ΤΕΙ Κρήτης

Τμήμα Εφαρμοσμένης Πληροφορικής Και Πολυμέσων

Ασφάλεια Πληροφοριακών Συστημάτων

Πτυχιακή Εργασία

"Υλοποίηση τεχνικών για τον έλεγχο κωδικών, την πιστοποίηση ταυτότητας και τον έλεγχο πρόσβασης με τη χρήση εργαλείων για password cracking, wireless security και authorization devices."

Επιβλέπων καθηγητής
Δρ. Χαράλαμπος Μανιφάβας

Φοιτητές
Μαθιουδάκης Ιωάννης
Ψυχομάνης Νεκτάριος

Ηράκλειο
Μάιος 2012

Πτυχιακή Εργασία

Υλοποίηση τεχνικών για τον έλεγχο κωδικών, την πιστοποίηση ταυτότητας και τον έλεγχο πρόσβασης με τη χρήση εργαλείων για password cracking, wireless security και authorization devices.

Μαθιουδάκης Ιωάννης
Ψυχομάνης Νεκτάριος

Επιβλέπων καθηγητής: Δρ. Χαράλαμπος Μανιφάβας
Επίκουρος Καθηγητής

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ……

……..	……..	……..
Χ. Μανιφάβας	Γ. Κορνάρος	Ι. Παχουλάκης
Επίκουρος Καθηγητής	Καθηγητής Εφαρμογών	Επίκουρος Καθηγητής

Υπεύθυνη Δήλωση

Βεβαιώνουμε ότι είμαστε συγγραφείς αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχαμε για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχουμε αναφέρει τις όποιες πηγές από τις οποίες κάναμε χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνουμε ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμάς για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι. Κρήτης.

Νεκτάριος Ψυχομάνης
Ιωάννης Μαθιουδάκης

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τους γονείς μου και τις αδερφές μου για την υποστήριξη που μου παρείχαν όλα αυτά τα χρόνια των σπουδών μου.

Ευχαριστώ τους καθηγητές για τις γνώσεις που μου πρόσφεραν στο Τμήμα Εφαρμοσμένης Πληροφορικής και Πολυμέσων του ΤΕΙ Κρήτης και τους συμφοιτητές μου και φίλους μου για τις ωραίες εμπειρίες.

Νεκτάριος Ψυχομάνης

Θέλω να ευχαριστήσω τους γονείς μου για την στήριξή τους στην απόφαση και επιθυμία μου για τη συνέχιση απόκτησης γνώσεων και τη σύζυγό μου για την υποστήριξη στη δεύτερη σπουδαστική περίοδο της ζωής μου.

Επίσης, θέλω να ευχαριστήσω τα μέλη του εκπαιδευτικού προσωπικού του τμήματος για την θέληση και επιμονή τους στην προσφορά γνώσεων, καθώς και τους συμφοιτητές μου για τις ωραίες στιγμές που ζήσαμε μαζί όλα αυτά τα χρόνια.

Ιωάννης Μαθιουδάκης

Οι συγγραφείς της πτυχιακής αυτής θεωρούν πολύ σημαντικό να ευχαριστήσουν τον επιβλέποντα Επίκουρο Καθηγητή κ. Δρ. Χαράλαμπο Μανιφάβα για την υποστήριξη, τη βοήθεια και τη συνεργασία που είχαμε στην υλοποίηση της πτυχιακής αυτής.

"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 – Καθηγητής Επιστήμης Υπολογιστών

"Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain."
Kevin Mitnick – Συγγραφέας και hacker

"Passwords are like underwear: you don't let people see it, you should change it very often and you shouldn't share it with strangers."
Chris Pirillo - Συγγραφέας

Περίληψη

Στην κρυπτανάλυση και την ασφάλεια του υπολογιστή, η αποκρυπτογράφηση κωδικών είναι η διαδικασία ανάκτησης των κωδικών πρόσβασης από τα δεδομένα που έχουν αποθηκευθεί ή μεταδίδονται από ένα σύστημα υπολογιστή. Μια κοινή προσέγγιση είναι η επανειλημμένη προσπάθεια να βρεθεί ο κωδικός πρόσβασης μέσω επαναλαμβανόμενων υποθέσεων.

Ο σκοπός της αποκρυπτογράφησης του κωδικού πρόσβασης θα μπορούσε να είναι να βοηθηθεί ένας χρήστης να ανακτήσει τον ξεχασμένο κωδικό πρόσβασης (αν και η εγκατάσταση ενός εντελώς νέου κωδικού πρόσβασης έχει μικρότερο κίνδυνο για την ασφάλεια, αλλά απαιτεί προνόμια διαχείρισης συστήματος).

Με τη χρήση αποκρυπτογράφησης κωδικών μπορούν να αποκτήσουν ορισμένα άτομα μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα ή μπορεί να χρησιμοποιηθεί ως ένα προληπτικό μέτρο από τους διαχειριστές κάποιου συστήματος για να ελέγξουν εύκολα πόσο ευάλωτοι είναι οι κωδικοί πρόσβασης.

Σήμερα με τον πολλαπλασιασμό των πληροφοριακών συστημάτων και των δικτύων με τα οποία έρχεται σε επαφή κάποιος, λόγω της προόδου της τεχνολογίας σε όλες τις οικονομικές και κοινωνικές δραστηριότητες του ανθρώπου, η ύπαρξη πολλών διαφορετικών κωδικών ασφαλείας τους καθιστά άχρηστους και δύσκολους για την απομνημόνευσή τους από τον μέσο άνθρωπο. Επίσης, η εξέλιξη των μεθόδων κυβερνοεγκλήματος οδήγησε στην ανάγκη δημιουργίας νέων μεθόδων προστασίας πληροφοριακών συστημάτων και δικτύων, χωρίς καμιά από αυτές να παρέχει απόλυτη προστασία.

Η παρούσα πτυχιακή εργασία ασχολείται με τα παρακάτω θέματα:

- Αποκρυπτογράφηση κωδικών (password cracking)
- Επιθέσεις σε ασύρματα δίκτυα

Για το password cracking θα χρησιμοποιηθούν software εργαλεία όπως το John The Ripper και aircrack-ng κ.α. είτε σε περιβάλλον Windows είτε σε περιβάλλον Linux ανάλογα με τη διαθεσιμότητά τους σε κάθε λειτουργικό σύστημα. Επίσης, για το password cracking θα εξετασθούν δυνατότητες και απόδοσης των ορισμένων από τα παραπάνω εργαλεία, με τη χρήση multicore συστημάτων. Δηλαδή με τη χρήση multicore CPU, όπου υπάρχει η δυνατότητα μείωσης του χρόνου password cracking λόγω συμμετρικής παράλληλης επεξεργασίας hardware (SMP - Symmetric multiprocessing).

Σημαντικός τομέας εφαρμογής τεχνικών ασφάλειας είναι τα wireless LAN. Η τεράστια διάδοσή τους και η λειτουργία τους με ραδιοκύματα, τα καθιστά ευαίσθητα σε απειλές ασφάλειας. Στην εργασία αυτή θα αναλυθούν κάποια είδη επιθέσεων σε ασύρματα δίκτυα. Θα υλοποιηθούν επιθέσεις σε «συνθήκες εργαστηρίου» και θα παρουσιαστούν τα βήματα για να γίνουν αυτές. Σκοπός είναι να φανεί πόσο σημαντικό είναι η λήψη πολλαπλών μέτρων για την προστασία των WLANs.

Abstract

In computer security, password decryption is the process of recovering a password from data stored or transmitted by a computer system. A common approach is the attempt to find the password through repeated guesses (dictionary or brute force attack).

The purpose of decrypting a password is to help a user recover forgotten passwords. Installing an entirely new password is considered safer, but requires privileges management system.

By cracking passwords, attackers can get unauthorized access to a system. On the other hand, administrators can check for vulnerable passwords and alert their owners. This is a preventive measure to increase the security of a system.

Today, with the proliferation of information systems, communication networks and on-line services the average user is faced with the challenging task to manage a large number of passwords that are difficult to memorize. In general, users are advised to pay attention to their on-line behavior because cybercrime is on the rise. However, there is no 100% protection.

In this thesis we discuss and demonstrate a number of attacks regarding:

- Password Cracking
- Attacks on wireless networks

For password cracking, we demonstrate the use of tools like John The Ripper and aircrack-ng, both on Windows and on Linux operating systems. We measure the performance of the attack on both single-core and multi-core systems. Multicore systems achieve symmetric parallel processing (SMP - Symmetric multiprocessing) and as a result the time needed to crack passwords is significantly reduced.

Wireless LANs based on different technologies are in everyday use by many users accessing all kinds of on-line services. Their widespread use makes them a convenient target. Attackers use protocol, implementation or improper use caused vulnerabilities to extract personal information or to gain unauthorized access to services. In this thesis we analyze and demonstrate step by step, in laboratory conditions, a number of attacks on wireless LANs. Our aim is to show how important it is for everyone to take appropriate measures to protect his on-line presence.

Πίνακας Περιεχομένων

Πίνακας εικόνων

Πίνακας Πινάκων

1. Κεφάλαιο – Backtrack 5 R2 (Linux)

1.1 Συνοπτική Περιγραφή

Το Backtrack θεωρείται κάτι σαν ελβετικός σουγιάς για Hackers, Penetration Testers και γενικότερα για όσους ενδιαφέρονται για τον παράγοντα ασφάλεια. Η αξιοπιστία του και η χρησιμότητα του είναι δεδομένη, ειδικά αν σκεφτούμε πως χρησιμοποιείται από οργανισμούς όπως ο SANS και από κρατικές υπηρεσίες όπως το FBI! Η νέα έκδοση ονομάζεται Revolution και όχι άδικα, αφού τα πάντα έχουν φτιαχτεί από την αρχή και οι αλλαγές του είναι επαναστατικές. Το Backtrack 5 έχει βασιστεί στο Ubuntu 10.04 LTS, έχοντας όμως το νεότερο πυρήνα 2.6.38. Το KDE 3.5 αντικαταστάθηκε με το KDE 4 και για πρώτη φορά υπάρχει, σε ξεχωριστό iso, το Gnome. Όσοι επιθυμούν μεγαλύτερη ταχύτητα μπορούν να χρησιμοποιήσουν το μινιμαλιστικό Fluxbox.

Εικόνα 1. Backtrack 5 R2

Η εγκατάσταση του δεν διαφέρει και πολύ από αυτή του Ubuntu, οπότε μπορούμε άνετα να το περάσουμε σε σκληρό δίσκο. Λειτουργεί όμως εξίσου ικανοποιητικά σαν Live DVD ή ακόμα και μέσω εικονικών μηχανών, όπως το Virtual Box. Υπάρχουν έτοιμα και Vmware iso ενώ η υποστήριξη φθάνει μέχρι την 64 bit αρχιτεκτονική και τους επεξεργαστές ARM. Ο χαρακτήρας του γίνεται φανερός με το πρώτο άνοιγμα του Firefox, ο οποίος έχει προεγκατεστημένο το πρόσθετο Noscript για την προστασία μας από κακόβουλα scripts και το Tamper Data για την αλλαγή σε HTTP Headers. Ενημερωτικά, να πούμε πως στο Tamper Data οφείλονται τα εξωπραγματικά σκορ που βλέπετε σε διάφορα on line Games. Αυτή βέβαια είναι η πιο αθώα χρήση του.

Ο όγκος των εργαλείων που έχουν συγκεντρωθεί είναι εντυπωσιακός, καλύπτοντας κάθε πλευρά του Penetration Testing. Η πιο γνωστή χρήση της διανομής είναι αυτή του ελέγχου ασύρματων συσκευών. Δεν θα μπορούσαν λοιπόν να απουσιάζουν Wi-Fi εργαλεία, όπως το Kismet ή ακόμα και εφαρμογές Bluetooth, όπως το Bluediving. Όσον αφορά το Information Gathering, δεν περιορίζεται μόνο στους γνωστούς scanners όπως οι Nmap και Nessus. Φθάνει μέχρι τους Routers, με στόχο την εύρεση συσκευών της Cisco στις οποίες οι διαχειριστές παρέλειψαν να αλλάξουν τον εργοστασιακό κωδικό.

Διαθέσιμο είναι και ένα πλήθος εργαλείων για να δούμε τις αντοχές ενός δικτύου ή την αποτελεσματικότητα των κανόνων στο Firewall της διανομής μας. Πρόκειται για το λεγόμενο Stress Testing που αφορά επιθέσεις Denial Of Service. Μεγάλη είναι και η βάση δεδομένων με συγκεντρωμένα διάφορα exploits για κάθε λειτουργικό σύστημα. Η λίστα εφαρμογών είναι ατελείωτη και συνεχίζεται με sniffers, debuggers, forensics tools κλπ. Δεν του ξεφεύγει ούτε το VOIP ή ακόμα και η δυνατότητα αλλαγής Mac Address.

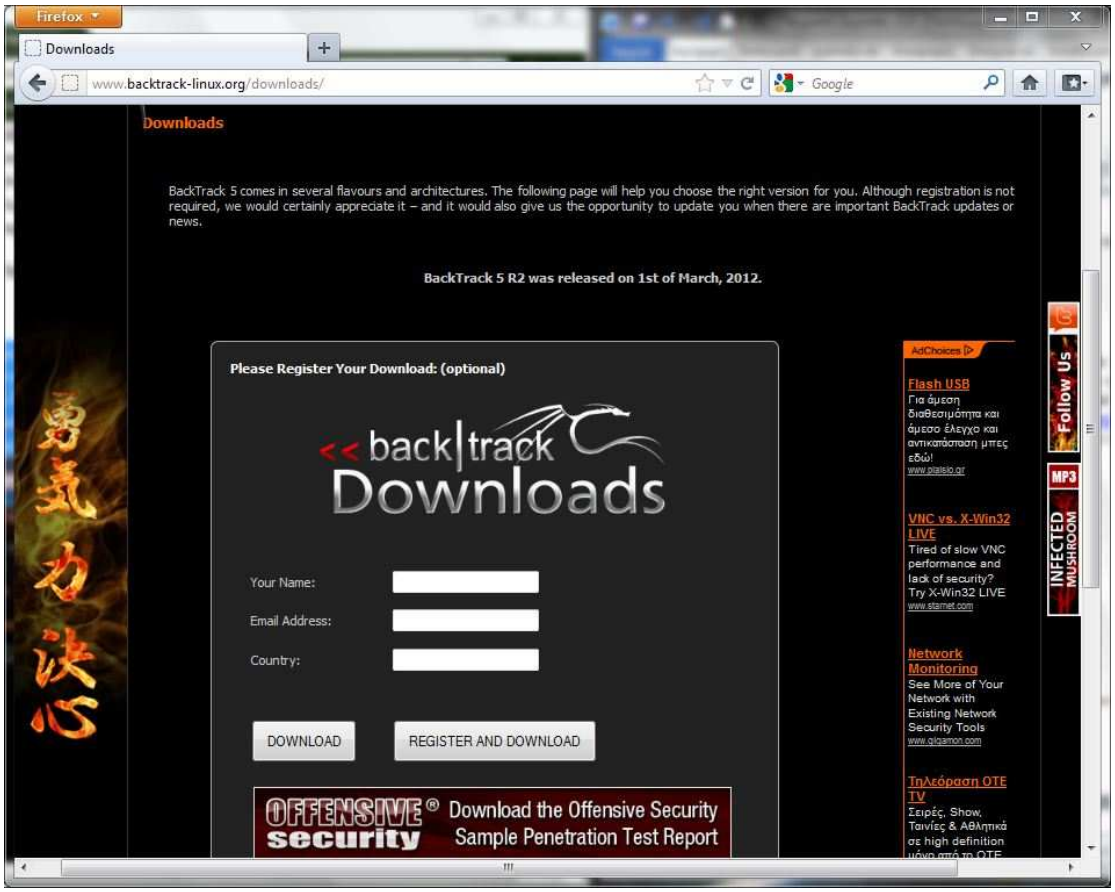
Συνοψίζοντας, το ήδη άριστο Backtrack βελτιώθηκε ακόμα πιο πολύ. Είναι φιλικότερο, ευέλικτο και με περισσότερες επιλογές. Για όσους παίρνουν στα σοβαρά την ασφάλεια του υπολογιστή τους είναι απαραίτητο.

1.2 Install BackTrack to Hard Disk

Στο υποκεφάλαιο αυτό θα αναλύσουμε το πώς μπορείτε να εγκαταστήσετε τη διανομή του Linux ,BackTrack 5 R2 στον σκληρό σας δίσκο.

Βήμα 1^{ο} – Download BackTrack 5 R2

Το βασικότερο βήμα ,χωρίς το οποίο δεν μπορείτε να προχωρήσετε στα επόμενα, είναι να κατεβάσετε το αρχείο εικόνας του δίσκου του Backtrack 5.Για αυτό το σκοπό θα πάτε στην ιστοσελίδα του Backtrack και ποιό συγκεκριμένα στο Section των Downloads (http://www.backtrack-linux.org/downloads/). Στη σελίδα αυτή θα πατήσετε την επιλογή Download και θα συνεχίσετε σε μια σελίδα στην οποία θα δώσετε τις προτιμήσεις σας σχετικά με το λειτουργικό που θα εγκατασταθεί το BackTrack.



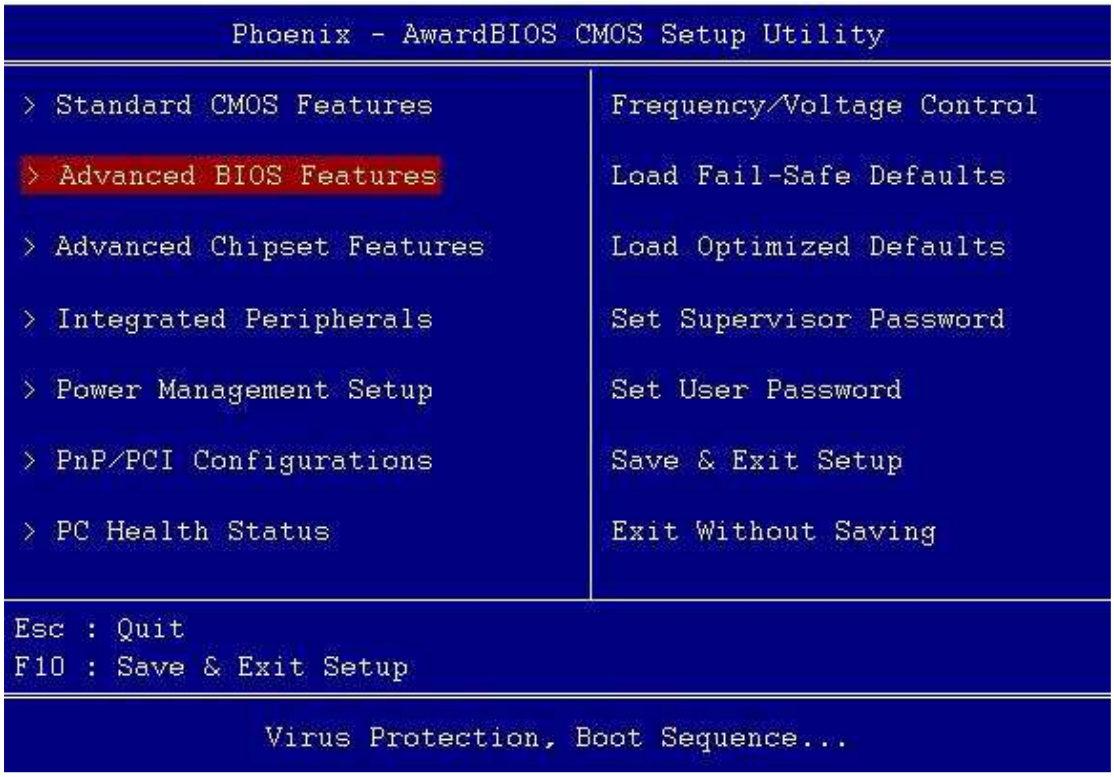
Εικόνα 2. Download BackTrack 5 R2

Βήμα 2ο – Burn the .iso file to a disk

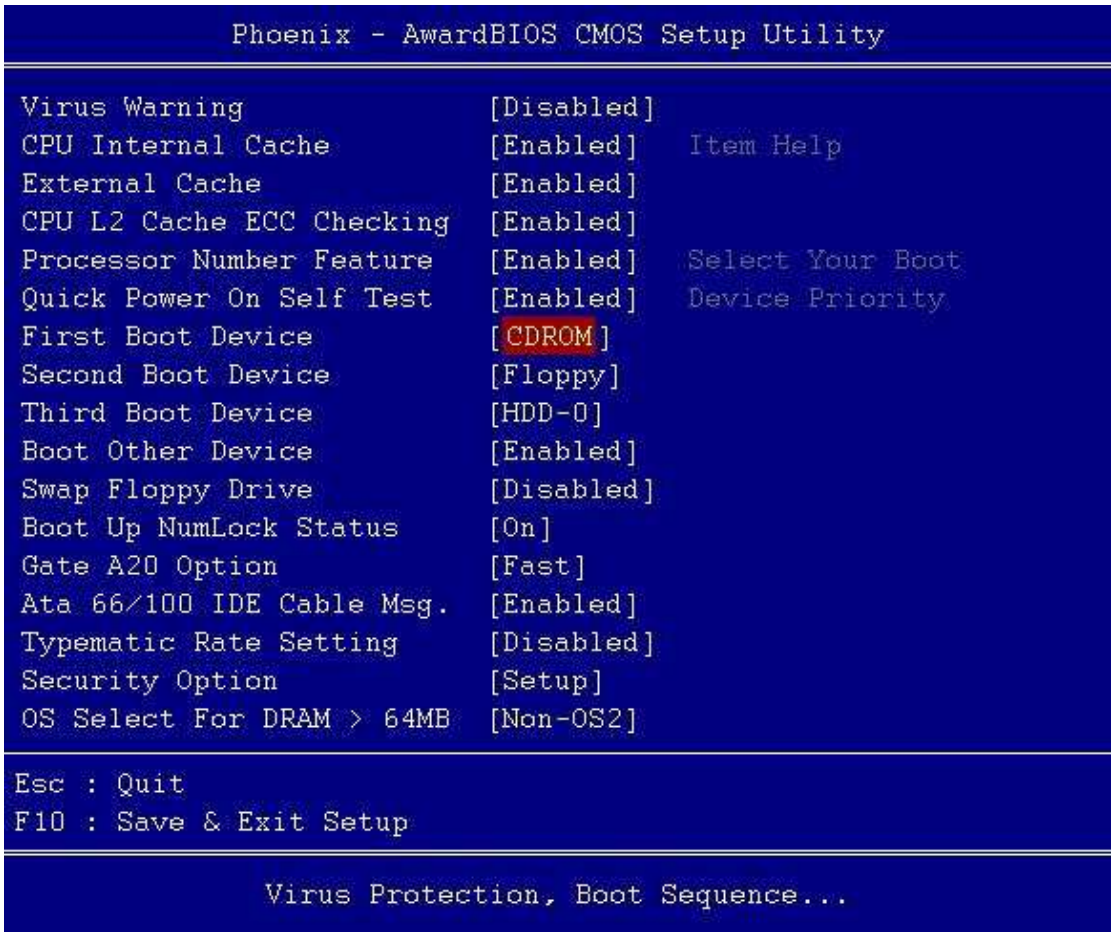
Αφού λοιπόν κατέβει το αρχείο .iso πρέπει να το κάψετε στην συνέχεια σε ένα δίσκο DVD. Στα Windows 7 υπάρχει προεγκατεστημένο πρόγραμμα για την εγγραφή εικονικών δίσκων. Αλλιώς κατεβάστε ένα πρόγραμμα όπως το Alcohol 120%, Nero , κτλ.

Βήμα 3ο – Boot from DVD

Σε αυτό το βήμα θα πρέπει να "πείτε" στον υπολογιστή σας να κάνει boot από το DVD και όχι από τον σκληρό δίσκο προκειμένου να φορτώσει το BackTrack. Αρχικά βάλτε το δισκάκι στο Drive και επανεκκινήστε τον υπολογιστή. Την ώρα που ξεκινάει το BIOS θα πρέπει να σας εμφανίζει κάποιες επιλογές μέσα στις οποίες θα υπάρχει ένα "BIOS Setup" και δίπλα το αντίστοιχο πλήκτρο για να μπείτε μέσα (συνήθως είναι ένα από τα F1,…,F8 ή Del). Εσείς αφού βρείτε ποιο είναι το πλήκτρο που σας δίνει το BIOS πηγαίνετε στο "Advanced Bios Features" και στην συνέχεια επιλέξτε CD-ROM από το "First Boot Device". Τέλος βγείτε στην αρχική οθόνη, και αποθηκεύστε τις αλλαγές που κάνατε. Το μηχάνημά σας στην συνέχεια θα κάνει επανεκκίνηση και θα ξεκινήσει να φορτώνει το DVD αντί να μπει στα Windows.



Εικόνα 3. Advanced BIOS Features



Εικόνα 4. Bios - First Boot Device

Βήμα 4^{ο} – Choose BackTrack Package for installation

Αφού κάνετε Boot από το δισκάκι σας μετά από λίγο θα μπείτε στο menu του Backtrack και θα επιλέξετε το package “Default Boot Text Mode”.

Εικόνα 5. Selection BackTrack Package

Βήμα 5^{0} – Εισαγωγή στο γραφικό περιβάλλον

Μετά από λίγη ώρα και πολλές γραμμές εντολών του λειτουργικού, το πρόγραμμα θα σταματήσει και θα είναι έτοιμο για χρήση. Ωστόσο το BackTrack προσφέρει και την δυνατότητα να το τρέξετε και σε γραφικό περιβάλλον (GUI) αρκεί να πληκτρολογήσετε την εντολή “**startx**”.

Εικόνα 6. Είσοδος στο γραφικό περιβάλλον του BackTrack

Βήμα 6ο – Εγκατάσταση BackTrack

Στην επιφάνεια εργασίας υπάρχει ένα εικονίδιο που λέγεται "**Install BackTrack**" (το μόνο δηλαδή) στο οποίο κάνετε διπλό κλικ.

Βήμα 7ο – Επιλογή γλώσσα εγκατάστασης

Μετά από αυτό θα εμφανιστεί ο Installer του BackTrack και αρχικά η Welcome Screen στην οποία πρέπει να επιλέξετε τη γλώσσα εγκατάστασης. Επιλέξτε λοιπόν αυτή που σας ταιριάζει και πατήστε Forward.

Εικόνα 7. Επιλογή γλώσσα εγκατάστασης BackTrack 5

Βήμα 8^{ο} – Επιλογή τοποθεσίας σας

Τώρα απλά επιλέγετε τη χώρα στην οποία είσαστε και πατάτε ξανά Forward.

Εικόνα 8. Επιλογή τοποθεσίας

Και αμέσως μετά επιλέγουμε τη γλώσσα πληκτρολογίου.

Εικόνα 9. Επιλογή γλώσσας πληκτρολογίου

Βήμα 9ο – Προετοιμασία σκληρού δίσκου για την εγκατάσταση του BackTrack

Αυτό το βήμα είναι και το βασικότερο. Αφού πατήσετε Forward στο Βήμα 8 τώρα καλείστε να επιλέξετε που και πώς θα εγκαταστήσετε το λειτουργικό μέσω των παρακάτω επιλογών:

- Η πρώτη επιλογή σας λέει να εγκαταστήσετε το BackTrack δίπλα στο βασικό σας λειτουργικό σύστημα και κάθε φορά που ανοίγετε τον Η/Υ να επιλέγετε πιο λειτουργικό θέλετε να ανοίξει (προτεινόμενη επιλογή), εφόσον εγκαθιστάτε το Backtrack σε υπολογιστή με υφιστάμενο άλλο λειτουργικό, όπως Windows). Για να καθορίσετε τα GB του κάθε λειτουργικού απλά μετακινείτε την άσπρη μπάρα δεξιά-αριστερά.
- Η δεύτερη επιλογή σας λέει να διαγράψετε τα πάντα στο δίσκο αυτό, και στη συνέχεια να εγκαταστήσετε το λειτουργικό.
- Και τρίτον να καθορίσετε μόνοι σας τα partitions το οποίο δεν είναι και τόσο δύσκολο αλλά δεν συνιστάτε.

Εικόνα 10. Προετοιμασία σκληρού δίσκου για την εγκατάσταση του BackTrack

Βήμα 10^{ο} – Επαλήθευση επιλογών

Στο τελευταίο βήμα μπορείτε να δείτε όλες τις επιλογές που έχετε κάνει πριν την εγκατάσταση του BackTrack.

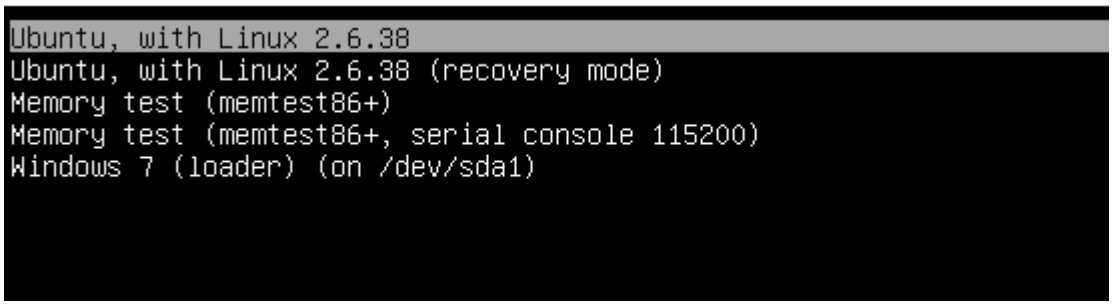
Εικόνα 11. Επαλήθευση επιλογών

Με το πάτημα του Install θα ξεκινήσει η εγκατάσταση και μετά από λίγη ώρα θα σας εμφανίσει το εξής μήνυμα με το οποίο ξέρετε ότι τελείωσε επιτυχημένα η εγκατάσταση και πρέπει να επανεκκινήσετε τον Η/Υ.

Εικόνα 12. Επανεκκίνηση συστήματος για την ολοκλήρωση της εγκατάστασης

Βήμα 11ο – Ολοκλήρωση εγκατάστασης

Αφού γίνει η επανεκκίνηση θα ανοίξει από μόνος του ο GRUB Bootloader στον οποίο κάθε φορά θα σας δίνει κάποιες επιλογές, όπως κανονικής φόρτωσης του Backtrack ή φόρτωσης σε recovery mode και επιλογές για το εργαλείο memtest. Σε περίπτωση που η εγκατάσταση του Backtrack έχει γίνει σε δίσκο με ήδη εγκατεστημένα Windows, ο GRUB Bootloader θα σας δίνει την δυνατότητα φόρτωσής τους με μια εικόνα σαν την παρακάτω.



Εικόνα 13. GRUB Bootloader

Έτσι όταν ανοίξετε το BackTrack θα σας ζητήσει όνομα χρήστη και κωδικό.

Στο username θα γράψετε **root** ενώ το password είναι **toor**. Αν θέλετε να αλλάξετε τον κωδικό χρήστη απλά ανοίξτε ένα τερματικό (terminal) ,πληκτρολογήστε την εντολή passwd και δώστε τον καινούριο σας κωδικό.

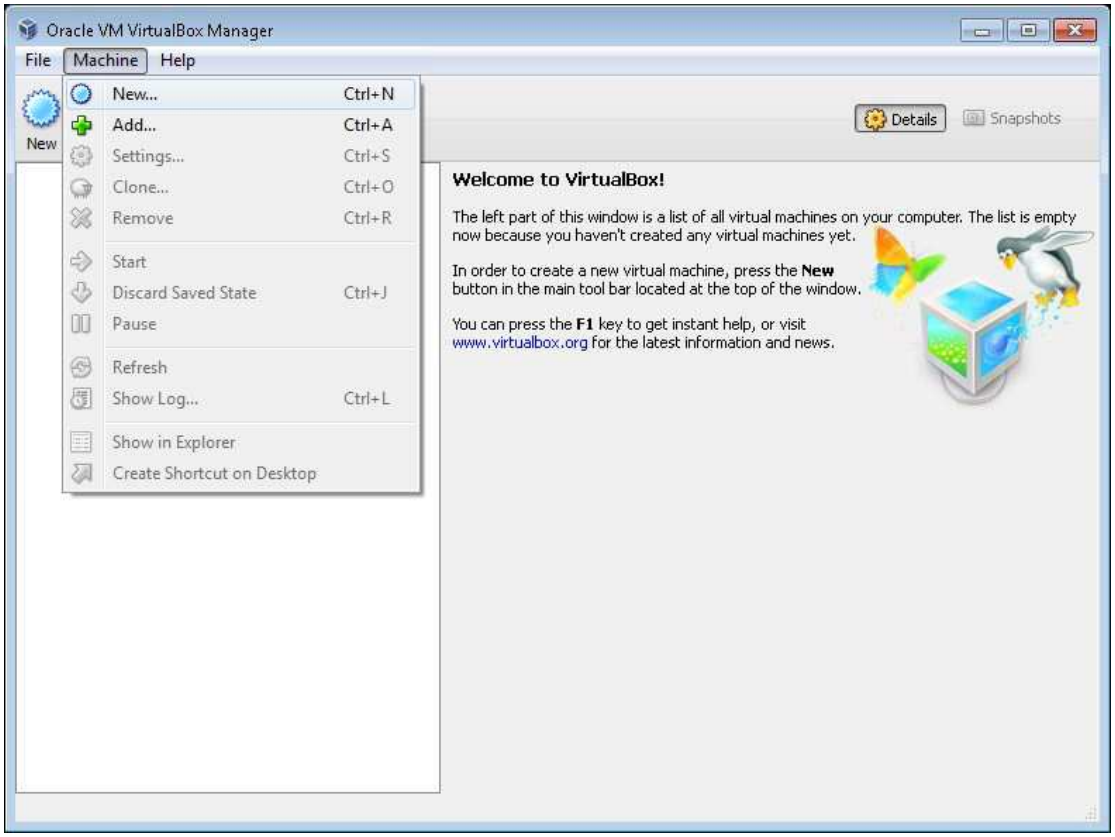
1.3 Install BackTrack to VirtualBox

Στο υποκεφάλαιο αυτό θα δείξουμε μια εναλλακτική εγκατάσταση του BackTrack. Συγκεκριμένα θα αναλύσουμε το πώς μπορείτε να εγκαταστήσετε τη διανομή του Linux ,BackTrack 5 R2 σε VirtualBox.

Βήμα 1^{ο} – Δημιουργία και ρύθμιση εικονικής μηχανής

Βασικό βήμα για να κάνετε την εγκατάσταση του BackTrack είναι να φτιάξετε μία εικονική μηχανή στο VirtualBox.

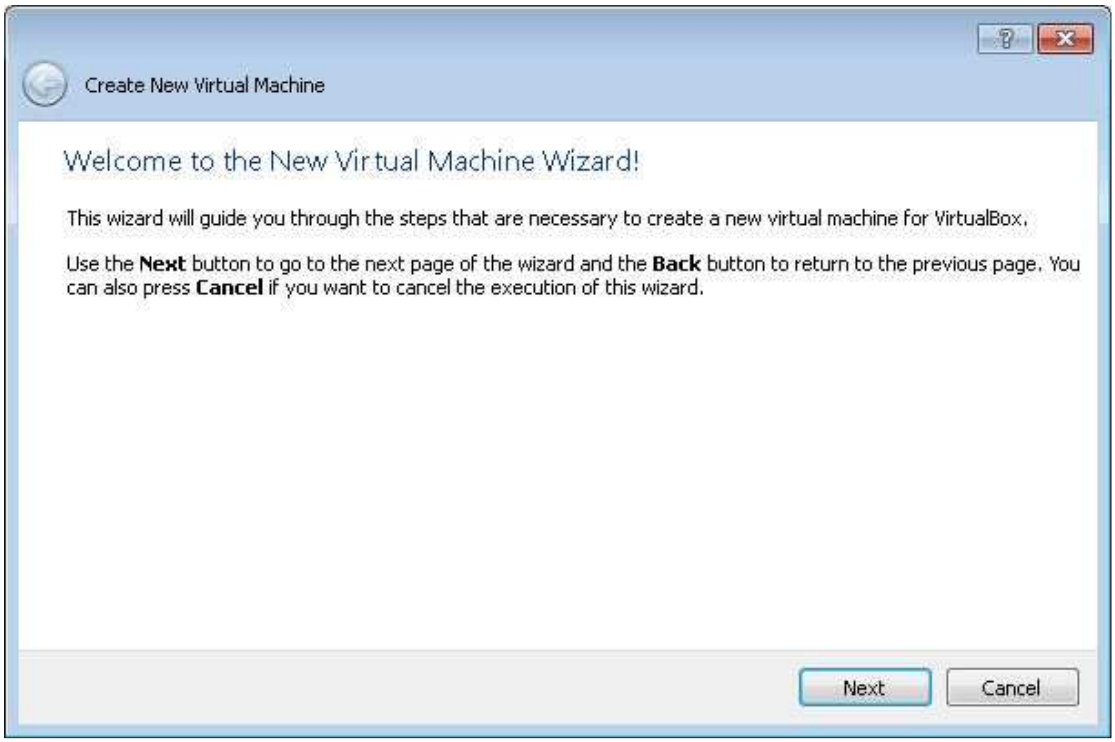
Πηγαίνετε λοιπόν, **Machine → New**



Εικόνα 14. Δημιουργία εικονικής μηχανής

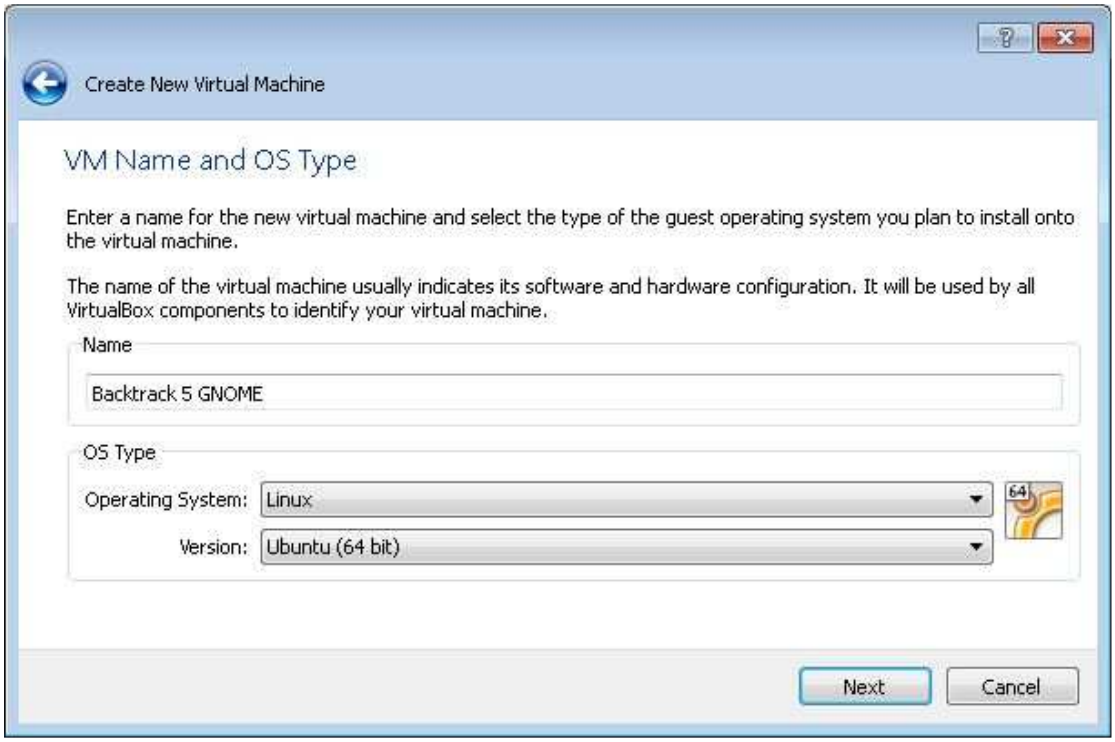
Σε αυτό το σημείο ξεκινά ο οδηγός μέσω του οποίου θα γίνει το στήσιμο του εικονικού σας συστήματος.

Εκεί αργότερα θα εγκαταστήσουμε και το λειτουργικό σας σύστημα BackTrack.



Εικόνα 15. Οδηγός ρύθμισης Virtual Machine

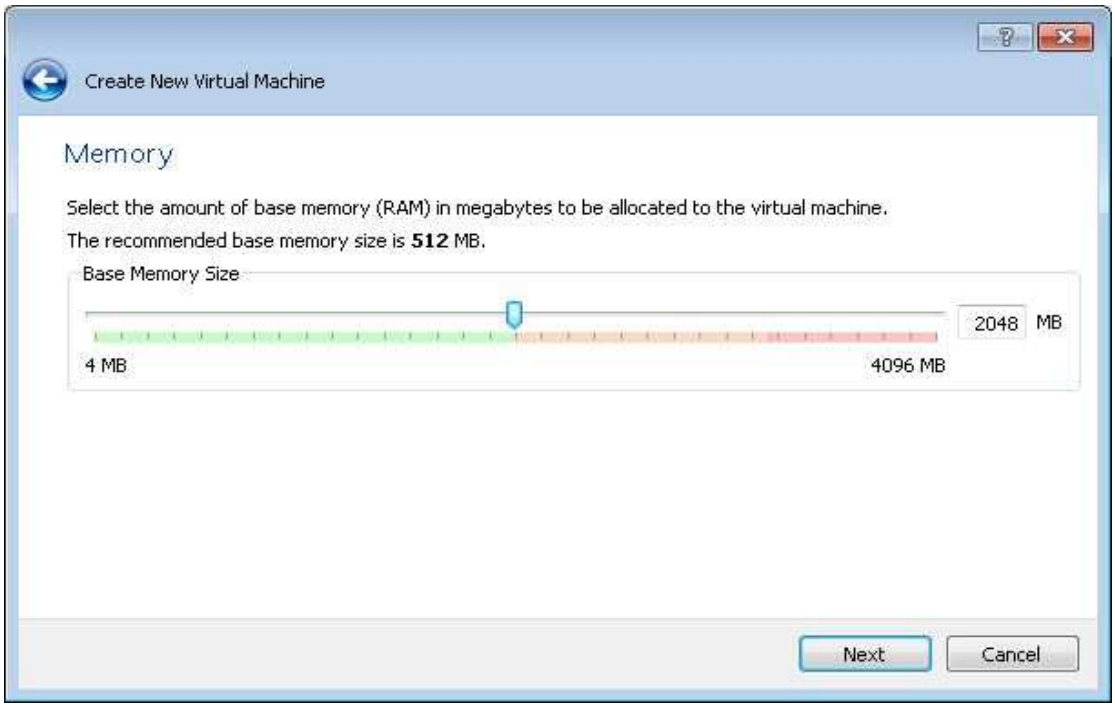
Επιλέγουμε Operating System: Linux και Version: Ubuntu. Στην συνέχεια πληκτρολογείστε το όνομα που θα έχει το μηχάνημά σας, δηλαδή BackTrack 5 Gnome και τέλος πατάτε Next.



Εικόνα 16. Καθορισμός ονόματος και τύπου Λειτουργικού Συστήματος που θα "φιλοξενηθεί"

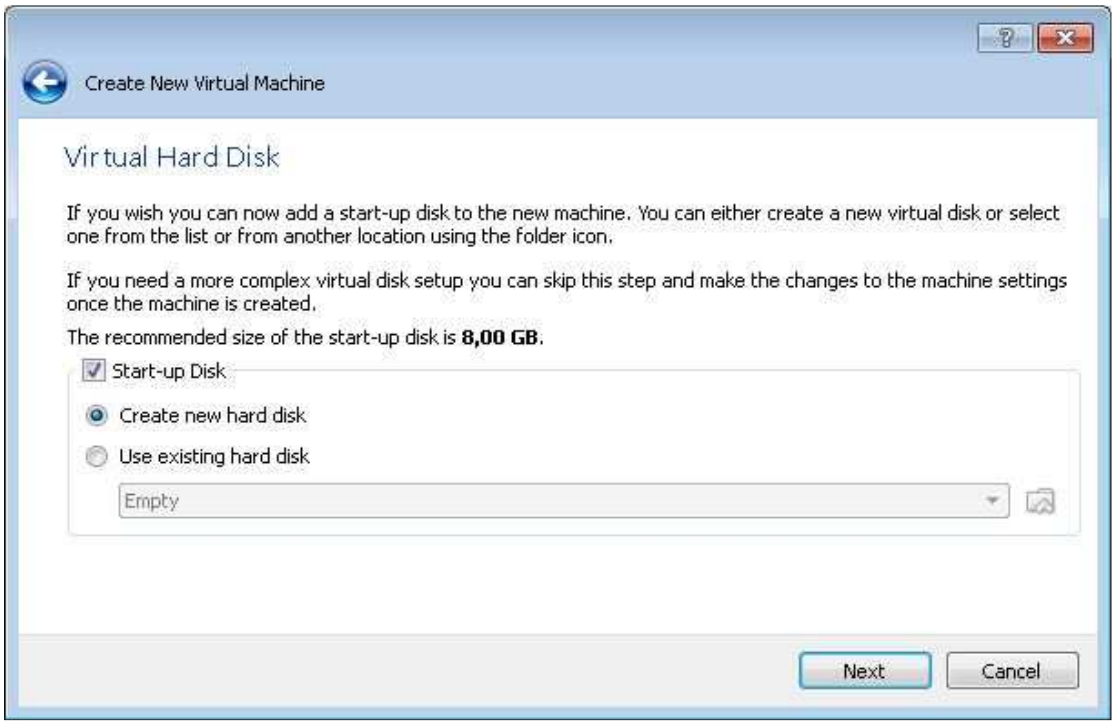
Στην συνέχεια επιλέγετε πόση μνήμη θέλετε να παραχωρήσετε στην εικονική

μηχανή (η μνήμη που θα χρησιμοποιεί το BackTrack). Μόλις επιλέξετε την μνήμη που θέλετε πατάτε Next για να συνεχίσετε παρακάτω.



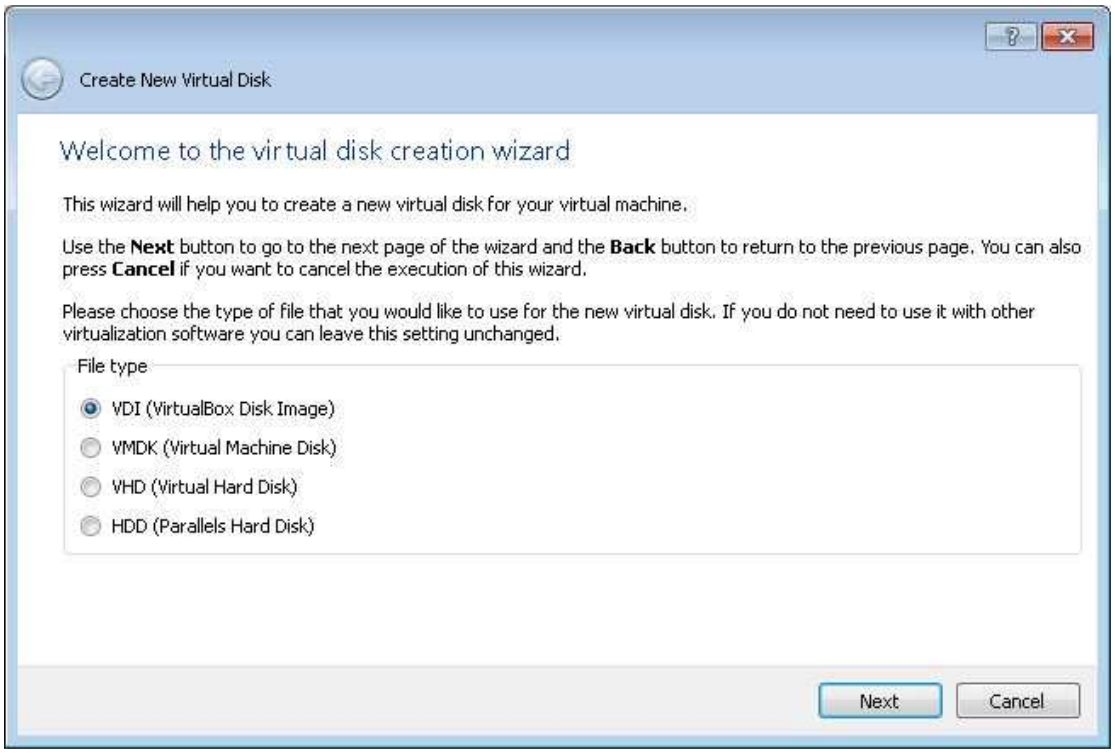
Εικόνα 17. Επιλογή μνήμης που θα χρησιμοποιηθεί από το Virtual Machine

Εφόσον έχετε καθορίσει την μνήμη που θα χρησιμοποιείτε κατά την εκτέλεση του Virtual Machine, στην επόμενη οθόνη επιλέγετε Next για να ξεκινήσει ο οδηγός με την βοήθεια του οποίου θα φτιάξετε έναν εικονικό σκληρό δίσκο γι'αυτή την μηχανή.



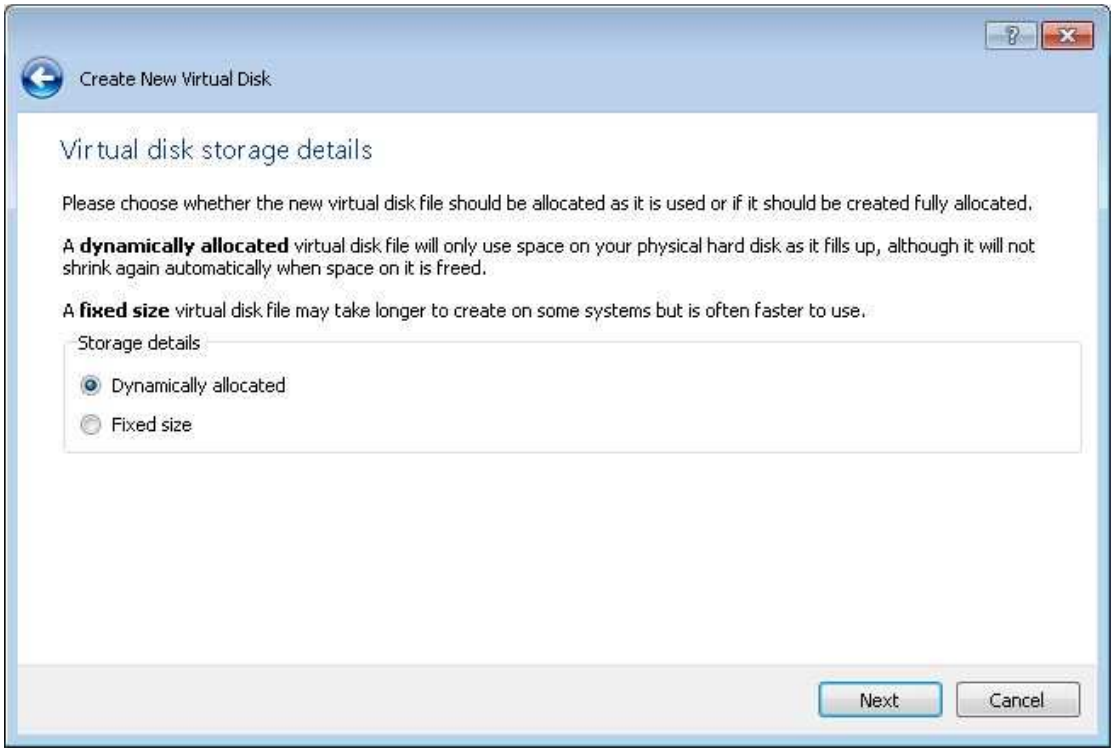
Εικόνα 18. Δημιουργία εικονικού δίσκου για την εγκατάσταση του BackTrack

Στο επόμενο παράθυρο τσεκάρετε την επιλογή VDI (VirtualBox Disk Image) και πατάτε Next.



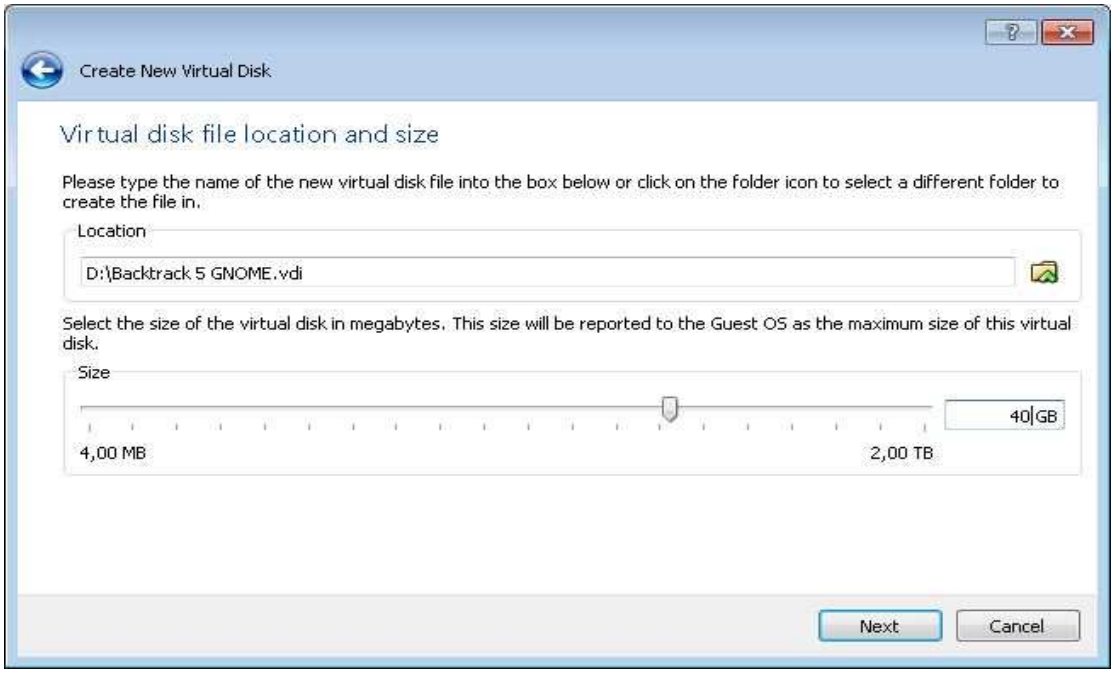
Εικόνα 19. File type - Virtual Disk Image

Στην συνέχεια τσεκάρετε την επιλογή Dynamically allocated και πατάτε Next.



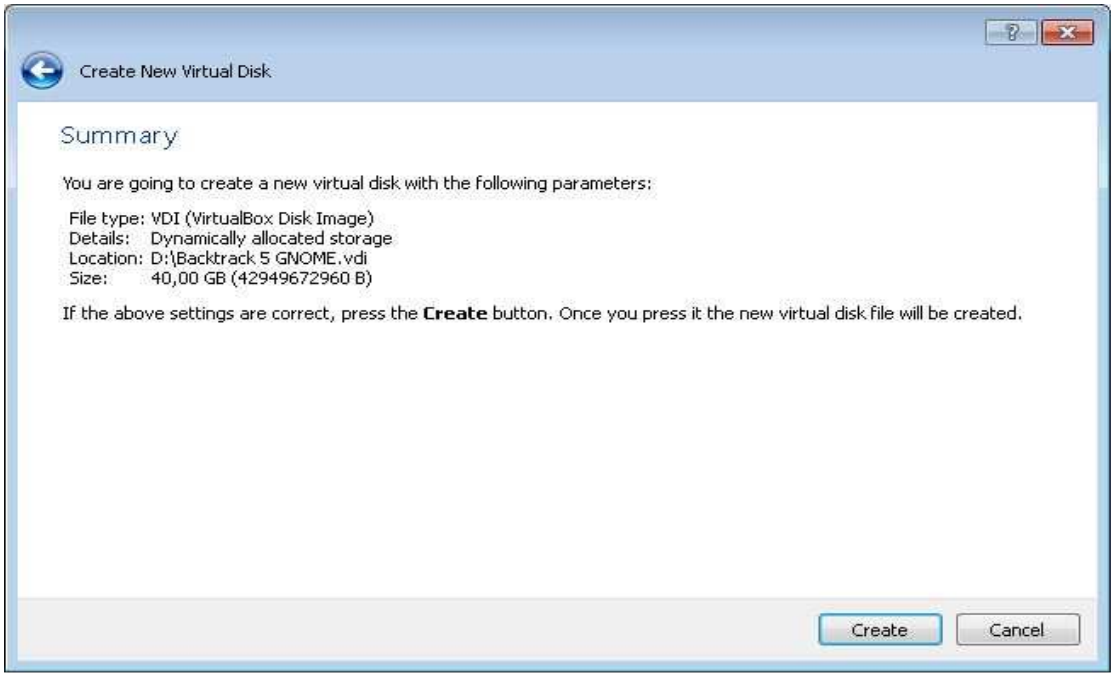
Εικόνα 20. Λεπτομέρειες εικονικού δίσκου

Στο επόμενο παράθυρο καθορίζετε δύο πράγματα. Το ένα είναι που θα αποθηκευθεί το αρχείο που αναπαριστά τον εικονικό σας σκληρό δίσκο. Το δεύτερο είναι το μέγεθος του εικονικού σας σκληρού δίσκου. Αφήνετε το Location όπως είναι ή αν θέλετε βάζετε το path της επιλογής σας (αποθηκεύεται αυτόματα στο C:\Users \Administrator\VirtualBox\HardDisks\). Τέλος εισάγετε το μέγεθος (σε GB) που θέλετε να παραχωρήσετε στον εικονικό σκληρό σας και στην συνέχεια πατάτε Next.

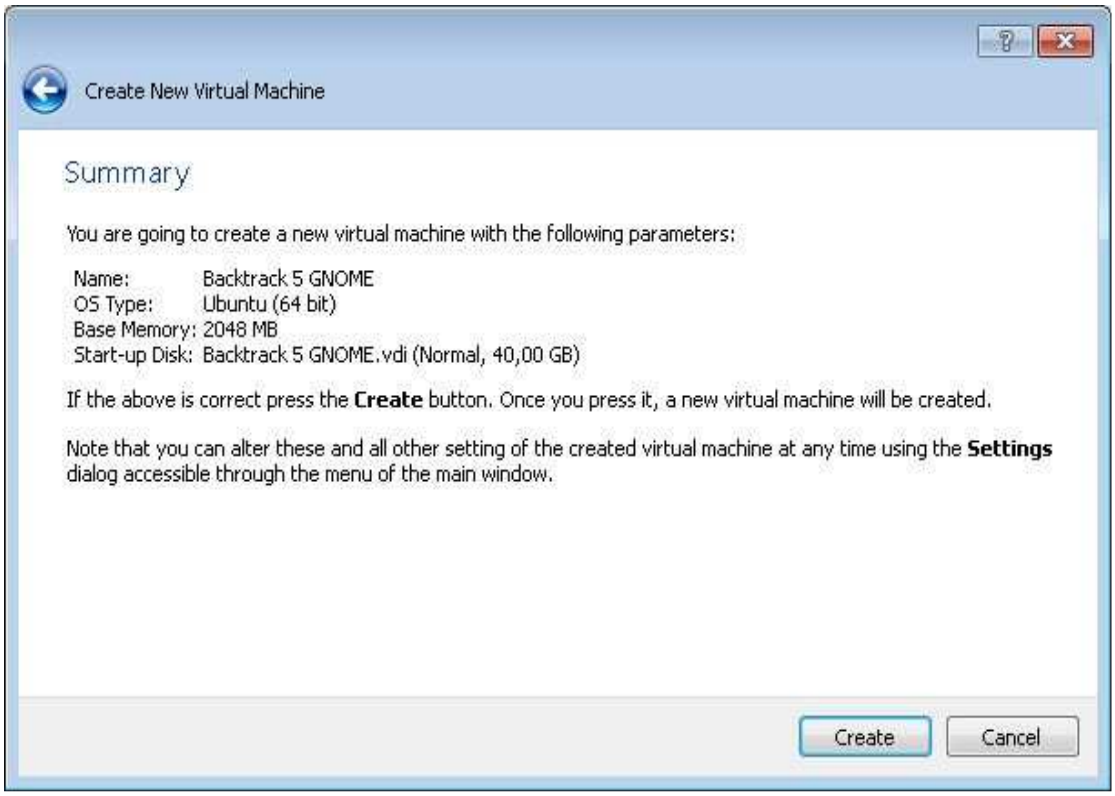


Εικόνα 21. Installation path and Size of Virtual Disk

Στα επόμενα δυο παράθυρα το πρόγραμμα θα σας επαληθεύση τις επιλογές που έχετε δώσει σχετικά με την δημιουργία του εικονικού σας δίσκου. Αν όλες οι επιλογές είναι σωστές τότε αρκεί να πατήσετε Create προκειμένου να δημιουργηθεί το εικονικό σας περιβάλλον



Εικόνα 22. Επαλήθευση επιλογών για την δημιουργία του εικονικού δίσκου (1)

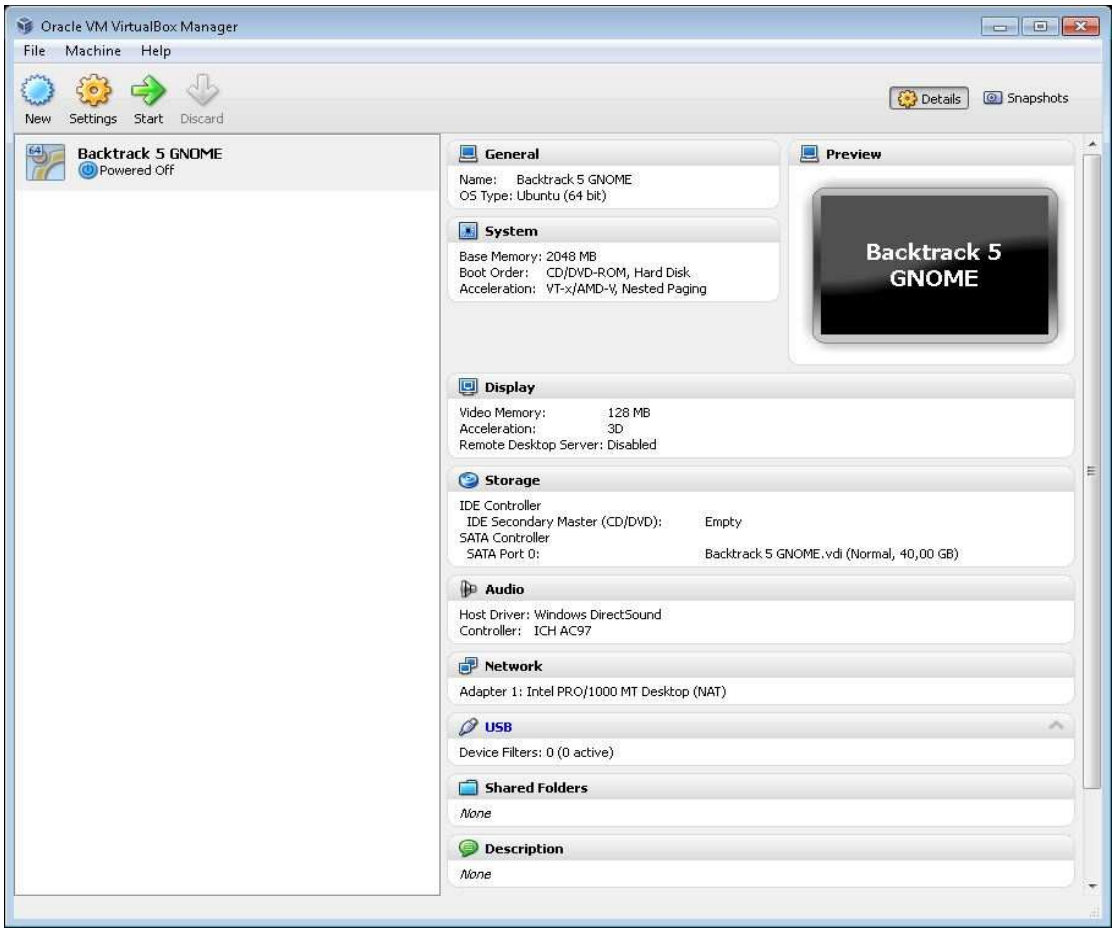


Εικόνα 23. Επαλήθευση επιλογών για την δημιουργία του εικονικού δίσκου (2)

Βήμα 2^{ο} – Εγκατάσταση BackTrack to Virtual Machine

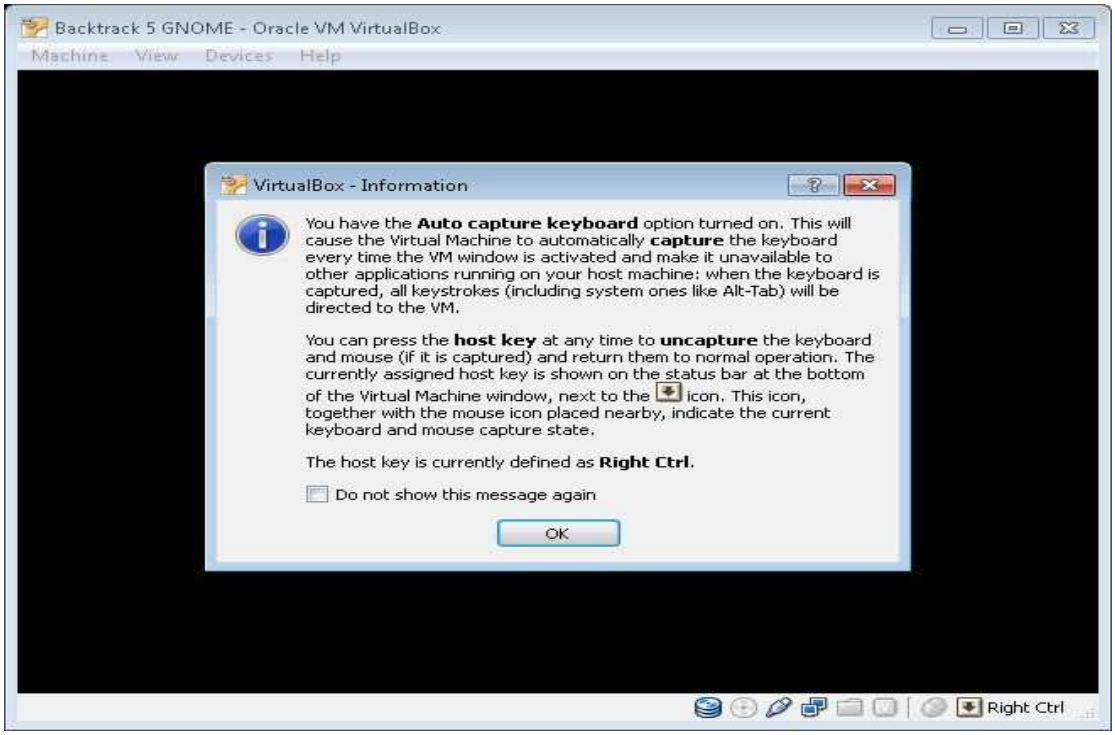
Στο βήμα αυτό ξεκίνα η διαδικασία εγκατάστασης του BackTrack στον εικονικό δίσκο. Συγκεκριμένα επιστρέφετε στην αρχική οθόνη του προγράμματος όπου έχει δημιουργηθεί η εικονική μηχανή σας. Η εικονική μηχανή έχει τα στοιχεία που φαίνονται δεξιά.

