2)

Το πρωτόκολλο κρυπτογράφησης WPA2 είναι ο διάδοχος του WPA. Αποτελεί μέρος του προτύπου 802.11i. Η κρυπτογράφηση γίνεται με τον αλγόριθμο CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), ο οποίος για την ανάπτυξή του βασίστηκε στο CCM (Counter Mode with CBC-MAC) του αλγορίθμου AES (Advanced Encryption Standard), για την προστασία της ιδιωτικότητας.

Με την είσοδο του νέου αλγορίθμου αντικαταστάθηκε ο RC4. Όπως το TKIP, έτσι και ο CCMP χρησιμοποιεί πίνακα αρχικοποίησης 48 bit, αλλά αντί για την ακολουθία αριθμών ανά πακέτο χρησιμοποιεί AES κλειδιά για την προστασία της εμπιστευτικότητας και ακεραιότητας του πακέτου. Χρησιμοποιεί πίνακα αρχικοποίησης 48 bit με 128 bit κλειδί κρυπτογράφησης το οποίο ελαχιστοποιεί την ευπάθεια του συστήματος σε επαναλαμβανόμενες επιθέσεις. Η ενισχυμένη προστασία που παρέχει το CCMP σε σύγκριση με το TKIP απαιτεί μεγαλύτερη επεξεργαστική ισχύ, και συχνά χρειάζεται νέο ή αναβαθμισμένο hardware.

ΚΕΦΆΛΑΙΟ 3: ΕΠΙΘΕΣΕΙΣ

3.1 Γενικά στοιχεία του όρου Επίθεση

Επίθεση είναι οποιαδήποτε προσπάθεια για παραβίαση της εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας ενός συστήματος ή ενός δικτύου. Επίσης είναι οποιαδήποτε μη εξουσιοδοτημένη ενέργεια που έχει σκοπό να εμποδίσει, να παρακάμψει ή να αχρηστεύσει τους μηχανισμούς ασφάλειας και ελέγχου πρόσβασης ενός συστήματος ή ενός δικτύου.

Ο στόχος μίας επίθεσης ποικίλει ανάλογα με τις ικανότητες και τους σκοπούς του κάθε επιτιθέμενου, καθώς και τον βαθμό δυσκολίας της υλοποίησης της επίθεσης όσο αναφορά τα μέτρα ασφάλειας που πρέπει να αντιμετωπιστούν. Παρόλα αυτά οι πιο συνήθεις στόχοι μίας επίθεσης μπορεί να είναι:

- Μικρά τοπικά δίκτυα LAN'S
- Πανεπιστήμια
- Κυβερνητικά Sites ή διάφοροι μεγάλοι οργανισμοί

Μία επίθεση σε κάποιο δίκτυο ή σύστημα θα μπορεί να συμβεί οποιαδήποτε στιγμή αυτό είναι συνδεδεμένο στο Internet. Τα σημερινά δίκτυα συνήθως συνδέονται στο Internet 24 ώρες την ημέρα. Η καταλληλότερη ώρα για να γίνει μια επίθεση, εφόσον γίνεται από κάποιον απομακρυσμένο χρήστη, είναι αργά το βράδυ σε σχέση με την τοποθεσία το στόχου.

Εικόνα 6 – Επίθεση σε wi-fi

3.2 Ποιοι Εξαπολύουν Επιθέσεις

Οι επιθέσεις πραγματοποιούνται από άτομα που έχουν πρόσβαση στους στόχους τους μέσω του Internet, από εξουσιοδοτημένους χρήστες που προσπαθούν να αποκτήσουν περισσότερα δικαιώματα από αυτά που τους έχουν δοθεί και από

εξουσιοδοτημένους χρήστες οι οποίοι εκμεταλλεύονται τα δικαιώματα που τους έχουν δοθεί με κακό σκοπό.

Συνήθως αυτοί που πραγματοποιούν τις επιθέσεις είναι γνωστοί ως **Hackers** ή **Crackers**. Παρόλο που αυτοί ο όροι λανθασμένα χρησιμοποιούνται κατά κόρον για να χαρακτηριστούν οι κακόβουλοι χρήστες, υπάρχουν διάφορες απόψεις που διαφοροποιούν την σημασία των δύο όρων. Η πιο κοινά αποδεκτή προσέγγιση για τον διαχωρισμό των δύο παραπάνω εννοιών είναι η παρακάτω:

Hackers θεωρούνται αυτοί που συνεχώς προσπαθούν να διευρύνουν την γνώση τους γύρω από τον τρόπο λειτουργίας, οπουδήποτε υπολογιστικού συστήματος, λειτουργικού συστήματος ή λογισμικού γενικότερα. Μέσα από εξαντλητική χρήση των παραπάνω και εξέταση των λειτουργιών τους σε βάθος, εντοπίζουν διάφορα ελαττώματα και ατέλειες που μπορεί αυτά να έχουν, τις οποίες γνωστοποιούν στο ευρύ κοινό ώστε να διορθωθούν από τους αρμόδιους. Συνήθως οι Hackers έχουν ανεπτυγμένες προγραμματιστικές ικανότητες και ευρεία γνώση και ενθουσιασμό για αυτό που κάνουν. Σημαντικό χαρακτηριστικό των Hackers είναι ότι διαχέουν την γνώση που προκύπτει από την δραστηριότητά τους και σε καμία περίπτωση με τις ενέργειές τους δεν προκαλούν εθελημένα κάποια ζημιά σε άλλους.

Crackers είναι οι Hackers που χρησιμοποιούν τις ικανότητές τους με κακόβουλους σκοπούς. Παραβιάζουν συστήματα στα οποία δεν έχουν εξουσιοδοτημένη πρόσβαση και προκαλούν προβλήματα σε αυτά και στους νόμιμους χρήστες τους.

Συνήθως οι Hackers είναι γνωστοί και σαν Whitehats ενώ οι Crackers σαν Blachats.

- Γνωρίζει να προγραμματίζει και να κατανοεί προγράμματα σε C ,C++ και Perl, κυρίως γιατί τα περισσότερα εργαλεία ασφάλειας είναι γραμμένα σε αυτές τις γλώσσες.
- Έχει αρκετή γνώση για το πώς δουλεύει το TCP/IP και γενικότερα το Internet.
- Χρησιμοποιεί το Internet πολλές ώρες τον μήνα και έχει πλήρη γνώση του συστήματός του.
- Γνωρίζει καλά την χρήση και τον τρόπο λειτουργίας τουλάχιστον δύο λειτουργικών συστημάτων, το ένα από τα οποία είναι το Unix ή το VMS. Το είδος των λειτουργικών συστημάτων που συνήθως οι επιτιθέμενοι χρησιμοποιούν έχει να κάνει με το κόστος απόκτησής τους και τις

δυνατότητες που τους προσφέρουν για να πραγματοποιήσουν τις ενέργειές τους.

3.3 Επιθέσεις σε Δίκτυα Wi-Fi

Το φυσικό μέσο μετάδοσης σε ένα δίκτυο Wi-Fi είναι η ατμόσφαιρα, όπου καθιστά το δίκτυο ευάλωτο σε επιθέσεις. Ως επίθεση ορίζεται η μη εξουσιοδοτημένη παρέμβαση στο δίκτυο, στην ασφάλεια της μεταδιδόμενης πληροφορίας αλλά και διακύβευση υποκλοπής της. Λόγοι επίθεσης σε κάποιο Wi-Fi δίκτυο μπορεί να είναι απλή περιέργεια γα προσπάθεια πρόσβασης σε κάποιο ξένο δίκτυο, κλοπή πληροφοριών, έλεγχο κίνησης ή απλά δωρεάν πρόσβαση, μέσω του υπάρχοντος wi-fi δικτύου, στο διαδίκτυο.

Οι προθέσεις και οι στόχοι κάθε επίθεσης μπορεί να διαφέρουν και γενικά οι επιθέσεις σε ασύρματα δίκτυα μπορούν να χωριστούν σε **παθητικές** και **ενεργητικές.** Ως **παθητικές** ορίζονται οι επιθέσεις που δε συμπεριλαμβάνουν συμμετοχή του επιτιθέμενου στο δίκτυο και τέτοιου τύπου επίθεση αποτελεί η Λήψη Πληροφοριών (Snooping/Footprinting). Οι **ενεργητικές** επιθέσεις προϋποθέτουν ότι ο επιτιθέμενος αναλαμβάνει ενεργή συμμετοχή στο δίκτυο και χωρίζονται, σύμφωνα με το σκοπό που έχουν οι επιτιθέμενοι, σε τέσσερις βασικές κατηγορίες:

- Ανάκτηση κωδικού WEP (WEP Cracking)
- Τροποποίηση Δεδομένων (Man in the Middle Attack)
- Μεταμφίεση (Spoofing)
- Άρνηση Υπηρεσιών (Denial of Service)

3.3.1 Παθητικές Επιθέσεις

Η λήψη πληροφοριών (snooping) σχετίζεται με την ανάκτηση απόρρητων προσωπικών δεδομένων από μη εξουσιοδοτημένους χρήστες. Σε αυτή την περίπτωση για να αντιμετωπισθούν τυχόν επιθέσεις, επιβάλλεται μία ασφαλής μέθοδος κρυπτογράφησης. Ο επιτιθέμενος μπορεί να διαβάσει όλες τις πληροφορίες που προέρχονται από τα σημεία πρόσβασης, επομένως ξέρει το όνομα δικτύου (ή SSID) και είναι πιθανό να προσδιορίσει τον κατασκευαστή κάθε σημείου πρόσβασης με την εξέταση της διεύθυνσης MAC. Η παρακολούθηση της πορείας μιας μεγάλης ποσότητας πακέτων προς σημεία πρόσβασης, μπορεί να δώσει τον αριθμό των

ασύρματων συσκευών που συνδέονται με κάθε σημείο πρόσβασης. Εάν στο δίκτυο χρησιμοποιείται κρυπτογράφηση WEP, τότε μπορεί να εξετάσει εάν ο καθένας χρησιμοποιεί το ίδιο κλειδί ή αν κάθε συσκευή έχει ένα ξεχωριστό κλειδί με την εξέταση των bit στην IEEE 802.11 επιγραφή.

Μπορεί να χρησιμοποιηθεί μία άλλη μέθοδος η τεχνική της ανάλυσης κυκλοφορίας. Η ανάλυση κυκλοφορίας αποτελεί τη μελέτη των εξωτερικών στοιχείων των μηνυμάτων, όπως για παράδειγμα τη συχνότητα επικοινωνίας και το μέγεθος του μηνύματος. Δυστυχώς, είναι δυνατό να μαθευτεί ολόκληρο ή ένα μέρος για τους τύπους των πραγμάτων που συμβαίνουν σε ένα δίκτυο ακριβώς με την προσοχή των μηκών πακέτων και τη σημείωση του συγχρονισμού χωρίς κοίταγμα μέσα στα πακέτα. Παρόλα αυτά δεν υπάρχει άμεση πρόσβαση στο περιεχόμενο μηνυμάτων. Ένα πολύ χρήσιμο εργαλείο που χρησιμοποιείται στην ανάλυση, παρακολούθηση και στον εντοπισμό και αντιμετώπιση προβλημάτων στα δίκτυα αλλά και στην εκπαίδευση είναι το Wireshark.

3.3.2 Ενεργητικές Επιθέσεις

Όπως αναφέραμε προηγουμένως, η μέθοδος κρυπτογράφησης του WEP έχει χάσει την παλιά της ποιότητα, εφόσον μέσα σε λίγα λεπτά μπορεί να ανακτηθεί ο μυστικός κωδικός που χρειάζεται για την παραβίαση ενός ασύρματου δικτύου. Οι μέθοδοι που χρησιμοποιούνται σήμερα για το WEP Cracking επικεντρώνονται στην συλλογή μεγάλου ποσοστού IV's πακέτων. Η διαδικασία αυτή πραγματοποιείται μέσω της συλλογής και αναμετάδοσης πακέτων ARP (Address Resolution Protocol) στο σημείο πρόσβασης.

Το Address Resolution Protocol (ARP) (πρωτόκολλο επίλυσης διευθύνσεων) χρησιμοποιείται με σκοπό να βρεθεί μια διεύθυνση του στρώματος συνδέσμου (link layer) ή διεύθυνση εξοπλισμού (hardware address) ενός host με βάση μια διεύθυνση του επιπέδου επικοινωνίας (network layer). Κάθε host που είναι συνδεδεμένος σε ένα δίκτυο που βασίζεται στο ARP κρατάει έναν κατάλογο (ARP table) ζεύγων.

Τα ερωτήματα ARP στέλνονται με broadcast, που σημαίνει πως διάφοροι host τα λαμβάνουν. Σε γενικές γραμμές η επίθεση σε συστήματα WEP πραγματοποιείται μέσω συλλογής είτε αδύναμων είτε μοναδικών IV's πακέτων. Ωστόσο πάντα απαιτείται η συλλογή μεγάλου ποσοστού κρυπτογραφημένων πακέτων. Ενδιαφέρουσα περίπτωση αποτελεί και η μέθοδος "Caffe Latte Attack", με τη βοήθεια της οποίας ο επιτιθέμενος μπορεί να ανακαλύψει το WEP κλειδί του δικτύου

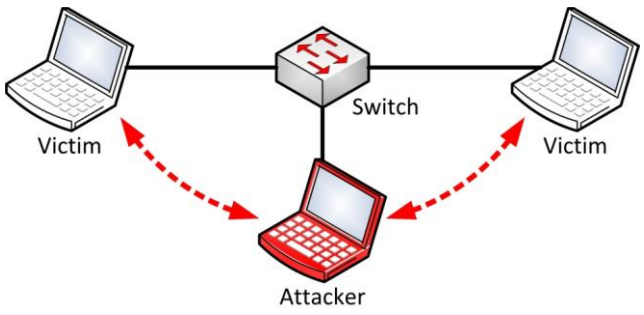
χωρίς να βρίσκεται στην ίδια περιοχή με το δίκτυο – στόχο απλά στοχεύοντας συγκεκριμένους πελάτες σε δημόσιες περιοχές.

3.3.3 Ενεργητικές: Τροποποίηση δεδομένων

Αυτές οι μέθοδοι τροποποίησης δεδομένων έχουν πολλούς διαφορετικούς στόχους, που κυμαίνονται από την τροποποίηση του ηλεκτρονικού ταχυδρομείου με κακόβουλο περιεχόμενο, έως και την αλλαγή αριθμών σε μια ηλεκτρονική τραπεζική μεταφορά. Ωστόσο παρότι τέτοιες υψηλού επιπέδου τροποποιήσεις έχουν πραγματοποιηθεί, είναι αρκετά περιορισμένες στην πράξη λόγω του βαθμού δυσκολίας που έχουν. Η επιγραφή IP είναι ευκολότερο να δεχτεί επίθεση γιατί είναι μια γνωστή μορφή. Μια επίθεση τροποποίησης είναι η Man-in-the-Middle επίθεση (άτομο στην μέση).

