ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Επίδειξη Επιθέσεων σε Αστικά Ασύρματα Δίκτυα

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αριστείδης Χρονάκης

Α.Μ. ΜΕ/0634

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του μεταπτυχιακού προγράμματος ***Διδακτική της Τεχνολογίας και Ψηφιακά Συστήματα*** στην κατεύθυνση ***Ψηφιακών Επικοινωνιών και Δικτύων*** του τμήματος ***Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων*** του ***Πανεπιστημίου Πειραιώς.***

Ο κύριος σκοπός της παρούσης διπλωματικής εργασίας είναι η επίδειξη επίθεσης εναντίων ασυρμάτων δικτύων.

Στο πρώτο και δεύτερο μέρος παρατίθενται γενικές πληροφορές για τα ασύρματα δίκτυα και την ασφάλεια τους παρέχοντας στους αναγνώστες πληροφορίες σχετικά με τους κινδύνους που διατρέχουν και μερικούς απο τους κύριους μηχανισμούς ασφαλείας που έχουν αναπτυχθεί.

Στο μεγαλύτερο μέρος της παρατίθενται βήμα προς βήμα η διαδικασία παραβίασης των κυρίων μηχανισμών ασφαλείας που χρησιμοποιούνται απο ένα Access Point. Η επίθεση διενεργείτε με την βοήθεια εργαλείων και στις πλατφόρμες, των λειτουργικών Windows και Linux.

Τέλος προτείνονται αντίμετρα τα οποία κάθε χρήστης ενός ασυρμάτου δικτύου θα μπορούσε να υϊοθετήσει για να προστατευθεί απο κακόβουλες επθέσεις.

<u>Λέξεις Κλειδιά</u>

ασφάλεια, κινητές επικοινωνίες, ασύρματες επικοινωνίες, ασύρματα δίκτυα,
WPA, aircrack, omnipeek, WEP, kismet, netstumbler

ΕΥΧΑΡΙΣΤΙΕΣ

Η πραγματοποίηση της παρούσας διπλωματικής εργασίας δεν θα ήταν εφικτή χωρίς την βοήθεα του καθηγητή Ξενάκη Χρήστου λέκτορα του Πανεπιστημίου Πειραιώς και επιβλέποντα για την ευκαιρία που μας έδωσε να εργαστώ σε ένα τόσο σύγχρονο και συνάμα ενδιαφέρον αντικείμενο, καθώς και για τη συνεχή βοήθεια και καθοδήγηση που μου παρείχε καθόλη την διάρκεια της εργασίας.

Κλείνοντας θα ήθελα να ευχαριστήσω τους γονείς μου και την πολυαγαπημένη μου Παρασκευή για την αμέρηστη συμπαράσταση και βοήθεια που μου παρείχαν καθόλη την διάρκεια της διετής φοίτησής μου στο μεταπτυχιακό.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΕΙΣΑΓΩΓΗ - ΠΡΟΛΟΓΟΣ

Οι ασύρματες τεχνολογίες γνωρίζουν μεγάλη άνθηση την τελευταία δεκαετία. Η κινητικότητα που παρέχουν και η ευκολία πρόσβασης του χρήστη στο τηλεφωνικό δίκτυο είναι δύο από τους πολλούς λόγους για αυτή την ανάπτυξη της συγκεκριμένης αγοράς. Η ασφάλεια που παρέχουν είναι λοιπόν ένα αρκετά σημαντικό θέμα αφού λόγω της χρήσης τους σε μεγάλη κλίμακα σε σημείο πια που ολόκληρες εταιρείες παιρνούν τεράστιο όγκο σημαντικών δεδομένων μέσα απο αυτά κάνουν ακόμα μεγαλύτερη την όποια αδυναμία τους. Τα ασύρματα συστήματα είναι πολύ πιο ευάλωτα από τα ενσύρματα συστήματα σε ότι αφορά την ασφάλεια, αφού ως μέσο μετάδοσης χρησιμοποιούν τον αέρα. Οποιοσδήποτε μπορεί να λάβει δεδομένα που μεταδίδονται στον αέρα ακόμα και αν δεν προορίζονται για αυτόν. Την τελευταία δεκαετία είναι δημοφιλές το wardriving. Το wardriving είναι μια πρακτική κατα την οποία ένας χρήστης του διαδικτύου περιπλανιέται στους δρόμους συνοικιών εφοδιασμένος με συσκευή που έχει δυνατότητα ασύρματης πρόσβασης στο Διαδίκτυο με σκοπό να εντοπίσει ασύρματα δίκτυα πρόσβασης στο Διαδίκτυο οικιακής ή επαγγελματικής χρήσης και να χαρτογραφήσει την ύπαρξή . Εκτός του σκοπού της χαρτογράφησης το wardriving χρησιμοποιείται απο κακόβουλους χρήστες οι οποίοι ψάχνουν για δίκτυα με σκοπό την παράνομη χρήση των πόρων τους. Αυτό το κομμάτι των κακόβουλων χρηστών στς μέρες μας έχει γίνει πραγματικός πονοκέφαλος στους ιδιοκτήτες και τους διαχειριστές ασυρμάτων δικτύων.

1.1 ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΣΥΡΜΑΤΗ ΤΕΧΝΟΛΟΓΙΑ

Οι ασύρματες τεχνολογίες καθιστούν δυνατή την επικοινωνία δύο ή περισσοτέρων συσκευών, χωρίς να απαιτείται η χρήση δικτύου ή κάποιας περιφερειακής καλωδίωσης. Αυτό που ξεχωρίζει τις τεχνολογίες ασύρματης διάδοσης από εκείνες

της ενσύρματης είναι η χρήση πομπών ραδιοκυμάτων, ως μέσα μετάδοσης δεδομένων, σε αντίθεση με τις δεύτερες, οι οποίες χρησιμοποιούν καλώδια.

Οι ασύρματες τεχνολογίες ποικίλουν από πολύπλοκα συστήματα, όπως τα ασύρματα δίκτυα (Wireless Local Area Networks – WLANs) και τα κινητά τηλέφωνα, σε απλές συσκευές, όπως τα ασύρματα τηλέφωνα και μικρόφωνα, καθώς και άλλες συσκευές οι οποίες δεν επεξεργάζονται ή αποθηκεύουν πληροφορίες. Επιπλέον, αυτές οι τεχνολογίες χρησιμοποιούν και συσκευές υπερύθρων (IR), όπως ασύρματα τηλεχειριστήρια, ασύρματα πληκτρολόγια και ποντίκια υπολογιστών, καθώς και ασύρματα ακουστικά στερεοφωνικών, τα οποία απαιτούν άμεση οπτική επαφή και μικρή απόσταση μεταξύ του πομπού και του δέκτη.

Στο κεφάλαιο αυτό θα κάνουμε μία διεξοδική ανάλυση των ασύρματων δικτύων, συσκευών και κριτηρίων που απαρτίζουν μία ασύρματη τεχνολογία, καθώς και των θεμάτων ασφάλειας που προβληματίζουν τους κατασκευαστές και διαχειριστές μίας τέτοιας τεχνολογίας.

1.2 Ασύρματα Δίκτυα

Τα ασύρματα δίκτυα (Wireless Networks) εξυπηρετούν ως μηχανισμοί μετάδοσης μεταξύ δύο συσκευών, και μεταξύ συσκευών και των παραδοσιακών ενσύρματων δικτύων. Τα ασύρματα δίκτυα μπορεί να ποικίλουν αλλά χωρίζονται κυρίως σε τρεις κατηγορίες, ανάλογα με την περιοχή κάλυψής τους [1][7][8]:

- Τα ***Ασύρματα Δίκτυα Ευρείας Περιοχής*** (Wireless Wide Area Networks – WWANs), τα οποία περιλαμβάνουν τεχνολογίες ευρείας κάλυψης όπως το CDPD, το GSM, και το Mobitex.
- Τα ***Ασύρματα Τοπικά Δίκτυα*** (Wireless Local Area Networks – WLANs), τα οποία περιλαμβάνουν τα 802.11, τα HiperLANs και πολλά άλλα.
- Τα ***Ασύρματα Ιδιωτικά Δίκτυα*** (Wireless Personal Area Networks – WPANs), τα οποία αντιπροσωπεύουν τεχνολογίες όπως τα Bluetooth και τις IR.

1.2.1 Ασύρματα Τοπικά Δίκτυα (WLANs)

Τα WLANs παρέχουν μεγαλύτερη ευελιξία και φορητότητα, λόγω της χρήσης των σημείων πρόσβασης (Access Points – APs) για την σύνδεση των υπολογιστών ή άλλων εξαρτημάτων στο δίκτυο, αναλογικά με τα παραδοσιακά τοπικά ενσύρματα δίκτυα (Local Area Networks - LANs), τα οποία χρησιμοποιούν καλώδια.

Η τεχνολογία WLAN χρονολογείται από τα μέσα της δεκαετίας του ’80, όταν η Ομοσπονδιακή Επιτροπή Τηλεπικοινωνιών (Federal Communications Commission – FCC) κατέστησε για πρώτη φορά διαθέσιμο το φάσμα RF στην βιομηχανία. Από τότε έως και τις αρχές της δεκαετίας του ’90 η ανάπτυξή της ήταν σχετικά αργή, ενώ σήμερα η τεχνολογία WLAN υπόκειται σε εκπληκτικά μεγάλη ανάπτυξη. Το κλειδί για αυτήν την ανάπτυξη είναι η αυξανόμενο εύρος ζώνης το οποίο κατέστη εφικτό από το πρότυπο IEEE 802.11.

1.2.1.1 Κατανομές Συχνότητας και Δεδομένων

Ο οργανισμός IEEE έχει ορίσει πολλά πρότυπα για τα WLANs, μερικά από τα οποία συνοψίζονται στον παρακάτω πίνακα (Πίνακας 1-1) [2].

Το πρότυπο 802.11a είναι το πιο διαδεδομένο από την οικογένεια των 802.11. Λειτουργεί στην περιοχή συχνοτήτων των 5 GHz και χρησιμοποιεί OFDM πολυπλεξία (Orthogonal Frequency Division Multiplexing) για μείωση των παρεμβολών. Το 802.11b λειτουργεί στην περιοχή συχνοτήτων 2,4 – 2,5 GHz και χρησιμοποιεί την τεχνολογία απευθείας διάδοσης φάσματος (direct sequence spread – spectrum).

Πρότυπο	Περιγραφή	Διαθεσιμότητα
IEEE 802.11	Ρυθμοί δεδομένων μέχρι	Ιούλιος 1997

	2Mbps στην 2.4GHz ISM μπάντα.	
IEEE 802.11a	Ρυθμοί δεδομένων μέχρι 54Mbps στην 5GHz UNII μπάντα.	Σεπτέμβριος 1999
IEEE 802.11b	Ρυθμοί δεδομένων μέχρι 11Mbps στην 2.4 ISM μπάντα.	Σεπτέμβριος 1999

Πίνακας 1-1 Πρότυπα Ασύρματων Δικτύων

1.2.1.2 Αρχιτεκτονική ενός 802.11

Το πρότυπο IEEE 802.11 επιτρέπει την κατασκευή είτε από σημείο σε σημείο (peer-to-peer) δικτύων είτε δικτύων βασισμένων σε σταθερά access points (AP), με τα οποία μπορούν να επικοινωνήσουν οι κινητοί κόμβοι. Για το λόγο αυτόν, το δεδομένο πρότυπο καθορίζει δύο βασικές τοπολογίες δικτύου: το δίκτυο υποδομής (infrastructure network) και το δίκτυο συγκεκριμένου σκοπού (ad hoc network) [1][7].

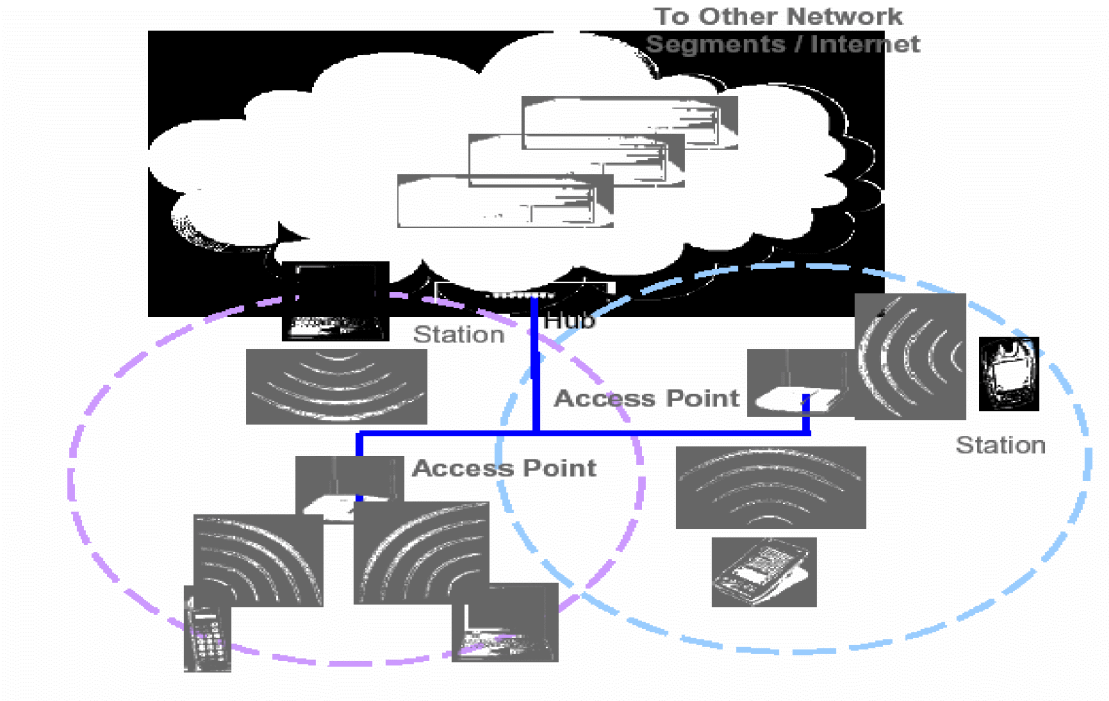
1.2.1.2.1 Δίκτυο Υποδομής

Το **δίκτυο υποδομής (infrastructure network)** είναι φτιαγμένο για να επεκτείνει την εμβέλεια του ενσύρματου LAN σε ασύρματες κυψέλες. Ένας φορητός υπολογιστής ή άλλη κινητή συσκευή μπορεί να κινείται από κυψέλη σε κυψέλη (από AP σε AP) διατηρώντας ταυτόχρονα πρόσβαση στους πόρους του LAN. Μια κυψέλη είναι η περιοχή που καλύπτεται από ένα AP και καλείται **BSS** (*Basic Service Set*). Το σύνολο όλων των κυψελών ενός δικτύου υποδομής λέγεται **ESS** (*Extended Service Set*). Αυτή η τοπολογία είναι χρήσιμη για την παροχή ασύρματης κάλυψης κτιρίων ή πανεπιστημιουπόλεων. Παρατάσσοντας πολλά APs με επικαλυπτόμενες περιοχές κάλυψης, οι οργανισμοί μπορούν να πετύχουν κάλυψη ευρείας περιοχής (WLAN). Η τεχνολογία WLAN μπορεί να χρησιμοποιηθεί για να αντικαταστήσει ολοκληρωτικά τα ενσύρματα LANs και να επεκτείνει την υποδομή τους.

Ένα περιβάλλον WLAN έχει ασύρματους σταθμούς – πελάτες (clients) που χρησιμοποιούν ασύρματα μόντεμ για την επικοινωνία τους με ένα AP. Οι σταθμοί

αυτοί είναι εξοπλισμένοι με μια ασύρματη κάρτα δικτύου (*Network Interface Card* - **NIC**) που αποτελείται από έναν ασύρματο πομποδέκτη και την λογική ώστε να αλληλεπιδρά με την μηχανή και το λογισμικό του client. Ένα AP, το οποίο καλύπτει τυπικά περιοχές μεγαλύτερες από περίπου 100 μέτρα, αποτελείται από έναν ασύρματο πομποδέκτη από τη μια πλευρά και μια γέφυρα στο ενσύρματο backbone από την άλλη. Το AP, μια στατική συσκευή που αποτελεί μέρος της ενσύρματης υποδομής, είναι το ανάλογο του σταθμού βάσης στις κυψελοειδείς επικοινωνίες. Όλες οι μεταδόσεις μεταξύ των σταθμών πελατών και των σταθμών και ενσύρματου δικτύου περνούν μέσα από το AP.

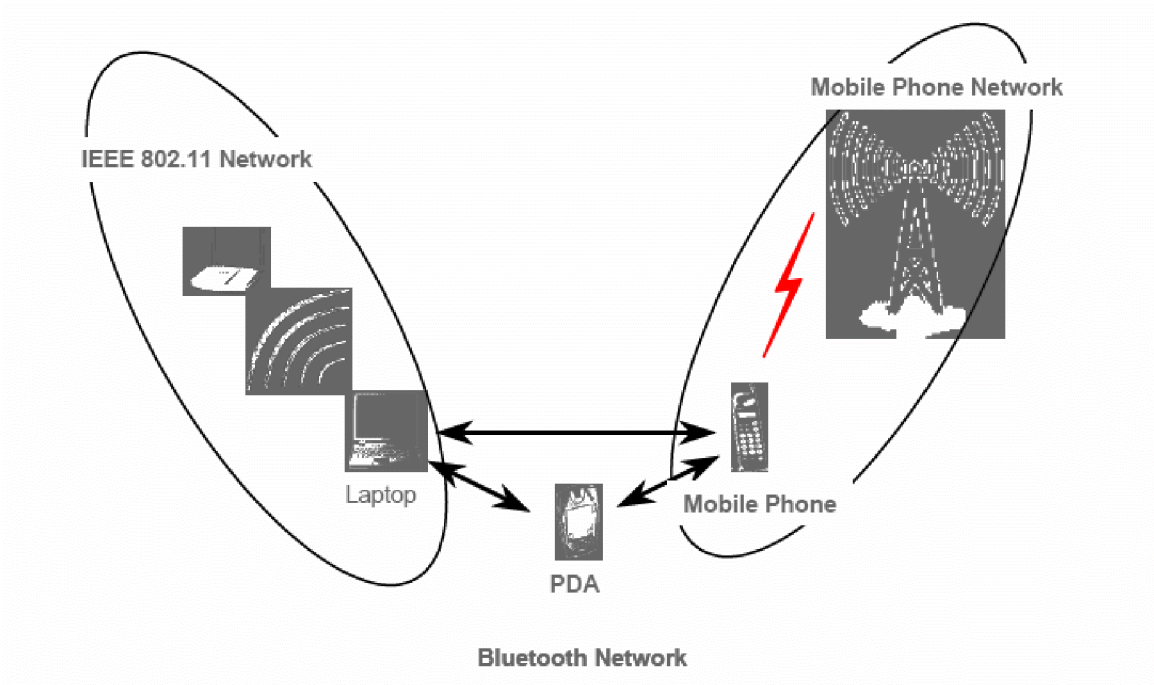
Η βασική τοπολογία ενός WLAN απεικονίζεται στο σχήμα 1.1.



Σχήμα 1.1 ***Βασική Τοπολογία ενός 802.11 Ασύρματου LAN***

1.2.1.2.2 Ad Hoc Δίκτυο

Τα Ad hoc δίκτυα, όπως τα Bluetooth, είναι δίκτυα σχεδιασμένα ώστε να συνδέουν δυναμικά απομακρυσμένες συσκευές όπως κινητά τηλέφωνα, φορητούς υπολογιστές (laptops), και PDAs. Αυτά τα δίκτυα ονομάζονται “ad hoc” εξαιτίας των ευέλικτων δικτυακών τοπολογιών τους. Ενώ τα WLANs χρησιμοποιούν μία σταθερή δικτυακή υποδομή, τα ad hoc δίκτυα υποστηρίζουν τυχαίους δικτυακούς σχηματισμούς, στηριζόμενα σε ένα master-slave σύστημα το οποίο είναι συνδεδεμένο ασύρματα, ώστε να καθιστά τις συσκευές ικανές να επικοινωνήσουν.



Σχήμα 1.2 **Ενδεικτικό Ad Hoc Δίκτυο**

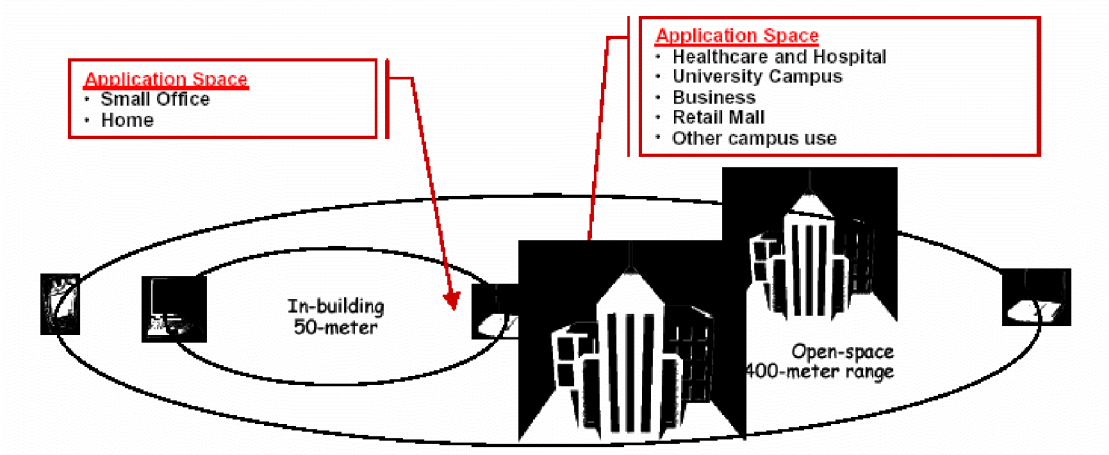
1.2.1.2.3 Συστατικά ενός Ασύρματου LAN

Ένα WLAN συνίσταται από δύο τύπους εξοπλισμού: έναν **ασύρματο σταθμό** και ένα **access point**. Ο ασύρματος σταθμός, ή πελάτης, είναι τυπικά ένας φορητός υπολογιστής εξοπλισμένος με μία ασύρματη κάρτα δικτύου NIC. Οι κάρτες δικτύου χρησιμοποιούν ραδιοσήματα για την δημιουργία συνδέσεων στο WLAN. Το AP, το οποίο δρα ως γέφυρα μεταξύ των ασύρματων και ενσύρματων δικτύων, αποτελείται από ένα ραδιοπομπό, από μία διεπαφή ενσύρματου δικτύου τύπου 802.3, και από ένα λογισμικό γεφυροποίησης. Το AP λειτουργεί ως βασικός σταθμός για το ασύρματο δίκτυο, συγκεντρώνοντας πολλαπλούς ασύρματους σταθμούς στο ενσύρματο δίκτυο.

1.2.1.4 Εμβέλεια

Η αξιόπιστη κάλυψη για τα 802.11 WLANs εξαρτάται από διάφορους παράγοντες, συμπεριλαμβανομένου του απαιτούμενου ρυθμού δεδομένων και της χωρητικότητας, των πηγών παρεμβολών των ραδιοσυχνοτήτων, της φυσικής περιοχής και των χαρακτηριστικών της, και την ισχύ, την συνδετικότητα, και χρήση της κεραίας. Θεωρητικά, οι εμβέλειες κυμαίνονται από **29 μέτρα (για 11 Mbps),** σε μια κλειστή περιοχή, έως και **485 μέτρα (για 1 Mbps)** σε μια ανοιχτή περιοχή. Εντούτοις, σύμφωνα με εμπειρικές αναλύσεις, η τυπική εμβέλεια για την διασύνδεση του

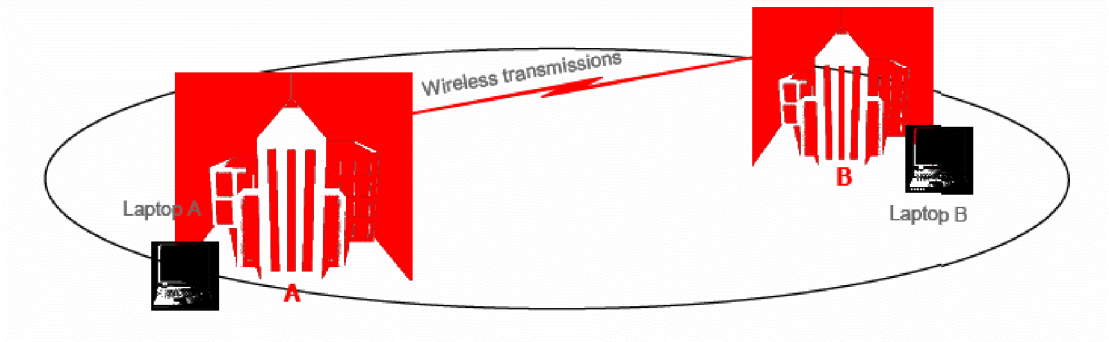
εξοπλισμού ενός 802.11 είναι περίπου **50 μέτρα,** για εσωτερικούς χώρους. Μία εμβέλεια **400 μέτρων** καθιστά τα WLANs την ιδανική τεχνολογία για πολλές εφαρμογές σε πανεπιστημιουπόλεις. Είναι σημαντικό να σημειωθεί ότι η χρήση ειδικών κεραιών με αυξημένο κέρδος είναι δυνατόν να συντελέσει στην αύξηση της εμβέλειας.



Σχήμα 1.3 Τυπική εμβέλεια ενός 802.11 WLAN

Τα APs μπορούν επίσης να παρέχουν την λειτουργία "γεφυροποίησης" (bridging). Η γεφυροποίηση συνδέει δύο ή περισσότερα δίκτυα με τέτοιο τρόπο, ώστε να μπορούν να επικοινωνούν μεταξύ τους και να ανταλλάσσουν την κίνηση του δικτύου. Η λειτουργία αυτή εμπεριέχει είτε μία από σημείο σε σημείο (point-to-point) είτε από ένα σημείο προς πολλά (point-to-multipoint) αρχιτεκτονική. Σύμφωνα με την point-to-point αρχιτεκτονική, δύο LANs συνδέονται μεταξύ τους δια μέσου των αντίστοιχων APs των LANs. Όσον αφορά την multipoint γεφυροποίηση, το υποδίκτυο ενός LAN συνδέεται με άλλα υποδίκτυα ενός άλλου LAN μέσω του AP κάθε υποδικτύου.

Το σχήμα 1.4 απεικονίζει την point-to-point γεφυροποίηση μεταξύ δύο LAN.



Σχήμα 1.4 ***Γεφυροποίηση των Access Points***

1.2.2 Πλεονεκτήματα Ασύρματων Δικτύων

Τα WLANs διαθέτουν τέσσερα θεμελιώδη πλεονεκτήματα:

- **Κινητικότητα Χρήστη:** Οι χρήστες μπορούν να έχουν πρόσβαση σε αρχεία, στους πόρους του δικτύου και στο διαδίκτυο, χωρίς την ύπαρξη σύνδεσης τους με καλώδια.
- **Γρήγορη Εγκατάσταση:** Ο απαιτούμενος χρόνος εγκατάστασης ενός δικτύου έχει μειωθεί διότι οι συνδέσεις στο δίκτυο γίνονται πλέον χωρίς την χρήση καλωδίων και την προσαρμογή τους ανάμεσα από τοίχους και οροφές.
- **Ευελιξία:** Τα ασύρματα δίκτυα διαθέτουν, επίσης, μεγάλη ευελιξία εξαιτίας της ευκολίας με την οποία εγκαθίστανται ή γκρεμίζονται, ανάλογα με τις ανάγκες κάθε οργανισμού.
- **Ευκολία Κλιμάκωσης:** Οι τοπολογίες WLAN δικτύων μπορούν να κλιμακώνονται, από μικρά peer-to-peer δίκτυα σε πολύ μεγάλα δίκτυα επιχειρήσεων, έτσι ώστε να ικανοποιούν συγκεκριμένες ανάγκες ως προς την εγκατάσταση και την εφαρμογή τους.

- Σε αντίθεση με τα συστήματα packet radio το Wi-Fi χρησιμοποιεί μη κατοχυρωμένο ραδιοφάσμα και δεν χρειάζεται έγκριση των αρχών για ιδιωτική ανάπτυξη .
- Επιτρέπει στα LANs να αναπτυχθούν χωρίς καλωδίωση , πιθανώς μειώνοντας το κόστος της ανάπτυξης και επέκτασης του δικτύου . Μέρη όπου τα καλώδια δεν μπορούν να υπάρχουν όπως εξωτερικές περιοχές και ιστορικά κτίρια , μπορούν να φιλοξενήσουν ασύρματα δίκτυα .
- Προ'ι'όντα Wi-Fi χρησιμοποιούνται μαζικά στην αγορά . Διαφορετικές μάρκες σημείων πρόσβασης και διεπαφών δικτύου πελατών συνεργάζονται σε ένα βασικό επίπεδο της υπηρεσίας .
- Ο ανταγωνισμός μεταξύ των πωλητών έχει μειώσει τις τιμές σημαντικά από την κυκλοφορία τους .
- Πολλά δίκτυα Wi-Fi υποστηρίζουν το roaming , στο οποίο μία φορητή συσκευή πελάτη όπως ένας φορητός υπολογιστής , μπορεί να μετακινηθεί από ένα σημείο πρόσβασης σε ένα άλλο καθώς ο χρήστης μετακινείται σε ένα κτίριο ή σε μια περιοχή .
- Πολλά σημεία πρόσβασης και διεπαφές δικτύων υποστηρίζουν διάφορα επίπεδα κρυπτογράφησης για να προστατέψουν τα δεδομένα από υποκλοπή.
- Το Wi-Fi είναι ένα παγκόσμιο σετ από στάνταρς . Αντίθετα με τους πελάτες δικτύου κυψελών , ο ίδιος Wi-Fi πελάτης μπορεί να δουλέψει σε διαφορετικές χώρες ανά τον κόσμο (αν και μπορεί να χρειαστεί κάποιες ρυθμίσεις στο λογισμικό) .

1.2.3 Μειονεκτήματα Ασύρματων Δικτύων

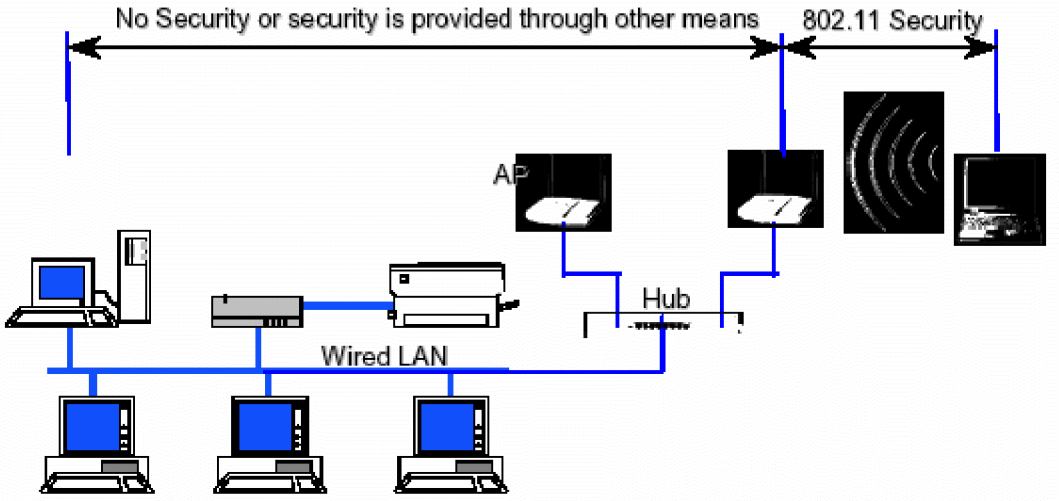
- Η χρησιμοποίηση της συχνότητας των 2.4GHz από το Wi-Fi δεν απαιτεί άδεια από τον περισσότερο κόσμο με την προϋπόθεση ότι κάποιος μένει κάτω από τα θεσμοθετημένα τυπικά όρια και με την προϋπόθεση ότι κάποιος δέχεται παρεμβολές από άλλες πηγές , συμπεριλαμβανομένων παρεμβολές που προκαλούν την δυσλειτουργία των συσκευών του .
- Η νομοθεσία δεν είναι ίδια παντού . Οι περισσότερες ευρωπα'ι'κές χώρες επιτρέπουν 2 κανάλια παραπάνω από αυτά των προδιαγραφών b , g . Η Ιαπωνία έχει και ένα ακόμα κανάλι , και χώρες όπως η Ισπανία απαγορεύουν την χρήση καναλιών με μικρότερους αριθμούς . Επιπλέον κάποιες χώρες όπως

η Ιταλία συνήθιζε να ζητά μία «γενική άδεια» για οποιοδήποτε Wi-Fi που χρησιμοποιούνταν έξω από τα επιτρεπτά όρια ή ζητούσε κάτι παρόμοιο με εγγραφή χειριστή.

- Το 802.11b και το 802.11g χρησιμοποιούν το φάσμα των 2.4GHz , στο οποίο υπάρχει συνωστισμός από άλλες συσκευές όπως το Bluetooth , φούρνων μικροκυμάτων , ασύρματα τηλέφωνα (τα 900MHz ή τα 5.8GHz είναι εναλλακτικές συχνότητες τηλεφωνικές που μπορούν να χρησιμοποιηθούν για αποφυγή παρεμβολών με ένα Wi-Fi δίκτυο) και συσκευές αποστολής βίντεο ανάμεσασε πολλές άλλες . Αυτό μπορεί να προκαλέσει μία στατική μείωση στην απόδοση. Άλλες συσκευές που χρησιμοποιούν αυτές τις συχνότητες μικροκυμάτων μπορούν επίσης να προκαλέσουν σταδιακή μείωση στην απόδοση .
- Κλειστά σημεία πρόσβασης μπορούν να παρεμβάλλονται με σωστά ρυθμισμένα ανοιχτά σημεία πρόσβασης στην ίδια συχνότητα , εμποδίζοντας την λειτουργία των ανοιχτών σημείων πρόσβασης από άλλους .
- Η κατανάλωση ενέργειας είναι συγκριτικά πολύ μεγαλύτερη σε σχέση με άλλα στάνταρ κάνοντας την διάρκεια ζωής της μπαταρίας και την εκπεμπόμενη θερμότητα , πρόβλημα .

2.1 ΑΣΦΑΛΕΙΑ ΤΩΝ 802.11 ΑΣΥΡΜΑΤΩΝ LAN

Η ασφάλεια του προτύπου IEEE 802.11 εξασφαλίζεται κατά κύριο λόγο από το πρωτόκολλο WEP (Wired Equivalence Protocol) για την προστασία της ασύρματης μετάδοσης πακέτων μεταξύ των πελατών (clients) και των σημείων πρόσβασης (Access Points – AP's). Το μειονέκτημα του WEP είναι ότι προσφέρει από σημείο σε σημείο (end–to–end) ασφάλεια μόνο για το ασύρματο κομμάτι της μετάδοσης, όπως παρουσιάζεται στο σχήμα 2.1 [1][8].