Αφού έχετε κατεβάσει την έκδοση του BackTrack σε iso είσαστε πλέον έτοιμοι να ξεκινήσετε την εγκατάσταση του λειτουργικού. Επιλέγετε την εικονική μηχανή που έχετε φτιάξει και πατάτε στο πράσινο βέλος **Start**, για να ξεκινήσει το Boot.



Εικόνα 24. Επιτυχής δημιουργία εικονικής μηχανής

Στην οθόνη λοιπόν που θα σας εμφανιστεί επιλέγετε την επιλογή "**Do not show this message again**" και στην συνέχεια πατήστε το κουμπί OK.

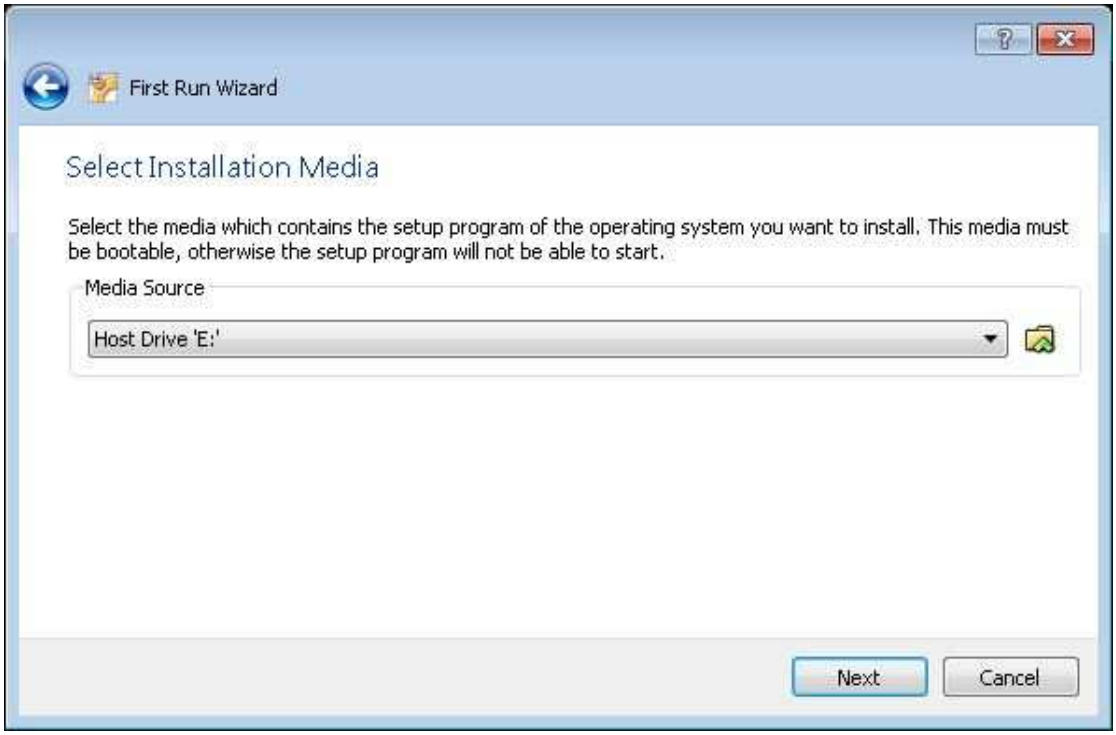


Εικόνα 25. Εγκατάσταση BackTrack στον εικονικό δίσκο

Όπως μπορείτε να δείτε έχει ξεκινήσει ο οδηγός εγκατάστασης του BackTrack στον εικονικό δίσκο. Για να προχωρήσετε παρακάτω αρκεί να πατήσετε Next.

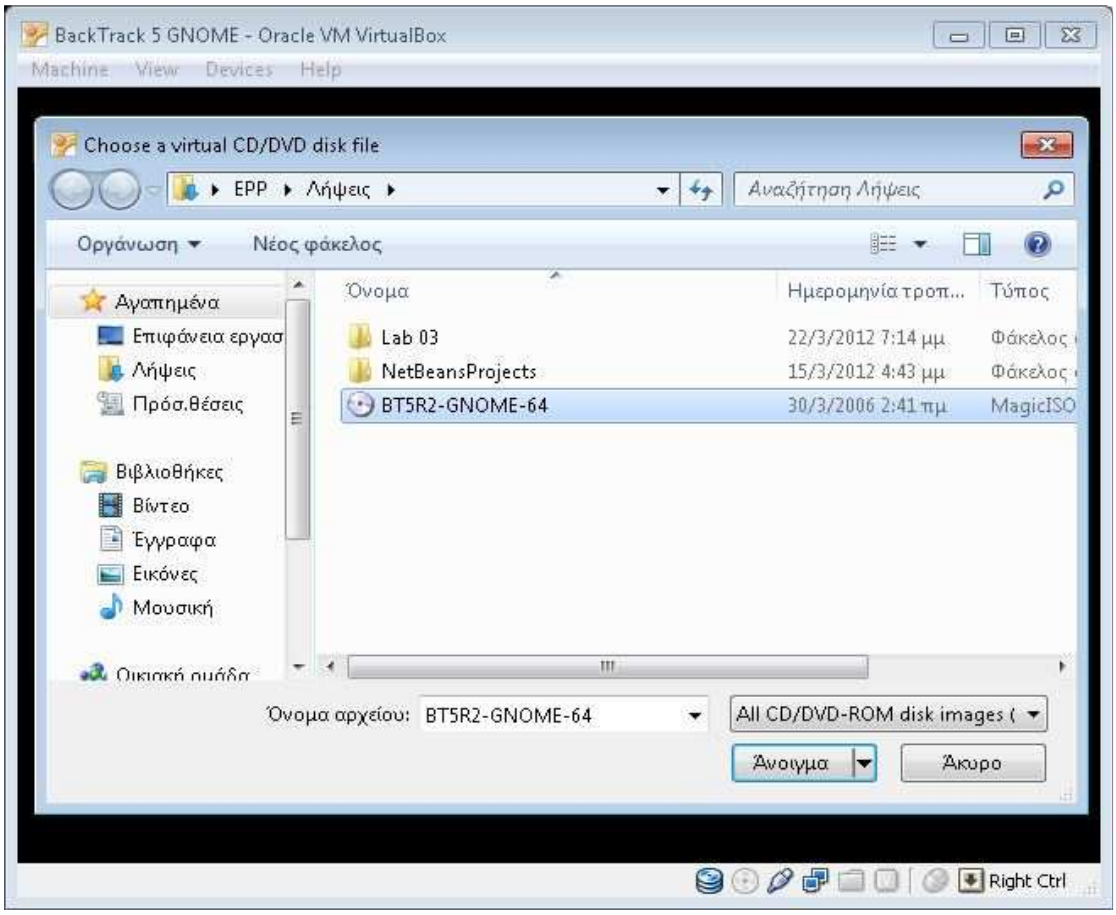
Εικόνα 26. Οδηγός εγκατάστασης για το BackTrack 5 R2

Στο επόμενο βήμα θα πρέπει να επιλέξετε το αρχείο .iso που κατεβάσατε προκειμένου να φορτωθεί στο VirtualBox και να ξεκινήσει η εγκατάσταση του λειτουργικού σας. Έτσι λοιπόν, στο "Media Source" πατάτε το κουμπί browse που βρίσκετε στα δεξιά.

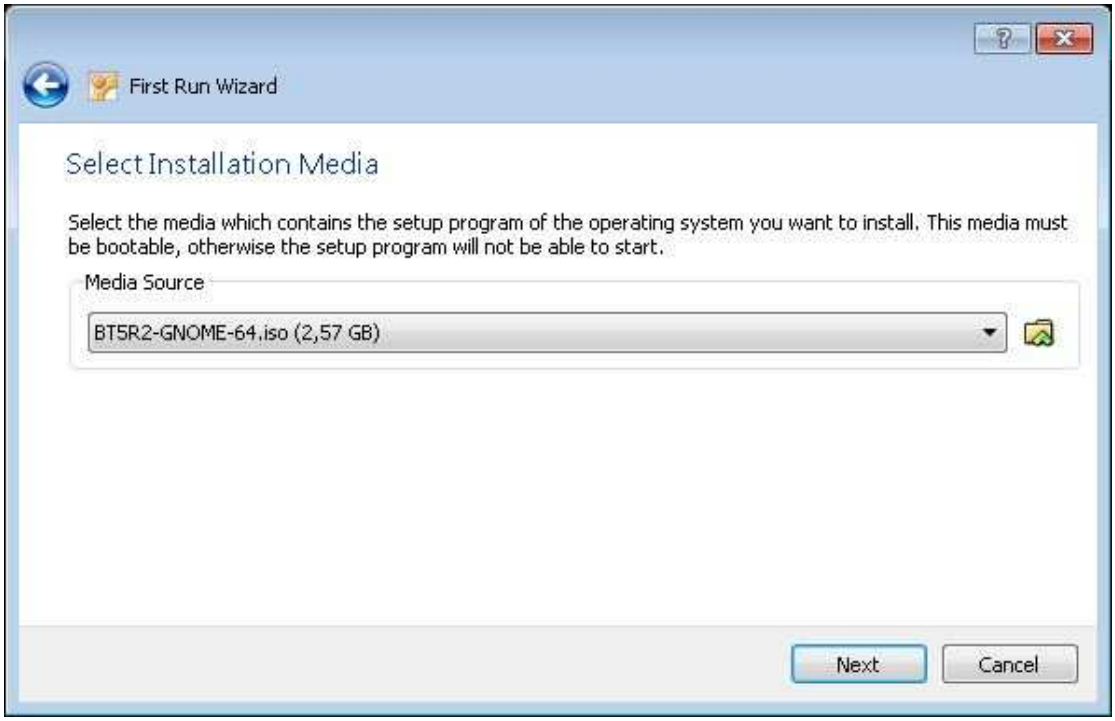


Εικόνα 27. Φόρτωμα αρχείου .iso για να ξεκινήσει η διαδικασία εγκατάστασης

Βρίσκετε το ISO αρχείο που κατεβάσατε από το site του BackTrack, το επιλέγετε και πατάτε Open.

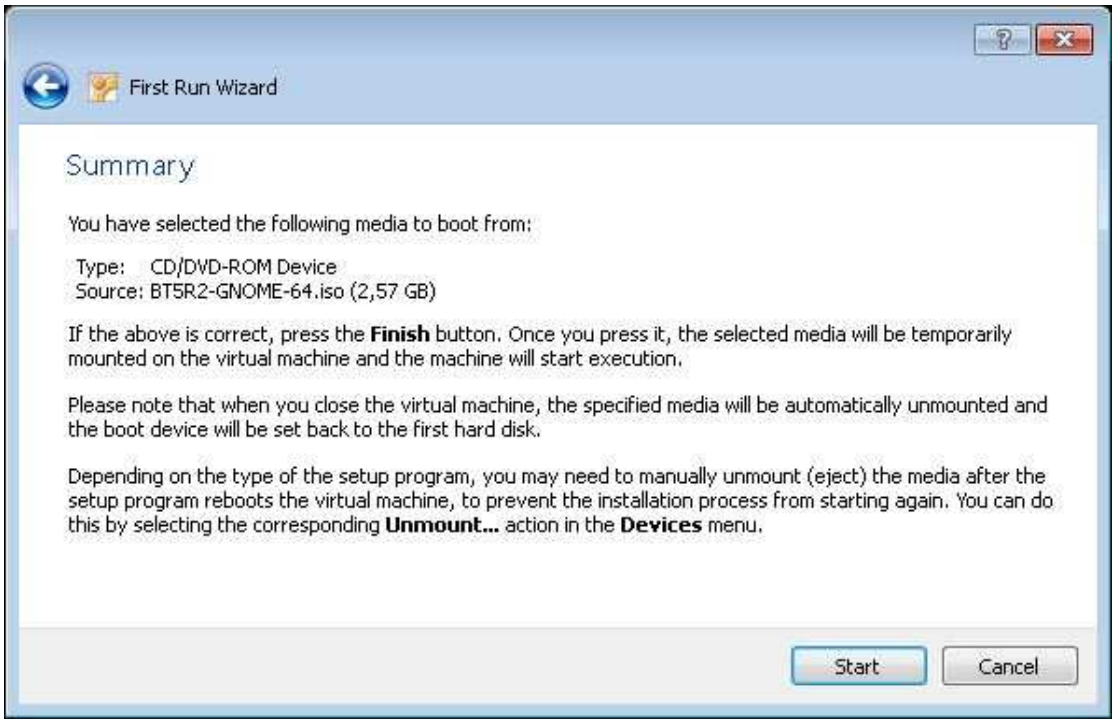


Εικόνα 28. Επιλογή αρχείου image για το ξεκίνημα της διαδικασίας εγκατάστασης

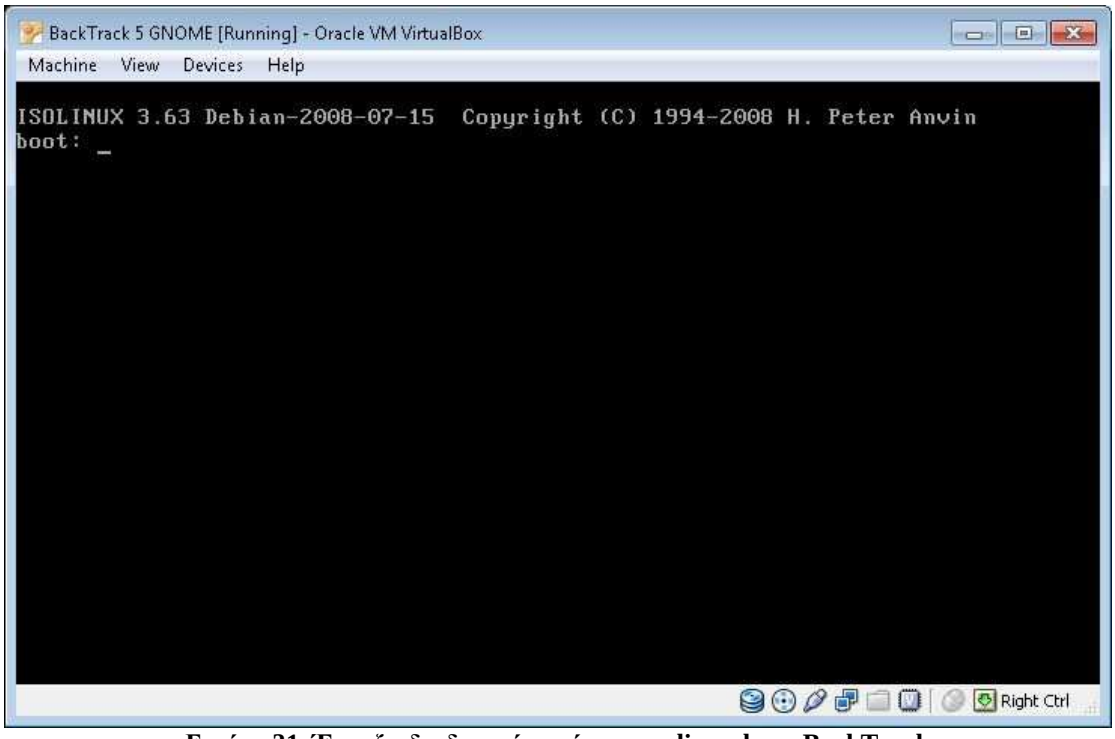


Εικόνα 29. Φόρτωση εικονικού δίσκου BackTrack

Επιλέγετε Start για να ξεκινήσει η διαδικασία εγκατάστασης του λειτουργικού συστήματος Backtrack στην εικονική μηχανή σας.



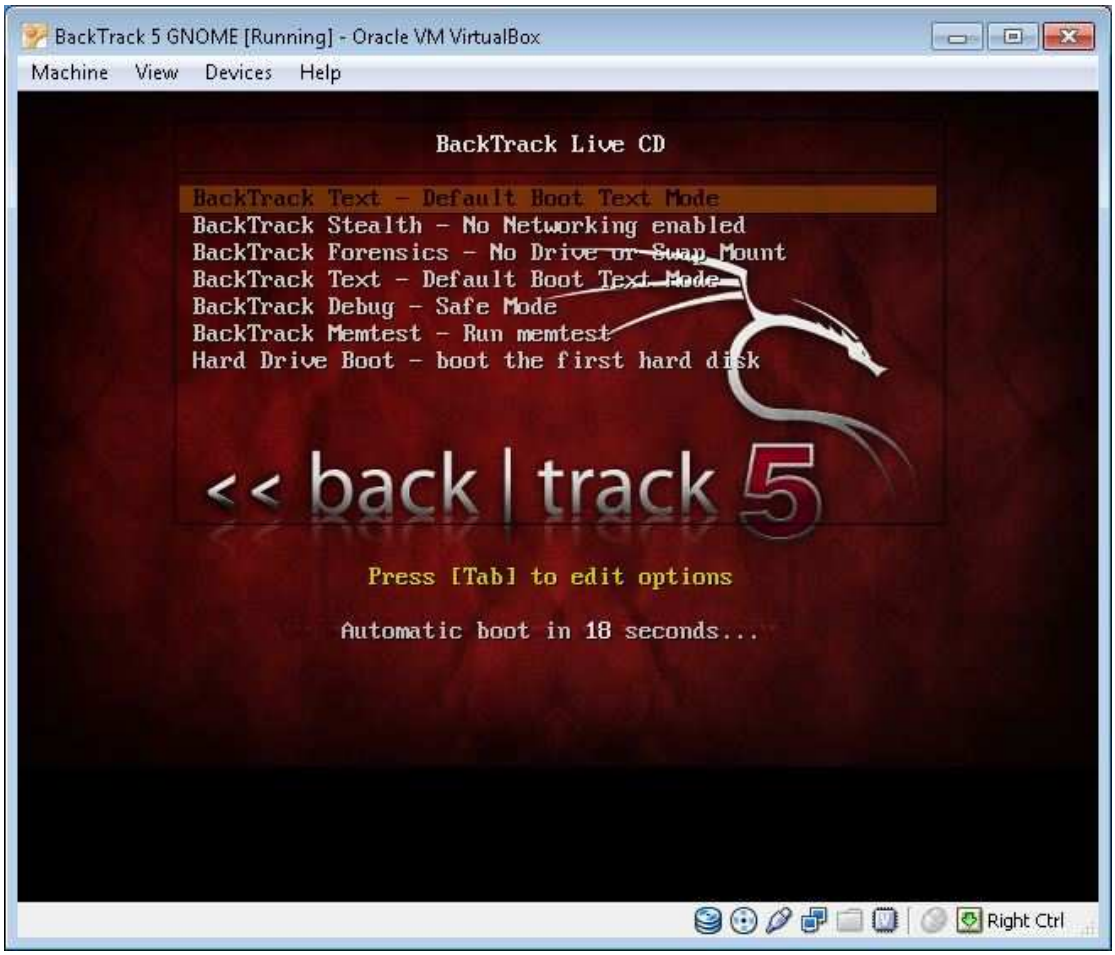
Εικόνα 30. Περίληψη λεπτομερειών εικονικού δίσκου



Εικόνα 31. Έναρξη διαδικασίας φόρτωσης live cd του BackTrack

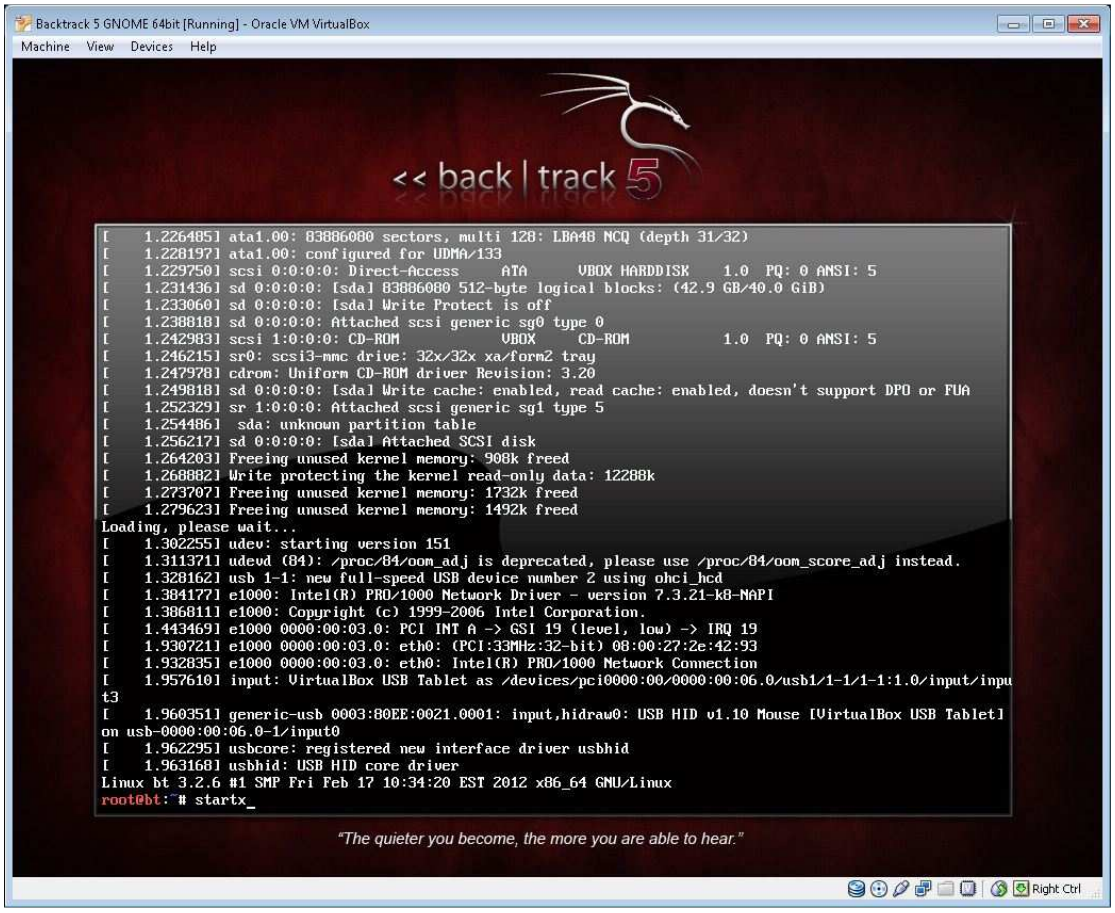
Παρακάτω βλέπετε τις επιλογές που εμφανίζονται από το Live CD.

- Η Default Boot Text Mode είναι η επιλογή που σας ενδιαφέρει για να μπορέσει να φορτώσει πλήρως το live cd με πλήρεις επιλογές.
- Η επιλογή Stealth φορτώνει το Backtrack χωρίς δυνατότητα δικτύου
- Η Text επιλογή σας φορτώνει το Backtrack μόνο με δυνατότητα command prompt.
- Η επιλογή Debug φορτώνει το Backtrack σε Safe Mode
- Το Memtest εκτελεί κάποια τεστ για τη μνήμη RAM του υπολογιστή
- Με την επιλογή Hard Drive Boot το live cd αφήνει να γίνει φόρτωση όποιου λειτουργικού υπάρχει ήδη εγκατεστημένο στο σκληρό δίσκο.



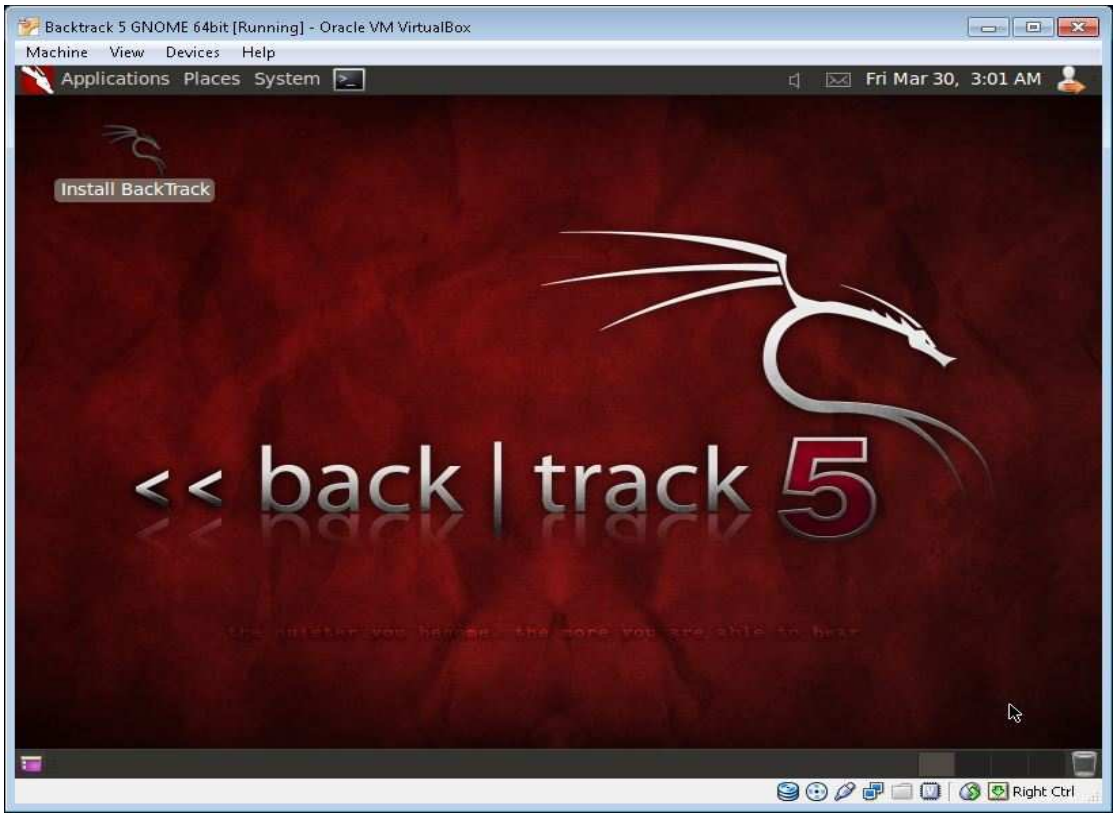
Εικόνα 32. Μενού επιλογών φόρτωσης του Backtrack Live CD

Όπως μπορείτε να δείτε και παρακάτω το VirtualBox έχει φορτώσει πλήρως το αρχείο .iso του BackTrack και είναι έτοιμο για χρήση (το BackTrack λειτουργεί και ως Live CD οπότε μπορείτε να το χρησιμοποιήσετε και χωρίς εγκατάσταση). Για να ξεκινήσει η εγκατάσταση λοιπόν, πρέπει να μπείτε αρχικά στο γραφικό περιβάλλον του BackTrack. Για να γίνει αυτό αρκεί να πληκτρολογήσετε την εντολή **startx** όπως μπορείτε να δείτε και παρακάτω.



Εικόνα 33. Εισαγωγή στο γραφικό περιβάλλον του BackTrack

Εφόσον μπείτε στο γραφικό περιβάλλον του BackTrack, θα δείτε στην επάνω αριστερή γωνία το εικονίδιο **Install BackTrack**. Για να ξεκινήσει λοιπόν η εγκατάσταση θα πρέπει να πατήσετε διπλό κλικ στο εικονίδιο της εγκατάστασης.



Εικόνα 34. Ξεκίνημα διαδικασίας εγκατάστασης BackTrack to Virtual Machine

Έχοντας ξεκινήσει η διαδικασία εγκατάστασης στο πρώτο βήμα θα πρέπει να επιλέξετε την γλώσσα εγκατάστασης του BackTrack.

Εικόνα 35. Επιλογή γλώσσας εγκατάστασης BackTrack

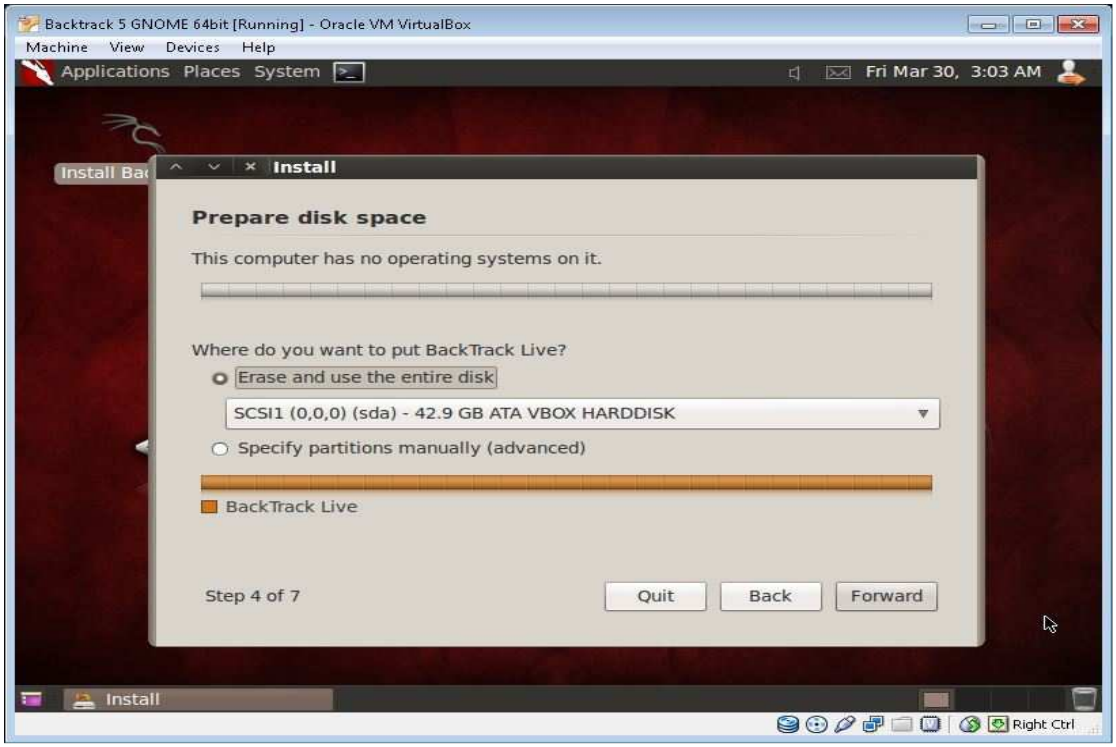
Στην συνέχεια επιλέγετε την ζώνη ώρας με βάση την τοποθεσία και την χώρα που είσαστε.

Εικόνα 36. Select Region and Time Zone

Στο επόμενο βήμα διαλέγετε την διάταξη που θέλετε να έχει το πληκτρολόγιό σας.

Εικόνα 37. Keyboard layout

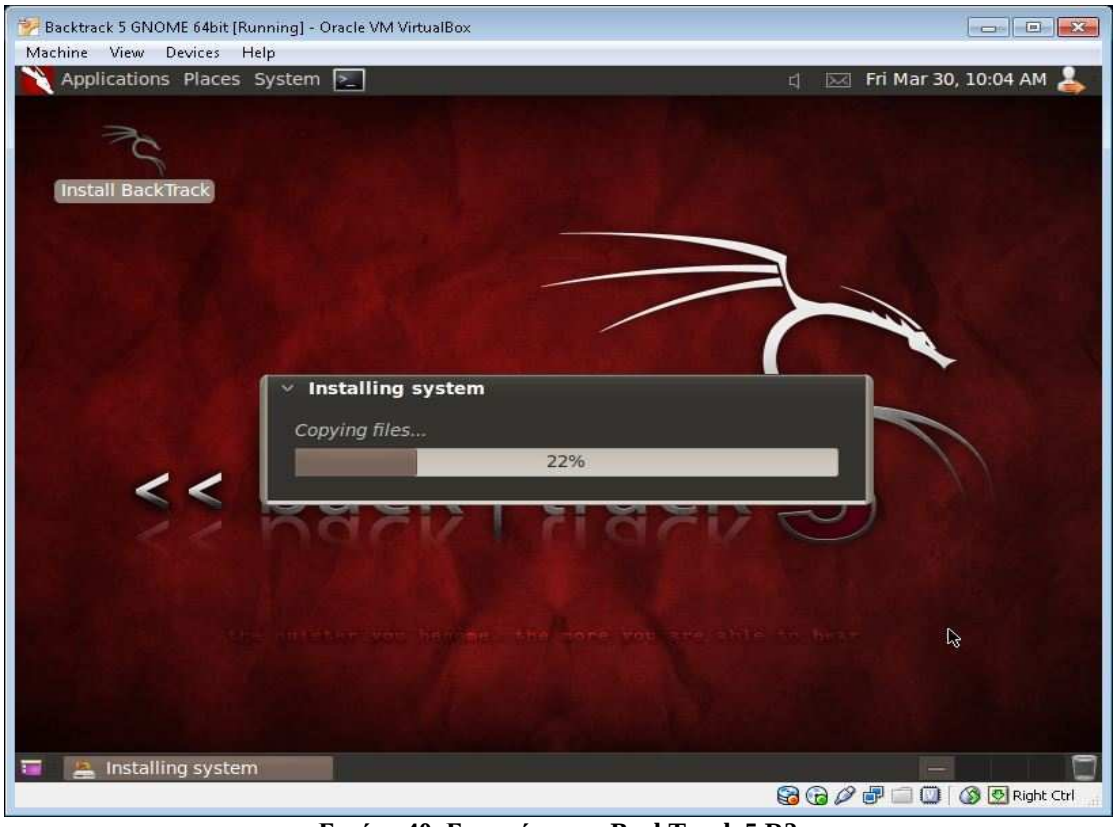
Το επόμενο βήμα είναι και το σημαντικότερο. Σας λέει που θέλετε να εγκαταστήσετε το BackTrack. Όπως μπορείτε να προσέξετε και παρακάτω πρόκειται να χρησιμοποιήσει όλο τον εικονικό δίσκο που είχατε φτιάξει στην αρχή.



Εικόνα 38. Επιλογή εικονικού δίσκου για την εγκατάσταση του BackTrack

Έχοντας επιλέξει τον εικονικό σας δίσκο το λειτουργικό σας σύστημα είναι πια έτοιμο για εγκατάσταση.

Εικόνα 39. BackTrack - Ready to Install



Εικόνα 40. Εγκατάσταση BackTrack 5 R2

Τέλος μόλις τελειώσει την εγκατάσταση του λειτουργικού συστήματος θα σας ζητηθεί από το πρόγραμμα να κάνετε επανεκκίνηση για την ολοκλήρωση της εγκατάστασης.

Εικόνα 41. Επανεκκίνηση συστήματος για την ολοκλήρωση εγκατάστασης

1.4 Install BackTrack Live to USB

Στο υποκεφάλαιο αυτό, θα δείξουμε με απλά βήματα πως μπορείτε να δημιουργήσετε ένα **bootable flash-drive** για το BackTrack 5 R2. Η μέθοδος αυτή είναι πολύ απλή αφού το μόνο που θα χρειαστείτε είναι η έκδοση του BackTrack 5 R2 σε μορφή ISO καθώς και το πρόγραμμα Unebootin.

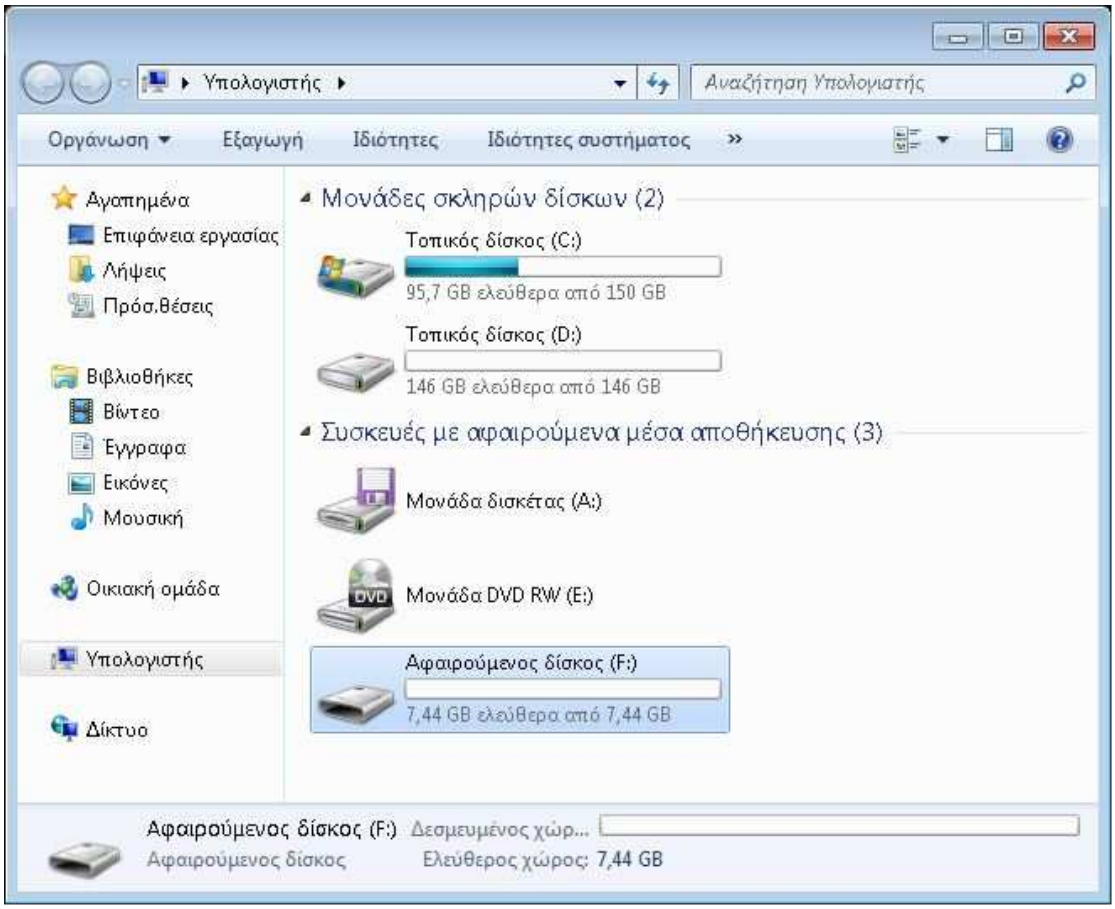
Βήμα 1^{ο} – Σύνδεση USB

Αρχικά αυτό που έχετε να κάνετε είναι να συνδέσετε το USB σας πάνω στο μηχάνημά σας.

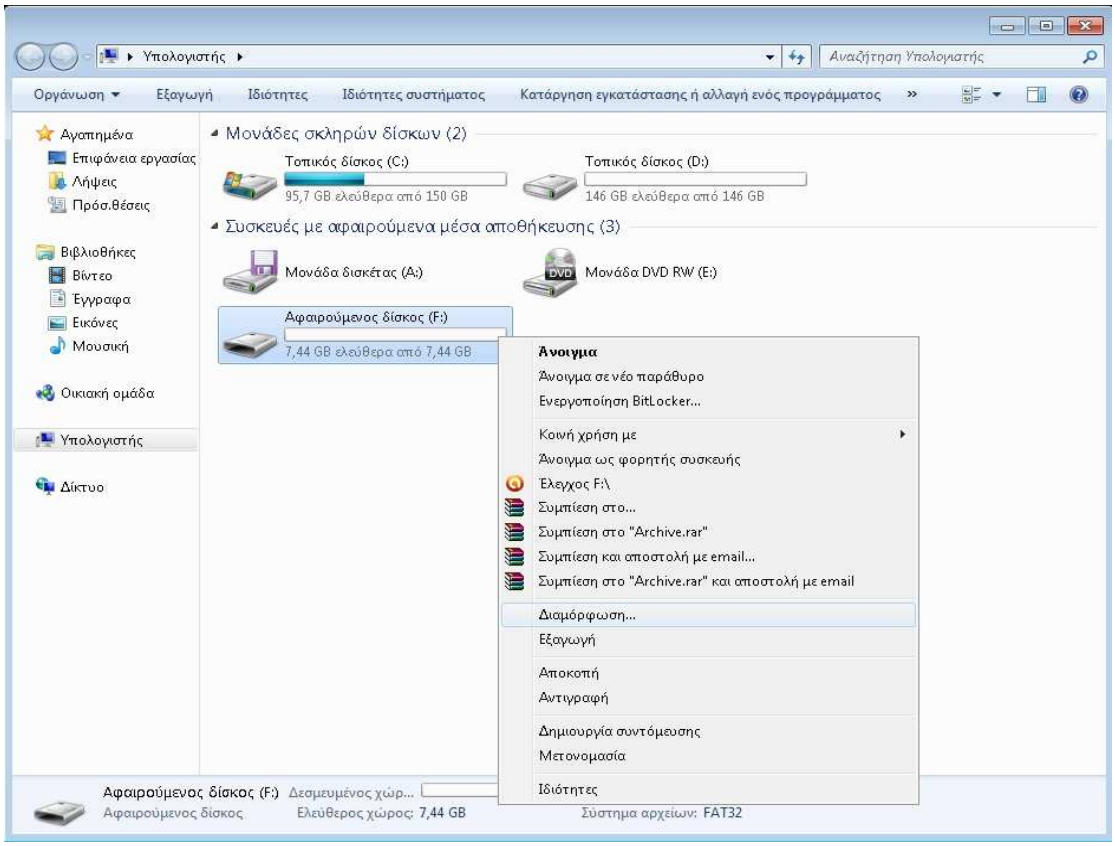
Σημείωση: *Για να εγκατασταθεί το BackTrack 5 απαιτείται το USB να έχει σαν ελάχιστη χωρητικότητα τα 2 GB.*

Βήμα 2^{ο} – Διαμόρφωση USB

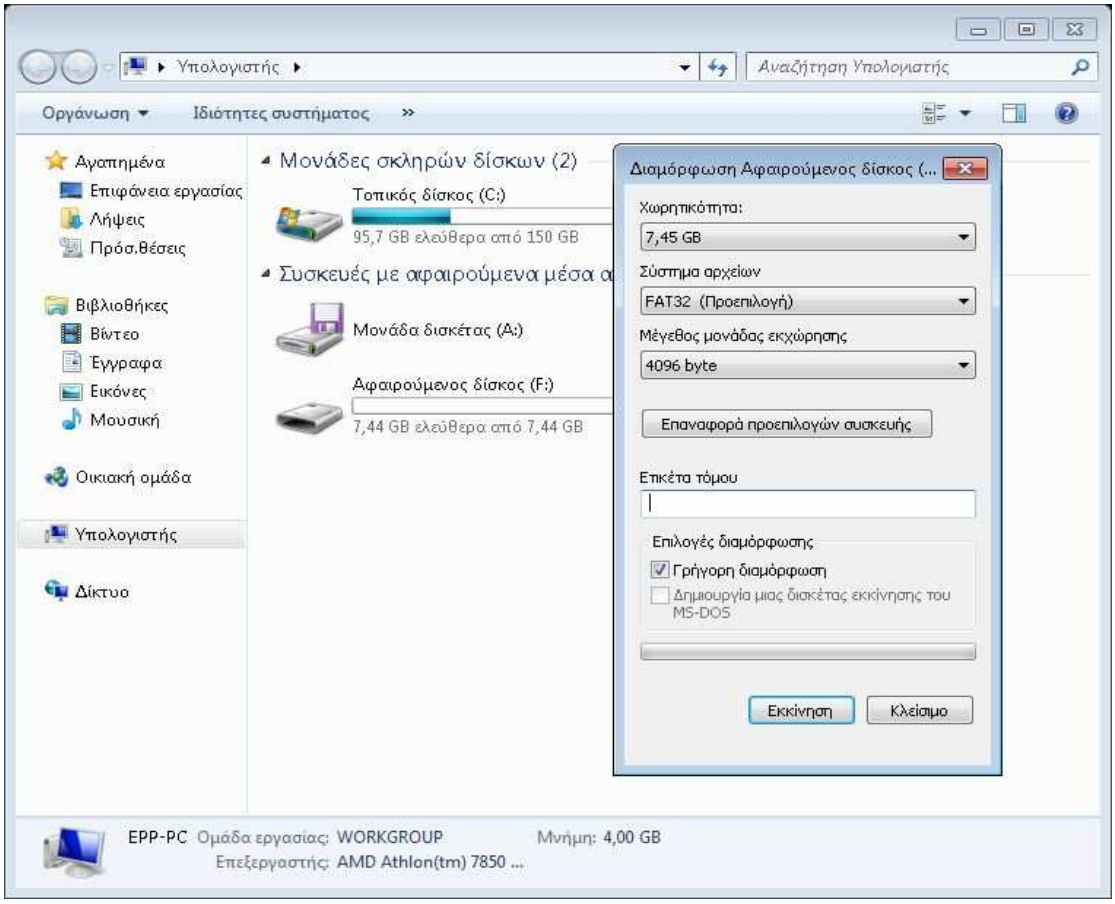
Στην συνέχεια, όπως μπορείτε να δείτε και παρακάτω στα Screenshots που ακλουθούν θα πρέπει να διαμορφώσετε το USB σε σύστημα αρχείων FAT32.



Εικόνα 42. Διαμόρφωση δίσκου USB



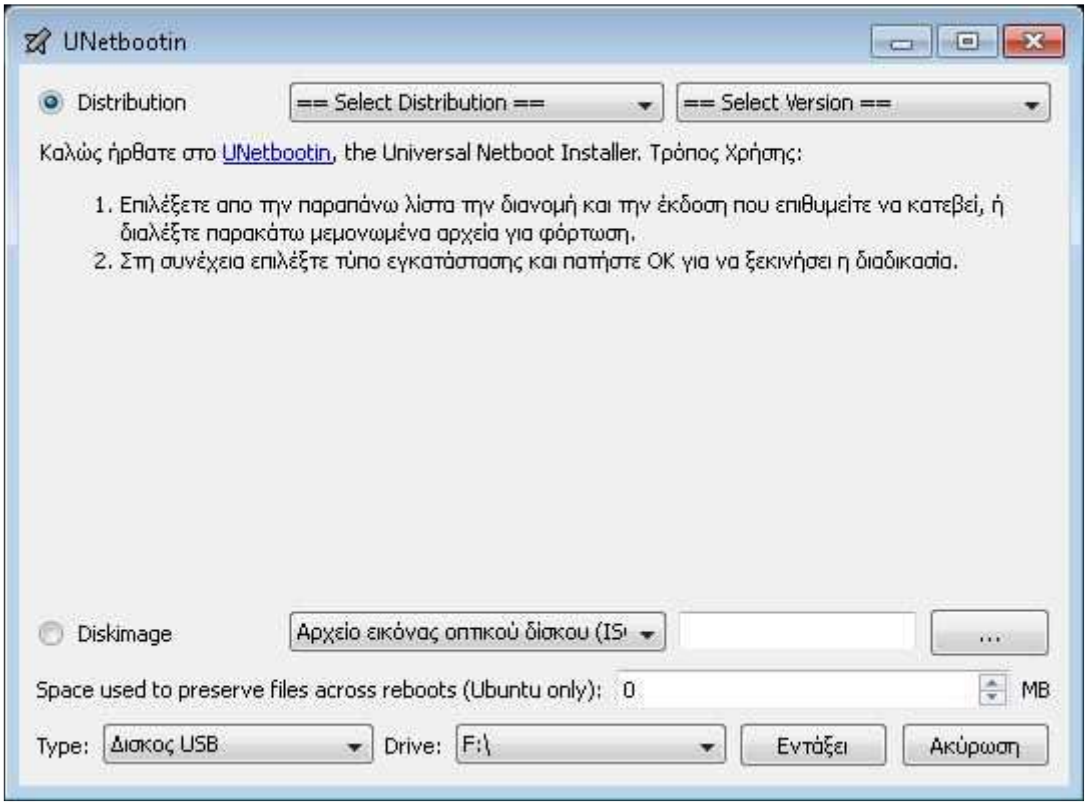
Εικόνα 43. Διαμόρφωση δίσκου USB (2)



Εικόνα 44. Διαμόρφωση δίσκου USB σε συστημα αρχειων FAT32

Βήμα 3ο – Download Unetbootin

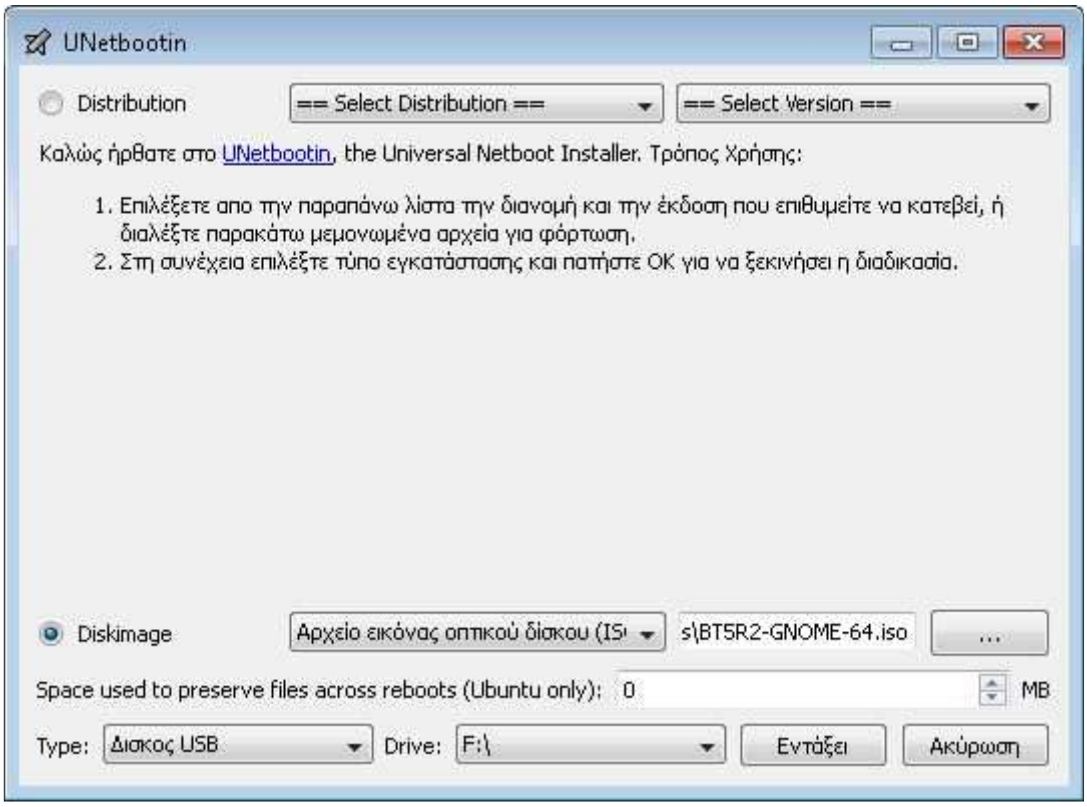
Το Unetbootin είναι ένα εργαλείο δημιουργίας Live USB που μπορεί να χρησιμοποιηθεί για την δημιουργία ενός Live Linux USB flash drive από ένα αρχείο ISO. Πολλές διανομές Linux υποστηρίζονται εξ ορισμού, ενώ υπάρχουν ειδικές επιλογές εγκατάστασης για διανομές που δεν υποστηρίζονται. Είναι σημαντικό να αναφέρουμε ότι Live Linux USB flash drives που δημιουργούνται μ' αυτό το εργαλείο θα λειτουργεί ακριβώς όπως κι ένα Live CD. Το UNetbootin είναι διαθέσιμο στη διεύθυνση http://unetbootin.sourceforge.net/



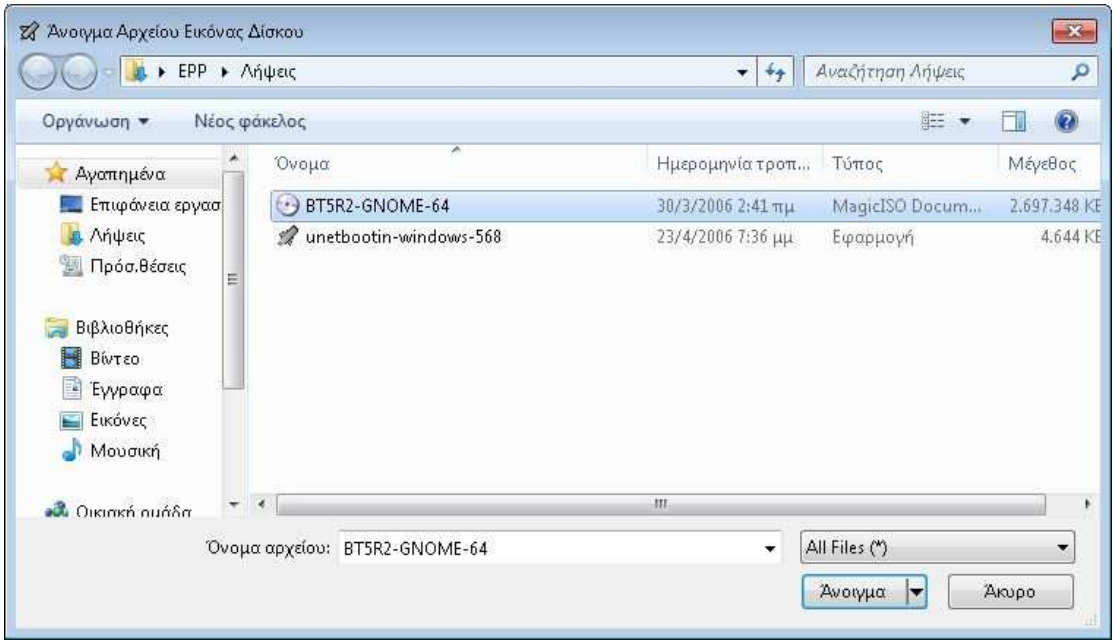
Εικόνα 45. UNetbootin

Βήμα 4ο – Εγκατάσταση BackTrack σε USB με χρήση UNetbootin

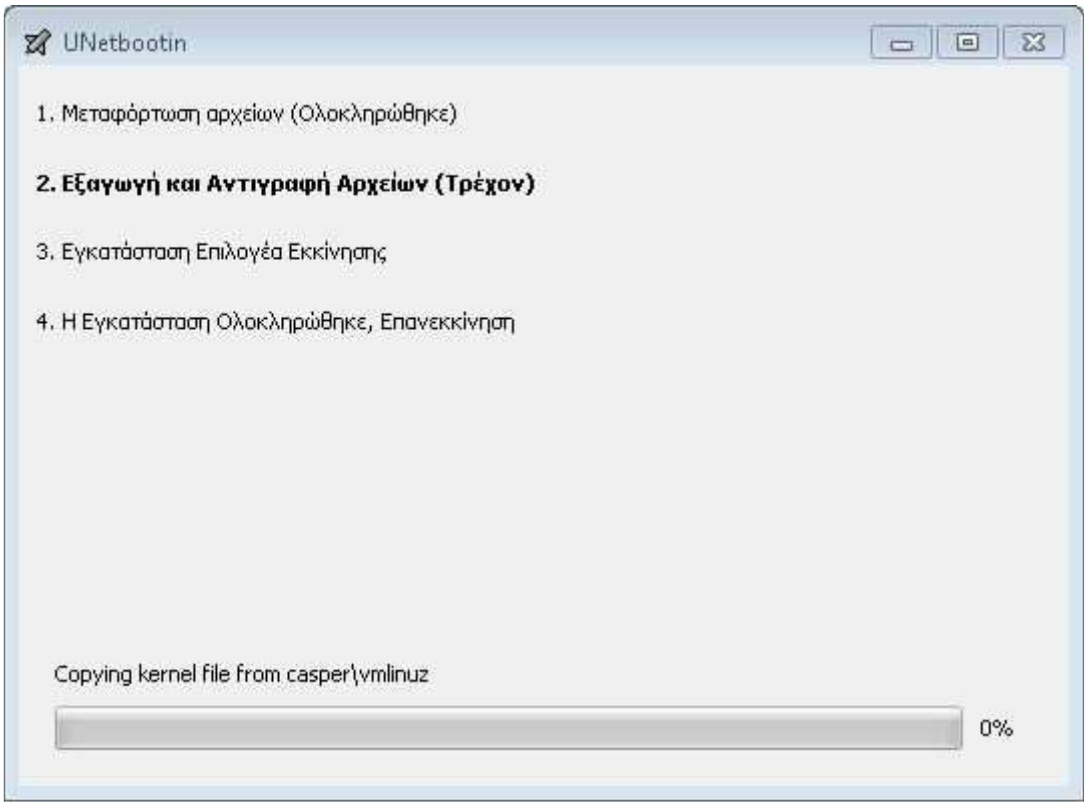
Στο βήμα αυτό τα πράγματα είναι ακόμα πιο απλά. Τρέχετε το UNetbootin (στα Windows δεν χρειάζεται εγκατάσταση) και αφού ανοίξει επιλέγετε το Disk Image καθώς και το Drive στο οποίο αντιστοιχεί το USB Stick σας. Έπειτα κάνετε Browse για να επιλέξετε το αρχείο .ISO που έχετε κατεβάσει και πατάτε OK για να ξεκινήσει η μεταφορά των αρχείων στο USB. Όταν ολοκληρωθεί η διαδικασία μπορείτε να πατήσετε exit αφού η επανεκκίνηση δεν είναι απαραίτητη. Αν όλα έχουν γίνει σωστά και έχετε ρυθμίσει τον υπολογιστή από τα Bios Settings να κάνει boot από USB, θα μπορείτε να τρέξετε το BackTrack 5 R2.