- Man in the Middle Attack

  Σε αυτό το είδος της επίθεσης, ο επιτιθέμενος βρίσκεται στη μέση της συνομιλίας δυο συμμετεχόντων στο δίκτυο, Π1 και Π2. Σε μια πραγματική επικοινωνία ο Π1 θα λάμβανε μηνύματα από τον Π2 και ο Π2 από τον Π1. Ο εισβολέας όμως μπορεί να μιμηθεί καθέναν από τους δυο και να στέλνει μηνύματα τα οποία φαίνεται ότι προήλθαν από την πραγματική τους επικοινωνία. Συνήθως τέτοιου είδους επιθέσεις χρησιμοποιούνται για την τροποποίηση μηνυμάτων κατά τη μεταφορά χωρίς να υπάρχει περίπτωση να ανιχνευθούν. Για την εφαρμογή μιας τέτοιας επίθεσης σε ένα ασύρματο δίκτυο υπάρχουν δυο διαφορετικές μέθοδοι, τα πλαίσια διαχείρισης, συγκεκριμένα για την ασύρματη δικτύωση και το ARP Spoofing, το οποίο αποτελεί απειλή ακόμα και για τα ενσύρματα δίκτυα.



Εικόνα 7 – Man In The Middle Attack

3.3.4 Ενεργητικές: Μεταμφίεση (SPOOFING)

Σε αυτού του είδους τις επιθέσεις, ο επιτιθέμενος, υποκρίνεται κάποιον νόμιμο χρήστη του δικτύου ώστε να αποκτήσει τα δικαιώματα πρόσβασης σε υπηρεσίες που επιθυμεί. Στην ουσία χρησιμοποιούνται στοιχεία πρόσβασης ενός νόμιμου χρήστη. Αυτά τα στοιχεία μπορούν να γίνουν βορά στα χέρια ενός επιτιθέμενου στις εξής περιπτώσεις :

- Όταν δεν χρησιμοποιείται κρυπτογράφηση στο δίκτυο
- Όταν χρησιμοποιούνται εύκολοι κωδικοί
- Όταν δεν ακολουθούνται οι κανόνες προστασίας κωδικών πρόσβασης. Η μέθοδος αυτή είναι ιδανική εάν ένας επιτιθέμενος θέλει να μην αποκαλυφθεί. Εάν η συσκευή καταφέρει να ξεγελάσει το δίκτυο ως εξουσιοδοτημένη συσκευή, τότε ο επιτιθέμενος παίρνει όλα τα δικαιώματα πρόσβασης που επιθυμεί από την εξουσιοδοτημένη. Επιπλέον, δεν θα υπάρξει καμία προειδοποίηση ασφάλειας.

3.3.5 Ενεργητικές: άρνηση υπηρεσιών (DENIAL OF SERVICE)

Σκοπός μιας τέτοιας επίθεσης είναι η ολική αχρήστευση του ασύρματου δικτύου για ένα χρονικό διάστημα. Ουσιαστικά αφαιρούνται τα δικαιώματα από όλους τους νόμιμους και μη νόμιμους χρήστες του δικτύου και στόχος είναι η διαταραχή της ομαλής λειτουργίας του δικτύου. Μια τέτοια επίθεση μπορεί να πραγματοποιηθεί με δυο τρόπους. Η πρώτη μέθοδος απλά κατακλύζει το στόχο υπολογιστή ή τη συσκευή υλικού με πληροφορίες ώστε να μπλοκάρει. Σύμφωνα με τη δεύτερη μέθοδος στέλνονται καλά διατυπωμένες εντολές ή λάθος δεδομένα με στόχο να κολλήσει το σύστημα. Οι επιθέσεις αυτού του είδους είναι οι πιο επικίνδυνες διότι υπάρχει μικρότερο περιθώριο προστασίας.

Οι πέντε πιο σημαντικοί τύποι επιθέσεων DOS περιγράφονται παρακάτω:

- Επίθεση πλημμύρας (Flood Attack): Αυτές είναι οι πιο γνωστές του είδους των DoS επιθέσεων. Ο μηχανισμός αυτής της επίθεσης είναι απλός. Ο επιτιθέμενος δημιουργεί στον server περισσότερη κίνηση από αυτή που μπορεί να διαχειριστεί. Εάν όμως ο υπολογιστής – θύμα διαθέτει ένα πολύ καλό bandwidth τότε έχει πολύ καλές πιθανότητες να μην επηρεαστεί. Ωστόσο η αύξηση του bandwidth, δεν είναι από μόνη της μιας επαρκής προστασία ενάντια σε μια τέτοια επίθεση. Παρόλα αυτά, εάν είναι ανεπαρκές, ακόμα και ένας

φυσιολογικός όγκος αιτημάτων μπορεί να οδηγήσει σε μια τέτοια δύσκολη κατάσταση.

- Επίθεση Ping of Death: Η επίθεση Ping of Death είναι μια άλλη παλιότερη μορφή επίθεσης DoS. Η βασική αρχή της δεν είναι τόσο έξυπνη όμως καταφέρνει να εκμεταλλευτεί την αδυναμία του TCP/IP πρωτοκόλλου. Η μέθοδος αυτή απλά στέλνει ένα διάγραμμα δεδομένων, το μέγεθος του οποίου ξεπερνάει τα συνηθισμένα. Όταν ένα τέτοιο διάγραμμα φτάσει στον προορισμό του, το σύστημα που το παραλαμβάνει καταρρέει. Ευτυχώς όμως , τέτοιου είδους επιθέσεις τώρα πια είναι ιστορία επειδή όλοι οι σύγχρονοι εξοπλισμοί διαθέτουν μηχανισμούς άμυνας ενάντια σε τέτοιες επιθέσεις.
- Επίθεση SYN: Οι επιθέσεις SYN εκμεταλλεύονται επίσης αδυναμίες του TCP/IP πρωτοκόλλου. Η εγκαθίδρυση μιας σύνδεσης μέσω του TCP/IP, συμπεριλαμβάνει έναν μηχανισμό χειραψίας, στον οποίο έχουμε ανταλλαγή μηνυμάτων συγχρονισμού (Synchronize) και επιβεβαίωσης (Acknowledgment). Όταν ένας επιτιθέμενος καταφέρει να γεμίσει τον προορισμό με μηνύματα συγχρονισμού (SYN), τότε γεμίζει και ο αποθηκευτικός χώρος τους. Σε αυτή την περίπτωση, δεν είναι δυνατόν να αποσταλούν μηνύματα επιβεβαίωσης (ACK) και κατ' επέκταση δεν είναι δυνατή η δημιουργία TCP/IP συνδέσεων με οποιονδήποτε το επιχειρήσει.
- Επίθεση Teardrop: Στην επίθεση αυτή τα πακέτα που στέλνονται υπερκαλύπτουν το ένα το άλλο με αποτέλεσμα όταν το σύστημα που τα λαμβάνει προσπαθεί να τα συναρμολογήσει (reassembly) παθαίνει κατάρρευση (crash) ή/και «πάγωμα» (hang) ή/και επανεκκίνηση (reboot). Όπως και η Ping of Death, η επίθεση αυτή είναι τώρα πια ιστορία.
- Επίθεση Smurf: Κατά την έναρξη μίας επίθεσης Smurf, ο επιτιθέμενος στέλνει μία πληθώρα πακέτων ping ICMP Echo Request σε διευθύνσεις IP broadcast διαφόρων δικτύων. Τα πακέτα αυτά έχουν τροποποιηθεί κατάλληλα ούτως ώστε στο πεδίο source της κεφαλίδας IP να αναγράφεται η διεύθυνση IP του θύματος και όχι του επιτιθέμενου. Επίσης, δεδομένου ότι στάλθηκαν στην διεύθυνση IP Broadcast των διαφόρων δικτύων, τα λαμβάνουν όλοι οι υπολογιστές που ανήκουν σε αυτά. Αυτό έχει ως συνέπεια όλοι οι υπολογιστές να απαντούν στο ping με πακέτα ICMP Echo Reply, τα οποία έχουν ως διεύθυνση προορισμού την διεύθυνση IP του θύματος. Άρα λοιπόν το θύμα πλημμυρίζει με πακέτα ping και οδηγείται σε κατάρρευση. Οι επιθέσεις αυτές είναι πιο δύσκολα ανιχνεύσιμες,

όμως εάν ένα δίκτυο είναι πολύ καλά οργανωμένο και συντηρείται σωστά, η επίθεση αυτή δε θα είναι καταστροφική. Πριν από αρκετά χρόνια τα περισσότερα δίκτυα υπολογιστών ήταν ευπαθή σε τέτοιου είδους επιθέσεις. Σήμερα όμως έχουν αναπτυχθεί οι κατάλληλες τεχνολογίες ούτως ώστε οι επιθέσεις Smurf να μην αποδίδουν.

ΚΕΦΑΛΑΙΟ 4 : HACKING ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ

4.1 Τι είναι ο Hacker

Hacker ονομάζεται το άτομο το οποίο χρησιμοποιεί τους ηλεκτρονικούς υπολογιστές πιο πολύ ως αντικείμενο μελέτης παρά ως εργαλείο δουλειάς. Κάποτε ο τίτλος hacker θεωρούνταν τιμητικός αλλά τα ΜΜΕ τον μετέτρεψαν σε κάποιον εγκληματία.

Κάποιοι από τους πιο γνωστούς Hackers στο ευρή κοινό του διαδικτύου είναι :

ο Loyd Blankenship με ψευδώνυμο The Mentor,

ο Eric Corley γνωστός επίσης με το ψευδώνυμο Emmanuel Goldstein,

Kevin Mitnick με ψευδώνυμο Condor και ο

Steve Wozniak με ψευδώνυμο Woz, δημιουργός των Apple I και II

4.2 Αρχάριοι του hacking

Αυτό που ζητάν οι αρχάριοι είναι μαγικό. Θέλουν ένα εργαλείο το οποίο να είναι εύκολο στη χρήση, να λειτουργεί σε Windows, το οποίο να μπορούν να το κατεβάσουν με την αναζήτηση στο Google και κάνοντας κλικ στον πρώτο σύνδεσμο που βλέπουν, να κάνει όλες τις λειτουργίες hacking με το πάτημα ενός κουμπιού. Δυστυχώς, δεν υπάρχει τέτοιο εργαλείο (για παράδειγμα, για τους χιλιάδες χρήστες που χρησιμοποιούν το Facebook, αν υπήρχε ένα εργαλείο το οποίο θα μπορούσε να εγκατασταθεί στα Windows, και απλά πληκτρολογώντας τα στοιχεία ενός ατόμου, το ψευδώνυμο / αριθμό κινητού τηλεφώνου / email και, στη συνέχεια, έτσι απλά να παίρναμε τον κωδικό του Facebook του;). Το Hacking είναι μια τέχνη, και παίρνει χρόνια για να κατανοηθεί κ να γίνει κάποιος εξπέρ. Να λοιπόν πώς να ξεκινήσετε. Το να μην έχει κάποιος ιδέα για το hacking εντάξει, αλλά να είναι κάποιος τόσο

αρχάριος ο όποιος ασχολείται με τους υπολογιστές δεν επιτρέπεται. Όταν λέω αρχάριος, εννοώ κάποιον που δεν έχει καμία εμπειρία με τον προγραμματισμό και με τις μεθόδους hacking. Δεν εννοούμε κάποιον που χρειάζεται έναν οδηγό μιας σελίδας για το πώς να κατεβάσετε ένα εργαλείο. Αν θέλει κάποιος να λέγεται hacker, θα πρέπει να δουλέψει σκληρά. Πώς να ξεκινήσετε; Μπορείτε να εγκαταστήσετε το Kali Linux. Θα αναφερθούμε πιο αναλυτικά στο Kali Linux σε επόμενο κεφάλαιο.

4.3 WPA2 Hacking

Νομίζετε ότι το ασύρματο δίκτυό σας είναι ασφαλές, επειδή χρησιμοποιείτε κρυπτογράφηση ***WPA2*** αντί της ***WEP***; Σκεφτείτε το πάλι. Σχεδόν όλοι όσοι ασχολούνται με την τεχνολογία, έχουν διαβάσει ένα ή περισσότερα άρθρα σχετικά με το πως οι hackers καταφέρνουν να έχουν πρόσβαση σε ασύρματα δίκτυα που χρησιμοποιούν κρυπτογράφηση Wired Equivalent Privacy (WEP). Αυτά είναι τα παλιά νέα. Εάν εξακολουθείτε να χρησιμοποιείτε WEP, ίσως είναι καλύτερο να δώσετε στους hackers και ένα κλειδί για το σπίτι σας, ή ακόμα καλύτερα να ανοίξετε το Wi-Fi σας και να το αφήσετε ελεύθερο για όλους. Οι περισσότεροι γνωρίζουν ότι η κρυπτογράφηση WEP μπορεί να παραβιαστεί σε δευτερόλεπτα.

Οι περισσότεροι λοιπόν έχετε διαβάσει ή έχετε ακούσει συμβουλές από geeks ασφαλείας, για την χρησιμοποίηση της κρυπτογράφησης Wi-Fi Protected Access 2 (WPA2) σαν μέσο για την προστασία του ασύρματου δικτύου σας. Η WPA2 είναι η πιο πρόσφατη και η πιο ισχυρή μέθοδος κρυπτογράφησης ασύρματων δικτύων που είναι διαθέσιμη αυτή τη στιγμή.

Καλό θα ήταν να γνωρίζετε ότι hackers που δοκίμασαν να παραβιάσουν το shell του WPA2 τα έχουν καταφέρει (σε ένα βαθμό).

Για να είμαστε σαφείς, οι hackers κατάφεραν να σπάσουν το WPA2-PSK (Pre Shared Key), το οποίο χρησιμοποιείται κυρίως από τους περισσότερους στο σπίτι και σε μικρές επιχειρήσεις. Η κρυπτογράφηση WPA2-Enterprise, που χρησιμοποιείται σε μεγάλες επιχειρήσεις, διαθέτει πολύ πιο περίπλοκες ρυθμίσεις που περιλαμβάνουν και τη χρήση ενός διακομιστή ελέγχου ταυτότητας RADIUS. Η συγκεκριμένη προστασία εξακολουθεί να είναι η πιο ασφαλής ασύρματη προστασία. Η WPA2-Enterprise δεν έχει σπάσει ακόμα.

Αν όμως η WPA2 ήταν ο καλύτερος τρόπος προστασίας ενός ασύρματου δικτύου στο σπίτι τι γίνεται τώρα;

Εικόνα 8 – Ηλεκτρονική Επίθεση

Μην πανικοβάλλεστε, υπάρχουν ακόμα τρόποι για την προστασία του δικτύου σας που χρησιμοποιεί WPA2-PSK. Έτσι θα μπορείτε να αποτρέψετε τους περισσότερους hackers να σπάσουν την κρυπτογράφηση σας και να αποκτήσουν πρόσβαση στο δίκτυό σας.
Πριν φτάσουμε όμως εκεί ας δούμε όμως μερικά επεξηγηματικά.