Σχήμα 2.1 ***Ασφάλεια του 802.11 σε ένα τυπικό Ασύρματο Δίκτυο***

2.2 Χαρακτηριστικά της Ασφάλειας των 802.11 Ασύρματων LAN σύμφωνα με το Πρότυπο

Οι τρεις βασικές υπηρεσίες ασφάλειας, οι οποίες καθορίζονται από την επιτροπή IEEE για το WLAN, εξασφαλίζονται, όπως αναφέρθηκε, από το πρωτόκολλο WEP και είναι οι ακόλουθες [1]:

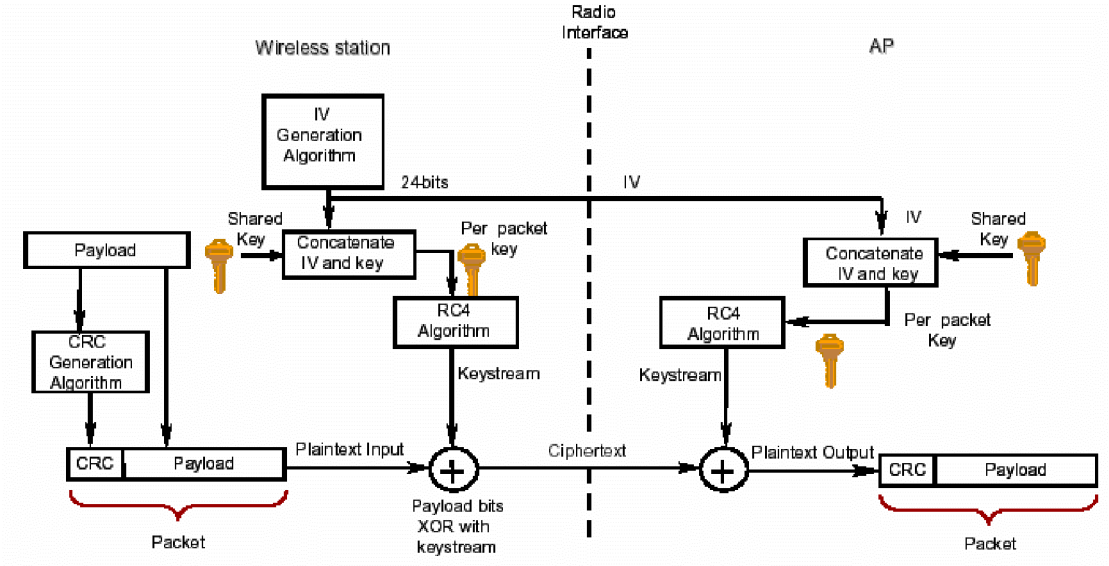
- **Εμπιστευτικότητα (Confidentiality):** Η εμπιστευτικότητα, ή ιδιωτικότητα (privacy), αναπτύχθηκαν ώστε να εξασφαλίζουν την αποκάλυψη δεδομένων μόνο σε εξουσιοδοτημένους χρήστες.
- **Ακεραιότητα (Integrity):** Η ακεραιότητα διαβεβαιώνει ότι τα μηνύματα δεν τροποποιήθηκαν κατά την μεταφορά τους από τους ασύρματους πελάτες στο σημείο πρόσβασης.
- **Αυθεντικοποίηση (Authentication):** Ένας από τους πρωτεύοντες σκοπούς του WEP ήταν να παρέχει μία υπηρεσία ασφάλειας για την επαλήθευση της ταυτότητας των επικοινωνούντων πελατών. Η δεδομένη υπηρεσία εξασφαλίζει τον έλεγχο πρόσβασης στο δίκτυο, με την άρνηση της προσπέλασης του δικτύου από μη αυθεντικοποιημένους χρήστες.

2.2.1 Εμπιστευτικότητα

Το πρότυπο 802.11 υποστηρίζει την εμπιστευτικότητα (ιδιωτικότητα) μέσω της χρήσης τεχνικών κρυπτογράφησης για την ασύρματη διεπαφή. Συγκεκριμένα χρησιμοποιείται η τεχνική του WEP, η οποία κάνει χρήση του αλγορίθμου συμμετρικού κλειδιού RC4 για τη δημιουργία μιας τυχαίας ακολουθίας χαρακτήρων. Αυτή η ακολουθία προστίθεται στα προς μετάδοση δεδομένα με χρήση της λογικής πράξης XOR. Μέσω της τεχνικής αυτής, τα δεδομένα μπορούν να προστατευθούν από τυχόν αποκάλυψή τους κατά τη διάρκεια της μετάδοσής τους στην ασύρματη ζεύξη.

Η τεχνική WEP, σύμφωνα με το πρότυπο 802.11, υποστηρίζει κλειδιά μεγέθους 40 bits, ως διαμοιραζόμενα κλειδιά. Εντούτοις, κάποιοι κατασκευαστές έχουν προσφέρει κατά καιρούς επεκτάσεις του WEP οι οποίες υποστηρίζουν μεγέθη κλειδιών από 40 bits έως 104 bits, εκ των οποίων τα τελευταία μπορούν να φτάσουν και τα 128 bits, συμπεριλαμβανομένου του διανύσματος αρχικοποίησης (Initialization Vector-IV). Είναι γνωστό ότι καθώς μεγαλώνει το μήκος του κλειδιού, αυξάνεται αντίστοιχα και η ασφάλεια της κρυπτογραφικής τεχνικής, παρόλο που τυχόν υποτιθέμενες εσφαλμένες υλοποιήσεις ή κατασκευές κλειδιών είναι πιθανό να εμποδίσουν την αύξηση αυτή. Έρευνες έχουν δείξει ότι κλειδιά μήκους από 80 bits και πάνω κάνουν την κρυπτανάλυση με τη μέθοδο brute force ένα σχεδόν αδύνατο εγχείρημα. Για ένα κλειδί μήκους 80 bits ο αριθμός των δυνατών κλειδιών είναι μεγαλύτερος από 10^{26}!!!

Στο σχήμα 2.2 παρουσιάζεται η θεμελίωση της εμπιστευτικότητας με την χρήση του WEP.



Σχήμα 2.2 ***Εμπιστευτικότητα κατά WEP με χρήση του Αλγορίθμου RC4***

2.2.2 Ακεραιότητα

Το πρότυπο 802.11 παρέχει μια υπηρεσία για να εξασφαλίσει την ακεραιότητα, στα μηνύματα που μεταδίδονται μεταξύ των πελατών του ασύρματου δικτύου και των σημείων πρόσβασης. Αυτή η υπηρεσία έχει σχεδιασθεί για να απορρίπτει μηνύματα τα οποία έχουν τροποποιηθεί από ένα κακόβουλο τρίτο άτομο (man-in-the-middle).

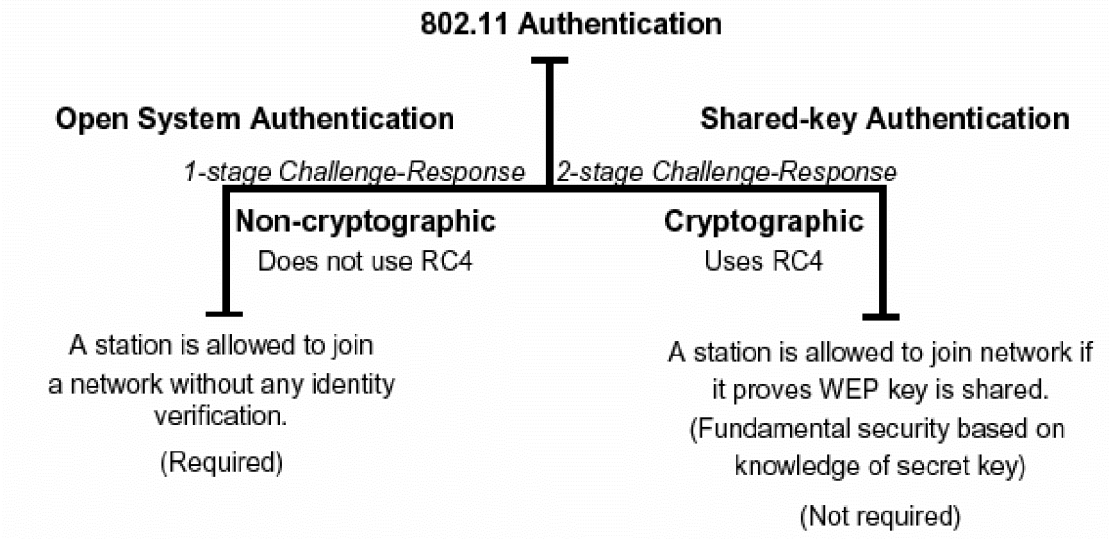
Γίνεται χρήση ενός απλού κρυπτογραφημένου κώδικα **CRC** (*Cyclic Redundancy Check* – Έλεγχος Κυκλικού Πλεονασμού). Όπως φαίνεται και στο σχήμα 2.2, υπολογίζεται μια ακολουθία ελέγχου πλαισίου (**CRC - 32**) για κάθε πακέτο (payload) πριν την μετάδοση. Το πακέτο κρυπτογραφείται, έπειτα, με την τυχαία ακολουθία του RC4 και παρέχεται το κρυπτογραφημένο κείμενο (cipher-text). Στο άκρο της λήψης γίνεται αποκρυπτογράφηση και υπολογίζεται η ακολουθία ελέγχου πλαισίου (CRC) του ληφθέντος μηνύματος. Αν οι δύο ακολουθίες ελέγχου πλαισίου δεν είναι ίδιες, έχουμε παραβίαση της ακεραιότητας και το πακέτο απορρίπτεται.

Παρόλα αυτά η υπηρεσία είναι ευάλωτη σε διάφορες επιθέσεις, κυρίως γιατί ο έλεγχος κυκλικού πλεονασμού δεν είναι αρκετά ασφαλής κρυπτογραφική τεχνική όπως είναι μια συνάρτηση κατακερματισμού ή ένας MAC (Message Authentication Code).

2.2.3 Αυθεντικοποίηση

Το πρότυπο IEEE 802.11 χρησιμοποιεί δύο τεχνικές για την επαλήθευση της ταυτότητας των ασύρματων χρηστών που επιθυμούν να προσπελάσουν το ενσύρματο δίκτυο: την αυθεντικοποίηση ανοιχτού συστήματος **(open system authentication)** και την αυθεντικοποίηση διαμοιραζόμενου κλειδιού **(shared-key authentication)**, εκ των οποίων η δεύτερη βασίζεται στην κρυπτογραφία ενώ η πρώτη όχι.

Στο σχήμα 2.3 παρατίθενται οι δύο τεχνικές αυθεντικοποίησης.



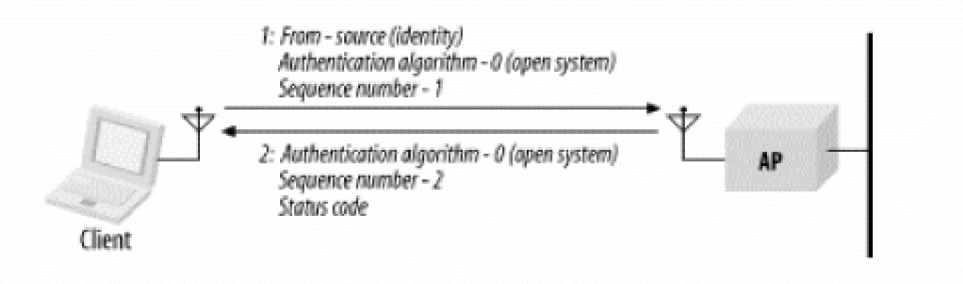
Σχήμα 2.3 ***Ταξινομία των τεχνικών Αυθεντικοποίησης του προτύπου 802.11***

2.2.3.1 Τεχνική Αυθεντικοποίησης Ανοιχτού Συστήματος

Η **τεχνική αυθεντικοποίησης ανοιχτού συστήματος** δεν είναι στην πραγματικότητα αυθεντικοποίηση, διότι ο κινητός σταθμός προσπελάζει το σημείο πρόσβασης χωρίς να εξακριβωθεί η ταυτότητά του. Επιπλέον, θα πρέπει να σημειωθεί ότι η αυθεντικοποίηση είναι μονόδρομη, δηλαδή μόνο ο κινητός σταθμός μπορεί να αυθεντικοποιηθεί, και πρέπει αυτός να θεωρήσει ότι επικοινωνεί με ένα πραγματικό σημείο πρόσβασης. Ο πελάτης αυθεντικοποιείται απλά ανταποκρινόμενος με μια MAC διεύθυνση κατά την ανταλλαγή των δύο μηνυμάτων με ένα σημείο πρόσβασης. Κατά τη διάρκεια της ανταλλαγής ο πελάτης δεν επικυρώνεται πραγματικά αλλά απλά απαντά με τα σωστά πεδία στην ανταλλαγή μηνυμάτων. Είναι φανερό ότι, χωρίς

την χρήση κάποιας μεθόδου κρυπτογράφησης, η δεδομένη τεχνική είναι εξαιρετικά ευάλωτη στις επιθέσεις από μη εξουσιοδοτημένους χρήστες [1].

Η διαδικασία ανταλλαγής μιας αυθεντικοποίησης ανοιχτού συστήματος αποτελείται από δύο πλαίσια, τα οποία παρουσιάζονται στο σχήμα 2.4 [5].



Σχήμα 2.4 ***Αυθεντικοποίηση Ανοιχτού Συστήματος***

Το πρώτο πλαίσιο, το οποίο προέρχεται από τον κινητό σταθμό, είναι ουσιαστικά ένα πλαίσιο διαχείρισης μιας υποκατηγορίας αυθεντικοποίησης. Το πρότυπο 802.11 δεν αναφέρει επισήμως αυτό το πλαίσιο ως αίτηση (request) αυθεντικοποίησης, αλλά αυτός είναι και ο πρακτικός του σκοπός. Κατά το 802.11, η ταυτότητα του κάθε σταθμού είναι η MAC διεύθυνσή του. Όπως και στα δίκτυα Ethernet, οι διευθύνσεις MAC πρέπει να είναι μοναδικές σε κάθε σημείο του δικτύου και μπορούν εύκολα να παίξουν και τον ρόλο των αναγνωριστικών των κινητών σταθμών. Τα σημεία πρόσβασης χρησιμοποιούν την πηγαία διεύθυνση των πλαισίων ως ταυτότητα του αποστολέα, χωρίς την χρήση πεδίων εντός του πλαισίου, για την επιπλέον ταυτοποίηση του αποστολέα. Υπάρχουν δύο πληροφοριακά στοιχεία στο κύριο μέρος της αίτησης αυθεντικοποίησης. Πρώτον, το στοιχείο αναγνώρισης του αλγορίθμου αυθεντικοποίησης (Authentication Algorithm Identification), το οποίο είναι ρυθμισμένο στο 0 ώστε να δείχνει ότι η μέθοδος ανοιχτού συστήματος είναι σε λειτουργία. Δεύτερον, ο αριθμός της ακολουθίας ανταλλαγής της αυθεντικοποίησης (Authentication Transaction Sequence number), ο οποίος είναι ρυθμισμένος στο 1, ώστε να δείχνει ότι το πρώτο πλαίσιο είναι ουσιαστικά το πρώτο πλαίσιο της ακολουθίας.

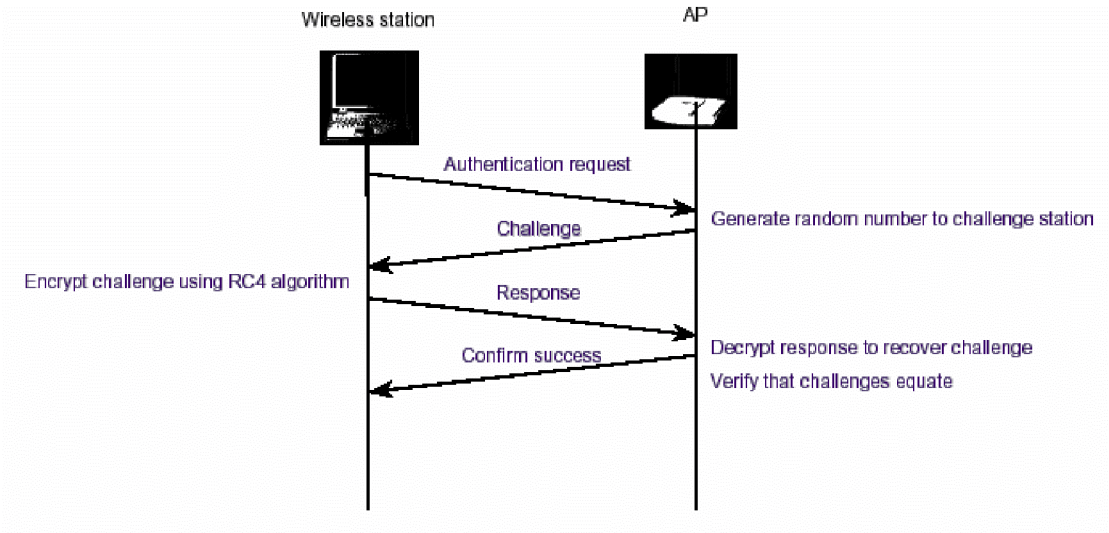
Στην συνέχεια, το σημείο πρόσβασης επεξεργάζεται την αίτηση αυθεντικοποίησης και επιστρέφει την απόκριση (response) του. Όμοια με το πρώτο πλαίσιο, το πλαίσιο απόκρισης είναι ένα πλαίσιο διαχείρισης μιας υποκατηγορίας αυθεντικοποίησης. Τρία

πληροφοριακά στοιχεία είναι παρόντα: Το πεδίο του στοιχείου αναγνώρισης του αλγορίθμου αυθεντικοποίησης (Authentication Algorithm Identification), το οποίο είναι ρυθμισμένο στο 0 ώστε να δείχνει την ύπαρξη αυθεντικοποίησης ανοιχτού συστήματος, ο αριθμός ακολουθίας (Sequence Number) που είναι 2, και ο κώδικας κατάστασης (Status Code), ο οποίος δείχνει την έκβαση της αίτησης αυθεντικοποίησης.

2.2.3.2 Τεχνική Αυθεντικοποίησης Διαμοιραζόμενου κλειδιού

Η **τεχνική αυθεντικοποίησης διαμοιραζόμενου κλειδιού**, όπως αναφέρθηκε και παραπάνω, χρησιμοποιεί την κρυπτογραφία και βασίζεται στη γνώση του διαμοιραζόμενου κλειδιού από τον πελάτη (ο αλγόριθμος που χρησιμοποιείται είναι συμμετρικός και είναι ο RC4). Αρχικά το AP δημιουργεί και στέλνει στον πελάτη μια τυχαία ακολουθία χαρακτήρων μήκους 128 bits (***challenge***). Ο πελάτης, χρησιμοποιώντας το μυστικό κλειδί (που μοιράζεται με το AP), κρυπτογραφεί την ακολουθία αυτή και στέλνει το αποτέλεσμα της κρυπτογράφησης στο AP (***response***). Το AP αποκρυπτογραφεί την ακολουθία που μόλις στάλθηκε από τον πελάτη και του επιτρέπει την πρόσβαση μόνο αν είναι ίδια με την ακολουθία που είχε σταλεί αρχικά. Πρέπει να σημειωθεί ότι και αυτή η τεχνική πάσχει αμοιβαίας αυθεντικοποίησης. Επομένως, είναι ευπαθής σε διαφόρων ειδών επιθέσεις, συμπεριλαμβανομένης και της γνωστής man-in-the-middle [1].

Το σχήμα 2.5 είναι ένα διάγραμμα ροής το οποίο αναπαριστά την διαδικασία αυθεντικοποίησης με τη χρήση της τεχνικής διαμοιραζόμενου κλειδιού.



Σχήμα 2.5 ***Αυθεντικοποίηση Μηνύματος με την χρήση Διαμοιραζόμενου κλειδιού***

2.3 Βασικοί Μηχανισμοί Ασφάλειας

Έχουν αναπτυχθεί τέσσερις βασικοί μηχανισμοί για την ασφάλιση ενός σημείου πρόσβασης (Access Point) στα 802.11 δίκτυα [4]:

- Το **SSID** (Service set identifier)
- Το **MAC** (Media Access Control) address filtering
- Το **WEP** (Wired Equivalent Privacy)
- Το **WPA** (Wi-Fi Protected Access)

Σε ένα ασύρματο δίκτυο μπορεί να εφαρμοστεί ένας ή και περισσότεροι από τους παραπάνω μηχανισμούς. Εντούτοις, θα πρέπει να γνωρίζουμε ότι η καλύτερη ασφάλεια επιτυγχάνεται όταν εφαρμόζονται και οι τέσσερις μηχανισμοί μαζί.

2.3.1 SSID (Service Set Identifier)

Ο έλεγχος πρόσβασης σε ένα δίκτυο μπορεί να εφαρμοστεί χρησιμοποιώντας ένα SSID σε συνδυασμό, είτε με ένα είτε με μία ομάδα από Access Points. Το SSID, δρώντας ως αναγνωριστικό ενός WLAN, παρέχει ένα μηχανισμό ο οποίος "τεμαχίζει" ένα ασύρματο δίκτυο σε μία υπηρεσία πολλαπλών δικτύων αποτελούμενων από ένα ή περισσότερα APs. Κάθε AP είναι εφοδιασμένο με ένα SSID, το οποίο ανταποκρίνεται σε ένα συγκεκριμένο ασύρματο δίκτυο. Επομένως, για να προσπελάσει ένας υπολογιστής το δίκτυο, θα πρέπει να είναι ρυθμισμένος με το σωστό SSID, το οποίο προστίθεται στην επικεφαλίδα (header) κάθε πακέτου που στέλνεται μέσω του WLAN και, έπειτα, επαληθεύεται από το AP [2][4][8].

Η πιστοποίηση ενός υπολογιστή σε ένα AP μέσω του SSID καθιστά το AP ικανό να δρα ως κωδικός πρόσβασης, πράγμα το οποίο παρέχει ένα μέτρο ασφάλειας σε ένα WLAN. Εντούτοις, η εν λόγω υποτυπώδης ασφάλεια ενδέχεται να παραβιαστεί στην περίπτωση κατά την οποία το AP είναι ρυθμισμένο ώστε να γνωστοποιεί το SSID του [2][4].

2.3.2 MAC Address Filtering

Ενώ ένα AP, ή ένα σύνολο από APs, μπορούν να πιστοποιηθούν μέσω ενός SSID, ένας υπολογιστής είναι δυνατόν να πιστοποιηθεί μέσω της μοναδικής διεύθυνσης MAC που διαθέτει η κάρτα δικτύου του σύμφωνα με το πρότυπο 802.11. Για να επιτευχθεί αύξηση της ασφάλειας ενός 802.11 δικτύου, κάθε AP μπορεί να εφοδιαστεί με μία λίστα η οποία περιλαμβάνει τις διευθύνσεις MAC που συσχετίζονται με τους υπολογιστές που επιτρέπεται να προσπελάσουν το AP. Σε περίπτωση που η διεύθυνση MAC ενός υπολογιστή δεν περιέχεται στην λίστα, τότε δεν θα του επιτραπεί η σύνδεση με το AP [4].

Η προκείμενη ασφάλεια παρέχει υψηλό επίπεδο ασφάλειας, αλλά ενδείκνυται για μικρά μόνο δίκτυα. Η δημιουργία της λίστας των διευθύνσεων MAC πρέπει να γίνεται χειροκίνητα σε κάθε AP, και, επιπλέον, η λίστα θα πρέπει να ενημερώνεται συνεχώς, με αποτέλεσμα η υπερκείμενη διαχειριστικότητα να περιορίζει την κλιμάκωση αυτής της προσέγγισης [4].

2.3.3 WEP (Wired Equivalent Privacy)

Το WEP παρέχει κρυπτογραφημένη επικοινωνία, χρησιμοποιώντας ένα κλειδί κρυπτογράφησης για την κρυπτογράφηση και την αποκρυπτογράφηση δεδομένων. Το δεδομένο κλειδί υπάρχει και στον client αλλά και σε κάθε AP, ώστε και τα δύο μέρη να πιστοποιούν την ταυτότητά τους προτού προχωρήσουν σε επικοινωνία [3][4].

Το πρόβλημα της χρήσης WEP είναι ότι το πρότυπο 802.11 δεν υποστηρίζει κάποιο πρωτόκολλο διαχείρισης για ηλεκτρονική διαχείριση κλειδιών, με αποτέλεσμα όλα τα κλειδιά να εισάγονται χειροκίνητα στα APs από τους διαχειριστές. Επομένως, η διαδικασία αυτή καθιστά πολύ δύσκολη την χρήση WEP στα μεγάλα σε αριθμό συσκευών ασύρματα δίκτυα [3][4].

2.3.4 Wi-Fi Προστατευμένη Πρόσβαση (Wi-Fi Protected Access, WPA)

Το πρότυπο IEEE 802.11i αποτελεί μια νεότερη έκδοση του αρχικού 802.11, που ενσωματώνει ένα καινούριο σύστημα ασφάλειας, το οποίο αναπτύχθηκε από την ομάδα εργασίας i του Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE TGi). Με το νέο πρότυπο επιδιώκεται να αντιμετωπιστούν οι αδυναμίες του πρωτοκόλλου Ενσύρματου Ισοδύναμου Απόρρητου (WEP).

Για να το επιτύχει αυτό περιλαμβάνει το πλαίσιο εργασίας της διαδικασίας πιστοποίησης του προτύπου IEEE 802.1X, το Πρωτόκολλο Χρονικού Κλειδιού Ακεραιότητας (Temporal Key Integrity Protocol, TKIP), το Πρότυπο Προηγμένης Κρυπτογράφησης (Advanced Encryption Standard,AES), ιεραρχία κλειδιών και νέα χαρακτηριστικά διαχείρισής τους καθώς και διαδικασίες διαπραγμάτευσης για την κρυπτογράφηση των δεδομένων και την πιστοποίηση της ταυτότητας του σταθμού. Στο μμεταξύ εξαιτίας των όλο και αυξανόμενων απαιτήσεων ασφάλειας από το 802.11 η WECA (Wireless Ethernet Compatibility Alliance), γνωστή και ως Συμμαχία Wi-Fi, υιοθέτησε κάποια κομμάτια του 802.11i και δημιούργησε ένα καινούριο πρότυπο ασφάλειας, γνωστό ως Wi-Fi Προστατευμένη Πρόσβαση (Wi-Fi Protected Access, WPA), το οποίο μπορεί να ενσωματωθεί στο 802.11 με απλή αναβάθμιση του λογισμικού. Ουσιαστικά το μόνο κομμάτι του 802.11i που δεν ενσωματώθηκε είναι αυτό που αναφέρεται στην κρυπτογράφηση των δεδομένων, αφού κάτι τέτοιο απαιτεί την αναβάθμιση του υπάρχοντος εξοπλισμού. Έτσι τα τμήματα που αποτελούν την Wi-Fi Προστατευμένη Πρόσβαση είναι:

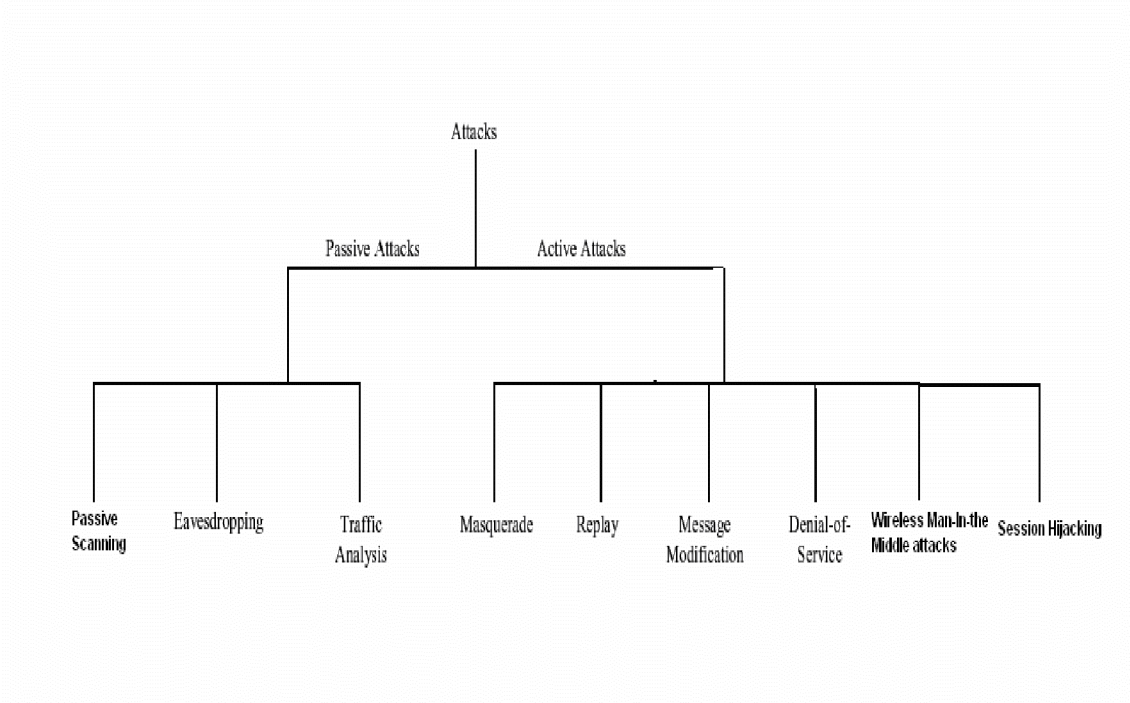
- Το πλαίσιο εργασίας της διαδικασίας πιστοποίησης του πρότυπου 802.1X.
- Το Πρωτόκολλο Χρονικού Κλειδιού Ακεραιότητας (TKIP).
- Η ιεραρχία των κλειδιών και τα νέα χαρακτηριστικά διαχείρισής τους.
- Οι διαδικασίες διαπραγμάτευσης για την κρυπτογράφηση των δεδομένων και την πιστοποίηση της ταυτότητας του σταθμού.

2.4 Ευπάθειες των 802.11 WLANs

Αν και η πορεία των 802.11 WLANs είναι εξελικτική, παρατηρήθηκε το γεγονός ότι τα δίκτυα αυτά αντιμετωπίζουν τρομερά προβλήματα ασφάλειας. Πολλές αναφορές σχετικές με τα 802.11 WLANs περιγράφουν τις επιθέσεις που γίνονται συνεχώς και αναφέρουν τους κινδύνους στους οποίους εκτίθενται οι οργανισμοί.

2.4.1 Ευπάθειες ενός Ασύρματου Δικτύου

Το σχήμα 2.6 παρουσιάζει μία γενική ταξινομία των επιθέσεων κατά της ασφάλειας ώστε να βοηθήσει τους οργανισμούς και τους χρήστες να αντιληφθούν το είδος και τον τύπο της καθεμιάς.



Σχήμα 2.6 Ταξινομία των Επιθέσεων κατά της Ασφάλειας

Οι επιθέσεις κατά της ασφάλειας των δικτύων χωρίζονται τυπικά σε δύο κατηγορίες, τις ακούσιες και τις εκούσιες. Αυτές οι δύο μεγάλες κατηγορίες μπορούν να υποδιαιρεθούν και σε άλλους τύπους επιθέσεων. Όλοι αυτοί οι τύποι επιθέσεων περιγράφονται ακολούθως [1]:

- **Ακούσια Επίθεση (Passive Attack)** – Είναι η επίθεση κατά την οποία ένα μη εξουσιοδοτημένο μέλος αποκτά το πλεονέκτημα πρόσβασης σε έναν πόρο, χωρίς όμως να αλλάζει το περιεχόμενο του (π.χ., παρακολούθηση συνόδου ή ανάλυση της κίνησης).
    - **Παρακολούθηση συνόδου (Eavesdropping)** – Ο επιτιθέμενος παρακολουθεί τις μεταδόσεις για να δει το περιεχόμενο του μηνύματος.

- **Ανάλυση της Κίνησης (Traffic analysis)** – Ο επιτιθέμενος αποκτά πληροφορίες, με πιο επιδέξιο τρόπο, παρακολουθώντας τις μεταδόσεις και συμπεραίνοντας τον τρόπο επικοινωνίας.
- **Passive Scanning** – Ειναι μια μέθοδος sniffing κατα την οποία ο επιτιθέμενος χρησιμοποιεί μια κάρτα ασύρματης δικτυακής πρόσβασης (hardware) για να συντονιστεί στις ραδιοσυχνότητες μεταξύ 2.4 GHz και 2.5 GHz τις οποίες χρησιμοποιούν τ' ασύρματα σημεία πρόσβασης. Ο συντονισμός του Passive Scanner στις εν λόγω ραδιοσυχνότητες μπορεί να γίνει χωρίς καμία αναγνώριση του δράστη από το δίκτυο.

- **Εκούσια Επίθεση (Active Attack)** – Κατά την εκούσια επίθεση, ένα μη εξουσιοδοτημένο μέλος κάνει τροποποιήσεις σε ένα μήνυμα, μία ακολουθία δεδομένων, ή ένα αρχείο. Είναι πιθανό η επίθεση αυτή να ανιχνευθεί, αλλά δυστυχώς δεν είναι δυνατόν να εξαλειφθεί. Οι τύποι των εκούσιων επιθέσεων αναλύονται ακολούθως [1][2].
  - **Προσποίηση (Masquerading)** – Ο επιτιθέμενος προσποιείται έναν εξουσιοδοτημένο χρήστη, με αποτέλεσμα να κερδίζει συγκεκριμένα προνόμια τα οποία δεν του ανήκουν.
  - **Επανάληψη (Replay)** – Ο επιτιθέμενος παρακολουθεί τις μεταδόσεις και αναμεταδίδει μηνύματα σαν νόμιμος χρήστης.
  - **Τροποποίηση μηνύματος (Message modification)** – Ο επιτιθέμενος αλλάζει το κανονικό μήνυμα, διαγράφοντας, προσθέτοντας, αλλάζοντας, ή αναδιατάσσοντας το περιεχόμενό του.
  - **Άρνηση Εξυπηρέτησης (Denial-of-Service)** – Ο επιτιθέμενος εμποδίζει την κανονική χρήση ή διαχείριση των υπηρεσιών από τους νόμιμους χρήστες.
  - **Ανακατεύθυνση της Κίνησης (Traffic Redirection)** – Ένας εισβολέας μπορεί να αλλάξει την πορεία της κίνησης, με αποτέλεσμα, τα πακέτα που προορίζονταν αρχικά για έναν συγκεκριμένο προορισμό, να ανακατευθύνονται στον επιτιθέμενο σταθμό.
  - **Παράνομα Σημεία Πρόσβασης (Rogue Access Points)** – Ένα τέτοιο AP εγκαθίσταται από κάποιον επιτιθέμενο (συνήθως σε δημόσιες περιοχές όπως κοινόχρηστους εργασιακούς χώρους, αεροδρόμια κτλ.),

ώστε να προσποιείται μία έγκυρη συσκευή αυθεντικοποίησης και να δέχεται την κίνηση από τους clients. Με αυτόν τον τρόπο είναι δυνατόν να αποσπώνται ευαίσθητες πληροφορίες από τα πακέτα, ή ακόμα και να τροποποιείται το περιεχόμενό τους.

- **Εισβολή και υποκλοπή των πόρων ενός δικτύου (Intrusion & Resource Stealing)** − Οι πόροι ενός δικτύου περιλαμβάνουν την πρόσβαση σε ποικίλες συσκευές (όπως για παράδειγμα εκτυπωτές και εξυπηρετητές) και υπηρεσίες (όπως η επικοινωνία σε ένα εσωτερικό δίκτυο ή στο Internet). Για την εισβολή σε ένα δίκτυο, ο επιτιθέμενος αποκτά αρχικά γνώση των παραμέτρων πρόσβασης για το συγκεκριμένο δίκτυο. Για παράδειγμα, εάν το υποκείμενο δίκτυο χρησιμοποιεί φιλτράρισμα των clients βάσει των MAC διευθύνσεων τους, τότε το μόνο που χρειάζεται να κάνει ο εισβολέας είναι να μάθει την MAC και την IP διεύθυνση ενός client και να χρησιμοποιεί το δίκτυο, και τους πόρους του γενικότερα, ως έγκυρος χρήστης όταν ο client θα είναι αποσυνδεδεμένος.

- **Wireless Man-In-The-Middle (MITM)-** Στις επιθέσεις αυτές ο δράστης διεισδύει μεταξύ δύο επικοινωνούντων σημείων ασύρματης πρόσβασης (AP) ενός δικτύου εξαναγκάζοντας καθένα από αυτά να εξουσιοδοτήσει και πιστοποιηθεί με το σημείο ή συσκευή ασύρματης πρόσβασης του δράστη. Έτσι, το περιεχόμενο της επικοινωνίας των δύο σημείων ασύρματης πρόσβασης στο δίκτυο κατευθύνεται από τον αποστολέα στον λήπτη μέσω του ασύρματου σημείου ή συσκευής πρόσβασης του δράστη, ο οποίος φυσικά υποκλέπτει πλήρως το περιεχόμενο της επικοινωνίας.
- **Session Hijacking-** Στις επιθέσεις αυτές ο δράστης προκαλεί στιγμιαία, ή τουλάχιστον προσωρινή, απώλεια σύνδεσης ενός χρήστη με τον διακομιστή του δικτύου στο οποίο είναι συνδεδεμένος. Κατά τη διάρκεια της διακοπής, ο δράστης ιδιοποιείται παράνομα την ταυτότητα του χρήστη για να επιτύχει τη σύνδεσή του με τον διακομιστή του δικτύου με τα προνόμια που είχε ο χρήστης. Αφού, ο δράστης, εμφανιζόμενος με την ταυτότητα του νόμιμου χρήστη,

αντλήσει από τον διακομιστή του δικτύου τα πληροφοριακά δεδομένα που τον ενδιαφέρουν, επαναφέρει τον νόμιμο χρήστη σε σύνδεση με τον διακομιστή, συνήθως χωρίς ο χρήστης ν' αντιληφθεί την πραγματική αιτία της προσωρινής διακοπής της σύνδεσής του. Οι διαγνωσθείσες ελλείψεις στο ζήτημα της θωράκισης της ασφάλειας των ασύρματων συστημάτων και η συστηματική έρευνα, καταγραφή και ταξινόμηση των δυνατών επιθέσεων hacking κατά των εν λόγω συστημάτων οδήγησε στη λήψη πρόσθετων τεχνολογικών μέτρων, αλλά και στη χάραξη πολιτικής ασφαλείας (συνήθως αποκαλούμενη «Wireless Local Area Network» ή WLAN πολιτική ασφαλείας) για τη διασφάλιση των ασύρματων συστημάτων από οποιοδήποτε είδος hacking κατ' αυτών.