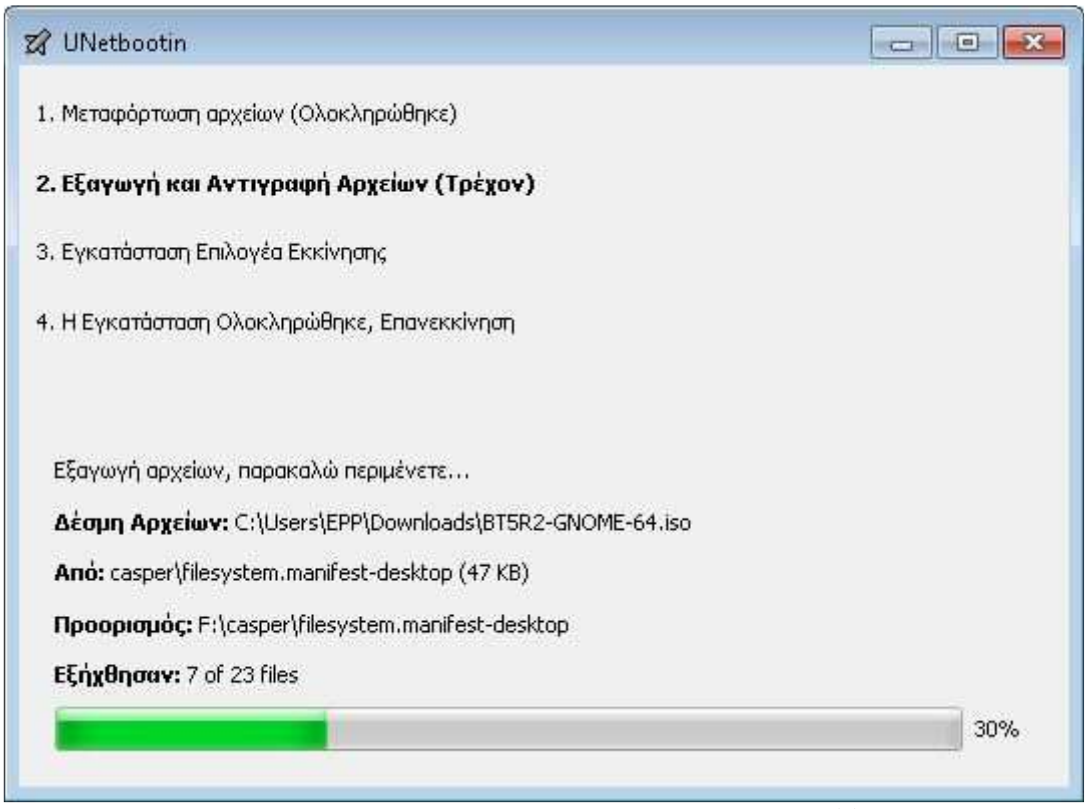
Εικόνα 46. Browse αρχείου .iso και επιλογή Drive



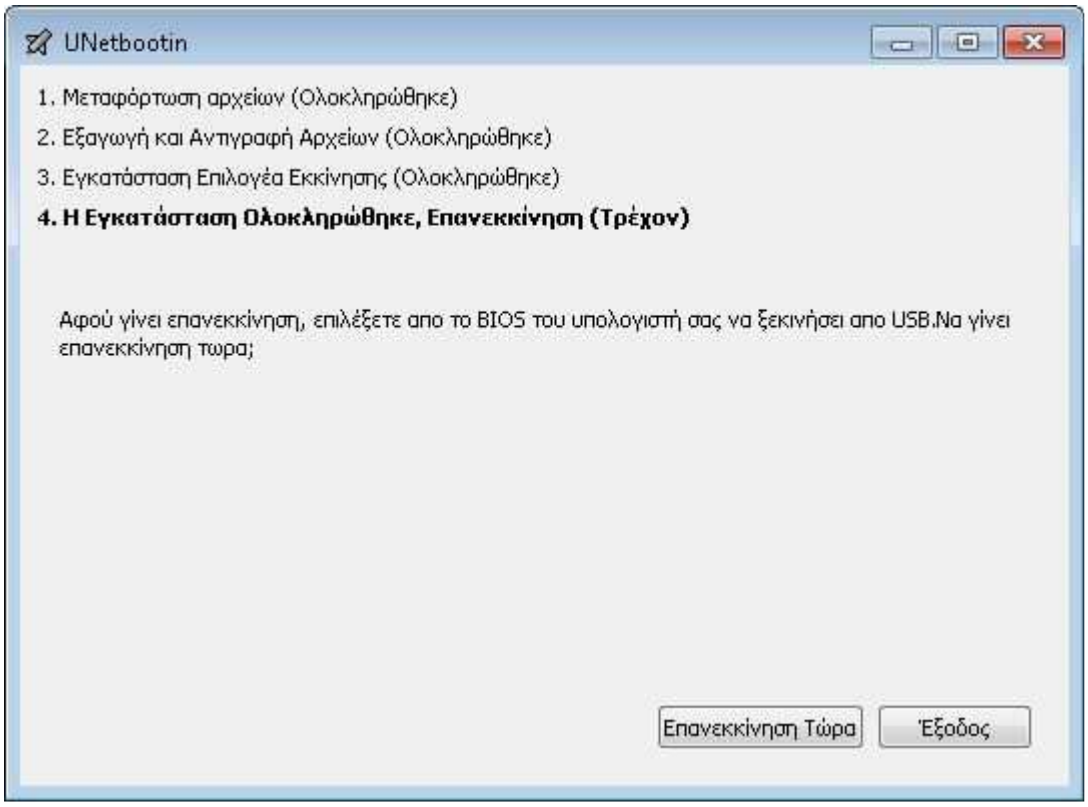
Εικόνα 47. Επιλογή αρχείου image



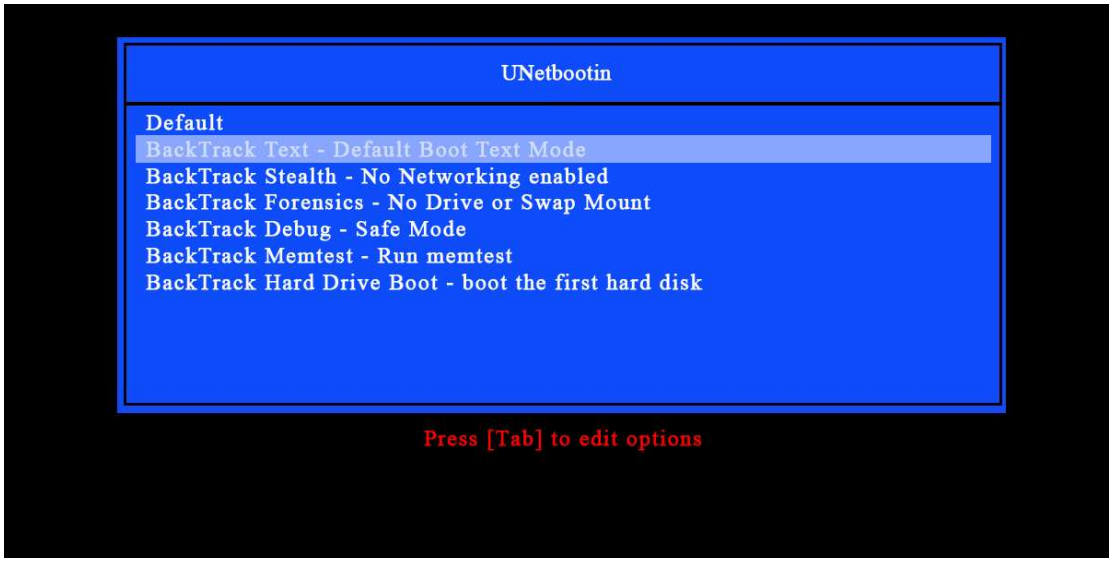
Εικόνα 48. Διαδικασία αντιγραφής αρχείων στο USB



Εικόνα 49. Διαδικασία αντιγραφής αρχείων στο USB (2)



Εικόνα 50. Ολοκλήρωση διαδικασία εγκατάστασης BackTrack σε USB



Εικόνα 51. Επιλογές εκκίνησης BackTrack από USB

1.5 Unix Live CD

Η λειτουργία του Live CD[1] βασίζεται στην δημιουργία ενός εικονικού δίσκου στη μνήμη RAM του υπολογιστή, από τον οπτικό δίσκο όταν φορτώνει. Δηλαδή ουσιαστικά δημιουργείται ένα RAM Disk το οποίο λειτουργεί σαν σκληρός δίσκος. Αυτό έχει σαν αποτέλεσμα αφού δεσμεύεται κάποιο μέρος της RAM από το Live CD να μειώνεται η διαθέσιμη χωρητικότητα της RAM για τις εφαρμογές που θα τρέχουν από το «λειτουργικό σύστημα».

Γενικά η χρήση των Live CD επιτρέπει την χρήση προεγκατεστημένων προγραμμάτων που υπάρχουν σε αυτό, την πλοήγηση στο διαδίκτυο, τη δημιουργία αρχείων, παίξιμο video games, δοκιμές δικτύου και ασφάλειας, δοκιμές hardware κλπ.

Η αποθήκευση των αρχείων που δημιουργεί και αποθηκεύει ο χρήστης με τη χρήση ενός Live CD μπορεί να γίνει σε οποιοδήποτε αποθηκευτικό χώρο όπως USB drive, δικτυακό δίσκο, partition σκληρού δίσκου ή άλλο προσβάσιμο αποθηκευτικό χώρο.

Κατά συνέπεια η αποθήκευση αρχείων στο «λειτουργικό σύστημα» που φορτώνεται από το Live CD δεν ενδείκνυται γιατί από τη στιγμή που αυτό λειτουργεί μέσω RAM disc, όταν τερματιστεί η λειτουργία του όλα τα δεδομένα θα χαθούν.

[1] http://en.wikipedia.org/wiki/Live_CD

2. Κεφάλαιο – Σουίτα εργαλείων Aircrack-ng

2.1 Aircrack-ng Suite

Το Aircrack-ng είναι ένα δυνατό λογισμικό που σχεδιάστηκε για να αποκωδικοποιεί κωδικούς πρόσβασης ενός δικτύου. Πώς είναι δυνατό αυτό; Το εργαλείο αυτό αποσπά πακέτα πληροφοριών, στη συνέχεια τα αναλύει και σε λίγα λεπτά, το πρόγραμμα σας δίνει τον κωδικό πρόσβασης που αναζητούσατε. Είναι πολύ αποτελεσματικό και αν ο υπολογιστής, από τον οποίο αποσπώνται τα δεδομένα δεν είναι κατάλληλα ασφαλισμένος, τότε μπορεί να αποσπάσει τις ζητούμενες πληροφορίες χωρίς κανένα πρόβλημα.

Υπάρχουν δύο τρόποι για να χρησιμοποιηθούν τα πακέτα πληροφοριών που αποσπάστηκαν από άλλα δίκτυα: Ο πρώτος τρόπος είναι η αυτόματη απόσπαση με ανίχνευση της κάρτας σας χωρίς να χρειάζεται να καθορίσετε τίποτα. Και ο δεύτερος είναι για εντοπισμένη έρευνα.

Αυτό το ισχυρό εργαλείο που ονομάζεται Aircrack-ng είναι το σωστό είδος λογισμικού που χρειάζεστε για να γνωρίζετε τους κωδικούς πρόσβασης άλλων δικτύων. Αξιοποιώντας λοιπόν πλήρως όλα τα εργαλεία της Suite Aircrack-ng είναι θέμα χρόνου να έχετε πρόσβαση σε οποιοδήποτε δίκτυο.

Η Suite Aircrack-ng περιλαμβάνει όλα τα παρακάτω χρήσιμα προγράμματα, οπού θα δούμε και θα αναλύσουμε στην συνέχεια του κεφαλαίου καθένα από αυτά ξεχωριστά:

- Airbase-ng
- Aircrack-ng
- Airdecap-ng
- Airdecloak-ng
- Airdriver-ng
- Airdrop-ng
- Aireplay-ng
- Airgraph-ng
- Airmon-ng
- Airodump-ng
- Airolib-ng
- Airserv-ng
- Airtun-ng
- Easside-ng
- Packetforge-ng
- Tkiptun-ng
- Wesside-ng

2.1.1 Airbase-ng

Το Airbase-ng είναι ένα εργαλείο πολλαπλών χρήσεων με στόχο την επίθεση σε Clients, σε αντίθεση με την επίθεση σε κάποιο Access Point (AP). Η βασική ιδέα της εφαρμογής είναι να ενθαρρύνει με κάποιον τρόπο τους Clients να συνδεθούν στο ψεύτικο AP που θα δημιουργηθεί σε αντίθεση με τα πραγματικό. Δεδομένου ότι είναι τόσο ευέλικτο και ευπροσάρμοστο μπορεί να θεωρηθεί μια πρόκληση για την υποκλοπή στοιχείων. Εδώ είναι μερικά από τα χαρακτηριστικά του:

- Εφαρμόζει την επίθεση Caffe Latte WEP Client.[2]
- Εφαρμόζει την επίθεση Hirte WEP Client.
- Δυνατότητα να προκαλέσει την καταγραφή μηνύματος WPA/WPA2 Handshake.
- Δυνατότητα να ενεργεί σαν ad-hoc AP.[3]
- Δυνατότητα να λειτουργεί σαν ένα πλήρως AP.
- Δυνατότητα να φιλτράρετε με SSID ή διευθύνσεις MAC των Clients.
- Δυνατότητα να χειραγωγεί και να ξαναστέλνει πίσω πακέτα.
- Δυνατότητα να αποκρυπτογραφεί – κρυπτογραφεί τα πακέτα που λαμβάνει.

Η γενική σύνταξη της εντολής Airbase-ng είναι η παρακάτω:

- ***Airbase-ng [options] <replay interface>***

Για περισσότερες πληροφορίες σχετικά με την χρήση της Airbase-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=airbase-ng&DokuWiki=33cbc2bedbbd66b36cc5f10502dc1202

2.1.2 Aircrack-ng

Το Aircrack-ng μπορεί να ανακτήσει το WEP κλειδί έχοντας συλλέξει αρκετά κρυπτογραφημένα πακέτα με την βοήθεια του Airodump-ng. Το συγκεκριμένο κομμάτι του Aircrack-ng καθορίζει το WEP κλειδί χρησιμοποιώντας δυο (2) βασικές μεθόδους. Η πρώτη μέθοδος είναι μέσω της προσέγγισης PTW[4] (Pyshkin, Tews, Weinmann) η οποία και είναι η προεπιλεγμένη μέθοδος που χρησιμοποιεί το Aircrac-ng είναι το PTW. Αυτό γίνεται σε δυο (2) φάσεις. Στην πρώτη φάση, το Aircrack-ng χρησιμοποιεί μόνο πακέτα ARP. Εάν το κλειδί δεν έχει βρεθεί με τα πακέτα ARP τότε το Aircrack χρησιμοποιεί όλα τα πακέτα που έχει κάνει capture. Φυσικά δεν είναι δυνατόν να χρησιμοποιηθούν όλα τα πακέτα που έχουν καταγραφεί μέσα στο αρχείο[5]. Ένας σημαντικός περιορισμός είναι ότι η επίθεση PTW μπορεί να σπάσει μόνο 40 και 104 bit WEP keys. Το κύριο πλεονέκτημα της προσέγγισης PTW είναι ότι απαιτούνται πολύ λίγα πακέτα δεδομένων για να σπάσει το WEP κλειδί. Η

[2] http://www.aircrack-ng.org/doku.php?id=cafe-latte
[3] http://compnetworking.about.com/cs/wirelessfaqs/f/adhocwireless.htm
[4] http://www.darknet.org.uk/2007/09/aircrack-ptw-fast-wep-cracking-tool-for-wireless-hacking/
[5] Για τα πακέτα που μπορούν να χρησιμοποιηθούν για την ανάκτηση ενός WEP key μπορείτε να δείτε την σχετική σελίδα: http://www.aircrack-ng.org/doku.php?id=supported_packets

δεύτερη μέθοδος είναι η λύση της FMS / KoreK. Η μέθοδος FMS / KoreK περιλαμβάνει διάφορα στατιστικά επιθέσεων για να ανακαλύψει το WEP κλειδί και χρησιμοποιεί αυτά σε συνδυασμό με την Brute-Force attack. Επίσης το πρόγραμμα προσφέρει και την μέθοδο λεξικού (Wordlist) για τον προσδιορισμού του WEP και αντίστοιχα WPA κλειδιού.

Από την άλλη για να σπάσετε έναν κωδικό WPA/WPA2 χρησιμοποιείτε μόνο η μέθοδος λεξικού. Ωστόσο για να χρησιμοποιηθεί η μέθοδος λεξικού πρέπει πρώτα να έχει καταγραφεί ένα πακέτο Handshake με την χρήση του Airodump-ng. Αυτό γιατί μέσα στο πακέτο Handshake περιέχονται όλες οι πληροφορίες για το δίκτυο καθώς και για τον κωδικό. Ωστόσο όσο πιο δύσκολος είναι ο κωδικός του δικτύου τόσο πιο δύσκολο είναι να καταγραφεί ένα τέτοιο πακέτο. Περισσότερες πληροφορίες σχετικά με το “σπάσιμο” ενός κλειδιού WPA θα δούμε στην συνέχεια του κεφαλαίου.

Μια τέτοια επιτυχημένη έκβαση του Aircrack μπορούμε να δούμε και στο επόμενο Screenshot. Όπως μπορείτε να δείτε η πρώτη στήλη αφορά τα Kbytes, η δεύτερη το βάθος που ψάχνει για το κλειδί εκείνη την δεδομένη στιγμή, η τρίτη τα bytes που διέρρευσαν (αυτά που κάνατε capture) και η τέταρτη στήλη οι ψήφοι που δέχτηκε ότι αυτό το κομμάτι password είναι το σωστό.

Εικόνα 52. Aircrack-ng - Find Password

Η γενική σύνταξη της εντολής Aircrack-ng είναι η παρακάτω:

- ***aircrack-ng [options] <capture file(s)>***

Παρακάτω λοιπόν θα δούμε μια περίληψη όλων των διαθέσιμων επιλογών του Aircrack-ng.

-a	Force attack mode (1 = static WEP, 2 = WPA/WPA2-PSK).
-b	Επιλέξτε το δίκτυο που θα κάνετε επίθεση με βάση την διεύθυνση MAC του σημείου πρόσβασης.

-e	Εάν οριστεί, θα χρησιμοποιηθούν όλα τα IVs που έχουν καταγραφεί από το δίκτυο με το ίδιο ESSID. Απαιτείται επίσης για WPA/WPA2.
-p	Αφορά σύστημα πολυεπεξεργαστών. Με την επιλογή αυτή ορίζετε πόσα CPU θα χρησιμοποιηθούν για την εύρεση του κλειδιού.
-q	Ενεργοποίηση αθόρυβης λειτουργίας (stealth mode).
-c	(WEP cracking). Περιορισμός της αναζήτησης μόνο σε αλφαριθμητικούς χαρακτήρες. (0x20 – 0x7F)
-t	(WEP cracking). Περιορισμός της αναζήτησης στο δυαδικό σύστημα κωδικοποιημένων δεκαδικών – δεκαεξαδικών χαρακτήρων.
-h	(WEP cracking). Περιορισμός της αναζήτησης μόνο σε αριθμητικούς χαρακτήρες.
-d	(WEP cracking). Set the beginning of the WEP key (in hex), for debugging purposes.
-m	(WEP cracking). Φιλτράρισμα της MAC address για WEP data packets.
-M	(WEP cracking). Ορίζει το μέγιστο αριθμό IVs που θα χρησιμοποιήσετε.
-n	(WEP cracking). Καθορίστε το μήκος του κλειδιού. 64 for 40-bit WEP, 128 for 104-bit WEP, etc. Η προεπιλεγμένη τιμή είναι 128.
-i	(WEP cracking). Να διατηρούν τα IVs που έχουν αυτό το βασικό δείκτη (1 έως 4). Η προεπιλογή είναι να αγνοείτε ο βασικός δείκτης.
-f	(WEP cracking). Από προεπιλογή, αυτή η παράμετρος έχει οριστεί σε 2 για 104-bit WEP και με 5 για 40-bit WEP. Ορίστε μια υψηλότερη τιμή για να αυξήσει το επίπεδο bruteforce attack. Ωστόσο θα χρειαστεί περισσότερο χρόνο, αλλά με υψηλότερο ποσοστό επιτυχίας για την εύρεση του κλειδιού.
-H	Δείχνει την οθόνη βοήθειας.
-I	Καταγράφει το κλειδί για ένα καθορισμένο αρχείο.
-K	Επικαλείται την μέθοδο Korek WEP cracking mode.
-k	(WEP cracking). Υπάρχουν 17 είδη στατικών επιθέσεων Korek. Μερικές φορές μια επίθεση δημιουργεί ψεύτικα “θετικά” αποτελέσματα που εμποδίζει να βρεθεί το κλειδί έστω και με πολλά IVs. Δοκιμάστε –k 1, -k 2, … -k 17 για να απενεργοποιήσετε επιλεκτικά την κάθε επίθεση.
-p	Allow the number of threads for cracking even if you have a non-SMP computer.
-r	Χρησιμοποιείτε μια βάση δεδομένων που έχει δημιουργηθεί από το Airolib-ng για τον καθορισμό του κλειδιού.
-x/ -x0	(WEP cracking). Disable last keybytes brutforce.
-x1	(WEP cracking). Enable last keybyte bruteforcing (default).
-x2	(WEP cracking). Enable last two keybytes bruteforcing.
-X	(WEP cracking). Disable bruteforce multithreading (SMP only).

-y	(WEP cracking) Experimental single bruteforce attack which should only be used when the standard attack mode fails with more than one million IVs.
-u	Παροχή πληροφοριών σχετικά με τον αριθμό των CPU και την υποστήριξη MMX. Παράδειγμα απαντήσεις σε "aircrack-ng-CPU-detect" είναι "Nb CPU detect: 2" ή "Nb CPU detect: 1 (MMX διαθέσιμο)".
-w	(WEP cracking). Διαδρομή για την εύρεση του WEP κλειδιού μέσα από μια Wordlist.
-z	Επικαλείται την μέθοδο PTW WEP cracking mode.
-P	Επικαλείται την λειτουργία PTW για εντοπισμό σφαλμάτων.
-C	Merge the given APs to a virtual one.
-D	Εκτέλεση σε λειτουργία WEP decloack.
-V	Run in visual inspection mode.
-1	Run in oneshot mode.
-S	WPA cracking speed test.

Πίνακας 1. Επιλογές σύνταξης της Aircrack-ng

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Aircrack-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=aircrack-ng&DokuWiki=a4faceb91332419da221752adac306ac

2.1.3 Airdecap-ng

Με την χρήση του Airdecap-ng μπορείτε να αποκρυπτογραφήσετε αρχεία καταγραφής WEP/WPA/WPA2. Επίσης μπορεί να χρησιμοποιηθεί για να αφαιρέσει τις επικεφαλίδες του ασύρματου από μια κρυπτογραφημένη καταγραφή. Το αποτέλεσμα αυτού θα είναι να εξάγει ένα νέο αρχείο με την κατάληξη “-dec.cap” που είναι η αποκρυπτογραφημένη έκδοση του αρχείου εισόδου.

Η γενική σύνταξη της εντολής Airdecap-ng είναι η παρακάτω:

- ***airdecap-ng [options] <pcap file>***

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Airdecap-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=airdecap-ng

2.1.4 Airdecloak-ng

Το Airdecloak-ng, είναι ένα εργαλείο που αφαιρεί τα cloaked packets (τα

spoofed πακέτα) από το pcap file και έτσι επιτρέπει το aircrack-ng να σπάσει το κλειδί της ασύρματης κρυπτογράφησης WEP. Εσωτερικά η λογική είναι, αρχικά να εντοπίσει τα πακέτα αυτά τα spoofed chaff packets αναλύοντας το sequence number και το IV field.

Η γενική σύνταξη της εντολής Airdecloak-ng είναι η παρακάτω:

- ***airdecloak-ng [options]***

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Airdecloak-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=airdecloak-ng

2.1.5 Airdriver-ng

Το Airdriver-ng είναι ένα Script που περιέχει πληροφορίες, για την κατάσταση σχετικά με τους ασύρματους drivers στο συστημά σας, συν του ότι έχει την δυνατότητα να φορτώνει προγράμματα οδήγησης όταν εντοπίζει νέες συσκευές. Επιπλέον, το Airdriver-ng έχει την ικανότητα να εγκαθιστά και αποκαθιστά τους drivers για οποιαδήποτε ασύρματη συσκευή στο σύστημά σας.

Η γενική σύνταξη της εντολής Airdriver-ng είναι η παρακάτω:

- ***airdriver-ng <command> [driver number | driver name]***

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Airdriver-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=airdriver-ng

2.1.6 Airdrop-ng

Το Airdrop-ng είναι ένα πρόγραμμα που χρησιμεύει για τη στοχευόμενη επίθεση σε χρήστες. Μπορεί να στοχεύει με βάση την διεύθυνση MAC του χρήστη, τον τύπο του υλικού, ή εφαρμόζοντας όλα τα παραπάνω.

Η γενική σύνταξη της εντολής Airdrop-ng είναι η παρακάτω:

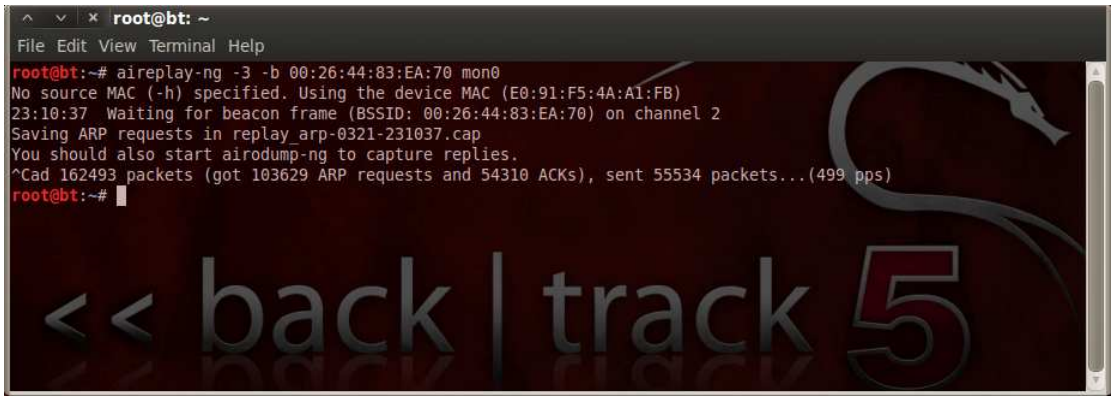
- ***airdrop-ng [options] <pcap file>***

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Airdrop-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=airdrop-ng

2.1.7 Aireplay-ng

Το Aireplay-ng χρησιμοποιείται για να κάνουμε inject πακέτα σε κάποιο

ασύρματο δίκτυο – στόχο. Η κύρια λειτουργία του είναι να δημιουργήσουμε κυκλοφορία πακέτων ώστε να καταγράφουμε πολύ περισσότερα πακέτα από αυτά που ανταλλάσσονται πραγματικά στο δίκτυο. Ωστόσο, μπορεί να χρησιμοποιηθεί ώστε να αναγκάσει κάποιον ασύρματο client να συνδεθεί ή να αποσυνδεθεί από το AP και να εκτελέσει ψεύτικες πιστοποιήσεις ώστε να συνδεθούμε εμείς με το AP στόχο (αυτό μας βοηθάει στην περίπτωση που δεν υπάρχει άλλος πελάτης συνδεδεμένος).



Εικόνα 53. Δημιουργία κυκλοφορίας πακέτων - Aireplay-ng

2.1.7.1 Επιθέσεις που υποστηρίζονται

Το Aireplay-ng υλοποιεί σήμερα πολλές διαφορετικές επιθέσεις. Οι επιθέσεις αυτές είναι:

- **Attack 0: Deauthentication.** Η επίθεση αυτή στέλνει πακέτα αποσυσχέτισης (disasociate) σε έναν ή περισσότερους clients οι οποίοι είναι συνδεδεμένοι στο ασύρματο δίκτυο στόχο. Η αποσυσχέτιση κάποιου client μας βοηθάει να:
  - δημιουργηθούν πακέτα ARP requests κατά την αποσυσχέτιση τα οποία θα τα καταγράψουμε και στη συνέχεια θα τα χρησιμοποιήσουμε κάνοντάς τα inject
  - καταγράψουμε το WPA/WPA2 handshake κάνοντας τον client που αποσυσχετίσαμε να ξανασυσχετιστεί με το Access Point (AP).

  Χαρακτηριστικό παράδειγμα εντολής:

  - ***aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:34:30:30 ath0***

- **Attack 1: Fake authentication.** Η επίθεση αυτή μας επιτρέπει να εκτελέσουμε τους δύο τύπους της πιστοποίησης WEP (Open/ Shared key) καθώς και να συσχετιστούμε (associate) με το AP. Είναι πολύ χρήσιμη στην περίπτωση που κανείς άλλος client δεν είναι συνδεδεμένος στο AP στόχο. Να σημειώσουμε ότι κατά τη διάρκεια του fake authentication δε δημιουργούνται πακέτα ARP και ότι η επίθεση αυτή δε μπορεί να χρησιμοποιηθεί για να συσχετιστούμε με ένα AP που χρησιμοποιεί WPA/ WPA2.
  Χαρακτηριστικό παράδειγμα εντολής:

  - ***aireplay-ng -1 0 -e teddy -a 00:14:6C:7E:40:80 -h 00:09:5B:EC:EE:F2 -y sharedkeyxor ath0***

- **Attack 2: Interactive packet replay.** Αυτή η επίθεση μας επιτρέπει να επιλέξουμε ένα συγκεκριμένο πακέτο το οποίο θα γίνει inject στο AP στόχο. Ωστόσο δε μπορούμε να κάνουμε inject οποιοδήποτε πακέτο αλλά μόνο συγκεκριμένα πακέτα μπορούν να γίνουν inject επιτυχώς και να οδηγήσουν το σταθμό AP να εκπέμψει ένα νέο πακέτο το οποίο να περιέχει ένα νέο IV. Ας δούμε κάποια από τα χαρακτηριστικά που πρέπει να έχει ένα πακέτο ώστε να γίνει δεκτό από το AP.
  - τα Access points πάντα κάνουν αποδεκτό και επαναλαμβάνουν ένα πακέτο το οποίο έχει προορισμό τη διεύθυνση broadcast: FF:FF:FF:FF:FF:FF.Τα πακέτα ARP έχουν αυτό το χαρακτηριστικό
  - επίσης, το πακέτο πρέπει να κατευθύνεται από τον πελάτη στο ασύρματο δίκτυο. Κάθε τέτοιο πακέτο έχει το bit σημαίας το DS ίσο με 1.

  Χαρακτηριστικό παράδειγμα εντολής:

  - ***aireplay-ng -2 <filter options> <replay options> -r <file name> <replay interface>***

- **Attack 3: ARP request replay attack.** Η επίθεση αυτή εκτελείτε όταν υπάρχει έστω και ένας πελάτης συνδεδεμένος στον client. Αρχικά το aireplay καταγράφει τα πακέτα που κυκλοφορούν στο δίκτυο. Μόλις συναντήσει ένα πακέτο ARP request το κάνει inject στο δίκτυο με στόχο να πολλαπλασιάσει την κίνηση πακέτων. Για να δημιουργηθεί ένα πακέτο ARP replay μπορούμε να αποσυσχετίσουμε κάποιον συνδεδεμένο client, συνδυάζοντας έτσι την επίθεση αυτή με την επίθεση deauthentication, ή απλά να περιμένουμε (αν έχουμε υπομονή) για ένα πακέτο ARP request.

  Χαρακτηριστικό παράδειγμα εντολής:

  - ***aireplay-ng -3 -b 00:13:10:30:24:9C -h 00:11:22:33:44:55 ath0***

- **Attack 4: KoreK chopchop attack.** Ο στόχος αυτής της επίθεσης είναι να υποκλέψουμε τον αλγόριθμο PRGA που χρησιμοποιεί το AP στόχος. Το PRGA δε μπορεί να χρησιμοποιηθεί για να αποκρυπτογραφήσουμε πακέτα, ωστόσο μπορεί να χρησιμοποιηθεί για να δημιουργήσουμε νέα πακέτα τα οποία και θα κάνουμε inject στο δίκτυο.

  Πλεονεκτήματα

  - Μπορεί να λειτουργήσει σε περιπτώσεις όπου δε τα καταφέρνει η επίθεση fragmentation
  - Δεν απαιτείται να γνωρίζουμε πληροφορίες για διευθύνσεις IP που χρησιμοποιούνται στο δίκτυο

  Μειονεκτήματα

  - Δε μπορεί να χρησιμοποιηθεί για όλα τα AP
  - Αρκετά πιο αργή από την επίθεση fragmentation
  - Το μέγεθος του πακέτου xor περιορίζεται στο μέγεθος του πακέτου στο οποίο εκτελούμε την chopchop

Για να λειτουργήσει η επίθεση chopchop θα πρέπει να έχουμε πραγματοποιήσει fake authentication με το AP στόχο.

Χαρακτηριστικό παράδειγμα εντολής:

- ***aireplay-ng -4 -h 00:09:5B:EC:EE:F2 -b 00:14:6C:7E:40:80 ath0***

- **Attack 5: Fragmentation attack.** Ομοίως με την επίθεση chopchop ο στόχος της επίθεσης fragmentation είναι να υποκλέψει το PRGA. Θα ρωτηθείτε: γιατί να υπάρχουν δύο επιθέσεις που κάνουν το ίδιο πράγμα; Ο λόγος είναι ότι εκεί που δε δουλεύει η πρώτη μπορεί να δουλεύει η δεύτερη και το αντίθετο. Για να λειτουργήσει η επίθεση fragmentation θα πρέπει να έχουμε πραγματοποιήσει fake authentication με το AP στόχο.

  Και στις δυο επιθέσεις fragmentation, chopchop όπως είπαμε, στόχος είναι να υποκλέψουμε το PRGA. Σε επόμενο βήμα, θα χρησιμοποιήσουμε το PRGA ώστε να δημιουργήσουμε πακέτα ARP request τα οποία θα τα κάνουμε interactive replay στο δίκτυο στόχο για να δημιουργήσουμε κυκλοφορία πακέτων. Έτσι, αυτές οι δύο επιθέσεις συνδυάζονται με την επίθεση fake authentication και την επίθεση Interactive packet replay.

  Πλεονεκτήματα

  - Υποκλέπτει ολόκληρο το πακέτο xor μεγέθους 1500 byte
  - Μπορεί να λειτουργεί εκεί όπου δε λειτουργεί η επίθεση chopchop
  - Είναι πολύ γρήγορη

  Μειονεκτήματα

  - Χρειάζεται περισσότερες πληροφορίες για να ξεκινήσει, για παράδειγμα πληροφορίες για IP διευθύνσεις που χρησιμοποιούνται εντός του ασύρματου δικτύου. Ωστόσο η χρήση της διεύθυνσης broadcast (255.255.255.255) αρκεί για τα περισσότερα AP
  - Πρέπει να είμαστε αρκετά κοντά στο AP
  - Η επίθεση θα αποτύχει σε AP τα οποία δε χειρίζονται σωστά τα πακέτα fragmentation (θραύσματα)

  Χαρακτηριστικό παράδειγμα εντολής:

  - ***aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0***

- **Attack 6: Cafe-latte attack.** Η επίθεση Cafe-latte attack σας επιτρέπει να αποκτήσετε ένα κλειδί WEP από ένα σύστημα - πελάτη. Εν συντομία, αυτό γίνεται με την λήψη πακέτων ARP από τον πελάτη, στην συνέχεια χειρίζονται από το πρόγραμμά σας και στην συνέχεια το στέλνει πίσω στον πελάτη. Ο πελάτης με την σειρά του δημιουργεί πακέτα που μπορούν να συλληφθούν από το Airodump-ng. Στην συνέχεια, μπορεί να χρησιμοποιηθεί το Aircrack-ng για τον προσδιορισμό του κλειδιού WEP.

Χαρακτηριστικό παράδειγμα εντολής:

- ***aireplay-ng -6 -h 00:09:5B:EC:EE:F2 -b 00:13:10:30:24:9C -D rausb0***

- **Attack 7: Client-oriented fragmentation attack (Hirte).** Η επίθεση Hirte είναι και αυτή ένα είδος επίθεσης σε πελάτη, η οποία μπορεί να χρησιμοποιήσει οποιαδήποτε IP ή ARP πακέτα. Είναι επέκταση της επίθεσης Café-latte, επιτρέποντας κάθε πακέτο να χρησιμοποιηθεί με αποτέλεσμα να μην περιορίζεται μόνο σε πακέτα ARP.

  Χαρακτηριστικό παράδειγμα εντολής:

  - ***aireplay-ng -6 -h 00:09:5B:EC:EE:F2 -b 00:13:10:30:24:9C -D rausb0***

- **Attack 8: WPA Migration Mode** – διαθέσιμη σε επόμενη έκδοση.

- **Attack 9: Packet Injection test.** Το packet injection είναι η τεχνική κατά την οποία ένας client στέλνει ένα πακέτο σε ένα σταθμό access point χωρίς ο client να είναι κόμβος του δικτύου. Η Προϋπόθεση για να δουλέψει το packet injection είναι ο client να έχει πραγματοποιήσει fake authentication με το σταθμό AP. Το packet injection μας βοηθάει να πολλαπλασιάσουμε την κίνηση πακέτων σε ένα ασύρματο δίκτυο συλλέγοντας έτσι τα IVs πολύ πιο γρήγορα. Πως γίνεται αυτό; Πολύ απλά, κάνουμε inject στο σταθμό AP ένα πακέτο ARP request και μόλις ο AP το λάβει θα στείλει αμέσως ένα κρυπτογραφημένο πακέτο ARP reply το οποίο μπορούμε να υποκλέψουμε με το πρόγραμμα airodump-ng.

  Χαρακτηριστικό παράδειγμα εντολής:

  - ***aireplay-ng -9 -e teddy -a 00:de:ad:ca:fe:00 -i wlan1 wlan0***

Η γενική σύνταξη της εντολής Aireplay-ng είναι η παρακάτω:

- ***aireplay-ng <options> <replay interface>***

Για το **φιλτράρισμα των πακέτων** που θα σταλούν ισχύουν τα παρακάτω φίλτρα:

-b	bssid	MAC address, Access Point
-d	dmac	MAC address, Destination (προορισμός)
-s	smac	MAC address, Source (πηγή)
-m	len	Ελάχιστο μήκος πακέτων
-n	len	Μέγιστο μήκος πακέτων

-u	type	Frame control, type field
-v	subt	Frame control, subtype field
-t	tods	Frame control, To DS bit
-f	fromds	Frame control, From DS bit
-w	iswep	Frame control, WEP bi

Πίνακας 2. Φιλτράρισμα πακέτων - Aireplay-ng

Για **package injection** ισχύουν οι εξής επιλογές:

-x	nbpps	Number of packets per second
-p	fctrl	Frame control word (hex)
-a	bssid	Access Point MAC address
-c	dmac	Destination MAC address
-h	smac	Source MAC address
-e	essid	Fakeauth attack : το AP SSID στο οποίο θέλουμε να κάνουμε authentication
-j	-	Inject FromDS πακέτα
-g	value	Αλλαγή του μεγέθους του ring buffer (default: 8)
-k	IP	Destination IP in fragments
-l	IP	Source IP in fragments
-o	npckts	Number of packets per burst (-1)
-q	sec	Δευτερόλεπτα μεταξύ των keep-alives, σε περίπτωση dynamic wep (-1)
-y	prga	Keystream για shared key authentication

Πίνακας 3. Package injection - Aireplay-ng

Attack modes, επιθέσεις που μπορούν να γίνουν με το aireplay (Μπορούν να χρησιμοποιηθούν και οι αριθμοί):

--deauth count	deauthenticate 1 ή όλους τους stations (-0)
--fakeauth delay	fake authentication με το AP (-1)

--interactive	interactive frame selection (-2)
--arpreplay	κλασσική ARP-request replay (-3)
--chopchop	decrypt/chopchop WEP packet (-4)
--fragment	Δημιουργεί μια έγκυρη keystream (-5)
--test	injection test (-9)

Πίνακας 4. Attack modes - Aireplay-ng

Ένα τέτοιο παράδειγμα χρήσης της Aireplay-ng μπορούμε να δούμε παρακάτω. Όπως μπορείτε να προσέξετε, χρησιμοποιούμε διάφορες παραμέτρους από αυτές που αναφέραμε παραπάνω.

Παράδειγμα εντολής:

aireplay -1 0 –e [Essid] -a [Bssid τουAP] –b [bssid του AP] –h [bssid του station] [interface]

- -1 = fake authentication
- 0 = delay στο οποίο θα περιμένουμε για την απάντηση από το AP
- -e = το AP στο οποίο θέλουμε να κάνουμε authentication
- -a = η mac του AP στην οποία θα κάνουμε το injection
- -b = η mac του AP
- -h = η δική μας mac
- interface = το wlan interface μας, πχ ath0

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Aireplay-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=aireplay-ng&DokuWiki=efb8f737c2e7eafffbf7e3eebc8e49b1

2.1.8 Airgraph-ng

Σκοπός του Airgraph-ng είναι να σχεδιάζει το αποτέλεσμα του .txt αρχείου που δημιουργήθηκε καθώς ολοκληρώθηκε η καταγραφή τον πακέτων με το Airodump-ng. Η κεντρική ιδέα είναι ότι δείχνει τις “σχέσεις” των πελατών με το Access Point που έχουν συνδεθεί. Δηλαδή έχει την ικανότητα να δείχνει αναλυτικά όλη την κίνηση και συγκεκριμένα τα πακέτα που έχουν ανταλλαχτεί μεταξύ client και AP.

Η γενική σύνταξη της εντολής Airgraph-ng είναι η παρακάτω:

- ***python airgraph-ng -i [airodumpfile.txt] -o [outputfile.png] -g [CAPR OR CPG]***

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Airgraph-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=airgraph-ng&DokuWiki=efb8f737c2e7eafffbf7e3eebc8e49b1

2.1.9 Airmon-ng

Το Airmon-ng είναι ένα script το οποίο μας βοηθάει να θέσουμε την κάρτα δικτύου μας σε monitor mode. Επίσης, μπορεί να χρησιμοποιηθεί ώστε να γυρίσουμε την κάρτα δικτύου μας σε κατάσταση managed. Το Airmon-ng το χρησιμοποιούμε πριν από τα υπόλοιπα εργαλεία ώστε να θέσουμε την κάρτα μας σε κατάσταση monitor.

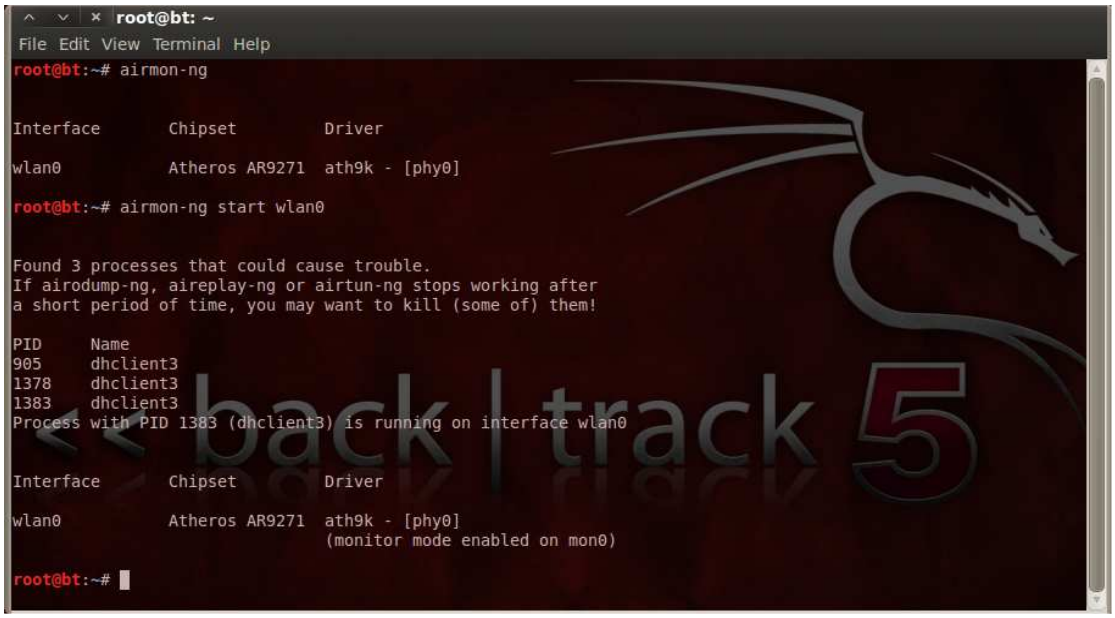
Η γενική σύνταξη της εντολής Airmon-ng είναι η παρακάτω:

- ***airmon-ng {start|stop} {interface}[channel]***

- Το start|stop προσδιορίζει αν θα ενεργοποιήσουμε ή αν θα απενεργοποιήσουμε την κατάσταση monitor της ασύρματης κάρτας μας.
- Το interface προσδιορίζει την κάρτα δικτύου για την οποία θέλουμε να ενεργοποιήσουμε/ απενεργοποιήσουμε την κατάσταση monitor.
- Το channel προσδιορίζει το κανάλι στο οποίο θέλουμε να δουλέψει η κάρτα μας. Την χρησιμοποιούμε αν γνωρίζουμε ήδη σε πιο κανάλι εκπέμπει το AP στόχος.

Ας δούμε κάποιες τυπικές περιπτώσεις χρήσης του:

- Αν θέλουμε να ενεργοποιήσουμε την κατάσταση monitor στη διεπαφή δικτύου wlan0 εκτελούμε:
  - **airmon-ng start wlan0**
- Αν θέλουμε να απενεργοποιήσουμε την κατάσταση monitor στη διεπαφή wlan0 εκτελούμε:
  - **airmon-ng stop wlan0**
- Αν θέλουμε να ενεργοποιήσουμε την κατάσταση monitor στη διεπαφή eth1 και θέλουμε αυτή να λειτουργήσει στο κανάλι 11 εκτελούμε:
  - **airmon-ng start eth1 11**
- Αν θέλουμε να πάρουμε πληροφορίες για τη διεπαφή wifi0 εκτελούμε:
  - **airmon-ng wifi0**
- Για να σιγουρευτούμε ότι το monitor ενεργοποιήθηκε για παράδειγμα στη διεπαφή wifi0 μπορούμε να εκτελέσουμε:
  - **iwconfig wifi0**



Εικόνα 54. Χρήση της Airmon-ng

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Airmon-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=airmon-ng&DokuWiki=efb8f737c2e7eafffbf7e3eebc8e49b1

2.1.10 Airodump-ng

Το airodump-ng χρησιμοποιείται για την καταγραφή πακέτων από 802.11 δίκτυα και για τη συλλογή των WEP IVs (Initialization Vectors). Επίσης, μπορεί να χρησιμοποιηθεί για τον εντοπισμό των δικτύων 802.11 που βρίσκονται εντός της κάλυψης της κάρτας μας. Πριν τρέξετε το airodump-ng θα πρέπει να έχετε θέσει την κάρτα σας σε κατάσταση monitor όπως είδαμε χαρακτηριστικά και στην προηγούμενη εντολή (Airmon-ng).

Η γενική σύνταξη της εντολής Airodump-ng είναι η παρακάτω:

- ***airodump-ng {options} {interface}[,{interface},...]***

Οι επιλογές οπού μπορούν να χρησιμοποιηθούν στο Airodump είναι οι παρακάτω:

--ivs	Σώζει μόνο IVs και όχι όλα τα πακέτα που λαμβάνει.
--gpsd	Για χρήση GPSd.
--write	Prefix του αρχείου καταγραφής των πακέτων δηλαδή το όνομα του αρχείου οπού θα σωθεί η κίνηση των πακέτων.
-w	Ίδιο με το --write.
--beacons	Καταγραφή όλων των beacons σε ένα dump file.
--update	Ανανέωση της οθόνης σε secs.

--showack	Εμφανίζει στατιστικά των ack/cts/rts πακέτων.
-h	Κρύβει γνωστούς stations για το --showack.
-f	Χρόνος ανάμεσα στην αλλαγή channel σε ms.
--berlin	Χρόνος πριν την απομάκρυνση από την οθόνη ενός AP/client όταν δεν υπάρχει δραστηριότητα (Default: 120 seconds).
-r	Ανάγνωση πακέτων από το file.

Πίνακας 5. Airodump-ng – Options

Οι επιλογές όπου μπορούν να χρησιμοποιηθούν για φιλτράρισμα στο Airodump είναι οι παρακάτω:

--encrypt	Φιλτράρισμα APs ανάλογα με τον cipher τους.
--netmask	Φιλτράρισμα APs ανάλογα με τη mask.
--bssid	Φιλτράρισμα APs ανάλογα BSSID.
-a	Φιλτράρισμα unassociated clients.

Πίνακας 6. Airodump-ng - Filter Options

Εξ' ορισμού το Airodump-ng θα αλλάζει κανάλια στην μπάντα των 2.4Ghz. Μπορούμε να το κάνουμε να καταγράφει σε άλλα κανάλια ή/και άλλες μπάντες:

--channel	Καταγραφή σε συγκεκριμένα κανάλια	
--band	Μπάντα στην οποία το airodump-ng θα αλλάζει κανάλια	
--cswitch	method	Τρόπος αλλαγής καναλιών:
	0	FIFO (default)
	1	Round Robin
	2	Hop on last
-s	Ίδιο με το --cswitch.	
--help	Δείχνει την οθόνη βοήθειας.	

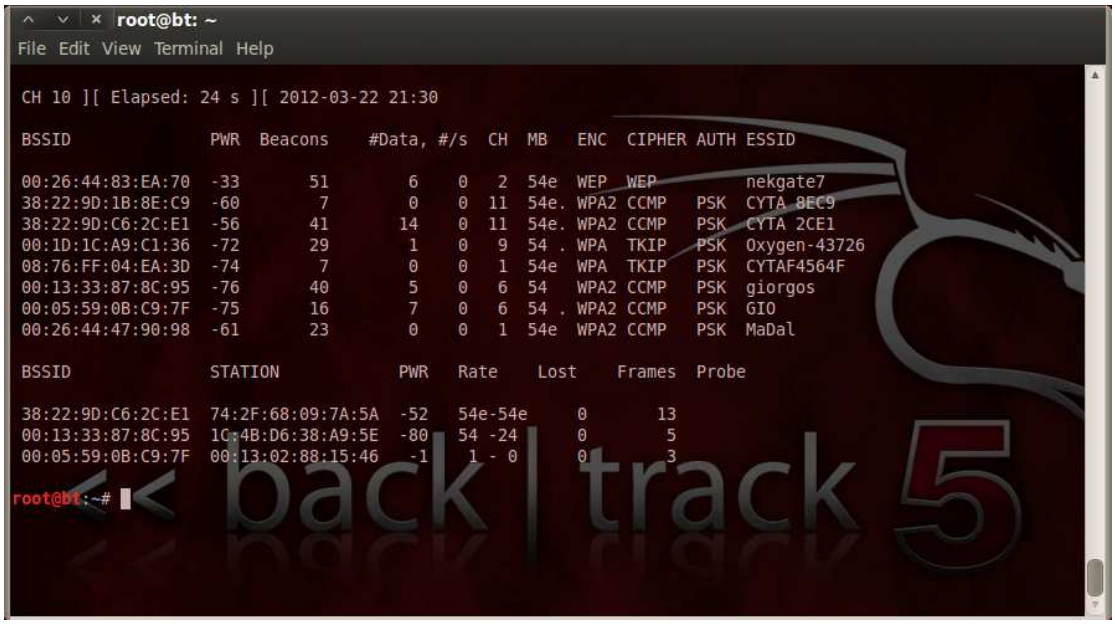
Πίνακας 7. Airodump-ng - Channel and Band Selection

Το interface προσδιορίζει την κάρτα δικτύου που θα χρησιμοποιείται ώστε να καταγράφουμε πακέτα. Παρατηρήστε ότι μπορούμε να χρησιμοποιήσουμε πολλές διεπαφές αρκεί να τις χωρίσουμε με κόμμα. Η διεπαφή που χρησιμοποιούμε έχει το αναγνωριστικό mon0.

Ας δούμε τώρα μερικές περιπτώσεις χρήσης του airodump-ng. Αρχικά, θέλουμε να εντοπίσουμε τα ασύρματα δίκτυα που είναι εντός της εμβέλειας της κάρτας μας. Για το σκοπό αυτό εκτελούμε:

- airodump-ng mon0

Στην έξοδο θα πάρουμε κάτι σαν και αυτό που βλέπουμε παρακάτω:



Εικόνα 55. Χρήση της Airodump-ng

Ας αναλύσουμε λίγο το αποτέλεσμα:

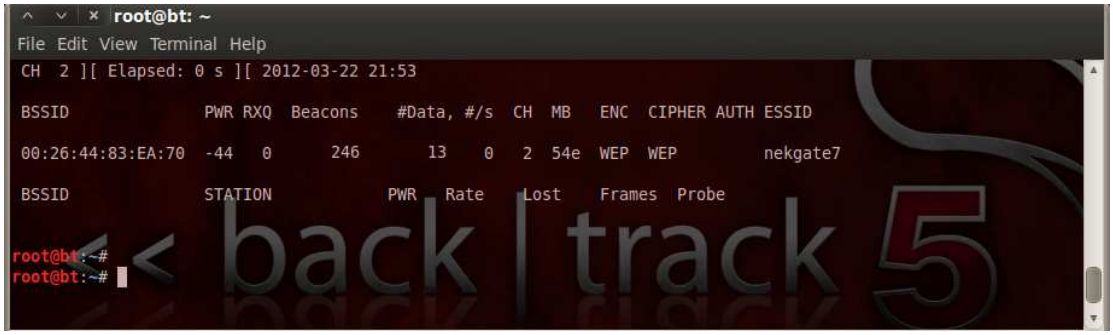
- Στην καρτέλα BSSID εμφανίζεται η MAC address των APs που βρίσκονται εντός της εμβέλειας της κάρτας μας.
- Στην καρτέλα PWR βλέπουμε την ισχύ του σήματος
- Στην καρτέλα Beacon βλέπουμε τα beacon frames που έχει έχουμε λάβει από κάθε AP
- Στην καρτέλα #Data βλέπουμε τα πακέτα που έχουμε λάβει από κάθε AP
- Στην καρτέλα #/s βλέπουμε το ρυθμό με τον οποίο εμείς στέλνουμε πακέτα στο AP
- Στην καρτέλα CH βλέπουμε το κανάλι στο οποίο λειτουργεί το AP
- Στην καρτέλα ENC βλέπουμε το είδος της κρυπτογράφησης που χρησιμοποιείται.
- Στην καρτέλα ESSID βλέπουμε το όνομα του δικτύου
- Όταν υπάρχουν συνδεδεμένοι πελάτες στα AP εμφανίζονται κάτω από αυτά τα στοιχεία των πελατών. Για παράδειγμα:

Εικόνα 56. Χρήση της Airodump-ng (2)

- Κάτω από το BSSID φαίνεται η διεύθυνση του AP στο οποίο είναι συνδεδεμένος ο πελάτης.
- Κάτω από το Station φαίνεται η διεύθυνση MAC του πελάτη
- Κάτω από το Packets φαίνεται ο αριθμός των πακέτων που έχουν καταγραφεί και προορίζονται για τον συγκεκριμένο πελάτη

Για να λάβουμε γρηγορότερα τα πακέτα που στέλνει ο AP που μας ενδιαφέρει, και να καταγράψουμε τα πακέτα που θα κάνουμε inject πρέπει να επικεντρωθούμε στον συγκεκριμένο AP. Εκτελούμε:

- ***airodump-ng -c 11 --bssid 00:21:63:44:63:38 -w output mon0***



Εικόνα 57. Airodump-ng - Capture Packets

Ας δούμε τις επιλογές που χρησιμοποιούμε:

- -c: καθορίζει το κανάλι
- --bssid: καθορίζει τη διεύθυνση MAC του AP στόχου
- -w: καθορίζει το όνομα του αρχείου στο οποίο θα αποθηκευτούν τα πακέτα που καταγράφονται. Στο παραπάνω παράδειγμα αυτό θα ξεκινάει από τη συμβολοσειρά "output".

2.1.11 Airolib-ng

Το Airolib-ng χρησιμοποιεί μια Database για να διαχειριστεί τους καταλόγους / αρχεία με τα password και SSID.Αυτό του προσδίδει μια μεγαλύτερη ευελιξία και πλεονέκτημα. Για παράδειγμα μπορούμε να επιτύχουμε την πρόσθεση νέων "λέξεων" / password και SSID στην Database που χρησιμοποιούμε χωρίς αυτό να επηρεάζει στους υπολογισμούς όπου πραγματοποιήθηκαν πριν από την πρόσθεση

των νέων password και SSID.

Η γενική σύνταξη της εντολής Airolib-ng είναι η παρακάτω:

- ***airolib <database> <operation> [options]***

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Airolib-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=airolib-ng&DokuWiki=efb8f737c2e7eafffbf7e3eebc8e49b1

2.1.12 Airserv-ng

Το Airserv-ng χρησιμοποιείτε σαν ένας ασύρματος διακομιστείς κάτι που επιτρέπει σε πολλά ασύρματα προγράμματα να χρησιμοποιούν ανεξάρτητα μια ασύρματη κάρτα μέσω σύνδεσης με το δίκτυο TCP client-server. Όλα τα λειτουργικά συστήματα μαζί με τον κωδικό της ασύρματης κάρτας βρίσκονται ενσωματωμένα στο διακομιστεί. Αυτό εξαλείφει την ανάγκη για κάθε ασύρματη εφαρμογή να περιέχει τις πληροφορίες της ασύρματης κάρτας που χρησιμοποιεί.

Η γενική σύνταξη της εντολής Airserv-ng είναι η παρακάτω:

- ***airserv-ng <opts>***

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Airserv-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=airserv-ng&DokuWiki=efb8f737c2e7eafffbf7e3eebc8e49b1

2.1.13 Airtun-ng

Το Airtun-ng είναι ένα εικονικό περιβάλλον διεπαφής. Υπάρχουν δυο (2) βασικές λειτουργίες που πραγματοποιεί:

- Επιτρέπει την παρακολούθηση της κρυπτογραφημένης κίνησης με σκοπό να ανιχνεύσει οποιαδήποτε προσπάθεια εισβολής από κάποιον μη εξουσιοδοτημένο χρήστη στο δίκτυο (wIDS).
- Εισάγει αυθαίρετη κίνηση στο δίκτυο.

Για να γίνει φυσικά η παρακολούθηση κίνησης πρέπει να έχετε στην κατοχή σας το κλειδί κρυπτογράφησης και το bssid του δικτύου που θέλετε να παρακολουθήσετε.

Η γενική σύνταξη της εντολής Airtun-ng είναι η παρακάτω:

- ***airtun-ng <options> <replay interface>***

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Airtun-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=airtun-ng&DokuWiki=efb8f737c2e7eafffbf7e3eebc8e49b1

2.1.14 Easside-ng

Το Easside-ng είναι ένα εργαλείο που σας επιτρέπει την επικοινωνία με ένα κρυπτογραφημένο WEP Access Point χωρίς να γνωρίζετε το αντίστοιχο WEP κλειδί του.

Η γενική σύνταξη της εντολής Easside-ng είναι η παρακάτω:

- ***easside-ng <args>***

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Easside-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=easside-ng&DokuWiki=a0e82a76d7d1fbbbbb714261900cf514

2.1.15 Packetforge-ng

Σκοπός του Packetforge-ng είναι να δημιουργήσει κρυπτογραφημένα πακέτα που μπορούν στη συνέχεια να χρησιμοποιηθούν για injection στο δίκτυο. Μπορείτε να δημιουργήσετε διάφορους τύπους πακέτων, όπως αιτήσεις ARP, UDP, ICMP και προσαρμοσμένα πακέτα. Η πιο συνηθισμένη χρήση του Packetforge-ng είναι για την δημιουργία ARP πακέτων.

Η γενική σύνταξη της εντολής Packtegorge-ng είναι η παρακάτω:

- ***packetforge-ng <mode> <options>***

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Packetforge-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=packetforge-ng&DokuWiki=a0e82a76d7d1fbbbbb714261900cf514

2.1.16 Tkiptun-ng

Το εργαλείο αυτό είναι σε θέση να κάνει injection μερικά καρέ (frames) σε ένα δίκτυο WPA TKIP με QoS. Το Tkiptun-ng ξεκινάει από την απόκτηση ενός πακέτου και του MIC (Message Integrity Check). Αυτό γίνεται μέσω της μεθόδου chopchop. Μόλις γίνει αυτό, ο αλγόριθμος MICHAEL αντιστρέφει το MIC κλειδί που χρησιμοποιείτε για να προστατεύσει τα πακέτα που στέλνονται από το AP στον πελάτη. Σε αυτό το σημείο, Tkiptun-ng έχει ανακτήσει πλήρως το MIC οπότε και γνωρίζει το keystram για το σημείο πρόσβασης του πελάτη. Στη συνέχεια, χρησιμοποιώντας το αρχείο XOR, μπορείτε να δημιουργήσετε νέα πακέτα και να τα κάνετε injection στο δίκτυο. Η δημιουργία και το injection γίνονται με την χρήση των υπολοίπων προγραμμάτων της Suite Aircrack-ng.

Η γενική σύνταξη της εντολής Tkiptun-ng είναι η παρακάτω:

- ***tkiptun-ng <options> <replay interface>***

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Tkiptun-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=tkiptun-ng&DokuWiki=a0e82a76d7d1fbbbbb714261900cf514

2.1.17 Wesside-ng

Το Wesside-ng είναι ένα εργαλείο που σας επιτρέπει να αποκτήσετε το WEP κλειδί ενός Access Point μέσα σε λίγα μόλις λεπτά. Πρώτα εντοπίζει το δίκτυο και συσχετίζετε με αυτό, εξασφαλίζει PRGA (pseudo random generation algorithm) xor data, προσδιορίζει το μοντέλο του δικτύου και στην συνέχεια εγκαθιστά ένα TAP interface ώστε να μπορεί να επικοινωνήσει με το Access Point χωρίς να απαιτείται το κλειδί WEP. Όλα αυτά γίνονται χωρίς την δικιά σας παρέμβαση.

Η γενική σύνταξη της εντολής Wesside-ng είναι η παρακάτω:

- ***wesside-ng -i mon0***

Περισσότερες πληροφορίες και παραδείγματα σχετικά με την εκτέλεση της Wesside-ng μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.aircrack-ng.org/doku.php?id=wesside-ng&DokuWiki=a0e82a76d7d1fbbbbb714261900cf514

3. Κεφάλαιο – Password Cracking

3.1 Συνοπτική Περιγραφή

Στην κρυπτανάλυση καθώς και στην ασφάλεια πληροφοριακών συστημάτων, το Password Cracking είναι η διαδικασία ανάκτησης των κωδικών πρόσβασης από τα δεδομένα που έχουν αποθηκευτεί ή μεταδίδονται από ένα σύστημα υπολογιστών. Μια κοινή προσέγγιση είναι να προσπαθεί ο επιτιθέμενος με διάφορες πιθανές εικασίες να μαντέψει τον κωδικό ασφαλείας κάποιου χρήστη. Μια άλλη κοινή προσέγγιση είναι να θεωρήσουμε ότι ο χρήστης έχει 'ξεχάσει' τον κωδικό ασφαλείας του και ζητεί την αλλαγή του από κάποια υπηρεσία (π.χ. να του σταλθεί ένας καινούργιος κωδικός στον λογαριασμό αλληλογραφίας του).

Ο σκοπός του Password Cracking θα μπορούσε να βοηθήσει έναν χρήστη να ανακτήσει έναν ξεχασμένο κωδικό πρόσβασης (αν και η δημιουργία ενός νέου κωδικού πρόσβασης αποτελεί μικρότερο κίνδυνο για την ασφάλεια, αλλά απαιτεί την μεσολάβηση ενός διαχειριστή), να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα υπολογιστών ή ως ένα προληπτικό μέτρο από διαχειριστές ενός υπολογιστικού συστήματος προκειμένου να ελέγξουν για εύκολους κωδικούς πρόσβασης.[6]

3.2 Password Strength

Η ισχύς ενός κωδικού (Password Strength) είναι ένα μέτρο της αποτελεσματικότητας του κωδικού πρόσβασης στην αντίσταση να τον βρει κάποιος με μια επίθεση τύπου Brute-Force attack. Κατά κοινή ομολογία, εκτιμάτε πόσες φορές ο επιτιθέμενος θα χρειαστεί προκειμένου να βρει τον κωδικό. Η δύναμη λοιπόν ενός κωδικού εξαρτάται από την συνάρτηση μήκους του κωδικού, την αποτελεσματικότητα καθώς και ποσό απρόβλεπτος μπορεί να είναι.

Χρησιμοποιώντας ισχυρούς κωδικούς πρόσβασης μειώνετε συνολικά ο κίνδυνος παραβίασης της ασφάλειας, αλλά ισχυροί κωδικοί πρόσβασης δεν αντικαθιστούν την ανάγκη για επιπρόσθετα μέτρα ασφαλείας. Η αποτελεσματικότητα ενός κωδικού πρόσβασης καθορίζεται ιδιαίτερα από το σχεδιασμό και την υλοποίηση του λογισμικού του συστήματος ταυτότητας, τον αριθμό των προσπαθειών που ένας επιτιθέμενος μπορεί να επιχείρηση προκειμένου να βρει τον κωδικό και τον τρόπο με τον οποίο οι πληροφορίες σχετικά με τους κωδικούς πρόσβασης των χρηστών αποθηκεύονται και μεταδίδονται με ασφάλεια. Ωστόσο ελλοχεύουν και άλλοι κίνδυνοι που αφορούν τα μέτρα ασφαλείας που έχουν παρθεί σε ένα σύστημα υπολογιστών τα οποία παραβιαζοντάς τα, η ισχύς ενός κωδικού πρόσβασης δεν παίζει πια απολύτως κανέναν ρολό. Μέσα στους κινδύνους αυτούς περιλαμβάνονται wiretapping, phishing, keystroke logging, social engineering, dumpster diving, side-channel attacks, and software vulnerabilities.[7]

Υπάρχουν δυο (2) παράγοντες για να καθορίσουμε την ισχύ που θα έχει ο κωδικός πρόσβασης: ο πρώτος αφορά την ευκολία με την οποία ο επιτιθέμενος

[6] http://en.wikipedia.org/wiki/Password_cracking
[7] http://en.wikipedia.org/wiki/Password_strength

μπορεί να ελέγχει την εγκυρότητα των κωδικών που έχει μαντέψει και δεύτερον τον μέσο όρο προσπαθειών που θα χρειαστεί ο επιτιθέμενος να επιχειρήσει προκειμένου να βρει τον σωστό κωδικό πρόσβασης. Ο πρώτος παράγοντας προσδιορίζεται από το πώς ο κωδικός πρόσβασης αποθηκεύεται και ποια είναι η χρήση του (π.χ. είσοδος σε Web Banking Account), ενώ ο δεύτερος παράγοντας καθορίζεται από το πόσο 'χρονών' είναι ο κωδικός, ποια σύμβολα χρησιμοποιεί και πως έχει δημιουργηθεί.