Οι hackers έχουν καταφέρει να σπάσουν την κρυπτογράφηση WPA2-PSK για δυο λόγους:

1. Πολλοί χρήστες δημιουργούν αδύναμα Pre-Shared Keys (κωδικούς πρόσβασης ασύρματου δικτύου)

Στη web σελίδα του setup υπάρχει το σημείο που ρυθμίζετε την ασύρματη πρόσβαση και την χρησιμοποίηση της κρυπτογράφησης WPA2-PSK. Εκεί θα πρέπει να δημιουργήσετε ένα Pre-Shared Key. Πολλοί χρησιμοποιούν ένα εύκολο Pre-Shared Key, γιατί θα πρέπει να το πληκτρολογήσουν σε κάθε συσκευή που χρησιμοποιεί Wi-Fi για να συνδεθεί στο ασύρματο δίκτυό τους. Μπορεί επίσης να επιλέγουν να έχουν ένα απλό κωδικό, γιατί συνήθως οι φίλοι ρωτάνε ποιος είναι ο κωδικός πρόσβασης για να συνδέσουν κάποια συσκευή τους. Αν ο κωδικός σας είναι σικ «Mywifirocks» αλλά δεν είναι περίπλοκος είναι πολύ εύκολο να σπάσει.

Οι hackers μπορούν να σπάσουν αδύναμα Pre-Shared Keys με τη χρήση εργαλείων brute-force ή Rainbow Tables σε ένα πολύ σύντομο χρονικό διάστημα. Το μόνο που έχουν να κάνουν είναι να πιάσουν το handshake του SSID (όνομα ασύρματου δικτύου), μεταξύ του εξουσιοδοτημένου client του ασύρματου δικτύου και του δρομολογητή, και στη συνέχεια να πάρουν όλες τις πληροφορίες που χρειάζονται για να τις επεξεργαστούν με τα εργαλεία τους.

2. Οι περισσότεροι χρησιμοποιούν τα προεπιλεγμένα ή κοινά ονόματα ασύρματων δικτύων (SSID)

Στο web setup του router σας μπορείτε να αλλάξετε το όνομα του δικτύου σας. Πάρα πολλοί αφήνουν το προεπιλεγμένο SSID στο router τους, αυτό δηλαδή που έχει ορίσει ο κατασκευαστής.

Οι hackers έχουν λίστες με τα πιο κοινά SSIDs για να δημιουργήσουν password cracking Rainbow Tables. Έτσι μπορούν να σπάσουν τα Pre-Shared Keys των δικτύων που χρησιμοποιούν κοινά SSIDs γρήγορα και εύκολα.

Σημείωση: Ακόμα και αν το όνομα του δικτύου σας δεν είναι στη λίστα μπορούν ακόμα να δημιουργήσουν password cracking Rainbow Tables για κάποιο συγκεκριμένο όνομα δικτύου, μόνο που θα χρειαστούν πολύ περισσότερο χρόνο και πόρους συστήματος.

Τι μπορείτε να κάνετε για να είναι ασφαλέστερο το ασύρματο δίκτυό σας που χρησιμοποιεί WPA2-PSK;

Δημιουργήστε Pre-Shared Key με πάνω από 25 τυχαίους χαρακτήρες.

Τα εργαλεία Brute-force και το Rainbow Table έχουν τα όριά τους. Όσο μεγαλύτερο είναι το Pre-Shared Key, τόσο δυσκολότερο είναι να σπάσει. Η υπολογιστική ισχύς και η χωρητικότητα του σκληρού δίσκου που απαιτείται για να σπάσουν μεγάλα Pre-Shared Keys είναι τεράστια και σχεδόν ανέφικτο να παραχθεί από κοινά μηχανήματα, (λέμε πάντα σχεδόν γιατί κανείς δεν ξέρει τι μηχανήματα χρησιμοποιεί ο hacker)

Όσο και αν είναι δύσκολο να εισάγετε έναν κωδικό πρόσβασης 30 χαρακτήρων σε κάθε ασύρματη συσκευή που θέλετε να χρησιμοποιήσετε στο δίκτυο σας, συνήθως θα πρέπει να το κάνετε μόνο μια φορά.

Η κρυπτογράφηση WPA2-PSK υποστηρίζει Pre-Shared Keys έως και 63 χαρακτήρων.

Βεβαιωθείτε ότι το SSID (όνομα ασύρματου δικτύου) είναι τυχαίο όσο το δυνατόν

Μπορείτε να βεβαιωθείτε ότι το SSID σας δεν είναι στη λίστα των top 1000 πιο κοινών SSIDs όπως αναφέραμε προηγουμένως. Αυτό θα σας αποτρέψει από το να γίνετε ένας εύκολος στόχος για τους hackers οι οποίοι έχουν ήδη προ-χτισμένα Rainbow Table για το σπάσιμο δικτύων με κοινά SSID. Χρησιμοποιήστε ένα τυχαίο και μεγάλο όνομα δικτύου, όπως κάνατε και με τον κωδικό πρόσβασης.

Το μέγιστο μήκος για ένα SSID είναι 32 χαρακτήρες. Συνδυάζοντας τις δύο παραπάνω αλλαγές θα κάνετε το ασύρματο δίκτυο σας πολύ πιο δύσκολο στόχο για τους hackers. Ας ελπίσουμε ότι οι περισσότεροι hackers θα φύγουν και θα αναζητήσουν κάτι πιο εύκολο, όπως το ασύρματο δίκτυο του γείτονά σας, ο οποίος, εξακολουθεί να χρησιμοποιεί WEP.

4.4 Δημοφιλή εργαλεία hacking

Υπάρχουν πολλά εργαλεία που μπορούν να «σπάσουν» την κρυπτογράφηση Wi-Fi. Τα εργαλεία αυτά μπορούν είτε να επωφεληθούν από τις αδυναμίες της WEP ή με βίαιες επιθέσεις για WPA / WPA2. Πλέον πρέπει να ξέρουμε ότι ποτέ δεν πρέπει να χρησιμοποιούμε ασφάλεια WEP.

Τα βασικά εργαλεία για το ασύρματο hacking είναι δύο ειδών. Ένα από αυτά είναι ότι μπορούν να χρησιμοποιηθούν για την «όσφρηση» του δικτύου και να παρακολουθεί τι συμβαίνει στο δίκτυο. Και άλλα είδη εργαλείων είναι αυτά που χρησιμοποιούνται για να χακάρουν WEP κλειδιά / WPA. Αυτά είναι τα πιο δημοφιλή εργαλεία που χρησιμοποιούνται για την ασύρματη πυρόλυση κωδικό πρόσβασης (wireless password cracking) και την αντιμετώπιση προβλημάτων του δικτύου.

1. Aircrack

Aircrack είναι το πιο δημοφιλή και ευρέως γνωστό εργαλείο πυρόλυσης για ασύρματο κωδικό πρόσβασης (*wireless password cracking tool*). Χρησιμοποιείται ως 802.11 WEP και WPA-PSK κλειδιά «σπασίματος» (*keys cracking tool*) σε όλο τον κόσμο. Συλλαμβάνει, πρώτα, τα πακέτα του δικτύου και στη συνέχεια προσπαθεί να ανακτήσει τον κωδικό πρόσβασης του δικτύου με την ανάλυση των πακέτων. Υλοποιεί επίσης στάνταρ επιθέσεις FMS με κάποιες βελτιστοποιήσεις για να ανακτήσει ή να σπάσει τον κωδικό πρόσβασης του δικτύου. Οι βελτιστοποιήσεις περιλαμβάνουν επιθέσεις KoreK και PTW επίθεση για να κάνουν την επίθεση πολύ πιο γρήγορα από ό, τι άλλα εργαλεία κωδικό πρόσβασης WEP πυρόλυση (*WEP password cracking*). Αυτό το εργαλείο είναι ισχυρό και από τα πιο ευρέως χρησιμοποιούμενα σε όλο τον κόσμο. Αυτός είναι και ο λόγος που βρίσκεται στην κορυφή της λίστας.

Αυτό το εργαλείο είναι δύσκολο να χρησιμοποιηθεί, μπορείτε να δοκιμάσετε τα διαθέσιμα online tutorials. Η εταιρεία για αυτό το εργαλείο προσφέρει επίσης απευθείας σύνδεση φροντιστήριο για να διδαχθείτε μόνοι σας.

2. Airsnort

Airsnort είναι ένα άλλο δημοφιλές WLAN εργαλείο κωδικό πυρόλυση(cracking). Μπορεί να σπάσει τα κλειδιά WEP του δικτύου Wi-Fi 802.11b. Αυτό το εργαλείο λειτουργεί ουσιαστικά από παθητικές μεταδόσεις παρακολούθησης και στη συνέχεια υπολογίζει το κλειδί κρυπτογράφησης, όταν έχουν συγκεντρωθεί αρκετά πακέτα. Αυτό το εργαλείο είναι ελεύθερα διαθέσιμο για Linux και Windows πλατφόρμες. Είναι επίσης απλό στη χρήση. Το εργαλείο δεν έχει ενημερωθεί για περίπου τρία χρόνια, αλλά φαίνεται ότι η εταιρεία αυτού του εργαλείου ενδιαφέρεται για περαιτέρω ανάπτυξη. Αυτό το εργαλείο επίσης εμπλέκεται άμεσα σε WEP πυρόλυση (*cracking*) και ως εκ τούτου χρησιμοποιείτε ευρέως.

3. Kismet

Kismet είναι ένα άλλο Wi-Fi 802.11 a / b / g / n επιπέδου 2 εργαλείο ανίχνευσης εισβολής σε ασύρματο σύστημα. Αυτό το εργαλείο χρησιμοποιείται κατά κύριο λόγο σε αντιμετώπιση Wi-Fi προβλημάτων. Λειτουργεί καλά με οποιαδήποτε κάρτα Wi-Fi η οποία υποστηριζεί rfmon λειτουργία. Είναι διαθέσιμο για Windows, Linux, OS X και πλατφόρμες BSD. Αυτό το εργαλείο συλλέγει παθητικά τα πακέτα για τον εντοπισμό πρότυπου δικτύου και ανιχνεύει επίσης τα κρυμμένα δίκτυα. Χτισμένο σε μια αρχιτεκτονική σπονδυλωτή διακομιστή-πελάτη, αυτό το εργαλείο μπορεί να μυρίσει το 802.11b, 802.11a, 802.11g και 802.11n κυκλοφορίας. Είναι ένα ανοικτό εργαλείο πηγής και υποστηρίζει τα πρόσφατα ταχύτερα ασύρματα πρότυπα.

4. Cain & Able

Cain & Able είναι ένα άλλο δημοφιλές εργαλείο που χρησιμοποιείται για την πυρόλυση (*cracking*) στους κωδικούς πρόσβασης του ασύρματου δικτύου. Αυτό το εργαλείο αναπτύχθηκε για να παρακολουθήσει την κίνηση στο δίκτυο και στη συνέχεια χρησιμοποιεί brute forcing ώστε να ανακαλύψουν τους κωδικούς πρόσβασης. Ο λόγος που αυτό το εργαλείο βοηθά πολύ, ενώ βρίσκοντας τον κωδικό

πρόσβασης του ασύρματου δικτύου αναλύει τα πρωτοκόλλα δρομολόγησης. Αυτό το εργαλείο μπορεί επίσης να χρησιμοποιηθεί για να σπάσει άλλου είδους κωδικών πρόσβασης. Είναι ένα από τα πιο δημοφιλή εργαλεία για «σπάσιμο» κωδικού (*cracking password*).

Αυτό το εργαλείο δεν είναι μόνο για WEP «σπάσιμο» (*WEP cracking*). Βασικά χρησιμοποιείται για «σπάσιμο» κωδικών πρόσβασης των Windows. Αυτός είναι και ο λόγος που αυτό το εργαλείο είναι τόσο δημοφιλές μεταξύ των χρηστών.

6. Fern WiFi Wireless Cracker

Fern WiFi Wireless Cracker είναι ένα άλλο ωραίο εργαλείο που βοηθά για ασφάλεια του δικτύου. Αυτό σας επιτρέπει να δείτε την κίνηση του δικτύου σε πραγματικό χρόνο και να εντοπίσει οικοδεσπότες (hosts). Βασικά αυτό το εργαλείο αναπτύχθηκε για να βρει ελαττώματα σε δίκτυα υπολογιστών και διορθώνει τις ανιχνεύσιμες ατέλειες. Είναι διαθέσιμο για Apple, Windows και Linux πλατφόρμες.

Είναι σε θέση να «σπάσει» και να ανακτήσει WEP κλειδιά / WPA / WPS εύκολα. Μπορεί επίσης να εκτελέσει άλλες επιθέσεις που βασίζονται σε ασύρματα ή Ethernet δίκτυα. Για «σπάσιμο» (cracking) WPA / WPA2, χρησιμοποιεί WPS βασισμένο σε επιθέσεις. Για WEP «σπάσιμο», χρησιμοποιείτε κατακερματισμός, Chop-Chop, Caffe-Latte, Hirte, ARP Request Replay ή WPS επίθεση.

Αυτό το εργαλείο βρίσκεται ακόμα σε ανάπτυξη από την εταιρεία. Έτσι, μπορείτε να περιμένετε την έγκαιρη ενημέρωση με νέα χαρακτηριστικά. Η Pro έκδοση του εργαλείου είναι επίσης διαθέσιμη η οποία προσφέρει πολλά χαρακτηριστικά.

7. CoWPAtty

CoWPAtty είναι ένα άλλο ωραίο εργαλείο για «σπάσιμο» κωδικού. Πρόκειται για ένα αυτοματοποιημένο εργαλείο επίθεσης για WPA-PSK και σπάσιμο στους κωδικούς πρόσβασης του. Τρέχει σε λειτουργικό σύστημα Linux και προσφέρει μια λιγότερο ενδιαφέρουσα διεπαφή γραμμής εντολών με την οποία δουλεύει. Τρέχει σε μια λίστα λέξεων που περιέχει χιλιάδες κωδικούς πρόσβασης για χρήση στην επίθεση. Εάν ο κωδικός πρόσβασης είναι στη λίστα των κωδικών πρόσβασης, αυτό το εργαλείο σίγουρα θα σπάσει τον κωδικό πρόσβασης. Αλλά αυτό το εργαλείο έχει αργή ταχύτητα κ αυτό εξαρτάται από τη λίστα λέξεων και τη δύναμη του

κωδικού. Ένας άλλος λόγος για την αργή διαδικασία είναι ότι η hash χρησιμοποιεί SHA1 με έναν σπόρο του SSID. Αυτό σημαίνει ότι ο ίδιος κωδικός πρόσβασης θα έχει μια διαφορετική SSIM. Έτσι, δεν μπορείτε απλά να χρησιμοποιήσετε τον πίνακα ουράνιο τόξο εναντίον όλων των σημείων πρόσβασης. Γι αυτό, το εργαλείο χρησιμοποιεί το λεξικό κωδικών και δημιουργεί το hash για κάθε λέξη που περιλαμβάνεται στο λεξικό χρησιμοποιώντας το SSID. Αυτό το εργαλείο είναι απλό στη χρήση με τις διαθέσιμες εντολές.

Με τη νεότερη έκδοση του εργαλείου CoWPAtty προσπάθησαν να βελτιώσουν την ταχύτητα με τη χρήση ενός προ-υπολογισμένου αρχείου hash ώστε να αποφύγουμε τον υπολογισμό κατά το χρόνο του σπασίματος. Αυτος ο προ-υπολογισμός στο αρχείο έδειξε πως περιέχει περίπου 172.000 αρχεία λεξικού για περίπου 1000 πιο δημοφιλή SSIDs. Αλλά για επιτυχημένη επίθεση, το SSID σας πρέπει να είναι σε αυτή τη λίστα. Εάν το SSID δεν είναι σε αυτά τα 1000, είστε άτυχοι. Όμως, μπορείτε να δοκιμάσετε αυτό το εργαλείο για να δείτε πώς λειτουργεί.