2.4.2 Ευπάθειες του Προτύπου IEEE 802.11

Έχουν παρουσιαστεί κατά καιρούς πολλά προβλήματα σχετικά με την ασφάλεια των WLANs, τα οποία επιτρέπουν σε κακόβουλους χρήστες να βλάπτουν την ασφάλεια των δικτύων αυτών. Συνέπεια των παραπάνω είναι οι επιθέσεις ανάλυσης της κίνησης, αποκρυπτογράφησης της κίνησης, ο φόρτος της κίνησης από μη εξουσιοδοτημένους χρήστες και οι επιθέσεις λεξικού [1].

Οι ευπάθειες που αναφέρθηκαν παραπάνω σχετίζονταν με τα ασύρματα δίκτυα γενικότερα. Το μεγαλύτερο ενδιαφέρον για την ασφάλεια όμως επικεντρώνεται περισσότερο στο πρότυπο IEEE 802.11 δίκτυο, όσον αφορά τα ακόλουθα [1][2]:

1. **Αυθεντικοποίηση βάσει των διευθύνσεων MAC (MAC Address Authentication):** Αυτού του είδους η αυθεντικοποίηση επαληθεύει την ταυτότητα ενός μηχανήματος και όχι του χρήστη του. Επομένως, ένας επιτιθέμενος, ο οποίος καταφέρει να κλέψει έναν φορητό υπολογιστή, εμφανίζεται στο δίκτυο ως νόμιμος χρήστης.
2. **Μονόδρομη Αυθεντικοποίηση (One-way Authentication):** Η αυθεντικοποίηση με βάση το WEP είναι μονόδρομη. Αυτό σημαίνει ότι ο χρήστης αποδεικνύει την ταυτότητα του σε ένα AP αλλά όχι το αντίστροφο.

Επομένως, ένα παράνομο AP θα μπορούσε να αυθεντικοποιήσει επιτυχώς έναν χρήστη και στην συνέχεια να υποκλέψει όλα τα πακέτα που προορίζονται στον νόμιμο σταθμό.

3. **SSID:** Εφόσον το SSID προστίθεται στην επικεφαλίδα του πακέτου και μεταφέρεται σε καθαρή μορφή κειμένου, παρέχει, τελικώς, πολύ μικρή ασφάλεια. Επομένως, μπορεί να θεωρηθεί πιο πολύ ως ένα είδους αναγνώρισης του δικτύου παρά ένα χαρακτηριστικό ασφάλειας.
4. **Χρήση στατικών κλειδιών WEP:** Η χρήση κοινού κλειδιού από όλους τους σταθμούς είναι μεγάλη ευπάθεια του συστήματος, διότι μπορεί να οδηγήσει στην έκθεση ενός μεγάλου ποσού της κίνησης σε έναν υποτιθέμενο hacker ή ακόμα και την έκθεση του ίδιου κλειδιού σε περίπτωση κλοπής του φορητού υπολογιστή. Επιπλέον, όπως αναφέρθηκε και παραπάνω, η εισαγωγή των κλειδιών χειροκίνητα δημιουργεί ζητήματα διαχειριστικότητας.

5. **Ευπάθεια του κλειδιού WEP:** Η κρυπτογράφηση βάσει του κλειδιού WEP δημιουργήθηκε ώστε να προσφέρει ίδιο επίπεδο ασφάλειας με εκείνο των ενσύρματων δικτύων. Εντούτοις, προέκυψαν αργότερα πολλές ανησυχίες όσον αφορά την ασφάλεια του WEP [2]. Μερικά από αυτά περιγράφονται εκτενέστερα παρακάτω [1]:
    - **Το IV (Initialization Vector) στο WEP:** Το μήκος των 24 bits ενός IV θεωρείται πολύ μικρό όταν χρησιμοποιείται για κρυπτογραφικούς σκοπούς, με αποτέλεσμα να υπάρχει πιθανότητα επαναχρησιμοποίησης του και, επομένως, παραγωγής της ίδιας ακολουθίας χαρακτήρων.
    - **Το IV είναι μέρος του κλειδιού RC4:** Το γεγονός ότι ένας επιτιθέμενος είναι δυνατόν να γνωρίζει τα 24 bits κάθε πακέτου, σε συνδυασμό με την αδυναμία του αλγορίθμου RC4, οδηγεί σε μία επιτυχή επίθεση ανάλυσης, κατά την οποία ανακτάται το κλειδί, μετά την αναχαίτιση και την ανάλυση ενός μόνο μικρού μέρους της κίνησης.
    - **Το WEP δεν παρέχει καμία προστασία της ακεραιότητας:** Το πρωτόκολλο MAC του 802.11 χρησιμοποιεί τον αλγόριθμο CRC, ο οποίος είναι ένας μη κρυπτογραφικός αλγόριθμος, για τον έλεγχο της ακεραιότητας των πακέτων και την επιβεβαίωση λήψης τους με τον σωστό έλεγχο αθροίσματος. Ο συνδυασμός των μη κρυπτογραφικών ελέγχων αθροίσματος, με τους stream αλγορίθμους κρυπτογράφησης είναι επικίνδυνος και συχνά συνιστά στην δημιουργία ευπαθειών, όπως συμβαίνει και στην περίπτωση του WEP.

3.1 ΕΠΙΔΕΙΞΗ ΕΠΙΘΕΣΗΣ ΣΕ ΑΣΥΡΜΑΤΟ WI-FI ΔΙΚΤΥΟ

Στο κομμάτι αυτό της πτυχιακής θα γίνει επίδειξη επιθέσεων εναντίων ασυρμάτων δικτύων με την χρησιμοποίηση διαφόρων διαδεδομένων εργαλείων σε λειτουργικά Windows XP SP2 και Linux. Πιο συγκεκριμένα θα γίνει αξιολόγηση τριών βασικών μέτρων ασφαλείας που χρησιμοποιούνται κατά κόρον από τους χρήστες οικιακών δικτύων , αυτά είναι:

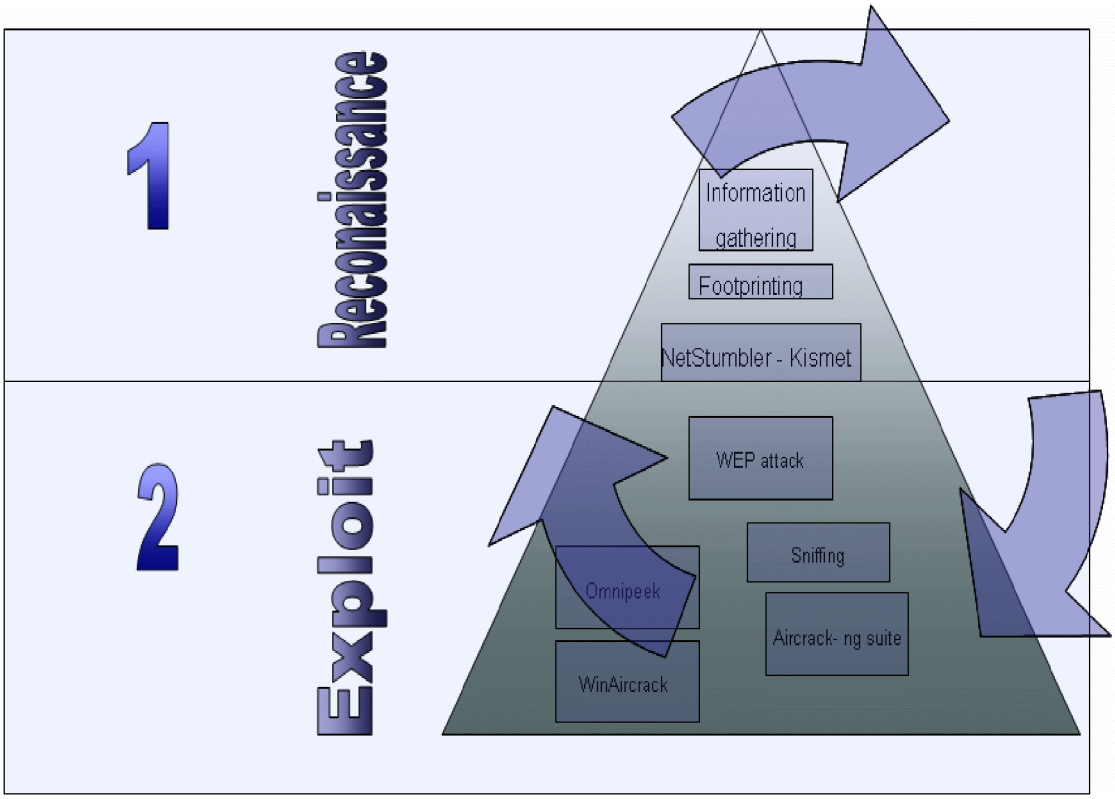
- Η απόκρυψη του SSID του Access Point
- Η χρησιμοποίηση WEP και WPA κρυπτογράφησης στην επικοινωνία του Access Point με τους υπόλοιπούς σταθμούς
- Η αυθεντικοποίηση των σταθμών που συνδέονται με την χρήση MAC διευθύνσεων.

3.1.1 Μεθοδολογία επίθεσης

Η μεθοδολογία που θα ακολουθηθεί και στις 2 επιδείξεις (Windows, Linux) αποτελείτε από 2 φάσεις:

- Την φάση της αναγνώρισης (reconnaissance phase) της οποίας σκοπός είναι η συλλογή όσο το δυνατόν περισσότερες πληροφορίες για τον στόχο. Στο πλαίσιο της φάσης αυτής μας ενδιαφέρουν κυρίως πληροφορίες σχετικές με το configuration του Access Point, την θέση του, το κανάλι που χρησιμοποιεί για να εκπέμψει, το όνομα του SSID που έχει και το είδος της κρυπτογράφησης που τυχόν χρησιμοποιεί.
- Την φάση εκμετάλλευσης (exploit phase) κατά την οποία αφού έχουν βρεθεί όλες οι απαραίτητες πληροφορίες κατά την φάση της αναγνώρισης, ψάχνουμε για αδυναμίες που μπορούμε να βρούμε και τις εκμεταλλευόμαστε. Με άλλα λόγια η φάση της εκμετάλλευσης περιλαμβάνει το hacking του στόχου.

Στο παρακάτω σχήμα φαίνεται όλη η μεθοδολογία της επίθεσης, μαζί με τα εργαλεία τα οποία χρησιμοποιήθηκαν στην κάθε φάση.

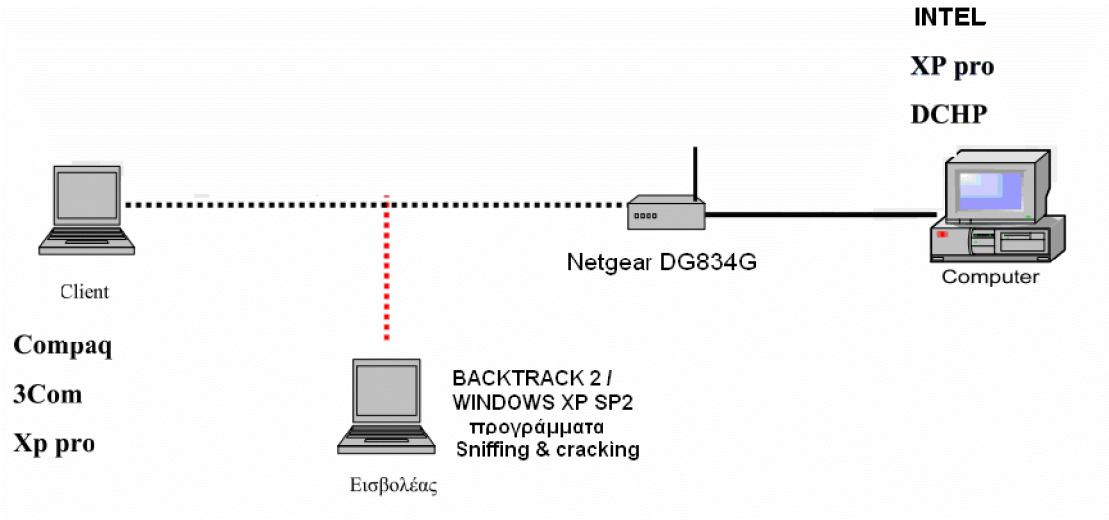


Σχήμα 3.1 ***Σχηματική αναπαράσταση της μεθοδολογίας επίθεσης***

3.1.2 Το configuration της επίδειξης

Το configuration της επίδειξης είναι το εξής:

Ένα laptop της Acer με λειτουργικά Microsoft Windows XP SP2 και Backtrack 2 (εικόνα 3.1) στα 1.6 GHZ με ασύρματη κάρτα την 3Com 11a/b/g Wireless PC Card with XJACK Antenna 3CRPAG175 (εικόνα 3.2) , έναν wireless router (Access Point) τον Netgear DG834G (εικόνα3.3) το οποίο είναι ένα μηχάνημα μεσαίων δυνατοτήτων όπως το μεγαλύτερο ποσοστό των Access point που χρησιμοποιούνται σε οικιακό περιβάλλον, έναν client Compaq με Windows XP pro και έναν σταθερό υπολογιστή με επεξεργαστή Intel Windows XP pro ο οποίος χρησιμοποιείται για DCHP server. Στο παρακάτω σχήμα φαίνεται σχηματικά η πειραματική διάταξη της επίδειξης.



Σχήμα 3.2 ***Πειραματική διάταξη της επίδειξης***

Processor: 1.6GHz Core 2 Duo T5200
Memory: 2GB DDR2
Storage: 120GB hard drive
Graphics: Integrated Intel GMA 950
Operating System: Windows XP Professional-Backtrack

Εικόνα 3.1 Ο φορητός υπολογιστής ο οποίος χρησιμοποιήθηκε κατά την επίδειξη

Τεχνικά Χαρακτηριστικά

Πρότυπο: IEEE 802.11b (11 Mbps) / IEEE 802.11g (54 Mbps)
Τοποθέτηση: Type II ή Type III 32-bit ή PC Card (PCMCIA)
Ασφάλεια: WEP (40/64, 128 και 154-bit), 802.1x, WPA, AES 128-bit, EAP-MD5/EAP-TLS/PEAP, MD5
Εμβέλεια: Έως 100m (σε εσωτερικό χώρο), έως 300m (σε εξωτερικό χώρο)
Τύπος Κεραίας: XJACK
Άλλα Χαρακτηριστικά: Ρυθμός μεταφοράς δεδομένων: 802.11b: 11, 5.5, 2 και 1Mbps / 802.11g: 54, 48, 36, 24, 18, 12, 9 και 6Mbps

Εικόνα 3.2 Η ασύρματη κάρτα που χρησιμοποιήθηκε κατά την επίδειξη

Features

- Wireless ADSL2+ Broadband modem router for Internet sharing
- Integrated 4-portswitch for wired connections
- Double firewall and wireless encryption protects your network and data
- Secure access to your office or corporate network using VPN pass-through
- Supports Windows® Vista™

Εικόνα 3.3 Το Router της επίδειξης

3.2 Χρήση εργαλείων σε περιβάλλον Windows

Τα προγράμματα που χρησιμοποιήθηκαν είναι το NetStumbler το οποίο είναι ένας wireless scanner που χρησιμοποιείται για την εύρεση ασυρμάτων δικτύων. Το δεύτερο πρόγραμμα που χρησιμοποιήθηκε είναι το Omnipeek. Το Omnipeek είναι ένα ολοκληρωμένο περιβάλλον που χρησιμοποιείται από πολλούς επαγγελματίες που ασχολούνται με δίκτυα για να ελέγξουν την ομαλή τους λειτουργία. Χρησιμοποιείται για detection, για sniffing και analyzing. Έχει την δυνατότητα να λαμβάνει πακέτα και να τα αναλύει με πολύ μεγάλη λεπτομέρεια. Μπορεί και δίνει λεπτομέρειες για τα πρωτοκόλλα που χρησιμοποιούνται κατά την μετάδοση , την ποιότητα του σήματος και πολλά άλλα. Για περισσότερες λεπτομέρειες περι του προγράμματος μπορούν να βρεθούν στην ιστοσελίδα της κατασκευάστριας εταιρείας (www.wildpackets.com). Η έκδοση του λογισμικού που χρησιμοποιήθηκε στην επίδειξη αυτή , πιο συγκεκριμένα Omnipeek 5.0, είναι μια trial έκδοση την οποία μπορεί να κατεβάσει ο καθένας από την ιστοσελίδα της εταιρείας. Το εργαλείο αυτό μας βοηθάει να κάνουμε traffic analysis στο ασύρματο δίκτυο που θα κάνουμε επίθεση.

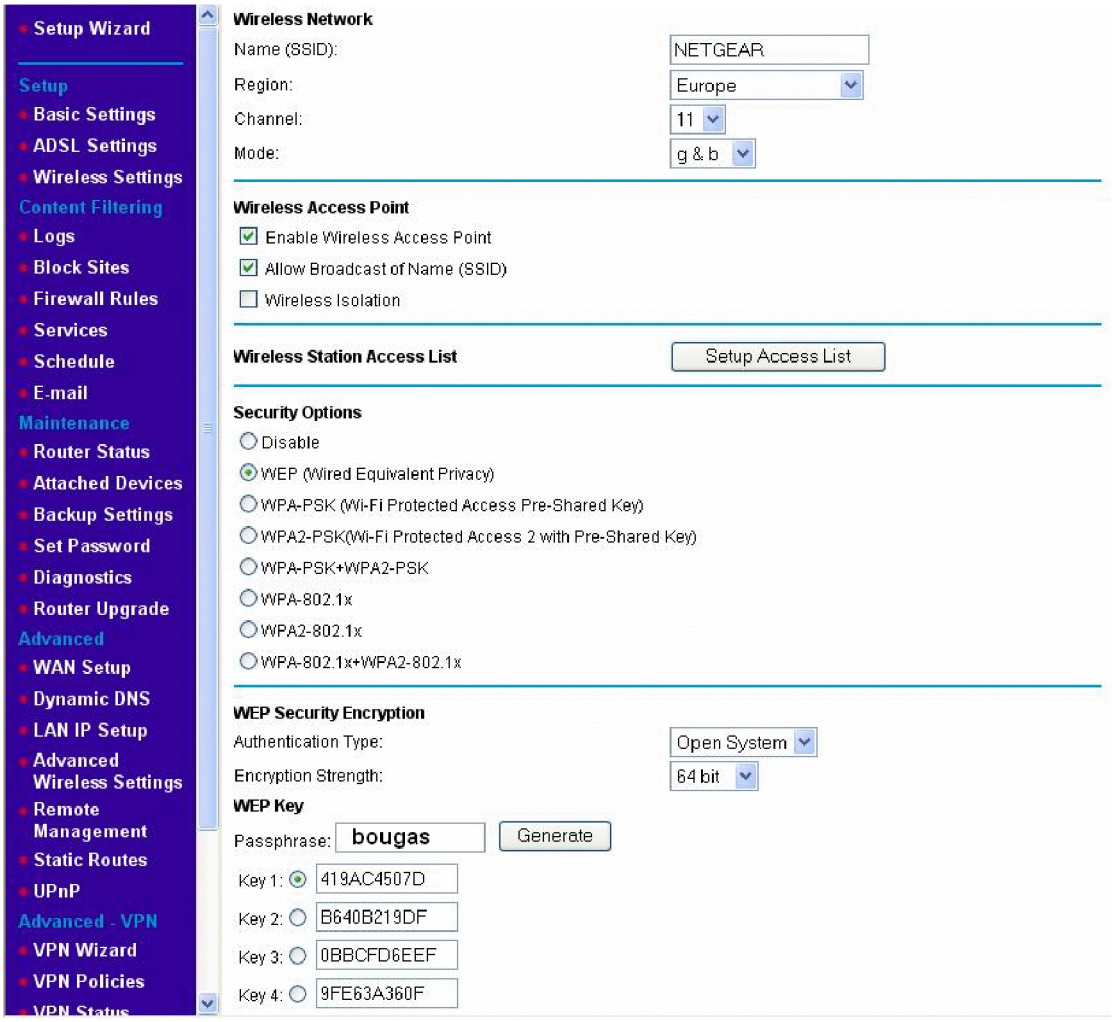
Τέλος χρησιμοποιήθηκε το WinAircrack για την εύρεση του WEP key. Το WinAircrack είναι μια έκδοση της πολύ δημοφιλής σουίτας προγραμμάτων Aircrack η οποία δουλεύει σε Linux συστήματα. Το WinAircrack περιλαμβάνει τα προγράμματα airodump, airdecap και aircrack. Τα airodump και airdecap χρησιμοποιούνται για sniffing και packet capturing. Τα προγράμματα αυτά σε αντίθεση με το Omnipeek μπορούν και λειτουργούν με συγκεκριμένα chipsets wireless καρτών και βεβαίως ούτε έχουν τις ίδιες δυνατότητες όπως το Omnipeek. Τέλος το aircrack είναι το πρόγραμμα που χρησιμοποιείται για την εύρεση του WEP κλειδιού από τα πακέτα που κάναμε capture με το data analyzer πρόγραμμα.

3.2.1 Εύρεση WEP κλειδιού

Αρχικά κάνουμε όλες τις απαραίτητες ρυθμίσεις στο Access Point για την χρησιμοποίηση WEP κλειδιού. Οι παρακάτω εικόνες εμφανίζουν την διαδικασία στο wireless Router. Στην πρώτη εικόνα φαίνεται το configuration του router που χρησιμοποιούμε.

Εικόνα 3.4 Το configuration του Router

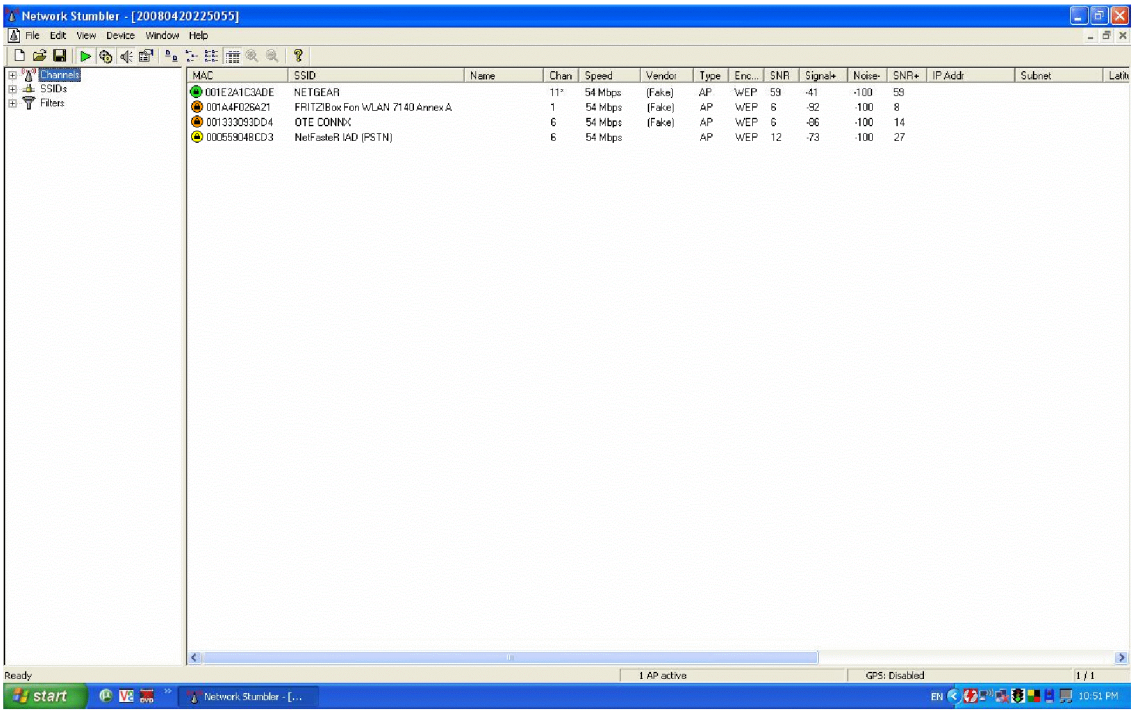
Αρχικά για να μπορέσουμε να χρησιμοποιήσουμε το WEP πρέπει να εισάγουμε το κλειδί στον router χειροκίνητα (εικόνα 3.5), αφού κάνουμε όλες τι απαραίτητες ενέργειες είμαστε έτοιμοι να ξεκινήσουμε την διαδικασία εύρεσης του κλειδιού.



Εικόνα 3.5 Δημιουργία WEP κλειδιού στον Router

Η διαδικασία εύρεσης του κλειδιού αρχίζει εντοπίζοντας το ασύρματο δίκτυο που μας ενδιαφέρει με την βοήθεια του Netstumbler. Όπως φαίνεται και από την εικόνα 3.6 έχουν εντοπιστεί 4 A.P. και μαζί με αυτά και το δικό μας που χρησιμοποιείται στην επίδειξη.

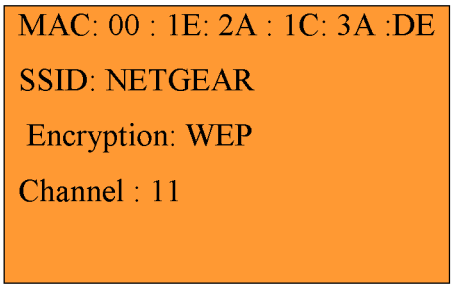
Τα τρία έχουν γνωστό SSID ενώ στο πρώτο έχει γίνει απόκρυψη του. Η σύνδεση ενός υπολογιστή σε ένα Access Point με κρυμμένο SSID θα παρουσιαστεί σε άλλο σημείο της πτυχιακής αυτής.



Εικόνα 3.6 Εύρεση Access Points με την βοήθεια του Netstumbler

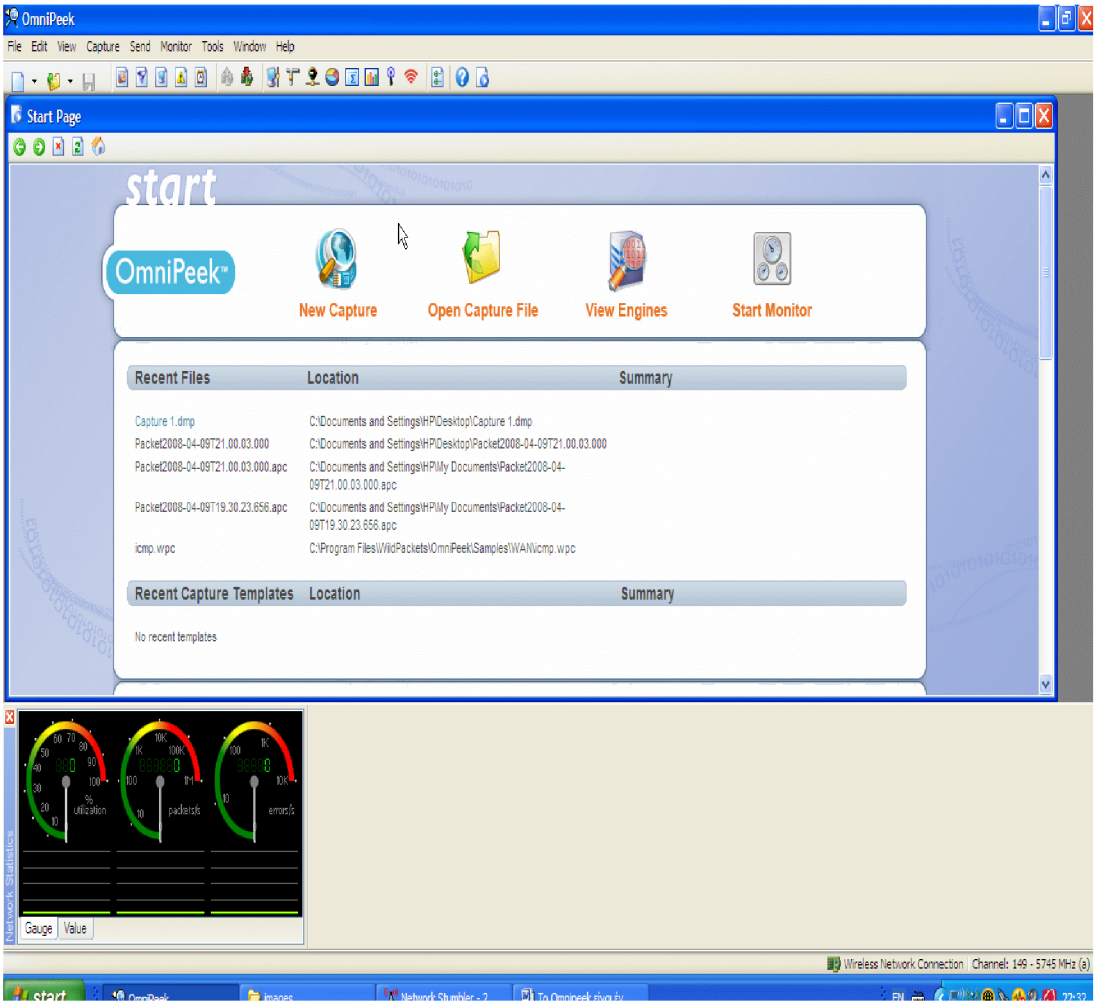
Το Netstumbler μας δίνει τις αρχικές πληροφορίες που χρειαζόμαστε για το εν επίθεση Access Point. . Οι πληροφορίες που παίρνουμε αφορούν την MAC διεύθυνση του, το SSID όνομα του, αν χρησιμοποιεί κάποιου είδους κρυπτογράφησης και το κανάλι που χρησιμοποιεί για να εκπέμψει.

Στην παρακάτω εικόνα φαίνονται τα χαρακτηριστικά του AP που μας ενδιαφέρει για να συνδεθούμε.

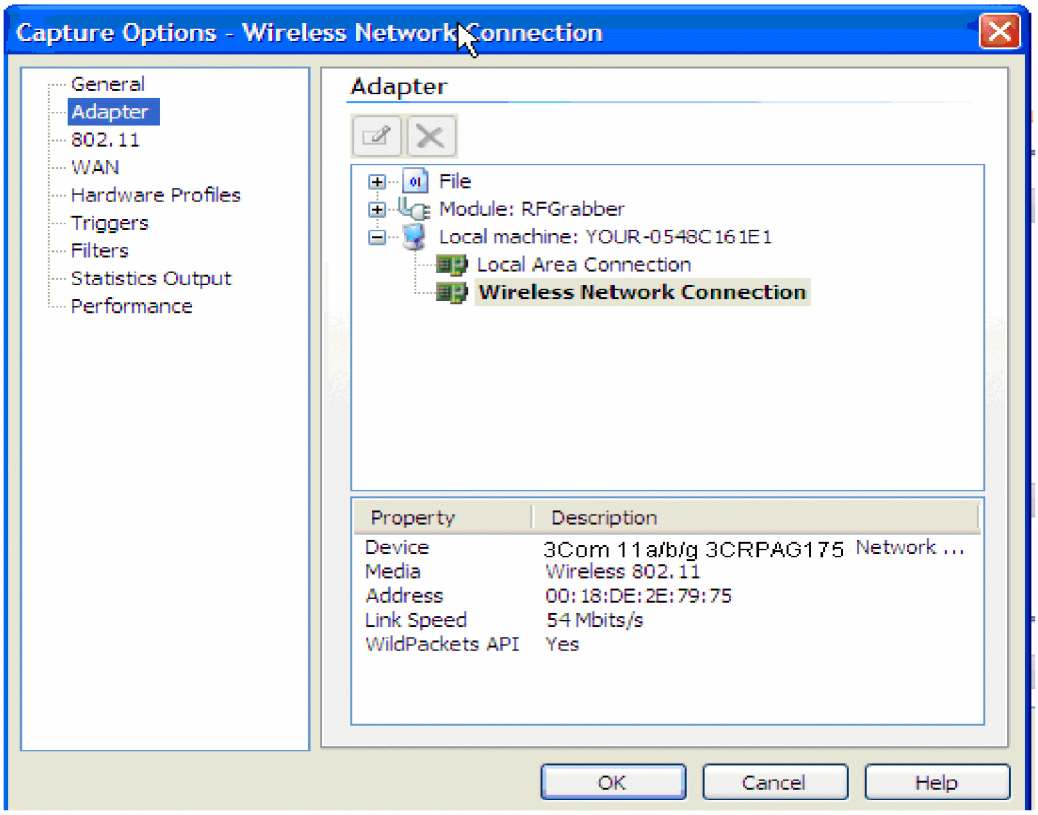


Εικόνα 3.7 Χαρακτηριστικά Α.Ρ.

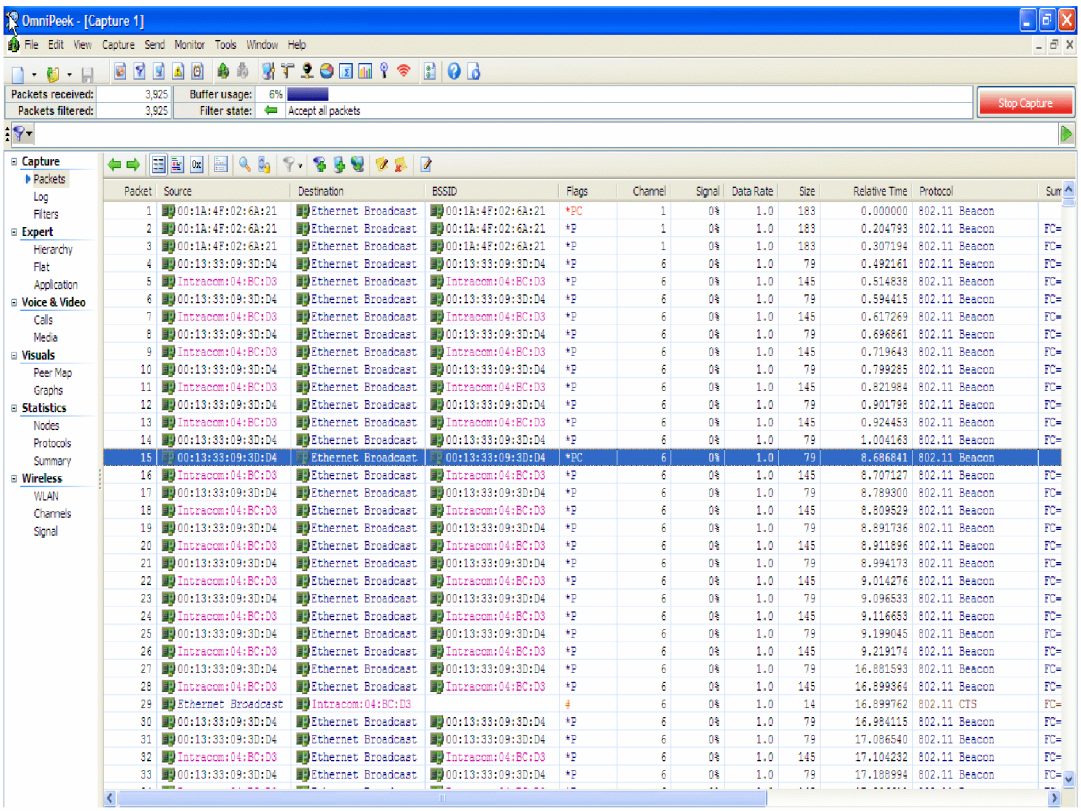
Όταν πάρουμε τις αρχικές πληροφορίες από το Netstumbler ανοίγουμε το OmniPeek βλέπε εικόνα 3.8 , στην συνέχεια πατάμε από το πάνελ του προγράμματος Capture εμφανίζεται ένα παράθυρο Από το οποίο επιλέγουμε τα χαρακτηριστικά τα οποία θα έχει το capturing, π.χ. την MAC διεύθυνση του σταθμού που μας ενδιαφέρει ,το SSID, τα είδη των πακέτων που θα γίνουν capture και άλλα (εικόνα 3.9). Αφού βάλλουμε τα settings που επιθυμούμε πατάμε capture και εμφανίζεται το αρχικό παράθυρο του capturing. Σε αυτό μπορούμε να πάρουμε διάφορα δεδομένα ,στην εικόνα 3.10 φαίνονται τα πακέτα και το είδος τους που στέλνονται από τους διάφορους σταθμούς που επικοινωνούν με το Access point που έχουμε βάλει στόχο.