3.3 Δημιουργία κωδικών πρόσβασης (Password Creation)

Οι κωδικοί πρόσβασης δημιουργούνται είτε αυτόματα[8] είτε από τον χρήστη. Συνήθως, μηχανές κατά την δημιουργία λογαριασμών για συστήματα υπολογιστών ή τοποθεσίες Web στο Internet, ζητούν από τους χρήστες να ακολουθήσουν ένα σύνολο από κανόνες προκειμένου να επιτευχτεί μεγάλη πολυπλοκότητα στο θέμα ασφαλείας του κωδικού. Στην περίπτωση αυτή ο επιτιθέμενος μόνο εκτιμήσεις μπορεί να κάνει όπως για παράδειγμα πιο είναι το μήκος του κωδικού δεδομένου ότι όλοι οι κωδικοί μπορεί να ξεκινάνε από 6 χαρακτήρες και πάνω.

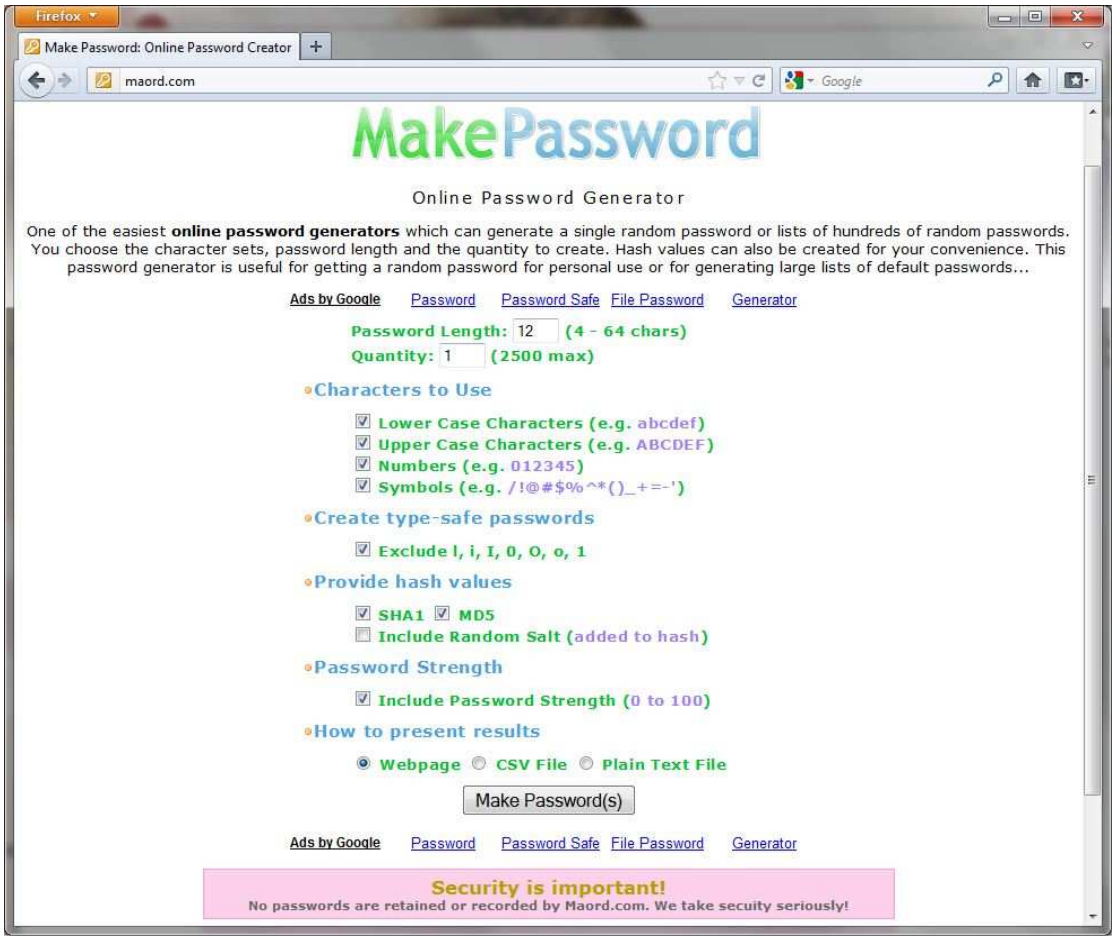
Χαρακτηριστικό παράδειγμα τέτοιου κωδικού φαίνετε παρακάτω. Συγκεκριμένα το πρόγραμμα ζητεί από τον χρήστη να ακολουθήσει κάποιους κανόνες. Οι κανόνες αυτοί είναι: ο κωδικός να έχει το ελάχιστο μήκος 8 χαρακτήρες καθώς και μέσα σε αυτούς τους χαρακτήρες να περιέχονται κεφαλαία και μικρά γράμματα, αριθμούς και σύμβολα.[9]

Εικόνα 58. The Password Meter.[10]

Από την άλλη η αυτόματη δημιουργία ενός κωδικού πρόσβασης αν γίνει με σωστό τρόπο μπορεί να αποφευχθεί η οποιαδήποτε σχέση μεταξύ ενός κωδικού πρόσβασης και του χρήστη του. Για παράδειγμα, το όνομα μιας πόλης είναι μάλλον απίθανο να προκύψει από ένα τέτοιο σύστημα. Για έναν κωδικό πρόσβασης που επιλέγεται από ένα τέτοιο αξιόπιστο σύστημα η επίθεση Brute-Force attack μπορεί να οδηγήσει σε αποτυχία. Ωστόσο, η δημιουργία τυχαίων κωδικών πρόσβασης καθιστά αρκετά δύσκολη την απομνημόνευση τους από τον χρήστη με αποτέλεσμα να αποφεύγεται η χρήση της.

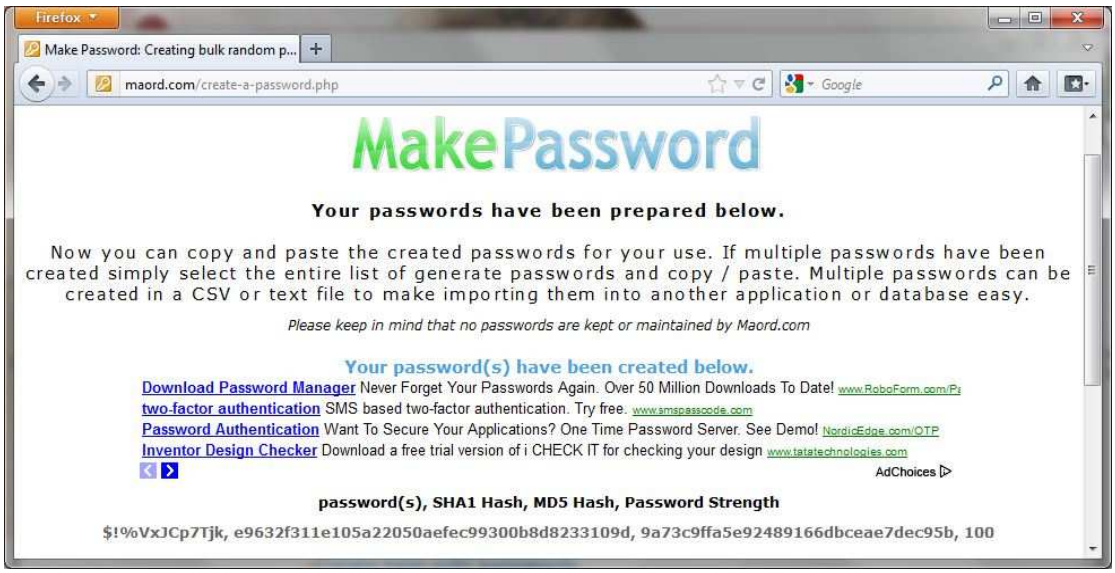
Και σε αυτή την περίπτωση μπορούμε να δούμε το παράδειγμα μιας τέτοιας εφαρμογής. Για την αυτόματη δημιουργία ενός κωδικού επισκεφτήκαμε την σελίδα http://maord.com/ όπως μπορούμε να δούμε και παρακάτω.

[8] Η δημιουργία τυχαίων κωδικών πρόσβασης κατά την επίθεση Brute-Force attack μπορούν να υπολογιστούν με δεδομένη ακρίβεια.
[9] http://en.wikipedia.org/wiki/Password_strength
[10] http://www.passwordmeter.com/



Εικόνα 59. Δημιουργία αυτόματου κωδικού ασφαλείας.

Όπως μπορούμε να δούμε και παρακάτω μας δημιούργησε τον κωδικό που του ζητήσαμε μαζί με την σύνοψη του SHA1 και MD5.



Εικόνα 60. Εμφάνιση κωδικού ασφαλείας.

3.4 Χρόνος απαίτησης για αναζήτηση κωδικών πρόσβασης

Ο χρόνος που απαιτείται για να 'σπάσετε' έναν κωδικό πρόσβασης σχετίζεται άμεσα με την δύναμη του συγκεκριμένου κωδικού πρόσβασης. Οι περισσότεροι μέθοδοι Password Cracking απαιτούν από κάποιον υπολογιστή να παράγει πολλούς διαφορετικούς κωδικούς για τον υποψήφιο όπου ταυτόχρονα εφαρμόζεται και ο καθένας από αυτούς. Χαρακτηριστικό είναι το παράδειγμα της τεχνικής Brute-Force στην οποία ένας υπολογιστής δοκιμάζει κάθε δυνατό συνδυασμό κλειδιών ή γραμμάτων μέχρι να επιτύχει.

Οι περισσότερες κοινές τεχνικές Password Cracking όπως για παράδειγμα η Brute-Force attack, Dictionary attack, Hybrid attack (αναλυτικότερα για τις τεχνικές Password Cracking θα δούμε παρακάτω) προσπαθούν να μειώσουν τον αριθμό δοκιμών που απαιτούνται προκειμένου να βρεθεί ένας κωδικός πρόσβασης. Φυσικά ένας πολύπλοκος κωδικός έχει σαν αποτέλεσμα να αυξάνει εκθετικά τον αριθμό των κωδικών πρόσβασης που πρέπει να ελέγξει ο επιτιθέμενος. Έτσι λοιπόν καθίσταται και δύσκολο η πιθανότητα να βρεθεί αυτός ο κωδικός χρησιμοποιώντας οποιαδήποτε από τις παραπάνω τεχνικές.

Κατά προσέγγιση λοιπόν, πόσο χρόνο απαιτείται από έναν υπολογιστή ή καλύτερα από ένα σύμπλεγμα από ηλεκτρονικούς υπολογιστές να μαντέψουν διάφορους κωδικούς; Τα στοιχεία που θα δείξουμε παρακάτω είναι κατά προσέγγιση και είναι ο μέγιστος χρόνος που απαιτείται για να βρούμε κωδικούς πρόσβασης χρησιμοποιώντας μια απλή περίπτωση της τεχνικής Brute-Force attack.[11]

Κατηγορίες Επιθέσεων (Classes of Attack)

Παρακάτω ακολουθούν 6 κλάσεις ανάλογα με την ταχύτητα σπασίματος κωδικών πρόσβασης. Αυτές είναι:

- **Class A: 10.000 passwords / sec**. Χρησιμοποιείται συνήθως για την ανάκτηση των κωδικών πρόσβασης του Microsoft Office σε έναν Pentium 100 (100MHz).
- **Class B: 100.000 passwords / sec**. Χρησιμοποιείται συνήθως για την ανάκτηση κωδικών Windows Password Cache (.PWL) σε έναν Pentium 100 (100MHz).
- **Class C: 1.000.000 passwords / sec**. Χρησιμοποιείτε συνήθως για την ανάκτηση κωδικών πρόσβασης σε αρχεία ARJ[12] ή ZIP σε έναν Pentium 100 (100MHz).
- **Class D: 10.000.000 passwords / sec**. Απευθύνεται σε Dual Processor Pc.
- **Class E: 100.000.000 passwords / sec**. Απευθύνεται σε Workstation ή σε πολλά Pc που δουλεύουν μαζί.
- **Class F: 1.000.000.000 passwords / sec**. Χρησιμοποιείτε για μεσαίας έως μεγάλης κλίμακας κατανεμημένα συστήματα πληροφορικής, υπερυπολογιστές.

[11] http://www.lockdown.co.uk/?pg=combi
[12] http://en.wikipedia.org/wiki/ARJ

10 Χαρακτήρες

Μονό αριθμοί. Όπως μπορείτε να δείτε, επιλέγοντας έναν κωδικό από ένα τόσο μικρό εύρος χαρακτήρων είναι μια κακή ιδέα.

Αριθμοί	0123456789						
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	100	Instant	Instant	Instant	Instant	Instant	Instant
3	1000	Instant	Instant	Instant	Instant	Instant	Instant
4	10000	Instant	Instant	Instant	Instant	Instant	Instant
5	100000	10 Sec	Instant	Instant	Instant	Instant	Instant
6	1 Million	$1^{1/2}$ Mins	10 Sec	Instant	Instant	Instant	Instant
7	10 Million	17 Mins	$1^{1/2}$ Mins	$1^{1/2}$ Mins	Instant	Instant	Instant
8	100 Million	$2^{3/4}$ Hours	17 Mins	$1^{1/2}$ Mins	10 Sec	Instant	Instant
9	1000 Million	28 Hours	$2^{3/4}$ Hours	17 Mins	$1^{1/2}$ Mins	10 Sec	Instant

Πίνακας 8. Χρόνοι Ανάκτησης Κωδικών - Μόνο Αριθμοί

26 Χαρακτήρες

Το πλήρες λατινικό αλφάβητο, είτε κεφάλαια είτε πεζά (όχι και τα δυο στην προκειμένη περίπτωση).

Κεφαλαία	ABCDEFGHIJKLMNOPQRSTUVWXYZ						
Μικρά	abcdefghijklmnopqrstuvwxyz						
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	676	Instant	Instant	Instant	Instant	Instant	Instant
3	17576	< 2 Sec	Instant	Instant	Instant	Instant	Instant
4	456976	46 Sec	5 Sec	Instant	Instant	Instant	Instant
5	11.8 Million	20 Mins	2 Mins	12 Sec	Instant	Instant	Instant
6	308.9 Million	$8^{1/2}$ Hours	$51^{1/2}$ Mins	5 Mins	30 Sec	3 Sec	Instant
7	8 Billion	9 Days	22 Hours	$2^{1/4}$ Hours	13 Mins	$1^{1/2}$ Mins	8 Sec
8	200 Billion	242 Days	24 Days	$2^{1/2}$ Days	348 Mins	35 Mins	$3^{1/2}$ Mins
9	5.4 Trillion	17 Years	21 Mon.	63 Days	$6^{1/4}$ Days	15 Hour	$1^{1/2}$ Hours
10	141 Trillion	447 Years	45 Years	$4^{1/2}$ Years	163 Days	16 Days	$39^{1/4}$ Hour
12	95 Quadrillion	302.603 Years	30.260 Y	3.026 Y	302 Years	30 Year	3 Year
15	1.6 Sextillion	53 Trillion Y	532 Mil. Y	53 Mill Y	5 Mill Y	531.855 Y	53.185 Y
20	19.9 Octillion	63 Quadr. Y	6.3 Qua Y	631 Tri Y	63.1 Tri Y	6.3 Tri. Y	631 Bil Y

Πίνακας 9. Χρόνοι Ανάκτησης Κωδικών - Κεφαλαία - Πεζά (όχι και τα 2)

36 Χαρακτήρες

Το πλήρες λατινικό αλφάβητο, είτε κεφαλαία είτε πεζά (όχι και τα δυο στην προκειμένη περίπτωση) καθώς και τους αριθμούς.

Κεφαλαία	ABCDEFGHIJKLMNOPQRSTUVWXYZ						
Μικρά	abcdefghijklmnopqrstuvwxyz						
Αριθμοί	0123456789						
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	1296	Instant	Instant	Instant	Instant	Instant	Instant
3	46656	4 Sec	Instant	Instant	Instant	Instant	Instant
4	1,6 Million	$2^{1/2}$ Mins	16 Sec	$1^{1/2}$ Sec	Instant	Instant	Instant
5	60.4 Million	$1^{1/2}$ Hours	10 Mins	1 Mins	Instant	Instant	Instant

Πίνακας 10. Χρόνοι Ανάκτησης Κωδικών-Αριθμοί, Κεφαλαία-Πεζά (οχι και τα 2)

52 Χαρακτήρες

Αυτή την φορά θα προσπαθήσουμε όλο το αλφάβητο, χρησιμοποιώντας ένα μίγμα των κεφαλαίων και πεζών γραμμάτων, που ουσιαστικά διπλασιάζει τον αριθμό των συνδυασμών, σε σύγκριση με μόλις μια μεμονωμένη περίπτωση (π.χ. Κεφαλαία ή πεζά).

Κεφαλαία & Πεζά	AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz					
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	2704	Instant	Instant	Instant	Instant	Instant	Instant
3	140608	14 Sec	< 2 Sec	Instant	Instant	Instant	Instant
4	7.3 Million	$12^{1/2}$ Mins	$1^{1/4}$ Mins	8 Sec	Instant	Instant	Instant
5	380 Million	$10^{1/2}$ Hours	1 Hour	6 Mins	38 Sec	4 Sec	Instant
6	19 Billion	23 Days	$2^{1/4}$ Days	$5^{1/2}$ Hours	33 Mins	$3^{1/4}$ Mins	19 Sec
7	1 Trillion	$3^{1/4}$ Years	119 Days	12 Days	$28^{1/2}$ Hour	3 Hours	17 Mins
8	53 Trillion	$169^{1/2}$ Years	17 Years	$1^{1/2}$ Years	62 Days	6 Days	15 Hours
9	2.7 Quadrillion	8.815 Years	881 Years	88 Years	9 Years	322 Days	32 Days

Πίνακας 11. Χρόνοι Ανάκτησης Κωδικών - Κεφαλαία - Πεζά

62 Χαρακτήρες

Συνδυασμός αριθμών, κεφαλαίων και πεζών γραμμάτων.

Κεφαλαία – Πεζά & Αριθμοί	0123456789AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz					
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	3844	Instant	Instant	Instant	Instant	Instant	Instant
3	238328	23 Sec	< 3 Sec	Instant	Instant	Instant	Instant
4	15 Million	24½ Mins	2½ Mins	15 Sec	< 2 Sec	Instant	Instant
5	916 Million	1 Days	2½ Hours	15¼ Mins	1½ Mins	9 Sec	Instant
6	57 Billion	66 Days	6½ Days	16 Hours	1½ Hours	9½ Mins	56 Sec
7	3.5 Trillion	11 Years	1 Year	41 Days	4 Days	10 Hours	58 Mins
8	218 Trillion	692 Years	69¼ Year	7 Years	253 Days	25¼ Days	60½ Hour

Πίνακας 12. Χρόνοι Ανάκτησης Κωδικών - Αριθμοί, Κεφαλαία - Πεζά

86 Χαρακτήρες

Συνδυασμός κεφαλαίων και πεζών γραμμάτων καθώς και ειδικών χαρακτήρων.

Κεφαλαία – Πεζά & Ειδικοί Χαρακτήρες		AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz <SP>!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~					
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	3844	Instant	Instant	Instant	Instant	Instant	Instant
8	218 Trillion	9.488 Years	948 Years	94 Years	57 Years	346 Days	34 Days

Πίνακας 13. Χρόνοι Ανάκτησης Κωδικών – Ειδικοί Χαρακτήρες, Κεφαλαία - Πεζά

96 Χαρακτήρες

Συνδυασμός κεφαλαίων και πεζών γραμμάτων, αριθμών και ειδικών χαρακτήρων.

Κεφαλαία – Πεζά, Αριθμοί & Ειδικοί Χαρακτήρες		0123456789AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz <SP>!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~					
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	9216	Instant	Instant	Instant	Instant	Instant	Instant
3	884736	88½ Secs	9 Sec	Instant	Instant	Instant	Instant
4	85 Million	2¼ Hours	14 Mins	1½ Mins	8½ Secs	Instant	Instant
5	8 Billion	9½ Days	22½ Hour	2¼ Hours	13½ Mins	1¼ Mins	8 Sec
6	782 Billion	2½ Years	90 Days	9 Days	22 Hours	2 Hours	13 Mins
7	75 Trillion	238 Years	24 Year	2½ Years	87 Days	8½ Days	20 Hours
8	7.2 Quadrillion	22.875 Year	2.287 Y	229 Years	23 Years	2¼ Years	83½ Days

Πίνακας 14. Χρόνοι Ανάκτησης Κωδικών - Αριθμοί, Κεφαλαία - Πεζά, Ειδικοί Χαρακτήρες

Παραδείγματα

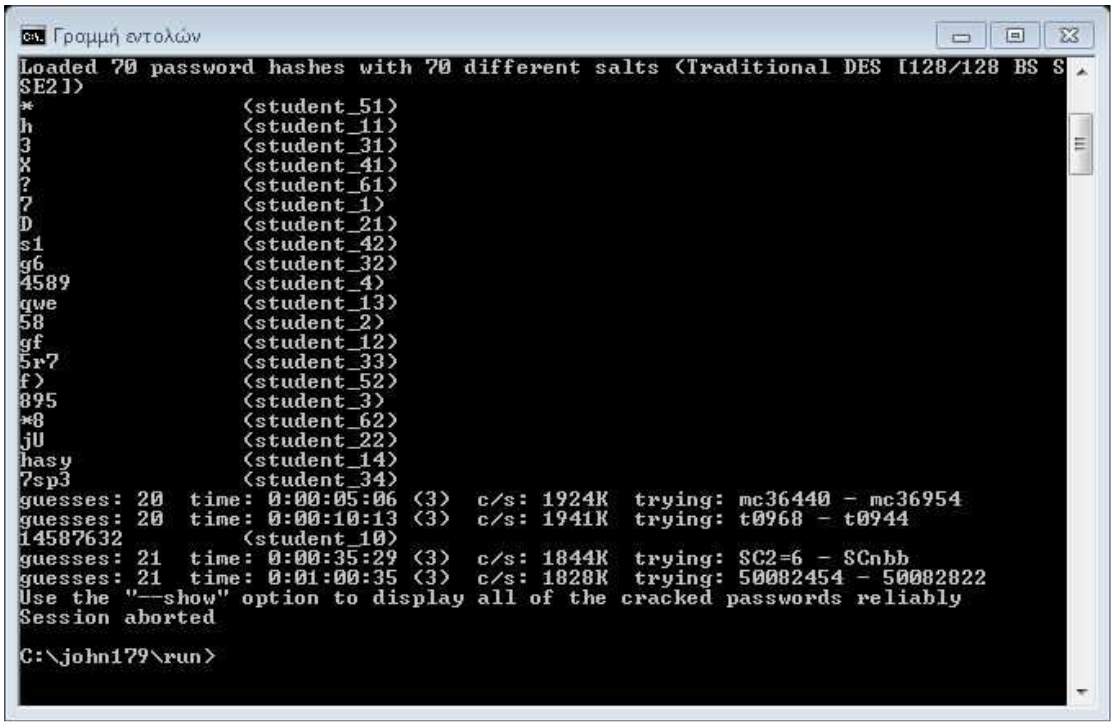
Στον επόμενο πίνακα βλέπουμε μόνο μερικά παραδείγματα που αποδεικνύουν την ορθότητα ορισμένων τύπων κωδικών πρόσβασης. Χρησιμοποιώντας λοιπόν τις πληροφορίες που αναφέρονται στους παραπάνω πίνακες θα είστε σε θέση να φτιάξετε τα δικά σας παραδείγματα.

Sample Passwords		Class of Attack					
Password	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
Darren	308.9 Million	8½ Hours	51½ Mins	5 Mins	30 Sec	3 Secs	Instant
Land3rz	3.5 Trillion	11 Years	1 Year	41 Days	4 Days	10 Hours	58 Mins
B33r&Mug	7.2 Quadrillion	22.875 Years	2.287 Years	229 Years	23 Years	2¼ Years	83½ Days

Πίνακας 15. Πίνακας 5. Χρόνοι Ανάκτησης Κωδικών - Παραδείγματα

Για να φτιάξετε ένα password για το Unix ουσιαστικά αυτό που έχετε να κάνετε είναι να προσθέσετε απλώς μια νέα γραμμή στο password αρχείο σας για κάθε νέο χρήστη. Έχοντας δημιουργήσει λοιπόν ένα τέτοιο αρχείο για όλες τις περιπτώσεις

κωδικών που αναφέραμε παραπάνω στην συνέχεια τρέξαμε το αρχείο newpasswds.txt με το John The Ripper στην απλή του μορφή (john newpasswds.txt). Όπως θα δούμε και παρακάτω, στο χρονικό διάστημα της μιας ώρας το πρόγραμμα κατάφερε να αποκρυπτογραφήσει 21 κωδικούς από αυτούς που δημιουργήσαμε.



Εικόνα 61. Αποκρυπτογράφηση Unix Passwords.

Περισσότερη βοήθεια σχετικά με την δημιουργία κωδικών Unix μπορείτε να επισκεφτείτε την διεύθυνση: http://www.javascriptsource.com/passwords/unix-crypt(3)-encryption.html.

3.5 Τεχνικές Password Cracking

Αφού οι κωδικοί αποτελούν ένα από τα θεμέλια της ασφάλειας για τα περισσότερα συστήματα και δίκτυα, το μάντεμα ή το "σπάσιμο" κωδικών βρίσκεται ψηλά στην λίστα προτεραιοτήτων των επίδοξων εισβολέων που προσπαθούν να αποκτήσουν πρόσβαση σε αυτά τα συστήματα.

Τα προγράμματα εύρεσης κωδικών πρόσβασης χρησιμοποιούν τρείς βασικές τεχνικές:[13]

- **Brute - Force attack:** Ο απλούστερος αλλά λιγότερο αποτελεσματικός και πιο αργός τρόπος εύρεσης κωδικών πρόσβασης είναι η επίθεση Brute - Force attack, η οποία δοκιμάζει συστηματικά όλους τους πιθανούς συνδυασμούς γραμμάτων, ψηφίων και ειδικών χαρακτήρων κάθε δυνατού μήκους μέχρι να βρεθεί κάποιος κωδικός ή μέχρι να κολλήσει το πρόγραμμα ή να τα παρατήσει ο εισβολέας. Για παράδειγμα ένα συνθηματικό μήκους M χαρακτήρων το χειρότερο σενάριο είναι η παραγωγή και δοκιμή M^N συνθηματικών, όπου N ο αριθμός των πιθανών χαρακτήρων που μπορούν να χρησιμοποιηθούν για την

[13] http://clubs.pathfinder.gr/OceanPasswordS/453738

παραγωγή του συνθηματικού. Μειώνοντας το σύνολο N, π.χ. λαμβάνοντας υπόψη μόνο τα γράμματα του αλφαβήτου, μικρά και κεφαλαία (που σύμφωνα με έρευνες συνήθως από αυτά κατασκευάζονται τα συνθηματικά), μειώνεται κατά πολύ ο χρόνος εκτέλεσης από ότι αν γινόταν χρήση του συνόλου των εκτυπώσιμων ASCII χαρακτήρων. Φυσικά, γρηγορότερα αποτελέσματα μπορούν να επιτευχθούν με τον συνδυασμό πολλαπλών συστημάτων. Η επίθεση Brute - Force attack χρησιμοποιείται συνήθως όταν αποτυγχάνει η επίθεση λεξικού.

- **Dictionary attack:** Η επίθεση λεξικού (dictionary attack), αποτελεί μια βελτιστοποίηση της επίθεσης Brute - Force attack. Χρησιμοποιεί ένα λεξικό (μια λίστα λέξεων που χρησιμοποιούνται συχνά σαν κωδικοί) κοινών κωδικών το οποίο έχει δημιουργηθεί από τις συνδυασμένες εμπειρίες των εισβολέων όσο αφορά τους περισσότερο κοινούς κωδικούς.

- **Hybrid attack:** Ο συνδυασμός επίθεσης λεξικού και Brute - Force attack λέγεται υβριδική επίθεση (hybrid attack). Οι χρήστες που προσθέτουν απλές δοκιμασμένες τεχνικές επιλογής κωδικών ασφάλειας όπως το να προσθέτουν αριθμούς στο τέλος του κωδικού τους μπορούν συχνά να παρακάμψουν τον κίνδυνο μιας επίθεσης λεξικού. Η καλύτερη προσέγγιση λοιπόν για την εύρεση κωδικών είναι γενικά η υβριδική επίθεση που χρησιμοποιεί επίθεση λεξικού αλλά εφαρμόζοντας παράλληλα και κάποιους κανόνες. Τυπικά, ένα πρόγραμμα που υλοποιεί αυτήν την επίθεση, μπορεί να εναλλάσσει συστηματικά τους πεζούς με τους κεφαλαίους χαρακτήρες όπως επίσης και να δημιουργεί μικρά κομμάτια χαρακτήρων και τα προσθέτει στην αρχή και στο τέλος των λέξεων από το λεξικό. Για παράδειγμα, ο κωδικός ασφαλείας “daisy123” πιθανότατα θα εντοπιζόταν πολύ γρήγορα από μια υβριδική επίθεση, η οποία θα δοκίμαζε την λέξη “daisy” προσθέτοντας διάφορους χαρακτήρες πριν και μετά από αυτήν. Το L0phtCrack[14] (η τωρινή του έκδοση ονομάζεται LC4) είναι ένα φημισμένο πρόγραμμα εύρεσης κωδικών πρόσβασης που μπορεί να υλοποιήσει υβριδικές επιθέσεις όπως επίσης και το πρόγραμμα John the Ripper.

3.6 Σκοπός

Στο κεφάλαιο αυτό θα επικεντρωθούμε με το πώς μπορούμε να επιτύχουμε την ανάκτηση διαφόρων κωδικών πρόσβασης από μια λίστα κρυπτογραφημένων κωδικών μέσα σε ένα συγκεκριμένο χρονικό διάστημα. Το πρόγραμμα που θα χρησιμοποιήσουμε είναι το JTR 1.7.9 (John The Ripper) στην έκδοση του.

3.7 JTR (John The Ripper)

Το JTR (John The Ripper)[15] είναι ένα δωρεάν πρόγραμμα για ‘σπάσιμο’ κωδικών. Αρχικά αναπτύχτηκε για το λειτουργικό σύστημα UNIX, ενώ σήμερα λειτούργει σε δεκαπέντε (15) διαφορετικές πλατφόρμες (για έντεκα συγκεκριμένες αρχιτεκτονικές του UNIX, DOS, WIN32, BeOS και OpenVMS). Μπορεί να χρησιμοποιηθεί για τον έλεγχο διαφορετικών κρυπτογραφημένων κωδικών

[14] http://en.wikipedia.org/wiki/L0phtCrack
[15] http://www.openwall.com/john/

πρόσβασης και κυρίως απευθύνεται σε UNIX.[16] Για να κατεβάσετε το πρόγραμμα αρκεί να επισκεφτείτε την παρακάτω διεύθυνση: http://www.openwall.com/john/[17]

Προς το παρόν το John The Ripper υποστηρίζει τους εξής τύπους κωδικών πρόσβασης:

- Το παραδοσιακό DES-based Unix crypt – για συστήματα Unix (Solaris, AIX), Mac OS X 10.2, Linux και *BSD
- BSDI-style extended DES-based crypt – BSD/OS, *BSD (όχι τα προεπιλεγμένα)
- FreeBSD-style MD5-based crypt – κυρίως Linux, FreeBSD, NetBSD, Cisco IOS, OpenBSD (όχι τα προεπιλεγμένα)
- OpenBSD-style Blowfish-based crypt – OpenBSD, ορισμένα Linux, άλλα *BSD και Solaris 10 (όχι τα προεπιλεγμένα)
- Kerberos AFS DES-based hashes
- LM (LanMan) DES-based hashes – Windows NT/2000/XP/2003, Mac OS X 10.3
- NTLM MD4-based hashes – Windows NT/2000/XP/2003/Vista (νέο στο 1.7.3 Pro)
- Mac OS X 10.4+ salted SHA-1 hashes (νέο στο 1.7.3 Pro)

Οι πληροφορίες για τους λογαριασμούς και passwords στο UNIX βρίσκονται συνήθως στο αρχείο /etc/passwd. Σε κάποια συστήματα το αρχείο αυτό είναι προσβάσιμο σε όλους τους χρήστες (κακή πρακτική από τον administrator). Για να δείτε τα αρχείο αυτό εκτελείτε σε ένα UNIX μηχάνημα την εντολή: > cat /etc/passwd OR > ypcat passwd. Ένα τέτοιο υπόδειγμα αρχείου είναι το παρακάτω (passwds.txt):

[16] http://en.wikipedia.org/wiki/John_the_Ripper

[17] Όταν κατεβάσετε το JTR δεν θα δείτε κάποιο εκτελέσιμο αρχείο. Αντ' αυτού θα κατέβουν τα δυαδικά αρχείου του προγράμματος και θα πρέπει στην συνεχεία να το εκτελέσετε μέσω cmd (Command Prompt). Κάνοντας λοιπόν αποσυμπίεση του φακέλου που θα κατέβει στην συνέχεια θα μεταφέρετε τα αρχεία σας στον "C:\" (Αυτό είναι ενδεικτικό και γίνεται για ευκολία περισσότερο του χρήστη).

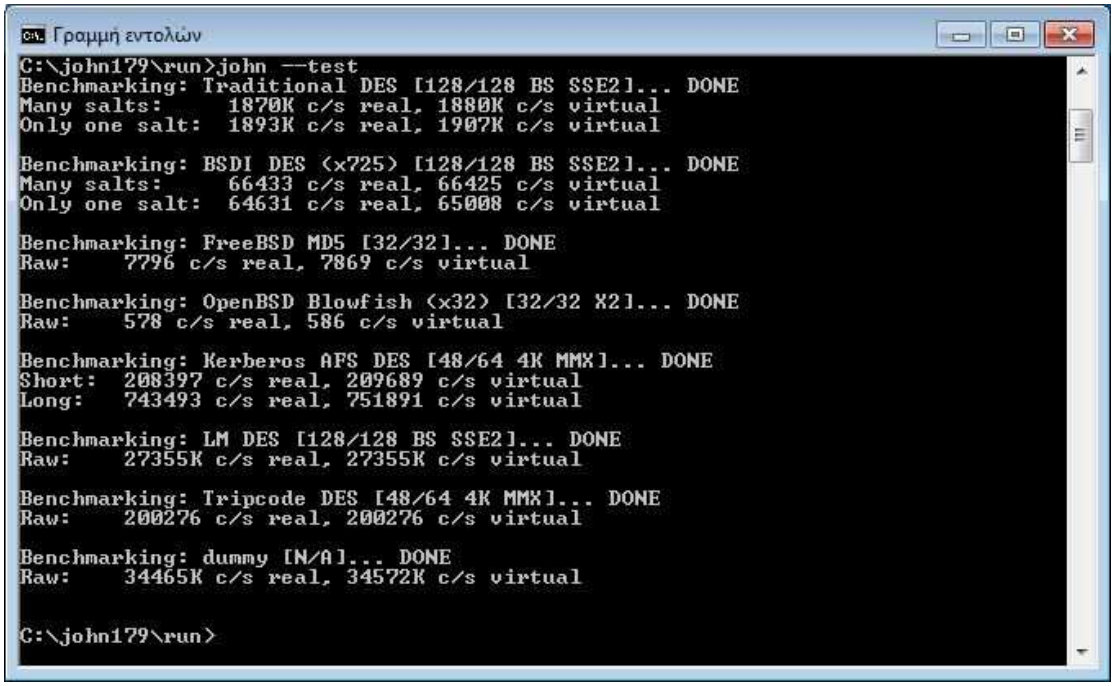
Εικόνα 62. Πληροφοριες λογαριασμων χρηστων.

Μια πολύ ενδιαφέρουσα δυνατότητα του John The Ripper είναι τα rules του, με τα οποία μπορείτε να αντικαταστήσετε το o με το 0, το i με το 1, το a με το @ και πάει λέγοντας. Έτσι θα μπορούσατε να δώσετε στο πρόγραμμα ένα dictionary που περιλαμβάνει λέξεις με ειδικούς χαρακτήρες όπου το JTR στην συνέχεια με τα κατάλληλα rules, θα μετατρέψει τις λέξεις που περιλαμβάνουν ειδικούς χαρακτήρες σε standard λέξεις του dictionary.

Περισσότερες πληροφορίες και παραδείγματα σχετικά με ρα rules του JTR μπορείτε να επισκεφτείτε την παρακάτω σελίδα: http://www.openwall.com/john/doc/RULES.shtml

3.8 JTR – Δοκιμές per second

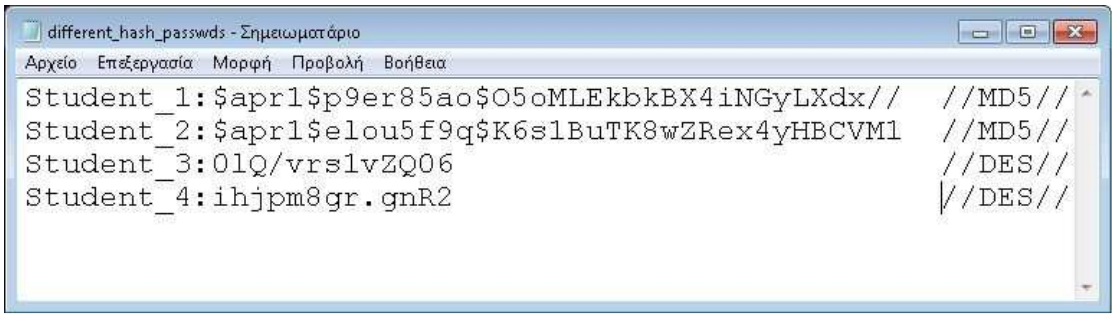
Το John The Ripper έχει την ικανότητα να διατρέχει το δευτερόλεπτο πολλούς πιθανούς συνδυασμούς κωδικών. Κύριος παράγοντας σε αυτό είναι το μηχάνημα που τρέχετε το JTR. Παρακάτω μπορούμε να δούμε τους συνδυασμούς κωδικών ανά δευτερόλεπτο σε μηχάνημα με Windows 7 Ultimate 64-bit, 4 GB RAM και επεξεργαστή Dual Core AMD Athlon X2 7850 (3.0GHz overclocked).



Εικόνα 63. John The Ripper - Test

Αυτό που θα πρέπει να προσέξετε είναι το C/S. Το C/S ουσιαστικά αναφέρεται στις λέξεις combinations per second, δηλαδή συνδυασμοί usernames και passwords το δευτερόλεπτο. Όπως παρατηρούμε λοιπόν έχουμε τα real c/s και virtual c/s. Αυτά αντιστοιχούν στον πραγματικό και εικονικό χρόνο επεξεργασίας αντίστοιχα. Τα δυο (2) αποτελέσματα θα διαφέρουν μεταξύ τους και γιατί το virtual σας δείχνει πόσους συνδυασμούς μπορεί να τρέξει όταν δεν τρέχει κάποια άλλη διεργασία στον υπολογιστή σας. Το real απευθύνεται στην εκτέλεση του προγράμματος την δεδομένη χρονική στιγμή.

Όπως μπορείτε να παρατηρήσετε και στην παραπάνω εικόνα το John The Ripper έχει την ικανότητα να αποκρυπτογραφήσει ένα μεγάλο εύρος κωδικών ανάλογα με το τύπο κρυπτογράφησής του. Τι συμβαίνει όμως στην περίπτωση που μέσα στο αρχείο .txt πολλοί κωδικοί δεν έχουν κρυπτογραφηθεί με τον ίδιο αλγόριθμο κρυπτογράφησης; Η απάντηση που θα έδιναν όλοι είναι ότι το πρόγραμμα θα ξεκινήσει την αποκρυπτογράφηση όλων των κωδικών ανεξαρτήτου κωδικοποίησης μέσα στο αρχείο με την σειρά. Αυτή η απάντηση λοιπόν θα ήταν λάθος. Όπως μπορείτε να δείτε και παρακάτω έχει δημιουργηθεί ένα νέο αρχείο με την χρήση διαφόρων αλγορίθμων κωδικοποίησης.



Εικόνα 64. Κρυπτογράφηση κωδικών με διαφόρους τύπους αλγορίθμων κωδικοποίησης.

Παρατηρώντας καλυτέρα πιο κάτω θα δείτε ότι εμφάνισε ένα μήνυμα προειδοποίησης κατά την αποκρυπτογράφηση των κωδικών. Το αρχείο μας όπως είπαμε και παραπάνω περιέχει μέσα διαφόρους τύπους αλγορίθμων κωδικοποίησης. Ωστόσο κατάφερε το πρόγραμμα να μας εμφανίσει και στην συνέχεια να αποκωδικοποιήσει ένας από τους δυο (2) αλγορίθμους. Αυτό συμβαίνει γιατί το John The Ripper δεν έχει την δυνατότητα να αποκρυπτογραφήσει ταυτόχρονα όλους τους τύπους αλγορίθμων. Ωστόσο αν θέλετε να αποκρυπτογραφήσετε όλους τους τύπους θα πρέπει να χρησιμοποιήσετε την εντολή ***--format***[18] μαζί με τον συγκεκριμένο τύπο αλγορίθμου τρέχοντας τον καθένα ωστόσο μόνο του.

Εικόνα 65. Αποκρυπτογράφηση ενός μόνο τύπου αλγορίθμου κωδικοποίησης.

3.9 Μέθοδοι εκτέλεσης John The Ripper

Το JTR υποστηρίζει 5 διαφορετικές μεθόδους cracking:[19]

- **Wordlist mode:** Αυτός είναι ο απλούστερος τρόπος cracking του John the Ripper. Το μόνο που χρειάζεται να κάνετε είναι να καθορίστε μια λίστα λέξεων (ένα αρχείο κειμένου που περιέχει μια λέξη ανά γραμμή). Με την μέθοδο αυτή μπορείτε να ενεργοποιήσετε και τους κανόνες παραμόρφωσης λέξεων (χρησιμοποιούνται για να τροποποιήσουν ή να 'μαρκάρουν' λέξεις που παράγουν άλλους πιθανούς κωδικούς πρόσβασης). Αν ενεργοποιηθούν, όλοι οι κανόνες θα εφαρμοστούν σε κάθε γραμμή στο αρχείο λέξεων παράγοντας πολλούς 'υποψήφιους' κωδικούς πρόσβασης από κάθε πηγαία λέξη.

  Χαρακτηριστικό παράδειγμα εντολής:

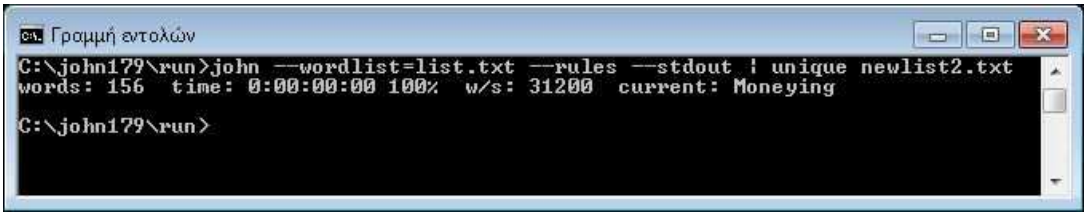
  - ***John --wordlist=password.lst --rules mypasswd.txt***

[18] Περισσότερες πληροφορίες για την σύνταξη της --format θα δούμε παρακάτω όπου αναλύουμε τις εντολές του John The Ripper.
[19] http://www.openwall.com/john/doc/MODES.shtml

Ο σημαντικότερος κανόνας – εντολή – που χρησιμοποιείτε επιπλέον με την μέθοδο Wordlist είναι η **--stdout**. Η εντολή αυτή έχει την ικανότητα να παράγει νέες λέξεις (πιθανούς κωδικούς) από τις ήδη υπάρχοντες τις λίστας που θα ορίσετε αρχικά κάνοντας χρήση όλων των χαρακτήρων όπως για παράδειγμα αριθμούς, γράμματα και ειδικών χαρακτήρων. Στην συνεχεία η νέα λίστα που θα προκύψει θα χρησιμοποιηθεί για την εύρεση των κρυπτογραφημένων κωδικών.

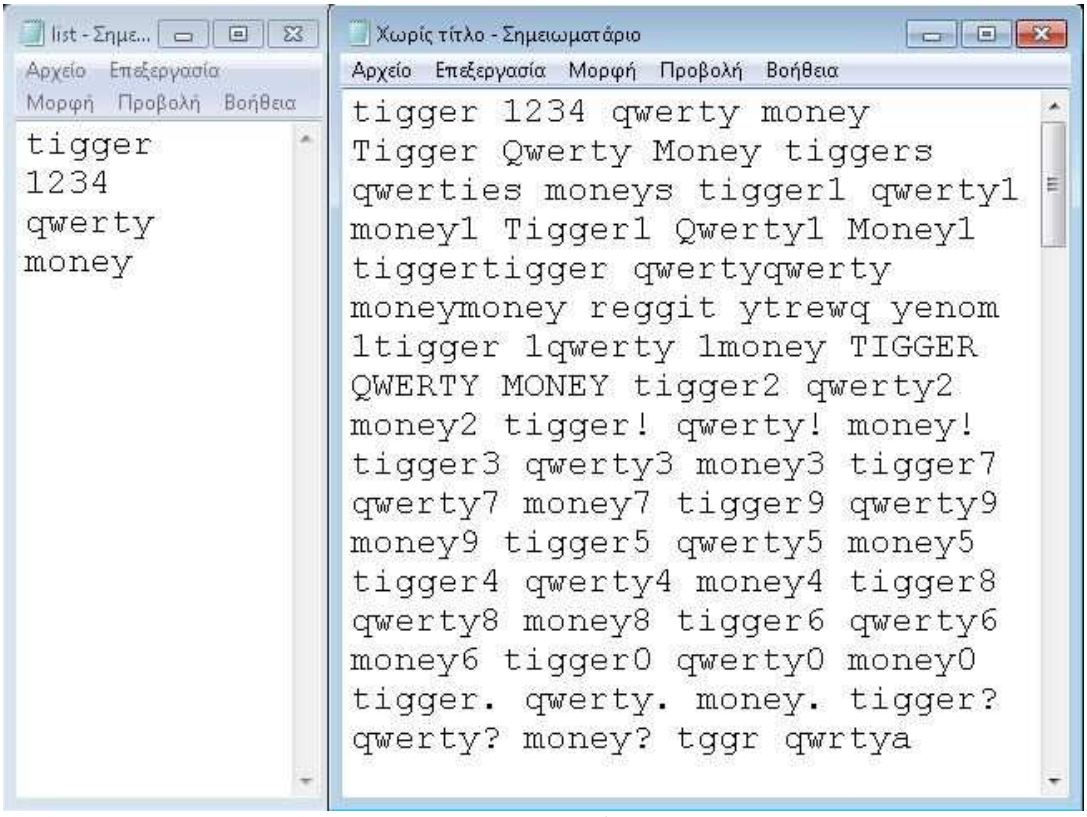
Χαρακτηριστικό παράδειγμα κανόνα:

- ***John --wordlist=password.lst --rules --stdout | unique newlist.lst***
- ***John --wordlist=newlist.lst mypasswd***



Εικόνα 66. Χρήση της --stdout.

Όπως μπορείτε να δείτε και παραπάνω το πρόγραμμα κατάφερε να δημιουργήσει 156 νέες λέξεις από τις τέσσερις που μόλις δώσαμε.

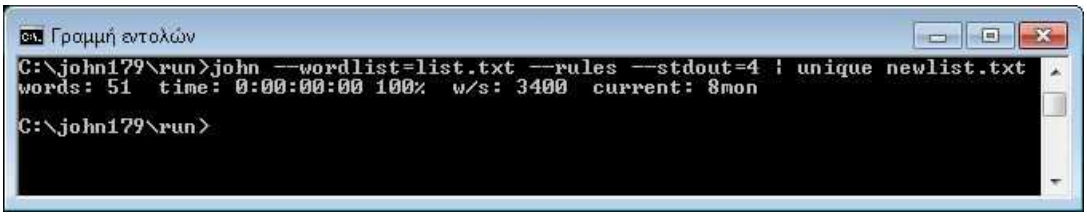


Εικόνα 67. Δημιουργία νέων λέξεων - κωδικών.

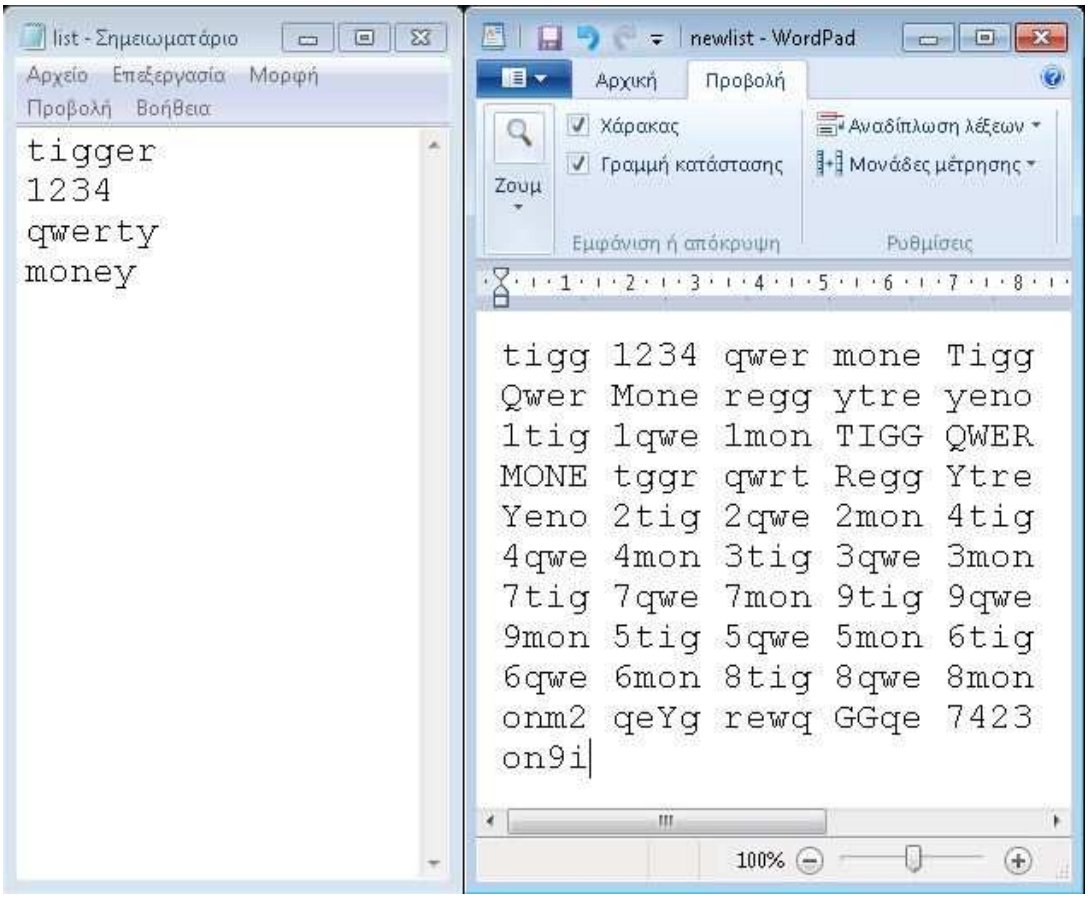
Ωστόσο μπορείτε από εξ αρχής να δηλώσετε το πλήθος των χαρακτήρων σε κάθε νέα λέξη που θα δημιουργείται από το πρόγραμμα. Για να γίνει αυτό αρκεί να καθορίσετε το πλήθος γράφοντας τον αριθμό διπλά από το --stdout. Ένα τέτοιο παράδειγμα μπορείτε να δείτε παρακάτω.

Χαρακτηριστικό παράδειγμα κανόνα με πλήθος χαρακτήρων:

- ***John --wordlist=password.lst --rules --stdout=4 | unique newlist2.lst***
- ***John --wordlist=newlist2.lst mypasswd***



Εικόνα 68. Χρήση της --stdout=[length]



Εικόνα 69. Παράδειγμα κανόνα --stdout=4

- **Single crack mode:** Η μέθοδος αυτή προτείνεται συνήθως για αδύναμους κωδικούς πρόσβασης καθώς περιλαμβάνει μόνο μερικούς κανόνες (login names, full names fields ή home directories names) και μια μικρή λίστα λέξεων για την ανεύρεση των κωδικών πρόσβασης. Η Single crack mode είναι σχετικά απλή στην χρήση της και είναι πιο γρήγορη από την Wordlist mode αλλά δεν εγγυάται για το σύνολο των αποτελεσμάτων.

Χαρακτηριστικό παράδειγμα εντολής:

- ***John --single mypasswd.txt***

- **Incremental mode:** Θεωρείται η πιο ισχυρή μέθοδος για cracking η οποία προσπαθεί να συνδυάσει όλους τους δυνατούς συνδυασμούς χαρακτήρων, όπως κωδικούς πρόσβασης. Ωστόσο κάνοντας χρήση αυτή της μεθόδου υπάρχει το ενδεχόμενο να μην τερματιστεί ποτέ, λόγο του αριθμού των συνδυασμών που είναι αναγκασμένη να διατρέξει (στην πραγματικότητα θα τερματίσει εάν ορίσετε εάν χαμηλό όριο μήκους του κωδικού όπου θέλετε να σπάσετε ή να χρησιμοποιήσετε ένα μικρό σύνολο χαρακτήρων). Για να χρησιμοποιήσετε λοιπόν αυτή την μέθοδο θα πρέπει να ορίσετε ένα συγκεκριμένο αριθμό παραμέτρων όπως για παράδειγμα το μήκος του κωδικού πρόσβασης καθώς και αν θέλετε να ελέγξει μόνο αριθμούς, χαρακτήρες, σύμβολα ή και τον συνδυασμό όλων των προηγούμενων.

  Χαρακτηριστικό παράδειγμα εντολών:

  - ***John --incremental:alpha mypasswd.txt* (μόνο γράμματα)**
  - ***John --incremental:digits mypasswd.txt* (μόνο αριθμούς)**
  - ***John --incremental:lanman mypasswd.txt* (αριθμούς, γράμματα, και ειδική χαρακτήρες)**
  - ***John --incremental:all mypasswd.txt* (όλοι οι χαρακτήρες)**

  Ωστόσο όπως αναφέραμε και παραπάνω το JTR σας δίνει την δυνατότητα να καθορίσετε το τρόπο αναζήτησης των κωδικών. Υπάρχουν λοιπόν οι ακόλουθες παράμετροι που υποστηρίζονται και μπορείτε να χρησιμοποιήσετε επιπλέον με την μέθοδο incremental. Αυτές είναι:

  Minlen: Το ελάχιστο μήκος κωδικού πρόσβασης (αριθμός χαρακτήρων) που θα προσπαθήσει να βρει αποτελέσματα. Η προεπιλεγμένη τιμή στο JTR είναι 0.

  - ***MinLen = 6***

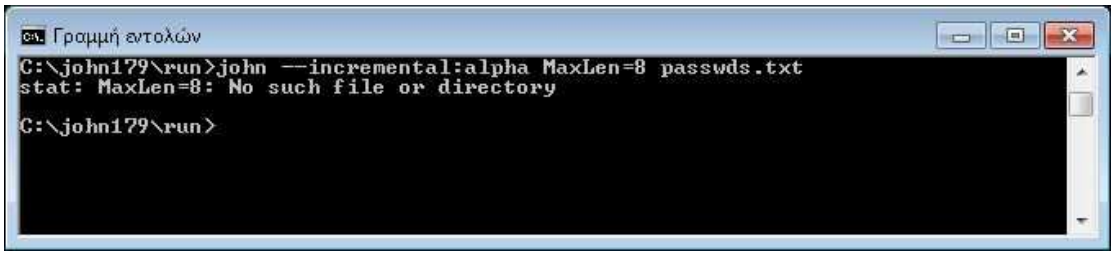
  MaxLen: Το μέγιστο μήκος κωδικού πρόσβασης (αριθμός χαρακτήρων) που θα προσπαθήσει να βρει αποτελέσματα. Η προεπιλεγμένη τιμή στο JTR είναι 8.

  - ***MaxLen = 8***

  CharCount: Αυτό σας επιτρέπει να περιορίσετε τον αριθμό των διαφορετικών χαρακτήρων που θα χρησιμοποιηθούν. Για παράδειγμα θα ψάχνει μέχρι 3 χαρακτήρες ίδιους σε κάθε κωδικό πρόσβασης (να περιέχετε π.χ. το κάθε γράμμα μονό τρεις φόρες μέσα στον κωδικό)

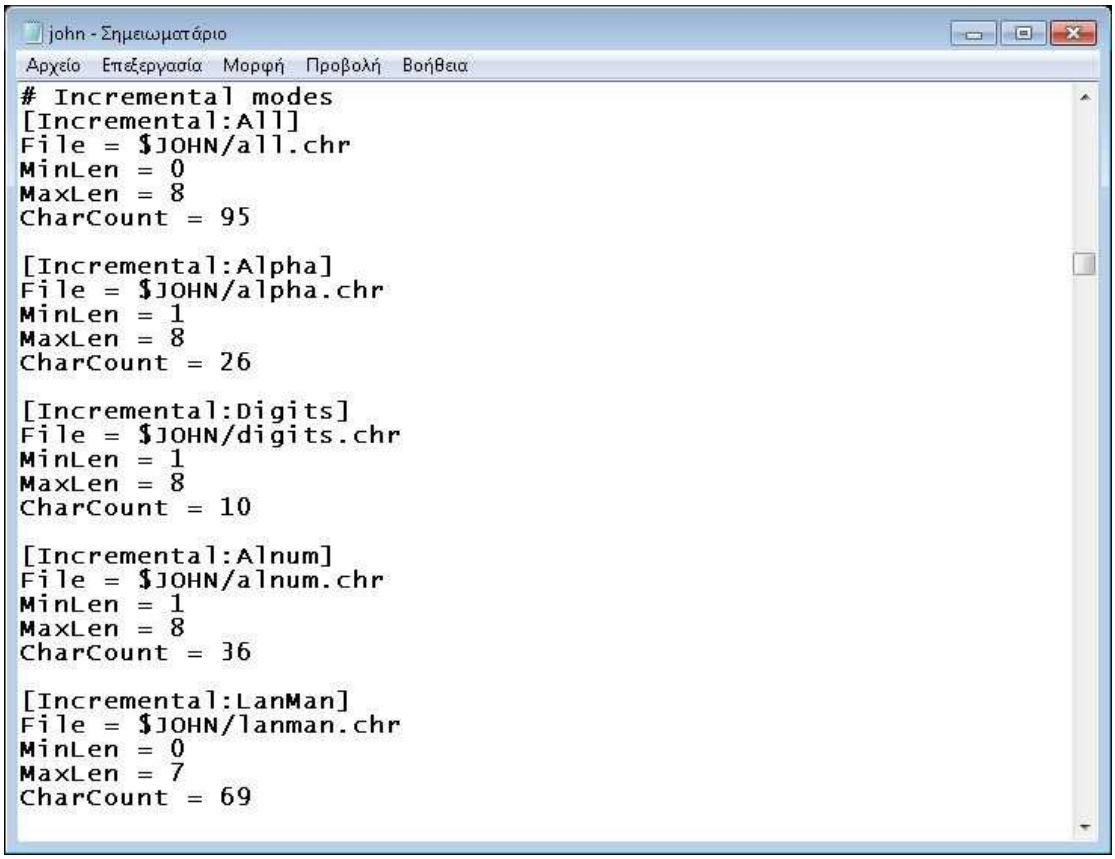
  - ***CharCount = 20***

  Για να μπορέσετε λοιπόν να χρησιμοποιήσετε τις παραπάνω παραμέτρους (MinLen, MaxLen και CharCount) δεν μπορείτε να τις χρησιμοποιήσετε κατευθείαν μέσα στην εντολή που θα συντάξετε για να ξεκινήσει η αποκρυπτογράφηση. Για παράδειγμα αν δώσετε την παρακάτω εντολή στο πρόγραμμα θα σας πετάξει μήνυμα λάθους:



Εικόνα 70. Λανθασμένη σύνταξη MaxLen.

Αυτό που θα πρέπει να κάνετε είναι να πάτε στο αρχείο john.ini το οποίο βρίσκετε στον φάκελο run του John The Ripper. Στην συνέχεια θα ανοίξετε το αρχείο με έναν Text Editor (Notepad) και θα προβείτε με μεγάλη προσοχή στις αλλαγές που θέλετε όπως φαίνετε και στην παρακάτω εικόνα. Τέλος πατάτε Ctrl+S προκειμένου να αποθηκευτούν οι αλλαγές σας.



Εικόνα 71. Αλλαγή παραμέτρων Incremental Modes.

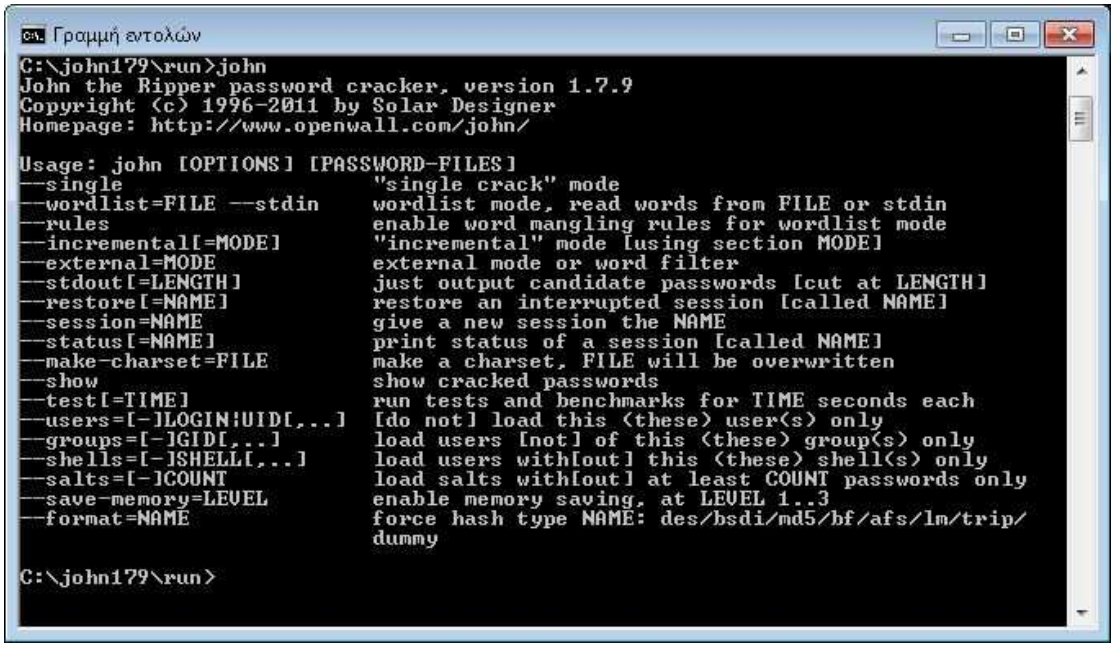
- **External mode:** Η μέθοδος αυτή είναι λίγο περιπλοκή, ωστόσο για να την χρησιμοποιήσετε πρέπει να είστε ειδικευμένοι με το John the Ripper. Για να οριστεί το external mode πρέπει να δημιουργήσετε σε ένα configuration file, ένα τμήμα με το όνομα [List.External:MODE], όπου με το MODE είναι το όνομα που θα δώσουμε στη συγκεκριμένη λειτουργία. Αυτό το τμήμα του configuration file περιέχει μερικές συναρτήσεις σε γλώσσα C, τις οποίες το JTR θα τις μεταγλωττίσει (compile) και θα τις χρησιμοποιήσει, εφόσον κληθεί και ενεργοποιηθεί η λειτουργία αυτή μέσα από το command line, με το όνομα που δώσαμε (MODE).