8. Airjack

Airjack είναι ένα εργαλείο έγχυση για πακέτα τύπου Wi-Fi 802.11. Χρησιμοποιείται για DOS και MIM επίθεση. Αυτό το ασύρματο εργαλείο σπασίματος είναι πολύ χρήσιμο σε πλαστά πακέτα και κάνοντας ένα δίκτυο εκτός υπηρεσίας. Αυτό το εργαλείο μπορεί επίσης να χρησιμοποιηθεί και για Man In The Middle επίθεσεις στο δίκτυο. Είναι δημοφιλές κ ισχυρό κ για τις δύο χρήσεις του.

9. WepAttack

WepAttack είναι άλλο ένα εργαλείο του Linux για το σπάσιμο των 802.11 κλειδιών WEP. Όπως και μερικά άλλα εργαλεία στη λίστα, εκτελεί μια ενεργή επίθεση. Δοκιμάζει εκατομμύρια λέξεις από το λεξικό του για να βρει το κλειδί εργασίας για το δίκτυο. Μόνο μια κάρτα WLAN εργασίας απαιτείται να συνεργαστεί με WepAttack για να εκτελέσει την επίθεση. Έχε περιορισμένη χρηστικότητα αλλά λειτουργεί φοβερά για τις υποστηριζόμενες κάρτες WLAN.

10. NetStumbler

NetStumbler είναι ένα άλλο εργαλείο για «σπάσιμο» κωδικού διαθέσιμο μόνο για την πλατφόρμα των Windows. Βοηθά στην εύρεση ανοικτών ασυρμάτων σημείων πρόσβασης. Είναι ελεύθερα διαθέσιμο. Βασικά το NetStumbler χρησιμοποιείται για

εντοπισμό ασυρμάτων δικτύων, για επαλήθευση δικτύου, για την εύρεση τοποθεσιών με μια κακή σύνδεση δικτύου, για τον εντοπισμό μη εξουσιοδοτημένων σημείων πρόσβασης, και πολλά άλλα.

Αυτό το εργαλείο δεν είναι πολύ αποτελεσματικό τώρα. Κύριος λόγος είναι ότι η τελευταία σταθερή έκδοση του εργαλείου ήταν τον Απρίλιο του 2004 περίπου πριν από 12 χρόνια. Έτσι, δεν λειτουργεί με 64-bit των Windows OS. Μπορεί επίσης εύκολα να ανιχνευθεί με τα περισσότερα από τα διαθέσιμα ασύρματα συστήματα ανίχνευσης εισβολής. Έτσι, μπορείτε να χρησιμοποιήσετε αυτό το εργαλείο για την εκμάθηση στο οικιακό δίκτυο για να δείτε πώς λειτουργεί.

Μια ακόμη έκδοση γνωστή ως «MiniStumbler» είναι επίσης διαθέσιμη. Αυτή η έκδοση του εργαλείου όμως είναι πολύ παλιά, αλλά εξακολουθεί να λειτουργεί καλά σε υποστηριζόμενα συστήματα.

11. Inssider

Inssider είναι ένα από τα πιο δημοφιλή εργαλεία σάρωσης Wi-Fi για Microsoft Windows και OS X πλατφόρμες. Αυτό το εργαλείο κυκλοφόρησε με άδεια ανοικτού κώδικα και επίσης έχει βραβευτεί ως «Καλύτερο Λογισμικό Ανοικτού Κώδικα στη δικτύωση". Αργότερα έγινε εργαλείο πριμοδότησης και τώρα κοστίζει γύρω στα $19.99. Το inssider Wi-Fi σαρωτής μπορεί να κάνει διάφορες εργασίες, συμπεριλαμβανομένης της εξεύρεσης ανοικτών Wi-Fi σημείων πρόσβασης, την παρακολούθηση της ισχύ του σήματος και την εξοικονόμηση κορμών με τα αρχεία GPS. Βασικά αυτό το εργαλείο χρησιμοποιείται από τους διαχειριστές του δικτύου για να εντοπίζει θέματα στα ασύρματα δίκτυα.

12. Wifiphisher

Wifiphisher είναι ένα άλλο ωραίο εργαλείο hacking για να πάρουμε τον κωδικό πρόσβασης του ασύρματου δικτύου. Αυτό το εργαλείο μπορεί να εκτελέσει γρήγορα αυτοματοποιημένη phishing επίθεση εναντίον ενός ασύρματου δικτύου Wi-Fi για να κλέψει τους κωδικούς πρόσβασης. Είναι προ-εγκατεστημένο σε Kali Linux. Είναι ελεύθερο να χρησιμοποιηθεί από τους χρήστες και διαθέσιμο για Windows, Mac και Linux.

13. Kismac

Kismac είναι εργαλείο πολύ παρόμοιο με το Kismet, το οποίο αναφέραμε παραπάνω. Διαθέτει χαρακτηριστικά παρόμοια με το Kismet και χρησιμοποιείται ως εργαλείο ανακάλυψης ασύρματου δικτύου. Όπως υποδηλώνει το όνομα του, αυτό το εργαλείο είναι διαθέσιμο μόνο για Mac. Σαρώνει τα δίκτυα μόνο παθητικά με τις υποστηριζόμενες κάρτες ασύρματου δικτύου. Προσπαθεί να σπάσει τα WEP και WPA κλειδιά με τη χρήση ωμής βίας.

14. Reaver

Reaver είναι ένα άλλο εργαλείο ανοικτού κώδικα για την εκτέλεση με επίθεση ωμής βίας εναντίον WPS για να ανακτήσει τα κλειδιά WPA2/ WPA. Αυτό το εργαλείο φιλοξενείται στον Κώδικα Google και μπορεί να εξαφανιστοεί σύντομα, αν ο εφευρέτης του δεν έχει μεταναστεύσει σε άλλη πλατφόρμα. Τελευταία ενημέρωση ήταν περίπου πριν από 4 χρόνια. Παρόμοιο με άλλα εργαλεία, το εργαλείο αυτό μπορεί να είναι μια καλή εναλλακτική στη λίστα εργαλείων που χρησιμοποιούν ίδια μέθοδο επίθεσης.

15. Wifite

Wifite είναι επίσης ένα ωραίο εργαλείο που υποστηρίζει την πυρόλυση (cracking) στα WPS κρυπτογραφημένα δίκτυα μέσω Reaver. Λειτουργεί σε Linux λειτουργικά συστήματα. Προσφέρει διάφορα ωραία χαρακτηριστικά που σχετίζονται με το «σπάσιμο» (cracking) του κωδικού του δικτύου.

16. WepDecrypt

WepDecrypt είναι ένα άλλο WLAN εργαλείο γραμμένο σε γλώσσα C. Αυτό το εργαλείο μπορεί να μαντέψει τα WEP κλειδιά εκτελώντας επίθεση-λεξικό, το οποίο διανέμει επίθεση στο δίκτυο, το κλειδί γεννήτριας και κάποιες άλλες μεθόδους. Αυτό το εργαλείο χρειάζεται μερικές βιβλιοθήκες για να εργαστούν. Μπορείτε να διαβάσετε περισσότερες λεπτομέρειες σχετικά με αυτό το εργαλείο στη σελίδα λήψης http://wepdecrypt.sourceforge.net/wepdecrypt-manual.html. Δεν είναι τόσο δημοφιλή, αλλά είναι καλό για αρχάριους ώστε να δούνε πώς λειτουργεί η επίθεση-λεξικό.

17. OmniPeek

OmniPeek είναι ένα πακέτο sniffer αλλά και πακέτα δικτύου ανάλυσης. Αυτό το εργαλείο είναι διαθέσιμο μόνο για σε πλατφόρμα Windows και μόνο για εμπορική χρήση. Απαιτεί από εσάς να έχετε καλή γνώση των πρωτοκόλλων δικτύου και την κατανόηση των πακέτων δικτύου. Λειτουργεί με τις περισσότερες από τις κάρτες διασύνδεσης δικτύου οι οποίες διατίθενται στην αγορά. Με διαθέσιμα plugins, το εργαλείο αυτό μπορεί να γίνει πιο ισχυρό. Περίπου 40 plugins είναι ήδη διαθέσιμα για να επεκτείνει τις λειτουργίες αυτού του εργαλείου.

18. CloudCracker

CloudCracker είναι ένα online εργαλείο για να σπάσουμε WPA κλειδιά του ασύρματου δικτύου. Μπορεί επίσης να χρησιμοποιηθεί για να σπάσουμε διάφορα άλλα είδη hashes κωδικού πρόσβασης. Το μόνο που χρειάζεται, να φορτώσετε το αρχείο χειραψία (handshake file) και να πληκτρολογήστε το όνομα του δικτύου για να ξεκινήσει η επίθεση. Με 3000 εκατομμύρια λέξεις του λεξικού, με αυτό το εργαλείο είναι πιθανό να σπάσουμε τον κωδικό πρόσβασης. Χρησιμοποιείται επίσης για MD5, SHA και μερικές άλλες ρωγμές. Είναι επίσης ένα αποτελεσματικό εργαλείο και αξίζει να το αναφέρουμε αν μιλάμε για ασύρματα εργαλεία πυρόλυσης.

19. CommonView για Wi-Fi

CommonView για Wi-Fi είναι επίσης ένα δημοφιλής εργαλείο με ασύρματη οθόνη δικτύου και αναλυτή συσκευαστή. Είναι εύκολο να κατανοηθεί αν χρησιμοποιηθεί με GUI. Αυτό το εργαλείο είναι βασικά για Wi-Fi διαχειριστές δικτύου και επαγγελματίες της ασφάλειας που θέλουν να παρακολουθούν και να αντιμετωπίσουν προβλήματα που σχετίζονται με τα δίκτυα. Λειτουργεί καλά με Wi-Fi 802.11 a / b / g / n / ac δίκτυα. Συλλαμβάνει κάθε πακέτο και σας επιτρέπει να δείτε χρήσιμες πληροφορίες του δικτύου. Μπορείτε επίσης να πάρετε χρήσιμες πληροφορίες, όπως τη διανομή του πρωτοκόλλου, τα σημεία πρόσβασης, την ισχύ του σήματος και άλλα. Αυτό το εργαλείο προσφέρει βασικές πληροφορίες σχετικά με ένα δίκτυο και έχει μια καλή αξία για διαχειριστές δικτύου.

20. Pyrit

Pyrit είναι επίσης ένα πολύ καλό εργαλείο το οποίο σας επιτρέπει να εκτελέσετε επίθεση στο IEEE 802.11 WPA/WPA2-PSK. Είναι διαθέσιμο δωρεάν και

φιλοξενείται στο Google Code. Έτσι, θα μπορούσε να εξαφανιστεί στους προσεχείς μήνες. Λειτουργεί σε ποικιλία από πλατφόρμες, συμπεριλαμβανομένων των FreeBSD, MacOS X και Linux.

Εκτελεί brute-force επίθεση ώστε να σπάσει τους WPA / WPA-2 κωδικούς πρόσβασης. Είναι πολύ αποτελεσματικό και συστήνεται για δοκιμή από πολλούς χρήστες του διαδικτύου. Μπορείτε να το κατεβάσετε από την εξής ιστοσελίδα : https://code.google.com/p/pyrit/

Περισσότερα από τα εργαλεία που αναφέρθηκαν παραπάνω είναι σε θέση να σπάσουν κωδικούς πρόσβασης ασύρματου δικτύου, αλλά ο χρόνος μπορεί να ποικίλλει ανάλογα με την πολυπλοκότητα και το μήκος του κωδικού πρόσβασης για αυτές τις ρωγμές. Μερικά εργαλεία δεν μπορούν να χρησιμοποιηθούν άμεσα στις ρωγμές κωδικών πρόσβασης, αλλά η ανάλυση πακέτων βοηθά στο να μαντέψουμε τον κωδικό πρόσβασης.

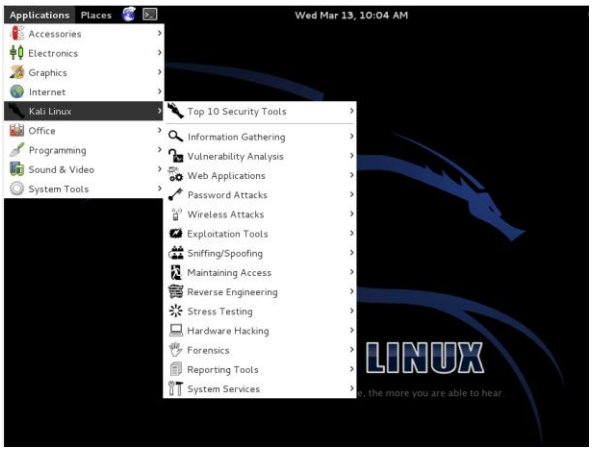
Συστήνεται επίσης από πολλούς έμπειρους χρήστες, η χρήση αυτών των εργαλείων μόνο με σκοπό τη μάθηση. Δεν ενθαρρύνουμε παράνομες δραστηριότητες και δεν υποστηρίζουμε αυτό το είδος των ανθρώπων, δλδ τους λεγόμενους hackers. Το Hacking του ασύρματου δικτύου για να πάρει τη μη εξουσιοδοτημένη πρόσβαση είναι ένα έγκλημα στον κυβερνοχώρο. Έτσι, μην θέτεται τον εαυτό σας σε κίνδυνο.

Αν κάποιος δουλεύει επαγγελματικά στο χώρο της ασφάλειας του δικτύου, θα πρέπει να γνωρίζει σχετικά με αυτά τα εργαλεία.

ΚΕΦΑΛΑΙΟ 5 : KALI LINUX

5.1 Kali Linux – Το λειτουργικό των Hacker

Με Kali Linux, το hacking γίνεται πολύ πιο εύκολο, δεδομένου ότι έχει όλα τα εργαλεία (πάνω από 300 προ-εγκατεστημένα εργαλεία) τα οποία πιθανώς πάντα είχαμε ανάγκη. Όλοι μπορούν εύκολα να το κατεβάσουν. Από τη στιγμή που θα κατεβάσετε κ θα αρχίσετε να δουλεύεται με αυτό το περιβάλλον (Kali Linux)



Εικόνα 9 – Περιβάλλον Kali Linux

θα μπείτε στο παιχνίδι και θα αρχίσετε να χακάρετε πριν καν το καταλάβετε.

Το Kali Linux είναι ο διάδοχος του BackTrack Linux. Όπως και ο προκάτοχός του, είναι μία διανομή αφιερωμένη στην ηλεκτρονική ασφάλεια, η οποία περιέχει ορισμένα από τα σημαντικότερα εργαλεία που χρησιμοποιούν hackers και ερευνητές ασφαλείας διεθνώς.

Ορισμένα από τα εργαλεία του Kali Linux που αφορούν την ασύρματη δικτύωση, απαιτούν ασύρματες κάρτες δικτύου με συγκεκριμένα chipset.

Πρόκειται για ένα πανίσχυρο εργαλείο για πολύ συγκεκριμένες εργασίες που αφορούν την ηλεκτρονική ασφάλεια.