Εικόνα 3.8 Αρχικό παράθυρο OmniPeek

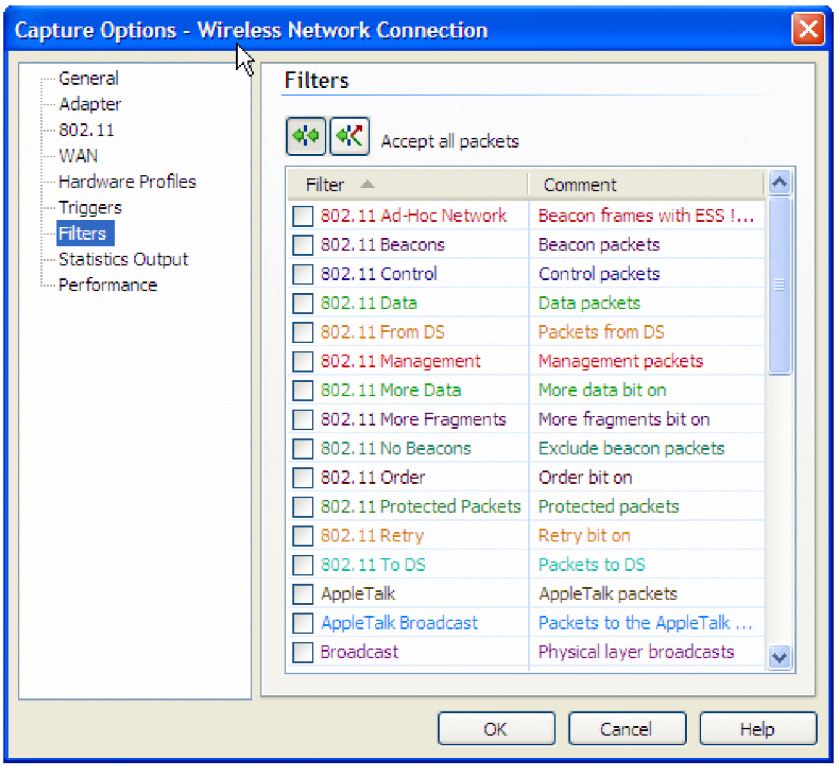


Εικόνα 3.9 Capture Options



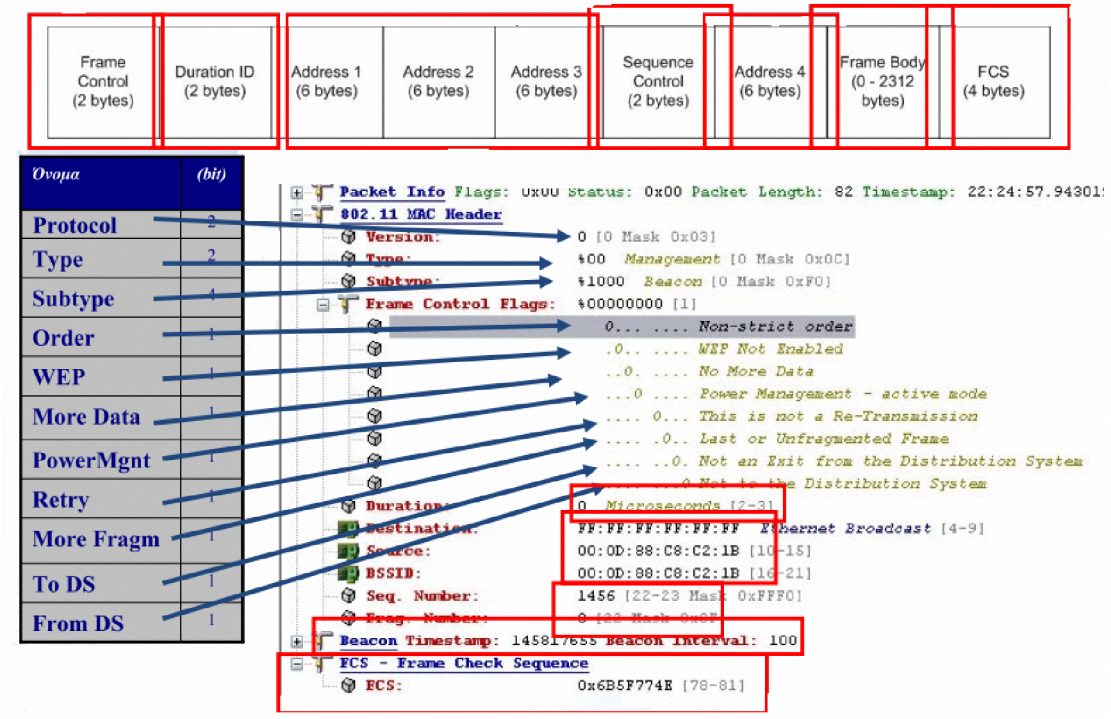
Εικόνα 3.10 Capturing packets

Το OmniPeek μας παρέχει μια πλειάδα ενσωματωμένων φίλτρων που μπορούμε να εισάγουμε στο capturing των πακέτων βοηθώντας μας έτσι να λαμβάνουμε συγκεκριμένα πακέτα χωρίς να γεμίζουμε το buffer με άχρηστα πακέτα (εικόνα 3.11)



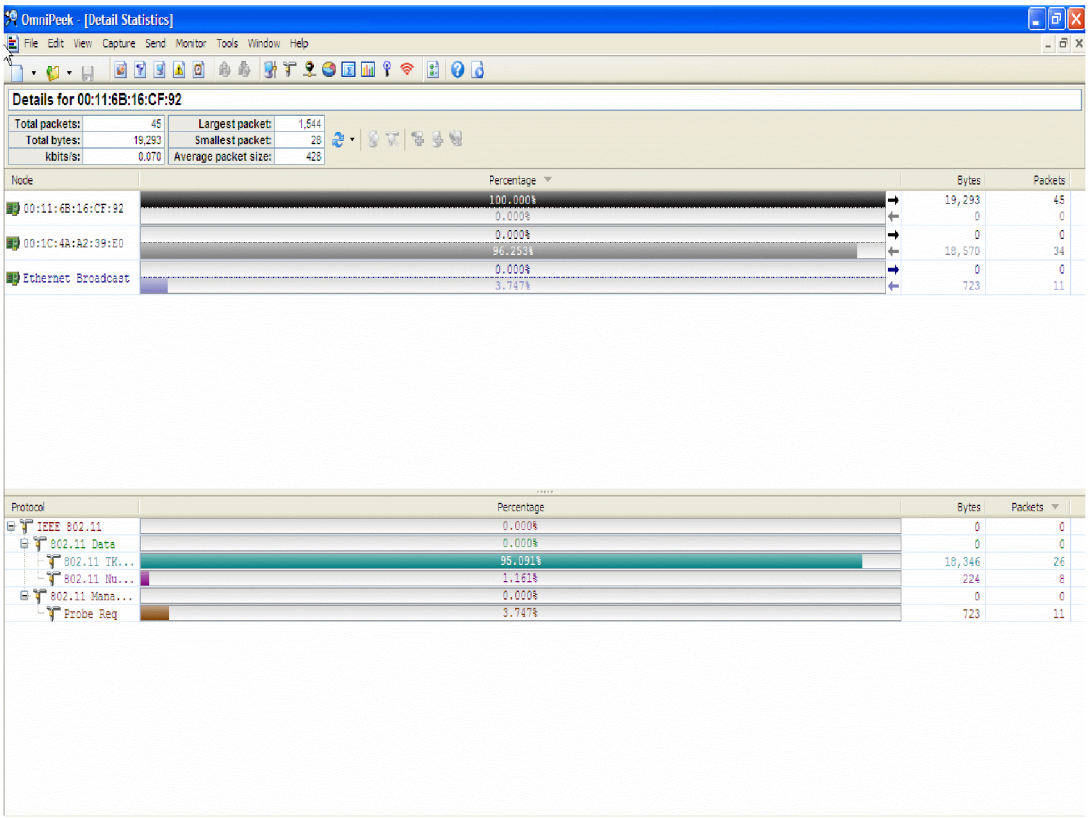
Εικόνα 3.11 Ενσωματωμένα φίλτρα

Η σουίτα αυτή μας δίνει την δυνατότητα να δούμε τα μέρη που αποτελείτε ένα πακέτο που γίνεται capture, πιο συγκεκριμένα στην εικόνα που ακολουθεί παρατίθεται ένα representation του Omnipeek για τα πακέτα που λαμβάνει.



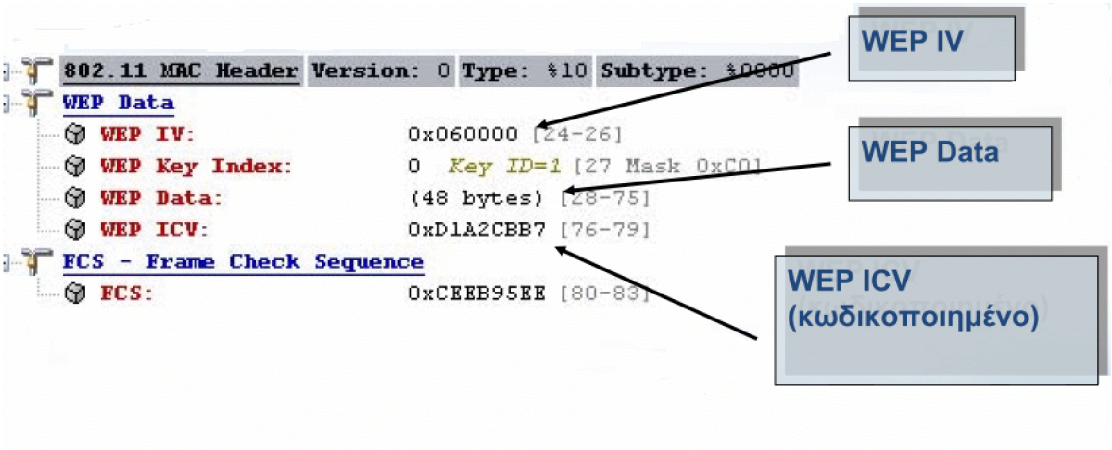
Εικόνα 3.12 Packet Representation

Επίσης με το Omnipeek έχουμε την δυνατότητα να δούμε συγκεκριμένα στατιστικά στοιχεία για το κάθε interface,για παράδειγμα στην εικόνα 3.10 φαίνονται πληροφορίες για τα είδη των πρωτοκόλλων των πακέτων που περνάνε από τον σταθμό με διεύθυνση MAC 00:11:6B:16:CF:92 και με ποιους άλλους σταθμούς επικοινωνεί χρησιμοποιώντας τα πρωτοκόλλα που βλέπουμε στην εικόνα. Αυτό το παράθυρο μας δίνει μια εικόνα, του ποιος στέλνει τι στο εν επιθέσει δίκτυο βοηθώντας μας να κάνουμε τις επιθέσεις μας πιο συγκεκριμένες, με αποτέλεσμα πιο ουσιώδεις , καλύτερες και πιο γρήγορες.



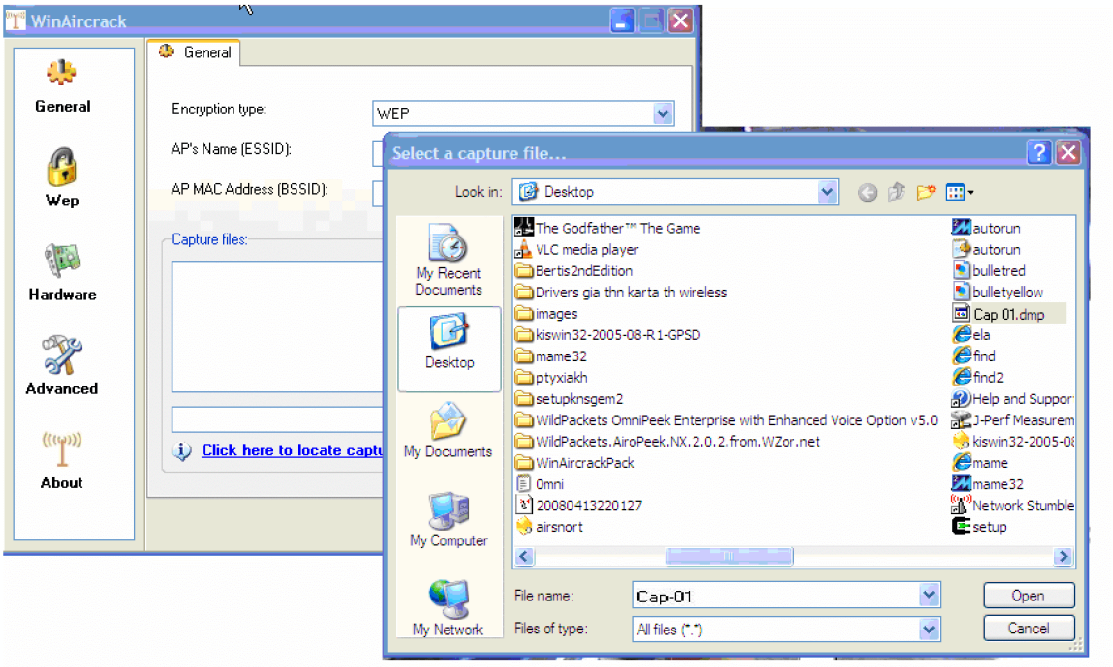
Εικόνα 3.13 Λεπτομέρειες συγκεκριμένου interface

Αυτό που προσπαθούμε να κάνουμε είναι να συλλάβουμε με τον sniffer όσο περισσότερα 802.11 WEP Data κρυπτογραφημένα πακέτα και αυτό γιατί το WinairCrack για να βρει το WEP κλειδί χρειάζεται όσο το δυνατόν περισσότερα WEP IV'S. Στην παρακάτω εικόνα φαίνεται ένα κομμάτι από ένα κρυπτογραφημένο πακέτο που έγινε capture από το Access Point.



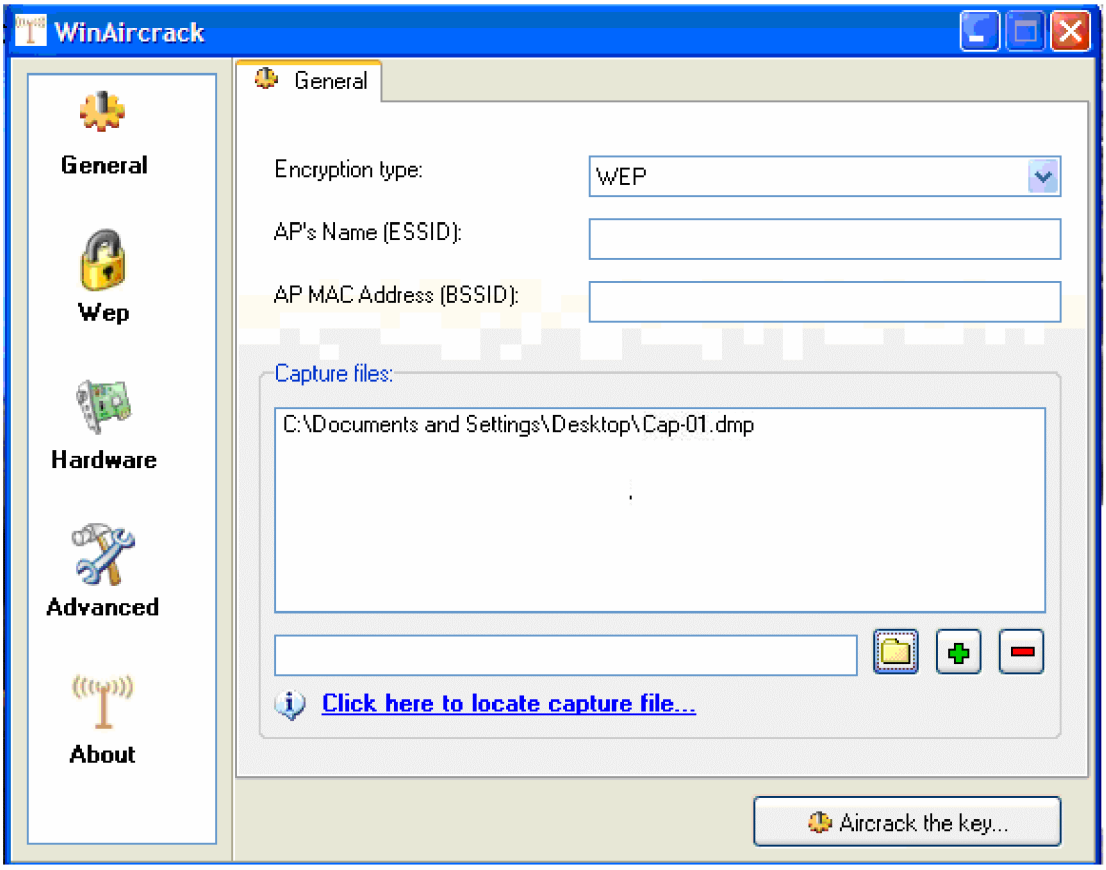
Εικόνα 3.14 Πακέτο WEP Data

Αφού τελειώσει το capture των πακέτων σώζουμε σαν Cap-01.dmp την όλη διαδικασία και ενεργοποιούμε το WinairCrack. Στο πρόγραμμα αυτό θα φορτώσουμε το αρχείο .dmp από το capturing των πακέτων για να βρούμε το WEP κλειδί



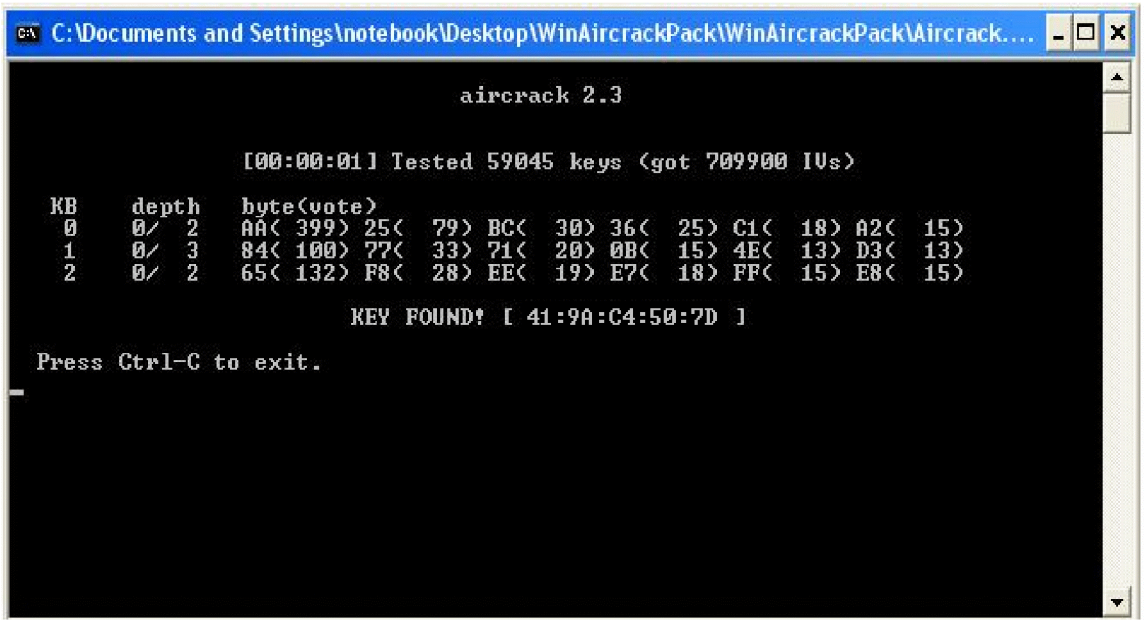
Εικόνα 3.15 Εισαγωγή .dmp αρχείου στο πρόγραμμα

Αφού φορτωθεί το αρχείο πατάμε το κουμπί Aircrack the key (εικόνα 3.16) και ξεκινάει η διαδικασία εύρεσης. Για να μπορέσουμε να βρούμε ένα 40 bit κλειδί θα πρέπει να έχουμε κάνει capture πάνω από 250000 IV's ενώ για ένα 104 bit κλειδί χρειαζόμαστε πάνω από 800000 IV's. Το WinairCrack εκτελεί την επίθεση σύμφωνα με την τεχνική που περιγράφεται στο «S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the Key Scheduling Algorithm of RC4»



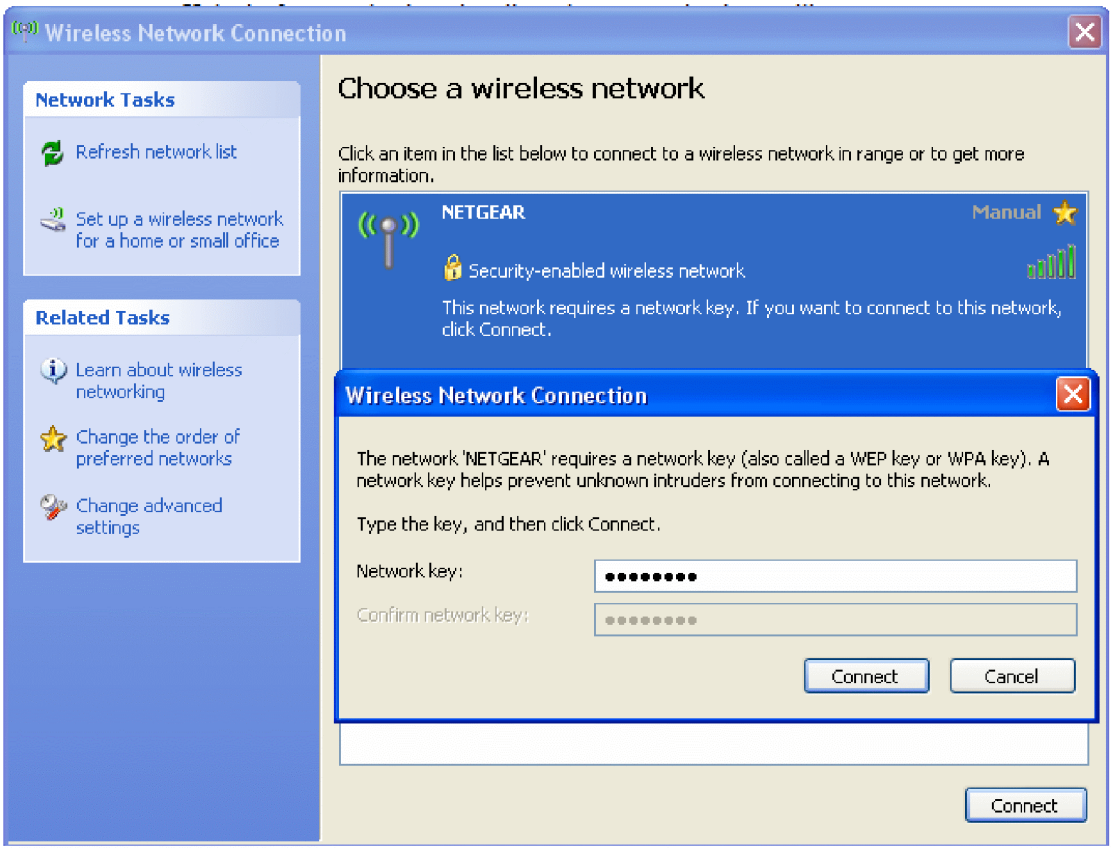
Εικόνα 3.16 Το πρόγραμμα WinAircrack

Στην συνέχεια θα εμφανιστεί ένα παράθυρο (command box) στο οποίο παρουσιάζεται η διαδικασία της εύρεσης του WEP κλειδιού. Στην παρακάτω εικόνα φαίνεται η επιτυχής εύρεση του κλειδιού που χρησιμοποιείται στο Access Point.



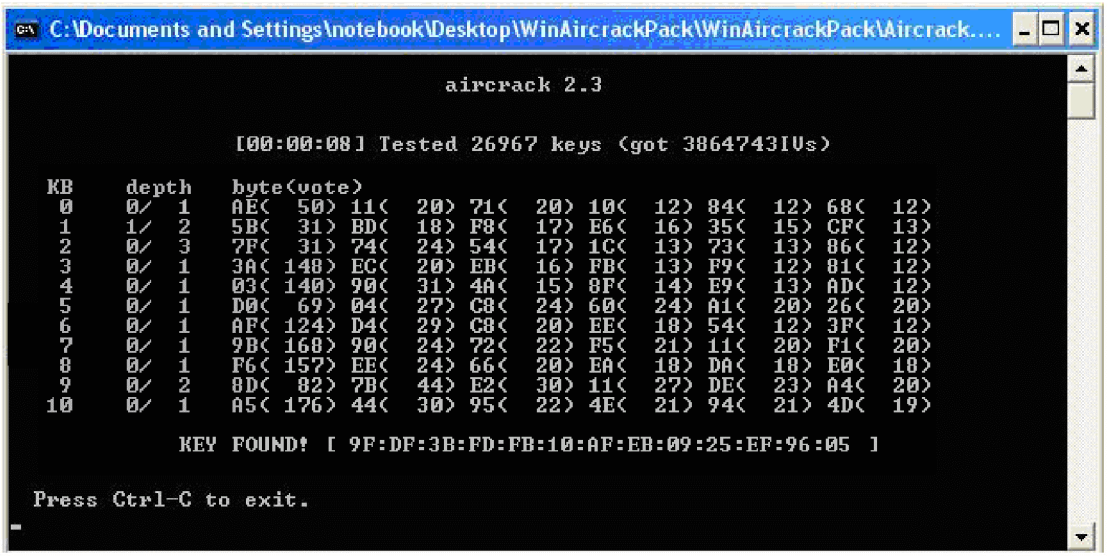
Εικόνα 3.17 Εύρεση WEP κλειδιού 64 bit

Αφού βρούμε το WEP κλειδί η είσοδος στο δίκτυο είναι πια πολύ εύκολη (εικόνα 3.18)



Εικόνα 3.18 Σύνδεση στο δίκτυο

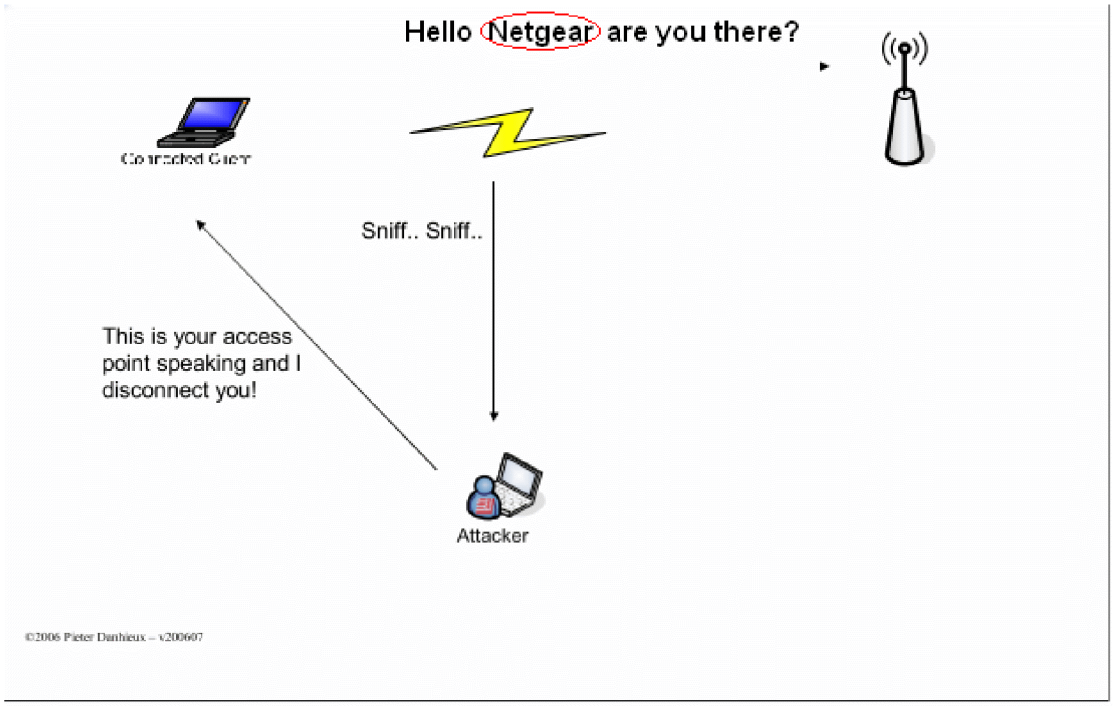
Η ίδια διαδικασία θα ακολουθηθεί σε περίπτωση που το WEP κλειδί με το ίδιο pass phrase είναι 128 bit. Το μόνο που θα αλλάξει είναι ο αριθμός των πακέτων που θα χρειαστούμε να μαζέψουμε με το Omnipeek . Το WEP κλειδί θα το βρούμε και αυτή την φορά με την βοήθεια του Winaircrack (εικόνα 3.19)



Εικόνα 3.19 Εύρεση WEP κλειδιού 128 bit

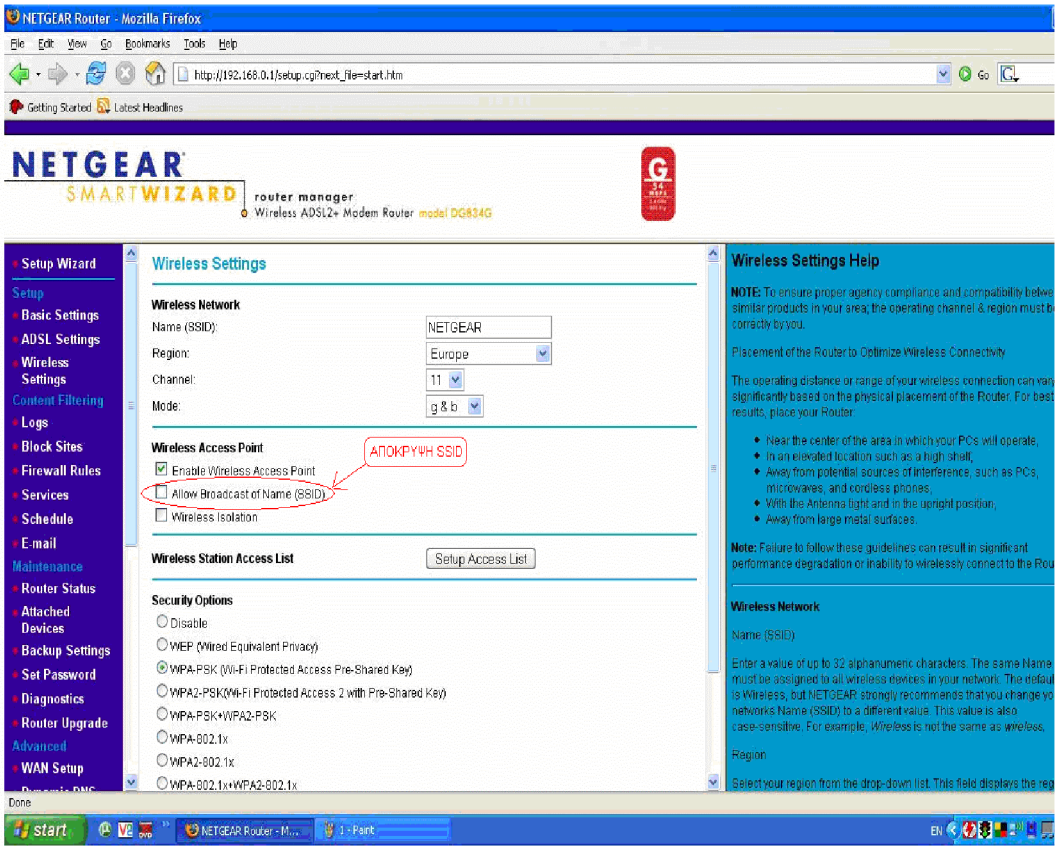
3.2.2 Απόκρυψη του SSID

Η απόκρυψη του SSID του Access Point είναι ακόμα ένας από τους κοινούς μηχανισμούς ασφαλείας που χρησιμοποιούνται κατά κόρον. Χωρίς το SSID δεν είναι δυνατόν να συνδεθούμε στο Access Point.Όταν όμως κάποιος client που το γνωρίζει ήδη προσπαθήσει να συνδεθεί, το SSID περιέχεται στο Probe Request Frame και έτσι ο επιτιθέμενος με το κατάλληλο λογισμικό μπορεί να ανακαλύψει το SSID σε τρία λεπτά.



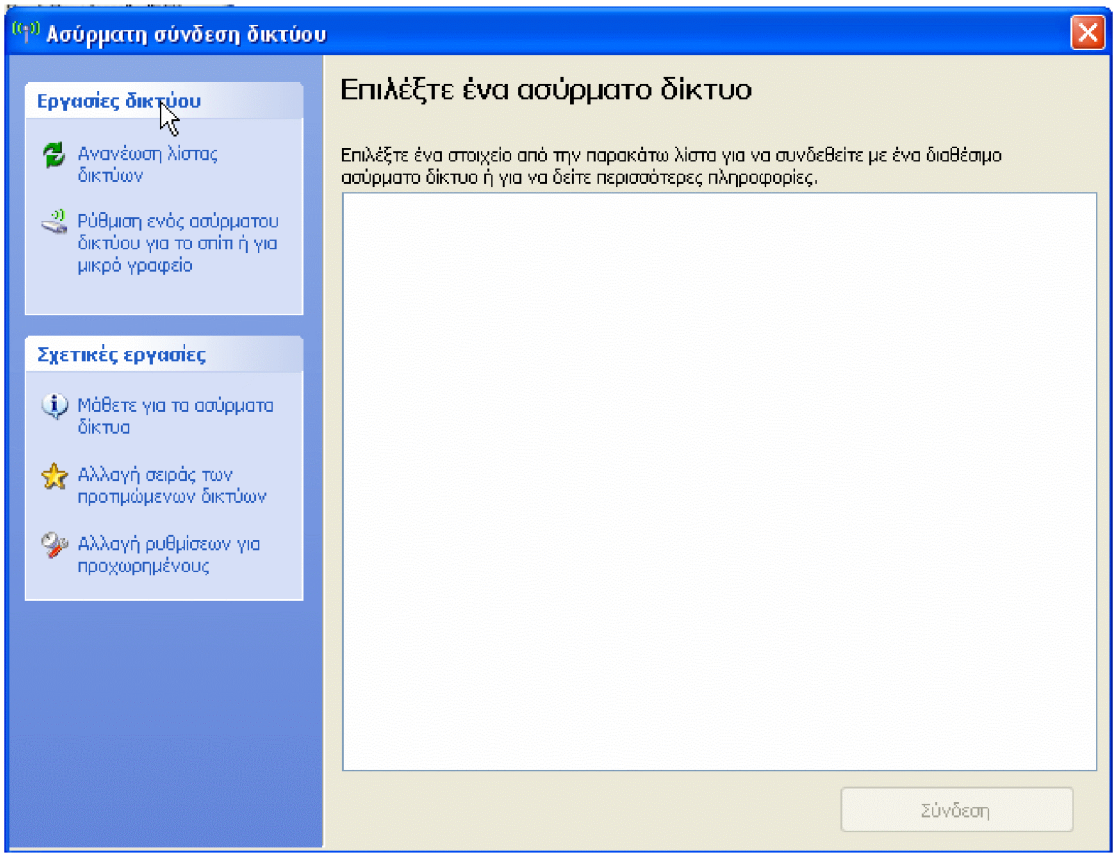
Εικόνα 3.20 Εύρεση κρυμμένου SSID

Η ρύθμιση απόκρυψης του SSID είναι μια πολύ εύκολη υπόθεση, στην παρακάτω εικόνα φαίνεται η διαδικασία απόκρυψης στο Access Point που χρησιμοποιήθηκε για την επίδειξη αυτή.