Χαρακτηριστικό παράδειγμα εντολής:

- ***John --external:[MODE] mypasswd.txt* (αντικαθιστάτε το MODE με το όνομα οποιαδήποτε μεθόδους που θέλετε να χρησιμοποιήσετε)**

3.10 John The Ripper Command Line Syntax

Στο κεφάλαιο αυτό θα αναλύσουμε μερικές από τις κύριες εντολές που χρησιμοποιούνται συχνά στο JTR. Για να δείτε αρχικά όλες τις εντολές που χρησιμοποιεί το πρόγραμμα αρκεί στην γραμμή εντολών να πληκτρολογήσετε την εντολή: ***john*** όπως φαίνετε και παρακάτω.



Εικόνα 72. John The Ripper Main Window.

Συνήθως δεν χρειάζεστε τις περισσότερες από αυτές τις επιλογές. Στην πραγματικότητα δεν χρειάζεστε καμιά από αυτές τις επιλογές γιατί πολύ άπλα μπορείτε να πληκτρολογήσετε την εντολή 'john [όνομα αρχείου]'. Το όνομα αρχείου περιλαμβάνει την επέκταση «.txt». Αυτή λοιπόν είναι και η βασική εντολή. Το πρόγραμμα θα χρησιμοποιήσει Brute-Force attack προκειμένου να αποκρυπτογραφήσει όλους τους κωδικούς πρόσβασης στο αρχείο. Αυτό φυσικά δεν είναι τόσο αποτελεσματικό αλλά είναι πιο γρήγορο από το να χρησιμοποιείτε την μέθοδο Incremental.

Ας δούμε λοιπόν αναλυτικά μερικές από τις βασικές επιλογές του προγράμματος που θα χρησιμοποιήσουμε.

- **Restore:** Υποθέτουμε ότι χρειάζεται να διακόψετε απότομα την διαδικασία cracking. Για να γίνει αυτό αρκεί να πατήσετε Crtl+C. Όταν λοιπόν το κάνετε αυτό θα δημιουργηθεί στο φάκελο run του JTR ένα αρχείο με το όνομα 'restore' όπου δείχνει το σημείο όπου σταμάτησε η τελευταία διαδικασία cracking. Εφόσον επιθυμείτε να συνεχίσετε από το σημείο εκείνο αρκεί να πληκτρολογήσετε την επιλογή ***restore***.

Χαρακτηριστικό παράδειγμα εντολής:

- ***John --restore***

- **Rules:** Η επιλογή αυτή χρησιμοποιείται για να ενεργοποιήσει την μέθοδο wordlist.

  Χαρακτηριστικό παράδειγμα εντολής:

  - ***John --wordlist=password.lst –rules mypassward.txt***

- **Session:** Χρησιμοποιήστε αυτή την εντολή μόνο αν γνωρίζετε ότι θα πρέπει να διακόψετε την διαδικασία cracking στην μέση. Σας επιτρέπει να κρατήσετε σε ένα νέο αρχείο τα δεδομένα που είχατε συλλέξει από το cracking μέχρι το σημείο της διακοπής. Μπορείτε να ξανά συνεχίσετε πάλι από το σημείο που είχατε σταματήσει.

  Χαρακτηριστικό παράδειγμα εντολής:

  - ***John --session [save to filename] mypasswd.txt***

- **Status:** Σας δείχνει πόσο μακριά είχατε φτάσει πριν σταματήσετε την διαδικασία cracking (χρησιμοποιείτε μόνο όταν έχετε χρησιμοποίηση την επιλογή ***session***).

  Χαρακτηριστικό παράδειγμα εντολής:

  - ***John --status [filename]***

- **Show:** Σας δείχνει πόσους κωδικούς πρόσβασης έχετε σπάσει μέχρι στιγμής και πόσοι ακόμα υπολείπονται.

  Χαρακτηριστικό παράδειγμα εντολής:

  - ***John --show mypasswd.txt***

- **Test:** Σας δείχνει πόσο γρήγορα τρέχει το John The Ripper στο μηχάνημά σας.

  Χαρακτηριστικό παράδειγμα εντολής:

  - ***John --test***

- **Users:** Με την επιλογή αυτή μπορείτε να επιλέξετε τον χρήστη ή τους χρήστες στους οποίους θέλετε να σπάσετε τους κωδικούς (χρησιμοποιείτε όταν θέλετε να κάνετε επιλεκτικό cracking).

  Χαρακτηριστικό παράδειγμα εντολής:

  - ***John --users User mypasswd.txt (αντικαθιστάται το User με το όνομα χρήστη που επιθυμείτε)***

- **Groups:** Μπορείτε να σπάσετε τους κωδικούς που ανήκουν μόνο σε αυτή την ομάδα ή ομάδες που θα του πείτε.

  Χαρακτηριστικό παράδειγμα εντολής:

  - ***John --group lamers mypasswd.txt***

- **Format:** Το JTR μπορεί να αποκρυπτογραφήσει κωδικούς από πολλά διαφορετικά format και όχι μόνο DES[20]. Χρησιμοποιήστε την εντολή ***format*** για να καθορίσετε τον τύπο κωδικοποίησης που θέλετε να αποκρυπτογραφήσετε.

  Χαρακτηριστικό παράδειγμα εντολής:

  - ***John --format DES mypasswd.txt (κρυπταλγόριθμος DES)***
  - ***John --format BSDI mypasswd.txt (κρυπταλγόριθμος BSDI)***
  - ***John --format MD5 mypasswd.txt (συνάρτηση κατακερματισμού MD5)***
  - ***John --format BF mypasswd.txt (κρυπταλγόριθμος BF)***
  - ***John --format AFS mypasswd.txt (κρυπταλγόριθμος AFS)***
  - ***John --format LM mypasswd.txt (κρυπταλγόριθμος LM)***

Όταν δώσετε μία από αυτές τις εντολές το JTR ξεκινάει να αποκρυπτογραφεί τον αντίστοιχης μορφής κωδικό και το αποτέλεσμα το εγγράφει στο αρχείο john.pot το οποίο είναι στο φάκελο run του προγράμματος.

Αν θέλετε να εμφανίσετε τη λίστα με όλους τους κωδικούς της συγκεκριμένης κατηγορίας που δώσατε εντολή να αποκρυπτογραφηθούν και οι οποίοι έχουν εγγραφεί στο αρχείο john.pot η εντολή είναι:

- ***john –show –format=DES passwds.txt***

Με αυτή την εντολή το JTR συσχετίζει το αρχείο passwds.txt με τα usernames και τα encrypted passwords με αυτά που έχει βρει και εγγράψει στο john.pot

Στην οθόνη απεικονίζει τα decrypted passwords σύμφωνα με το παρακάτω screenshot:

Εικόνα 73. DES only password decryption

Παρατηρούμε ότι στην γραμμή που είχε το αρχείο passwds.txt καταχωρημένο το username με το αντίστοιχο κρυπτογραφημένο password, τώρα αυτό έχει αντικατασταθεί από το αποκρυπτογραφημένο password, το οποίο είναι αυτό που βρήκε το JTR και το καταχώρησε το john.pot

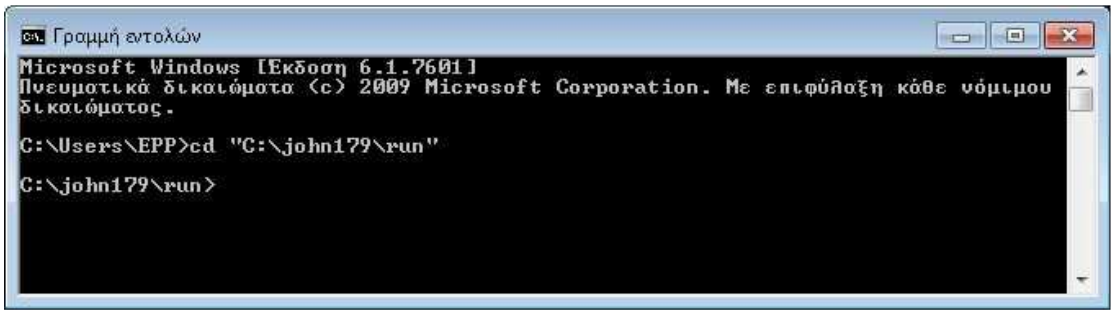
[20] http://en.wikipedia.org/wiki/Data_Encryption_Standard

Εικόνα 74. Εγγραφή decrypted password στο john.pot

3.11 Εκτέλεση του JTR (John The Ripper)

Το JTR έχει την ικανότητα να προσαρμόζεται άμεσα στο μηχάνημα που θα εκτελεστεί. Δηλαδή μπορεί να τρέξει τόσο σε ένα μηχάνημα με έναν πυρήνα όσο και σε ένα Multicore μηχάνημα (αξιοποιεί στο έπακρον όλους τους επεξεργαστές του συστήματος).

Όπως αναφέρθηκε λοιπόν και παραπάνω το JTR λειτούργει σε γραμμή εντολών (Command Prompt). Ανοίγοντας λοιπόν το cmd θα πρέπει να πάτε στον φάκελο όπου έχετε τοποθετήσει τα αρχεία σας προκειμένου να ξεκινήσετε την εκτέλεση του.



Εικόνα 75. Εκτέλεση John The Ripper.

3.11.1 Default Mode

Στο υποκεφάλαιο αυτό θα εκτελέσουμε το JTR στην απλή του μορφή δηλαδή με την χρήση ενός επεξεργαστή. Στην περίπτωση αυτή όπως θα δούμε και παρακάτω, θα υπάρξει μεγάλη διαφορά στους χρόνους με τους οποίους το πρόγραμμα βρίσκει τους κωδικούς όπου και αυτή είναι η κύρια διαφορά από την εκτέλεση του σε ένα Multicore σύστημα.

Στο φάκελο λοιπόν run του προγράμματος έχουμε τοποθετήσει το αρχείο που θα αποκρυπτογραφήσουμε και με τις τρεις (3) μεθόδους που μας δίνονται από το JTR.[21]

- Single crack Mode
- Incremental Mode
- Wordlist Mode

[21] Όλες οι μέθοδοι έχουν εκτελεστεί στο ίδιο χρονικό διάστημα δηλαδή για 1 ώρα. Επίσης σε κάθε Screenshot μπορούμε να παρατηρήσουμε τα χρονικά διαστήματα που βρέθηκε (στο περίπου) ο κάθε κωδικός. Τα χρονικά διαστήματα είναι: 5΄, 10΄, 35΄ και 1 ώρα αντίστοιχα.

Το πρόγραμμα χρησιμοποιεί και την default κατάσταση για την οποία θα αναφέρουμε λίγα λόγια.

- Simple Way Mode

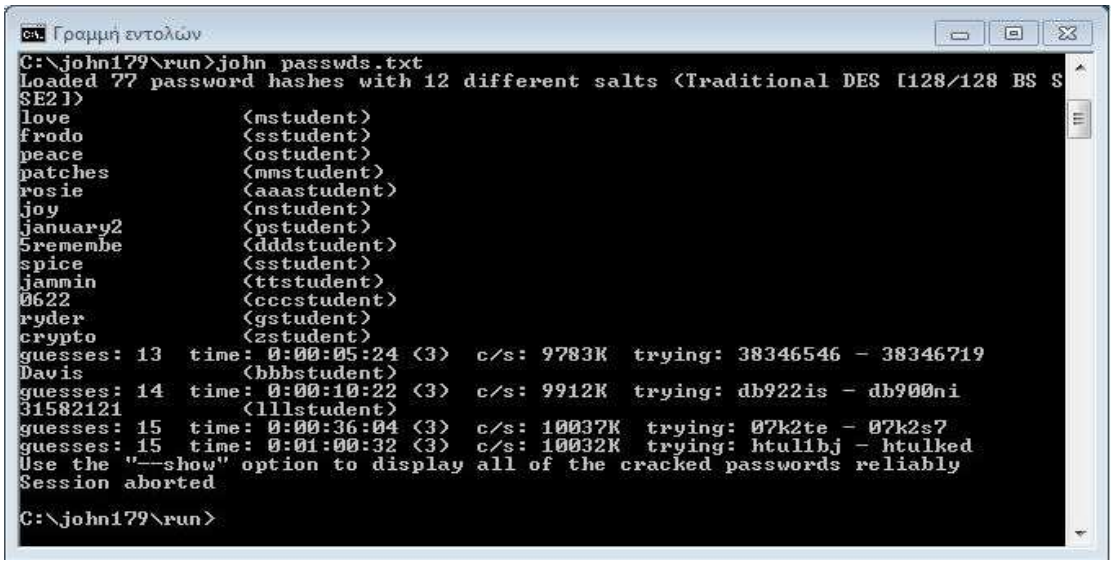
3.11.1.1 Simple Way Mode

Είναι ο απλούστερος τρόπος που διαθέτει το John The Ripper και για αυτό χρησιμοποιείται ως default από το ίδιο το πρόγραμμα. Το πρόγραμμα λοιπόν θα ξεκινήσει αρχικά με την μέθοδο ‘Single crack’ στην συνεχεία θα χρησιμοποιήσει την μέθοδο ‘Wordlist with rules’ και τέλος την μέθοδο ‘Incremental’.

Ο τρόπος αυτός απευθύνεται κυρίως σε χρήστες οι όποιοι δεν έχουν κάποια γνώση πάνω στο πρόγραμμα. Αυτός ο τρόπος πρέπει να αποφεύγετε επειδή είναι αρκετά χρονοβόρος και λειτουργεί σαν την τεχνική Brute-Force attack.

Για να τρέξετε τον απλό τρόπο αρκεί να πληκτρολογήσετε την εντολή john και διπλά το όνομα αρχείου που περιέχει τους κωδικούς. Συγκεκριμένα η εντολή που θα χρησιμοποιήσετε είναι:

- **john passwds.txt**



Εικόνα 76. John The Ripper - Simple Way

Αν χρειαστεί λοιπόν να σταματήσετε την διαδικασία και να δείτε τα αποτελέσματα που έχει βρει πατάτε Ctrl+C και μετά πληκτρολογείτε την εντολή:

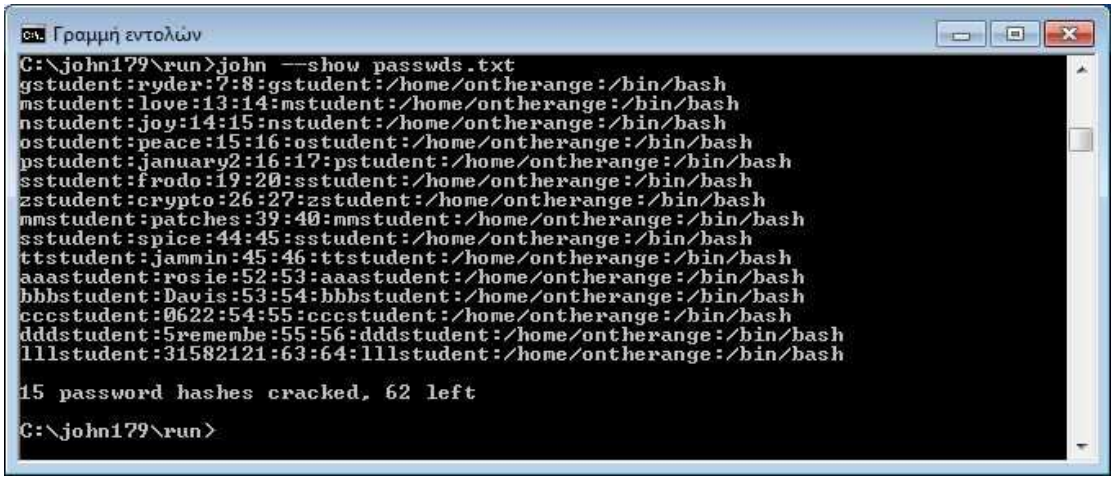
- **john –show passwds.txt**

Με την εντολή αυτή απεικονίζονται τρεις κατηγορίες ενδείξεων:

- **Guesses:** Δείχνει πόσους κωδικούς έχει μαντέψει μέχρι εκείνη τη στιγμή το JTR.
- **Time:** Είναι ο χρόνος που έχει διανύσει το πρόγραμμα μέχρι εκείνη τη στιγμή για την αποκρυπτογράφηση

- **C/S:** Αναφέρεται στις λέξεις combinations per second, δηλαδή συνδυασμοί usernames (αυτών που ήδη έχει) και passwords. Αυτή είναι ουσιαστικά ταχύτητα αποκρυπτογράφησης που σας δίνει το JTR για ένα συγκεκριμένο σετ password hashes.

- **Trying:** Είναι το εύρος τιμών των passwords που δοκιμάζει εκείνη τη στιγμή το JTR σε χρόνο μόλις 1 δευτερόλεπτο.

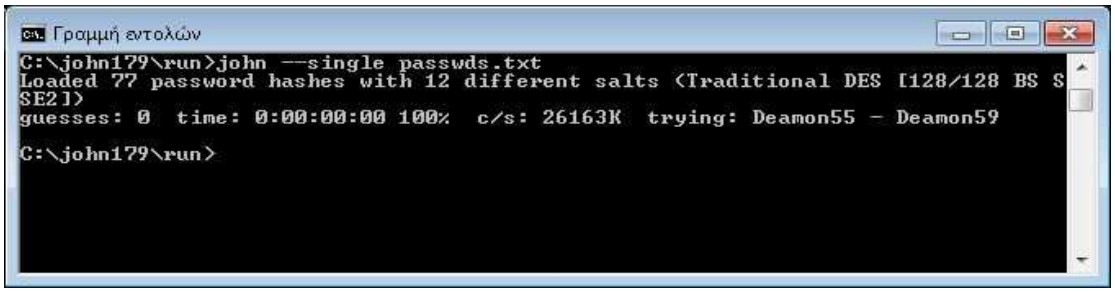


Εικόνα 77. Simple Way - Show Cracked Passwords.

3.11.1.2 Single crack Mode

Όπως έχουμε αναφέρει και παραπάνω η μέθοδος Single crack Mode χρησιμοποιείται κυρίως για να βρει αδύναμους κωδικούς. Τρέχοντας λοιπόν το αρχείο passwds.txt η μέθοδος αυτή δεν κατάφερε να ανακτήσει κάποιον κωδικό.

- **john --single passwds.txt**



Εικόνα 78. Single crack Mode - No guesses.

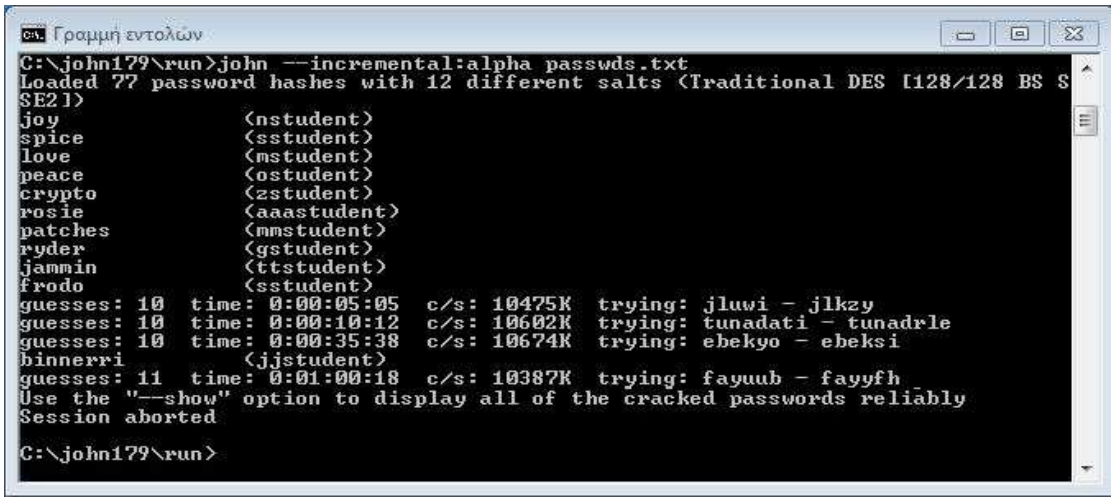
3.11.1.3 Incremental Mode

Στην Incremental mode έχετε την δυνατότητα να επιλέξετε ανάμεσα στους συνδυασμούς (αριθμούς, γράμματα, χαρακτήρες) που θα εφαρμοστούν. Παρακάτω μπορούμε να δούμε αναλυτικά την κάθε κατηγορία ξεχωριστά.

Incremental Mode – Alpha

Χρησιμοποιώντας την επιλογή Alpha το JTR θα ψάξει για κωδικούς χρηστών αποτελούμενοι μόνο από γράμματα. Η σύνταξη της εντολής είναι:

- **john --incremental:alpha passwds.txt**

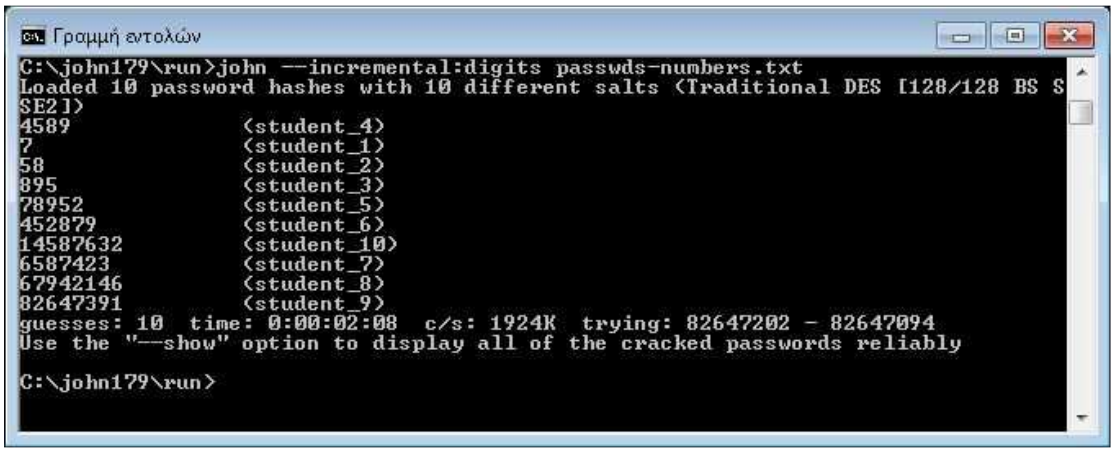


Εικόνα 79. Incremental Mode – Alpha.

Incremental Mode – Digits

Χρησιμοποιώντας την επιλογή Digits το JTR θα ψάξει για κωδικούς χρηστών αποτελούμενοι μόνο από αριθμούς. Η σύνταξη της εντολής είναι:

- **john --incremental:digits passwds.txt**

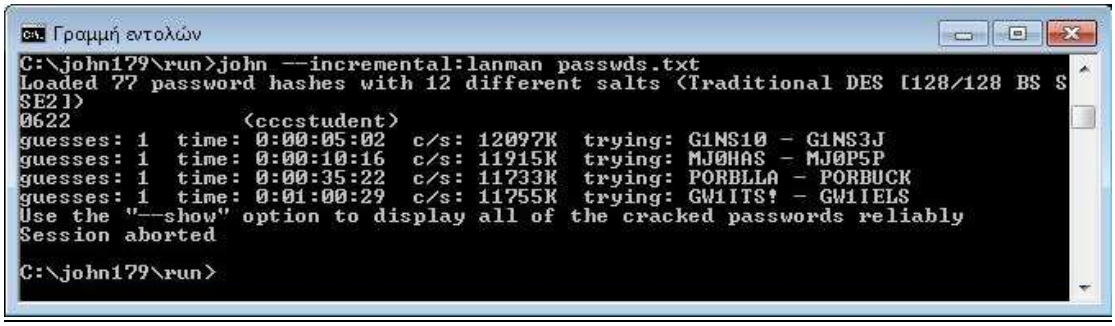


Εικόνα 80. Incremental Mode - Digits.

Incremental Mode – Lanman

Χρησιμοποιώντας την επιλογή Lanman το JTR θα ψάξει για κωδικούς χρηστών αποτελούμενοι από αριθμούς, γράμματα και μερικούς ειδικούς χαρακτήρες. Η σύνταξη της εντολής είναι:

- **john --incremental:lanman passwds.txt**

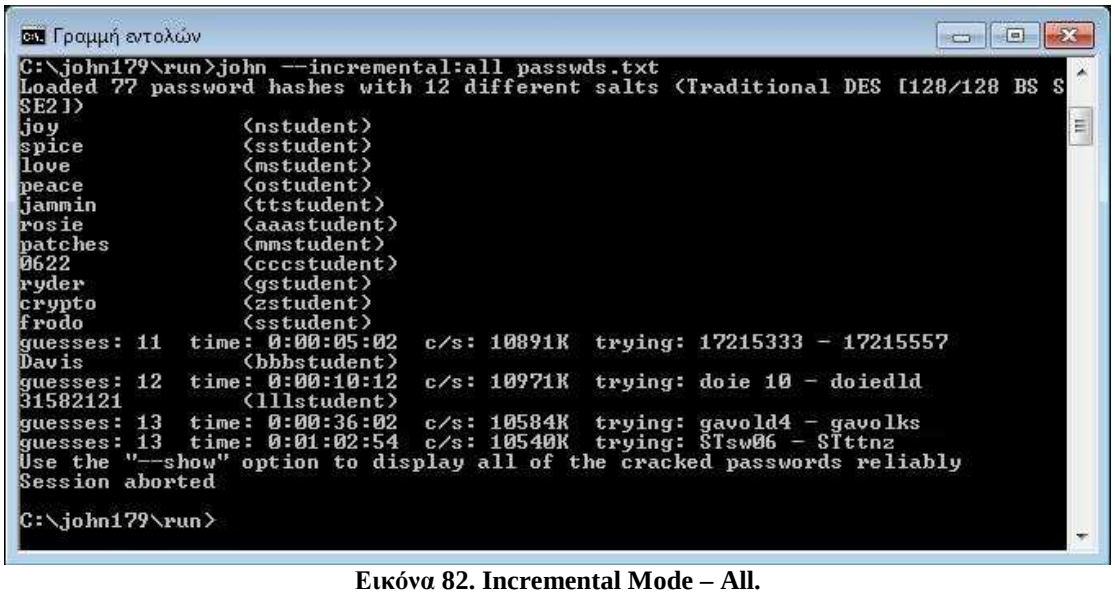


Εικόνα 81. Incremental Mode - Lanman.

Incremental Mode – All

Χρησιμοποιώντας την επιλογή All το JTR θα ψάξει για κωδικούς χρηστών αποτελούμενοι από όλους τους χαρακτήρες. Η σύνταξη της εντολής είναι:

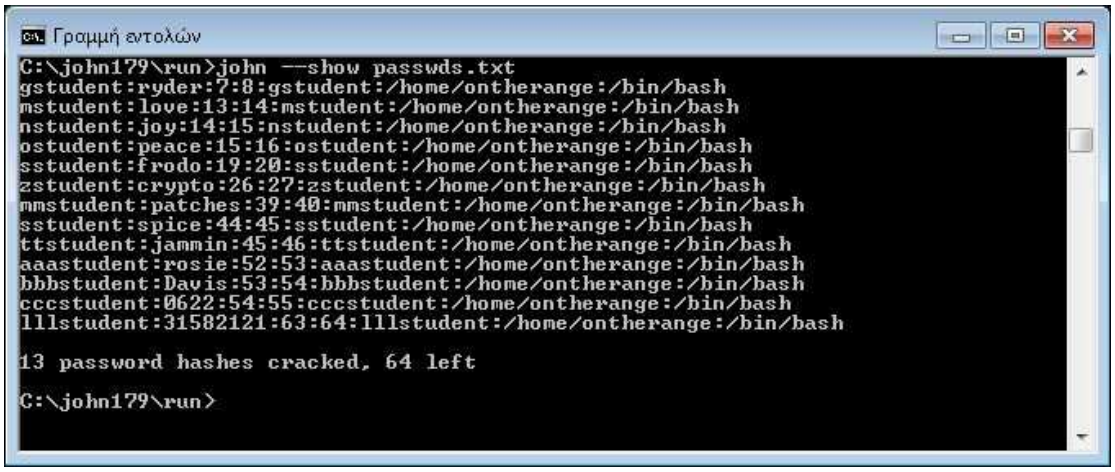
- **john --incremental:all passwds.txt**



Εικόνα 82. Incremental Mode – All.

Για να δείτε τα αποτελέσματα που βρήκατε αρκεί να πληκτρολογήσετε την εντολή:

- **john --show passwds.txt**

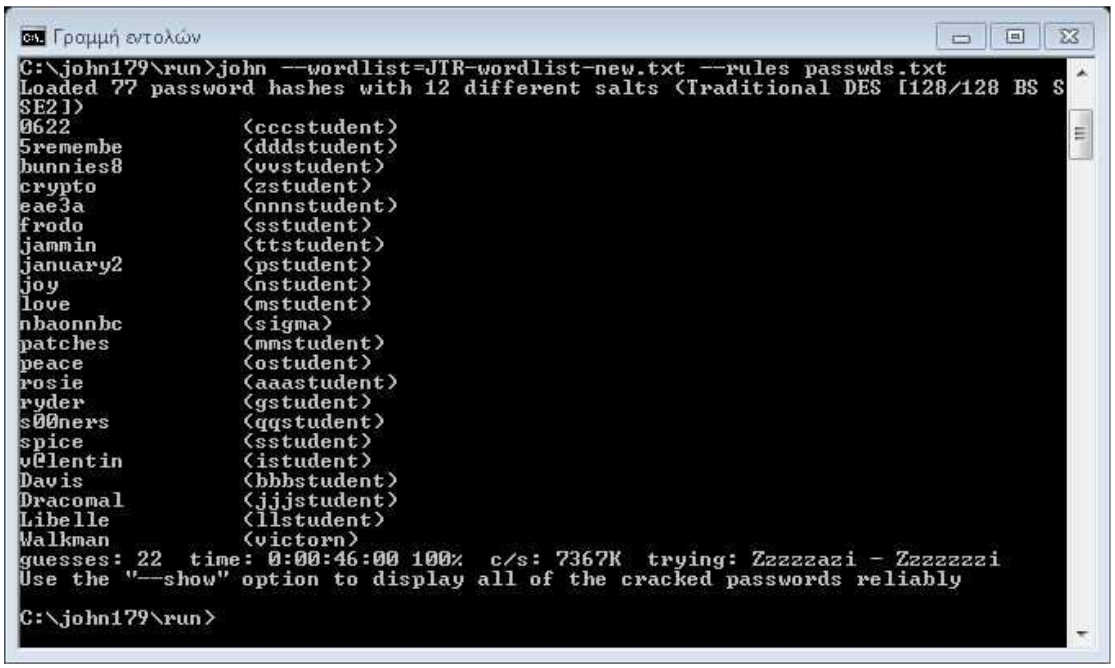


Εικόνα 83. Incremental Mode - Show Cracked Passwords.

3.11.1.4 Wordlist Mode

Στην Wordlist Mode όπως έχουμε αναφέρει και παραπάνω το μόνο που χρειάζεται να κάνετε είναι να καθορίστε μια λίστα λέξεων[22]. Συγκεκριμένα η εντολή που θα χρησιμοποιήσετε είναι:

- **john --wordlist=JTR-wordlist-new.txt --rules passwds.txt**

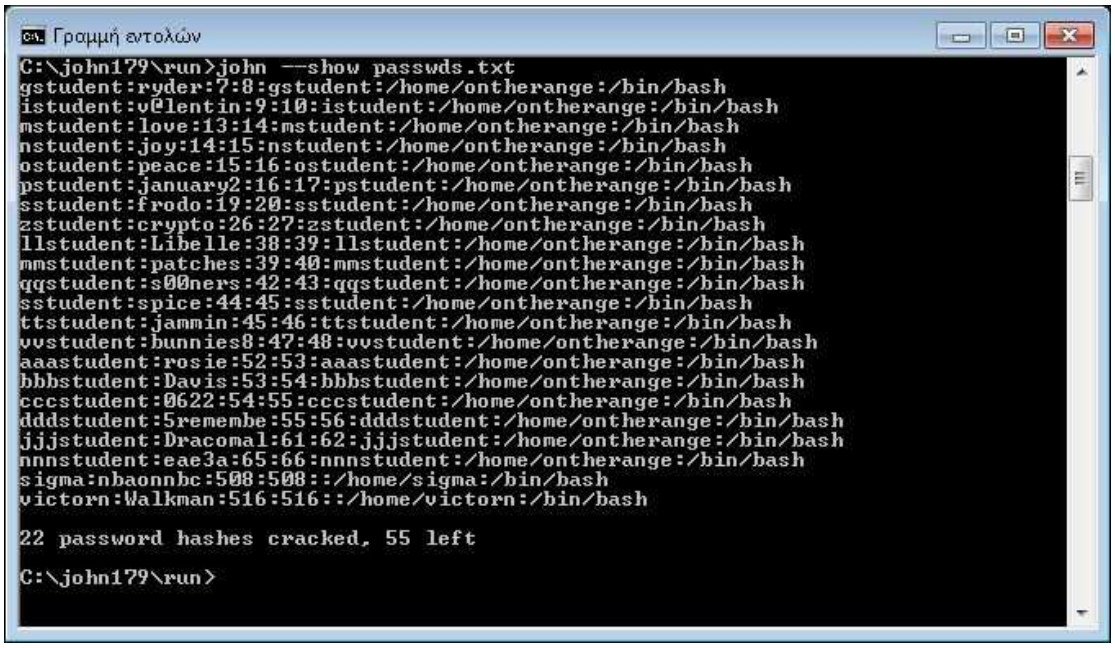


Εικόνα 84. Wordlist Mode.

Για να δείτε τα αποτελέσματα που βρήκατε αρκεί να πληκτρολογήσετε την εντολή:

- **john --show passwds.txt**

[22] Η λίστα που χρησιμοποιήσαμε για την Wordlist mode την προμηθευτήκαμε από την διεύθυνση: http://dazzlepod.com/uniqpass/



Εικόνα 85. Wordlist Mode - Show cracked Passwords.

3.11.2 Multiple Core

Σε αυτό το υποκεφάλαιο θα μελετήσετε την απόδοση του JTR σε υπολογιστή με επεξεργαστή ο οποίος έχει περισσότερους από ένα πυρήνες. Η αποτελεσματικότητα και η ταχύτητα εφαρμογών όπως το JTR αυξάνεται αρκετά σε συστήματα με πολυεπεξεργαστές ή με πολυπύρηνους επεξεργαστές. Εκτός αυτού η χρήση κατανεμημένων συστημάτων, δηλαδή ολόκληρου συμπλέγματος υπολογιστών για την βελτίωση της ταχύτητας της αποκρυπτογράφησης είναι κάτι εφικτό στις μέρες μας και χωρίς μεγάλο κόστος.

Για την αξιοποίηση της δυνατότητας συμμετρικής και παράλληλης επεξεργασίας σε ένα υπολογιστικό σύστημα θα πρέπει να χρησιμοποιηθεί κάποιο βοηθητικό πρόγραμμα ώστε να αξιοποιηθεί από το JTR και να μπορέσει να λειτουργήσει σε multicore hardware. Εδώ θα χρησιμοποιήσετε το MPICH2[23] που είναι μια υλοποίηση του προτύπου MPI.

Το πρότυπο MPI[24] σχεδιάστηκε πρωταρχικά για να υποστηρίξει το μοντέλο μοναδικού προγράμματος πολλαπλών δεδομένων (Single Program Multiple Data, SPMD), παρόλο που δουλεύει εξαιρετικά και για άλλα μοντέλα. Στην τεχνική προγραμματισμού μοναδικού προγράμματος πολλών δεδομένων, όλες οι διεργασίες εκτελούν το ίδιο πρόγραμμα σε διαφορετικά σύνολα δεδομένων. Όταν ένα MPI πρόγραμμα αρχίζει, δημιουργεί έναν αριθμό διεργασιών όπως έχει καθοριστεί από το χρήστη. Κάθε διεργασία καθώς εκτελείται επικοινωνεί με άλλες διεργασίες που μπορεί ενδεχομένως να τρέχουν στον ίδιο επεξεργαστή ή σε διαφορετικούς επεξεργαστές. Η βασική επικοινωνία αποτελείται από την αποστολή και τη λήψη δεδομένων από μια διεργασία σε άλλη. Στα απλούστερα MPI προγράμματα, μια κύρια διεργασία αποστέλλει εργασία σε διεργασίες εργάτες. Εκείνες οι διεργασίες λαμβάνουν τα δεδομένα, εκτελούν τους υπολογισμούς σε αυτά, και στέλνουν τα

[23] http://www.mcs.anl.gov/research/projects/mpich2/
[24] http://en.wikipedia.org/wiki/Message_Passing_Interface

αποτελέσματα πίσω στην κύρια διεργασία, η οποία συνδυάζει τα αποτελέσματα. Η ανάθεση της διεργασίας αυτής γίνεται από το πρόγραμμα που ξεκινάει το MPI πρόγραμμα και συνήθως καλείται με το mpiexec ή mpirun.

Από την άλλη το MPICH2 όπου και θα χρησιμοποιήσουμε είναι μία ανοιχτού κώδικα υλοποίηση του MPI η οποία παρέχει υποστήριξη σε πολλές διαφορετικές πλατφόρμες συμπεριλαμβανομένων μηχανημάτων που τρέχουν Linux αλλά και Microsoft Windows. Παρέχει τόσο τις απαραίτητες βιβλιοθήκες για τη μεταγλώττιση των MPI προγραμμάτων, όσο και το περιβάλλον εκτέλεσης των προγραμμάτων αυτών. Παρακάτω θα περιγράψουμε την εγκατάσταση του MPICH2 σε περιβάλλον Linux για την εκτέλεση του προγράμματος John The Ripper.

3.11.2.1 Εγκατάσταση JTR και MPICH2 σε LINUX (UBUNTU)

Για την εγκατάσταση του JTR και του MPICH2 σε Linux OS και συγκεκριμένα σε Ubuntu 64-bit δίνετε τις παρακάτω εντολές:

- ***$ sudo apt-get install john (κατεβάζει τα απαραίτητα αρχεία του JTR και τα εγκαθιστά)***

- ***$ sudo apt-get install libmpich1.0-dev***
- ***$ sudo apt-get install libmpich-mpd1.0-dev***
- ***$ sudo apt-get install libmpich-shmem1.0-dev***

} Με τις 3 αυτές εντολές εγκαθίστανται static libraries και development files του MPICH.

- ***$ sudo apt-get install mpich2 (ενσωμάτωση του MPI Message Passing Interface)***

- ***$ sudo apt-get install mpich2-doc (εγκαθιστά την τεκμηρίωση για το mpich2)***

- ***$ sudo apt-get install openssh-server (secure shell (SSH) server, για ασφαλή πρόσβαση από μακριά)***

Η εγκατάσταση όλων των παραπάνω μπορεί να γίνει και σε μία εντολή:

- ***~$ sudo apt-get install libmpich1.0-dev libmpich-mpd1.0-dev libmpich-shmem1.0-dev mpich2 mpich2-doc john openssh-server build-essentials***

Η εντολή για τη χρήση του MPICH2 μέσα από το JTR είναι η παρακάτω:

- ***mpirun –np <number_of_processes> ~/<folder_name>/run/john <program_name>***

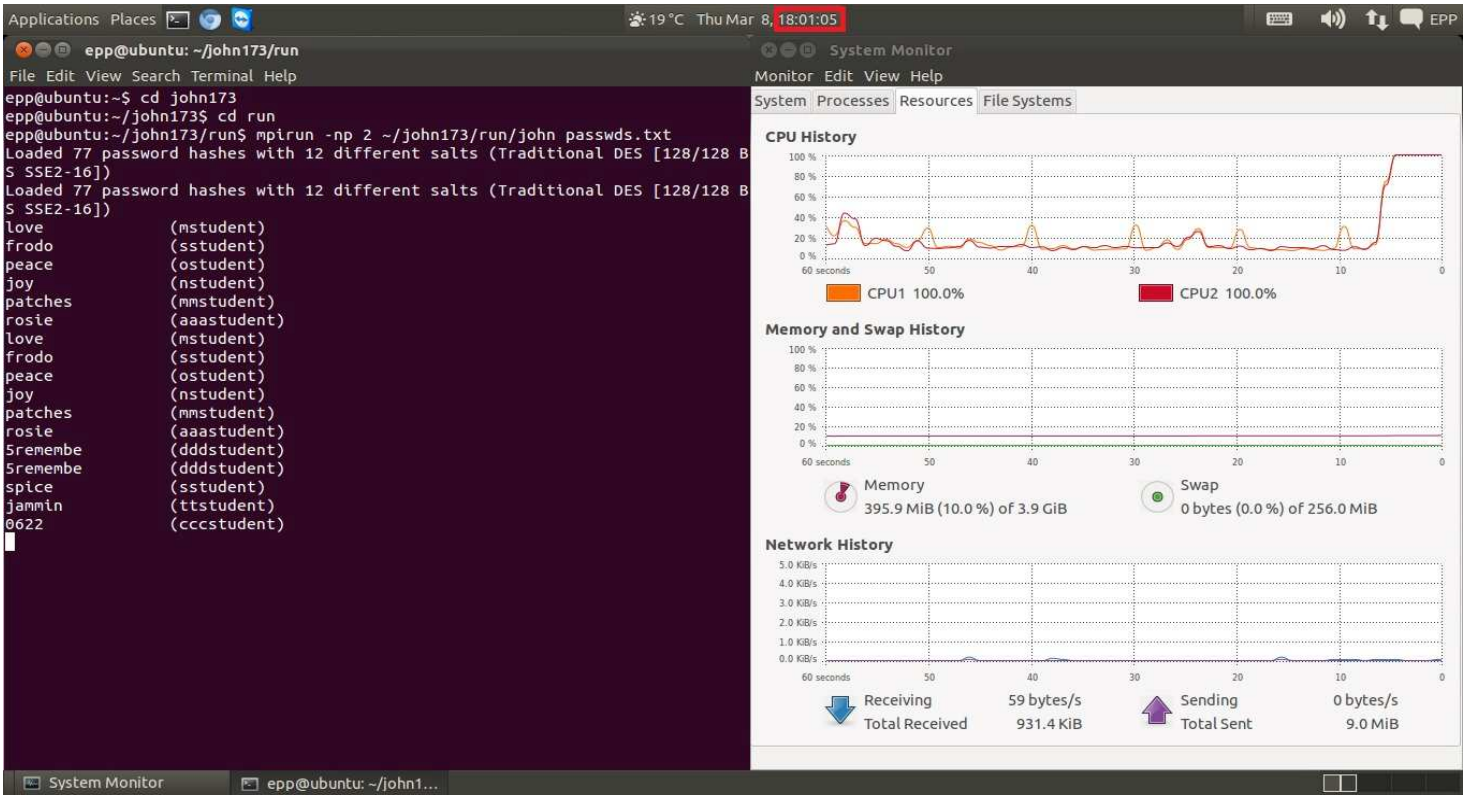
Το number of processes είναι ο συνολικός αριθμός πυρήνων που διαθέτει ο πολυπύρηνος επεξεργαστής ή το πολυεπεξεργαστικό μας σύστημα

Παράδειγμα για σύστημα dual core θα δώσετε την εντολή

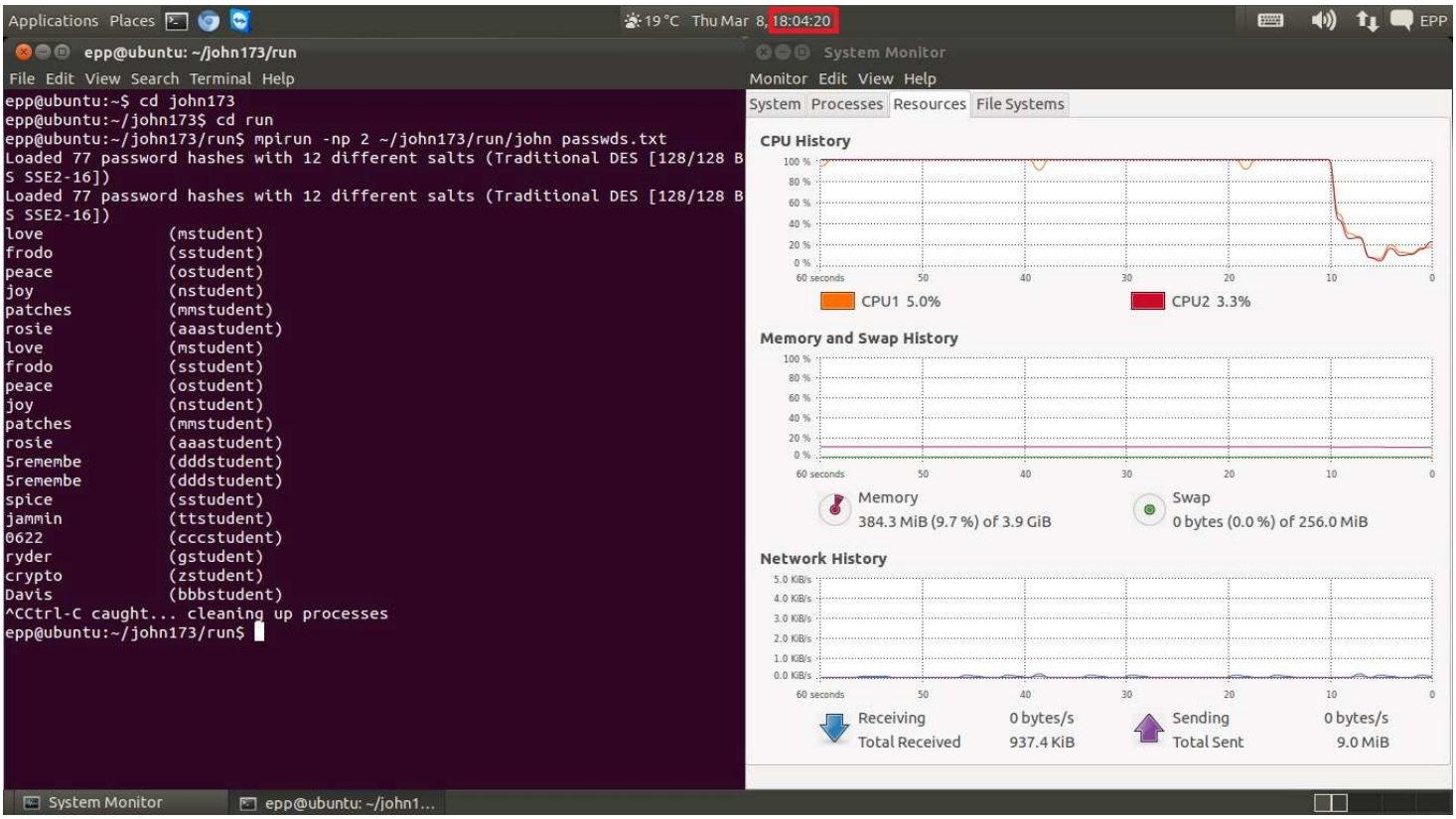
- ***mpirun –np 2 ~/john173/run/john mypasswd.txt***

Το πρόγραμμα MPICH2 μπορείτε να το κατεβάσετε από τη διεύθυνση http://www.mcs.anl.gov/research/projects/mpich2/.

Ανάλογα με το λειτουργικό που χρησιμοποιείτε θα πρέπει να κατεβάσετε την αντίστοιχη έκδοση για Linux ή για Windows. Στην περίπτωση των Windows άλλος installer είναι για 32bits και άλλος για 64 bits. Τα screenshots είναι με τη χρήση του MPICH2 το οποίο εγκαταστήσατε σύμφωνα με τις παραπάνω οδηγίες. Επίσης, το hardware που χρησιμοποιήθηκε είναι CPU dual core AMD Athlon X2 7850 (3.0GHz overclocked), 4GB DDR2 RAM, OS: Windows 7 64-bit.



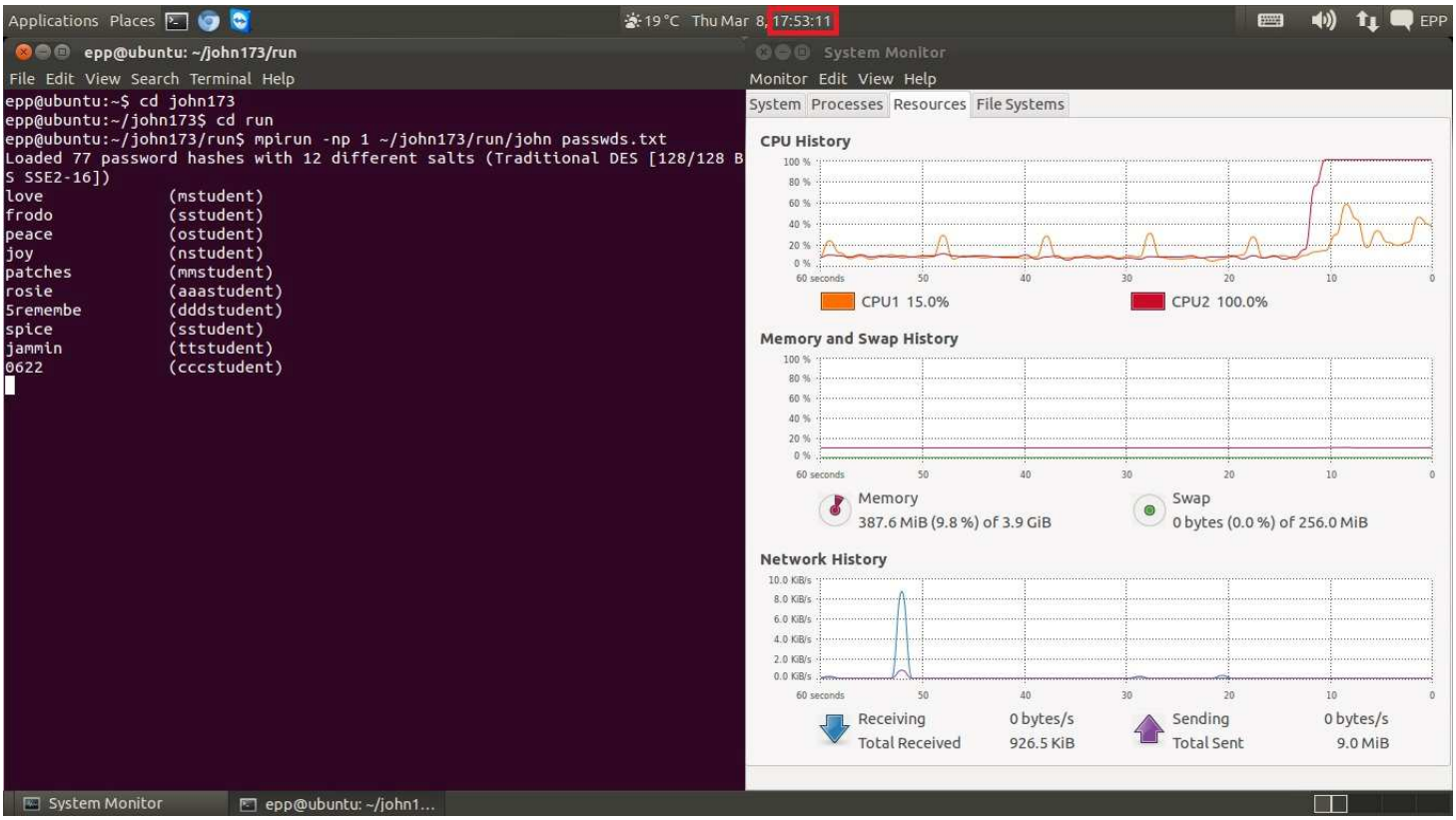
Εικόνα 86. Multicore Cracking (Start).



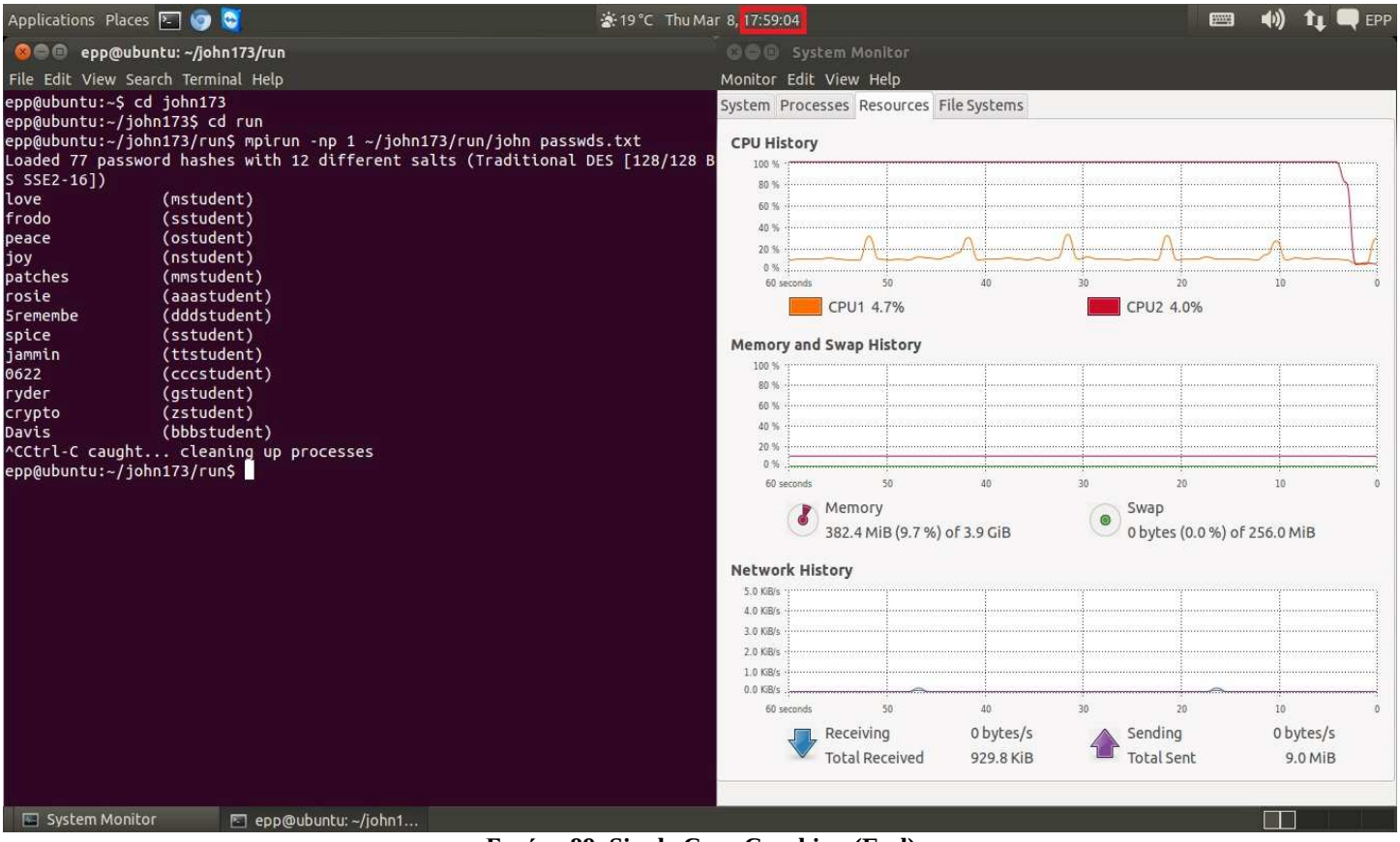
Εικόνα 87. Multicore Cracking (End).

Στις προηγούμενες εικόνες βλέπετε τη χρήση του JTR με δύο πυρήνες **ταυτόχρονα** σύμφωνα με την εντολή που δώσαμε παραπάνω. Παρατηρείτε ότι σύμφωνα με το χρόνο που κρατήθηκε με το ρολόι του λειτουργικού συστήματος απαιτήθηκε χρόνος περίπου 3 min και 15 sec για να βρει το password Davis.

Δίπλα από το παράθυρο του JTR βλέπετε το παράθυρο με το system monitor κατά την αρχή και το τέλος της αποκρυπτογράφησης όπου είναι εμφανές από την καμπύλη της CPU History ότι στις CPU 1 και CPU 2, που αντιστοιχούν στα cores του επεξεργαστή, το workload είναι 100%, άρα επιβεβαιώνεται η αξιοποίηση και των 2 cores του επεξεργαστή.



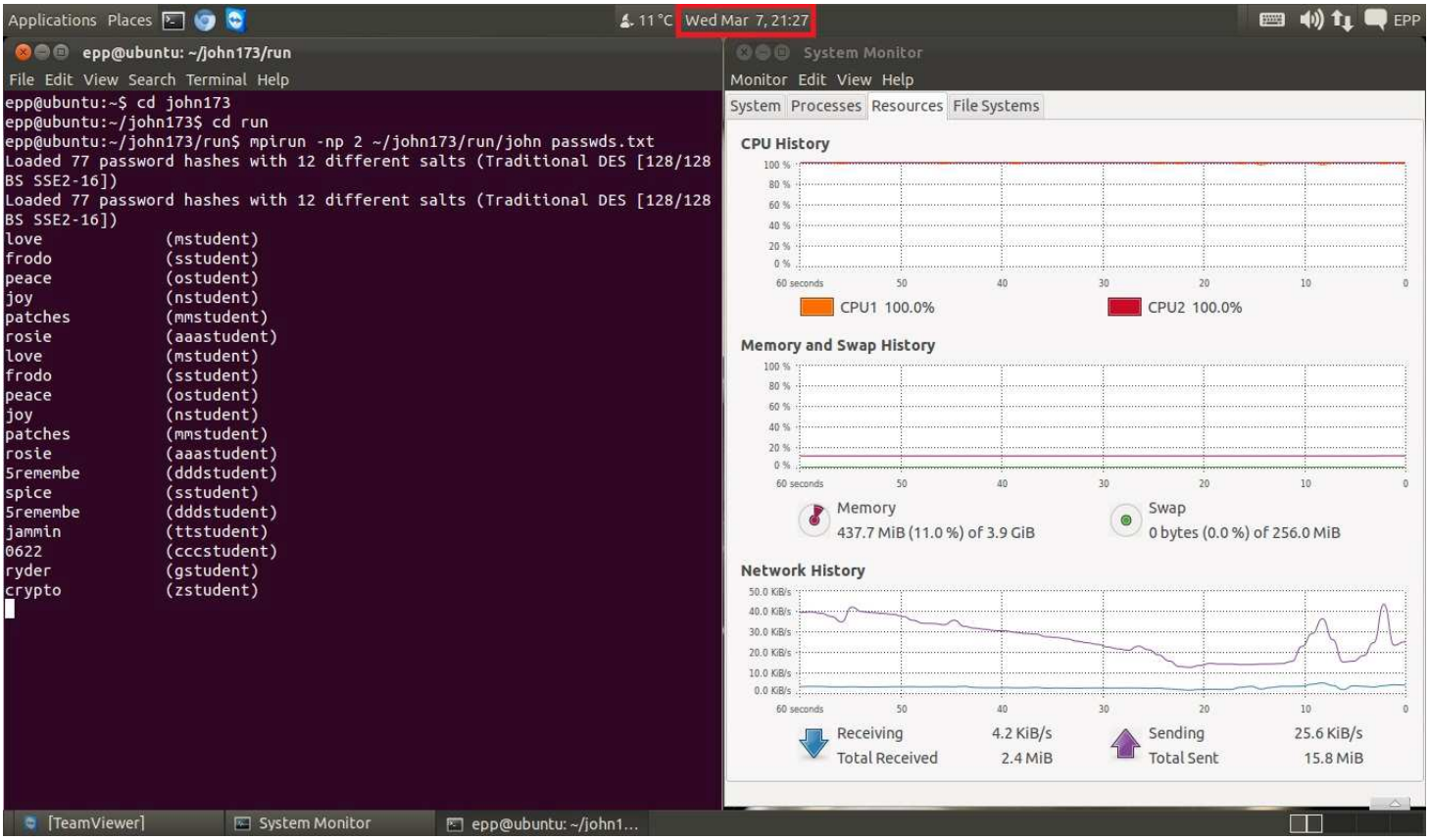
Εικόνα 88. Single Core Cracking (Start).



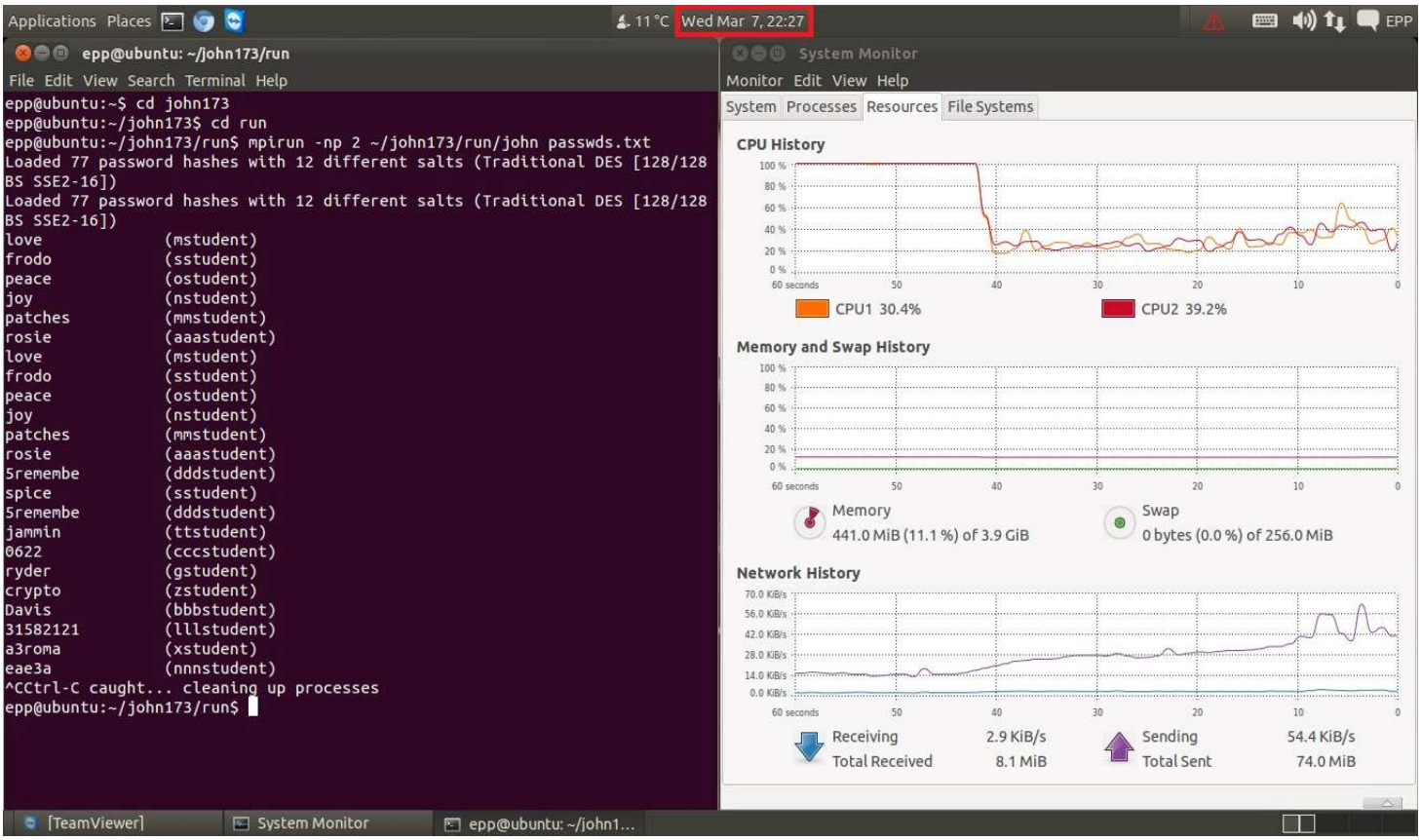
Εικόνα 89. Single Core Cracking (End).