Το να το χρησιμοποιούμε για καθημερινές εργασίες στον υπολογιστή είναι σαν να οδηγήσουμε μια μπουλντόζα για να πάμε σε μια φιλική επίσκεψη.

Με άλλα λόγια, γίνεται, αλλά δεν έχει νόημα. Πρακτικά, οποιαδήποτε άλλη διανομή Linux είναι καλύτερη τις καθημερινές μας εργασίες.

5.2 Επιλογές της εγκατάστασής του

Λόγω της ιδιαιτερότητας της διανομής του, έχουμε τρεις επιλογές για την εγκατάσταση Kali Linux.

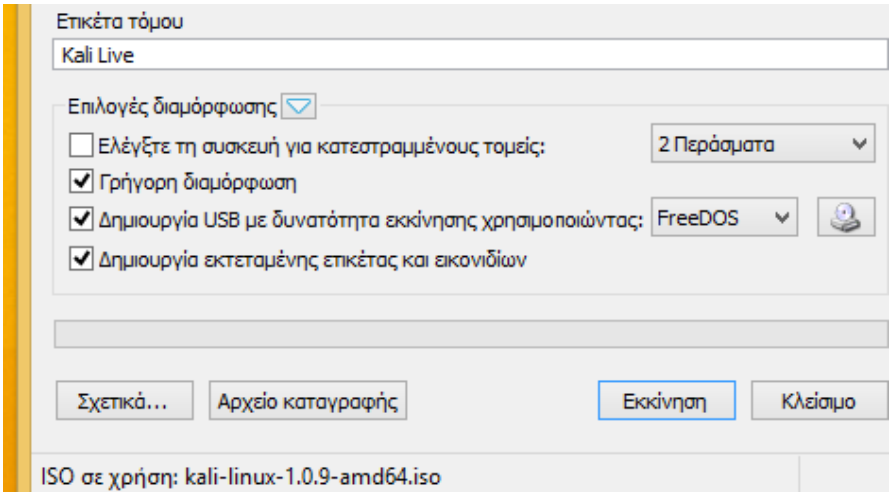
5.2.1 Χρήση του Live DVD/USB του Kali Linux

Η πρώτη από τις επιλογές, δεν περιλαμβάνει καν την εγκατάσταση Kali Linux. Ουσιαστικά θα χρησιμοποιήσουμε τη διανομή αποκλειστικά μέσα από το Live περιβάλλον.

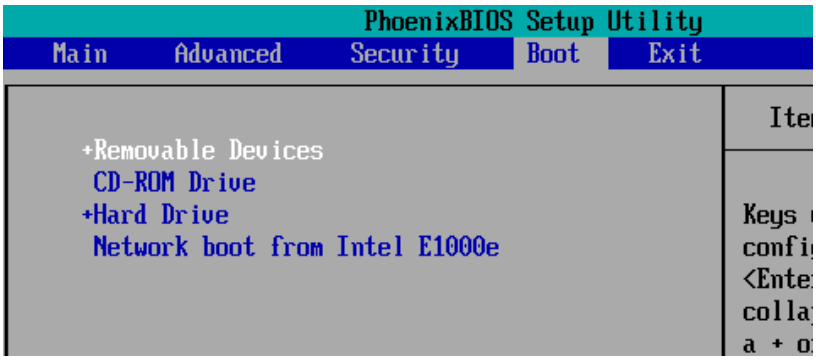
Αρκεί να μπούμε στη σελίδα http://www.kali.org/downloads/ και να κατεβάσουμε το 32 ή το 64bit ISO. Μπορούμε να κάνουμε Download μέσω του Browser (ISO) ή μέσω ενός προγράμματος BitTorent (Torrent).

Τα ARMEL και ARMHF images δεν μας απασχολούν, αφορούν ειδικές συσκευές με επεξεργαστές ARM, όχι τους συμβατικούς υπολογιστές, laptop ή desktop.

Αφού κατεβάσουμε το ISO, μπορούμε να το γράψουμε σε DVD μέσα από τα Windows. Εναλλακτικά, μπορούμε να το γράψουμε σε φλασάκι USB.

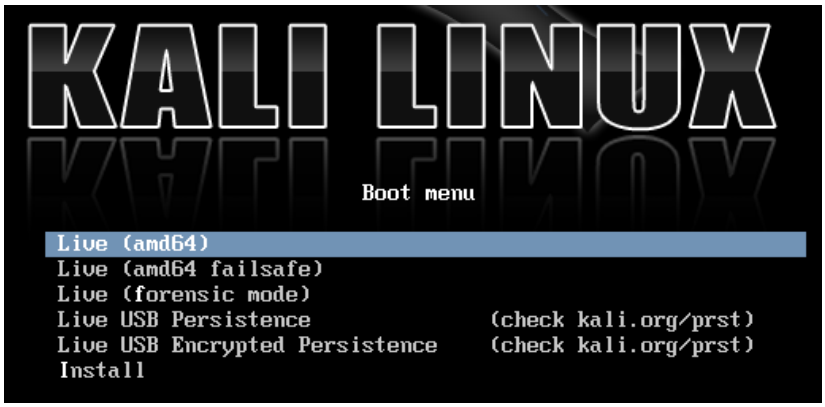


Τέλος, ρυθμίζουμε το BIOS του υπολογιστή να κάνει Boot από το κατάλληλο μέσον, DVD ή USB...

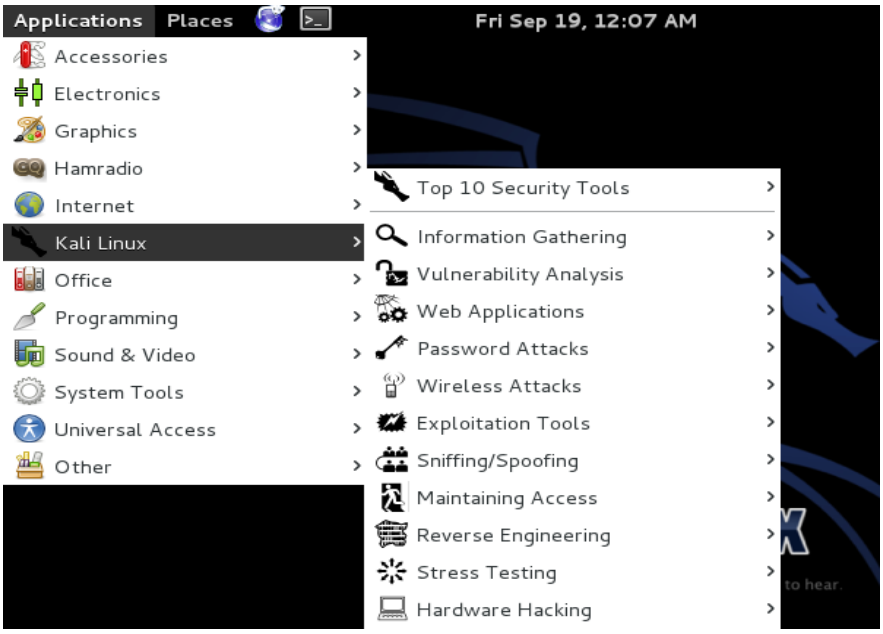


Εκκίνηση Live περιβάλλοντος από DVD/USB χωρίς Persistence

Στο παράδειγμα χρησιμοποιούμε την 64bit έκδοση του Kali Linux. Αρκεί να επιλέξουμε το Live (amd64).



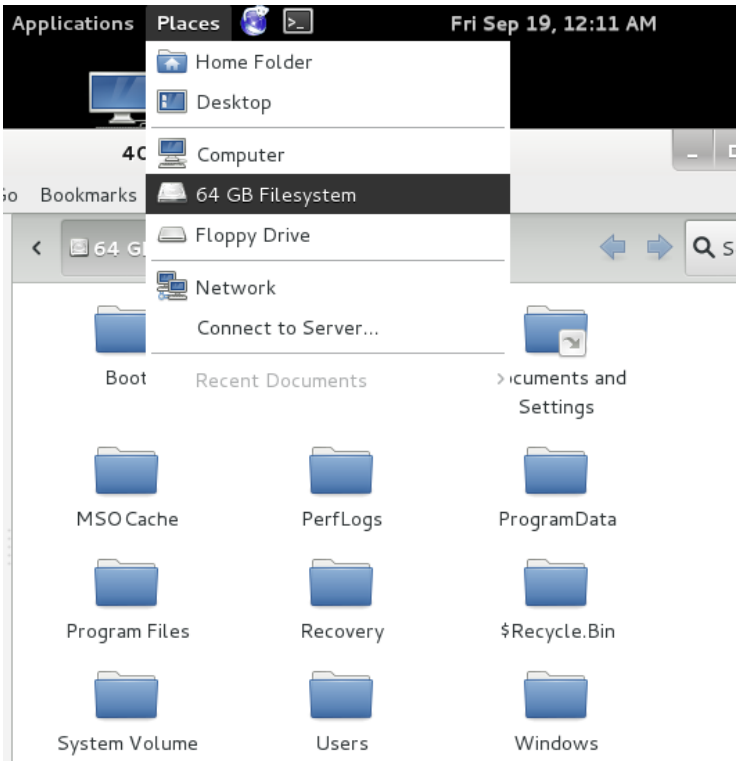
Σε λίγα δευτερόλεπτα, φορτώνεται το Live περιβάλλον του Kali Linux.



Μπορούμε να χρησιμοποιήσουμε κανονικά όλα τα εργαλεία, σαν να είχαμε κάνει την εγκατάσταση Kali Linux στον υπολογιστή μας.

Όμως, επειδή βρισκόμαστε σε Live περιβάλλον, οποιαδήποτε αλλαγή κάνουμε στις ρυθμίσεις ή όποιο αρχείο αποθηκεύσουμε, θα χαθεί στο επόμενο restart.

Ένας τρόπος να ξεπεράσουμε αυτόν τον περιορισμό, είναι να κάνουμε κλικ στο Places και να κάνουμε mount ένα από τα partition στο δίσκο του υπολογιστή - στο παράδειγμα έχει μόνο ένα partition των 64GB - για να αποθηκεύσουμε εκεί τυχών αρχεία.



Εκκίνηση Live περιβάλλοντος από USB με Persistence

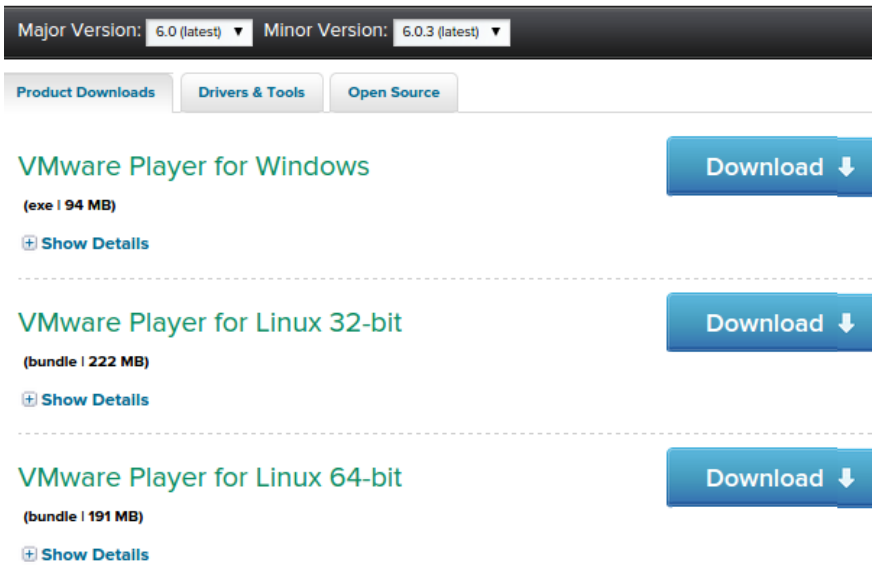
Το Kali Linux μας δίνει τη δυνατότητα να έχουμε Persistence στο USB, που σημαίνει πως ξεκινώντας το Live περιβάλλον, οι ρυθμίσεις και οι αλλαγές που θα κάνουμε θα μείνουν αποθηκευμένες στο USB.

Όμως για να είναι δυνατόν αυτό, θα χρειαστεί να ετοιμάσουμε το USB με διαφορετικό τρόπο, όχι να το δημιουργήσουμε με το Rufus ή άλλο σχετικό πρόγραμμα.

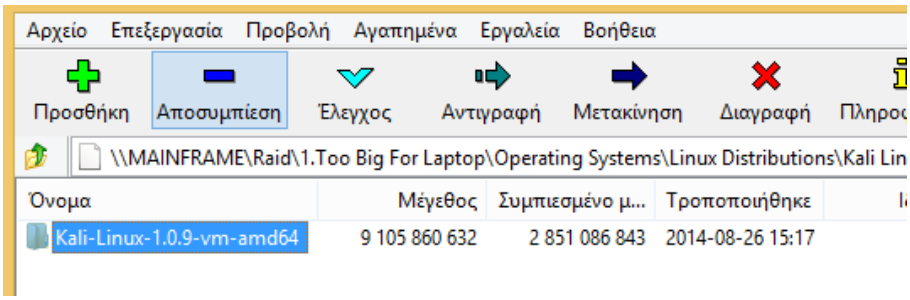
5.2.2 Εγκατάσταση Kali Linux σε έτοιμη VMware Virtual Machine

Αν σκοπεύουμε να χρησιμοποιούμε συχνά το Kali Linux, μακράν ο καλύτερος τρόπος είναι να κατεβάσουμε μία από τις έτοιμες VMware Virtual Machines που έχουν ετοιμάσει οι δημιουργοί του Kali Linux, Offensife Security.

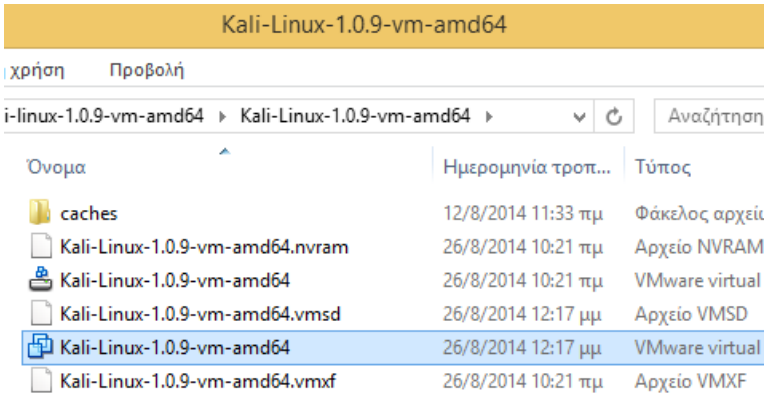
Για να αξιοποιήσουμε τη συγκεκριμένη Virtual Machine θα χρειαστεί να εγκαταστήσουμε τον δωρεάν VMware Player.