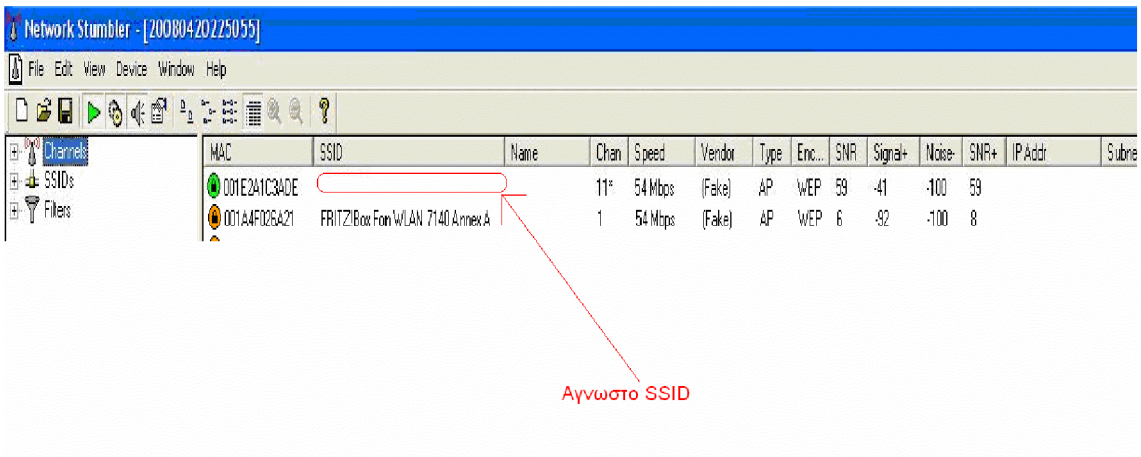


Εικόνα 3.21 Απόκρυψη του SSID στο Router

Αποτέλεσμα της απόκρυψης του SSID είναι να μην φαίνεται το Access Point στους υπολογιστές οι οποίοι θέλουν να συνδεθούν (εικόνα 3.22), ακόμα και για τα πιο διαδεδομένα προγράμματα wardriving όπως το NetStumbler (εικόνα 3.23).

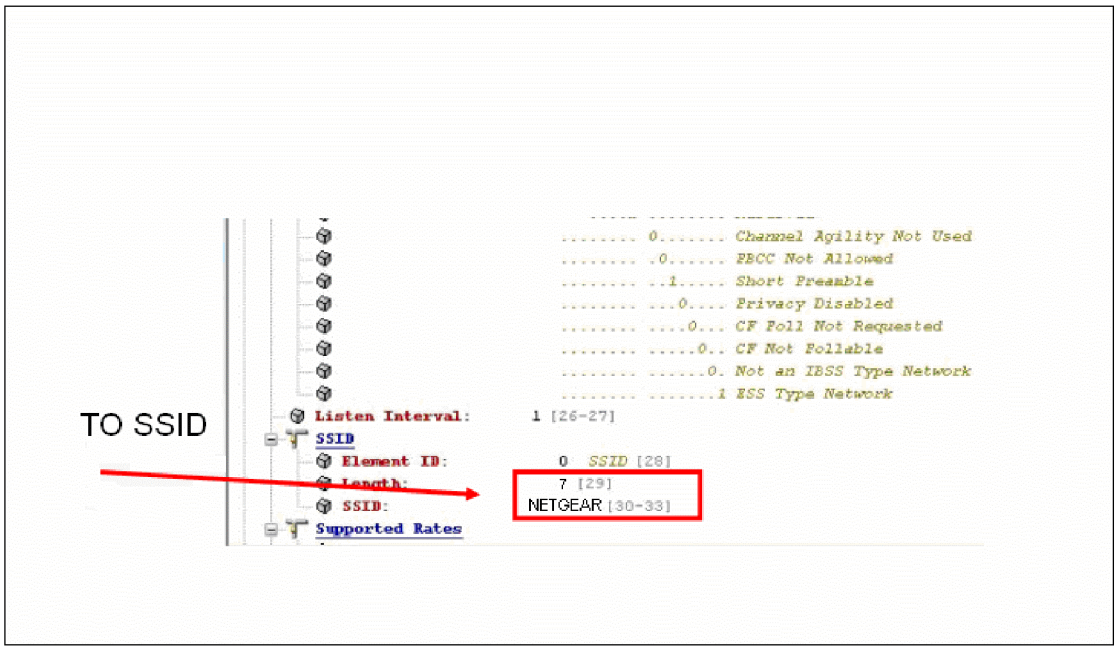


Εικόνα 3.22 Ο σταθμός δεν μπορεί να συνδεθεί λόγω απόκρυψης του SSID



Εικόνα 3.23 Αποτελέσματα απόκρυψης SSID στο NetStumbler

Για να μπορέσουμε να συνδεθούμε στο δίκτυο σε αυτή την φάση χρησιμοποιούμε το πρόγραμμα που κάνει sniffing και περιμένουμε έως ότου ένας κανονικός σταθμός συνδεθεί στο δίκτυο. Με τον sniffer (OmniPeek) θα μπορέσουμε να υποκλέψουμε τα πακέτα που ανταλλάσσει ο κανονικός σταθμός με το Access Point και να βρούμε το SSID. Στην παρακάτω εικόνα φαίνεται το κομμάτι ενός πακέτου, προϊόν υποκλοπής στο οποίο μπορούμε να διακρίνουμε καθαρά το SSID του Access Point.



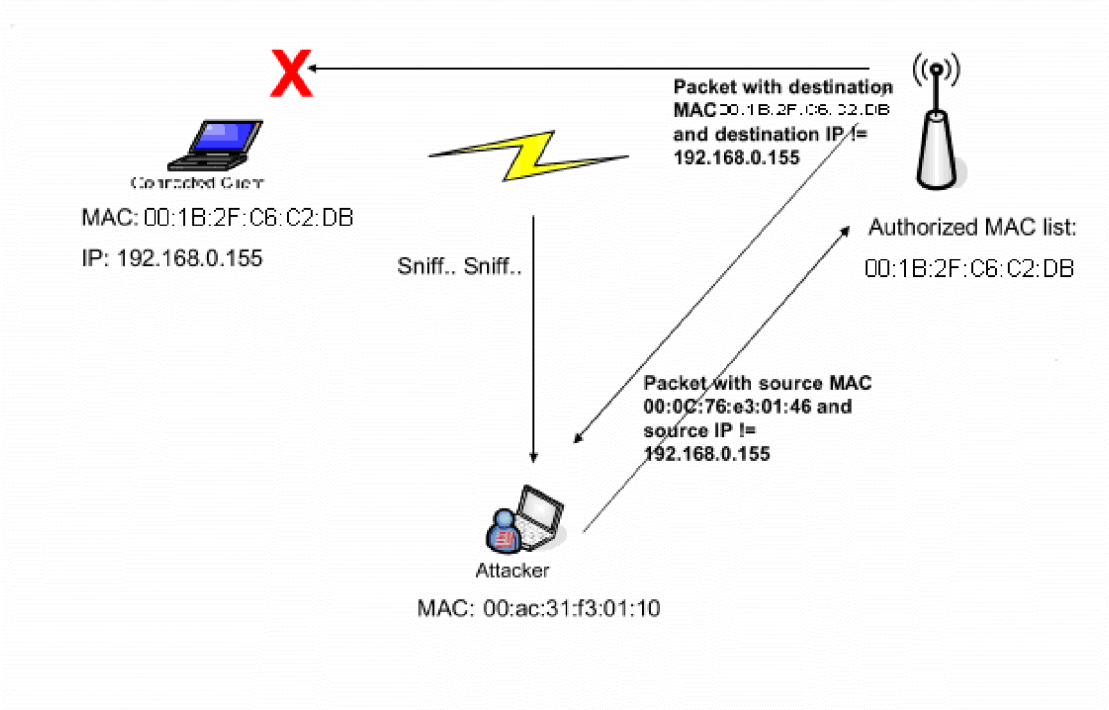
Εικόνα 3.24 Εύρεση κρυμμένου SSID με την βοήθεια του Omnipeek

Αφού βρεθεί το κρυμμένο SSID είμαστε σε θέση να συνδεθούμε στο Access Point

3.2.3 Ρύθμιση αυθεντικοποίησης με την χρήση Mac Διευθύνσεων (MAC Filtering)

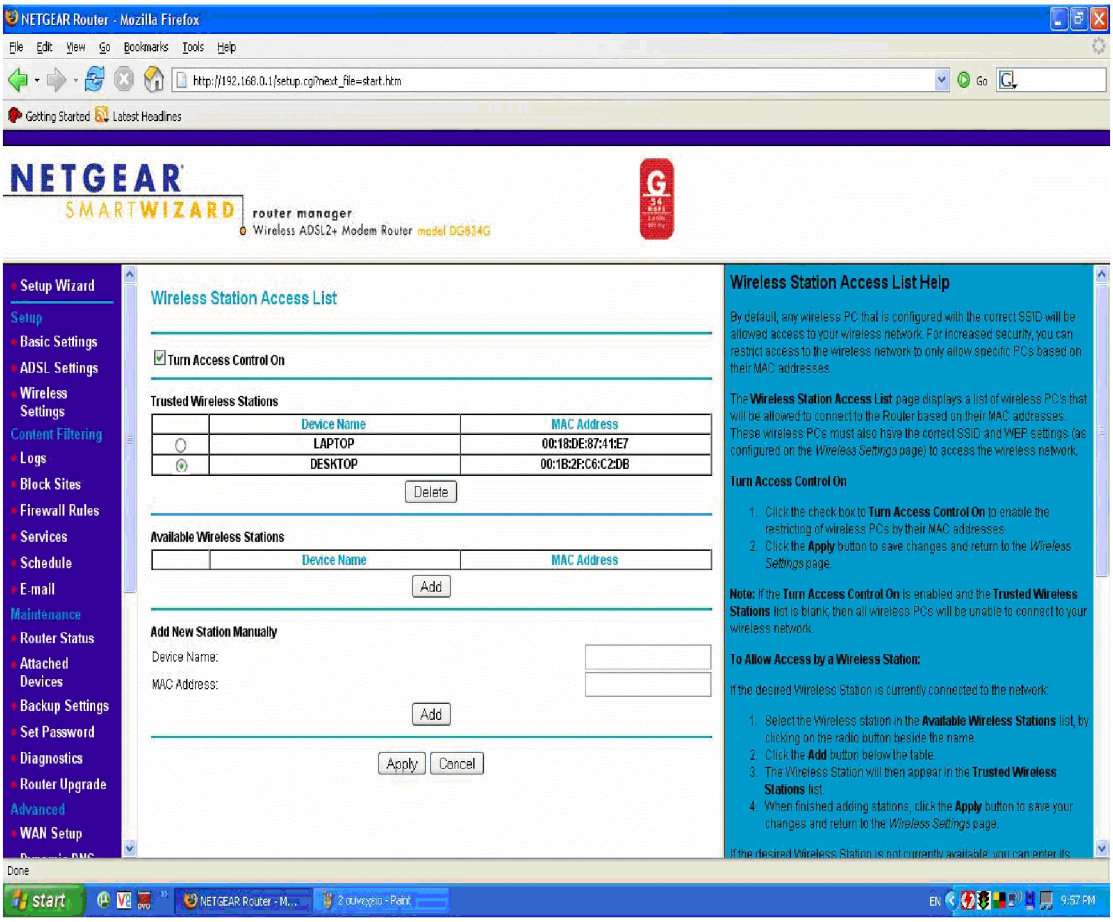
Σκοπός αυτής τεχνικής ασφαλείας είναι να φτιαχτεί ένα "δίκτυο" έμπιστων υπολογιστών με συγκεκριμένες MAC διευθύνσεις που θα έχουν πρόσβαση σύνδεσης σε ένα Access Point, αφήνοντας τους υπόλοιπους, του μη έχοντας την κατάλληλη άδεια (MAC) εκτός δικτύου. Και σε αυτή βέβαια την περίπτωση με τα κατάλληλα

εργαλεία ένας επιτιθέμενος μπορεί να εισέλθει στο δίκτυο χωρίς πολύ μεγάλη προσπάθεια. Αυτό συμβαίνει γιατί όταν frame φτάσει σε ένα ασύρματο σταθμό το πρώτο πράγμα που κάνει ο σταθμός είναι να κοιτάξει εάν είναι ο προορισμός του frame αυτού. Στην συνέχεια γίνεται de-capsulate του frame κοιτώντας αν η IP διεύθυνση του παραλήπτη είναι η δικιά του και το αποδέχεται αλλιώς το αποβάλει. Ο εισβολέας λοιπόν έχει την δυνατότητα να κάνει spoofing την MAC διεύθυνση ενός authorized client και με διαφορετική IP να συνδεθεί (εικόνα 3.25).



Εικόνα 3.25 MAC spoofing

Αρχικά ρυθμίζουμε τον router να δέχεται συνδέσεις από σταθμούς με συγκεκριμένες MAC διευθύνσεις όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 3.26 Επιλογή trusted MAC διευθύνσεων

Το αποτέλεσμα της ρύθμισης αυτής φαίνεται στην εικόνα όπού ένας σταθμός με διαφορετική MAC διεύθυνση από αυτές που δέχεται το Access Point προσπαθεί να συνδεθεί.

Το παραπάνω αποτέλεσμα φαίνεται και από το αποτέλεσμα sniffing όπου ο τερματικός σταθμός αν και ανακαλύπτει την ύπαρξη του ασύρματου δικτύου δεν παίρνει απάντηση-αυθεντικοποίηση από το Access Point (εικόνα.3.27).

24	00:12:A9:03:3F:9B	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	00,575082	802.11 Probe Req
25	00:0D:88:C8:C2:1B	00:12:A9:03:3F:9B	00:0D:88:C8:C2:1B	00,576191	802.11 Probe Rsp
26	00:12:A9:03:3F:9B			00,576512	802.11 Ack
27	00:0D:88:C8:C2:1B	00:12:A9:03:3F:9B	00:0D:88:C8:C2:1B	00,606285	802.11 Probe Rsp
28	00:12:A9:03:3F:9B	00:0D:88:C8:C2:1B		01,018678	802.11 Auth
29	00:0D:88:C8:C2:1B	00:12:A9:03:3F:9B		01,018988	802.11 Ack
30	00:12:A9:03:3F:9B	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	01,539501	802.11 Probe Req
31	00:0D:88:C8:C2:1B	00:12:A9:03:3F:9B	00:0D:88:C8:C2:1B	01,540637	802.11 Probe Rsp
32	00:12:A9:03:3F:9B	00:0D:88:C8:C2:1B		01,540957	802.11 Ack
33	00:12:A9:03:3F:9B	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	01,559215	802.11 Probe Req
34	00:0D:88:C8:C2:1B	00:12:A9:03:3F:9B	00:0D:88:C8:C2:1B	01,560337	802.11 Probe Rsp

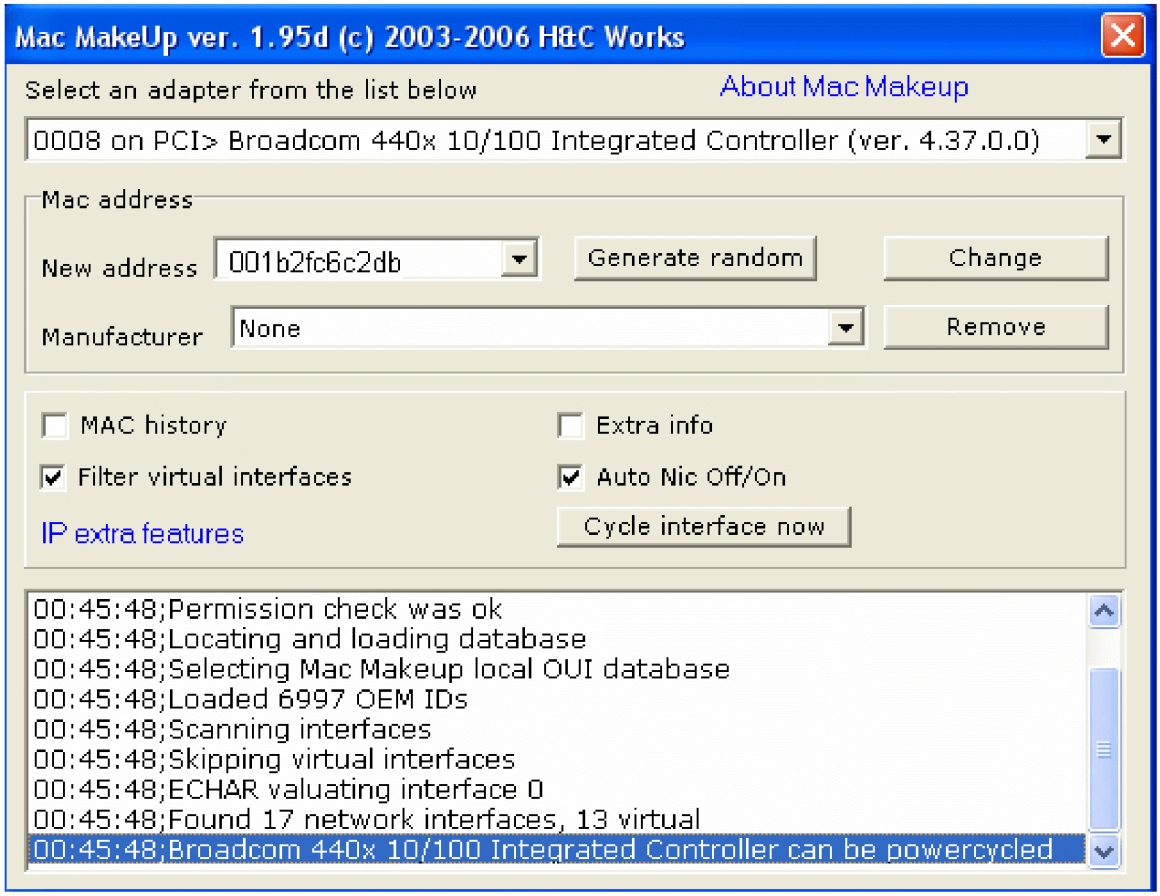
Εικόνα 3.27 Αποτελέσματα αυθεντικοποίησης με την χρήση MAC Διευθύνσεων

Για να παρακάμψουμε αυτό το εμπόδιο χρησιμοποιούμε πάλι το OmniPeek. Ξεκινάμε το capturing παρακολουθώντας τους σταθμούς που θα επικοινωνήσουν με το Access Point.Στην παρακάτω εικόνα βλέπουμε ένα σταθμό με διεύθυνση MAC την 00:18:DE:87:41:E7 να επικοινωνεί με τον router.

30	00:18:DE:87:41:E7	Ethernet Broadcast	00:13:33:09:3D:D4	*P	6	0%	1.0	79	16.984115	802.11 Beacon
31	00:13:33:09:3D:D4	Ethernet Broadcast	00:13:33:09:3D:D4	*P	6	0%	1.0	79	17.086540	802.11 Beacon

Εικόνα 3.28 Επικοινωνία ενός σταθμού με τον router

Στην επίδειξη αυτή θα προσπαθήσουμε να συνδεθούμε στο δίκτυο αλλάζοντας την διεύθυνση MAC του επιτιθέμενου σταθμού (laptop) με την βοήθεια του προγράμματος Mac MakeUp (εικόνα 3.29).



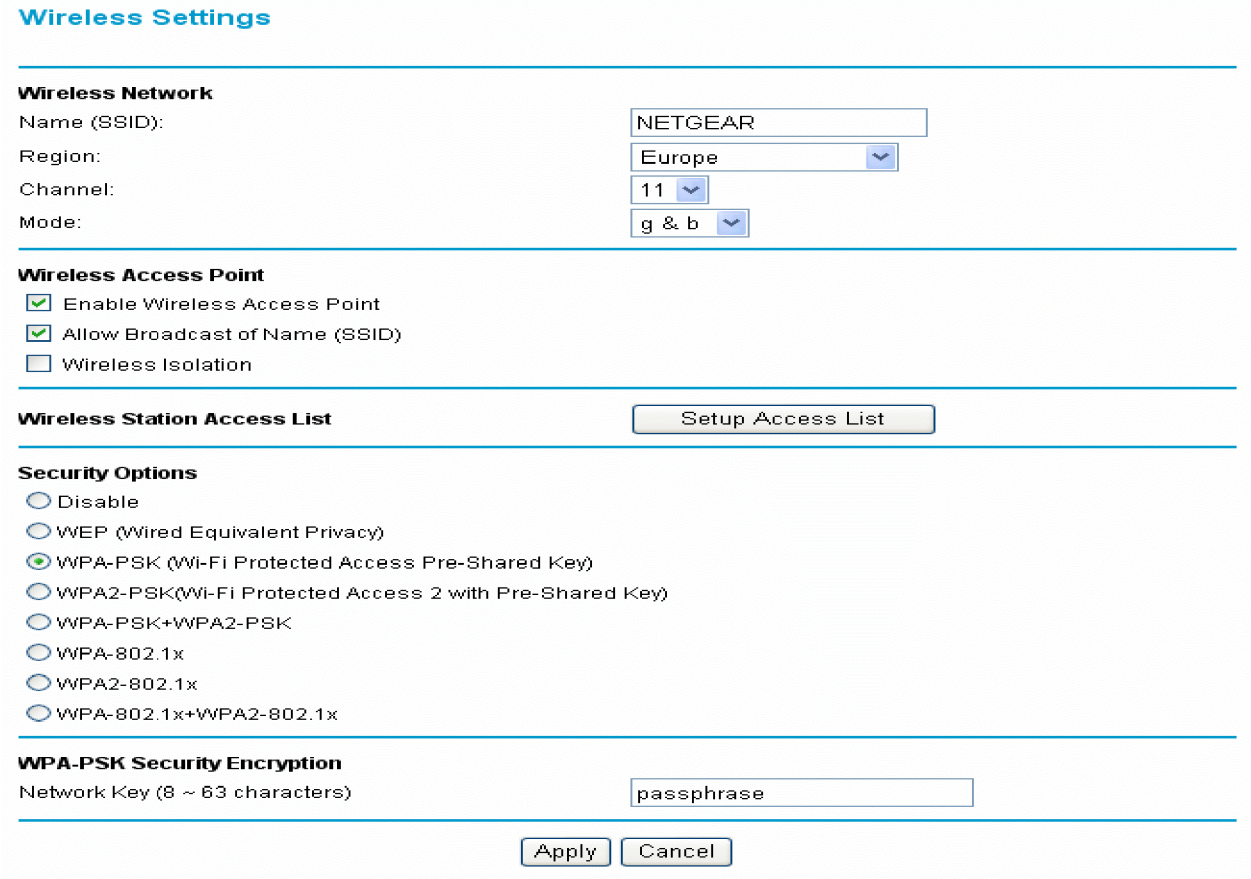
Εικόνα 3.29 Αλλαγή Mac διεύθυνσης του επιτιθέμενου σταθμού

Αφού γίνει η αλλαγή της MAC διεύθυνσης ο σταθμός συνδέεται στο δίκτυο κανονικά, με την προϋπόθεση βέβαια ότι ο κανονικός- αυθεντικός σταθμός δεν είναι ήδη συνδεδεμένος.

3.2.4 Εύρεση WPA-PSK κλειδιού

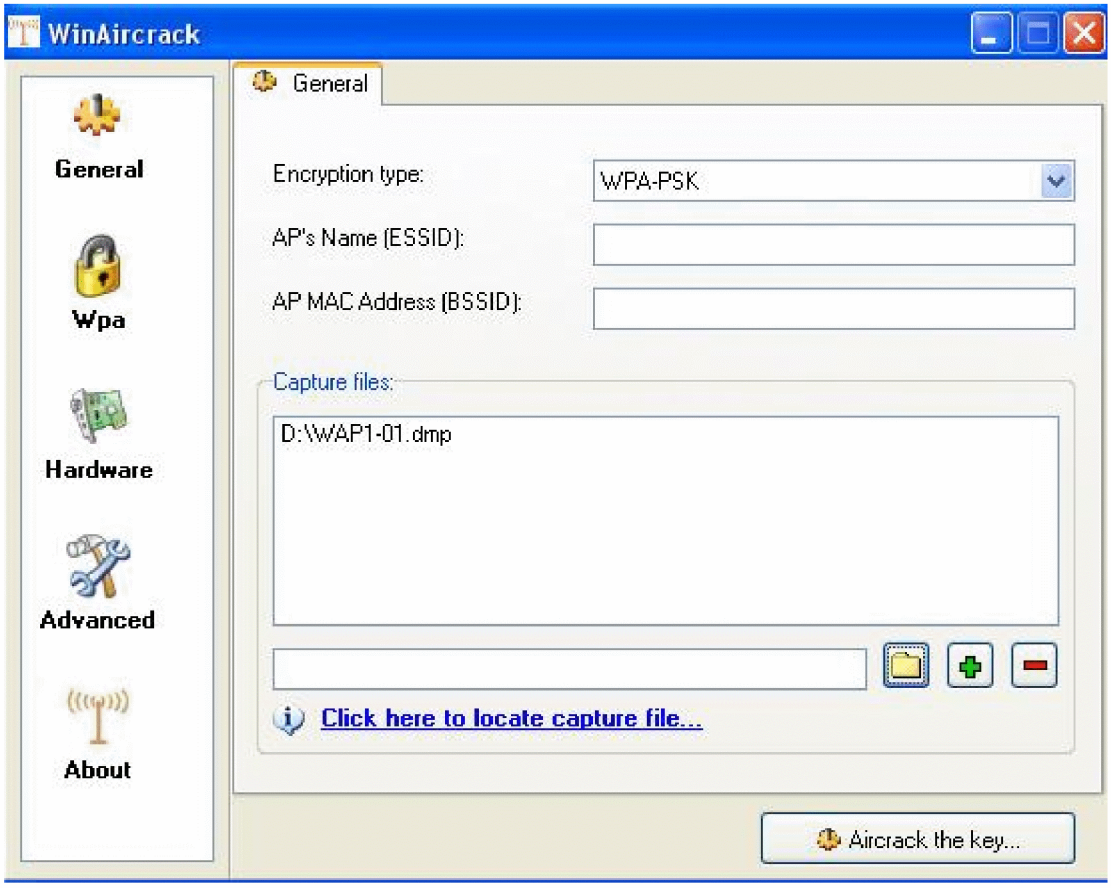
Η εύρεση του WPA-PSK κλειδιού σε περιβάλλον Windows γίνεται με την χρησιμοποίηση του Winaircrack. Αρχικά κάνουμε τις αναγκαίες ρυθμίσεις στον router για να λειτουργεί με WPA- PSK (εικόνα 3.30) , η λέξη που χρησιμοποιούμε για την παραγωγή του κλειδιού είναι η "passphrase". Η τεχνική η οποία χρησιμοποιήθηκε ονομάζεται επίθεση λεξικού (dictionary attack), για την επιτυχή έκβασή της χρειαζόμαστε το SSID του δικτύου και τα τέσσερα μηνύματα της «χειραψίας» μεταξύ του client και του Router και ένα αρχείο που περιέχει συνήθεις λέξεις που χρησιμοποιούνται για την δημιουργία των κλειδιών. Τα αρχεία που χρησιμοποιήθηκαν στην επίδειξη βρίσκονται στην διεύθυνση

http://www.leetupload.com/dbindex2/index.php?dir=Word%20Lists/. Κατά την επίθεση αυτή ο επιτιθέμενος δεν χρειάζεται να είναι συνδεδεμένος στο Access Point.

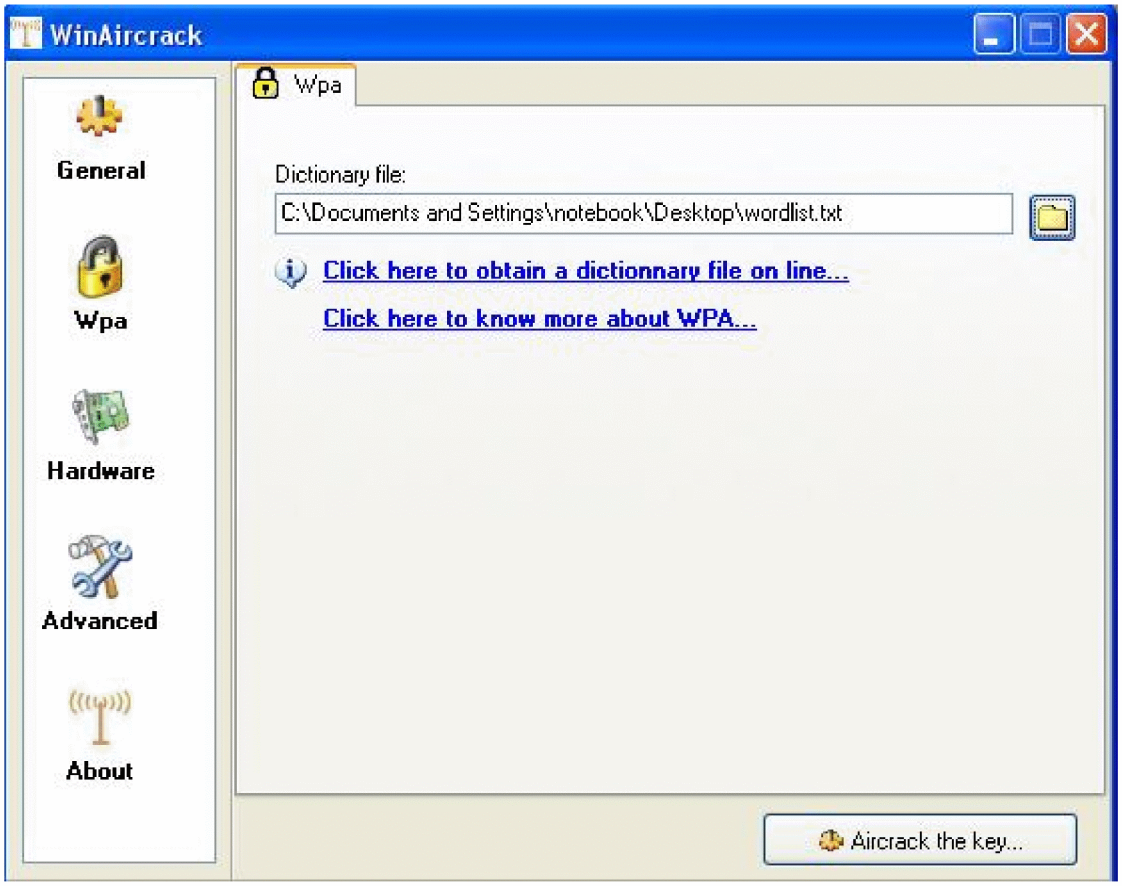


Εικόνα 3.30 Ρυθμίσεις στον Router για την χρησιμοποίηση του WPA- PSK

Για να ξεκινήσουμε το capturing των πακέτων περιμένουμε να συνδεθή ένας client με πρόσβαση και χρησμοποιούμε ξανά το λογισμικό Omnipeek. Αφού μαζέψουμε τα πακέτα που χρειαζόμαστε, ανοίγουμε το Winaircrack και κάνουμε χρήση των captured αρχείων και το wordlist που έχουμε. Στις παρακάτω εικόνες φαίνεται βήμα προς βήμα η διαδικασία που ακολουθείται με το Winaircrack.

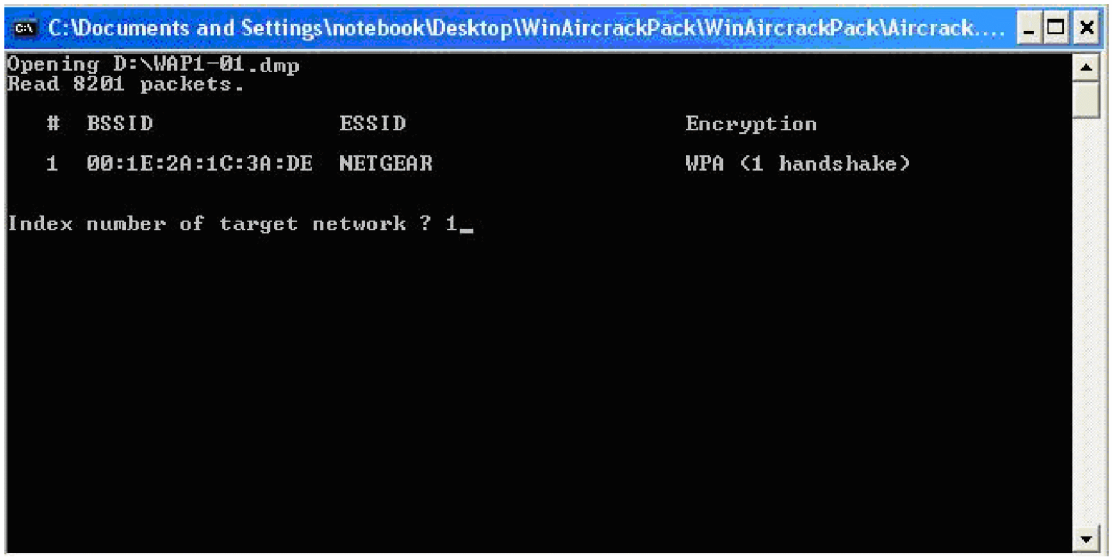


Εικόνα 3.31 Επιλογή τύπου encryption στο WinAircrack

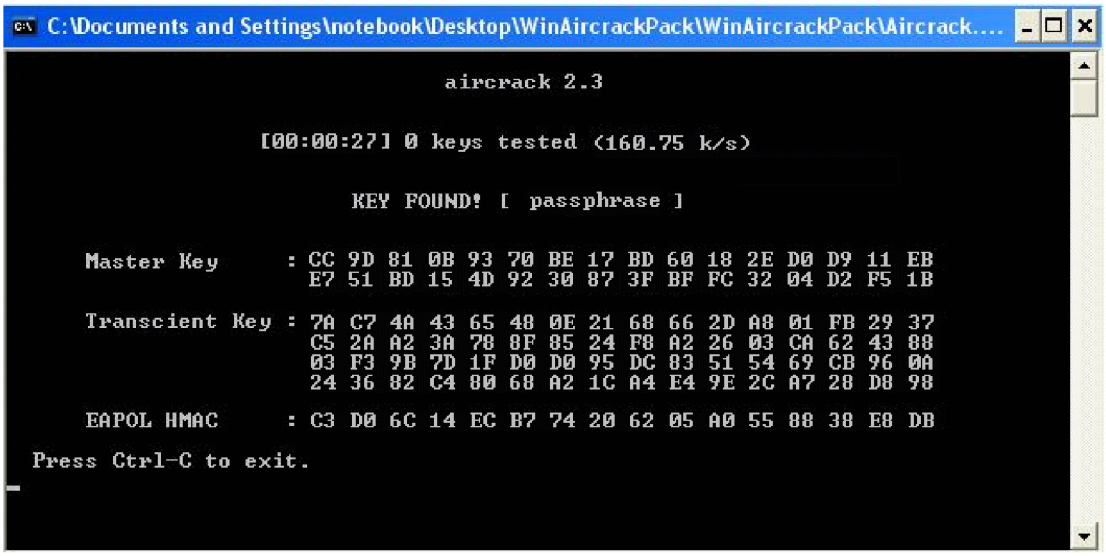


Εικόνα 3.32 Φόρτωση αρχείου wordlist

Αφού φορτώσουμε το wordlist στο πρόγραμμα ξεκινάμε την εύρεση του κλειδιού, διαλέγουμε το δίκτυο που θέλουμε (εικόνα 3.33) και τέλος το Winaircrack μας εμφανίζει την λέξη κλειδί που χρησιμοποιείται στο δίκτυο (εικόνα 3.34).