Στις προηγούμενες δύο εικόνες βλέπουμε ότι για να φτάσει το JTR με τη χρήση ενός core στον κωδικό Davis χρειάζεται χρόνο 5min και 53sec, σύμφωνα με το ρολόι του λειτουργικού συστήματος, δηλαδή περισσότερο από πριν, κάτι λογικό και αναμενόμενο. Από το διάγραμμα της χρήσης του επεξεργαστή βλέπουμε ότι μόνο ο ένας core είναι σε 100% workload και ο άλλος είναι σε σχετικά χαμηλά επίπεδα λειτουργίας, οπότε επιβεβαιώνεται ότι δεν χρησιμοποιήθηκαν και οι δύο cores.

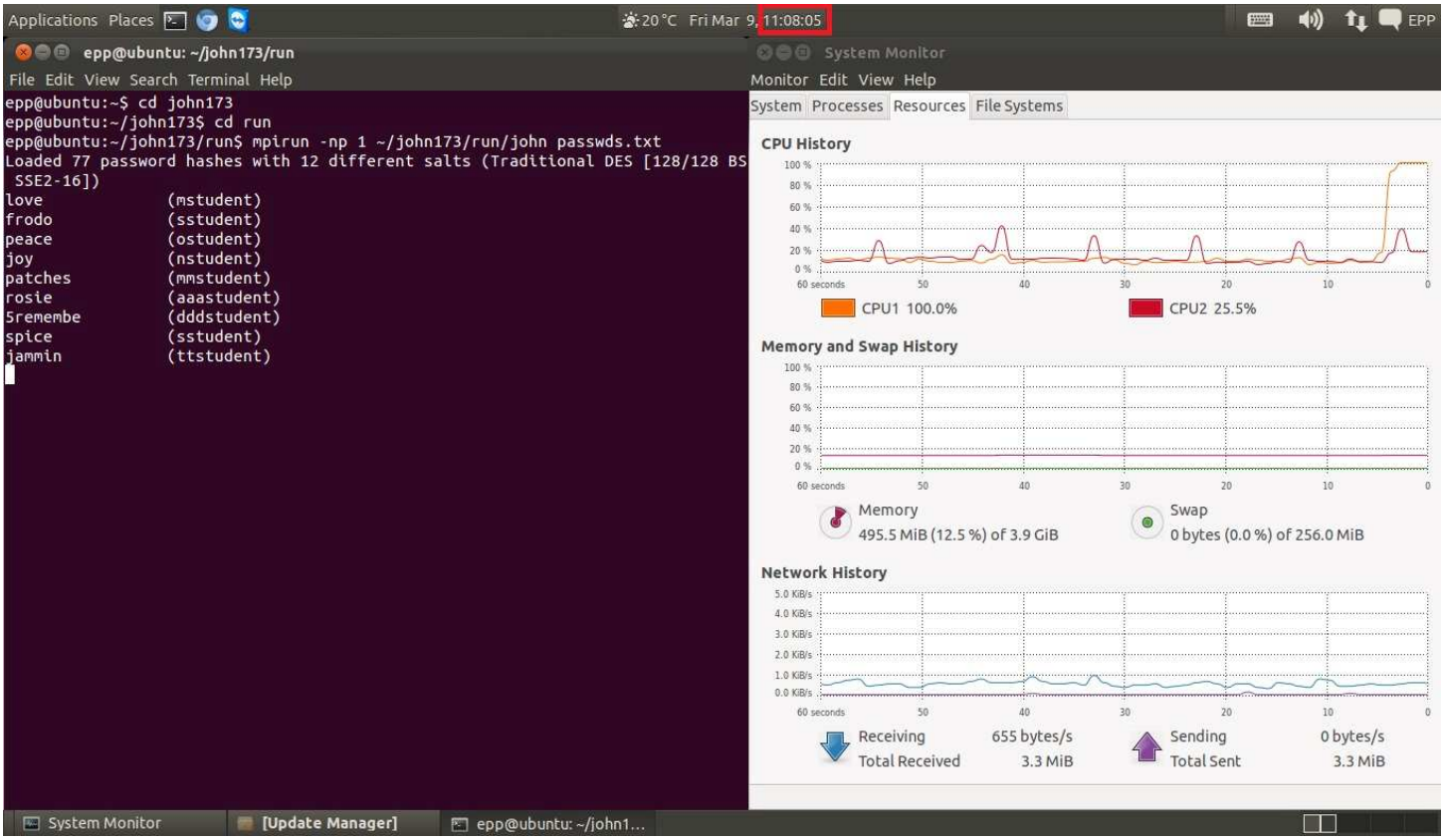
Ωστόσο πόσους κωδικούς μπορεί να βρει το πρόγραμμα τρέχοντας για ένα συγκεκριμένο χρονικό διάστημα τόσο σε Single όσο και σε Multicore κατάσταση; Όπως μπορούμε να δούμε και παρακάτω θέτοντας το χρονικό όριο της μιας (1) ώρας το πρόγραμμα δουλεύοντας σε κατάσταση Multicore κατάφερε να αποκρυπτογραφήσει δεκαεπτά (17) κωδικούς ενώ σε Single κατάσταση κατάφερε να αποκρυπτογραφήσει δεκαπέντε (15) κωδικούς.



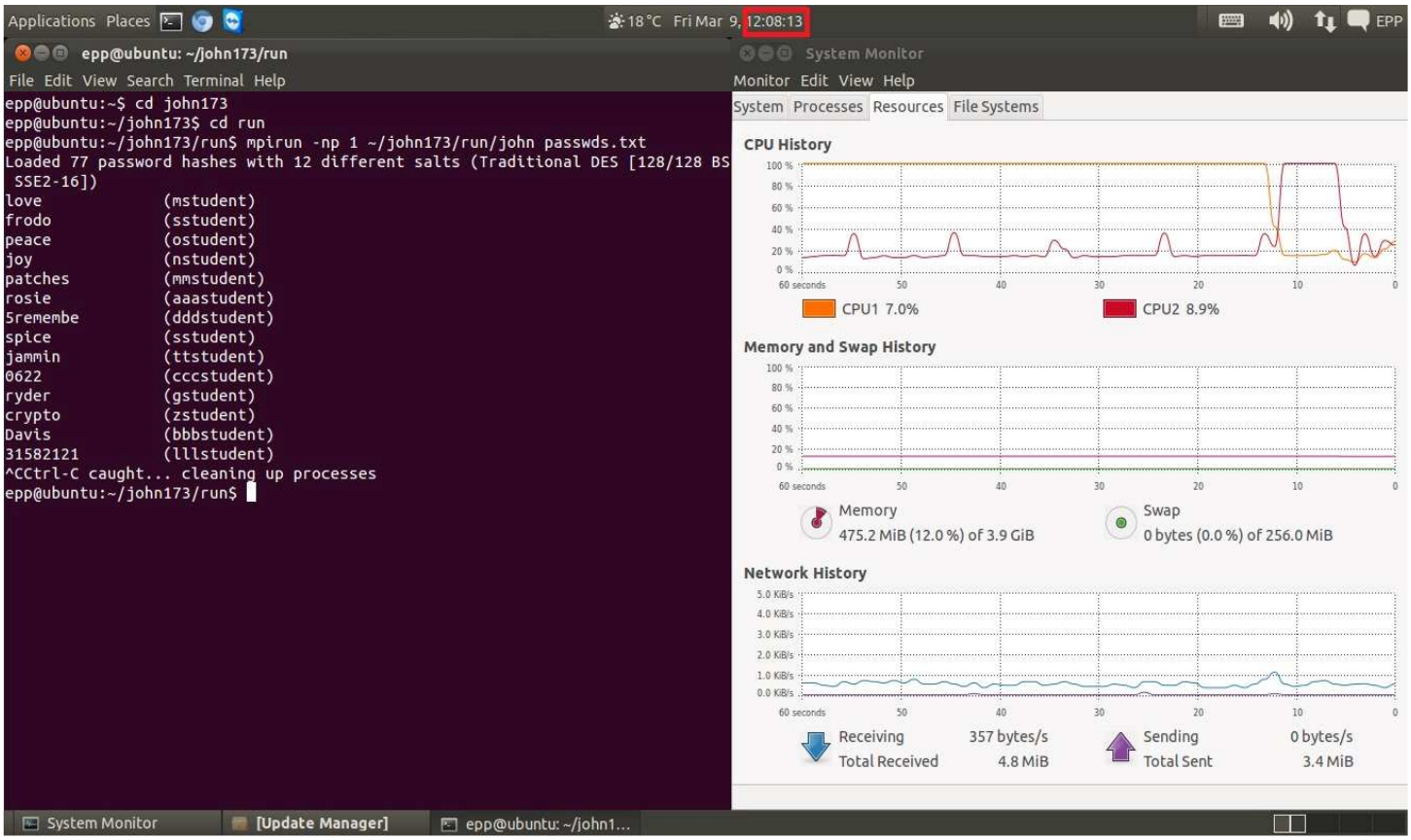
Εικόνα 90. Dual Core in Multicore Mode - One Hour (Start).



Εικόνα 91. Dual Core in Multicore Mode - One Hour (End).

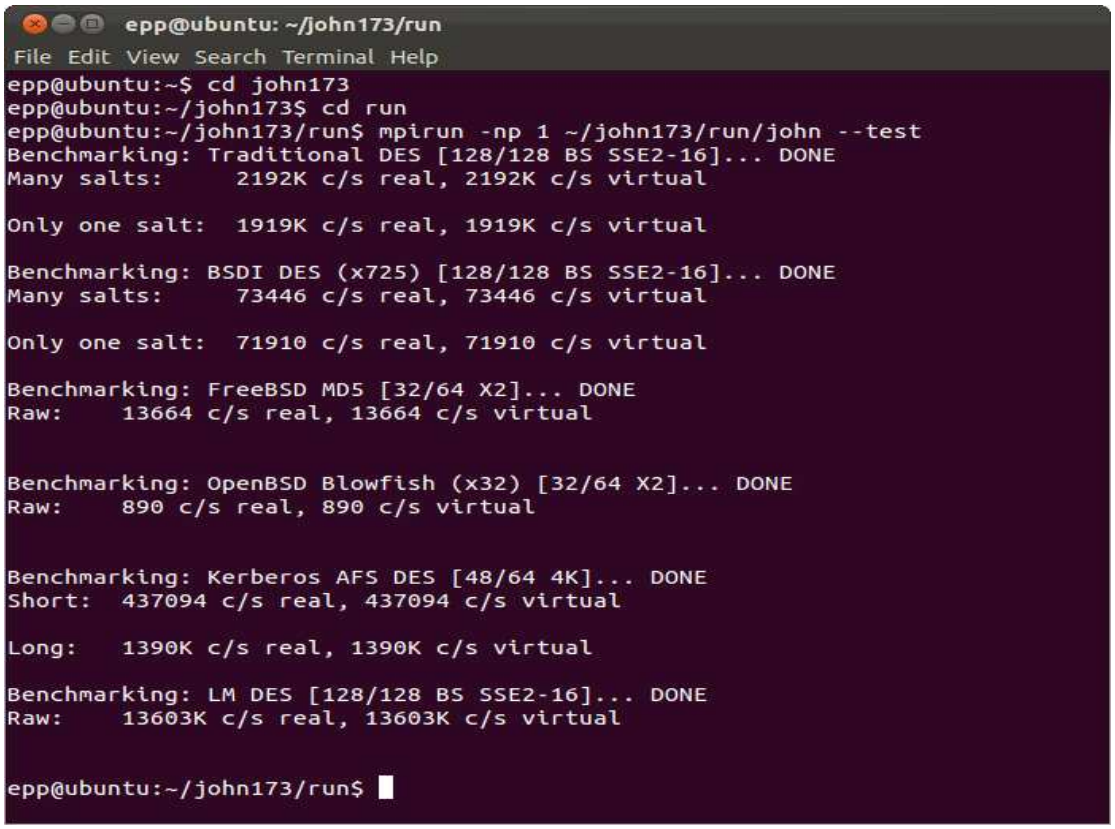


Εικόνα 92. One Core in Multicore Mode - One Hour (Start).

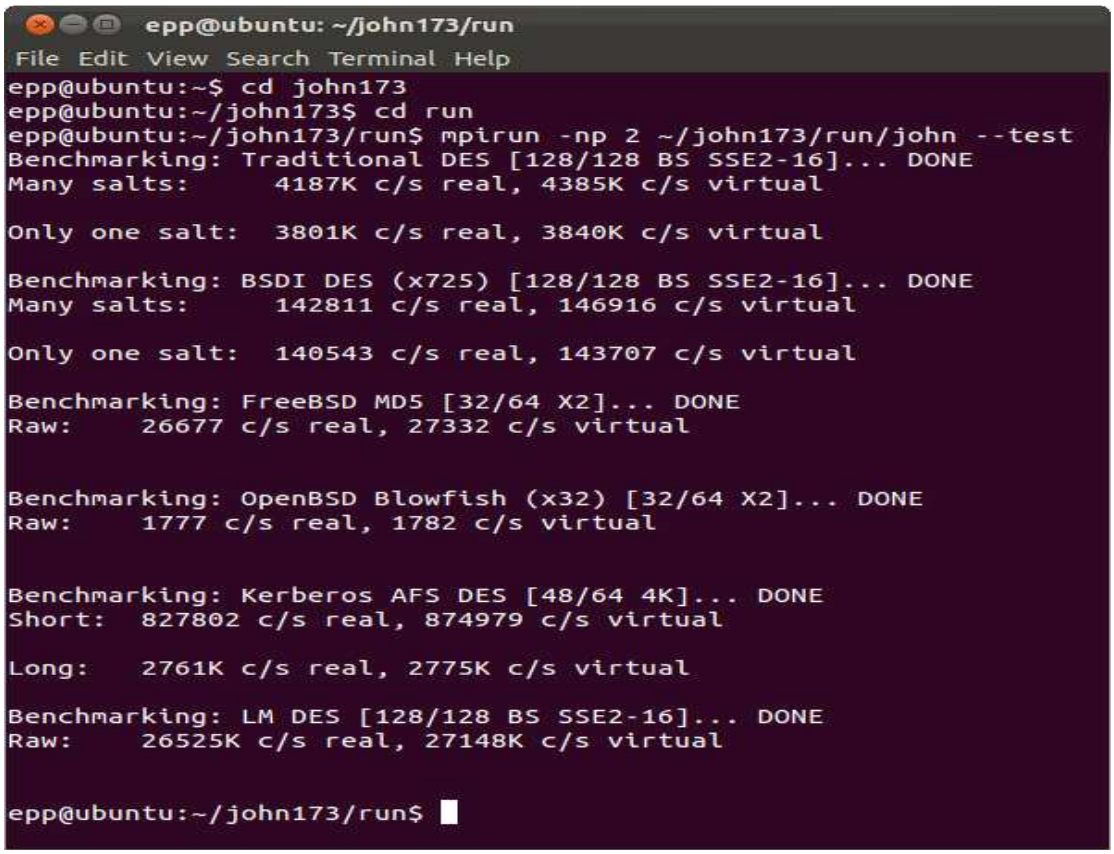


Εικόνα 93. One Core in Multicore Mode - One Hour (End).

Benchmark στον AMD Athlon X2 7850 (3.0GHz overclocked)



Εικόνα 94. Benchmark in a Single Core.



Εικόνα 95. Benchmark in a Dual Core.

Στον παρακάτω πίνακα παραθέτουμε συγκεντρωτικά όλα τα παραπάνω αποτελέσματα benchmarking.

Without MPI	With MPI
Benchmarking: Traditional DES [128/128 BS SSE2-16]... DONE	Benchmarking: Traditional DES [128/128 BS SSE2-16]...
Many salts: 2192K c/s real, 2192K c/s virtual	Many salts: 4187K c/s real, 4385K c/s virtual
Only one salt: 1919K c/s real, 1919K c/s virtual	Only one salt: 3801K c/s real, 3840K c/s virtual
Benchmarking: BSDI DES (x725) [128/128 BS SSE2-16]... DONE	Benchmarking: BSDI DES (x725) [128/128 BS SSE2-16]... DONE
Many salts: 73446 c/s real, 73446 c/s virtual	Many salts: 142811 c/s real, 146916 c/s virtual
Only one salt: 71910 c/s real, 71910 c/s virtual	Only one salt: 140543 c/s real, 143707 c/s virtual
Benchmarking: FreeBSD MD5 [32/64 X2]... DONE	Benchmarking: FreeBSD MD5 [32/64 X2]... DONE

Without MPI	With MPI
Raw: 13664 c/s real, 13664 c/s virtual	Raw: 26677 c/s real, 27332 c/s virtual
Benchmarking: OpenBSD Blowfish (x32) [32/64 X2]... DONE	Benchmarking: OpenBSD Blowfish (x32) [32/64 X2]... DONE
Raw: 890 c/s real, 890 c/s virtual	Raw: 1777 c/s real, 1782 c/s virtual
Benchmarking: Kerberos AFS DES [48/64 4K]... DONE	Benchmarking: Kerberos AFS DES [48/64 4K]... DONE
Short: 437094 c/s real, 437094 c/s virtual	Short: 827802 c/s real, 874979 c/s virtual
Long: 1390K c/s real, 1390K c/s virtual	Long: 2761K c/s real, 2775K c/s virtual
Benchmarking: LM DES [128/128 BS SSE2-16]... DONE	Benchmarking: LM DES [128/128 BS SSE2-16]... DONE
Raw: 13603K c/s real, 13603K c/s virtual	Raw: 26525K c/s real, 27148K c/s virtual

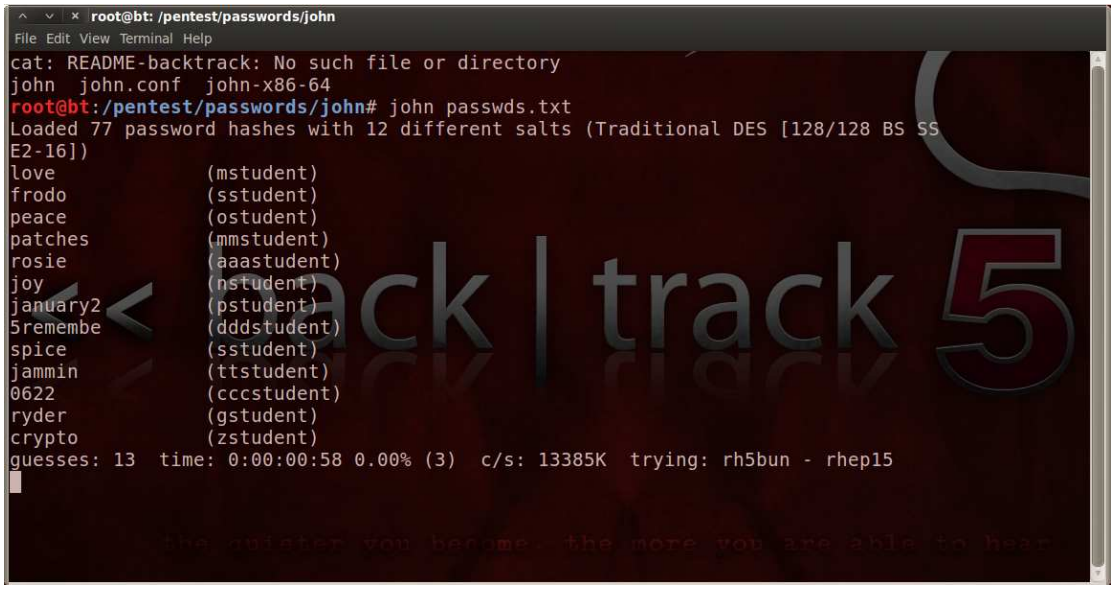
Πίνακας 16. Συγκεντρωτικός πίνακας Benchmark Single - Dual Core.

3.12 Χρήση John The Ripper σε περιβάλλον Backtrack OS

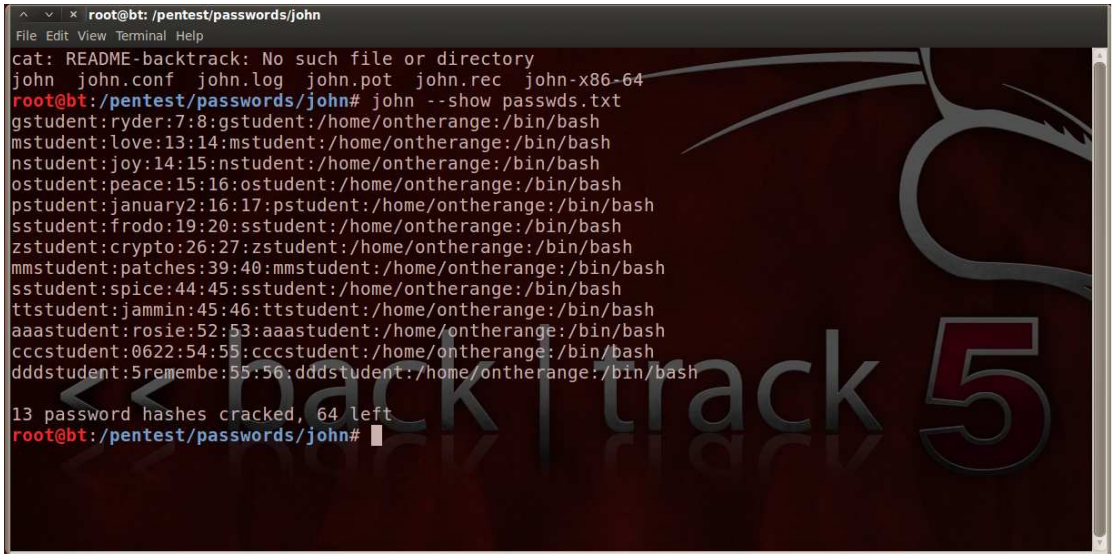
Στο υποκεφάλαιο αυτό θα κάνουμε μια επισκόπηση στο πως μπορεί να εκτελεστεί το John The Ripper σε περιβάλλον BackTrack. Για να μπορέσετε να τρέξετε το John The Ripper θα πάτε από το μενού του BackTrack: **Applications → Privilege Escalation → Password Attacks → Offline Attacks → John The Ripper**

Εικόνα 96. Εκτέλεση John The Ripper σε περιβάλλον BackTrack

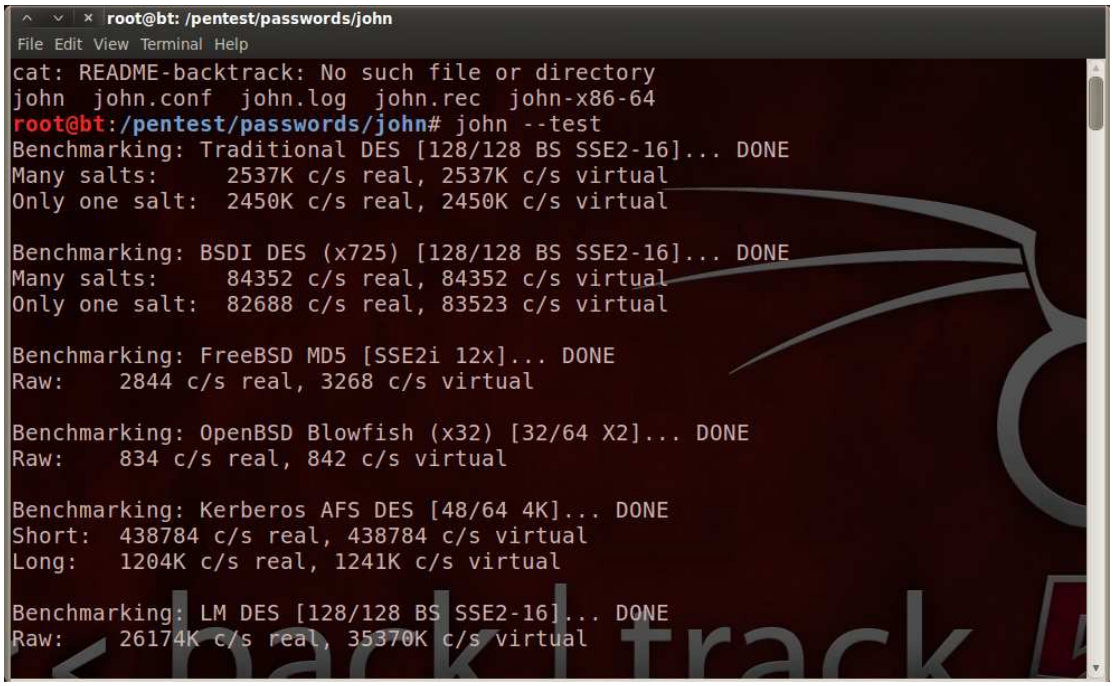
Η εκτέλεση του John The Ripper λοιπόν, δεν διαφέρει σε τίποτα παραπάνω από αυτά που ήδη έχετε μάθει. Οι εντολές εκτελούνται ακριβώς με τον ίδιο τρόπο που έχουμε δείξει και παραπάνω.



Εικόνα 97. John The Ripper - Simple Crack Mode in BackTrack



Εικόνα 98. Αποκρυπτογράφηση κωδικών



Εικόνα 99. John The Ripper - Benchmarking

4. Κεφάλαιο – Θέματα ασφάλειας WLAN

4.1 Συνοπτική Περιγραφή

Τα τελευταία χρόνια παρατηρείται μεγάλη αύξηση στις πωλήσεις φορητών ηλεκτρονικών υπολογιστών και PDA's. Στη ζωή μας έχει κυριαρχήσει η τάση για φορητότητα, κινητικότητα και συνεχή σμίκρυνση των συσκευών (με σκοπό την ευκολότερη μεταφορά τους). Όλα αυτά έχουν σαν αποτέλεσμα, οι παραδοσιακές ενσύρματες τεχνολογίες δικτύωσης, να αποδεικνύονται ανεπαρκείς για το νέο τρόπο ζωής του ανθρώπου.

Την λύση στο πρόβλημα της δικτύωσης, δίνουν οι τεχνολογίες ασύρματης δικτύωσης, που καταργούν τα καλώδια και δίνουν μεγάλο βαθμό ελευθερίας στους χρήστες τους.

Τα ασύρματα δίκτυα[25], όπως και τα ενσύρματα, μεταδίδουν δεδομένα μέσα από ένα μέσο διάδοσης. Το μέσο αυτό είναι οι ραδιοσυχνότητες (RF) που μεταδίδονται στον αέρα. Οι ραδιοσυχνότητες μεταδίδονται στον χώρο, άρα ένα ασύρματο δίκτυο δραστηριοποιείται σε μια συγκεκριμένη περιοχή κάλυψης, έξω από την οποία τα σήματα εξασθενούν σε βαθμό που δεν είναι αξιοποιήσιμα.

Η εγκατάσταση ενός ασύρματου δικτύου σε ένα χώρο απαιτεί την εγκατάσταση κάποιων κεντρικών ασύρματων σταθμών (στα δίκτυα 802.11 ονομάζονται σημεία ασύρματης πρόσβασης – wireless Access Points). Αντίστοιχα, κάθε χρήστης χρειάζεται μια ασύρματη συσκευή για να μπορεί να συνδεθεί σε κάποιον από τους κεντρικούς σταθμούς.

Ο τρόπος λειτουργίας των ασυρμάτων δικτύων τους δίνει τα παρακάτω πλεονεκτήματα σε σχέση με τα ενσύρματα δίκτυα:

- **Φορητότητα και κινητικότητα:** Το πλεονέκτημα αυτό είναι προφανές. Οι χρήστες ενός ασυρμάτου δικτύου μπορούν να συνδέονται στο δίκτυο από οποιοδήποτε σημείο της περιοχής κάλυψης και να μετακινούνται μέσα σε αυτή χωρίς να διακόπτεται η σύνδεση. Μπορούν ακόμα και να μεταπηδούν από μια περιοχή κάλυψης σε μια άλλη (εφόσον αυτές είναι διασυνδεδεμένες κατάλληλα μεταξύ τους), διατηρώντας και πάλι την σύνδεση με το δίκτυο.

- **Απλότητα εγκατάστασης:** Η εγκατάσταση και η σύνδεση σε ένα ασύρματο δίκτυο είναι πολύ απλή και γρήγορη, καθώς δεν απαιτείται εγκατάσταση καλωδίων.

- **Ευελιξία εγκατάστασης:** Η τεχνολογία ασύρματης δικτύωσης μας δίνει τη δυνατότητα να εγκαταστήσουμε δίκτυα σε σημεία ή περιοχές που η εγκατάσταση ενσύρματων δικτύων είναι δύσκολη ή ακόμα και αδύνατη. Για παράδειγμα η σύνδεση μεταξύ απομακρυσμένων κτηρίων ενός οργανισμού είναι μια εφαρμογή η οποία θα απαιτούσε πολύ χρόνο και υψηλό κόστος αν γινόταν με ενσύρματο δίκτυο (προφανώς με χρήση οπτικών ινών). Μια

[25] http://en.wikipedia.org/wiki/Wireless_network

εφαρμογή των ασύρματων δικτύων πέρα από τις παραδοσιακές, είναι η δημιουργία hotspots, δηλαδή ασύρματη κάλυψη δημόσιων ή πολύ εκτεταμένων χώρων με μεγάλη πυκνότητα χρηστών. Τέτοιοι χώροι είναι τα αεροδρόμια, τα λιμάνια, οι καφετέριες, ακόμα και οι πλατείες των πόλεων. Σε τέτοιους χώρους η μαζική παροχή υπηρεσιών δικτύωσης με ενσύρματες τεχνολογίες θα ήταν αδύνατη.

4.2 Απροστάτευτα ασύρματα δίκτυα

Το θέμα μας λοιπόν, είναι πως η αλματώδης αύξηση της χρήσης του internet μέσω ευρυζωνικών συνδέσεων, γίνεται χωρίς σαφείς οδηγίες για την ενεργοποίηση των συστημάτων ασφαλείας που διαθέτουν οι ασύρματοι routers, ούτε από τους παρόχους των υπηρεσιών internet ούτε και από τους κατασκευαστές των συσκευών αυτών. Ένας χρήστης που θέλει απλά να συνδεθεί στο internet, δεν θα κάνει τον κόπο να ασχοληθεί με το θέμα αυτό αφού ούτε γνωρίζει τις επιπτώσεις, ούτε επιθυμεί συνήθως να μπει σε διαδικασίες που του δυσκολεύουν τη ζωή. Δεν θα επιλέξει να πληρώσει το κόστος της (σωστής) εγκατάστασης στον πάροχό του και θα δοκιμάσει μόνος του όπως-όπως, χωρίς να προσλάβει δικό του τεχνικό, χωρίς να φροντίσει έστω να κάτσει να μάθει το πως και το γιατί. Τα αποτελέσματα αυτής της τακτικής είναι κάτι περισσότερο από τα αναμενόμενα. Σε κάθε γειτονιά υπάρχουν ενεργά δεκάδες ασύρματα δίκτυα, απ' τα οποία περισσότερα από τα μισά δεν έχουν τις σωστές ρυθμίσεις ασφαλείας, δηλαδή κρυπτογράφησης των δεδομένων που διακινούν αλλά και αποτροπή της πρόσβασης σε τρίτους, ρισκάροντας κάθε στιγμή σε πολλαπλά επίπεδα! Επίσης, σχεδόν όλες οι συσκευές αυτές διατηρούνται σε συνεχή λειτουργία, μέρα και νύχτα, με αποτέλεσμα να υπάρχει πολύ μεγάλη έκθεση σε επίδοξους εισβολείς.

4.3 Τεχνικές ασφαλείας WLAN

Για λόγους ασφάλειας τα WLAN διαθέτουν ορισμένες δικλείδες ασφαλείας για την προστασία τόσο των χρηστών που τα χρησιμοποιούν, όσο και για την προστασία των δεδομένων που διακινούνται σε αυτά.

a. Η κρυπτογράφηση των ασύρματων δικτύων με διάφορες μεθόδους (WEP, WPA, WPA2), είναι η μία τεχνική ασφαλείας και η οποία αναλύεται διεξοδικά στο επόμενο κεφάλαιο.

b. Μία άλλη τεχνική προστασίας ενός ασύρματου δικτύου είναι η απόκρυψή του, δηλαδή να μην είναι ορατό το όνομά του από μη εξουσιοδοτημένες συσκευές όταν εκπέμπει με απόκρυψη του Service Set Identifier ή αλλιώς SSID.
Το SSID είναι ένα μοναδικό αναγνωριστικό που αποτελείται από 32 χαρακτήρες και χρησιμοποιείται για την ονομασία των ασύρματων δικτύων.

   Το SSID μπορεί να είναι διαφορετικό από το όνομα που έχει εκχωρηθεί σε ένα ασύρματο δρομολογητή (router) από τον κατασκευαστή του. Για παράδειγμα, ο διαχειριστής (administrator) ενός ασύρματου δικτύου μπορεί να ορίσει το όνομα του router ή του ασύρματου σημείου πρόσβασης (access point), ως «Office». Αυτό θα είναι το όνομα που βλέπουν οι χρήστες κατά την

περιήγηση στα διαθέσιμα ασύρματα δίκτυα, αφού το SSID εξασφαλίζει ότι το όνομα του δικτύου θα είναι διαφορετικό από άλλα κοντινά δίκτυα.

Κάθε πακέτο που αποστέλλεται μέσω ενός ασύρματου δικτύου περιλαμβάνει το SSID, το οποίο εξασφαλίζει ότι τα δεδομένα που αποστέλλονται φτάνουν στο σωστό προορισμό. Χωρίς αναγνωριστικά SSID, η αποστολή και η λήψη δεδομένων σε μια τοποθεσία με πολλαπλά ασύρματα δίκτυα, θα ήταν χαοτική και απρόβλεπτη.

c. Άλλη τεχνική προστασίας του ασύρματου δικτύου από την είσοδο σε αυτό μη εξουσιοδοτημένων clients, είναι και ο έλεγχος της Media Access Control Address (MAC address) όσων ασύρματων συσκευών πρόκειται να συνδεθούν με αυτό.

Η διεύθυνση MAC είναι ένα αναγνωριστικό αριθμό υλικού που προσδιορίζει μοναδικά κάθε συσκευή στο δίκτυο. Η διεύθυνση MAC ορίζεται ξεχωριστά για κάθε κάρτα δικτύου, όπως μια Ethernet κάρτα ή Wi-Fi κάρτα και ως εκ τούτου δεν μπορεί να αλλάξει.

Επειδή υπάρχουν εκατομμύρια δικτυακών συσκευών και κάθε συσκευή πρέπει να έχει μια μοναδική διεύθυνση MAC, πρέπει να υπάρχει ένα πολύ ευρύ φάσμα των πιθανών διευθύνσεων. Για το λόγο αυτό, οι διευθύνσεις MAC αποτελούνται από έξι διψήφιους δεκαεξαδικούς αριθμούς, που χωρίζονται με άνω και κάτω τελεία. Για παράδειγμα, μια κάρτα Ethernet μπορεί να έχει μια διεύθυνση MAC 00:0D:83:B1:C0:8E.

4.3.1 MAC spoofing

Έπειτα από την παραπάνω συνοπτική αναφορά των τεχνικών ασφαλείας των ασύρματων δικτύων θα προχωρήσουμε στην ανάλυση πως μπορείτε να τις παρακάμψετε, όμως **απαραίτητο προληπτικό μέτρο** για να πραγματοποιήσει κάποιος επίθεση σε ασύρματο δίκτυο μέσω κάποιας ασύρματης συσκευής που διαθέτει είναι να μπορέσει να κρύψει τα ίχνη του, ώστε να μην μπορεί να αποκαλυφθεί.

Κλασσική τεχνική για να γίνει εφικτό αυτό είναι η αλλαγή της MAC address της ασύρματης κάρτας δικτύου που χρησιμοποιεί με μια εικονική. Η τεχνική αυτή λέγεται MAC address spoofing. Ο λόγος της τεχνικής αυτής είναι ότι με την κίνηση που υπάρχει προς και από ένα access point, εντοπίζονται όλες οι MAC addresses των συσκευών που προσπαθούν να συνδεθούν με αυτό ή που είναι συνδεδεμένες με αυτό. Αυτό σημαίνει ότι μπορεί να καταγράφονται με κάποια μέθοδο οι MAC addresses και να εντοπιστείτε.

Για το MAC spoofing θα χρησιμοποιήσετε το εργαλείο macchanger το οποίο υπάρχει ήδη μέσα στο Backtrack και δουλεύει μέσω terminal. Δίνοντας την εντολή

- **macchanger --help**

εμφανίζονται οι επιλογές της εντολής macchanger

Εικόνα 100. Οι επιλογές της εντολής macchanger

Η δομή της εντολής macchanger είναι:

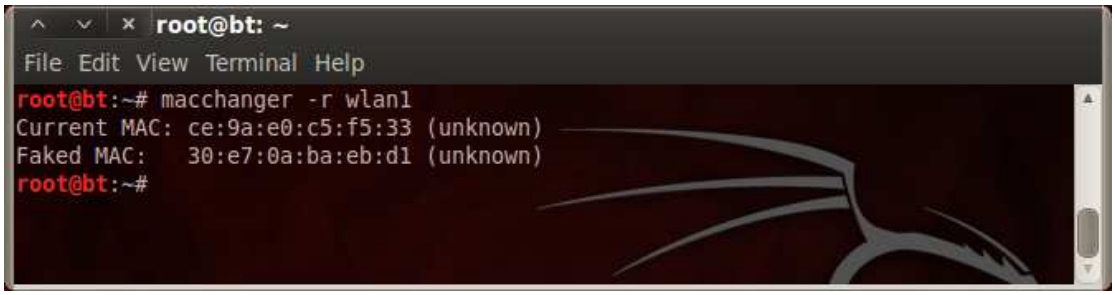
- **macchanger [options] device (πχ wlan1)**

-h	(εναλλακτικά) --help	Εκτυπώνει το μενού επιλογών της macchanger, ίδιο με την εντολή macchanger --help
-V	(εναλλακτικά) --version	Εκτυπώνει την έκδοση του macchanger
-s	(εναλλακτικά) --show	Δείχνει τη MAC address της κάρτας δικτύου που έχετε
-e	(εναλλακτικά) --endding	Δεν αλλάζει τα bytes της MAC που αφορούν τον κατασκευαστή
-a	(εναλλακτικά) --another	Καθορίζει MAC address του ίδιου κατασκευαστή με την κάρτα δικτύου που έχετε
-A		Καθορίζει MAC address οποιουδήποτε κατασκευαστή στην κάρτα δικτύου που έχετε
-r	(εναλλακτικά) --random	Δίνει στην κάρτα δικτύου εντελώς τυχαία MAC address
-l	(εναλλακτικά) --list[=keyword]	Εκτυπώνει τη λίστα κατασκευαστών καρτών δικτύων
-m	(εναλλακτικά) --mac=XX:XX:XX:XX:XX:XX	Με την εντολή αυτή καθορίζετε εσείς τη MAC address που θέλετε στην κάρτα δικτύου

Πίνακας 17. Ανάλυση παραμέτρων εντολής macchanger

Αν για παράδειγμα θέλετε να δώσετε μια τυχαία MAC address στην κάρτα δικτύου δίνετε την εντολή:

- **macchanger -r wlan1**



Εικόνα 101. Παράδειγμα εντολής macchanger

Όπως φαίνεται παραπάνω το macchanger εκτυπώνει την παλιά και νέα διεύθυνση MAC της κάρτας δικτύου.

4.3.2 Αποκάλυψη κρυφών SSIDs ασύρματων δικτύων

Σκοπός της «επίθεσης» αυτής είναι να μπορέσετε να αποκαλύψετε κρυφά δίκτυα των οποίων το SSID δεν εκπέμπεται και δεν μπορεί να τα βρει κάποιος με αναζήτηση ασύρματων δικτύων.

Συνήθως, τα access points στέλνουν το SSID τους μέσα στα Beacon frames για να μπορούν να τα εντοπίζονται από τους υποψήφιους clients. Τα beacon frames είναι frames διαχείρισης με βάση το πρότυπο IEEE 802.11 WLAN. Περιέχουν όλες τις πληροφορίες σχετικά με το δίκτυο και εκπέμπονται περιοδικά για να αναγγείλουν την παρουσία ενός WLAN. Στα κρυφά δίκτυα τα beacon frames δεν περιέχουν το SSID του WLAN. Αποτέλεσμα αυτού είναι μόνο χρήστες που ξέρουν ποιο είναι το SSID του access point να μπορούν να συνδεθούν με αυτό.

Όπως θα δείτε και από το παρακάτω πείραμα η τεχνική της απόκρυψης του SSID ενός WLAN δεν είναι επαρκής τεχνική ασφάλειας και προστασίας του, αν και μερικοί διαχειριστές νομίζουν ότι είναι.

Αρχικά για να δείτε το SSID του πειραματικού ασύρματου δικτύου στα beacon frames που αυτό εκπέμπει, θα πρέπει να χρησιμοποιήσετε το γνωστό εργαλείο σύλληψης πακέτων wireshark, το οποίο είναι προεγκατεστημένο στο Backtrack. Απαραίτητη προϋπόθεση είναι η ασύρματη κάρτα δικτύου με την οποία θα κάνετε capture τα πακέτα να είναι σε monitor mode.

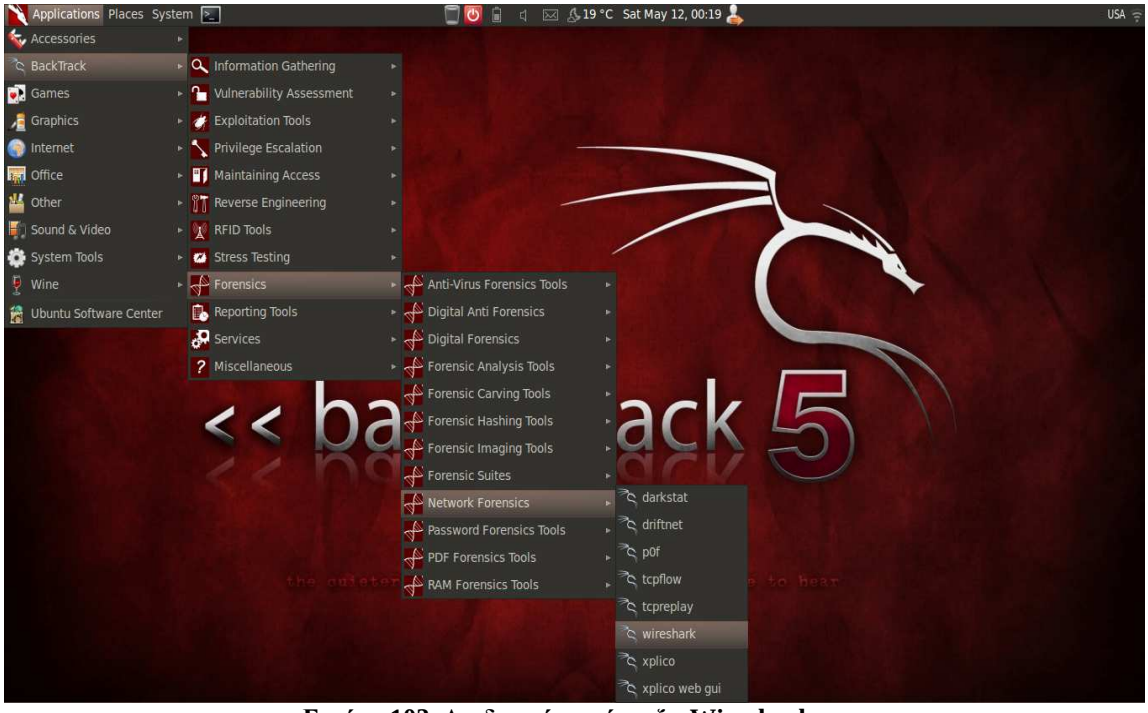
Για να τεθεί η κάρτα σας σε λειτουργία monitor mode δίνετε την εντολή

- **airmon-ng start wlanx (όπου x το νούμερο με το οποίο αντιστοιχεί την ασύρματη κάρτα δικτύου σας το Backtrack)**

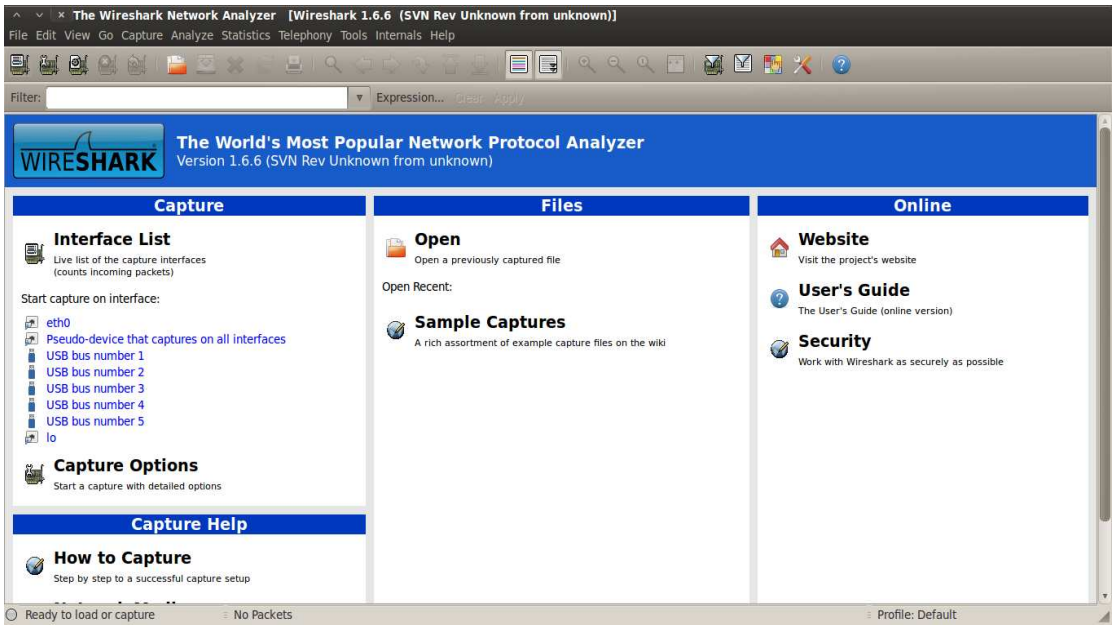
Εικόνα 102. Ρύθμιση ασύρματης κάρτας σε monitor mode

Έπειτα ξεκινάτε το wireshark ακολουθώντας την ακόλουθη διαδρομή στα μενού:

Applications ► Backtrack ► Forensics ► Network Forensics ► wireshark



Εικόνα 103. Διαδρομή για έναρξη Wireshark



Εικόνα 104. Εικόνα έναρξης του wireshark

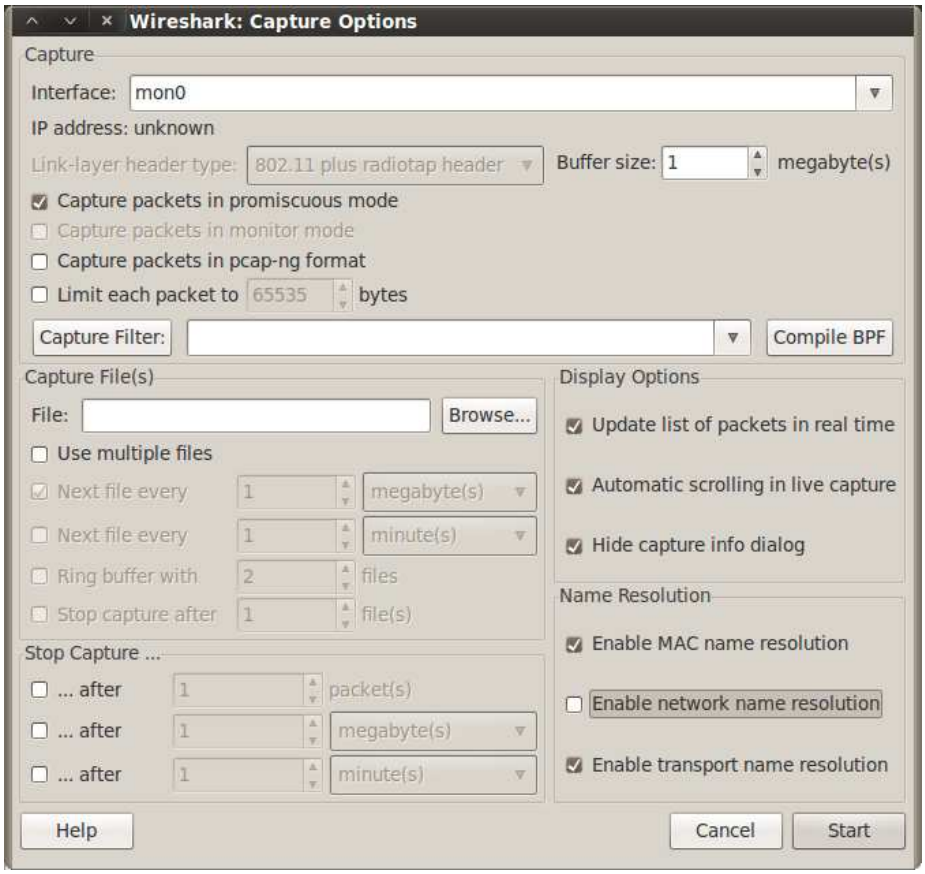
Από το μενού:

Capture ► Interfaces

σας εμφανίζεται το παράθυρο επιλογής interfaces για capture

Εικόνα 105. Παράθυρο capture interfaces

Πατάτε το κουμπί options του mon0 για να δείτε τις ρυθμίσεις του με τις οποίες το wireshark θα κάνει capture πακέτα από την ασύρματη κάρτα σας.



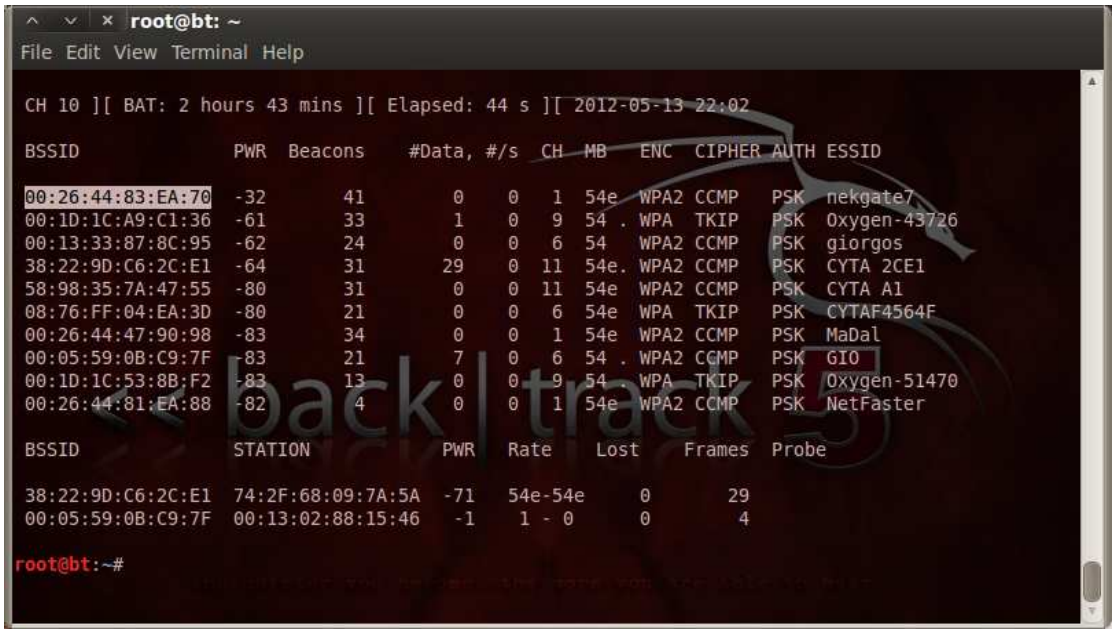
Εικόνα 106. Ρυθμίσεις interface πριν το capture

Θα πρέπει να είναι απενεργοποιημένη η επιλογή enable network name resolution για να μην σας βγάζει σφάλματα η κάρτα δικτύου και μετά πατάτε το κουμπί start για να ξεκινήσει η καταγραφή πακέτων.

Για να δείτε την mac address του router – στόχου μπορείτε να δώσετε σε ένα παράθυρο terminal την εντολή:

- **airodump-ng mon0**

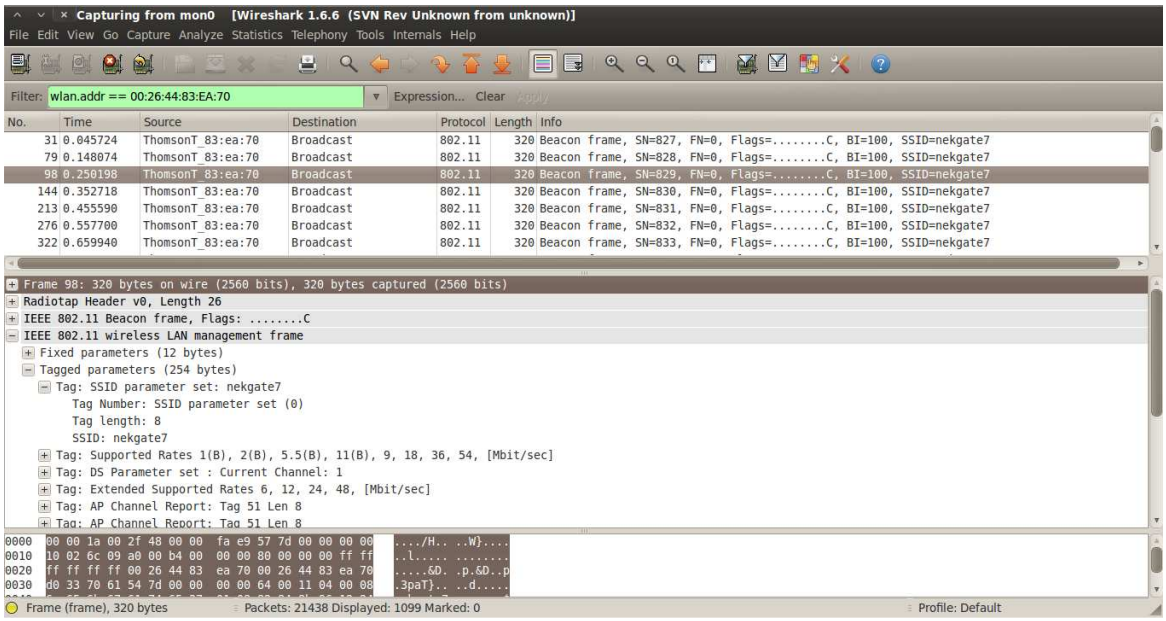
Στο συγκεκριμένο παράδειγμα το SSID του router – στόχου είναι nekgate7



Εικόνα 107. Λίστα SSIDs που εντοπίζει η ασύρματη κάρτα δικτύου και οι MAC

Γυρνώντας πάλι στο παράθυρο του wireshark, για να σας δείξει τα packets του router – στόχου, μπορείτε να επικεντρώσετε στα beacon frames του και να δείτε το SSID του, δίνοντας στο πλαίσιο filter το παρακάτω display filter:

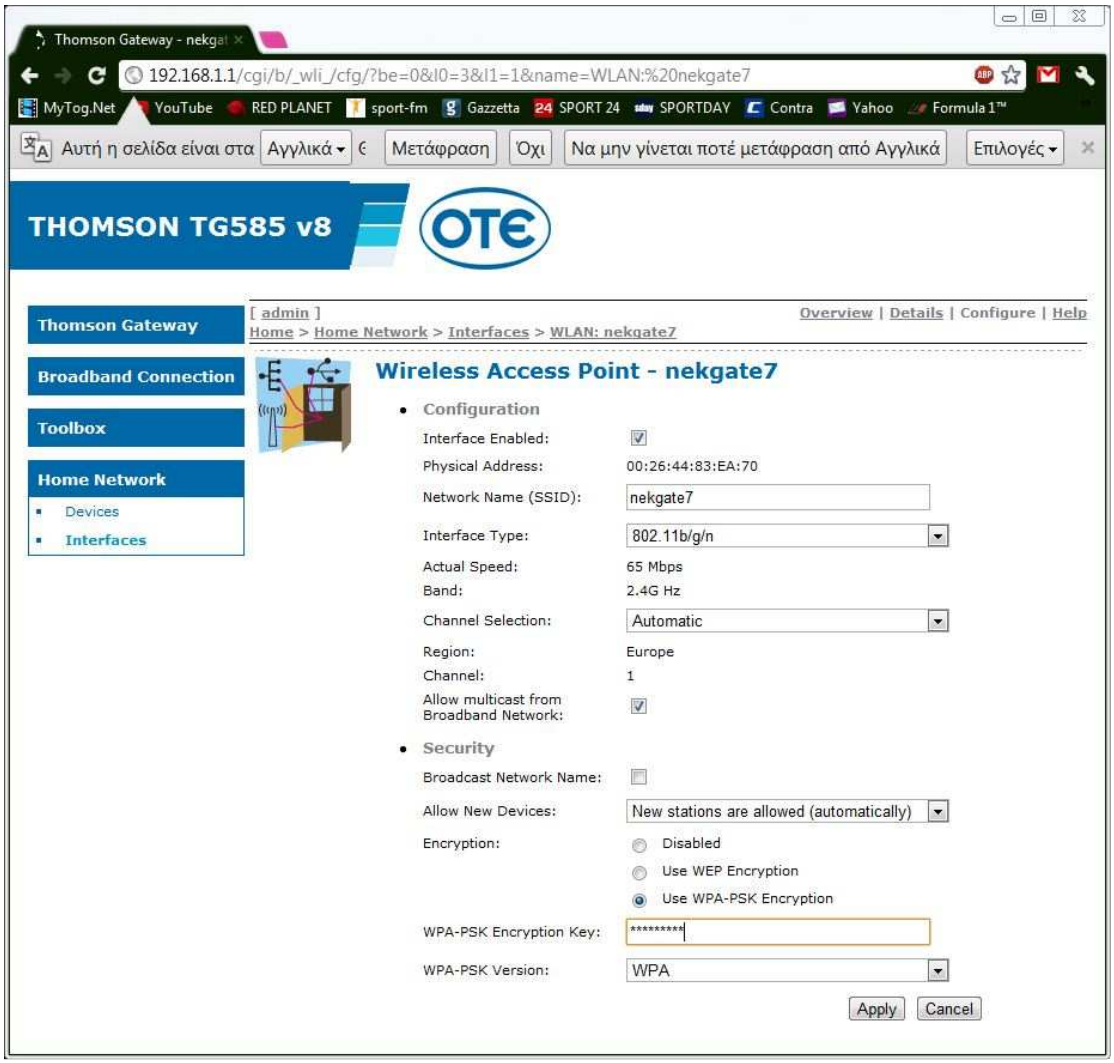
- **wlan.addr == mac address router – στόχου**



Εικόνα 108. Φιλτράρισμα beacon frames συγκεκριμένου router

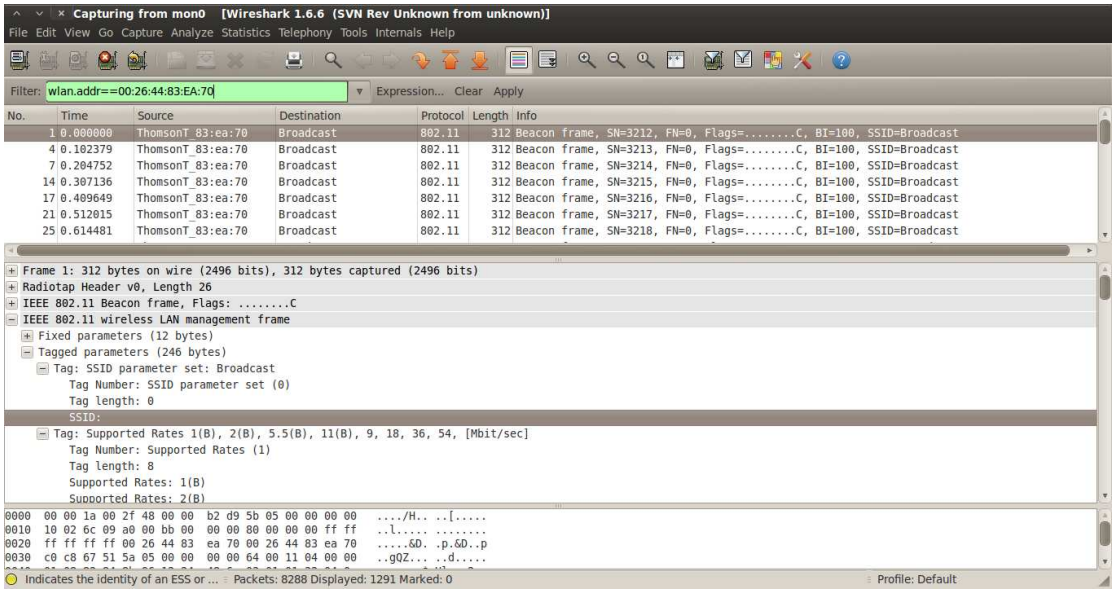
Αν επιλέξετε ένα beacon frame και ανοίξετε τις καρτέλες του από κάτω:
IEEE 802.11 wireless LAN management frame ► tagged parameters βλέπετε και εκεί το SSID του ασυρμάτου δικτύου που σας ενδιαφέρει.

Επόμενο στάδιο είναι να απενεργοποιήσετε στο router το SSID broadcast όπως παρακάτω, που απενεργοποιήθηκε η επιλογή Broadcast Network Name.



Εικόνα 109. Απενεργοποίηση SSID broadcast

Αν ξαναπάτε στην οθόνη του wireshark θα δείτε ότι το SSID δεν υπάρχει στα beacon frames.



Εικόνα 110. Εξαφάνιση SSID από τα Beacon frames

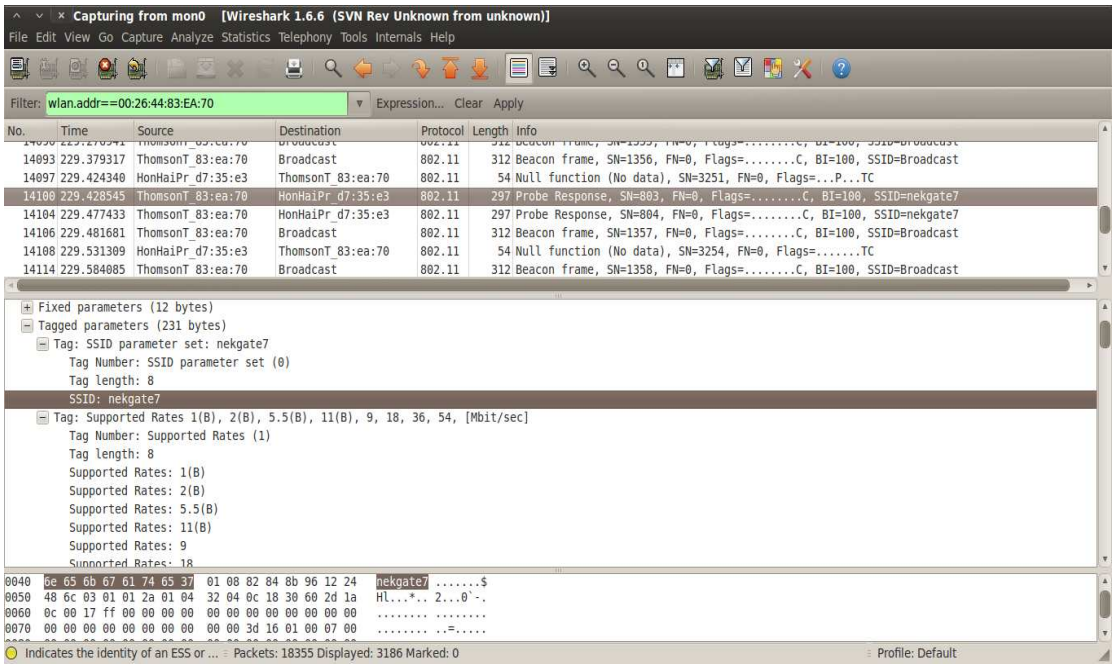
Για να εντοπιστεί το SSID υπάρχουν δύο τρόποι:

Α) Ο πρώτος είναι ο παθητικός (passive). Δηλαδή να περιμένετε να προσπαθήσει κάποιος client να συνδεθεί στο κρυφό ασύρματο δίκτυο, ώστε να κυκλοφορήσουν frames Probe Request και Probe Response. Αλλά τί είναι αυτά τα frames;

Probe request frame: Ένας σταθμός στέλνει το frame αυτό όταν χρειάζεται να πάρει πληροφορίες από άλλους σταθμούς, όπως πχ. ποια access points είναι εντός εμβέλειας του.