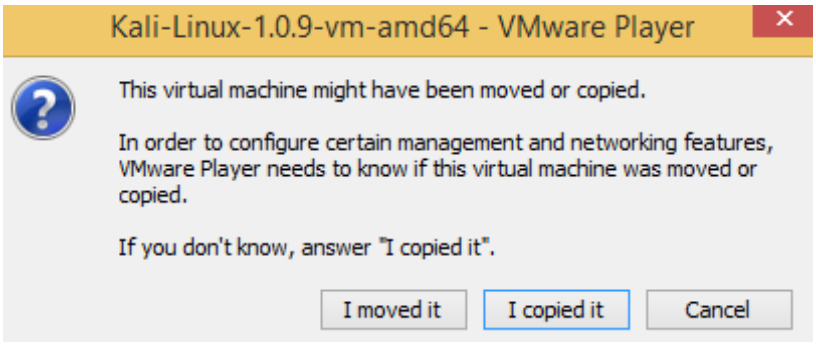
Το μόνο που περιλαμβάνει αυτή η μέθοδος για την εγκατάσταση Kali Linux είναι να αποσυμπιέσουμε το αρχείο τύπου .7z της Virtual Machine, χρησιμοποιώντας το 7zip (ή όποιο άλλο πρόγραμμα της επιλογής μας υποστηρίζει αρχεία .7z)



Αφού ολοκληρωθεί η αποσυμπίεση, και εφόσον έχουμε εγκατεστημένο το VMware Player, αρκεί να τρέξουμε το αρχείο με τύπο "VMware virtual machine configuration".



Ο VMware player θα μας εμφανίσει ένα παράθυρο, στο οποίο επιλέγουμε "I copied it".

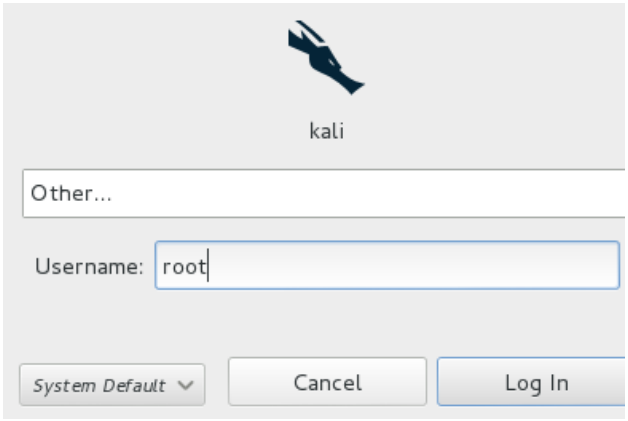


Πλέον ξεκινάει μια κανονική εγκατάσταση Kali Linux, όχι ένα Live περιβάλλον. Ό,τι αλλαγές κάνουμε, θα αποθηκευτούν στη Virtual Machine.

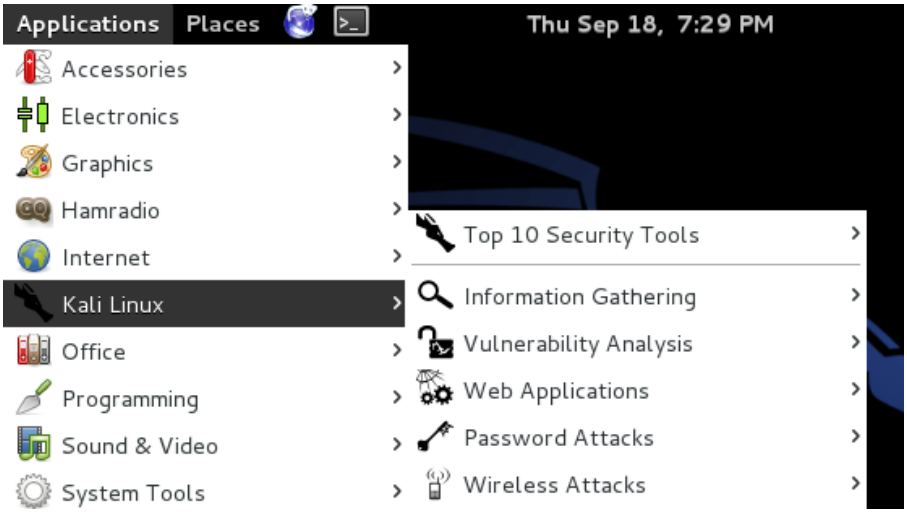
Στην οθόνη του login επιλέγουμε τη μοναδική επιλογή "Other"...

και κάνουμε login με τα εξής στοιχεία:

username: **root**
password: **toor**

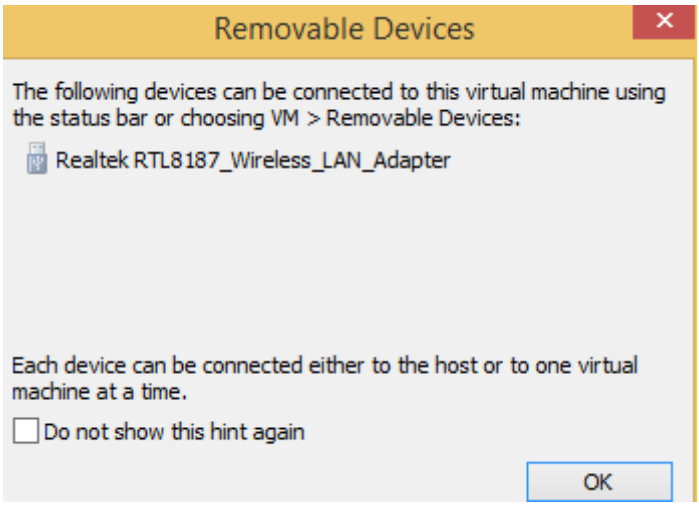


Πλέον έχουμε κανονική πρόσβαση στο περιβάλλον.

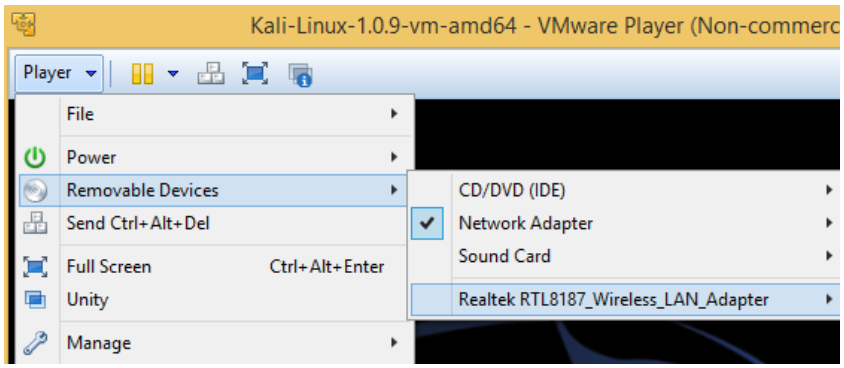


Το τελευταίο που χρειάζεται να κάνουμε στην εγκατάσταση Kali Linux με Virtual Machine, εφόσον μας ενδιαφέρουν τα χαρακτηριστικά ασφαλείας της ασύρματης δικτύωσης, είναι να συνδέσουμε την συμβατή κάρτα δικτύου στη Virtual Machine.

Αν είχαμε ήδη συνδεδεμένη την κάρτα δικτύου κατά το ξεκίνημα της Virtual Machine, κατά την έναρξη θα μας έβγαλε το παρακάτω μήνυμα για την δεύτερη κάρτα δικτύου.

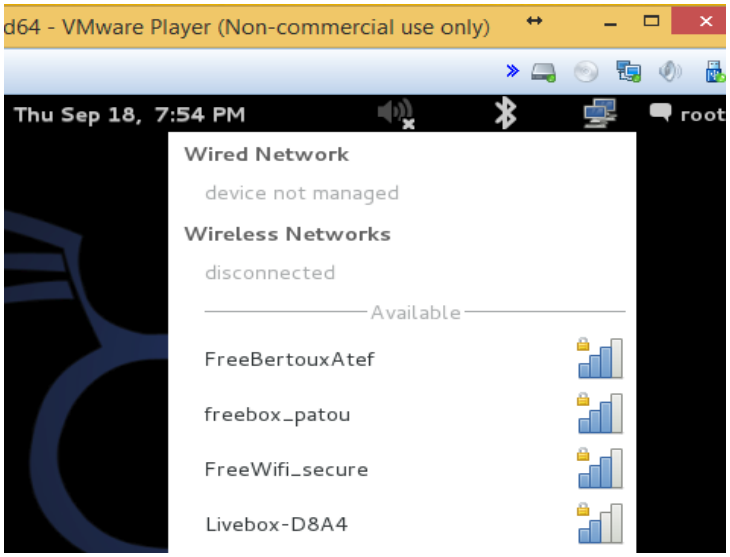


Αρκεί να πάμε στο Player -> Removable Devices, να επιλέξουμε την κάρτα...



...και να επιλέξουμε το Connect (Disconnect from host).

Σε λίγα δευτερόλεπτα, βλέπουμε κανονικά τα ασύρματα δίκτυα μέσα από την εγκατάσταση Kali Linux.



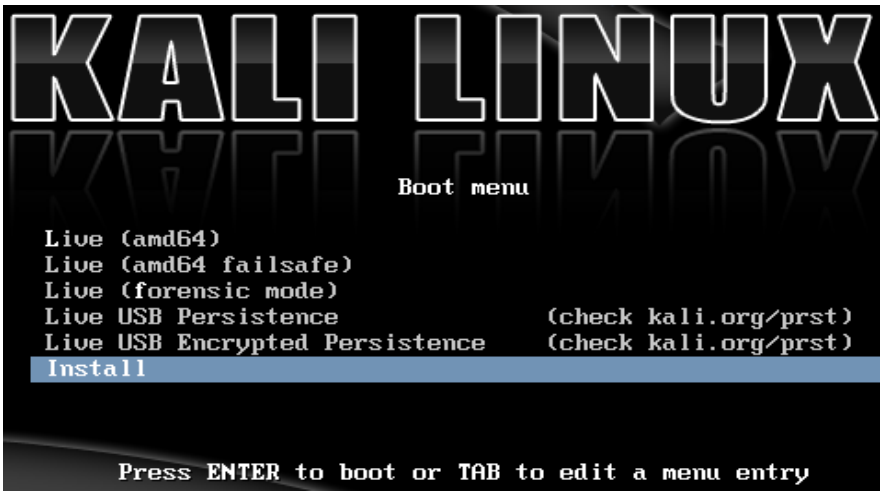
5.2.3 Εγκατάσταση Kali Linux σε Partition του υπολογιστή

Αυτή είναι η επιλογή που δεν προτείνουμε: να κάνουμε μια πλήρη εγκατάσταση του Kali Linux σαν λειτουργικό σύστημα στον υπολογιστή μας, παράλληλα με τα Windows.

Αν όμως θέλετε να έχετε έτσι το Kali Linux ντε και καλά, ποιοι είμαστε για να σας εμποδίσουμε? Επιπλέον, είναι η ευκολότερη μέθοδος για να έχουμε την εγκατάσταση Kali Linux στα Ελληνικά.

(αν και όποιος θέλει να γίνει ερευνητής ασφαλείας ή hacker και δεν γνωρίζει καλά Αγγλικά, δύσκολα θα φτάσει πολύ μακριά)

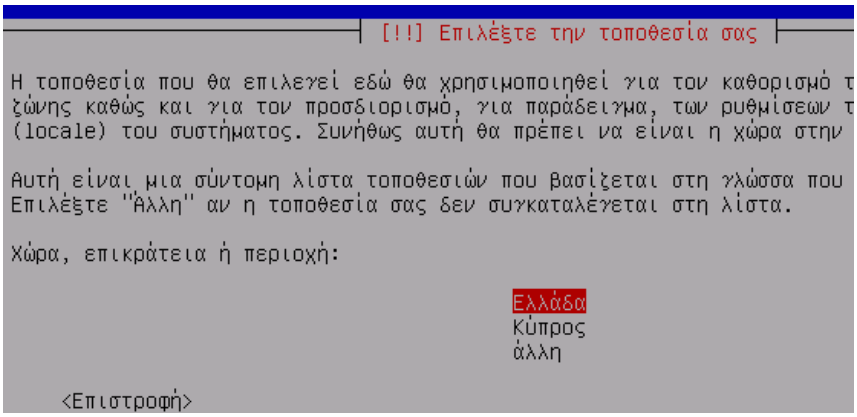
Ουσιαστικά ακολουθούμε την ίδια διαδικασία με το Live DVD ή USB που είδαμε παραπάνω, μόνο που στην αρχική οθόνη πηγαίνουμε στο "Install".



Επιλέγουμε τα Ελληνικά.

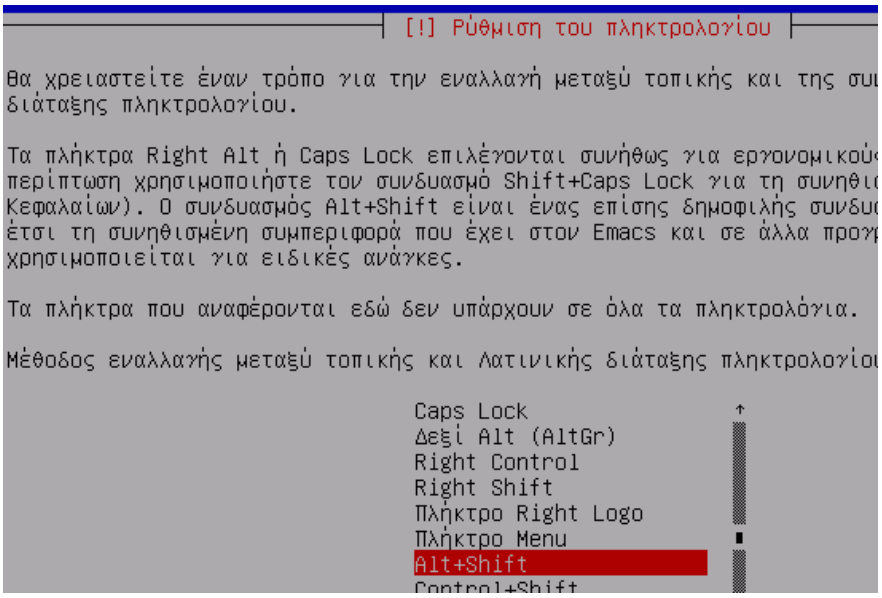
Το σύστημα μας προειδοποιεί πως η Ελληνική μετάφραση πιθανώς να μην είναι πλήρης. Το αποδεχόμαστε με "Ναι".

Κρατάμε τις προεπιλογές για την τοποθεσία...

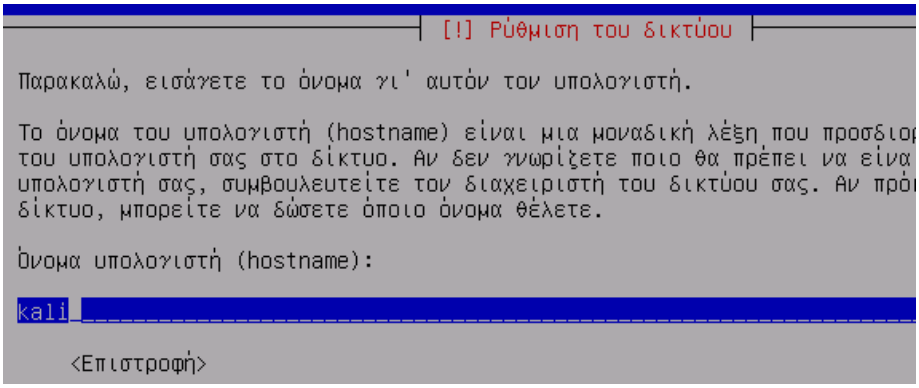


... και τη διάταξη πληκτρολογίου.