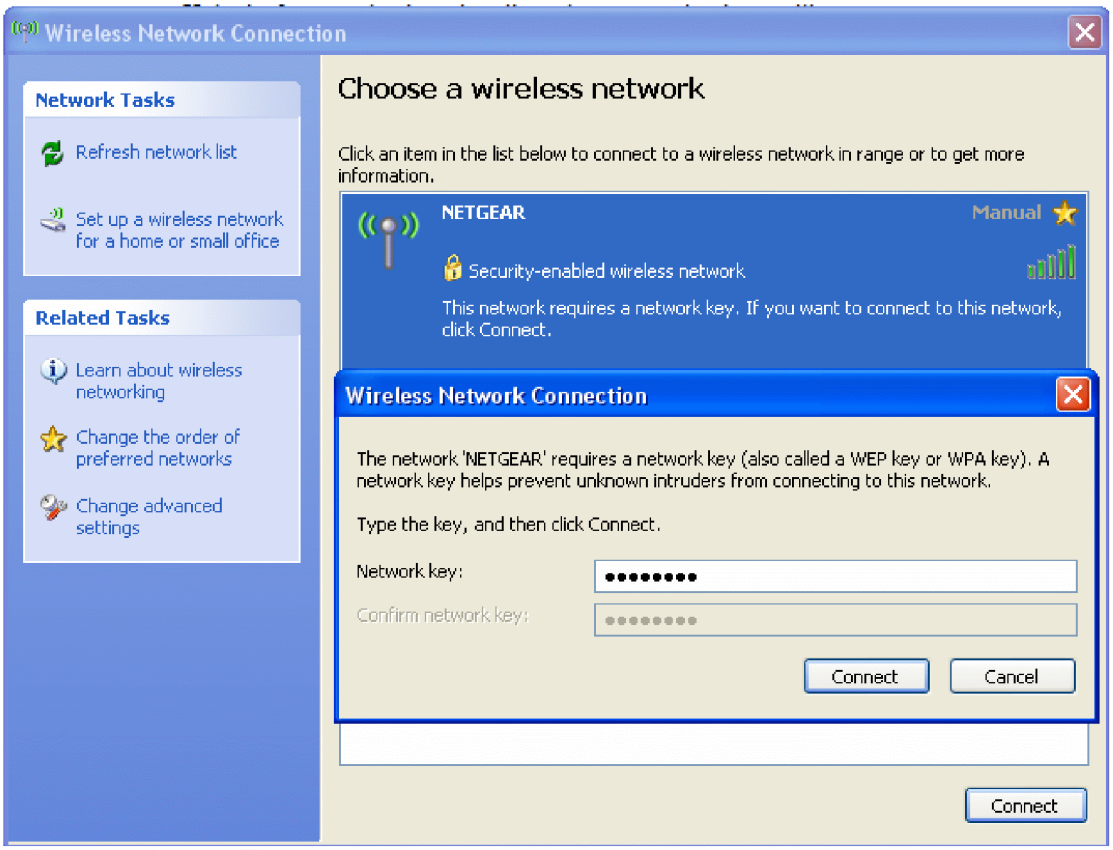


Εικόνα 3.33 Επιλογή δικτύου



Εικόνα 3.34 Εύρεση WPA φράσης κλειδί

Αφού βρούμε το κλειδί η είσοδος στο δίκτυο είναι πολύ εύκολη (εικόνα 3.35).



Εικόνα 3.35 Σύνδεση στο δίκτυο

4.1 ΧΡΗΣΗ ΕΡΓΑΛΕΙΩΝ ΣΕ ΠΕΡΙΒΑΛΛΟΝ LINUX

Για την υλοποίηση της επίδειξης αυτής χρησιμοποιήθηκε μια ειδική έκδοση (distribution) που ονομάζεται Back Track 2.

Η έκδοση Back Track 2 είναι ένα distribution (bootable live cd) η οποία είναι πλήρως παραμετροποιημένη και έχει ενσωματωμένα πλειάδα εργαλείων για wireless και TCP/IP networking. Για περισσότερες πληροφορίες υπάρχει το site http://www.remote-exploit.org/backtrack.html . Πιο συγκεκριμένα τα προγράμματα που χρησιμοποιήθηκαν είναι τα ακόλουθα. Το Kismet (www.**kismet**wireless.net) είναι ένας wireless network detector με ενσωματωμένες δυνατότητες packet sniffing. Είναι ένα συγγενές λογισμικό με το NetStumbler που χρησιμοποιείται στην πλατφόρμα Windows με πολύ μεγαλύτερες δυνατότητες από αυτό. Το επόμενο λογισμικό που χρησιμοποιήθηκε είναι το aircrack-ng (www.aircrack-ng.org) . Το aircrack-ng είναι μια σουίτα που περιλαμβάνει πολλά εργαλεία για επιθέσεις σε Access Points, αυτά είναι: Το airmon είναι ένα εργαλείο και χρησιμοποιείται για να βάζουμε την ασύρματη κάρτα σε monitor mode (rfmon). Το airodump , είναι ένα εργαλείο που χρησιμοποιείται για το capturing των πακέτων στο ασύρματο δίκτυο. Το aireplay το οποίο είναι ένα εργαλείο που χρησιμοποιείται στην πλαστή δημιουργία ARP requests. Το aircrack το οποίο είναι η έκδοση σε πλατφόρμα Linux του WinAircrack που χρησιμοποιήσαμε στην επίδειξη με το λειτουργικό Windows.

Επιπλέον ξέχωρα από την σουίτα του aircrack-ng χρησιμοποιείται το γνωστό ενσωματωμένο εργαλείο iwconfig το οποίο μας βοηθά στο configuration της ασύρματης κάρτας . Εδώ χρησιμοποιείται για να σιγουρευτούμε ότι η ασύρματη κάρτα μας έχει μπει σε monitor mode και στέλνει ψεύτικα ARP request στον υπό επίθεση wireless router(Access Point). Τέλος το macchanger το εργαλείο που χρησιμοποιείται για την αλλαγή της MAC διεύθυνσης της ασύρματης κάρτας.

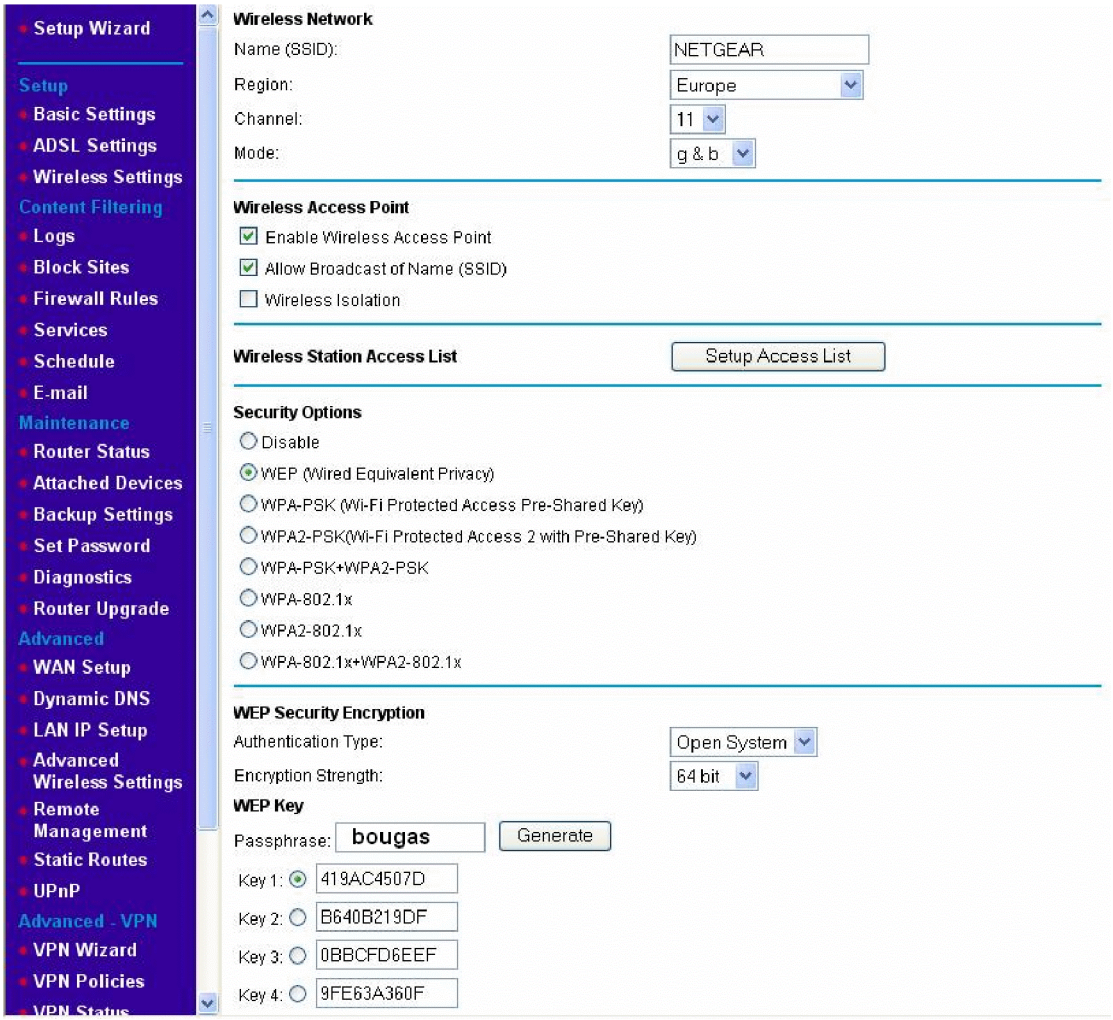
4.1.1 Εύρεση WEP κλειδιού

Αρχικά κάνουμε όλες τις απαραίτητες ρυθμίσεις στο Access Point για την χρησιμοποίηση WEP κλειδιού. Οι παρακάτω εικόνες εμφανίζουν την διαδικασία στο wireless Router. Στην πρώτη εικόνα φαίνεται το configuration του router που χρησιμοποιούμε.

Εικόνα 4.1 Το configuration του Router

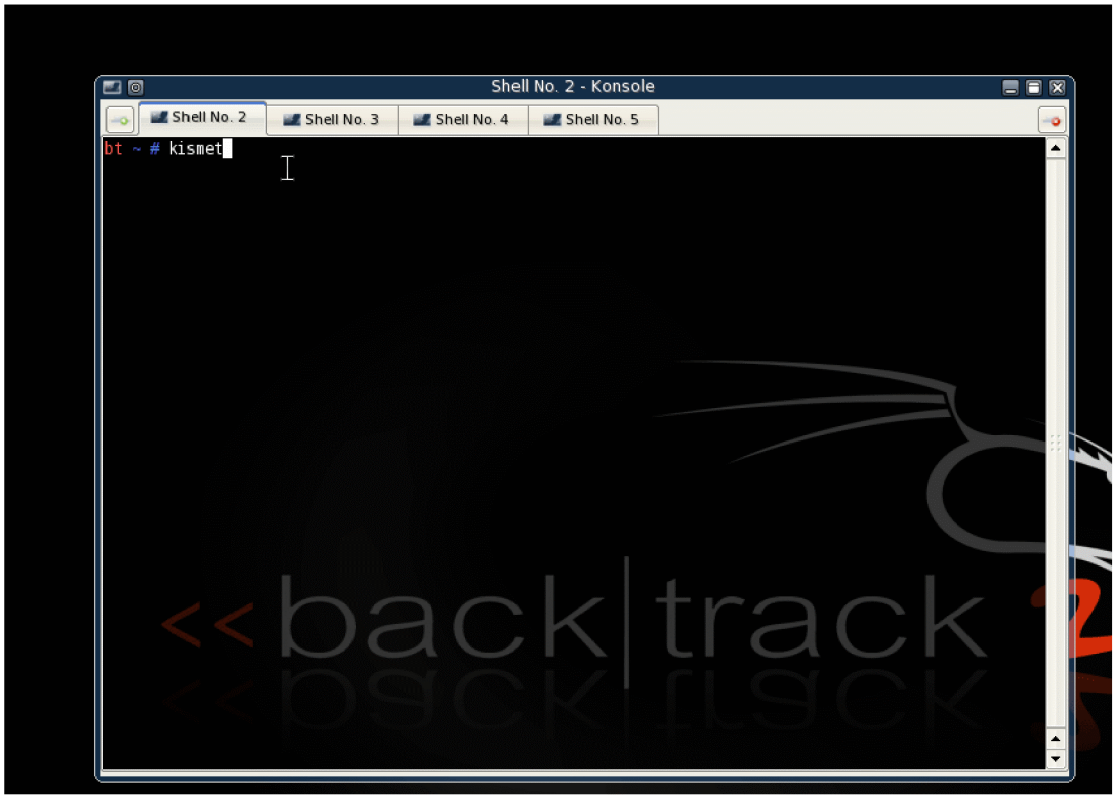
Αρχικά για να μπορέσουμε να χρησιμοποιήσουμε το WEP πρέπει να εισάγουμε το κλειδί στον router χειροκίνητα (εικόνα 4.2), το μέγεθος του κλειδιού που χρησιμοποιήθηκε με την passphrase bougas είναι στα 64 bit το οποίο είναι σχετικά μικρό και σπάει σε πολύ λίγο χρόνο μαζεύοντας μικρό αριθμό IV's. Αφού κάνουμε

όλες τι απαραίτητες ενέργειες είμαστε έτοιμοι να ξεκινήσουμε την διαδικασία εύρεσης του κλειδιού.



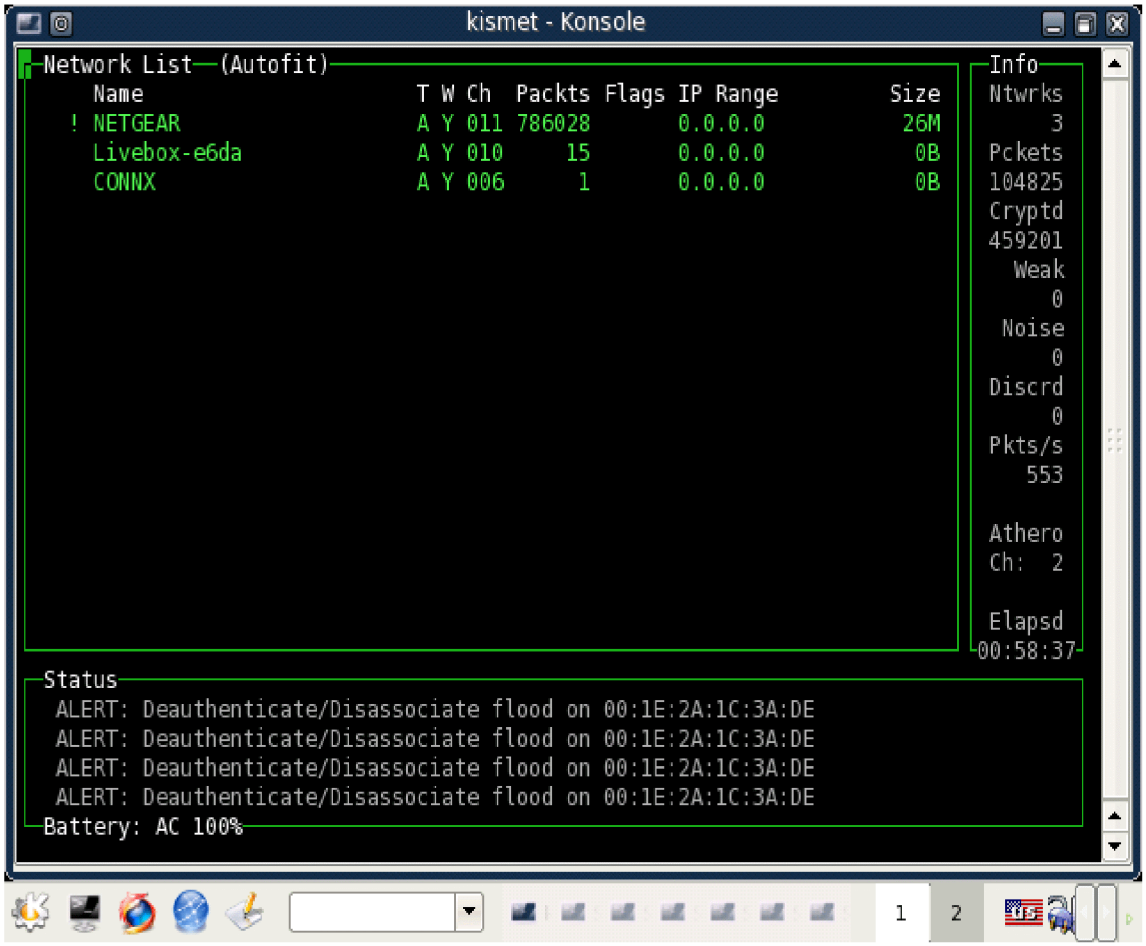
Εικόνα 4.2 Δημιουργία WEP κλειδιού στον Router

Όπως και στην πρώτη επίδειξη έτσι και εδώ ξεκινούμε εντοπίζοντας αρχικά το δίκτυο που μας ενδιαφέρει με την βοήθεια του Kismet αυτή την φορά. Ανοίγουμε ένα terminal πληκτρολογούμε την λέξη kismet (εικόνα 4.3). Το Kismet εν αντιθέσει με το NetStumbler που χρησιμοποιήθηκε στην επίδειξη με το λειτουργικό Windows είναι ένας παθητικός sniffer (passive sniffer). Το NetStumbler κάνει broadcast σε ένα Access Point αποκρίνεται σε SSID με όνομα "ANY". Το Kismet δεν στέλνει κανένα πακέτο , δουλεύει βάζοντας την ασύρματη κάρτα σε RF monitor mode. Οσο η κάρτα είναι σε RF monitor mode ο client δεν μπορεί να συνδεθεί σε κάποιο Access Point αλλά "ακούει" όλη την κίνηση στον αέρα (wireless traffic).

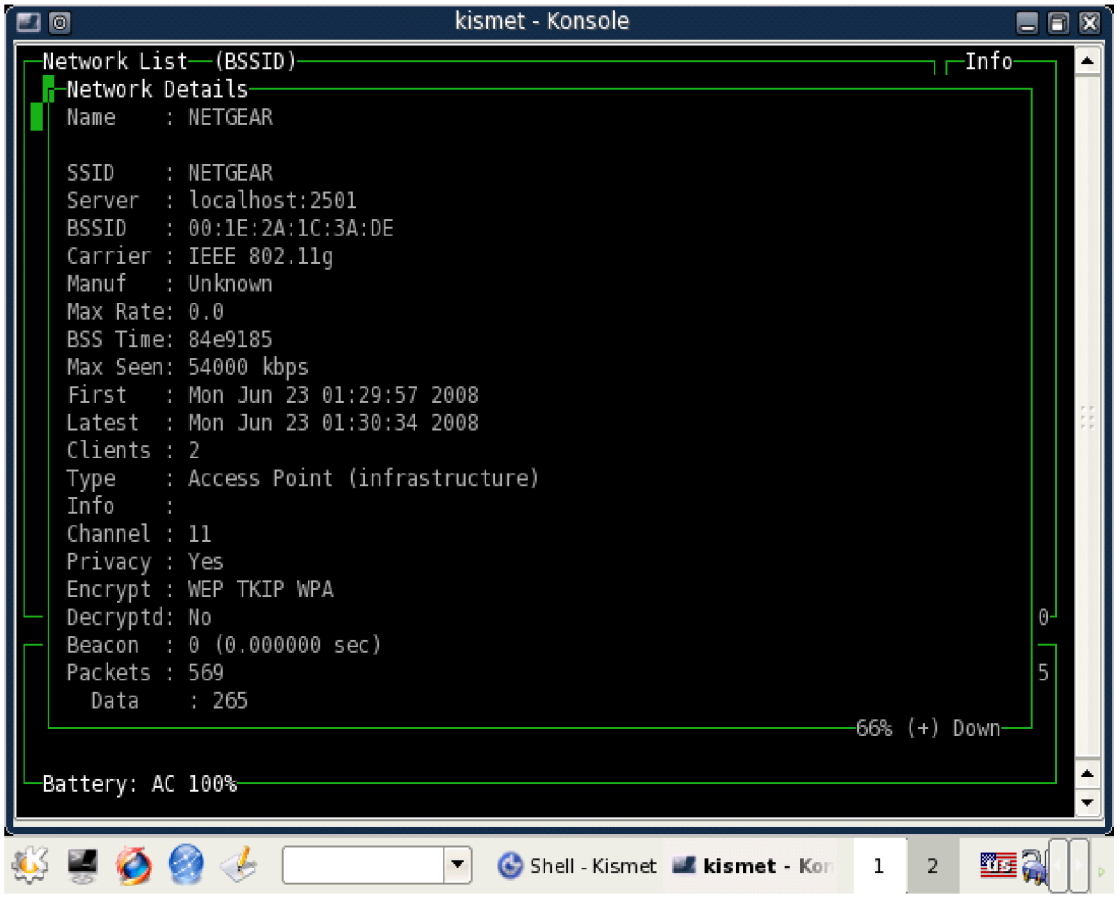


Εικόνα 4.3 Εκκίνηση του Kismet.

Όπως φαίνεται και από την εικόνα 4.4 έχουν εντοπιστεί 3 A.P. και μαζί με αυτά και το δικό μας που χρησιμοποιείται στην επίδειξη. Η εικόνα 4.5 δείχνει μια πιο λεπτομερής ανάλυση για το Access Point.



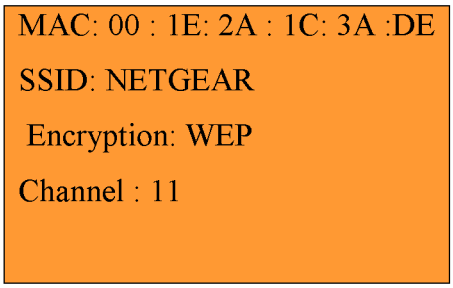
Εικόνα 4.4 Access Points με την βοήθεια του Kismet



Εικόνα 4.5 Κάρτα λεπτομερειών για το A.P. από το Kismet

Με το που ανοίξει το Kismet αυτομάτως η ασύρματη κάρτα μας μπαίνει σε monitor mode. Εκτός του Kismet ο άλλος τρόπος για να βάλλουμε την κάρτα μας σε monitor mode είναι με το airmon. Το Kismet μας δίνει τις αρχικές πληροφορίες που χρειαζόμαστε για το εν επίθεση Access Point. Οι πληροφορίες που παίρνουμε αφορούν την MAC διεύθυνση του, το SSID όνομα του, αν χρησιμοποιεί κάποιου είδους κρυπτογράφησης και το κανάλι που χρησιμοποιεί για να εκπέμψει.

Στην παρακάτω εικόνα φαίνονται τα χαρακτηριστικά του AP που μας ενδιαφέρει για να συνδεθούμε.



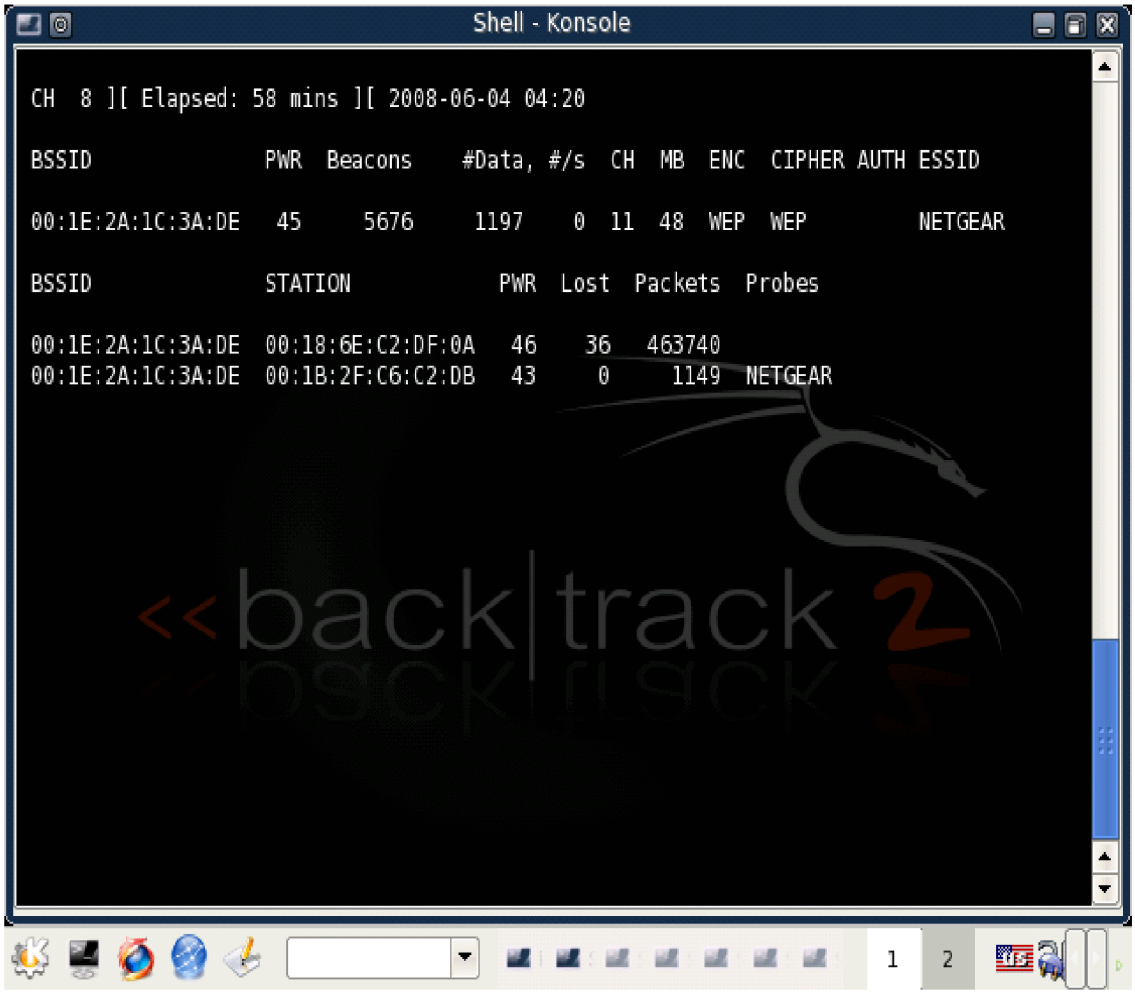
Εικόνα 4.6 Χαρακτηριστικά Α.Ρ.

Αφού συλλέξουμε τις πρώτες κρίσιμες πληροφορίες το επόμενο βήμα είναι να αρχίσουμε να καταγράφουμε τα IV's από το access point. Αυτό το καταφέρνουμε χρησιμοποιώντας το πρόγραμμα airdump. Ανοίγοντας ένα άλλο terminal και πληκτρολογώντας την παρακάτω εντολή:

```
airodump-ng -c  11 --ivs –w /root/Desktop/WEPIVS ath1
```

Όπου

- ath1: Η ασύρματη κάρτα μας
- –w: Λέει στο airdump να γράψει το αρχείο
- /root/Desktop/WEPIVS: Το path που θα αποθηκευτεί το capturing
- 11: Το κανάλι που εκπέμπει ο router.



Εικόνα 4.7 Αποτελέσματα του προγράμματος airodump

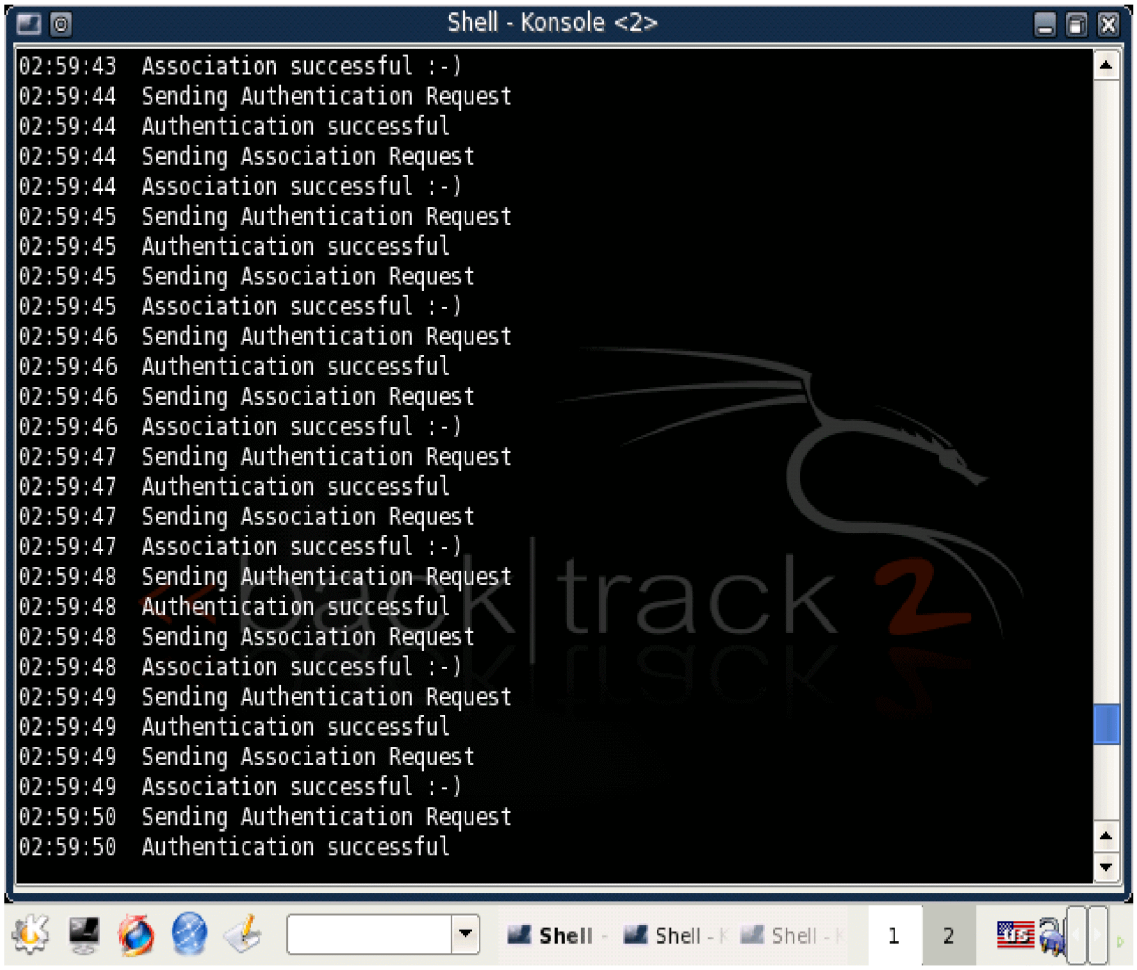
Το επόμενο βήμα είναι να πραγματοποιήσουμε σύνδεση χωρίς authentication με το Access Point (Fake authentication) παράλληλα με το airodump. Αυτό το επιτυγχάνουμε χρησιμοποιώντας το εργαλείο airplay. Ανοίγουμε πάλι καινούργιο terminal και πληκτρολογούμε την εντολή:

```
aireplay -1 -30 -e NETGEAR –a  001E2A1C3ADE -h 00:18:6E:C2:DF:0A ath1
```

Όπου

- -1: Το είδος της επίθεσης που θέλουμε να κάνουμε , στην περίπτωση αυτή Fake authentication
- 30: Προσδιορίζει το χρόνο μεταξύ των επιθέσεων
- -e: Το όνομα του essid στην περίπτωση αυτή είναι NETGEAR

- 001E2A1C3ADE: Η διεύθυνση MAC του Access Point
- -h 00:18:6E:C2:DF:0A: Η διεύθυνση MAC του client
- ath1: Το όνομα της ασύρματης κάρτας στο Linux



Εικόνα 4.8 Αποτέλεσμα επίθεσης Fake authentication

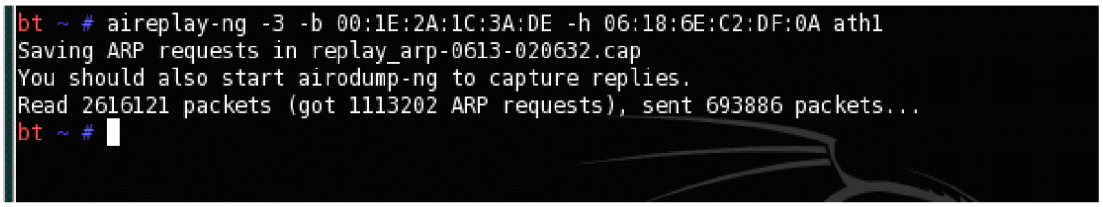
Στην συνέχεια ξεκινούμε το packet injection στο Access Point για να καταφέρουμε να μαζέψουμε όσο το δυνατόν πιο πολλά IV's, η διαδικασία αυτή είναι αδύνατον να επιτευχθεί χωρίς να έχει γίνει το προηγούμενο βήμα. Κατά το packet injection πετυχαίνουμε την λεγόμενη ARP request replay attack. Αυτή η επίθεση είναι ο πιο αποτελεσματικός τρόπος να δημιουργηθούν νέα IV's. Το πρόγραμμα "ακούει" για ARP πακέτα και τα επαναμεταδίδει πίσω στο Access Point. Το Access Point επαναμεταδίδει τα πακέτα με διαφορετικά IV's. Αυτή η διαδικασία επαναλαμβάνεται συνέχεια με αποτέλεσμα να μαζεύουμε όλο και περισσότερα IV's σε λιγότερο πολύ

λιγότερο χρόνο από τον οποίο θα απαιτούνταν. Η τεχνική αυτή είναι χρήσιμη για την επίθεση σε Access Points με σχετικά μικρή κίνηση. Την διαδικασία αυτή την επιτυγχάνουμε χρησιμοποιώντας πάλι το aireplay. Ανοίγουμε ένα καινούριο terminal και πληκτρολογούμε την παρακάτω εντολή.

```
aireplay -3 -b 00:1E:2A:1C:3A:DE -h  00:18:6E:C2:DF:0A  ath1
```

Όπου

- -3: Το είδος της επίθεσης , στην περίπτωση αυτή ARP request replay attack
- -b 001E2A1C3ADE: Η MAC διεύθυνση του Access Point
- h 00:18:6E:C2:DF:0A Η MAC διεύθυνση του client
- -x 1024 : Αριθμός πακέτων ανά δευτερόλεπτο
- ath1: Το interface της ασύρματης κάρτας



Εικόνα 4.9 Αποτέλεσμα επίθεσης ARP request replay attack

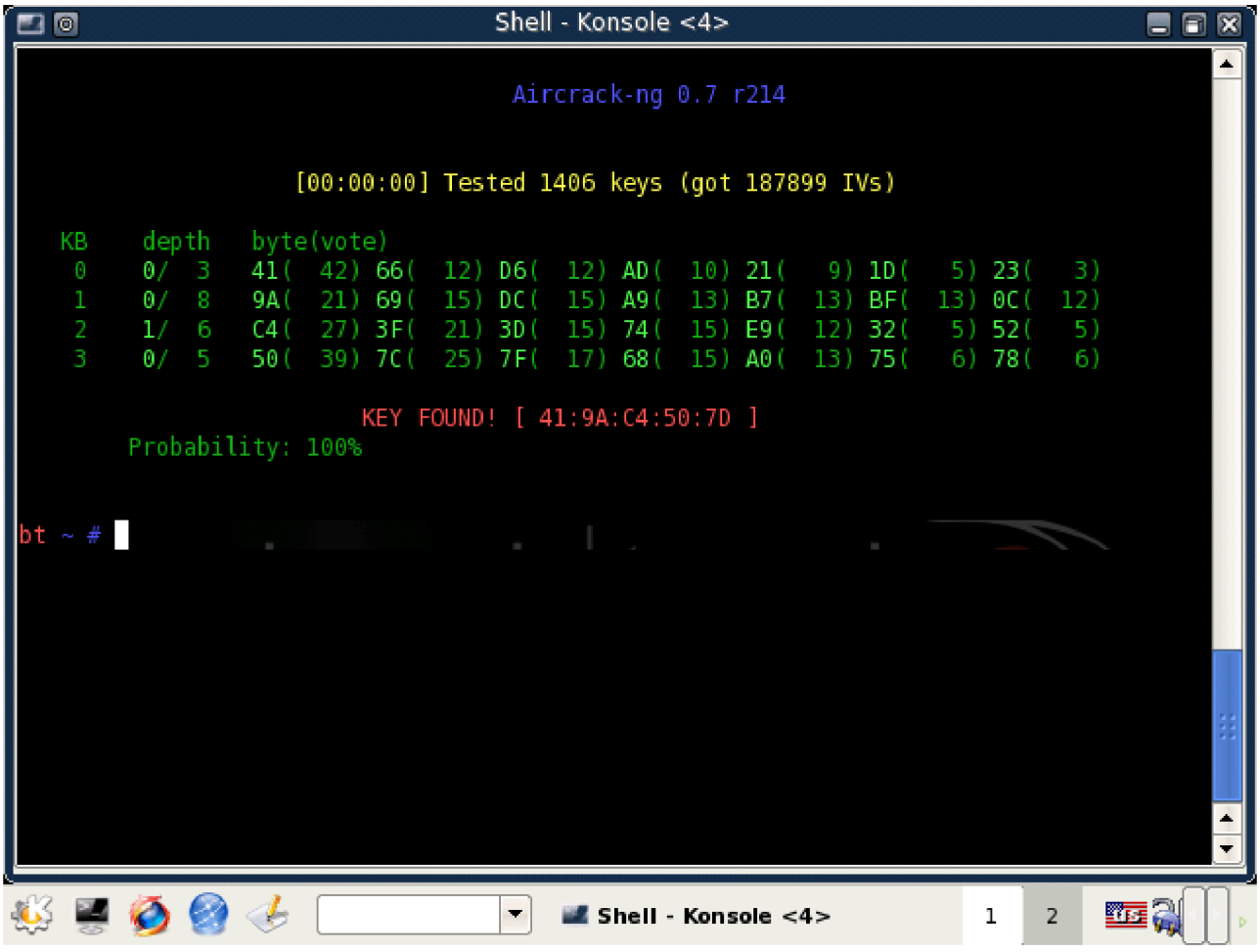
Το τελευταίο βήμα περιλαμβάνει την εύρεση του WEP κλειδιού, αυτό επιτυγχάνεται με την χρησιμοποίηση του προγράμματος aircrack. Αφού έχουμε μαζέψει αρκετά IV's κλείνουμε το airodump, βρίσκουμε που έχουμε αποθηκεύσει το αρχείο .ivs (WEPIVS-01.ivs) , ανοίγουμε ένα καινούργιο terminal και πληκτρολογούμε την εντολή:

```
aircrack-ng -0 -n -64 –f 17 /root/Desktop/WEPIVS-01.ivs
```

Όπου

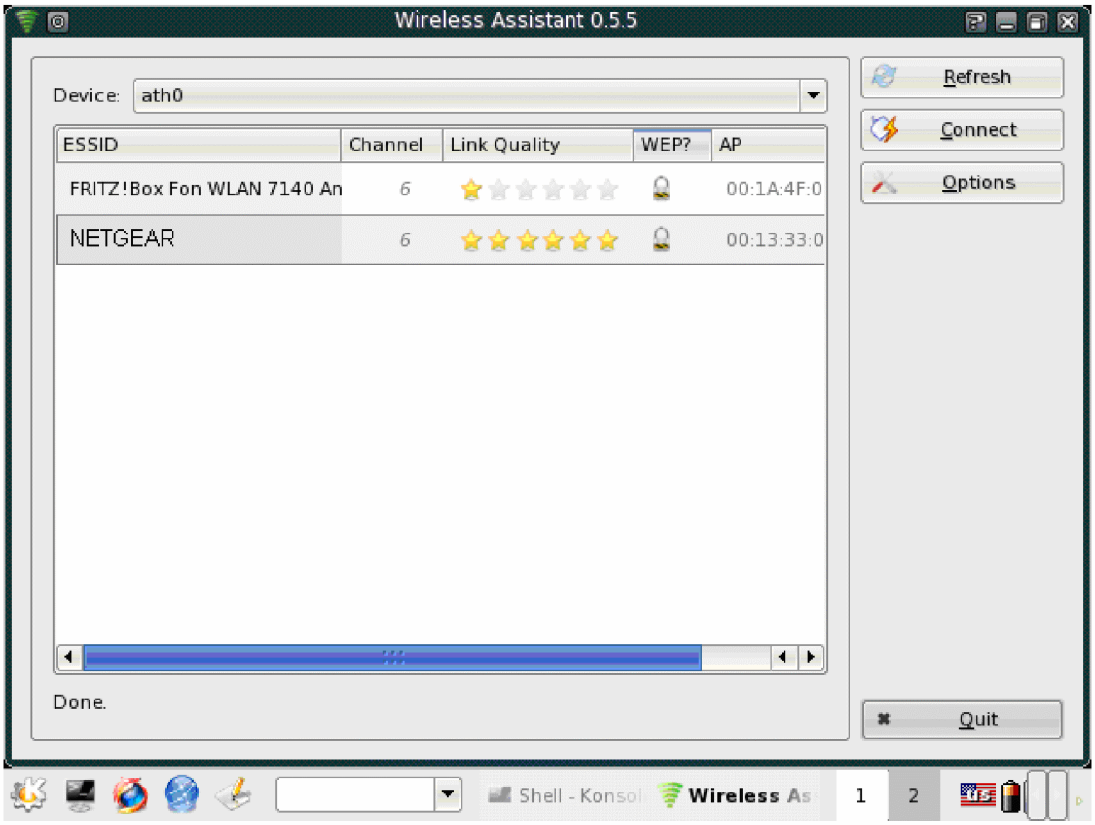
- -0:
- -n -64: Το μέγεθος του encryption

- –f 17: Brute fudge factor, στατιστική μεταβλητή
- /root/Desktop/WEPIVS-01.ivs: Το path του αρχείου που έχει κάνει capturing.