Probe response frame: ένας σταθμός θα απαντήσει με τέτοιο frame το οποίο περιέχει πληροφορίες όπως πχ τις ταχύτητες που υποστηρίζει, όταν του ζητηθεί με probe request frame.

Όταν κυκλοφορήσουν αυτά τα frames μεταξύ client και κρυφού access point περιέχουν το SSID του δικτύου που μας ενδιαφέρει να εντοπίσουμε και θα αποκαλυφτεί η παρουσία του.



Εικόνα 111. Probe response πακέτο με το SSID κρυφού access point

Β) Ο δεύτερος είναι ο ενεργητικός (active). Δηλαδή να προκαλέσετε το deauthentication των clients από το κρυφό access point για να αναγκαστούν να αποσυνδεθούν και να επανασυνδεθούν και έτσι να κυκλοφορήσουν Probe Request και Probe Response frames στα οποία θα υπάρχει το SSID του ασύρματου δικτύου.

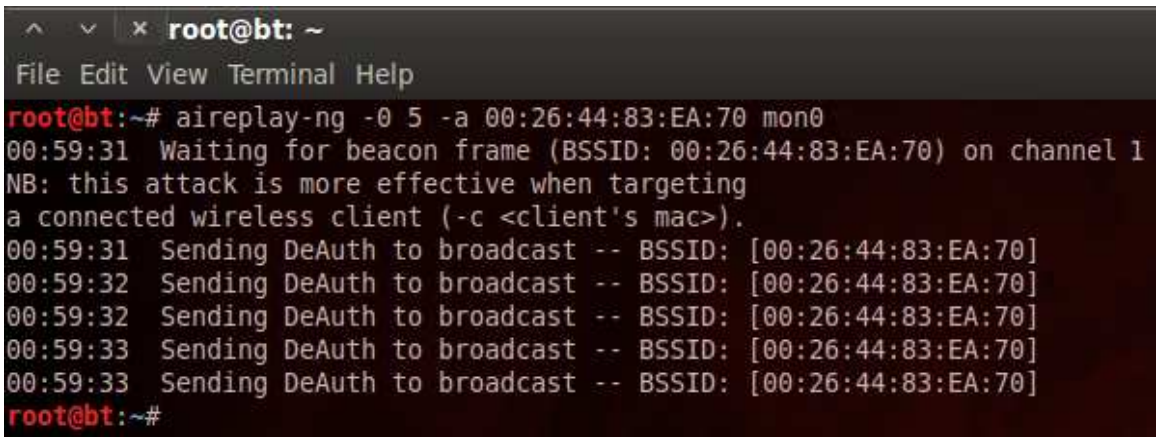
Το deauthentication θα το προκαλέσετε μέσω της εντολής:

- **aireplay-ng -0 x –a (mac address AP με hidden SSID) mon0**

  στο παράδειγμά μας

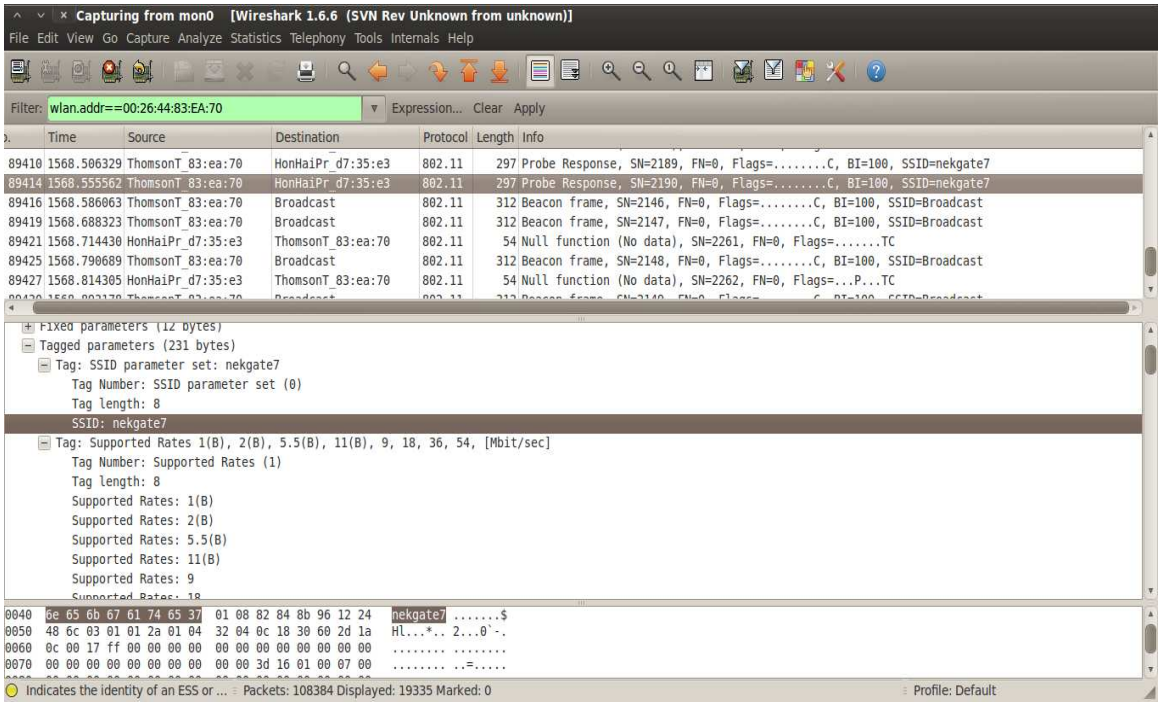
- **aireplay-ng -0 5 –a 00:26:44:83:EA:70 mon0**

Το -0 αντιστοιχεί στην επιλογή για deauthentication attack, το x ο αριθμός των deauthentication packets που θα σταλούν και το –a χρειάζεται για να προσδιοριστεί η MAC address του access point που στοχεύετε



Εικόνα 112. Deauthentication attack

Αυτό προκάλεσε τις αποσυνδέσεις των clients και οι οποίοι λόγω της προσπάθειας επανασύνδεσης εκπέμφθηκαν Probe Request και Probe Response frames, τα οποία τα βλέπετε παρακάτω στο wireshark με το κρυφό SSID να φαίνεται.



Εικόνα 113. Εμφάνιση SSID σε probe response frame

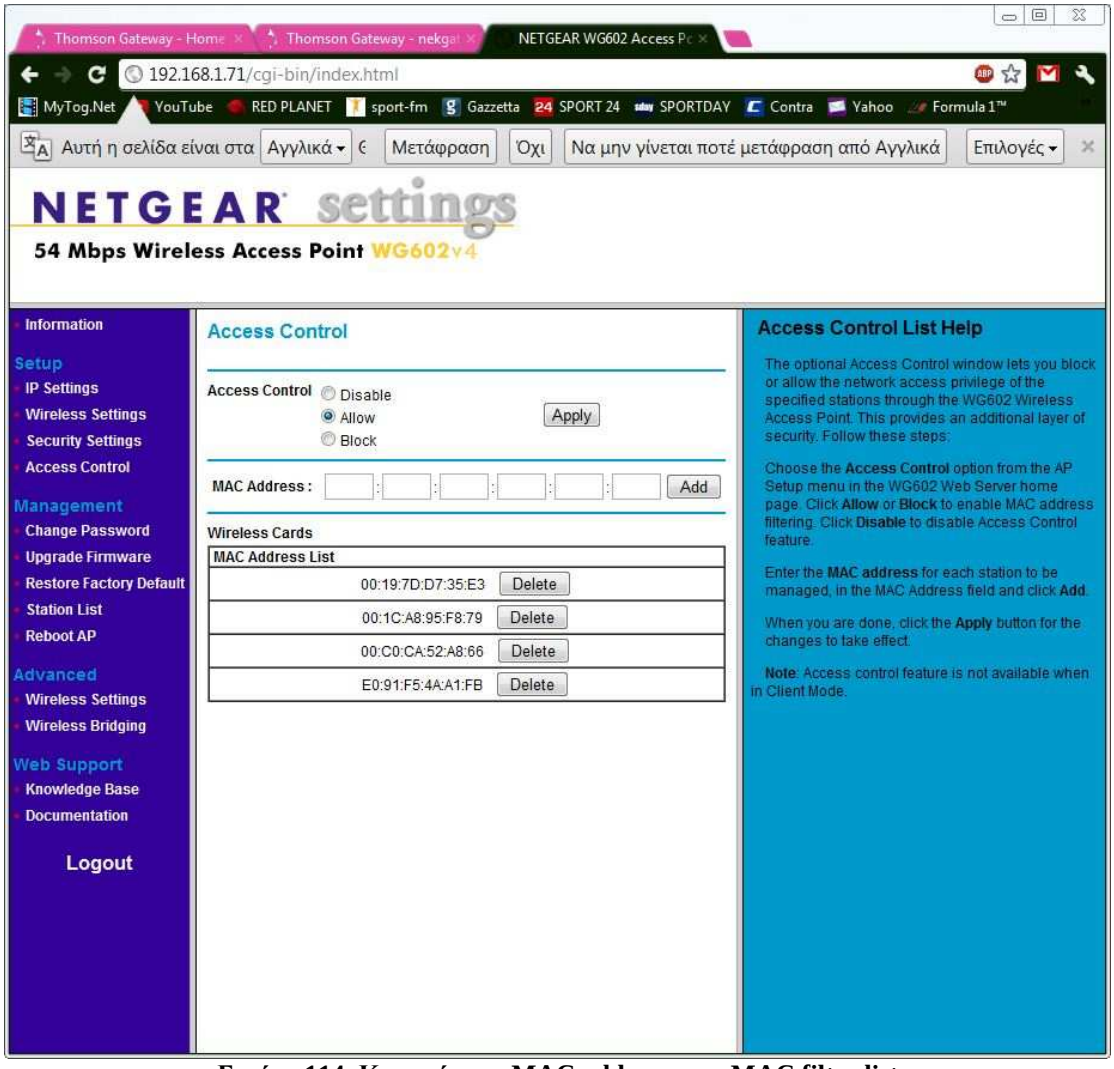
Από τα παραπάνω είναι προφανές ότι η απόκρυψη του SSID δεν είναι από μόνο του αποτελεσματικό μέτρο προστασίας ενός ασύρματου δικτύου και θα πρέπει να συνδυάζεται και με άλλες δικλείδες ασφαλείας.

4.3.3 MAC filters

Η προστασία ενός ασύρματου δικτύου από την ανεξέλεγκτη είσοδο clients σε αυτό είναι μια παλιά μέθοδος και η οποία χρησιμοποιούνταν για αυθεντικοποίηση (authentication) και εξουσιοδότηση (authorization) clients σε ενσύρματα δίκτυα, η οποία όμως στα ασύρματα δίκτυα αποδεικνύεται κακή επιλογή.

Η ιδέα πίσω από το συγκεκριμένο πείραμα στηρίζεται στο ότι ο διαχειριστής του ασύρματου δικτύου έχει εξουσιοδοτήσει συγκεκριμένες ασύρματες κάρτες συγκεκριμένων clients να συνδέονται σε αυτό. Αυτό γίνεται μέσω μιας λίστας MAC addresses που έχει καταχωρηθεί από τον διαχειριστή στον ασύρματο δρομολογητή (wireless router) ή στο ασύρματο AP και η οποία περιέχει τις MAC διευθύνσεις συγκεκριμένων ασύρματων καρτών.

Για να ξεκινήσετε την πραγματοποίηση του πειράματος καταχωρείτε στο ασύρματο router συγκεκριμένες MAC addresses που θα επιτρέψετε να συνδεθούν στο ασύρματο δίκτυο. Παρακάτω ακολουθεί η εικόνα μιας MAC address filter list.



Εικόνα 114. Καταχώριση MAC addresses σε MAC filter list

Αφού καταχωρήσετε τις MAC addresses θα πρέπει να ενεργοποιήσετε το access control μέσω MAC filter. Επίσης, για τους σκοπούς του πειράματος θα πρέπει

να έχετε απενεργοποιήσει άλλα είδη ασφάλειας όπως WEP, WPA, κλπ

Θα πρέπει και πάλι την ασύρματη κάρτα δικτύου σας στον υπολογιστή που θα κάνει την επίθεση, να έχει γυρίσει σε monitor mode, σύμφωνα με τα βήματα που περιγράφηκαν στο προηγούμενο υποκεφάλαιο και να τρέχετε το wireshark.

Είναι αναμενόμενο ότι η συσκευή της οποίας έχετε καταχωρίσει τη mac address θα συνδεθεί επιτυχώς με το ασύρματο δίκτυο. Θα πρέπει να δοκιμάσετε να συνδέσετε την μη καταχωρημένη ασύρματη κάρτα δικτύου στο ασύρματο δίκτυο. Αυτό για να το κάνετε δίνετε την εντολή

- **iwconfig wlanx essid “Wireless Security” channel x**
    - όπου το wlanx είναι η ασύρματη κάρτα δικτύου που διαθέτετε για την επίθεση, Wireless Security είναι το essid του δικτύου και channel x, το κανάλι στο οποίο εκπέμπει το συγκεκριμένο access point.

Τώρα θα πρέπει να δείτε αν έχετε συνδεθεί με το ασύρματο δίκτυο δίνοντας την εντολή

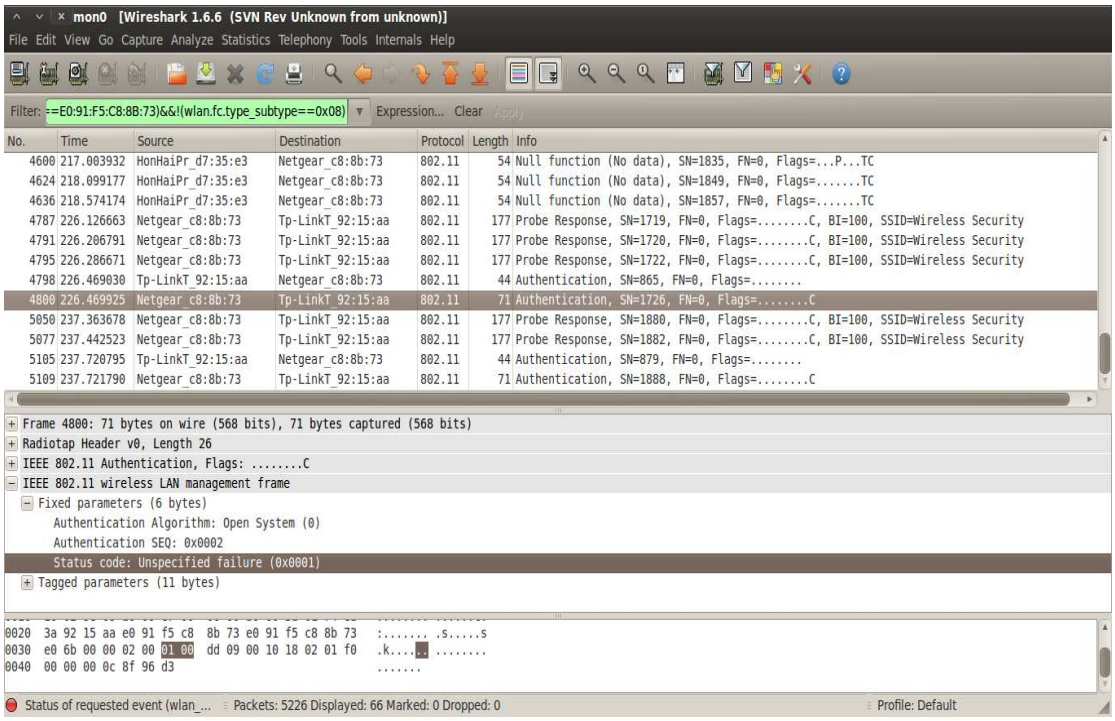
- **iwconfig**

Η εικόνα που παίρνετε είναι η παρακάτω

Εικόνα 115. Μη σύνδεση με MAC filter protected AP

Το ότι δεν έχετε συνδεθεί το διαπιστώνετε και από το γεγονός ότι στο πεδίο Access Point υπάρχει η ένδειξη Not-Associated.

Για να δείτε τι ακριβώς έχει συμβεί κοιτάζετε τα περιεχόμενα των Authentication packets στο wireshark.



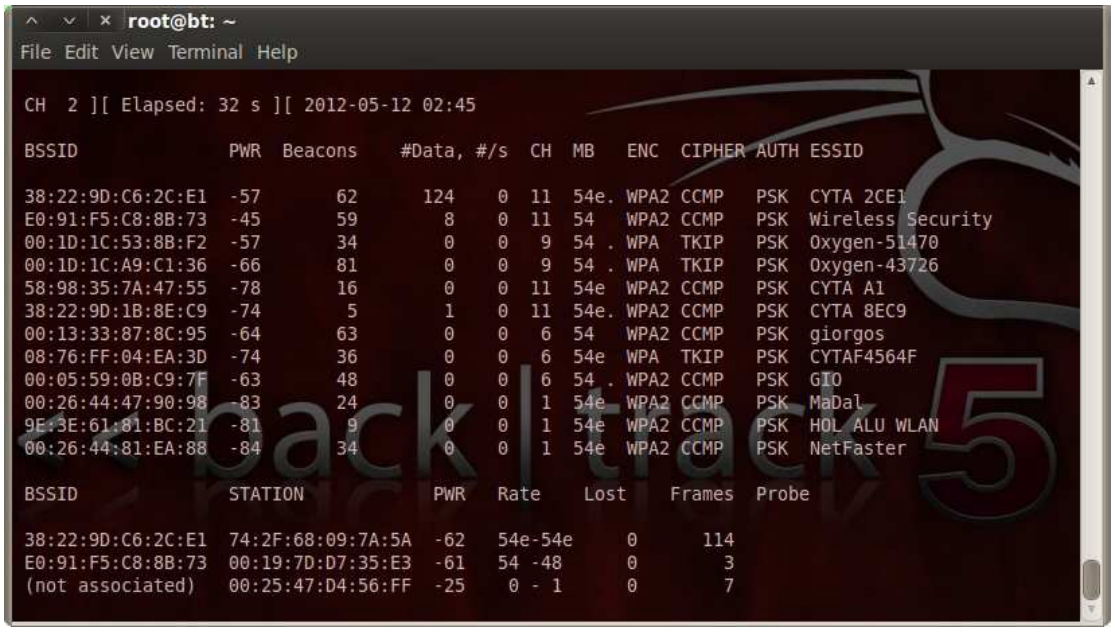
Εικόνα 116. MAC address authentication failure

Στην παραπάνω εικόνα βλέπετε κάτι λογικό και αναμενόμενο. Κοιτάζοντας το authentication frame στα περιεχόμενά του βλέπετε το μήνυμα Status code: Unspecified failure. Δηλαδή, ότι δεν έγινε σύνδεση της ασύρματης κάρτας δικτύου με το ασύρματο δίκτυο στόχο.

Για να μπορέσετε, να προχωρήσετε στην επίθεση θα πρέπει να εντοπίσετε ποιες ασύρματες συσκευές έχουν συνδεθεί με το ασύρματο AP στόχο, ώστε να δείτε ποιες είναι οι MAC addresses έχουν.

Για να το κάνετε αυτό θα χρησιμοποιήσετε το εργαλείο airodump-ng. Η εντολή που θα δώσετε είναι:

- **airodump-ng mon0**

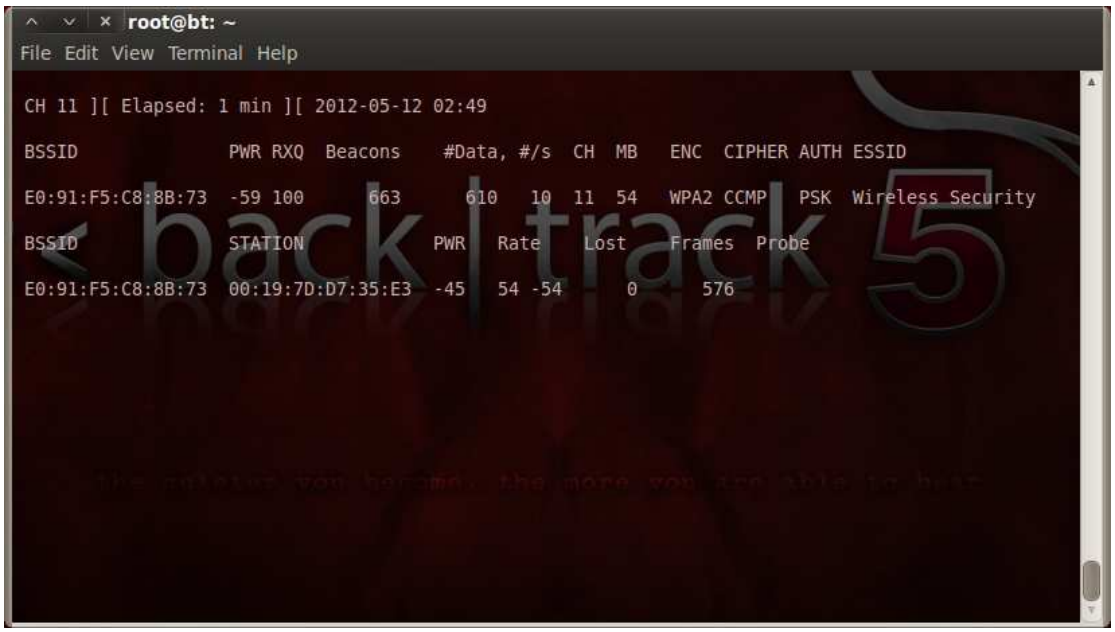


Εικόνα 117. Λίστα ασύρματων δικτύων με συνδεδεμένους clients

Αν πάλι θέλετε για να μη βλέπετε όλα τα ασύρματα δίκτυα να βλέπετε μόνο ένα συγκεκριμένο δίνετε την εντολή

- **airodump-ng -c x –a --bssid (access point στόχου) mon0**

το –c x ρυθμίζει την ασύρματη κάρτα στο κανάλι όπου λειτουργεί και το access point και το –a δείχνει στην οθόνη τους clients που είναι συνδεδεμένοι με το access point.



Εικόνα 118. Clients στο ασύρματο δίκτυο στόχο

Όταν βρείτε την MAC address του client με την οποία έχει συνδεθεί στο ασύρματο δίκτυο στόχο προχωράτε σε αλλαγή της MAC address της ασύρματης κάρτας που χρησιμοποιείτε με την τεχνική MAC spoofing και η οποία αναφέρθηκε στο υποκεφάλαιο 4.3.1. με τη χρήση του εργαλείου macchanger.

Η εντολή που θα δώσετε είναι

- **macchanger –m (επιθυμητή διεύθυνση MAC) wlanx**
  - wlanx η ασύρματη κάρτα που βλέπει το Backtrack

```
root@bt:~# macchanger -m 00:19:7D:D7:35:E3 wlan6
Current MAC: 74:ea:3a:92:15:aa (unknown)
Faked MAC:   00:19:7d:d7:35:e3 (unknown)
root@bt:~#
```

Εικόνα 119. Αλλαγή MAC address με το macchanger

Το επόμενο στάδιο είναι να συνδεθείτε με το ασύρματο AP και αυτό γίνεται με την εντολή

- **iwconfig wlanx essid "όνομα access point" channel x (το κανάλι λειτουργίας)**

και με την εντολή

- **iwconfig wlanx**

βλέπετε ότι έχετε συνδεθεί! Αυτό επιβεβαιώνεται επειδή εμφανίζεται η MAC address του Access Point

```
root@bt: ~
File  Edit  View  Terminal  Help
root@bt:~# ifconfig wlan6 down
root@bt:~# macchanger -m 00:19:7D:D7:35:E3 wlan6
Current MAC: 00:19:7d:d7:35:e3 (unknown)
Faked MAC:   00:19:7d:d7:35:e3 (unknown)
It's the same MAC!!
root@bt:~# ifconfig wlan6 up
root@bt:~# iwconfig wlan6 essid "Wireless Security" channel 11
root@bt:~# iwconfig wlan6
wlan6     IEEE 802.11bgn  ESSID:"Wireless Security"
          Mode:Managed  Frequency:2.462 GHz  Access Point: E0:91:F5:C8:8B:73
          Bit Rate=39 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=50/70  Signal level=-60 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@bt:~# clear

root@bt:~#
```

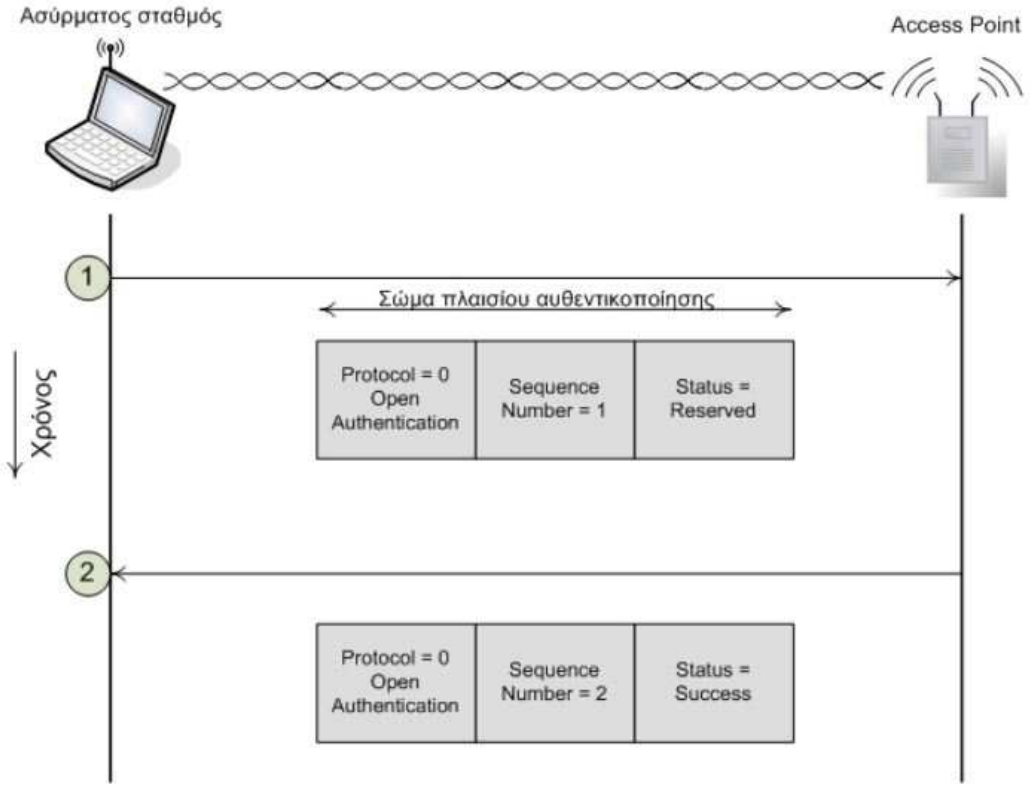
Εικόνα 120. Σύνδεση MAC spoofed wireless card

Από την παραπάνω εικόνα επιβεβαιώνεται ότι η τεχνική προστασίας ενός ασύρματου δικτύου μέσω MAC filter δεν είναι και η καλύτερη επιλογή και θα πρέπει να αναζητούνται άλλες επιλογές προστασίας.

4.3.4 Open Authentication

Η ανοιχτή αυθεντικοποίηση συνιστάται ουσιαστικά σε μία απλή ανταλλαγή μηνυμάτων και **δεν παρέχει από μόνη της κανενός είδους ασφάλεια.** Η μοναδική πληροφορία που πρέπει να είναι γνωστή σε ένα σταθμό για να συνδεθεί στο δίκτυο είναι το SSID του AP.

Στο παρακάτω σχήμα φαίνεται η διαδοχή των μηνυμάτων. Ο εναρκτήριος σταθμός είναι συνήθως μία ασύρματη κάρτα ενός σταθμού, ενώ ο σταθμός προορισμού είναι συνήθως μια ασύρματη κάρτα ενός AP. Το πρώτο μήνυμα το στέλνει ο εναρκτήριος σταθμός, το οποίο είναι ένα πλαίσιο διαχείρισης τύπου αυθεντικοποίησης. Το AP επεξεργάζεται το μήνυμα και στέλνει ως απόκριση στο σταθμό, το μήνυμα 2 που είναι ιδίου τύπου με το πρώτο. Η διαφορά είναι ότι το δεύτερο μήνυμα περιέχει τον κωδικό κατάστασης με τιμή Successful (Επιτυχής) ή κάποιο κωδικό αποτυχίας μαζί με την αιτιολογία αποτυχίας. Μόλις ο σταθμός λάβει το μήνυμα 2 και έχει κωδικό επιτυχίας, μεταβαίνει στην κατάσταση "Αυθεντικοποιημένος".

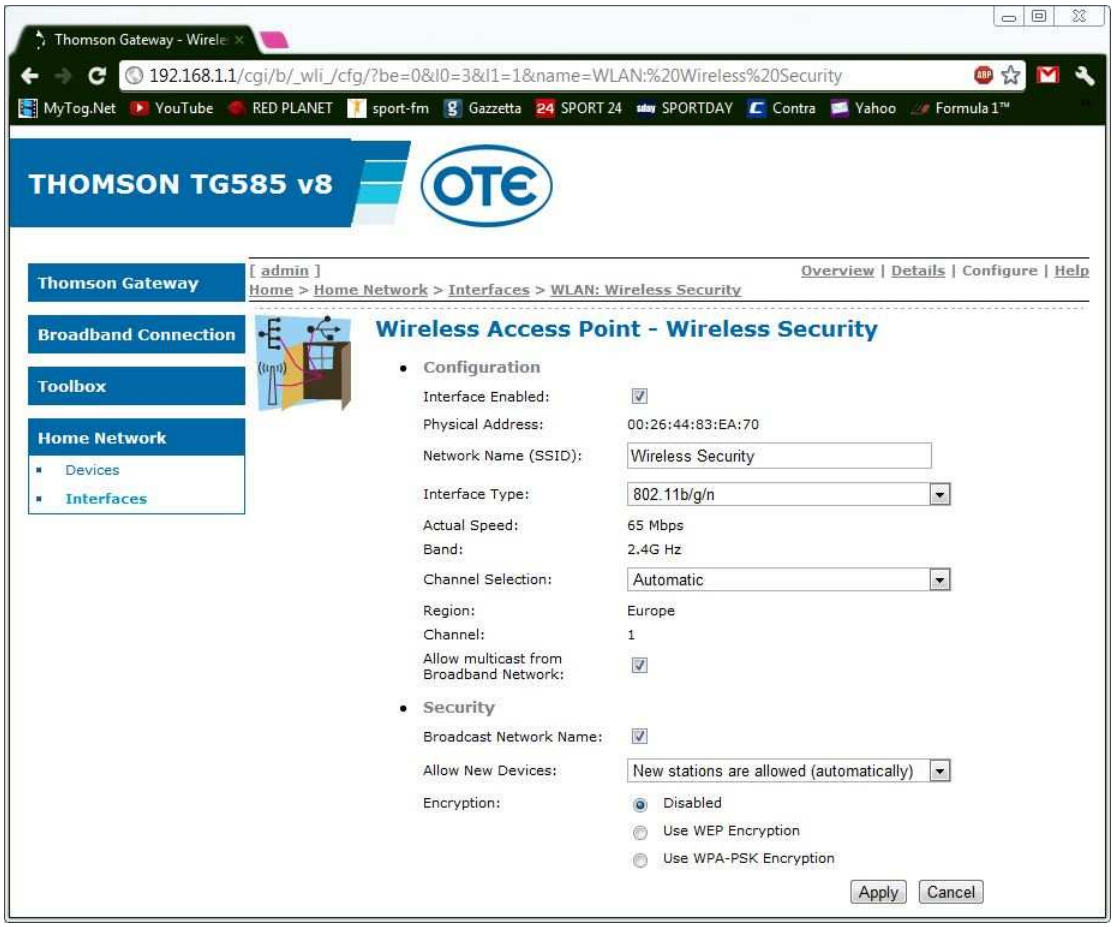


Εικόνα 121. Αυθεντικοποίηση Ανοιχτού Συστήματος

Δύο εύλογες περιπτώσεις χρήσης της Ανοιχτής Αυθεντικοποίησης είναι:

- Όταν ο απαιτούμενος βαθμός ασφάλειας εξασφαλίζεται σε ανώτερα επίπεδα με χρήση VPN / Ipsec. Για παράδειγμα μπορεί να χρησιμοποιηθεί σε Hotspot παροχής Internet (Ξενοδοχεία, Αεροδρόμια).
- Όταν το AP είναι μέρος ενός ελεύθερου/κοινοτικού δικτύου και επομένως η ύπαρξη κάποιου μηχανισμού αυθεντικοποίησης δεν έχει και τόσο νόημα.

Παρακάτω λοιπόν παρατηρείτε το δίκτυο “Wireless Security” το οποίο είναι ανοιχτό χωρίς κάποιο είδος ασφαλείας.



Εικόνα 122. Open Network

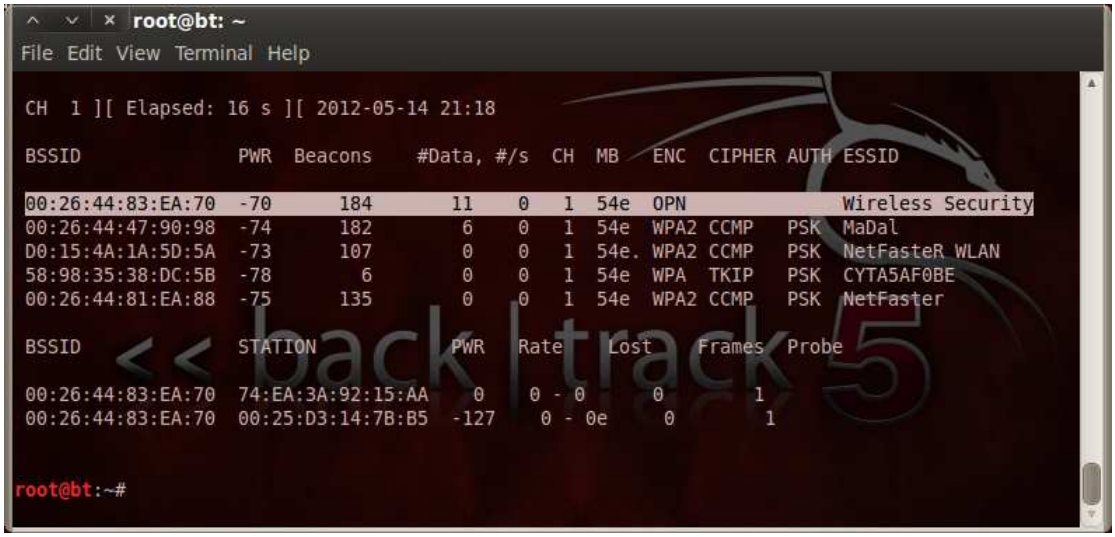
Χρησιμοποιείτε τις παρακάτω εντολές

- **iwconfig wlanx essid “όνομα δικτύου”**
  - wlanx η κάρτα δικτύου που χρησιμοποιείτε

- **iwconfig wlanx**

Εικόνα 123. Σύνδεση σε open authenticated WLAN

Στην παραπάνω εικόνα φαίνεται η σύνδεση της ασύρματης κάρτας με το WLAN και από την ένδειξη Encryption: off φαίνεται ότι δεν υπάρχει κρυπτογράφηση



Εικόνα 124. Δίκτυα που εντοπίζει η Wireless Card

Από την παραπάνω εικόνα φαίνεται επίσης η ένδειξη OPN επιβεβαιώνει τη μη κρυπτογράφηση του δικτύου.

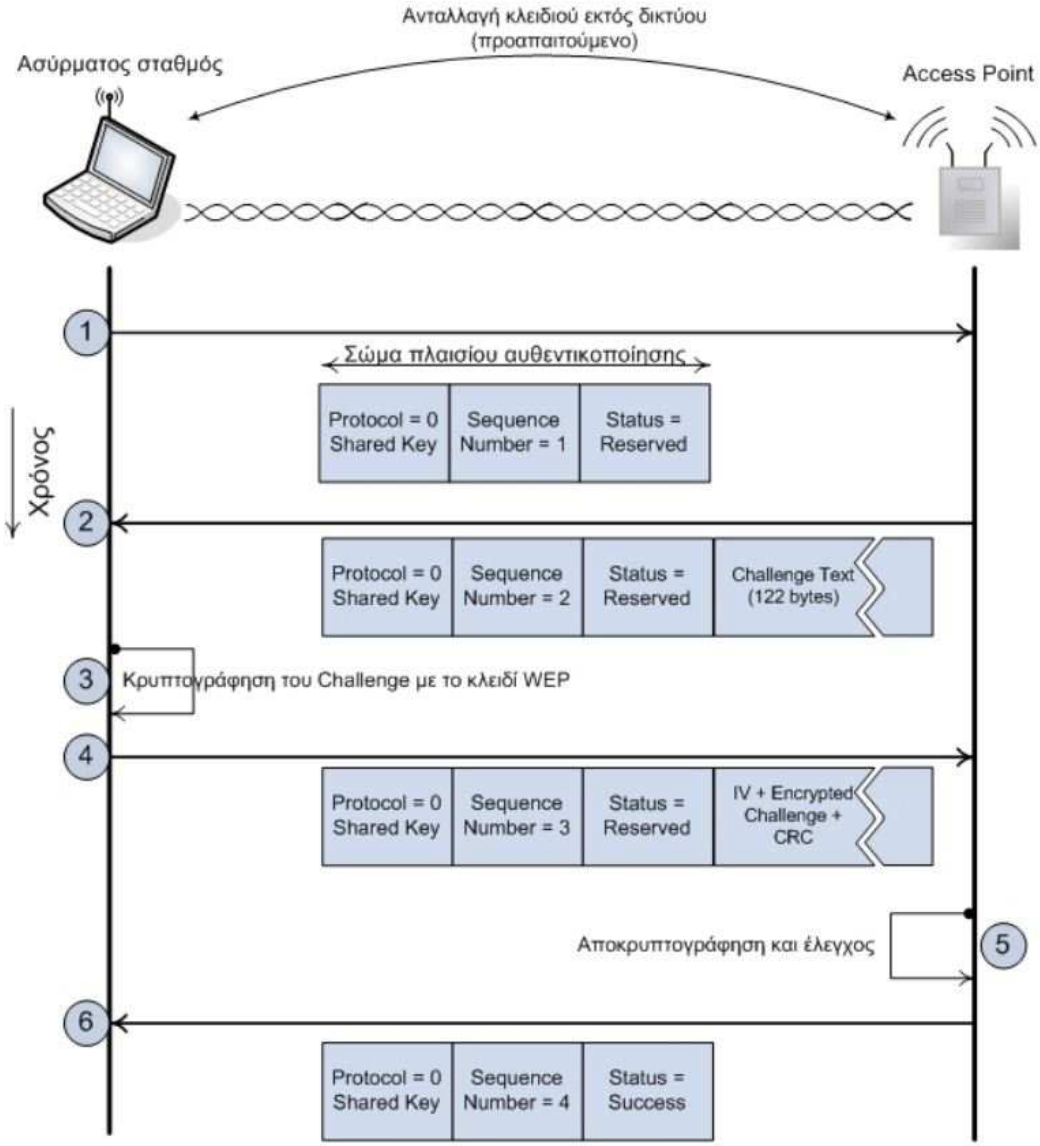
4.3.5 Shared Key Authentication

Η αυθεντικοποίηση διαμοιραζόμενου κλειδιού χρησιμοποιεί τον αλγόριθμο WEP (Wired Equivalent Privacy) και όπως υποδεικνύει το όνομα του, είχε σχεδιαστεί με την προοπτική να εξαλείψει την βασική αδυναμία ασφάλειας των ασυρμάτων δικτύων, που είναι η δυνατότητα οποιουδήποτε σταθμού εντός εμβέλειας να "ακούσει" την κίνηση του δικτύου. Στα ενσύρματα δίκτυα δεν γίνεται διάχυση της πληροφορίας στον χώρο, και έτσι απαιτείται φυσική επαφή με το καλώδιο για να μπορέσει κάποιος εισβολέας να υποκλέψει δεδομένα.

Σε ένα ασύρματο δίκτυο που χρησιμοποιεί WEP, κάθε σταθμός γνωρίζει ένα ή περισσότερα κλειδιά που του επιτρέπουν να αποκωδικοποιεί την κίνηση που δέχεται

και αντίστοιχα να κωδικοποιεί την κίνηση που στέλνει. Υπό αυτήν την έννοια, η αυθεντικοποίηση διαμοιραζόμενου κλειδιού δεν αποδεικνύει την ταυτότητα κάθε σταθμού, αλλά απλά πιστοποιεί ότι οι σταθμοί έχουν στην κατοχή τους το ίδιο κλειδί.

Η αυθεντικοποίηση διαμοιραζόμενου κλειδιού πραγματοποιείται σε έξι βήματα, όπως φαίνεται στο παρακάτω σχήμα:



Εικόνα 125. Αυθεντικοποίηση Διαμοιραζόμενου Κλειδιού

- **Βήμα 1ο:** Ο σταθμός που επιχειρεί να αυθεντικοποιηθεί, στέλνει αίτημα αυθεντικοποίησης στο AP (ή άλλο σταθμό εάν πρόκειται για ad-hoc δίκτυο).

- **Βήμα 2ο:** Το AP απαντάει με μία τυχαία συμβολοσειρά (Challenge Text). Η τυχαία συμβολοσειρά αποσκοπεί στην αποφυγή της επίθεσης Off-line Brute Force.

- **Βήμα 3ο:** Ο σταθμός κρυπτογραφεί την τυχαία συμβολοσειρά με το WEP κλειδί που διαθέτει.

- **Βήμα 4ο:** Ο σταθμός αποστέλλει το κρυπτογραφημένο αποτέλεσμα στο AP.

- **Βήμα 5ο:** Το AP αποκρυπτογραφεί την κρυπτογραφημένη τυχαία συμβολοσειρά με το δικό του WEP κλειδί. Αν η αποκρυπτογραφημένη τυχαία συμβολοσειρά είναι ίδια με την αρχική που είχε αποστείλει, συμπεραίνει ότι τα δύο κλειδιά είναι ίδια.

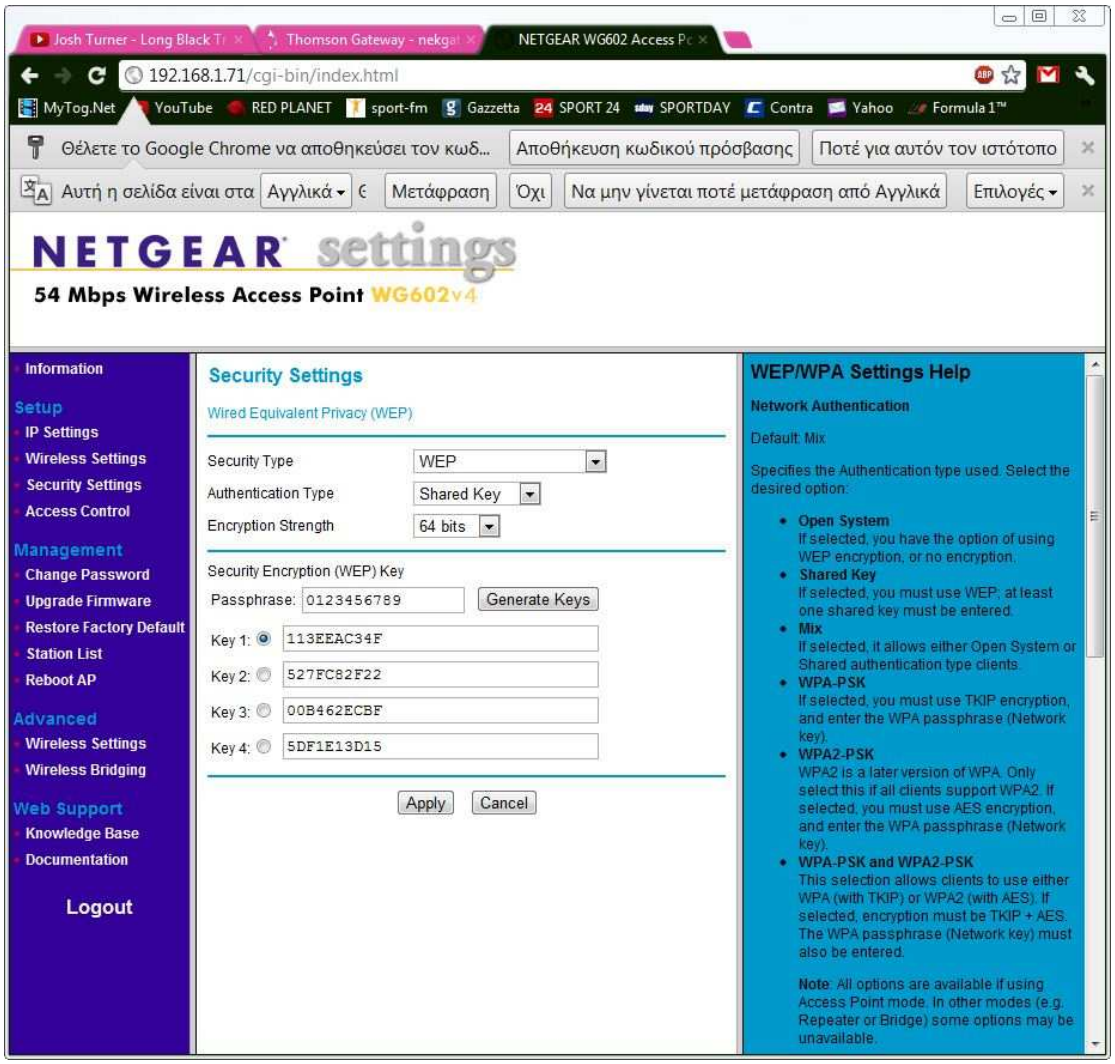
- **Βήμα 6ο:** Αν στο βήμα 5 αποδείχτηκε ότι τα κλειδιά είναι ίδια, τότε το AP αυθεντικοποιεί τον σταθμό.

Η αυθεντικοποίηση διαμοιραζόμενου κλειδιού έχει ένα σύνολο από αδυναμίες:

- Δεν προβλέπεται κάποιος μηχανισμός αυτόματης διαμοίρασης των κλειδιών. Τα κλειδιά επομένως θα πρέπει να διαμοιραστούν εκτός δικτύου και να καταχωρηθούν χειροκίνητα, πράγμα χρονοβόρο και επιρρεπές σε διαρροές και υποκλοπές.
- Δεν προβλέπεται κάποιος μηχανισμός βάσει του οποίου να καθορίζονται οι σταθμοί και τα AP που θα μοιράζονται το ίδιο κλειδί. Αυτό το ζήτημα θα πρέπει να το αντιμετωπίσει ο διαχειριστής του δικτύου, πράγμα όμως που περιορίζει την ευελιξία του δικτύου.
- Η απόκτηση του κλειδιού από έναν σταθμό, επιτρέπει σε έναν εισβολέα πλήρη πρόσβαση στο δίκτυο από οποιοδήποτε άλλο σταθμό.
- Είναι σύνηθες φαινόμενο να επιλέγονται ευκολομνημόνευτα κλειδιά, οπότε αυτό οδηγεί σε ακατάλληλη επιλογή κλειδιών (κοινές λέξεις, ημερομηνίες).
- Ο αλγόριθμος WEP έχει ένα αριθμό από αδυναμίες που τον καθιστούν ανασφαλή. Οι αδυναμίες αυτές θα αναλυθούν παρακάτω.

Σε αυτό την επίθεση σκοπός είναι να πραγματοποιήσετε παράκαμψη της διαμοιρασμένης αυθεντικοποίησης ενός ασύρματου δικτύου και το οποίο είναι λίγο πιο περίπλοκο από τις προηγούμενες επιθέσεις.

Αρχικά θα πρέπει να ρυθμιστούν οι παράμετροι ασφάλειας του access point για τη συγκεκριμένη επίθεση. Αυτό που κάνετε είναι να ενεργοποιήσετε την κρυπτογράφηση WEP του access point και να ορίσετε ένα κλειδί που μοιράζετε στους clients που θέλετε να εξουσιοδοτήσετε να συνδέονται στο ασύρματο δίκτυο.



Εικόνα 126. Ρυθμίσεις access point για shared key WEP encryption

Στην παραπάνω εικόνα φαίνεται το passphrase που ορίστηκε για τη συγκεκριμένη επίθεση και επιλέχθηκε η πρώτη έκδοση της δεκαεξαδικής κωδικοποίησής του. Επίσης, επιλέχθηκε ο τύπος αυθεντικοποίησης σε Shared Key και η δύναμη του κωδικού σε 64bit. Είναι σημαντικό για την επίδειξη της επίθεσης αυτής να απενεργοποιήσετε οποιοδήποτε άλλο είδος ασφάλειας του ασύρματου δικτύου.

Μπορείτε να επαληθεύσετε τη σωστή λειτουργία των ρυθμίσεων συνδέοντας ένα client ο οποίος γνωρίζει το WEP key για να δείτε αν συνδεθεί σωστά.

Στο επόμενο στάδιο της επίθεσης θα πρέπει να κάνετε sniffing πακέτων μεταξύ access point και client και θα ανοίξετε το wireshark για να τα κάνει capture στο background και η ασύρματη κάρτα λειτουργίας είναι σε monitor mode.

Πρώτη εντολή που δίνετε είναι η

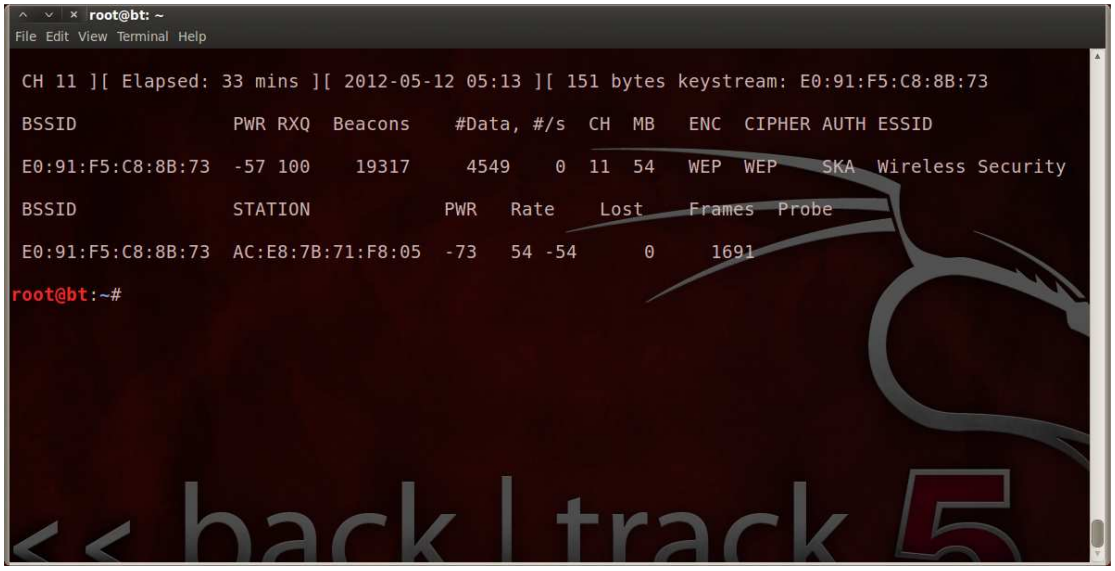
- **airodump-ng –c (channel access point στόχου) –bssid (mac address access point στόχου) mon0 –w keystream**

  Με την παράμετρο –w ορίζουμε το όνομα ενός αρχείου (στη συγκεκριμένη περίπτωση keystream) στο οποίο αποθηκεύονται τα πακέτα της κίνησης.

Εικόνα 127. Κίνηση client και access point στόχο

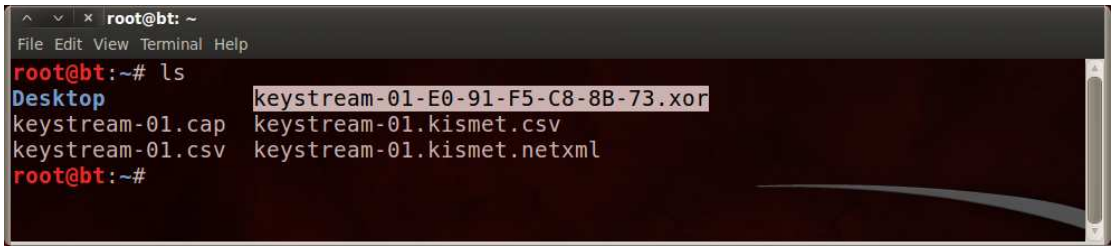
Στην παραπάνω εικόνα παρατηρείτε την στήλη AUTH στην οποία η ένδειξη είναι κενή.

Το μόνο που χρειάζεται τώρα είναι να περιμένετε να συνδεθεί κάποιος client στο ασύρματο δίκτυο. Εναλλακτικά μπορείτε να προκαλέσετε το deauthentication κάποιου client μόνο και μόνο για να επανασυνδεθεί στο δίκτυο. Όταν λοιπόν ο εξουσιοδοτημένος client συνδεθεί στο δίκτυο το airodump-ng θα συλλάβει όλη την κίνηση που αφοράει την διαδικασία για το authentication και θα την καταγράψει. Όταν γίνει το authentication, στην οθόνη του airodump-ng και συγκεκριμένα στη στήλη AUTH θα εμφανιστεί η ένδειξη SKA (Shared Key Authenication).



Εικόνα 128. Η ένδειξη SKA μόλις συνδέθηκε ο client στο WLAN

Θα παρατηρήσετε επίσης ότι επάνω δεξιά εμφανίζεται η ένδειξη keystream με τη MAC address του access point στόχου. Επίσης, το keystream που έγινε capture αποθηκεύεται σε αρχείο .xor μεγέθους 151bytes.



Εικόνα 129. Το αρχείο xor με το κλειδί WEP

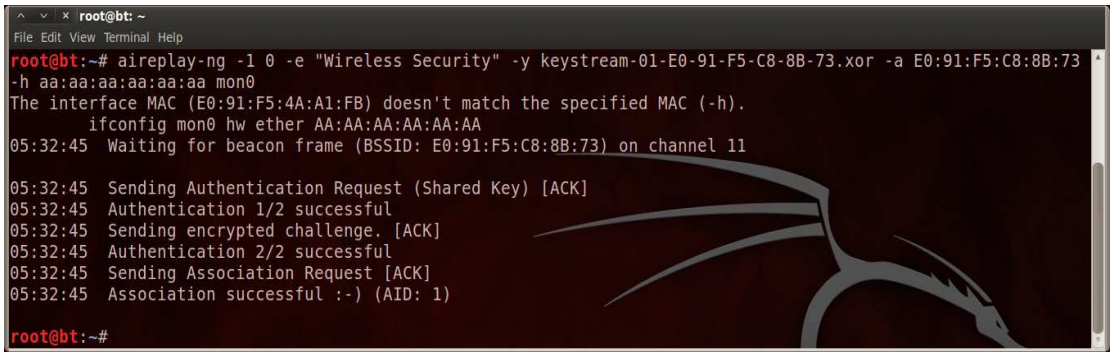
Σκοπός τώρα είναι να περάσετε στο access point μια ψεύτικη MAC address της ασύρματης κάρτας δικτύου που χρησιμοποιείτε μαζί με το αρχείο xor το οποίο

περιέχει τον κωδικό SKA, ώστε να της επιτραπεί από το access point να συνδεθεί. Η εντολή για το σκοπό αυτό είναι:

- **aireplay-ng -1 0 –e "όνομα WLAN" –y keystream-01-E0-91-F5-C8-8B-73.xor –a E0:91:F5:C8:8B:73 –h aa:aa:aa:aa:aa:aa mon0**
  - όπου keystream-01-E0-91-F5-C8-8B-73.xor το όνομα αρχείου xor που θα δημιουργηθεί στον υπολογιστή σας
  - E0:91:F5:C8:8B:73 η MAC του access point στο οποίο γίνεται επίθεση
  - aa:aa:aa:aa:aa:aa η fake MAC που θα τη χρησιμοποιήσετε στην ασύρματη κάρτα δικτύου σας και την οποία ενημερώνετε το access point ότι θα την κάνει δεκτή.

Εικόνα 130. Εντολή για καταχώρηση fake MAC στο access point

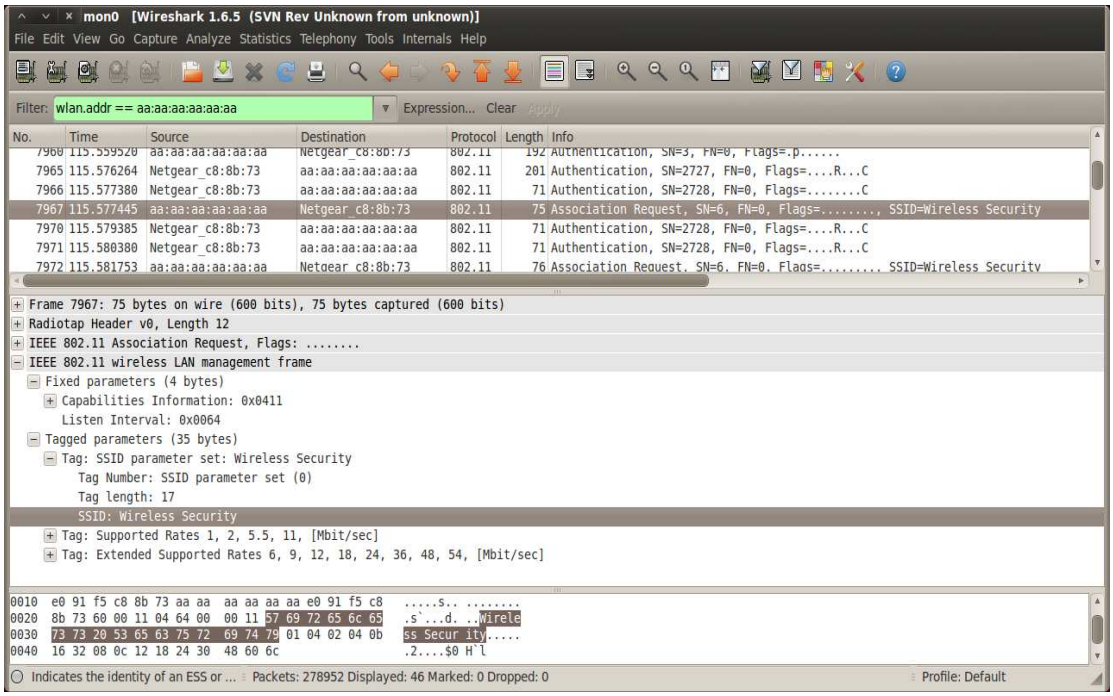
Και το αποτέλεσμα επιβεβαίωσης της σύνδεσης φαίνεται στην παρακάτω εικόνα μετά την εντολή



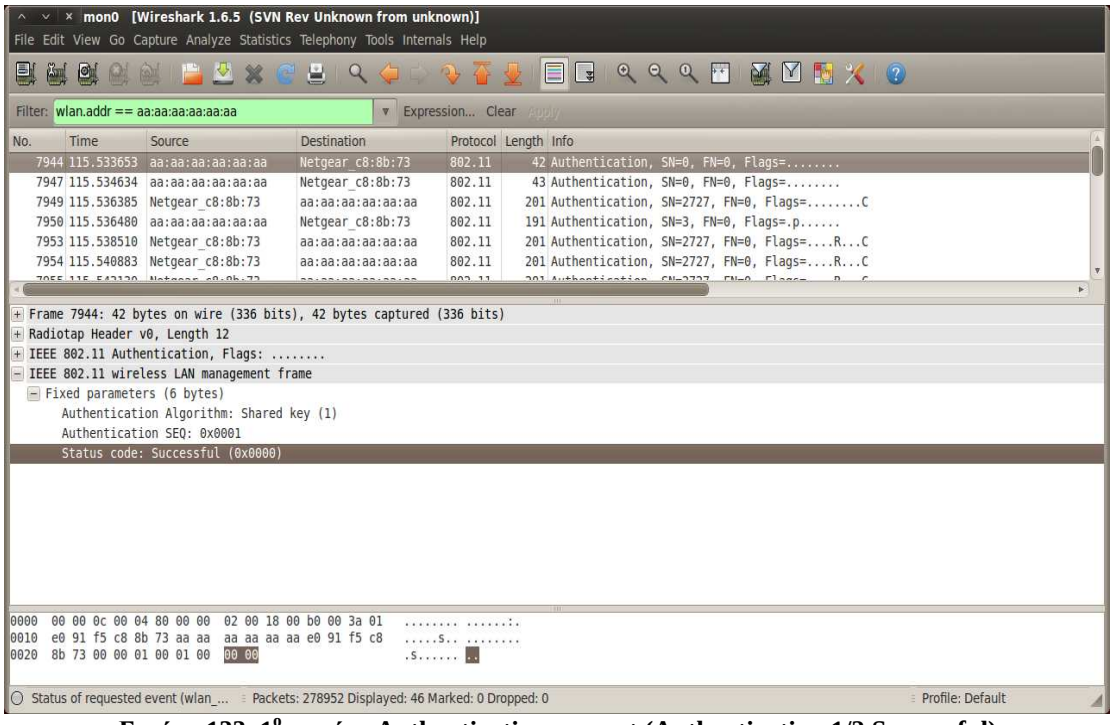
Εικόνα 131. Επιβεβαίωση wireless card με fake MAC στο AP στόχο

Με την ένδειξη association successful επιβεβαιώνεται η σύνδεση.

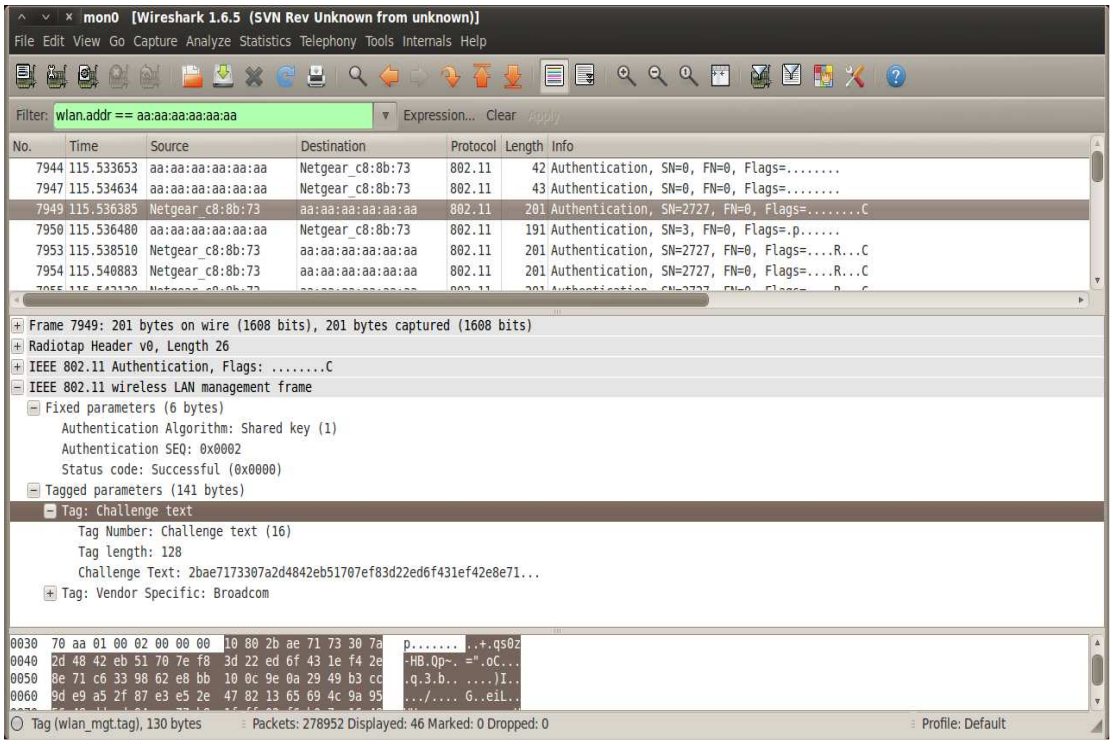
Την επιτυχή σύνδεση μπορούμε να την επιβεβαιώσουμε και από την κίνηση που πιάνει το wireshark.