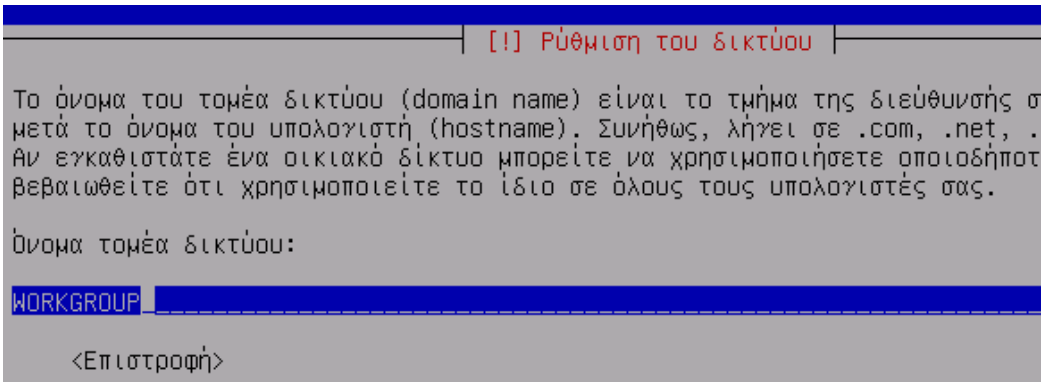
Αν θέλουμε, αλλάζουμε το συνδυασμό για την αλλαγή γλώσσας από το προεπιλεγμένο Alt+Shift.



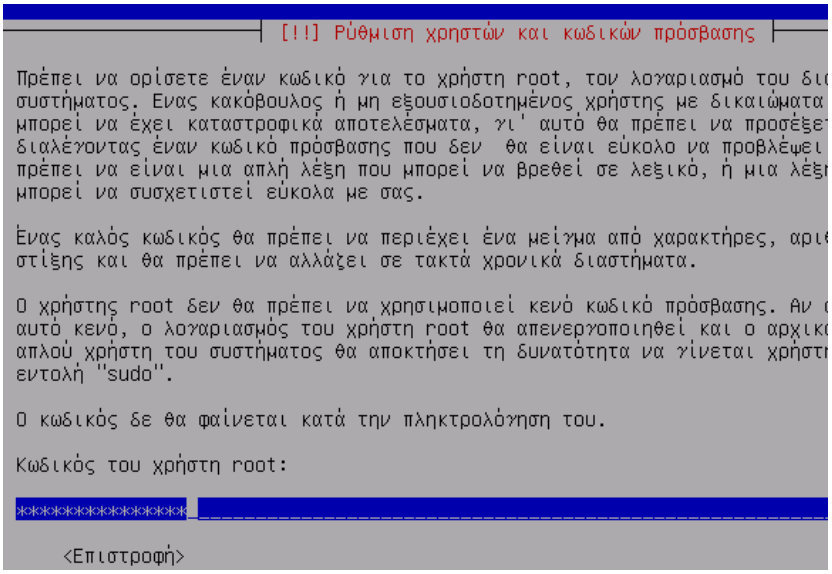
Στο όνομα του υπολογιστή βάζουμε ό,τι θέλουμε, αρκεί να μην έχει κενά ή σημεία στίξης και να είναι μοναδικό στο τοπικό δίκτυο.



Στον τομέα δικτύου γράφουμε "WORKGROUP", που είναι ο προεπιλεγμένος τομέας δικτύου που χρησιμοποιούν τα Windows.

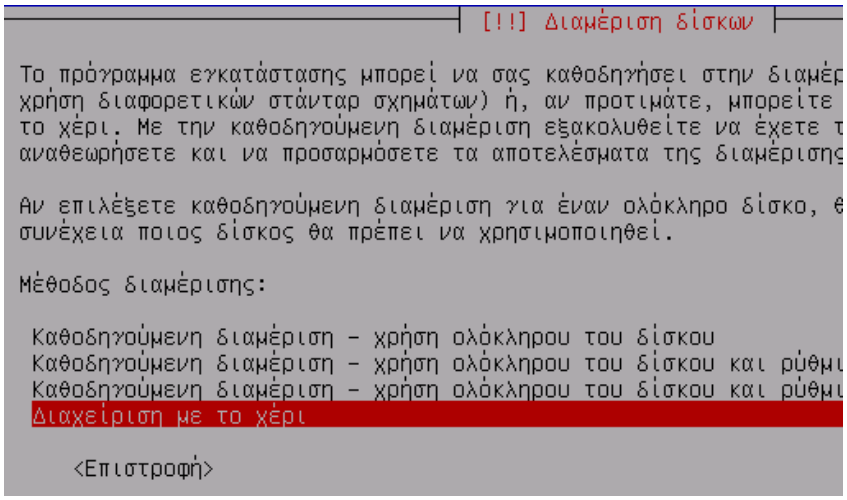


Δημιουργούμε έναν ισχυρό κωδικό για τον χρήστη root, που αμέσως μετά θα μας ζητηθεί να τον ξαναγράψουμε για επιβεβαίωση.

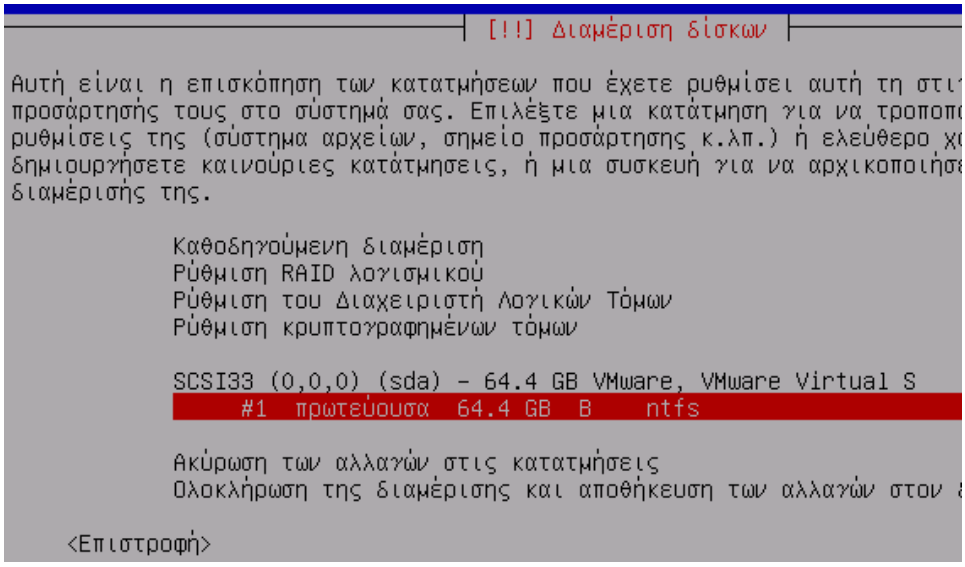


Εδώ είναι το σημαντικότερο κομμάτι σε όλη την εγκατάσταση Kali Linux: η διαχείριση των Partitions.

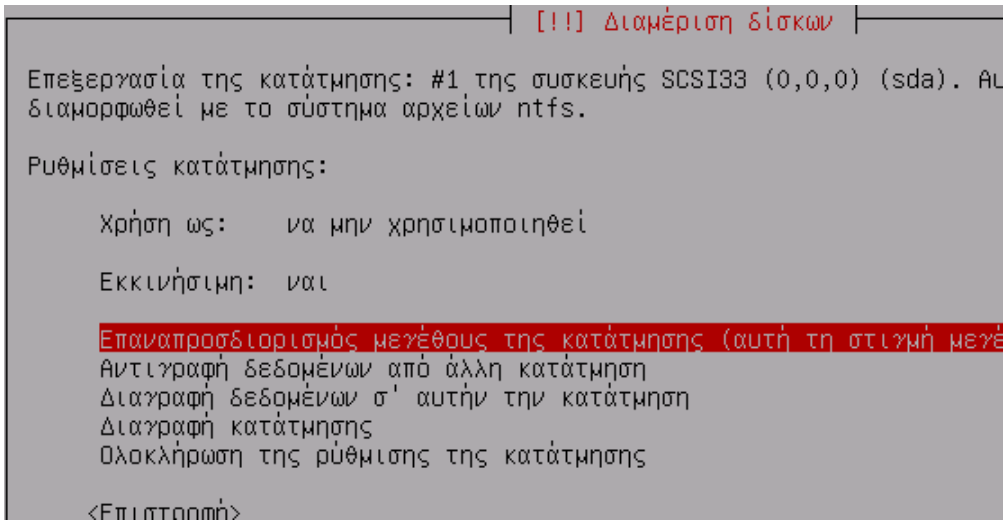
Σε περίπτωση που θέλουμε να κρατήσουμε τα Windows και να μην διαγραφεί όλο το περιεχόμενο του δίσκου, επιλέγουμε "Διαχείριση με το χέρι".



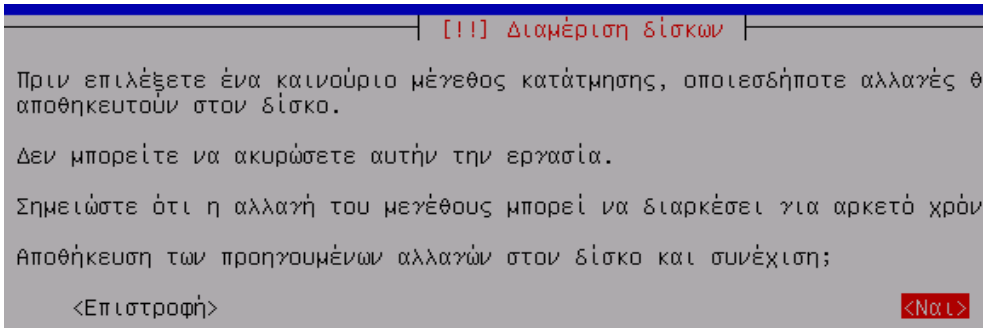
Πατάμε Enter στο partition με το σύστημα NTFS...



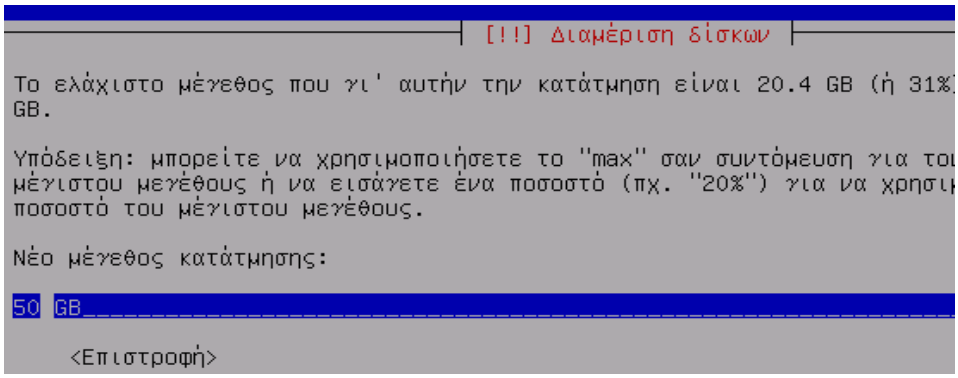
...και στην επόμενη οθόνη επιλέγουμε τον Επαναπροσδιορισμό μεγέθους της κατάτμησης.



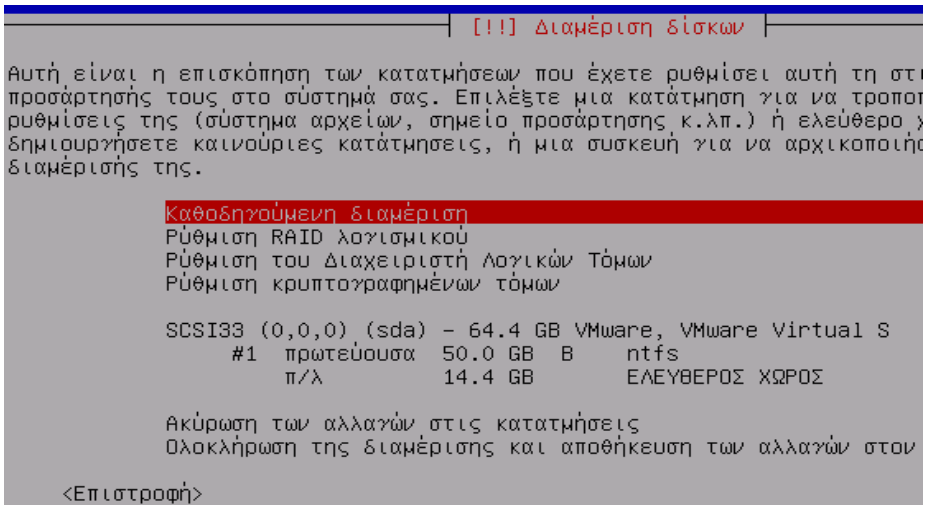
Το σύστημα μας προειδοποιεί πως πρέπει να έχουμε αποθηκεύσει προηγούμενες αλλαγές στο δίσκο για να προχωρήσει. Επιλέγουμε "Ναι".



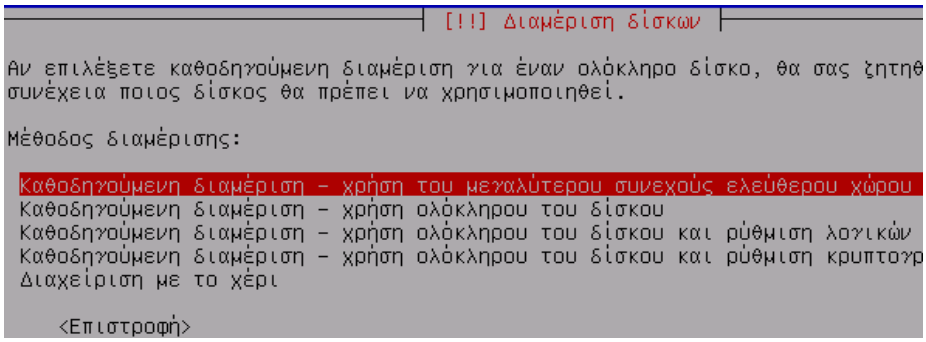
Γράφουμε το νέο μέγεθος που θέλουμε να είναι το NTFS partition. Στο παράδειγμα αφήσαμε 14,4GB για την εγκατάσταση Kali Linux, ορίζοντας το partition στα 50GB.