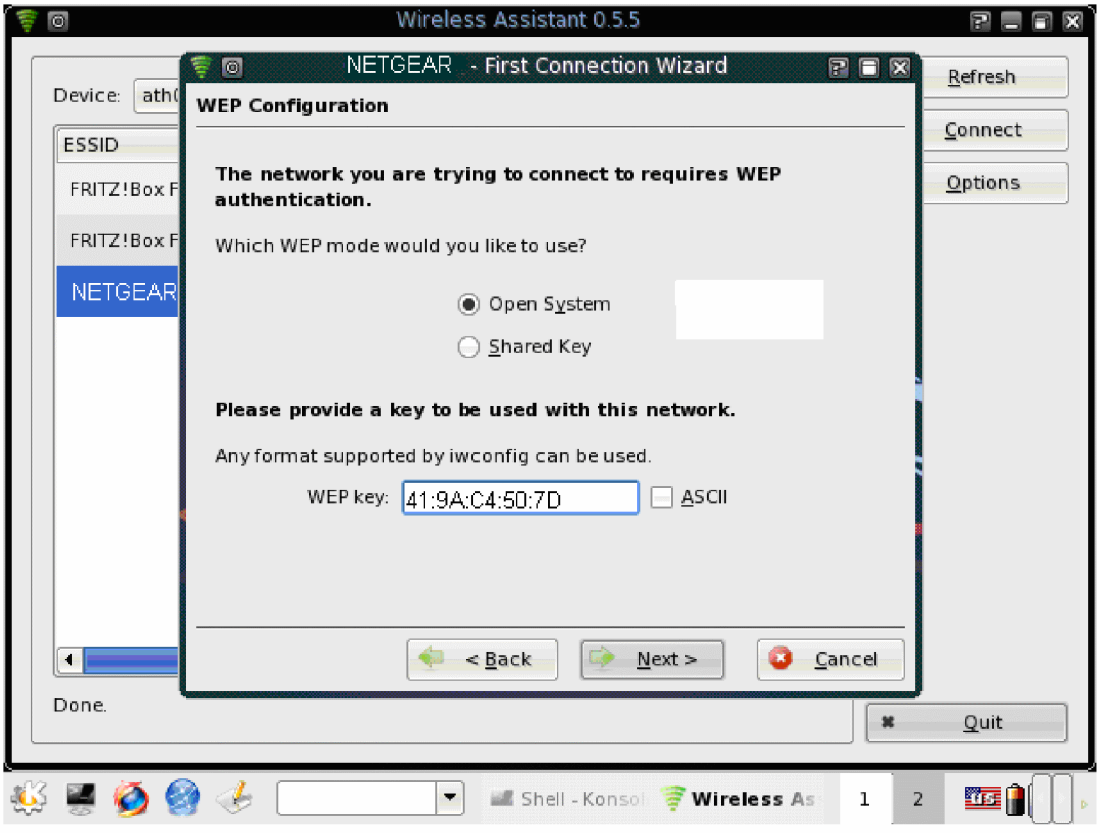


Εικόνα 4.10 Αποτελέσματα του προγράμματος aircrack, εύρεση του WEP key

Μετά την εύρεση του κλειδιού WEP η είσοδος στο δίκτυο είναι πια πολύ εύκολη, είτε κλείνουμε το BackTrack και εισερχόμαστε στα Windows και συνδεόμαστε όπως έχουμε προαναφέρει είτε μπορούμε να χρησιμοποιήσουμε το tool Wireless Assistant 0.5.5, οι παρακάτω δύο εικόνες δείχνουν την διαδικασία αυτή.

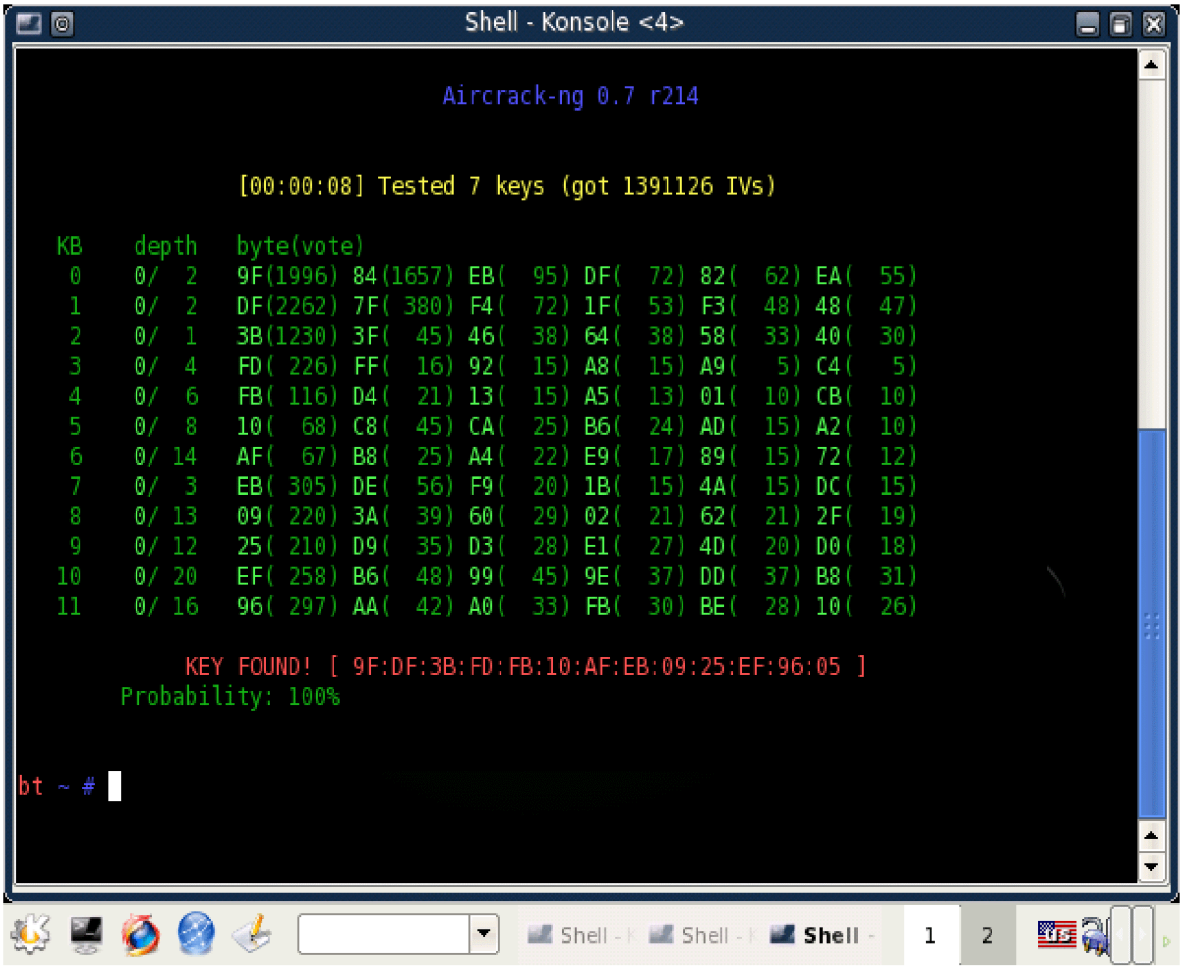


Εικόνα 4.11 Αρχική σελίδα του Wireless Assistant



Εικόνα 4.12 Είσοδος στο δίκτυο

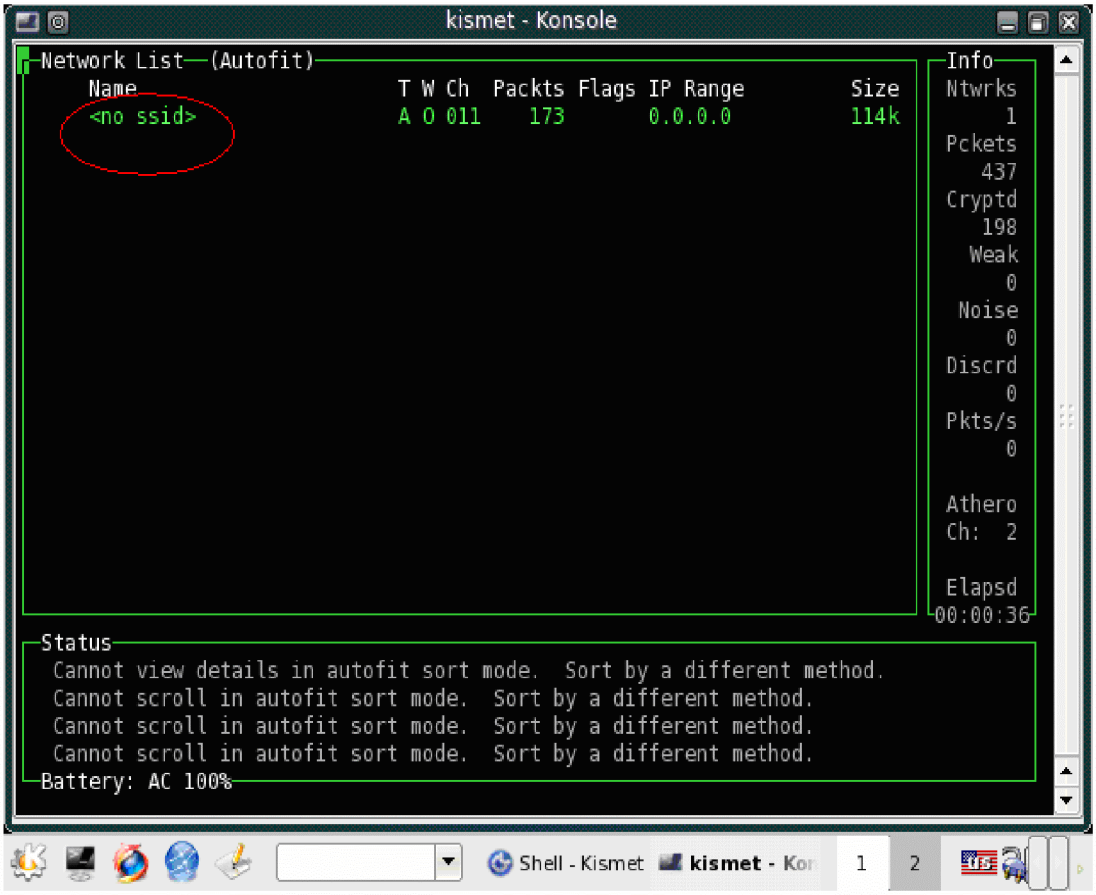
Η ίδια διαδικασία θα ακολουθηθεί σε περίπτωση που το WEP κλειδί με το ίδιο pass phrase είναι 128 bit. Το μόνο που θα αλλάξει είναι ο αριθμός των πακέτων που θα χρειαστούμε να μαζέψουμε με το airodump . Το WEP κλειδί θα το βρούμε και αυτή την φορά με την βοήθεια του aircrack (εικόνα 4.13)



Εικόνα 4.13 Αποτελέσματα του προγράμματος aircrack, εύρεση του WEP key (128 bit)

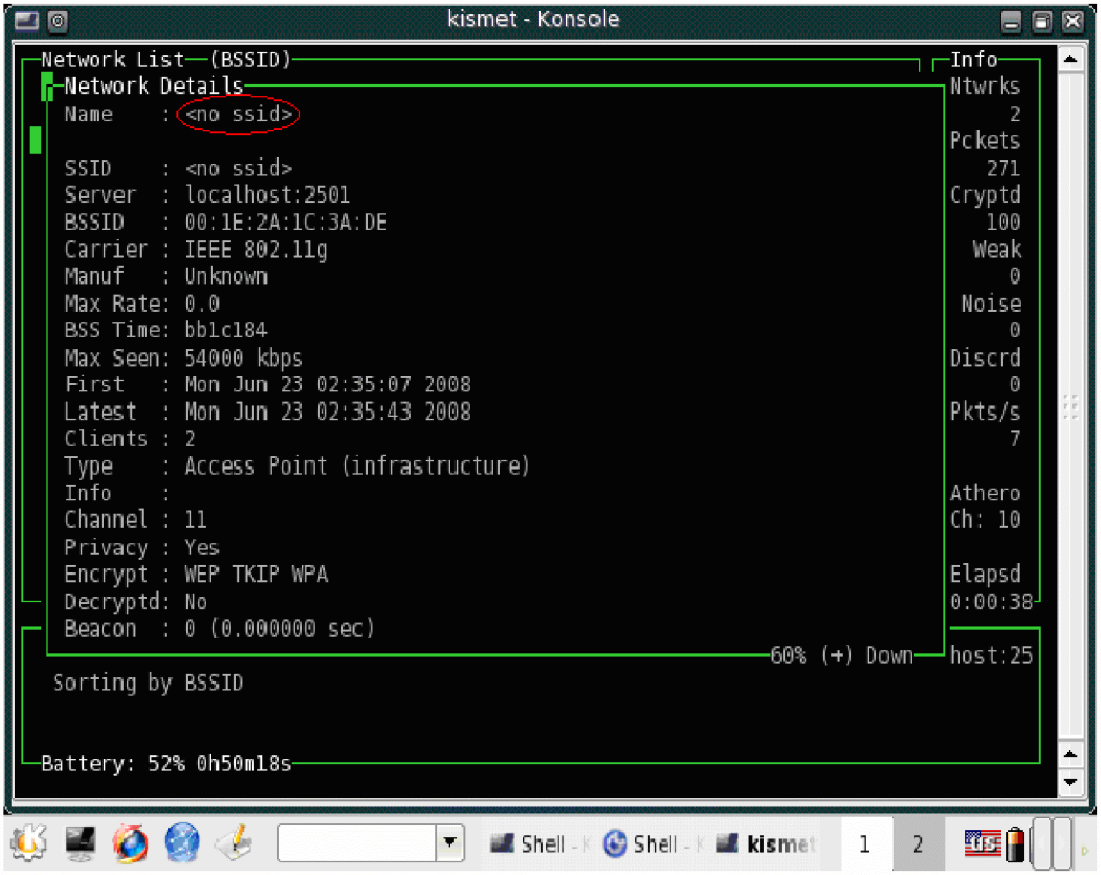
4.1.2 Απόκρυψη του SSID

Η υπερκέραση και αυτού του εμποδίου σε περιβάλλον Linux είναι αρκετά εύκολη διαδικασία. Τα αποτέλεσμα της απόκρυψης του SSID φαίνεται στην παρακάτω εικόνα , όταν πάμε να σκανάρουμε με το Kismet μία περιοχή και βλέπουμε ότι για το Access Point που μας ενδιαφέρει δεν παίρνουμε την πληροφορία του SSID.



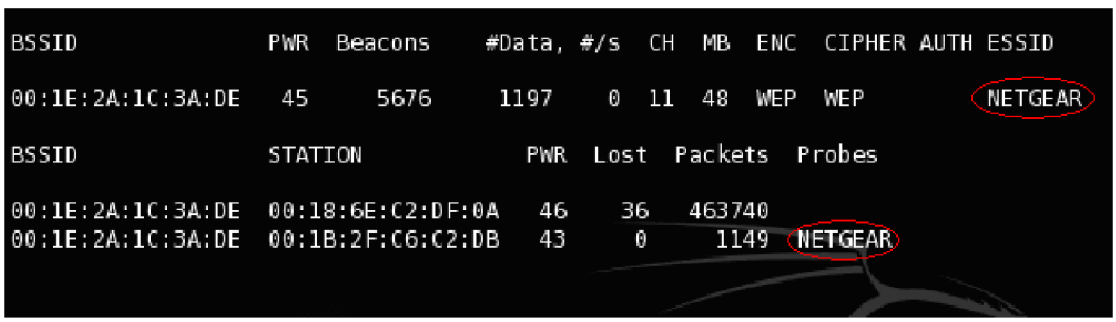
Εικόνα 4.14 Αποτέλεσμα απόκρυφης του SSID στο Kismet.

Την πληροφορία του SSID αδυνατούμε να την πάρουμε ακόμα και από την πιο λεπτομερή κάρτα που διαθέτει το Kismet (εικόνα 4.15).



Εικόνα 4.15 Αποτέλεσμα απόκρυφης του SSID

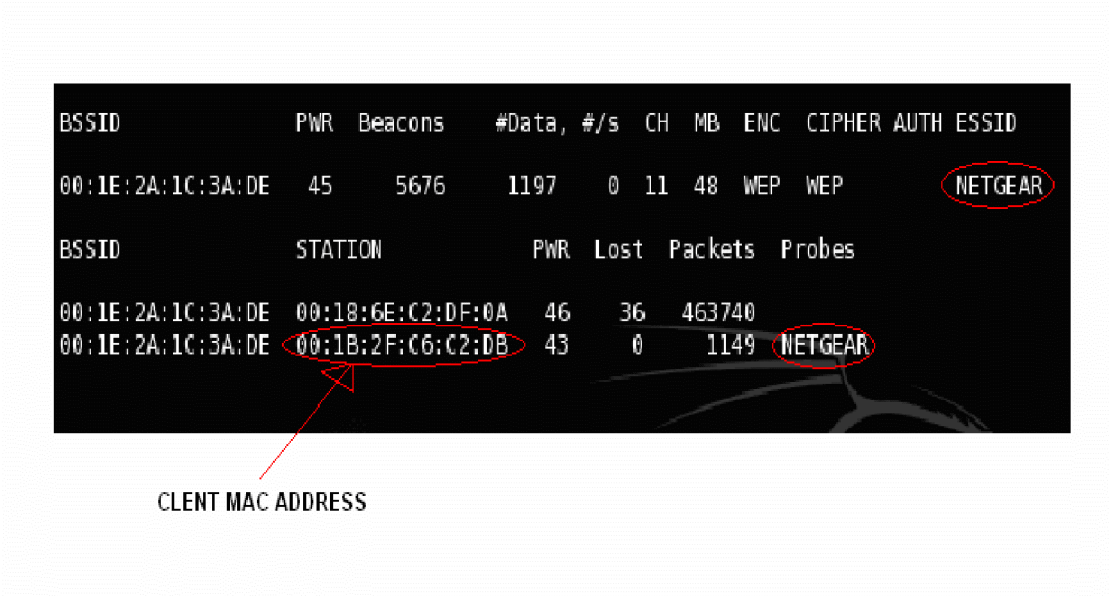
Η εύρεση του SSID μπορεί να γίνει παρακολουθώντας το Access Point έως ότου ένας κανονικός σταθμός συνδεθεί στο δίκτυο. Όπως έχουμε προαναφέρει για την σύνδεση ενός client στο Access Point το SSID πρέπει να γίνει broadcast . Όταν ένας σταθμός γίνει associated με το Access Point χρησιμοποιούμε το Airodump για την εύρεση του SSID (εικόνα 4.16).



Εικόνα 4.16 Εύρεση κρυμμένου SSID

4.1.3 Ρύθμιση αυθεντικοποίησης με την χρήση MAC διευθύνσεων (MAC Filtering)

Η παράκαμψη αυτής της τεχνικής ασφαλείας γίνεται σε περιβάλλον Linux με την ίδια μέθοδο όπως και σε περιβάλλον Windows. Αυτό που κάνουμε είναι να περιμένουμε να γίνει associated στο Access Point κάποιος client ο οποίος έχει μία γνωστή και νόμιμη MAC διεύθυνση, στην συνέχεια με την χρήση του εργαλείου airodump βρίσκουμε την MAC διεύθυνση του client και περιμένουμε μέχρι να αποσυνδεθεί.



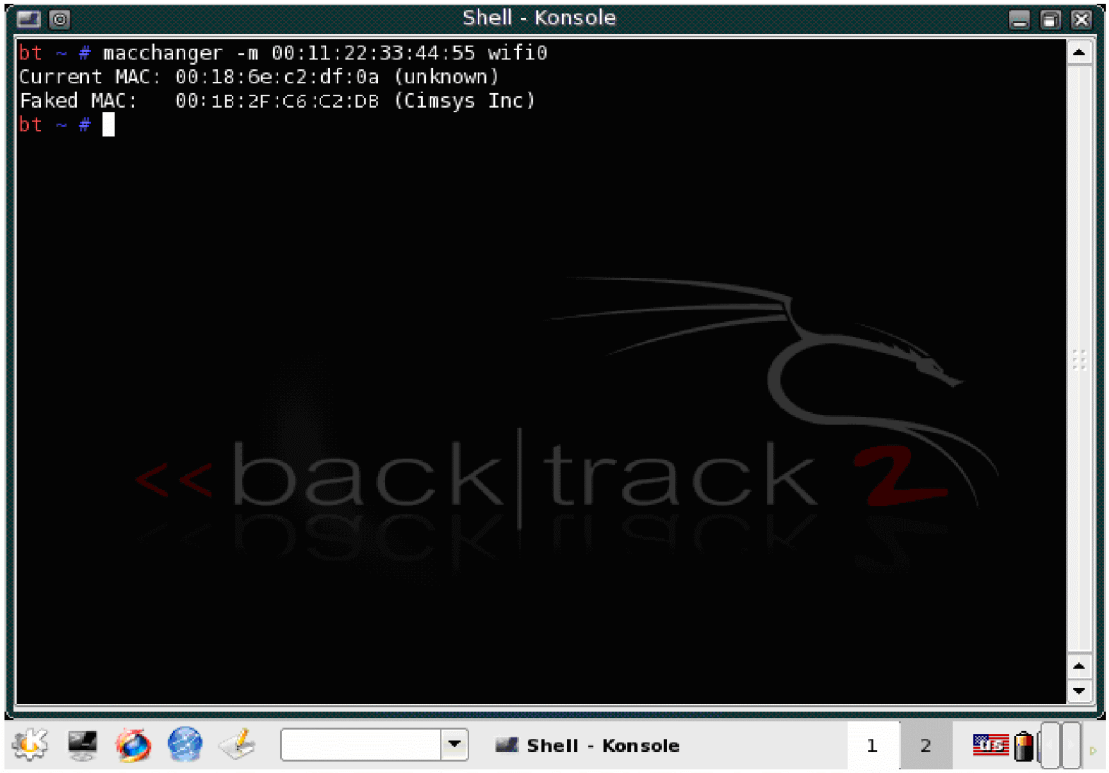
Εικόνα 4.17 Εύρεση ενός έμπιστου client που επικοινωνεί με το access Point

Εάν κάποιος client με μη εξουσιοδοτημένη MAC διεύθυνση προσπαθήσει να συνδεθεί στο Access Point θα λάβει ένα μήνυμα άρνησης (εικόνα 4.18)

```
13:45:00  Sending Authentication Request
13:45:00  AP rejects the source MAC address ?
13:45:00  Authentication failed (code 1)
```

Εικόνα 4.18 Μήνυμα άρνησης

Για να συνδεθεί ο επιτιθέμενος στο Access Point θα πρέπει αρχικά να αλλάξει την MAC διεύθυνση της ασύρματης κάρτας του. Αυτό επιτυγχάνεται με την χρησιμοποίηση του εργαλείου macchanger. Στην παρακάτω εικόνα φαίνεται η διαδικασία αλλαγής της MAC διεύθυνσης της ασύρματης κάρτας.



Εικόνα 4.19 Αλλαγή MAC διεύθυνσης της ασύρματης κάρτας

Αφού γίνει η αλλαγή της MAC address ο επιτιθέμενος σταθμός μπορεί να εισέλθει στο δίκτυο με την προϋπόθεση βέβαια ότι ο κανονικός client δεν είναι συνδεδεμένος.

4.1.4 Εύρεση WPA-PSK κλειδιού

Το WPA- PSK αν και πιο σύγχρονο της τεχνολογίας WEP μπορεί να παραβιαστεί και αυτό από έναν κακόβουλο χρήστη. Στην κατάσταση λειτουργίας PSK τόσο η αυθεντικοποίηση όσο και η δημιουργία κλειδιών βασίζεται στην γνώση μιας κοινά γνωστής μυστικής λέξης. Αφού κάνουμε τις ανάλογες ρυθμίσεις στον Router χρησιμοποιώντας την ίδια λέξη κλειδί όπως και στα Windows.

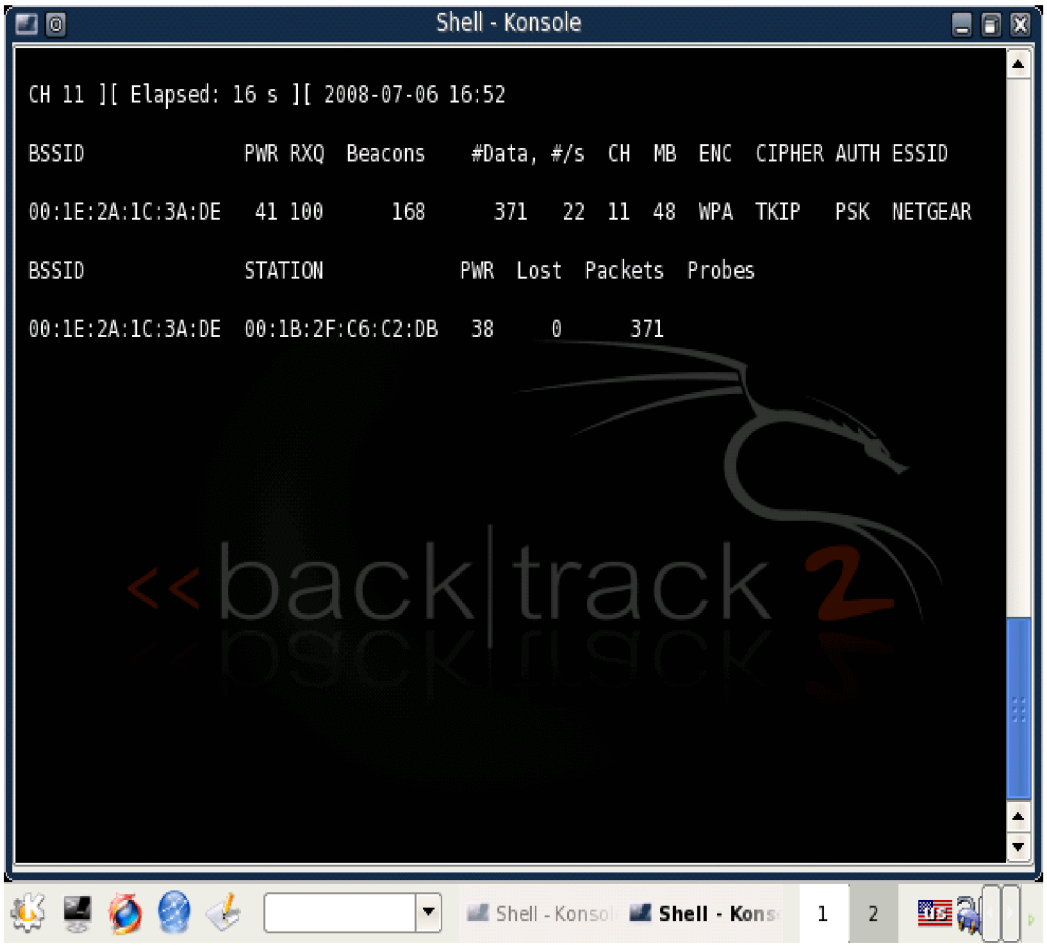
Για να βρούμε το κλειδί πραγματοποιείται μια τεχνική η οποία ονομάζεται επίθεση λεξικού (dictionary attack), για την επιτυχή έκβασή της χρειαζόμαστε το SSID του δικτύου και τα τέσσερα μηνύματα της «χειραψίας» μεταξύ του client και του Router και ένα αρχείο που περιέχει συνήθεις λέξεις που χρησιμοποιούνται για την δημιουργία των κλειδιών. Τα αρχεία που χρησιμοποιήθηκαν στην επίδειξη βρίσκονται στην διεύθυνση http://www.leetupload.com/dbindex2/index.php?dir=Word%20Lists/ Κατά την επίθεση αυτή ο επιτιθέμενος δεν χρειάζεται να είναι συνδεδεμένος στο Access Point που επιτίθεται , εν αντιθέσει με την περίπτωση του WEP κατά την οποία χρειάζεται να λαμβάνει δεδομένα και πληροφορίες συνεχώς από το Access Point. Τα προγράμματα που χρησιμοποιήθηκαν είναι τα ίδια όπως και στην περίπτωση εύρεσης του WEP κλειδιού.

Αρχικά χρησιμοποιούμε το airodump για να ξεκινήσουμε το capturing, ανοίγουμε ένα καινούριο shell και πληκτρολογούμε την παρακάτω εντολή:

```
airodump-ng -c 11 ath1 -w /root/Desktop/WPA
```

Όπου

- –w: Λέει στο airdump να γράψει το αρχείο
- /root/Desktop/**WPA**: Το path που θα αποθηκευτεί το capturing
- 11: Το κανάλι που εκπέμπει ο router.
- ath1: Το όνομα της ασύρματης κάρτας στο linux
- **-c:** Διευκρινίζει το κανάλι που εκπέμπει το AP για να μην αναγκάζεται το airodump να αναπηδά ανάμεσα στα κανάλια όταν κάνει capturing.



Εικόνα 4.20 Αποτελέσματα του προγράμματος airodump

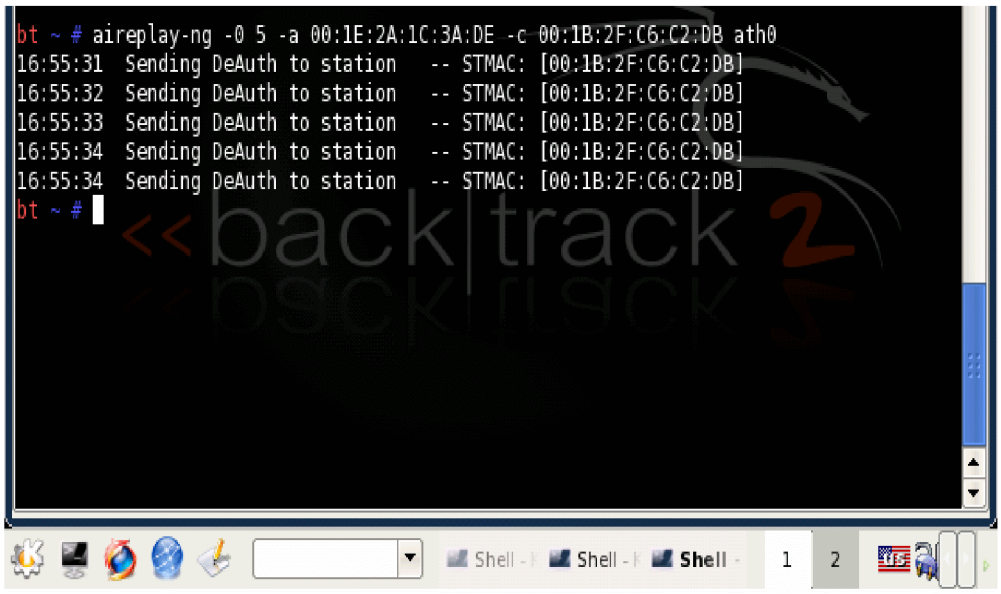
Παράλληλα στην συνέχεια ανοίγουμε ένα καινούριο terminal και χρησιμοποιούμε το aireplay πληκτρολογώντας την εντολή:

```
aireplay-ng -0 5 -a 00:1E:2A:1C:3A:DE -c 00:18:6E:C2:DF:0A ath0
```

Όπου

- -0: Το είδος της επίθεσης που θέλουμε να κάνουμε , στην περίπτωση αυτή Deauthentication
- 5: Προσδιορίζει το χρόνο μεταξύ των επιθέσεων
- -a 001E2A1C3ADE: Η διεύθυνση MAC του Access Point
- -c 00:18:6E:C2:DF:0A: Η διεύθυνση MAC του client

- ath0: Το όνομα της ασύρματης κάρτας στο Linux



Εικόνα 4.21 Αποτέλεσμα aireplay

Σε αυτό το σημείο σταματάμε το capturing αφού έχουμε πάρει τις πληροφορίες που θέλαμε. Οπότε σταματάμε το airodump με την εντολή:

```
airodump-ng -c 11 ath1 -w /root/Desktop/WPA
```

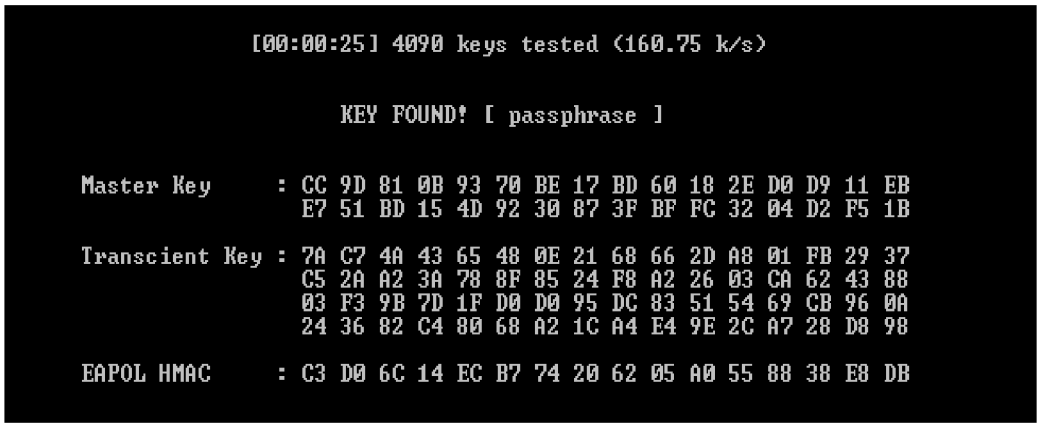
Στην συνέχεια ανοίγουμε ένα καινούριο terminal και κάνουμε χρήση τα captured αρχεία και το wordlist που έχουμε με το aircrack , πληκτρολογούμε την εντολή:

```
aircrack-ng -w /root/Desktop/pass.txt/root/Desktop/WPA.cap
```

Όπου

- **-w**: words – Το path για το αρχείο με τα password και το path με τα captured αρχεία.