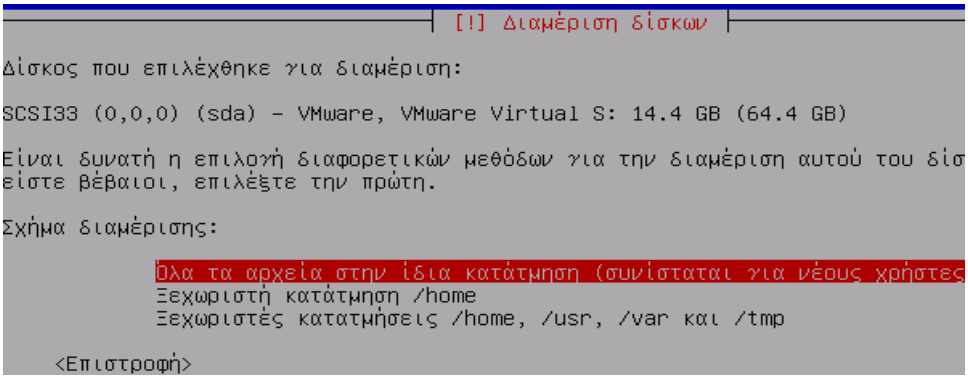
Πλέον, έχοντας ελεύθερο χώρο, επιστρέφουμε στην "Καθοδηγούμενη διαμέριση".



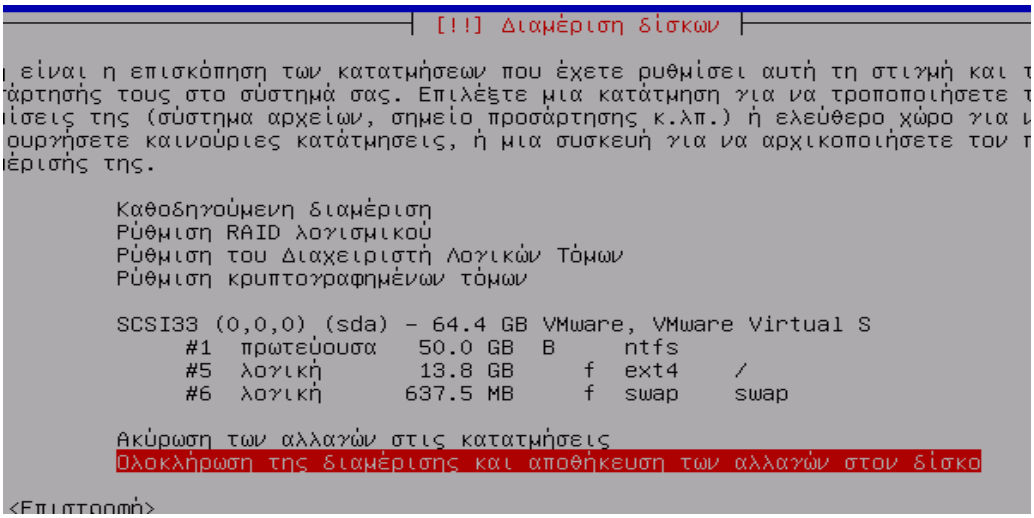
Έχει εμφανιστεί μια νέα επιλογή, "Χρήση του μεγαλύτερου συνεχούς ελεύθερου χώρου". Την επιλέγουμε.



Μπορούμε να έχουμε ξεχωριστό partition για το /home, αλλά αφού δεν θα χρησιμοποιούμε την εγκατάσταση Kali Linux σαν μια πλήρη διανομή, δεν έχει και τόσο μεγάλη σημασία.

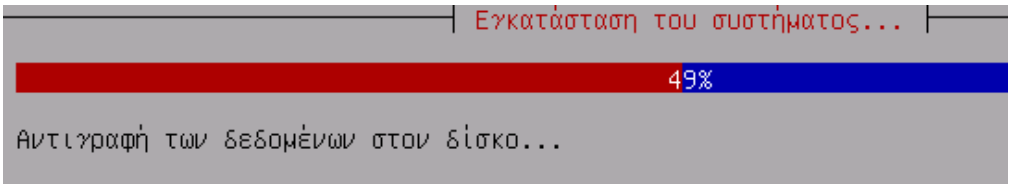


Το σύστημα μας δείχνει πως θα είναι τα partition. Αν είμαστε ευχαριστημένοι, επιλέγουμε ολοκλήρωση της διαμέρισης.



Επιβεβαιώνουμε τις αλλαγές επιλέγοντας το "Ναι"...

Από εδώ και μπρος στο μεγαλύτερο μέρος η εγκατάσταση είναι πλέον αυτόματη.

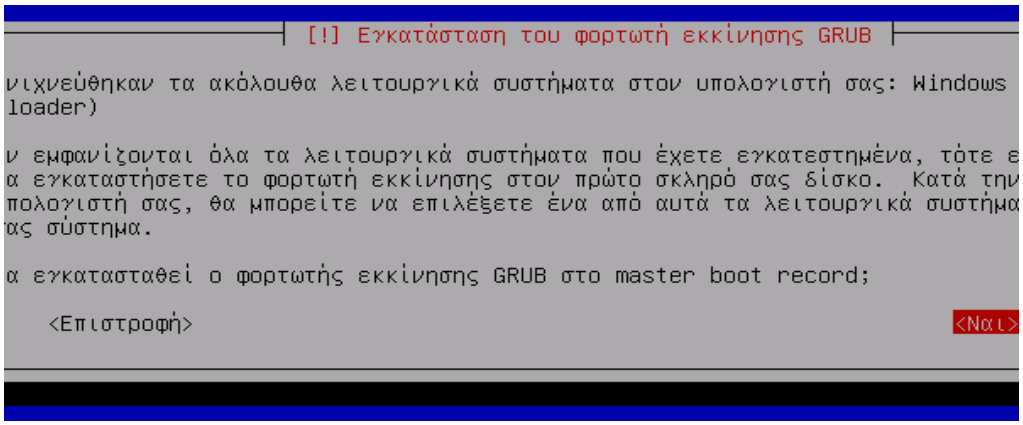


Απλά σε ένα σημείο θα ερωτηθούμε αν θέλουμε να κατεβάσουμε τα τελευταία αρχεία από τα mirrors του Kali Linux. Επιλέγουμε "Ναι".

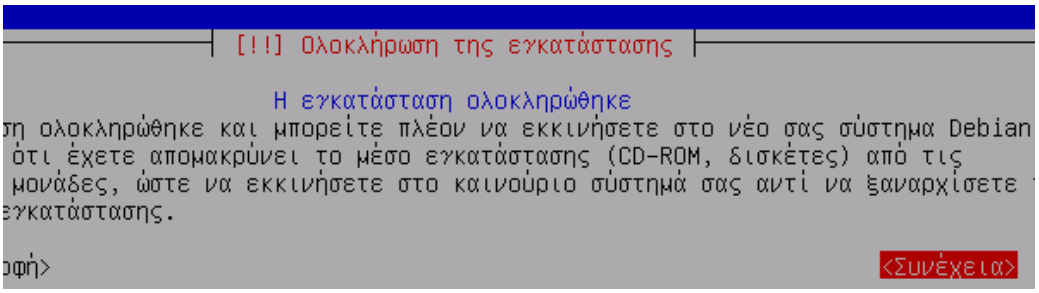
Εφόσον δεν χρησιμοποιούμε proxy server, αφήνουμε κενό το πεδίο στη ρύθμιση του Διαχειριστή πακέτων.

Η εγκατάσταση Kali Linux ολοκληρώνεται με το κατέβασμα πακέτων από το mirror.

Στο τελευταίο βήμα, επιλέγουμε το GRUB να αποθηκευτεί στο Master Boot Record.



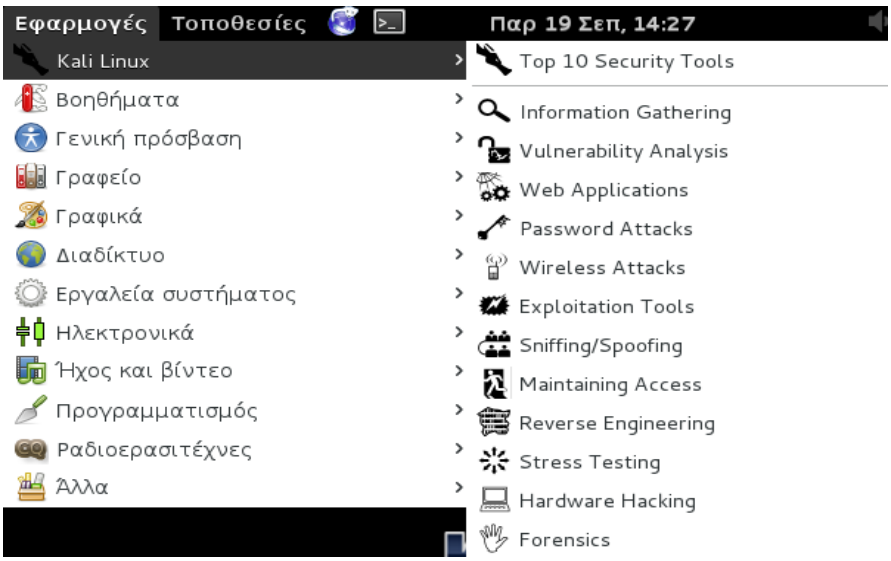
Η εγκατάσταση Kali Linux έχει πλέον ολοκληρωθεί. Αφαιρούμε το DVD ή το USB της εγκατάστασης και επιλέγουμε "Συνέχεια" για να κάνει ο υπολογιστής μας επανεκκίνηση.



Στην επόμενη εκκίνηση, μας υποδέχεται η οθόνη του GRUB για την επιλογή λειτουργικού συστήματος.

Αυτή τη φορά, η οθόνη για τη σύνδεση είναι στα Ελληνικά. Επιλέγουμε "Άλλος" και συνδεόμαστε ως root με το password που δημιουργήσαμε κατά την εγκατάσταση.

Επίσης στα Ελληνικά είναι τα μενού. Όμως όλα τα εργαλεία που αφορούν την ηλεκτρονική ασφάλεια είναι στα Αγγλικά.



ΣΥΜΠΕΡΑΣΜΑΤΑ

Η εργασία αυτή είχε σαν στόχο να παρουσιάσει τις αδυναμίες ενός ασύρματου δικτύου wi-fi, και πιο συγκεκριμένα των μεθόδων κρυπτογράφησης που χρησιμοποιούνται για την διασφάλιση της ασφάλειας κ τους τρόπους με τους οποίους προσπαθούν να διεισδύσουν οι χρήστες ,οι λεγόμενοι χάκερς (hackers), σε ένα ασύρματο δίκτυο.

Πέραν της ασφάλειας των δικτύων, γίνεται κατανοητή η ανάγκη για ασύρματη δικτύωση και τα πλεονεκτήματα της. Το σημερινό επίπεδο διάδοσης των δικτύων wi-fi, λόγω της ευελιξίας, της γρήγορης υλοποίησης και φυσικά το χαμηλό κόστος χρήσης, συντήρησης και εγκατάστασης έκανε την ασύρματη δικτύωση αρκετά προσιτή και ευρέως διαδεδομένη.

Με την διάδοση της ασύρματης δικτύωσης εμφανίστηκαν πολλές απειλές και σαν αποτέλεσμα να γίνουν εμφανή τα τρωτά σημεία των δικτύων.

Με τις επιθέσεις που έγιναν διαπιστώνονται στην πραγματικότητα οι αδυναμίες ενός ασύρματου δικτύου και η ευκολία παραβίασης του.

Το φυσικό μέσο μετάδοσης ενός δικτύου wi-fi είναι ταυτόχρονα πλεονέκτημα και μειονέκτημα. Λόγω της εύκολης πρόσβασης, είναι αρκετά ελκυστικό σε επιθέσεις. Το θέμα της ασφάλειας σε ένα ασύρματο δίκτυο είναι το πιο σημαντικό μειονέκτημα που μπορεί να οδηγήσει στην μη επιλογή τέτοιοι τύπου δικτύωσης.

Η κρυπτογράφηση WEP, αρχικά θεωρήθηκε επαρκής, αλλά με την εξέλιξη της τεχνολογίας και τη διακίνηση αρκετά σημαντικών και προσωπικών πληροφοριών κρίνεται ακατάλληλη.

Στην επίδειξη WEP cracking διαπιστώνεται πλήρως η αδυναμία της, γιατί με μια απλή προσπάθεια συλλογής αρκετών πακέτων IV’s ανακτήθηκε το WEP key μέσα σε λίγα λεπτά. Η WEP κρυπτογράφηση θα μπορούσε να εφαρμοστεί σε περιπτώσεις που η ασφάλεια της πληροφορίας που κινείται στο δίκτυο δεν έχει ιδιαίτερη σημασία.

Λύσεις που προτάθηκαν ήταν οι παραμετροποιήσεις του router-access point και η χρήση νεότερων τεχνολογιών όπως το WPA και το WPA2.

Ωστόσο, ακόμα και αυτές οι μέθοδοι έχουν αποδειχθεί αρκετά ανασφαλείς καθώς στις αρχές του 2008 παραβιάστηκε και η WPA. Βέβαια παρέχει τη δυνατότητα της χρήσης του αλγορίθμου AES που θωρακίζει σημαντικά το δίκτυο.

Το μέλλον της ασύρματης ασφάλειας βρίσκεται στις νεότερες εκδόσεις του προτύπου IEEE 802.11, όπως 802.11i και 802.11n.

Παρότι οι δυνατότητες μετάδοσης είναι υψηλές, έχει ακόμα προβλήματα ασφάλειας. Βεβαία αξίζει να σημειωθεί πως όσο εξελίσσονται τα επίπεδα ασφαλείας, τόσο εξελίσσονται και οι μηχανισμοί παραβίασης τους.

Και αυτό παρουσιάστηκε μέσα από την εργασία, πόσο καλά το γνωρίζουν οι hackers με τη βοήθεια διαφόρων προγραμμάτων και μέσα σε λίγο χρόνο μπορούν να αποκτήσουν πρόσβαση σε ένα οποιοδήποτε ασύρματο δίκτυο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

TANENBAUM – WETHERALL (2011). ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ 5η Αμερικανική Έκδοση. Αθήνα: Εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ

Μαρκομανωλάκη Αικατερίνη, Πτυχιακή εργασία «Ασφάλεια σε ασύρματα δίκτυα 802.11», Ηράκλειο 2010, ΤΕΙ Κρήτης

Πάλλης Ε., Εισαγωγή στα Ασύρματα Δίκτυα. Ηράκλειο Κρήτης: Τμήμα Εφαρμοσμένης Πληροφορικής, 2000

Κάτος Β. – Στεφανίδης Γ. , Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης, ΖΥΓΟΣ, 396, 2003

Frankel, S., Bemard, E., Les, O., & Scarfone, K. (2007). Establishing Wireless Robust Security Networks: A Guide to 802.11i. Special Publication 800-97.

Peikari C. & Fogie S., Maximum Wireless Security, 2002

Ιστοσελίδες

www.ebusinessforum.gr

http://greg61.gr/blog/

https://secnews.gr/126301/wpa2-hacking/ ------ Giorgos /inet Σεπτέμβριος 12, 2014 9:31 πμ

http://www.kalitutorials.net/2013/08/kali-linux.html ------ Shashwat Chaudhary 16 Ιουλίου 2014

https://www.pcsteps.gr/33049-%CE%B5%CE%B3%CE%BA%CE%B1%CF%84%CE%AC%CF%83%CF%84%CE%B1%CF%83%CE%B7-kali-linux-%CF%84%CE%BF-%CE%BB%CE%B5%CE%B9%CF%84%CE%BF%CF%85%CF%81%CE%B3%CE%B9%CE%BA%CF%8C-%CF%84%CF%89%CE%BD-hacker/