Το αποτέλεσμα της εντολής αυτής φαίνεται στην παρακάτω εικόνα.



Εικόνα 4.22 Εύρεση WPA φράσης

5.1 ΜΕΤΡΙΑΣΗ ΤΩΝ ΚΙΝΔΥΝΩΝ

Οι συνέπειες των επιθέσεων που αναφέρθηκαν στην προηγούμενη παράγραφο είναι καθοριστικές για τα 802.11 WLANs διότι επηρεάζουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριών. Για τον λόγο αυτόν, έχουν παρθεί κάποια αντίμετρα για την μετρίαση των κινδύνων και των ευπαθειών. Τα αντίμετρα διαχείρισης, σε συνδυασμό με τα λειτουργικά και τεχνικά αντίμετρα, μπορούν να μειώσουν αποτελεσματικά τους κινδύνους που σχετίζονται με τα WLANs.

Οι παρακάτω οδηγίες δεν εξαλείφουν ολοκληρωτικά τους κινδύνους σε ένα τέτοιο σύστημα, δίνουν όμως τις κατευθυντήριες γραμμές για την μετρίαση και την εξάλειψη πολλών, αν όχι όλων, από τους κινδύνους αυτούς. Θα πρέπει επίσης να σημειωθεί ότι δεν υπάρχει κανένα συγκεκριμένο σύνολο οδηγιών το οποίο να μπορεί να ταιριάξει στις ανάγκες όλων των συστημάτων όταν έχουμε να κάνουμε με θέματα ασφάλειας.

5.2 Αντίμετρα Διαχείρισης

Τα αντίμετρα διαχείρισης ξεκινούν με μία περιεκτική πολιτική, ώστε να εξασφαλίσουν την ασφάλεια σε ένα ασύρματο δίκτυο. Στην πολιτική αυτή θα στηριχτεί η λογική και υλοποίηση και των άλλων αντιμέτρων, των λειτουργικών και των τεχνικών. Μία πολιτική ασφάλειας θα πρέπει, λοιπόν, να εφαρμόζει τα ακόλουθα [1]:

- Αναγνώριση του ποιος θα χρησιμοποιεί την τεχνολογία WLAN σε έναν οργανισμό.
- Αναγνώριση του αν απαιτείται πρόσβαση στο Internet.
- Περιγραφή του ποιος θα εγκαθιστά σημεία πρόσβασης και άλλον ασύρματο εξοπλισμό.
- Εξασφάλιση περιορισμών όσον αφορά την τοποθεσία και τη φυσική ασφάλεια των σημείων πρόσβασης.
- Περιγραφή του τύπου των πληροφοριών που μπορούν να μεταδίδονται μέσω της ασύρματης ζεύξης.
- Περιγραφή των συνθηκών, σύμφωνα με τις οποίες θα επιτρέπονται ασύρματες συσκευές.
- Καθορισμός συγκεκριμένων ρυθμίσεων ασφαλείας για τα σημεία πρόσβασης.
- Καθορισμός περιορισμών, σύμφωνα με τους οποίους θα χρησιμοποιείται η ασύρματη συσκευή.
- Περιγραφή των ρυθμίσεων υλικού (hardware) και λογισμικού (software) για όλες τις ασύρματες συσκευές.
- Παροχή οδηγιών για την αναφορά απωλειών όσον αφορά τις ασύρματες συσκευές, την προστασία ασύρματων πελατών, την χρήση κρυπτογράφησης και διαχείρισης κλειδιών, και τα περιστατικά ασφάλειας.
- Καθορισμός της συχνότητας και του εύρους των εκτιμήσεων ασφάλειας, ώστε να περιλαμβάνουν την εύρεση όλων των σημείων πρόσβασης

5.2.1 Λειτουργικά Αντίμετρα

Η φυσική ασφάλεια είναι το πιο θεμελιώδες βήμα για την εξασφάλιση της πρόσβασης μόνο εξουσιοδοτημένων χρηστών στον ασύρματο εξοπλισμό. Η φυσική ασφάλεια

συνδυάζει τον έλεγχο πρόσβασης, την αυθεντικοποίηση χρηστών, και την εξωτερική περιοριστική προστασία.

Πολύ σημαντική είναι η γνώση της ακτίνας που καλύπτει ένα σημείο πρόσβασης, ώστε αυτή να μην ξεπερνά το χώρο των εγκαταστάσεων του δικτύου. Αν κάτι τέτοιο συμβεί (δηλαδή η εμβέλεια ενός σημείου πρόσβασης καλύπτει και χώρο εκτός των εγκαταστάσεων), τότε κάποιος μπορεί να το εκμεταλλευτεί για να κερδίσει πρόσβαση στο δίκτυο. Για να αποφευχθεί, λοιπόν, μια τέτοια ευπάθεια, κάποια σημεία πρόσβασης έχουν ειδικές λειτουργίες που ρυθμίζουν την ισχύ του σήματος τους, ώστε να ρυθμίζεται η ακτίνα κάλυψης τους σύμφωνα με τις ανάγκες σε κάθε περίπτωση.

5.2.2 Τεχνικά Αντίμετρα

Τα τεχνικά αντίμετρα περιλαμβάνουν λύσεις λογισμικού και υλικού που βοηθούν στην ασφάλεια του ασύρματου περιβάλλοντος.

5.2.3 Λύσεις Λογισμικού

Οι λύσεις λογισμικού συμπεριλαμβάνουν την ρύθμιση των σημείων πρόσβασης, την τακτική ενημέρωση του λογισμικού, την εκτέλεση κάποιων λεπτομερών εξετάσεων και την υιοθέτηση αποτελεσματικής κρυπτογράφησης.

5.2.3.1 Ρύθμιση των σημείων πρόσβασης

Οι διαχειριστές των δικτύων πρέπει να ρυθμίζουν τα σημεία πρόσβασης, σύμφωνα με τις πολιτικές ασφάλειας και τις απαιτήσεις του κάθε συστήματος. Οι ενέργειες που θα πρέπει να εκτελούν κάθε φορά είναι οι εξής [1]:

- **Αλλαγή των προκαθορισμένων συνθηματικών:** Κάθε συσκευή ασύρματου δικτύου έρχεται με τις προκαθορισμένες ρυθμίσεις της, μερικές από τις οποίες περιέχουν ευπάθειες ασφάλειας. Για παράδειγμα σε μερικά σημεία πρόσβασης δεν απαιτείται password (το πεδίο του password είναι κενό). Ο ρόλος ενός διαχειριστή είναι να αντικαθιστά την ρύθμιση αυτή με ένα "δυνατό" συνθηματικό (ένα τέτοιο συνθηματικό αποτελείται από 8 χαρακτήρες και άνω, και απαρτίζεται από έναν συνδυασμό γραμμάτων, αριθμών, ειδικών χαρακτήρων, κ.τ.λ.). Εάν οι απαιτήσεις ασφάλειας είναι ιδιαίτερα υψηλές, θα μπορούσε να χρησιμοποιηθεί μια γεννήτρια τυχαίων συνθηματικών.

- **Καθορισμός κατάλληλων κρυπτογραφικών ρυθμίσεων:** Οι ρυθμίσεις αυτές θα πρέπει να επιτρέπουν τη μέγιστη δυνατή κρυπτογράφηση που υποστηρίζει το προϊόν, και να εξαρτώνται από τις απαιτήσεις ασφάλειας του οργανισμού. Τυπικά, τα σημεία πρόσβασης έχουν μόνο μερικές κρυπτογραφικές ρυθμίσεις διαθέσιμες: είτε καμία, είτε κάποιο κοινό κλειδί μήκους 40 bits είτε κάποιο κοινό κλειδί μήκους 104 bits, με αυτή την κρυπτογράφηση να είναι η δυνατότερη. Η κρυπτογράφηση WEP, δεν παρουσιάζει προβλήματα απόδοσης στους υπολογιστές που πραγματοποιούν αυτή τη λειτουργία. Θα πρέπει όμως να αναφερθεί ότι προϊόντα που χρησιμοποιούν κλειδιά μήκους 128 bits δεν είναι εφικτό να λειτουργούν με εκείνα που χρησιμοποιούν κλειδιά μήκους 104 bits.
- **Έλεγχος της επαναφοράς των λειτουργιών:** Αυτή η λειτουργία θέτει ένα σοβαρό πρόβλημα ασφάλειας, διότι επιτρέπει σε έναν κακόβουλο χρήστη να ακυρώσει τις ρυθμίσεις που έχουν γίνει από τους διαχειριστές του σημείου πρόσβασης, επιστρέφοντας το σημείο πρόσβασης στις αρχικές του ρυθμίσεις, οι οποίες μπορεί να είναι, για παράδειγμα, χωρίς κρυπτογράφηση ή χωρίς password κ.τ.λ. Η επαναφορά των αρχικών ρυθμίσεων του σημείου πρόσβασης μπορεί να επιτευχθεί με την τοποθέτηση και πίεση ενός αιχμηρού αντικειμένου στην τρύπα που χρησιμεύει για την λειτουργία αυτή. Κάτι τέτοιο θα μπορούσε να προκαλέσει ακόμα και την άρνηση εξυπηρέτησης, γιατί τα σημεία πρόσβασης μπορεί να τεθούν εκτός λειτουργίας, αφού στην περίπτωση της επαναφοράς μπορεί να χαθούν πληροφορίες όπως IP διευθύνσεις ή κλειδιά. Επομένως, για να αποφευχθούν τέτοιες ενέργειες από κακόβουλους χρήστες, τα σημεία πρόσβασης χρειάζονται φυσική προστασία.
- **Χρήση λιστών ελέγχου πρόσβασης με MAC διευθύνσεις:** Όπως γνωρίζουμε, μια MAC διεύθυνση είναι μια διεύθυνση υλικού που αναγνωρίζει μοναδικά κάθε υπολογιστή σε ένα δίκτυο. Πολλά σημεία πρόσβασης παρέχουν τη δυνατότητα πρόσβασης στο δίκτυο, συσκευών με συγκεκριμένες MAC διευθύνσεις, μέσω λιστών (MAC Access Control Lists - ACLs) οι οποίες είναι αποθηκευμένες σε αυτά. Αυτή η μέθοδος όμως δεν είναι ασφαλής, γιατί η MAC διεύθυνση μεταδίδεται στο δίκτυο μη κρυπτογραφημένη και, κάποιος μπορεί να την χρησιμοποιήσει ώστε να αποκτήσει πρόσβαση στο δίκτυο. Επομένως, η λύση αυτή θα πρέπει να

χρησιμοποιείται σε συνδυασμό με άλλες και θα πρέπει μάλιστα να σημειωθεί ότι δεν προσφέρεται για μεσαίου και μεγάλου μεγέθους δίκτυα, εξ' αιτίας των πολλών συσκευών και της πολυπλοκότητας τους.

- **Αλλαγή του SSID:** Οι προκαθορισμένες ρυθμίσεις του SSID του σημείου πρόσβασης θα πρέπει να αλλάζουν, για την αποφυγή της εύκολης πρόσβασης. Αν και ένας καλά εξοπλισμένος αντίπαλος μπορεί να το βρει με διάφορους τρόπους, θα αποθαρρυνθούν με τον τρόπο αυτόν κακόβουλα άτομα με ελλιπείς γνώσεις. Μια επιπλέον τεχνική μέρος της διαδικασίας απόκρυψης του SSID είναι να χρησιμοποιούνται ψεύτικα access points. Με την χρησιμοποίηση του λογισμικού Fake AP από την Black Alchemy το οποίο δημιουργεί χιλιάδες ψεύτικα 802.11b access points τα οποία θα μπερδέψουν προγράμματα όπως το Netstumbler. Το Fake AP τρέχει σε Linux και χρειάζεται Perl 5.6 και πάνω. Για την περίπτωση που το λειτουργικό σύστημα που χρησιμοποιούμαι είναι Windows τότε ένα καλό πρόγραμμα που κάνει το ίδιο είναι το Honeyd το οποίο εκτός από την δημιουργία ψεύτικων access points, προσομοιώνει και πολλαπλά λειτουργικά συστήματα.

- **Μεγιστοποίηση του διαστήματος μεταξύ των ραδιοσημάτων:** Τα πλαίσια ραδιοσημάτων (beacon frames) ανακοινώνουν την ύπαρξη του ασύρματου δικτύου. Αυτά μεταδίδονται από τα σημεία πρόσβασης σε κανονικά διαστήματα και επιτρέπουν σε έναν ασύρματο πελάτη να ρυθμίσει τις παραμέτρους που απαιτούνται για την πρόσβαση του σε ένα ασύρματο δίκτυο. Ρυθμίζοντας το διάστημα στη μεγαλύτερη τιμή του (συνήθως 67 δευτερόλεπτα), γίνεται πιο δύσκολη η ακούσια ανίχνευση ενός ασύρματου δικτύου, εφόσον το σημείο πρόσβασης δεν εκπέμπει πλέον το ίδιο συχνά.
- **Αλλαγή των προκαθορισμένων κρυπτογραφικών κλειδιών:** Ο κατασκευαστής του σημείου πρόσβασης μπορεί να παρέχει ένα ή περισσότερα κλειδιά για shared-key αυθεντικοποίηση, μεταξύ μιας συσκευής που θέλει να αποκτήσει πρόσβαση στο δίκτυο και του σημείου πρόσβασης. Οι προκαθορισμένες τιμές πρέπει να αλλαχθούν, και μια καλή πολιτική είναι να αλλάζουν συχνά και ιδιαίτερα όταν συμβαίνουν αλλαγές προσωπικού στον οργανισμό.

- **Χρήση SNMP:** Εάν δεν απαιτείται η χρήση του SNMP σε ένα δίκτυο καλό είναι να απενεργοποιείται η λειτουργία του. Αν αυτό πρέπει να χρησιμοποιηθεί συνιστάται η χρήση της έκδοσης 3, SNMPv3, η οποία περιέχει μηχανισμούς που παρέχουν ενισχυμένη ασφάλεια, σε αντίθεση με τις προηγούμενες δύο εκδόσεις που παρέχουν ελαφρά αυθεντικοποίηση. Η προκαθορισμένη τιμή του community string που έχουν οι πράκτορες του SNMP είναι συνήθως **"public"** με δικαιώματα **"read"** ή **"read and write"**. Εάν ένας μη εξουσιοδοτημένος χρήστης αποκτήσει πρόσβαση στο σημείο πρόσβασης με δικαιώματα "read and write" θα μπορούσε να γράψει δεδομένα σε αυτό, προκαλώντας προβλήματα. Γι' αυτό, καλό είναι τα δικαιώματα να είναι σε τιμή **"read only"**, όπου και αν αυτό απαιτείται.
- **Αλλαγή του προκαθορισμένου καναλιού:** Οι κατασκευαστές χρησιμοποιούν συνήθως προκαθορισμένα κανάλια στα σημεία πρόσβασης, με αποτέλεσμα να υπάρξει η πιθανότητα παρεμβολής μεταξύ δύο σημείων πρόσβασης δύο διαφορετικών δικτύων που βρίσκονται σε κοντινές τοποθεσίες. Επειδή η παρεμβολή αυτή μπορεί να προκαλέσει άρνηση εξυπηρέτησης, οι διαχειριστές θα πρέπει να εξετάζουν εάν υπάρχουν τυχόν πηγές ραδιοπαρεμβολών, και να αποφασίζουν για την τοποθεσία και την ακτίνα κάλυψης των σημείων πρόσβασης, καθώς και για την ανάθεση των κατάλληλων ραδιοκαναλιών σε κάθε σημείο πρόσβασης.
- **Χρήση DHCP:** Ένας DHCP (Dynamic Host Control Protocol) server αναθέτει αυτόματα IP διευθύνσεις σε κάθε σταθμό εργασίας. Το πρόβλημα είναι ότι ένας κακόβουλος χρήστης με ένα φορητό υπολογιστή εξοπλισμένο με μια ασύρματη κάρτα, θα μπορούσε εύκολα να κερδίσει πρόσβαση στο δίκτυο, αφού ο DHCP server δε θα ξέρει απαραίτητα ποιες συσκευές έχουν πρόσβαση σε αυτό. Έτσι θα του ανέθετε μια έγκυρη IP διεύθυνση. Σε τέτοιες περιπτώσεις καλό θα ήταν να απενεργοποιηθεί το πρωτόκολλο DHCP και να χρησιμοποιηθούν στατικές διευθύνσεις στο ασύρματο δίκτυο, αν αυτό είναι δυνατό εξ' αιτίας του μεγέθους του.

5.2.3.2 Αναβαθμίσεις και Διορθώσεις Λογισμικού

Οι προμηθευτές προσπαθούν διαρκώς να διορθώσουν τυχόν ευπάθειες, όταν αυτές εντοπιστούν, σε υλικό και λογισμικό. Οι διαχειριστές των δικτύων πρέπει να επικοινωνούν τακτικά με τους προμηθευτές για να ελέγχουν εάν υπάρχουν διαθέσιμες διορθώσεις ή αναβαθμίσεις οι οποίες θα πρέπει να εφαρμοστούν κατάλληλα. Επιπλέον, οι διαχειριστές πρέπει να γραφτούν στις λίστες με τα e-mail πελατών που διαθέτουν οι προμηθευτές, μέσω των οποίων θα ενημερώνονται και θα καθοδηγούνται για γνωστές ευπάθειες και επιθέσεις.

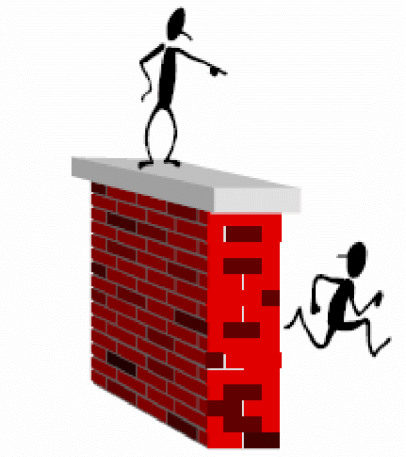
5.2.3.3 Αυθεντικοποίηση

Γενικά, οι αποτελεσματικές μέθοδοι αυθεντικοποίησης είναι ένας τρόπος να εμποδίζονται οι μη εξουσιοδοτημένοι χρήστες να προσπελάζουν ένα δίκτυο. Οι τεχνικές αυθεντικοποίησης περιλαμβάνουν την χρήση ονόματος χρήστη (user name) και κωδικού πρόσβασης (password), έξυπνων καρτών (smart cards), βιομετρίας, υποδομής δημοσίου κλειδιού (public key infrastructure – PKI), ή έναν συνδυασμό από όλα τα παραπάνω.

Όταν η αυθεντικοποίηση βασίζεται στην χρήση ονόματος χρήστη και κωδικού πρόσβασης, είναι σημαντικό να καθορίζεται, το ελάχιστο μήκος, οι απαιτούμενοι χαρακτήρες, και η λήξη του κωδικού πρόσβασης.

5.2.3.4 Τείχη Ασφαλείας (Firewalls)

Τα προσωπικά firewalls προσφέρουν ένα είδος προστασίας εναντίον ορισμένων επιθέσεων. Είναι λύσεις λογισμικού στο μηχάνημα ενός πελάτη και διαχειρίζονται από αυτόν, προσδιορίζοντας την επιθυμητή πολιτική ασφάλειας. Συνήθως χρησιμοποιούνται από χρήστες, οι οποίοι έχουν πρόσβαση σε δημόσια δίκτυα όπως αεροδρόμια, ξενοδοχεία κ.τ.λ, όπου μπορεί να υπάρχουν, για παράδειγμα, μη νόμιμα σημεία πρόσβασης εγκατεστημένα.



5.7.3.5 Συστήματα Ανίχνευσης Εισβολής (Intrusion Detection Systems – IDS)

Ένα τέτοιο σύστημα αποτελεί ένα καλό εργαλείο για να προσδιορισθεί αν κάποιος μη εξουσιοδοτημένος χρήστης προσπαθεί να κερδίσει πρόσβαση σε ένα δίκτυο. Μπορεί να είναι τριών ειδών: **host-based, network-based και hybrid** (υβριδικά, τα οποία συνδυάζουν τις δυνατότητες των δύο προηγούμενων ειδών). Ένα **host-based** σύστημα μπορεί να είναι εγκατεστημένο, για παράδειγμα, σε έναν server βάσης δεδομένων και να παρακολουθεί το σύστημα για ύποπτη συμπεριφορά, όπως επαναλαμβανόμενες αποτυχημένες απόπειρες εισόδου ενός χρήστη, ή αλλαγές στα δικαιώματα κάποιων αρχείων. Ένα **network-based** σύστημα παρακολουθεί, σε ένα τοπικό δίκτυο, την κίνηση των πακέτων σε πραγματικό χρόνο για να προσδιορίσει αν η κίνηση συμφωνεί με κάποια ήδη γνωστή επίθεση, που υπάρχει στη βάση δεδομένων του συστήματος.

5.2.3.6 Εκτιμήσεις Ασφάλειας

Οι εκτιμήσεις ασφάλειας είναι σημαντικό εργαλείο για να ελέγχεται η εικόνα της ασφάλειας ενός ασύρματου δικτύου. Οι διαχειριστές του δικτύου μπορούν, με τη χρήση προγραμμάτων παρακολούθησης της κίνησής του, να ελέγξουν αν οι ασύρματες συσκευές εκπέμπουν σωστά, να δουν αν υπάρχουν εγκατεστημένα μη εξουσιοδοτημένα σημεία πρόσβασης, κ.τ.λ.

5.2.3.7 Συστήματα HoneyPot

Η τεχνική HoneyPot είναι σχετικά μια καινούργια τεχνική εναντίων επιθέσεων από hackers σε συστήματα μεγάλων δικτύων δεδομένων η οποία βρίσκει εφαρμογή και στην καταπολέμηση του war driving. Η υλοποίηση αυτής της τεχνικής προβλέπεται σε περίπτωση που όλα τα προηγούμενα αντίμετρα αποτύχουν. Πιο συγκεκριμένα

βάζουμε σε κοινή θέα διάφορους ψεύτικους πόρους του ασύρματου δικτύου μας που θα μπορούσαν να δελεάσει τους hackers και να κρύψουμε τους σοβαρούς πόρους του συστήματός μας παρακολουθώντας τους πως συμπεριφέρονται καταφέρνοντας να βρούμε κάθε είδους αδυναμία τους που μπορούμε να χρησιμοποιήσουμε εναντίων τους. Η εγκατάσταση ενός τέτοιο σύστημα είναι πολύ εύκολη αρκεί να εγκαταστήσουμε αρχικά σε ένα pc, λογισμικό access point και την επιπλέον εγκατάσταση λογισμικών που έχουν δημιουργηθεί για τον σκοπό αυτό όπως τα Honeywall, Sebek, HoneyBow και άλλα.

ΠΑΡΑΡΤΗΜΑ Α: ΧΡΗΣΙΜΑ ΕΡΓΑΛΕΙΑ (AUDITING TOOLS)

Στο παρόν παράρτημα παρατίθενται τρεις συνοπτικοί πίνακες χρήσιμων εργαλειών που χρησιμοποιούνται στο wardriving και στην ανάλυση ασυρμάτων δικτύων [16].

Ονομα	**Πλατφόρμα**	**Ιστοσελίδα**
NetStumbler	Windows	http://www.NetStumbler.org/
Dstumbler	BSD	http://www.dachb0den.com/projects/dstumbler.html
MacStumble r	Macintosh	http://homepage.mac.com/macstumbler/
MiniStumbler	Pocket PC	http://www.NetStumbler.org/download.php?op=getit &lid=21
SSIDSniff	Unix	http://www.bastard.net/~kos/wifi/

Airosniff	Unix	http://gravitino.net/~bind/code/airosniff/
APScanner	Macintosh	http://homepage.mac.com/typexi/Personal1.html
wavemon	Linux	http://www.jm-music.de/projects.html
WLAN Expert	Windows	http://www.vector.kharkov.ua/download/WLAN/wlanexpert.zip
wavelan-tools	Linux	http://sourceforge.net/projects/wavelan-tools/
Kismet	Linux, iPaq, Zaurus	http://www.kismetwireless.net/
AiroPeek	Windows	http://www.wildpackets.com/products/airopeek/
Sniffer Wireless	Windows	http://www.sniffer.com/products/sniffer-wireless/
THC-WarDrive	Linux	http://www.thehackerschoice.com/download.php?t=r&d=wardrive-2.3.tar.gz
APSniff	Windows	http://www.bretmounet.com/ApSniff/
Wellenreiter	Linux	http://www.remote-exploit.org/
PrismStumbler	Linux	http://prismstumbler.sourceforge.net/
AirTraf	Linux	http://airtraf.sourceforge.net/

Πίνακας Α-1 WLAN Scanners

Ονομα	**Πλατφόρμα**	**Ιστοσελίδα**
Mognet	Java VM	http://chocobospore.org/mognet/
Kismet	Linux, Ipaq, Zaurus	http://www.kismetwireless.net/
Ethereal	Unix, Windows	http://www.ethereal.com/
TCPDump	Unix	http://www.tcpdump.org/
Prismdump	Unix	http://developer.axis.com/download/tools/
prism2dump	BSD	http://www.dachb0den.com/projects/prism2dump.ht

		ml
AiroPeek	Windows	http://www.wildpackets.com/products/airopeek/
Sniffer Wireless	Windows	http://www.sniffer.com/products/sniffer-wireless/

Πίνακας Α-2 WLAN Sniffers

Ονομα	**Πλατφόρμα**	**Ιστοσελίδα**
WEPCracker	Perl	http://sourceforge.net/projects/wepcrack/
AirSnort	Linux	http://www.be-secure.com/airsnort.html
AirSnort for BSD	BSD	http://www.dachb0den.com/projects/bsd-airsnort.html

Πίνακας Α-3 WEP Key Crackers

ΠΑΡΑΡΤΗΜΑ Β: IEEE TASK GROUPS

Η παρακάτω εικόνα δείχνει σε μορφή πίνακα τις ομάδες εργασίας που υπάρχουν και αφορούν το 802.11x.

802.11 Task Group	Name
802.11a	**High-speed Physical Layer in the 5GHz Band**
IEEE description	The family of specifications for wireless, Ethernet local area networks in 5-gigahertz bandwidth space.
URL	http://standards.ieee.org/getieee802/download/802.11a-1999.pdf
802.11b	**Higher-Speed Physical Layer Extension in the 2.4GHz Band**
IEEE description	The family of specifications for wireless, Ethernet local area networks in 2.4-gigahertz bandwidth space.
URL	http://standards.ieee.org/getieee802/download/802.11b-1999.pdf
802.11d	**Specification for Operation in Additional Regulatory Domains**
IEEE description	Define the physical layer requirements (channelization, hopping patterns, new values for current MIB attributes, and other requirements to extend the operation of 802.11 WLANs to new regulatory domains, or countries).
URL	http://standards.ieee.org/getieee802/download/802.11d-2001.pdf
802.11e	**MAC Enhancements for Quality of Service**
IEEE description	Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol.
URL	http://grouper.ieee.org/groups/802/11/Reports/tge_update.htm
802.11f	**Recommended Practice for Inter Access Point Protocol**
IEEE description	Develop recommended practices for an Inter-Access Point Protocol (IAPP), which provides the necessary capabilities to achieve multi-vendor Access Point interoperability across a Distribution System supporting IEEE P802.11 Wireless LAN Links.
URL	http://grouper.ieee.org/groups/802/11/Reports/tgf_update.htm
802.11g	**Standard for Higher Rate (20+ Mbps) Extensions in the 2.4GHz Band**
IEEE description	Develop a higher speed(s) physical layer extension to the 802.11b standard. The new standard shall be compatible with the IEEE 802.11 MAC. The maximum physical layer data rate targeted by this project shall be at least 20 Mbit/s. The new extension shall implement all mandatory portions of the IEEE 802.11b physical layer standard.
URL	http://grouper.ieee.org/groups/802/11/Reports/tgg_update.htm
802.11h	**SMa - Spectrum Managed 802.11a**
IEEE description	Enhance the 802.11 Medium Access Control (MAC) standard and 802.11a High Speed Physical Layer (PHY) in the 5GHz Band supplement to the standard; to add indoor and outdoor channel selection for 5GHz license exempt bands in Europe; and to enhance channel energy measurement and reporting mechanisms to improve spectrum and transmit power management (per CEPT and subsequent EU committee or body ruling incorporating CEPT Recommendation ERC 99/23).
URL	http://grouper.ieee.org/groups/802/11/Reports/tgh_update.htm
802.11i	**MAC Enhancements for Enhanced Security**
IEEE description	Enhance the current 802.11 MAC to provide improvements in security.
URL	http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm

Εικόνα Β-1 IEEE TASK GROUPS

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]. Wireless Network Security 802.11, Bluetooth and Handheld Devices (National Institute of Standards and Security - NIST)

[2]. Wireless LAN Security and Laboratory Designs

[3]. Ασφάλεια Πληροφοριακών Συστημάτων, Σωκράτης Κ. Κατσίκας – Δημήτρης Γκρίτζαλης, Στέφανος Γκρίτζαλης (Εκδόσεις Νέων Τεχνολογιών)

[4]. Wireless Security (http://home.no.net/coverage/SecurityinWLAN.htm)

[5]. 802.11 Wireless Networks: The Definitive Guide (By Matthew Gast)

[6]. IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.5B, May 2006

[7]. Wireless LAN Security: Securing Your Access Point-Sia Sie Tung , Nurul Nadia Ahmad, Tan Kim Geok Faculty of Information Science and Technology Multimedia University, Malaisia

[8]. WiFi Security –Stewart S. Miller

[9]. Wi-Fi for the Enterprise- Nathan J. Muller – 2003

[10]. Security and Routing in Wireless Networks - Yang Xiao, Jie Li, Yi Pan- 2005

[11]. Wireless Hacking. Projects for Wi-Fi Enthusiasts - Lee Barken with Eric Bermel, John Eder, Matthew Fanady Michael Mee, Marc Palumbo, Alan Koebrick

[12]. ANSI/IEEE Std 802.11, 1999 Edition

[13]. IEEE Std 802.11i, 2004 Edition

[14]. 802.11 Wireless Networks: The Definitive Guide, O' Reilly, Matthew Gast (2002)

[15]. Extensible Authentication Protocol Overview, http://www.microsoft.com/technet/prodtechnol/winxppro/evaluate/eap.mspx

[16]. Hacking the Invisible Network Insecurities in 802.11x By Michael Sutton iDEFENSE Labs msutton@idefense.com July 10, 2002

[17]. Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison Wesley, John Edney and William A. Arbaugh (2003)

[18]. Hacking Wireless Networks for Dummies, Kevin Beaver and Peter T. Davis

[19]. Wireless Hacking. Projects for Wi-Fi Enthusiasts, By the SoCalFreeNet.org WirelessUsers Group Lee Barken with Eric Bermel, John Eder, Matthew Fanady Michael Mee, Marc Palumbo, Alan Koebrick

[20]. ERNST & YANG - An Update on Wireless Security – 20060919, Matt Hynes

[21]. Senior Manager, Ernst & Young Technology & Security Risk Services, Nick Tobkin

[22]. Senior, Ernst & Young Technology & Security Risk Service

[23]. Real 802.11 Security , Edney, Arbaugh ISBN 0-321-13620-9

[24]. ERNST & YANG – Wireless Penetration Testing and Countermeasures for WiFi (802.11b/g) Technology, Matt Hynes , Senior Manager, Ernst & Young Technology & Security Risk Services

[25]. Wireless LAN Security: Securing Your Access Point, Sia Sie Tung , Nurul Nadia Ahmad, Tan Kim Geok , Faculty of Information Science and Technology Multimedia University, Malaysia

[26]. Computer Networks, 4th Edition, Prentice Hall, 2002, A. S. Tanenbaum.

[27]. "Your 802.11 Wireless Network has No Clothes." Arbaugh, William, Narendar Shankar and Justin Wan. http://downloads.securityfocus.com/library/wireless.pdf.

[28]. Brewin, Bob, Dan Verton and Jennifer DiSabatino. "Wireless LANs: Trouble intheAir."ComputerWorld. http://www.computerworld.com/securitytopics/security/story/0,10801,67344,00.html

[29]. Brown, Bruce. "Wireless Standards Up in the Air." http://www.extremetech.com/article2/0,3973,9164,00.asp

[30]. Cyclic Redundancy Check Polynomials Tutorial. http://www.cee.hw.ac.uk/~pjbk/nets/crctutorial.html

[31]. Kamerman, Ad and Nedim Erkoçevic. "Microwave Oven Interference on Wireless LANs Operating in the 2.4 GHz ISM Band."

[32]. Kerry, Stuart J. "Chair of IEEE 802.11 Responds to WEP Security Flaws." http://slashdot.org/articles/01/02/15/1745204.shtml

[33]. Noble, Ivan. "Wireless networks wide open." http://news.bbc.co.uk/hi/english/sci/tech/newsid_1638000/1638920.stm.

[34]. Schenk, Rob, Andrew Garcia and Russ Iwanchuk. "Wireless LAN Deployment and Security Basics." http://www.extremetech.com/article/0,3396,s=1034&a=13521,00.asp

[35]. Stanley, Richard A. "Wireless LAN Risks and Vulnerabilities." Information Systems Control Journal,Volume 2 (2002).
http://www.isaca.org/wirelesswhitepaper.pdf

[36]. Stubblefield, Adam, John Ioannidis and Aviel D. Rubin. "Using the Fluhrer, Mantin andShamirAttacktoBreakWEP."
http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

[37]. University of Berkeley FAQ.
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[38]. Walker, Jesse, "802.11 Security Series – Part II: The Temporal Key Integrity Protocol (TKIP)."
http://cedar.intel.com/media/pdf/security/80211_part2.pdf

[39]. 802.11 IEEE standard
http://standards.ieee.org/getieee802/download/802.11-1999.pdf

[40]. 802.11i IEEE standard
http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[41]. WepLab, analyzing WEP encryption security on wireless networks
http://weplab.sourceforge.net/

[42]. Top 100 Network Security Tools
http://sectools.org

[43]. NetStumbler
www.**netstumbler**.org

[44]. Omnipeek
www.wildpackets.com

[45]. Kismet

http://www.kismetwireless.net/

[46]. Airodump,Aircrack

http://www.wirelessdefence.org/Contents/Aircrack_airodump.htm

[47]. Back Track bootable wireless/security auditing

http://www.remote-exploit.org

[48]. Wardriving

www.wardrive.net/

http://www.worldwidewardrive.org

[49]. it_wifisecurity from HP

www.hp.com/sbso/productivity/howto/it_**wifisecurity**/

www.**security**-assessment.com/

[50]. The Honeynet Project

http://project.honeynet.org/

[51]. NETGEAR

http://www.netgear.com/Products/RoutersandGateways/GWirelessRouters/DG834G.aspx?detail=Specifications