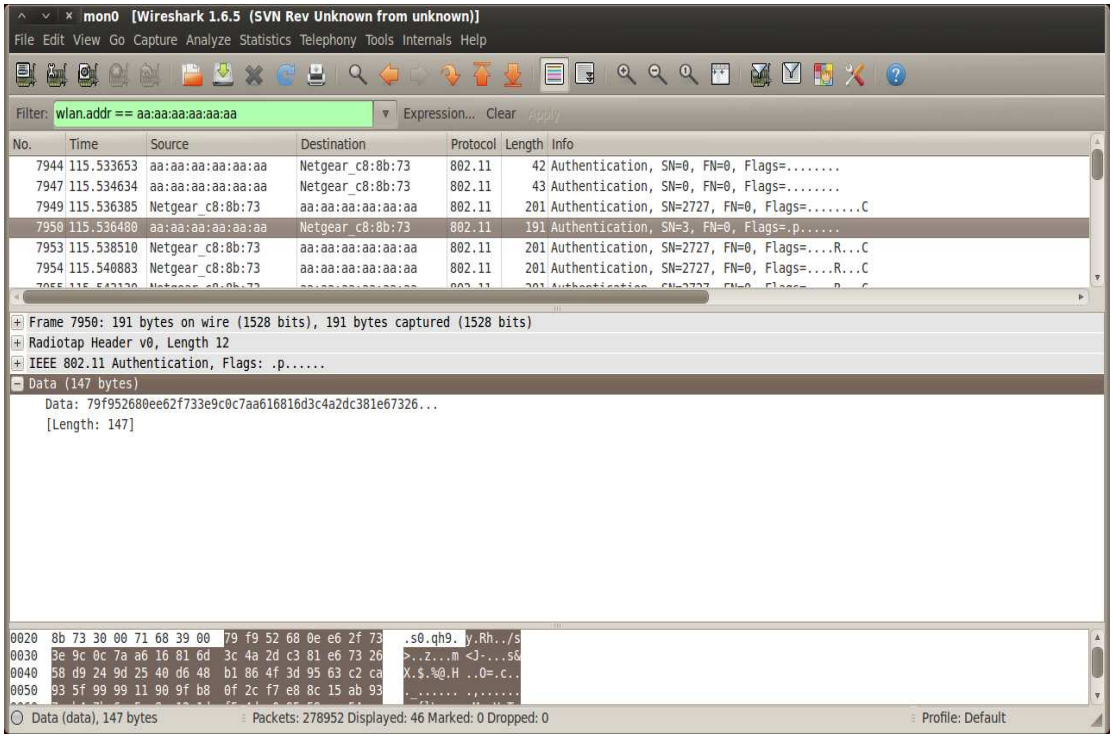
Εικόνα 132. Association request από τη wireless LAN card που έχει fake MAC στο AP στόχο



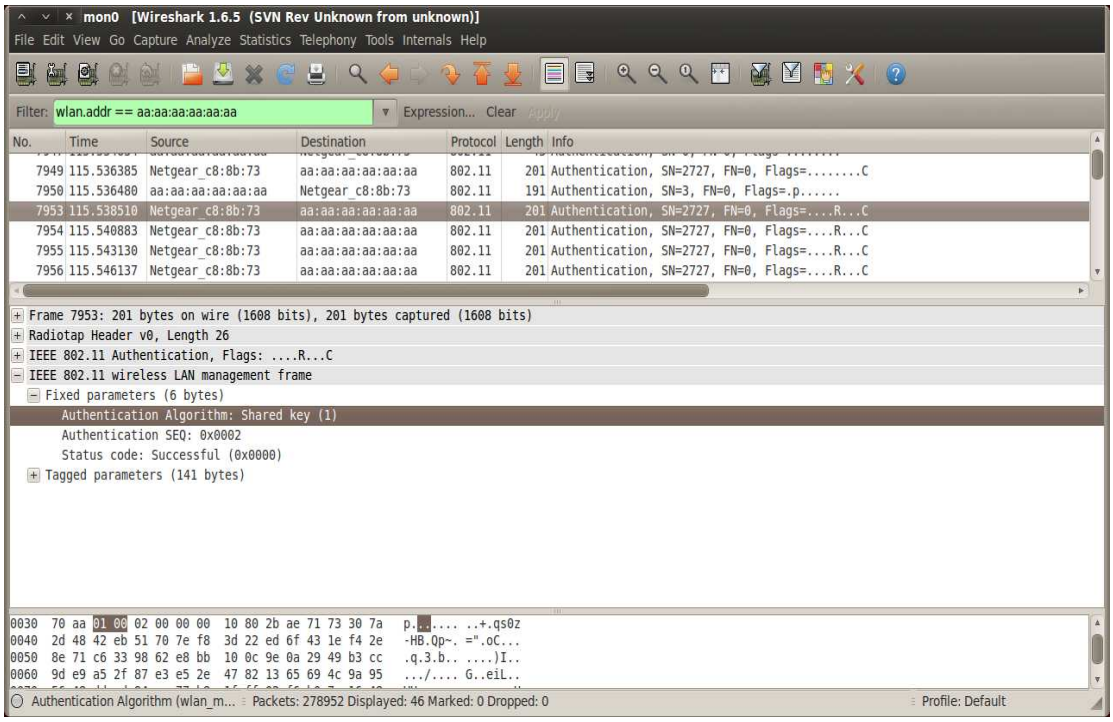
Εικόνα 133. 1ο πακέτο Authentication request (Authentication 1/2 Successful)



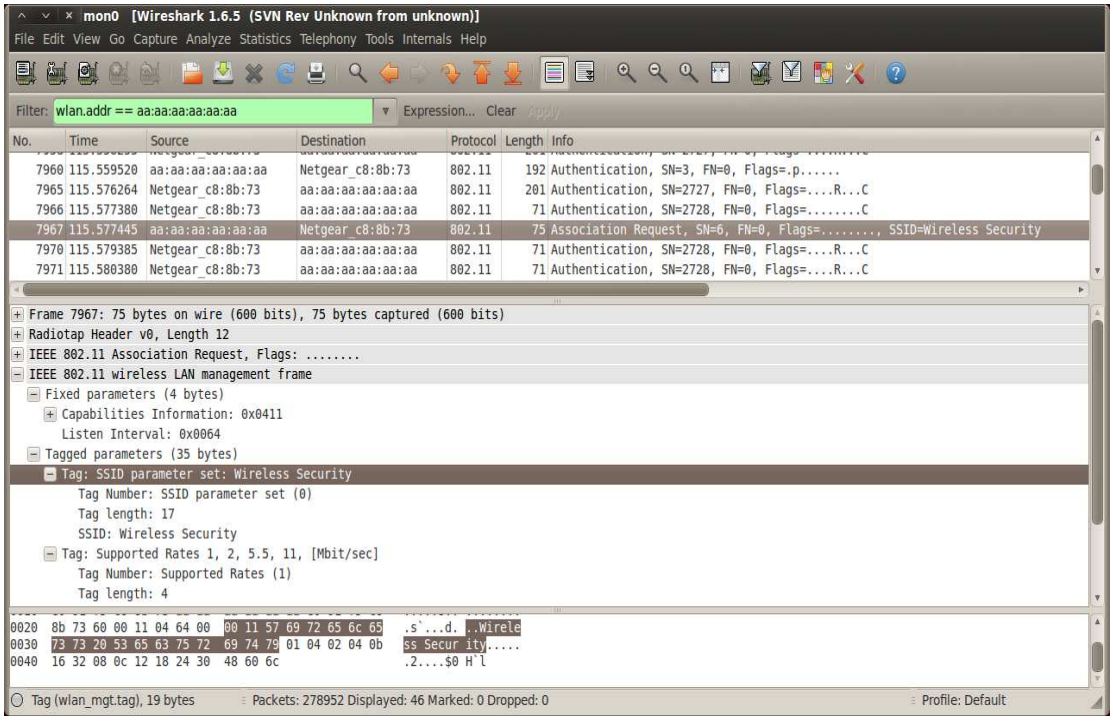
Εικόνα 134. Το challenge text του AP στη wireless LAN card



Εικόνα 135. Το aireplay-ng *απαντάει* στο challengge text του AP



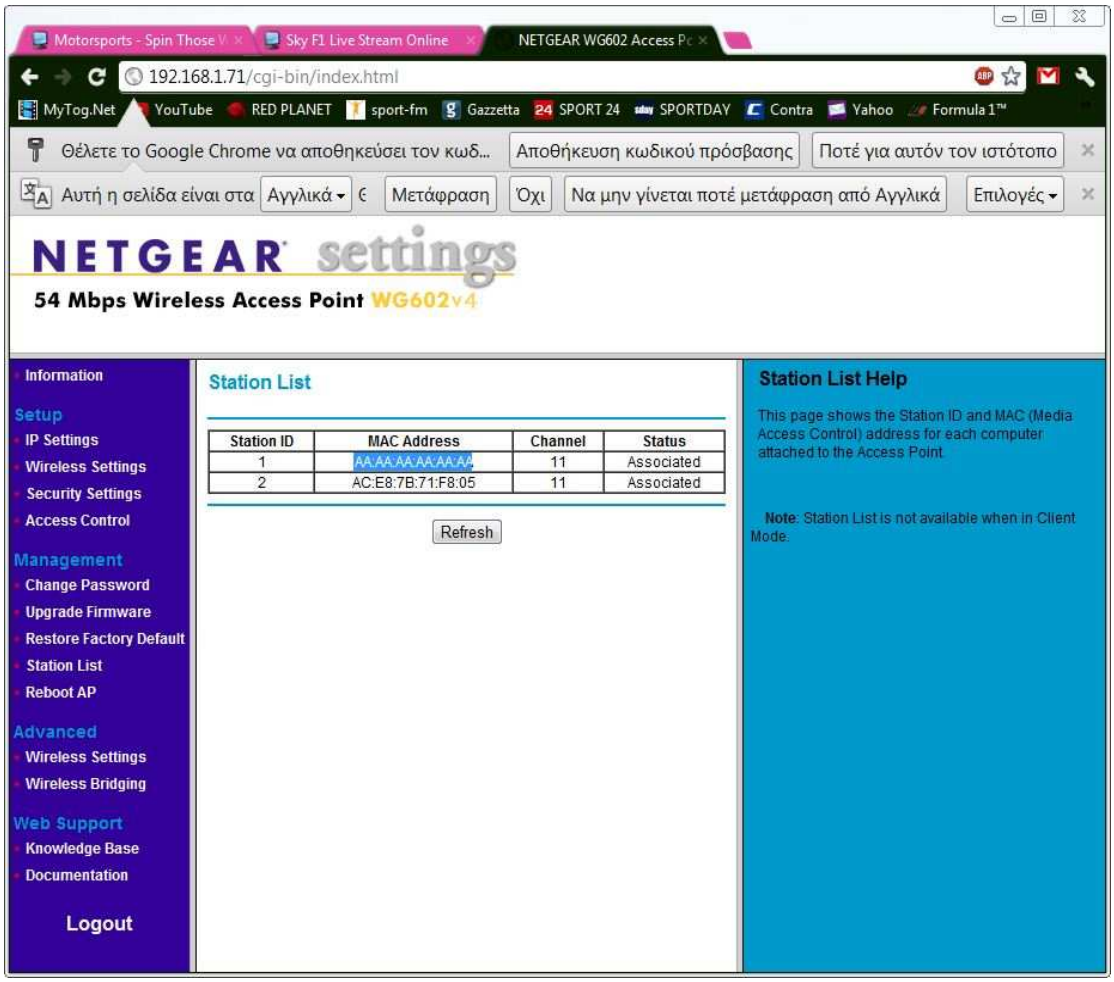
Εικόνα 136. Η δεύτερη αυθεντικοποίηση με το αρχείο keystream (Authentication 2/2 Successful)



Εικόνα 137. Association Request από το aireplay-ng

Στην παραπάνω εικόνα φαίνεται ότι ξεκινάει και τελειώνει η διαδικασία για association μεταξύ κάρτας και access point με τη χρήση του aireplay-ng.

Στην επόμενη εικόνα φαίνεται στη λίστα των wireless clients που έχουν συνδεθεί με το access point. Βλέπετε ότι έχει συνδεθεί η wlan card με τη fake address.



Εικόνα 138. Λιστα associated clients με το AP στόχο

Αυτό που πετύχατε με τη συγκεκριμένη επίθεση είναι η σύνδεση μέσω WEP Shared Key χωρίς να το γνωρίζετε, κάτι που αποδεικνύει άλλη μια αδυναμία της WEP κρυπτογράφησης.

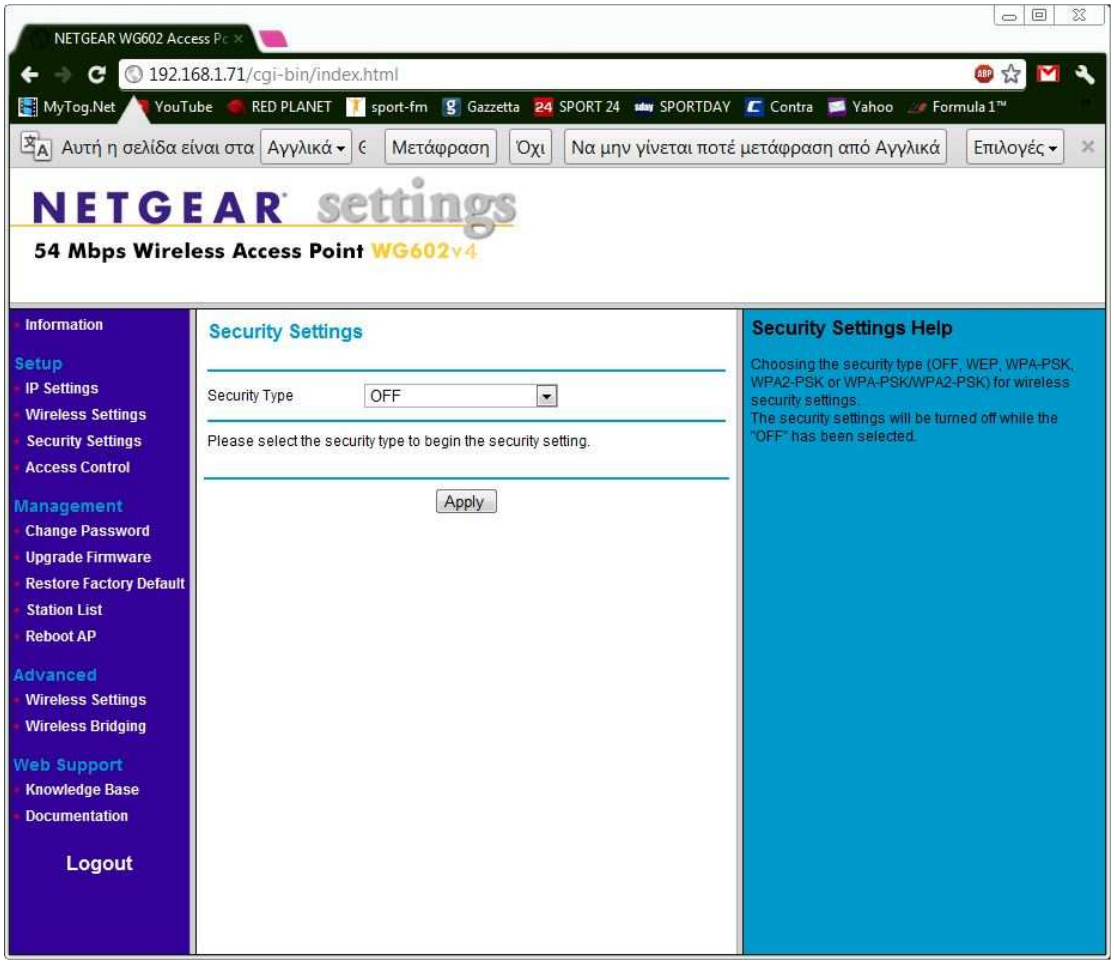
5. Επιθέσεις στην υποδομή των Wireless LANs

Η υποδομή των WLANs είναι αυτή που παρέχει όλες τις υπηρεσίες σε όλους τους clients του δικτύου. Αυτή μπορεί να περιλαμβάνει access points, wireless routers, servers, εκτυπωτές κλπ τα οποία όλα διασυνδέονται μεταξύ τους μέσω ενός κεντρικού ενσύρματου δικτύου ως κεντρική αρτηρία μετάδοσης δεδομένων backbone bus. Στο παρόν κεφάλαιο θα παρουσιαστούν κάποιες επιθέσεις στην υποδομή των WLANs

5.1 Επιθέσεις άρνησης υπηρεσιών (Denial of service attacks)

Η denial-of-service attack (DoS attack) ή η κατανεμημένη denial-of-service attack (DDoS attack) είναι ένα είδος επίθεσης προκειμένου ένας υπολογιστής ή ένα δίκτυο να καταστεί μη διαθέσιμο στους χρήστες του. Τα ασύρματα δίκτυα επειδή χρησιμοποιούν τη διάδοση των ραδιοκυμάτων είναι περισσότερο ευπαθή σε DoS attacks.

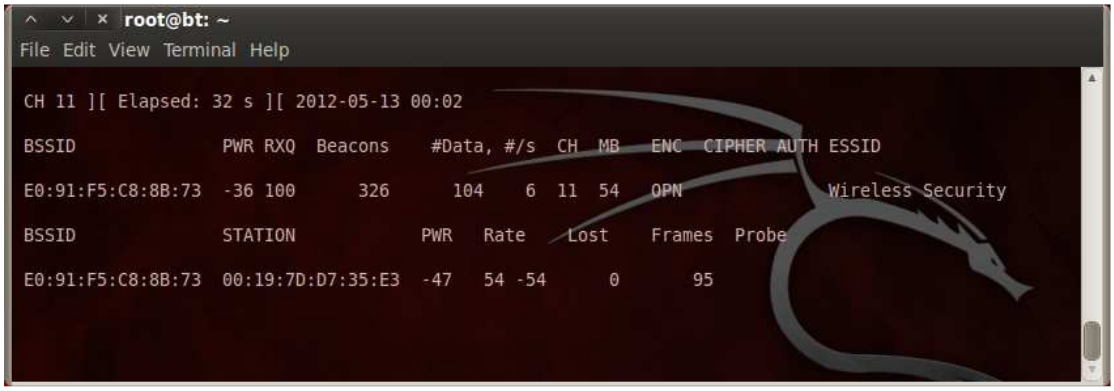
Για τη συγκεκριμένη επίθεση θα πρέπει να αφήσετε χωρίς προστασία το access point και χωρίς κρυπτογράφηση



Εικόνα 139. Κλείσιμο ασφάλειας access point

Ξεκινήστε την καταγραφή κίνησης με την κάρτα σε monitor mode, ανοικτό το wireshark και συνδεθείτε με κάποιο client στο ασύρματο δίκτυο. Με τη χρήση του

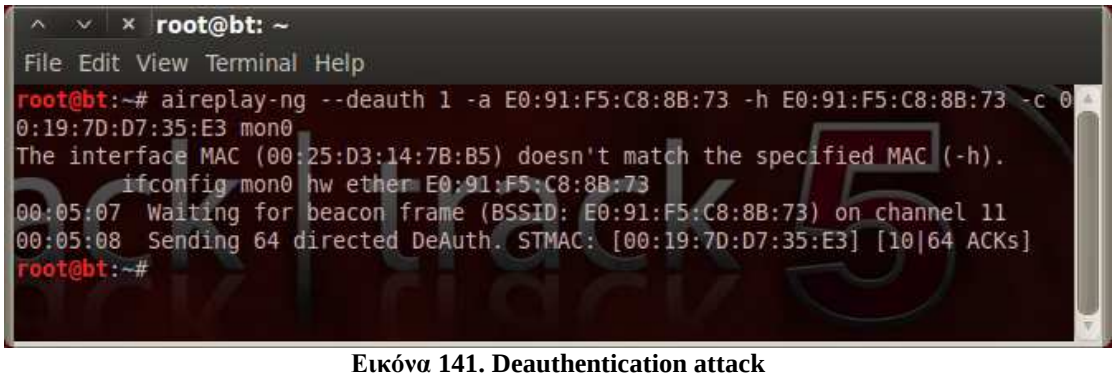
εργαλείου airodump-ng θα δείτε τη σύνδεση αυτή στην οθόνη.



Εικόνα 140. WLAN και connected client

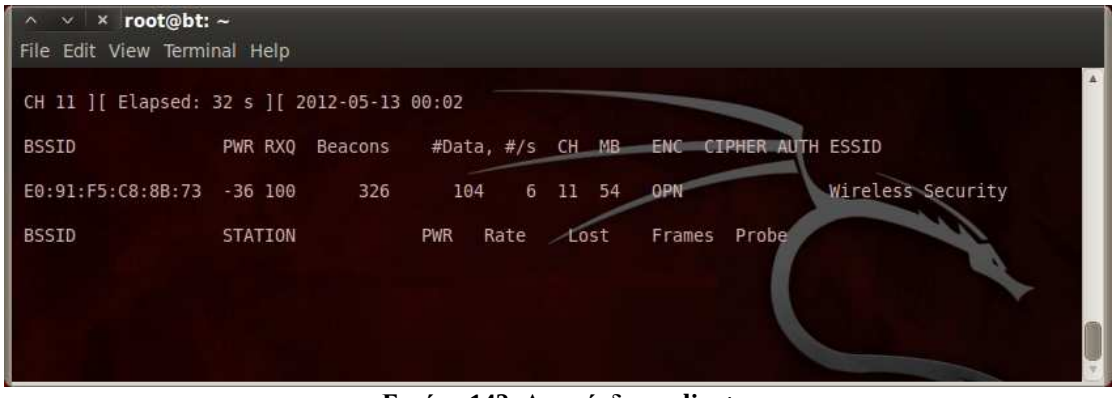
Με το εργαλείο aireplay-ng μπορείτε να προκαλέσετε την αποσύνδεση συγκεκριμένου client στέλνοντας deauthentication packets προσποιούμενοι το AP στον client με την εντολή

- **aireplay-ng --deauth 1 –a (mac address AP) –h (mac address AP) –c (mac address target client) mon0**
  - όπου με το –h παρουσιάζεται ο αποστολέας των deauthentication packets (η WLAN card σας) ως το AP.



Εικόνα 141. Deauthentication attack

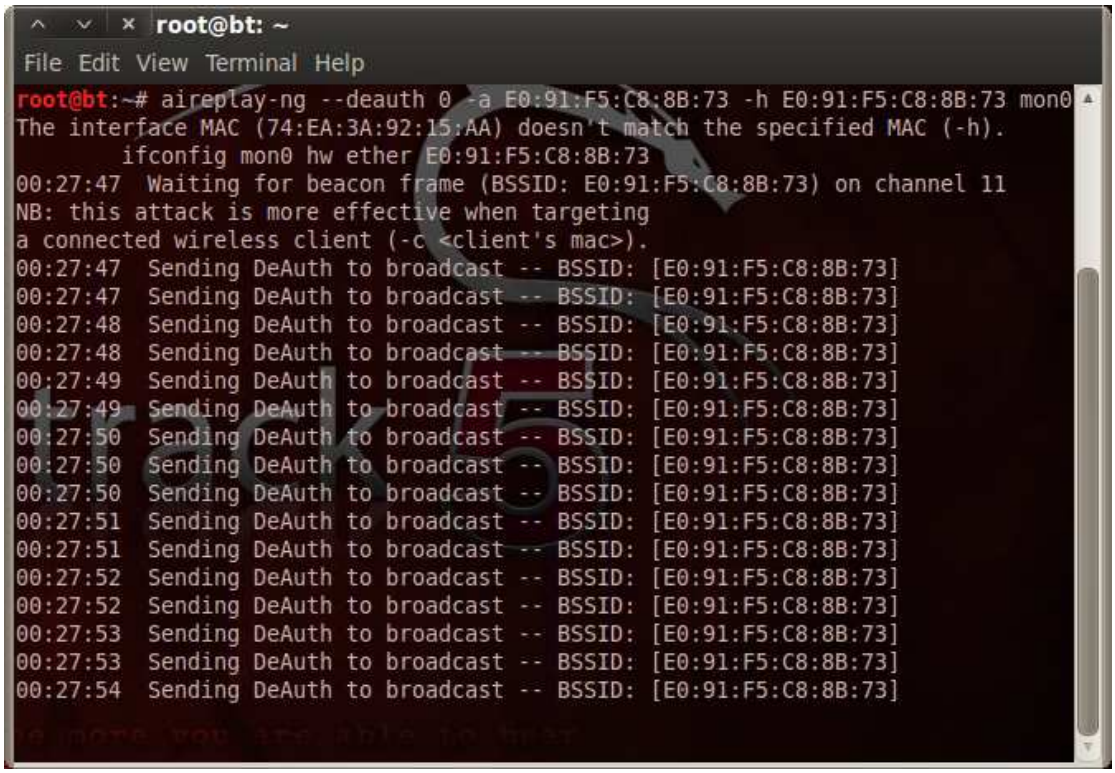
Το αποτέλεσμα είναι η αποσύνδεση του client



Εικόνα 142. Αποσύνδεση client

Αν κοιτάξετε στο wireshark θα δείτε τα deauthentication packets μεταξύ AP και wlan card. Η ίδια επίθεση μπορεί να γίνει με τη συνεχή εκπομπή Deauthentication

packets σε όλους τους clients του ασύρματου δικτύου προσποιούμενοι ότι τα στέλνει το AP αφού μιμείστε τη MAC address του με την παράμετρο -h.



Εικόνα 143. Μαζική εκπομπή deauthentication packets

5.2 Evil Twin και access point MAC spoofing

Μια από τις πιθανές επιθέσεις στην υποδομή είναι αυτή που ονομάζεται Evil Twin. Η λογική της επίθεσης αυτής είναι απλή. Ο επιτιθέμενος χρησιμοποιεί ένα access point στο οποίο έχει κάνει MAC spoofing την MAC address ενός access point, το οποίο χρησιμοποιεί το ασύρματο δίκτυο στο οποίο γίνεται η επίθεση. Δηλαδή ουσιαστικά ντουμπλάρεται ένα access point. Η διαφορά είναι ότι το access point με τη fake MAC address το διαχειρίζεται ο επιτιθέμενος με ό,τι μπορεί να σημαίνει αυτό για τους χρήστες του ασύρματου δικτύου.

Με το είδος αυτός της επίθεσης οι χρήστες μπορούν να συνδεθούν τυχαία στο fake access point και ο επιτιθέμενος να εξαπολύσει επιθέσεις τύπου Man In The Middle και να υποκλέψει την κίνηση. Ένα access point με ψεύτικη MAC address είναι πιο δύσκολο να εντοπιστεί και να αποτραπεί η λειτουργία του.

Με την WLAN card σε monitor mode και την εντολή

- **airodump-ng mon0**

μπορείτε να εντοπίσετε τα διαθέσιμα access points

Εικόνα 144. Λίστα πιθανών APs για επίθεση evil twin

Στην παραπάνω εικόνα εκτός από τη λίστα των διαθέσιμων access point παρατηρείτε και κάποιους clients συνδεδεμένους σε κάποια από αυτά. Από αυτή τη λίστα επιλέγετε το access point στόχο για evil twin attack.

Αρχικά για το σκοπό της επίθεσης αυτής θα δημιουργηθεί ένα access point με το ίδιο ESSID μόνο, δηλαδή το ίδιο όνομα και διαφορετικό BSSID, με την εντολή

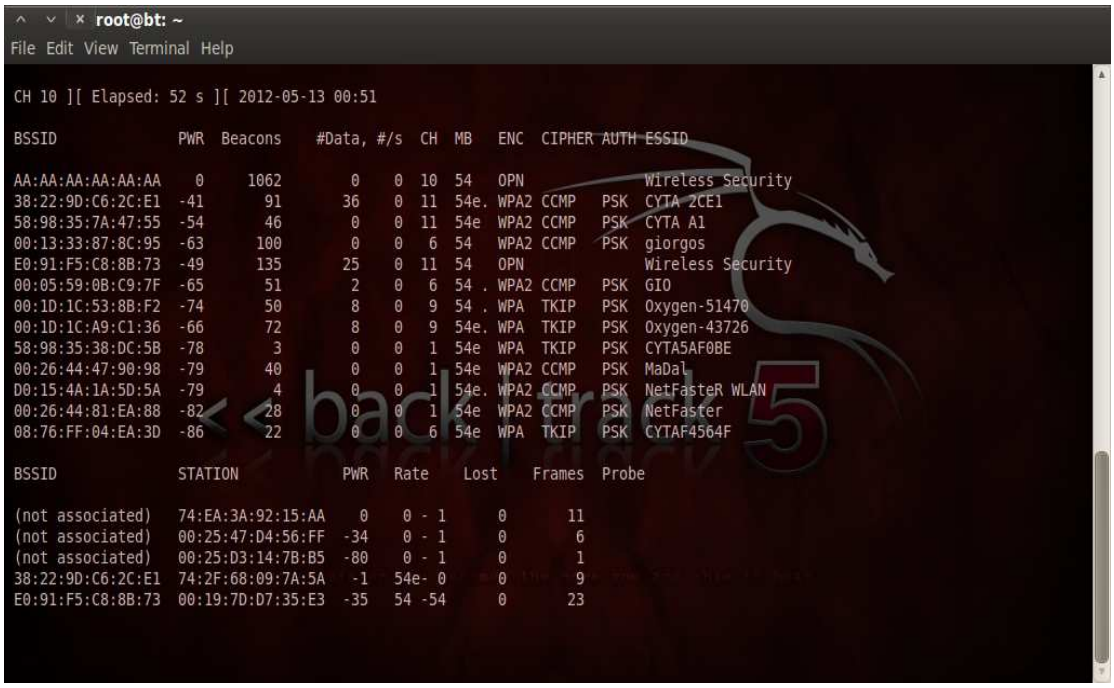
- **airebase-ng –a (MAC address που θέλετε να φαίνεται) --essid "όνομα essid που θα αντιγράψετε" –c (κανάλι λειτουργίας) mon0**
    - το κανάλι λειτουργίας επιλέγεται με βάση το κανάλι που λειτουργίας του access point στόχου.

Εικόνα 145. Δημιουργία εικονικού access point

Ουσιαστικά με την παραπάνω εντολή η ασύρματη κάρτα που χρησιμοποιείτε μετατρέπεται σε access point. Αυτό μπορεί να φανεί και από την εντολή σε νέο παράθυρο terminal

- **airodump-ng mon0**

όπου θα πάρετε την παρακάτω εικόνα.

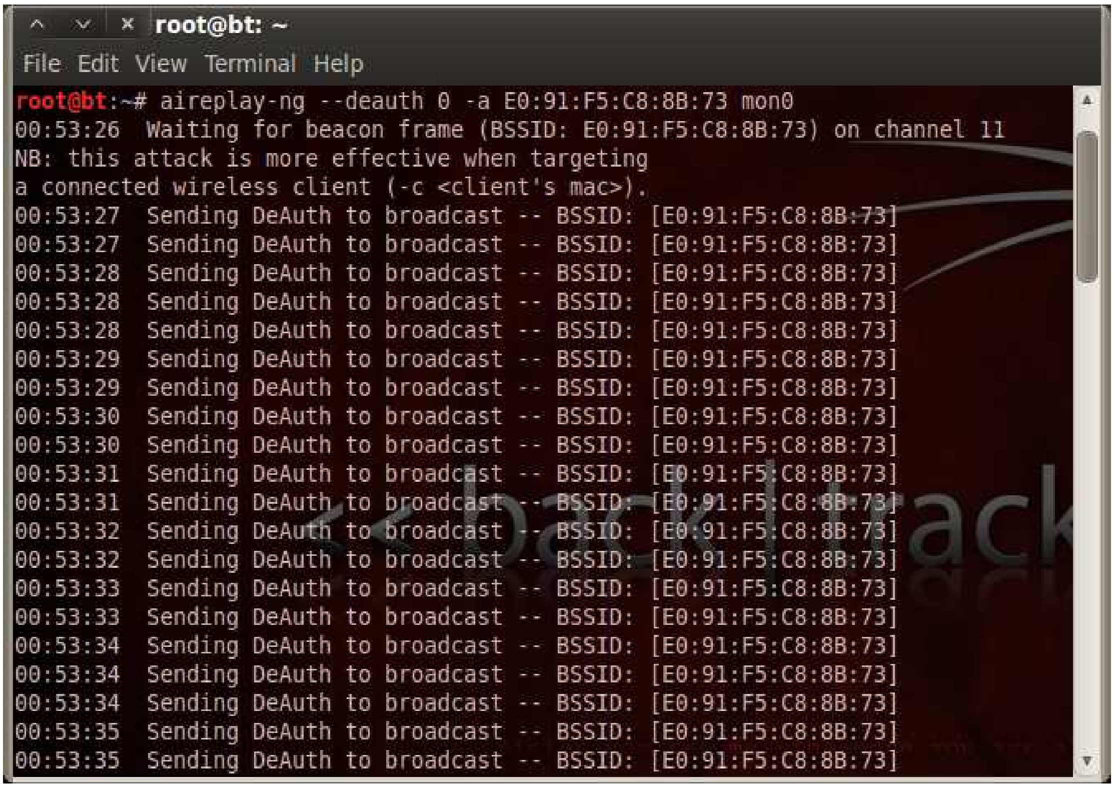


Εικόνα 146. Το fake AP μαζί με τα υπόλοιπα

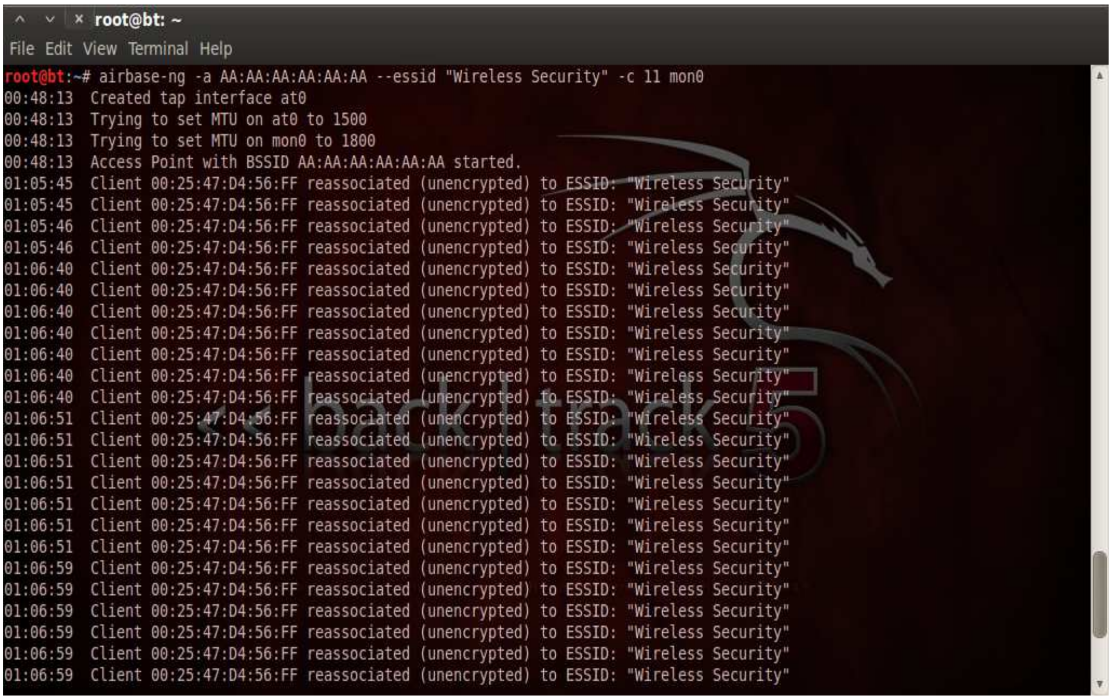
Στην παραπάνω εικόνα φαίνονται δύο APs με το ίδιο ESSID και προφανώς και αυτό που έχει το BSSID που ορίσαμε είναι το fake access point. Είναι και τα δύο με την ένδειξη OPN δηλαδή χωρίς κρυπτογράφηση.

Επόμενη κίνηση είναι να προκαλέσετε την αποσύνδεση των clients που είναι συνδεδεμένοι στο κανονικό AP προκειμένου να εξαναγκαστούν σε **πιθανή** επανασύνδεση με το fake AP. Για το λόγο αυτό μπορείτε να χρησιμοποιήσετε την εντολή

- **aireplay-ng --deauth 0 –a mon0**



Εικόνα 147. Deauthentication επίθεση σε συγκεκριμένο AP



Εικόνα 148. Σύνδεση client στο fake AP

Στην παραπάνω εικόνα που είναι σε συνέχεια της εικόνας 145 όπου φαίνεται η ενεργοποίηση του fake AP, φαίνεται η σύνδεση ενός client με τη MAC address 00:25:47:D4:56:FF με την ένδειξη reassociated.

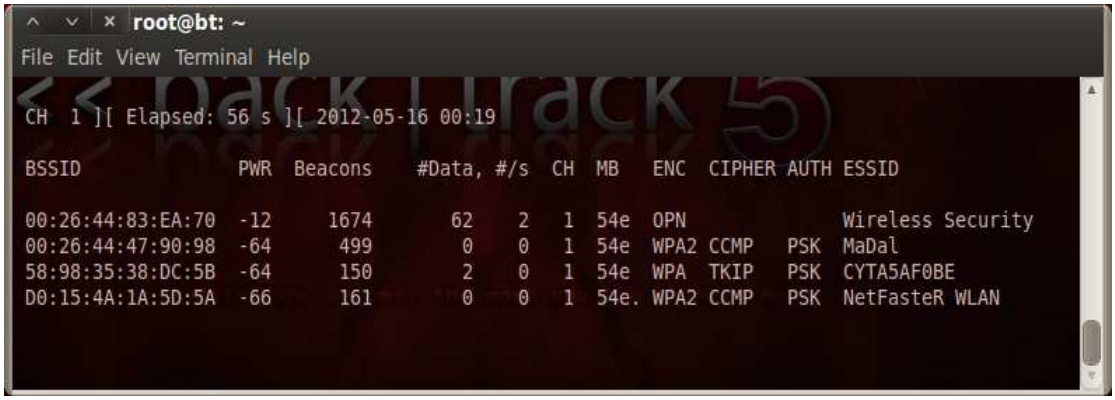
Εδώ θα πρέπει να σημειωθεί ότι η επανασύνδεση όλων των clients στο fake access points δεν είναι σίγουρη δεδομένου ότι έχει σημασία στην αυτόματη επιλογή του access point από τον client και η ένταση του σήματος. Όσο πιο δυνατό είναι το

σήμα του fake access point τόσο πιο πιθανό είναι να συνδεθούν clients σε αυτό.

Το ίδιο πράγμα μπορείτε να το κάνετε χρησιμοποιώντας το εργαλείο airbase-ng αυτή τη φορά όμως βάζοντας στο πεδίο bssid τη MAC address που θέλετε να κάνετε να εκπέμπει η ασύρματη κάρτα δικτύου.

Εικόνα 149. MAC spoofing access point

Με το εργαλείο airodump-ng εμφανίζεται η λίστα των access points και μάλιστα ούτε το airodump-ng μπορεί να ξεχωρίσει το αυθεντικό από το εικονικό.



Εικόνα 150. Το fake access point δεν εντοπίζεται από το airodump-ng

Η επίθεση evil twin access point που περιγράφηκε πιο πάνω, πραγματοποιήθηκε σε ξεκλείδωτο access point. Αν πραγματοποιηθεί σε access point με κωδικοποίηση WEP/WPA θα είναι πιο δύσκολη να ολοκληρωθεί δεδομένου ότι θα εμφανίζονται δύο access point. Ένα κλειδωμένο και ένα ξεκλείδωτο και αυτό ίσως γίνει αντιληπτό, οπότε μπορεί να μειωθεί η πιθανότητα υποκλοπής δεδομένων.

5.3 Man In The Middle Attack (MITM) και υποκλοπή δεδομένων

Man-in-the-middle επίθεση (MITM)[26] είναι μια κοινή παραβίαση ασφάλειας. Ο επιτιθέμενος παρεμποδίζει μια νόμιμη επικοινωνία μεταξύ δύο μερών, τα οποία είναι φιλικά μεταξύ τους. Στη συνέχεια, ο κακόβουλος host ελέγχει τη ροή επικοινωνίας και μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες

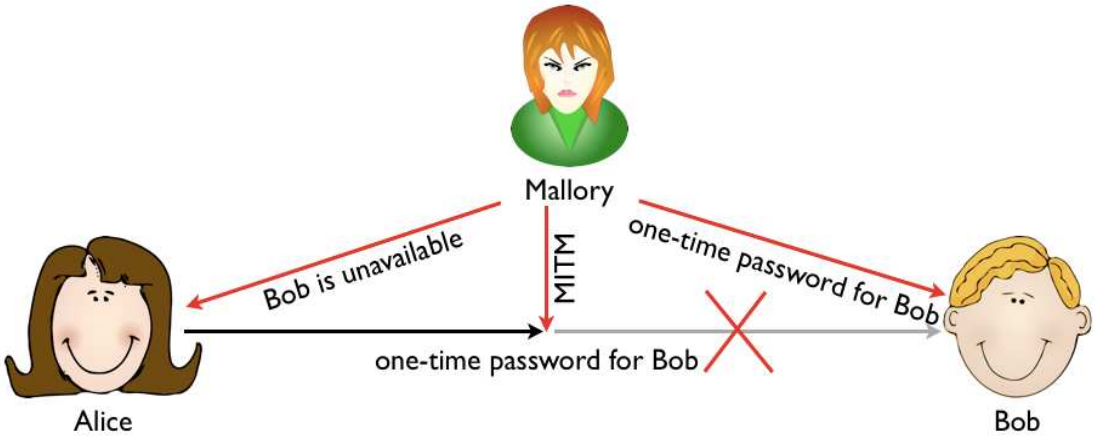
Οι man-in-the-middle επιθέσεις έχουν δύο κοινές μορφές:

[26] http://el.wikipedia.org/wiki/Man-in-the-middle_επίθεση

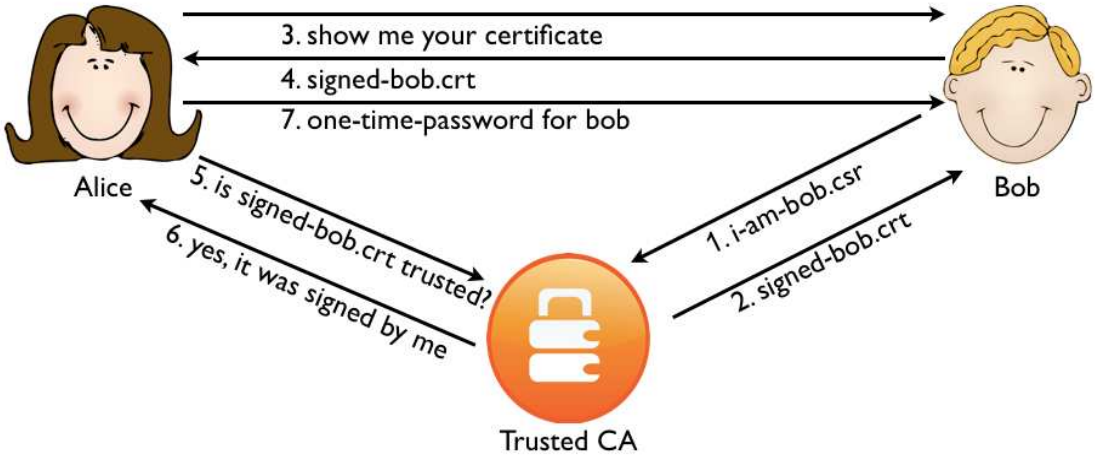
- ο επιτιθέμενος είτε κρυφακούει (eavesdropping)
- είτε και αλλοιώνει κατάλληλα το μήνυμα

Με eavesdropping (κρυφακοή), ένας επιτιθέμενος ακούει απλά ένα σύνολο μεταδόσεων σε και από διαφορετικούς hosts ακόμα κι αν ο υπολογιστής του επιτιθέμενου δεν είναι συμβαλλόμενο μέρος στη συνδιάλεξη. Πολλοί σχετίζουν αυτόν τον τύπο επίθεσης με διαρροή, κατά την οποία ευαίσθητες πληροφορίες μπορούν να αποκαλυφθούν σε έναν τρίτο, χωρίς αυτό να είναι εν γνώση των νόμιμων χρηστών.

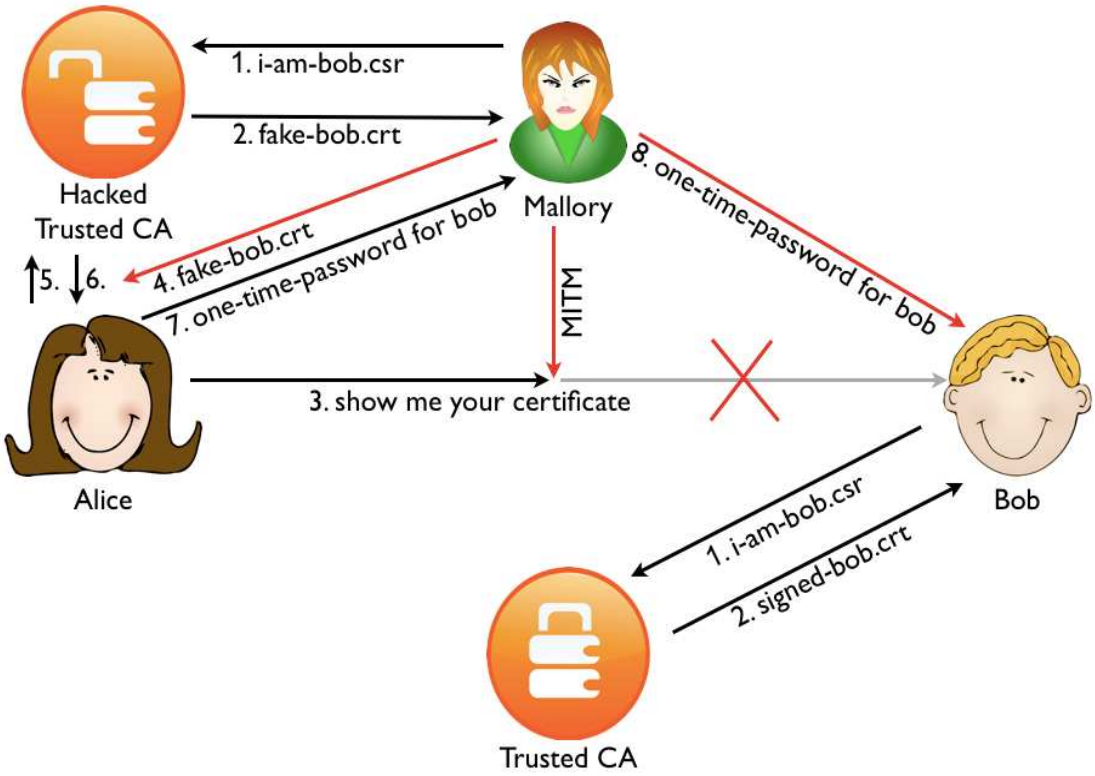
Οι επιθέσεις κατά τις οποίες προκαλείται αλλοίωση του μηνύματος βασίζονται στην ικανότητα του επιτιθέμενου να κρυφακούει. Ο επιτιθέμενος παίρνει αυτή την μη εξουσιοδοτημένη απόκριση, ένα ρεύμα δεδομένων (data stream), αλλάζοντας τα περιεχόμενα ώστε να ικανοποιούν έναν ορισμένο σκοπό - πιθανόν χρησιμοποιώντας ψευδή διεύθυνση IP, αλλάζοντας την διεύθυνση MAC για να μιμηθεί κάποιο άλλο host ή κάνοντας κάποια άλλη τροποποίηση.



Εικόνα 151. Η απλοϊκή προσέγγιση της MITM επίθεσης όπου η Mallory αποκτάει τους κωδικούς της Alice



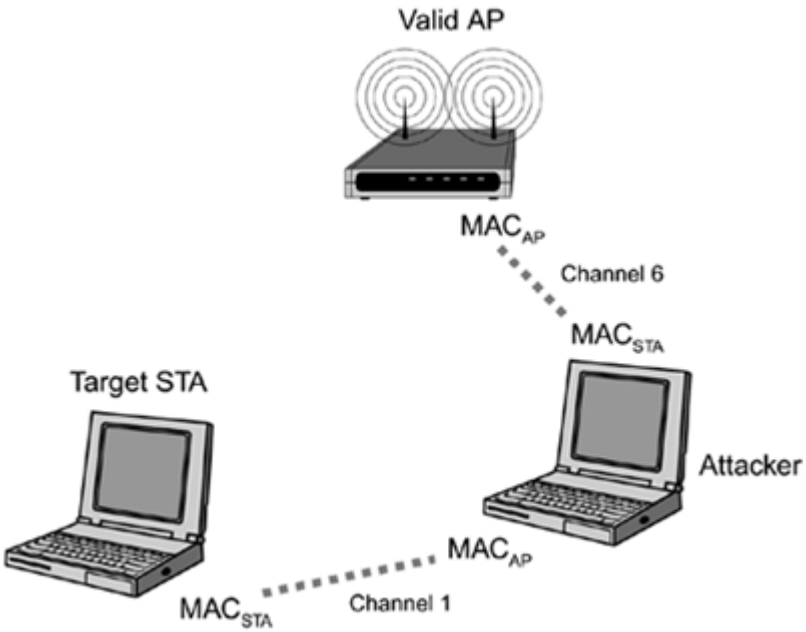
Εικόνα 152. Πιστοποίηση συνομιλίας Alice και Bob με trust certificate



Εικόνα 153. MITM attack με fake trust certificate

Οι επιθέσεις Man In The Middle είναι από τις πιο πιθανές που μπορούν να συμβούν σε ένα ασύρματο δίκτυο και με πολλούς πιθανούς τρόπους. Παρακάτω θα δειχθεί ο πιο απλός τρόπος στησίματος τέτοιας επίθεσης, ο οποίος ουσιαστικά αποτελεί μετεξέλιξη του evil twin είναι να δημιουργηθεί ένα software access point με μια ασύρματη κάρτα δικτύου, το οποίο θα εκπέμπει ένα SSID παρόμοιο με του ασύρματου δικτύου, με τη διαφορά ότι το fake access point θα είναι συνδεδεμένο σε ένα ενσύρματο δίκτυο.

Σκοπός του συγκεκριμένου υποκεφαλαίου είναι να στηθεί η υποδομή για man in the middle attack. Αυτό γίνεται με τη δημιουργία ενός software fake access point με το οποίο συνδέεται ο client και νομίζει ότι είναι συνδεδεμένος σε ένα ασύρματο δίκτυο όπου έχει παντού πρόσβαση. Ο επιτιθέμενος μπορεί και δρομολογεί έτσι την κίνηση του Internet από και προς τον client. Αυτό που δεν ξέρει ο client είναι ότι με αυτό τον τρόπο έχει δώσει τη δυνατότητα στον επιτιθέμενο να υποκλέπτει τα δεδομένα του και με τα κατάλληλα εργαλεία να μπορεί να τα αποκωδικοποιήσει. Η παρακάτω εικόνα δείχνει αυτό που θα στηθεί.



Εικόνα 154. Διάταξη attacker σε MITM επίθεση

Για να ξεκινήσει το στήσιμο της υποδομής για μια επίθεση MITM θα πρέπει να δημιουργηθεί ένα software access point. Η εντολή είναι:

- **airbase-ng --essid (όνομα SSID) –c (κανάλι λειτουργίας) mon0**

  και η λειτουργία του fake access point ξεκινάει

Εικόνα 155. Δημιουργία software access point

Το at0 που δημιουργεί το airbase-ng είναι ένα interface το οποίο ουσιαστικά αντιστοιχεί στην ασύρματη πλευρά του access point και φαίνεται στην παρακάτω εικόνα χρησιμοποιώντας την εντολή ifconfig at0, η οποία δείχνει τα στοιχεία του.

Εικόνα 156. Η λειτουργία του at0 interface ως Ethernet

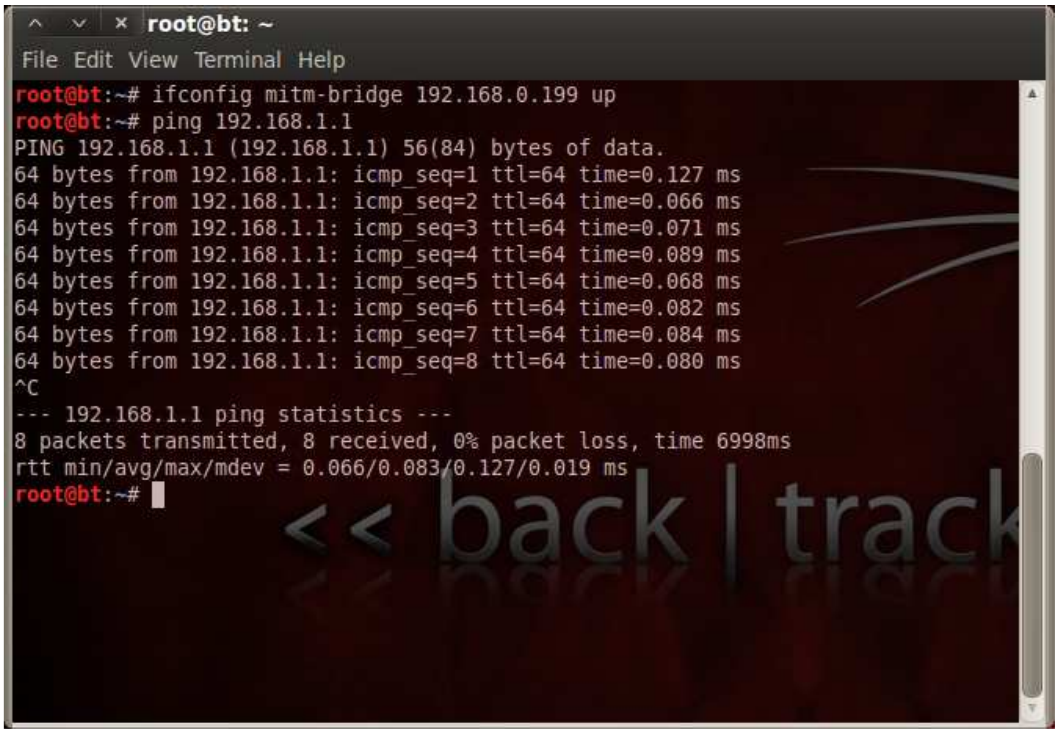
Το επόμενο στάδιο είναι να γεφυρώσετε το at0 interface με το eth0 interface το οποίο αντιστοιχεί στην ενσύρματη δικτυωμένη πλευρά του software access point. Οι βασικές εντολές για να γίνει αυτό είναι η brctl η οποία δημιουργεί ένα bridge ανάμεσα σε δύο interfaces και η ifconfig που ενεργοποιεί τα interfaces με την παράμετρο up και να τους καταχωρεί και IP.

- **brctl addbr (όνομα του bridge θα δημιουργηθεί)**
  - η παράμετρος addbr προσθέτει interfaces στο bridge.
- **brctl addif (όνομα του bridge που δημιουργήθηκε) eth0**
  - η παράμετρος addif προσθέτει interfaces στο bridge που δημιουργήσατε
- **brctl addif (όνομα του bridge που δημιουργήθηκε) at0**
- **ifconfig eth0 0.0.0.0 up**
- **ifconfig at0 0.0.0.0 up**

Εικόνα 157. Δημιουργία bridge, προσθήκη και ενεργοποίηση των interfaces που θα χρησιμοποιηθούν

Θα πρέπει να προστεθεί μια IP διεύθυνση στο bridge για να μπορέσετε να ελέγξετε την συνδεσιμότητα με το gateway. Η εντολή για την δήλωση μιας IP στο bridge είναι

- **ifconfig (όνομα bridge) IP address up**



Εικόνα 158. Δοκιμή λειτουργίας του bridge

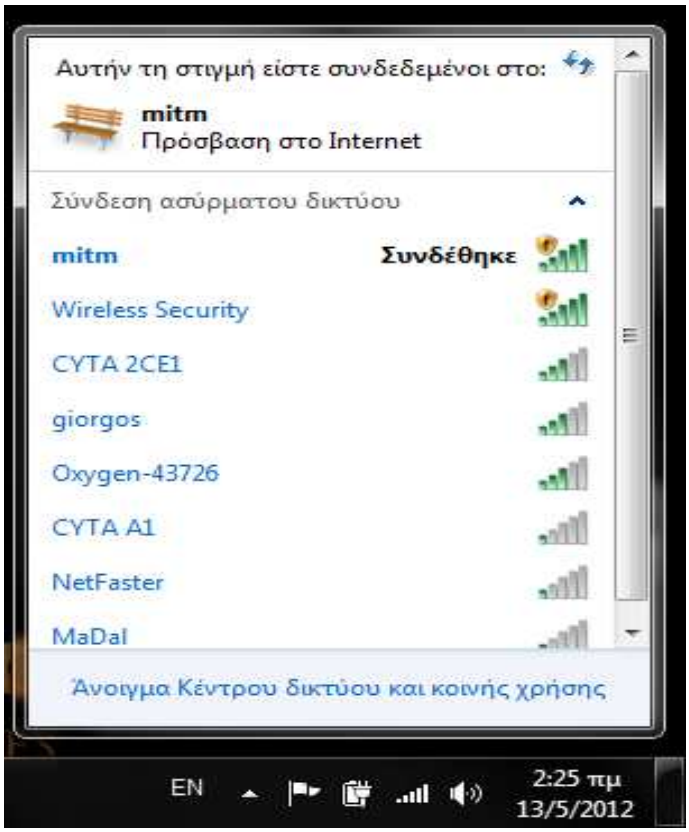
Στην παραπάνω εικόνα φαίνεται και η εντολή ping που δόθηκε για να δοκιμαστεί η επικοινωνία του bridge με την gateway, βάζοντας την IP της. Η λειτουργία της σύνδεσης με το gateway λογικά θα πρέπει να επιβεβαιωθεί.

Το επόμενο βήμα είναι να ρυθμίσετε να γίνονται forward και routing των πακέτων σωστά μεταξύ bridge και gateway, ώστε το θύμα να μην μπορεί να καταλάβει ότι δεν έχει σύνδεση με το δίκτυο. Η εντολή είναι:

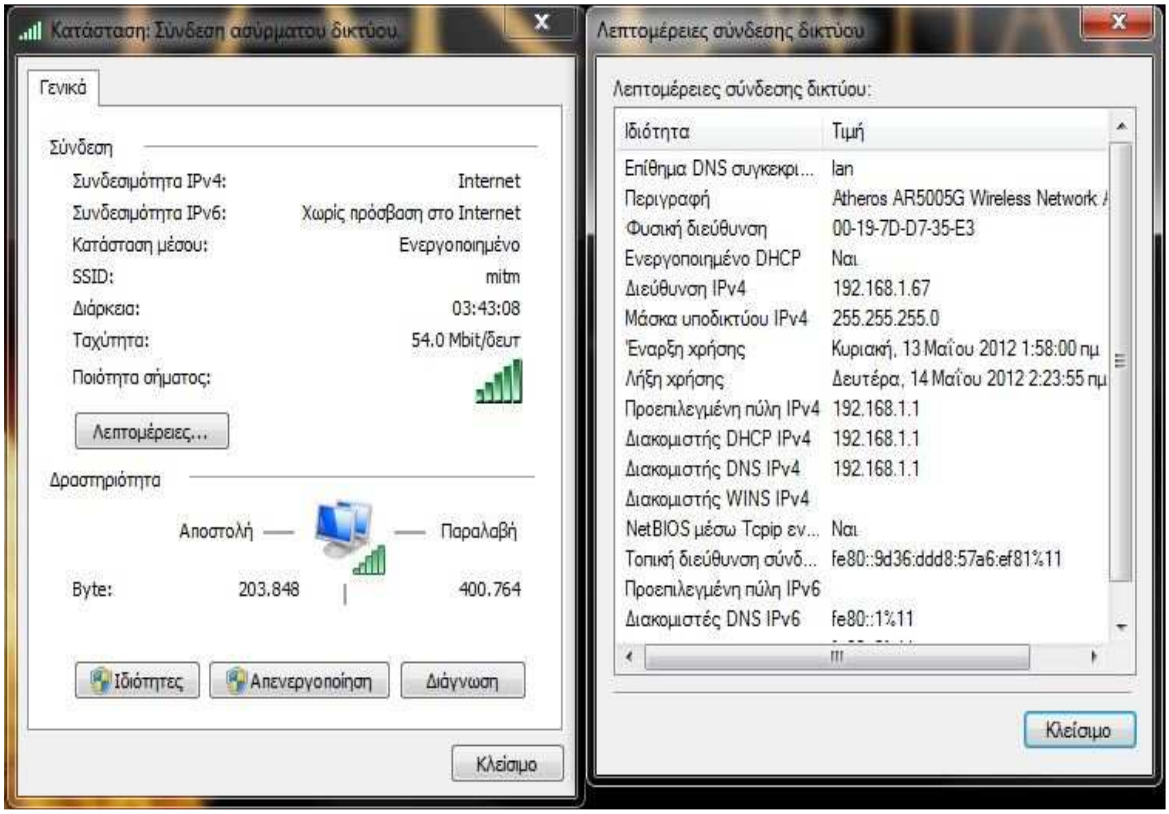
- **echo 1> /proc/sys/net/ipv4/ip_forward**

    - Η εντολή αυτή γράφει το 1 στο αρχείο ip_forward με το οποίο έτσι δηλώνει την ενεργοποίηση της λειτουργίας ip forwarding.

Εικόνα 159. Ενεργοποίηση IP forwarding

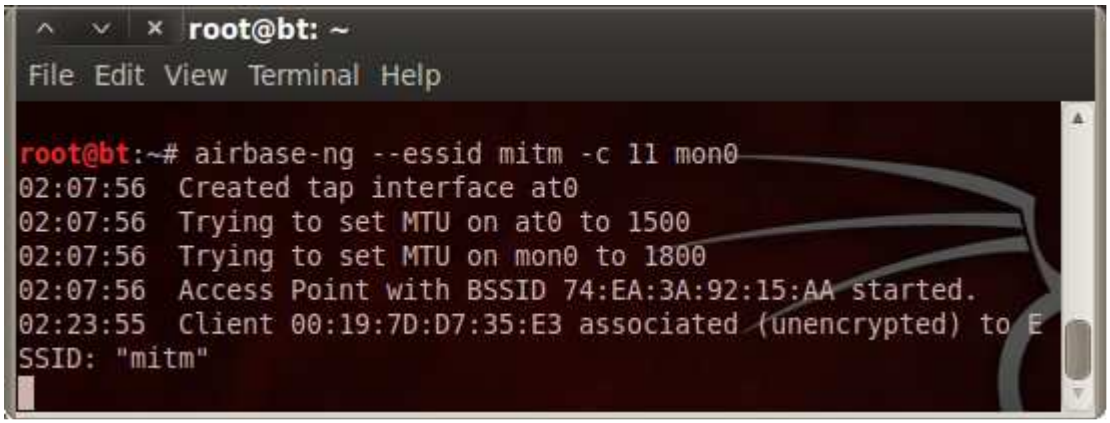


Εικόνα 160. Σύνδεση client με software access point



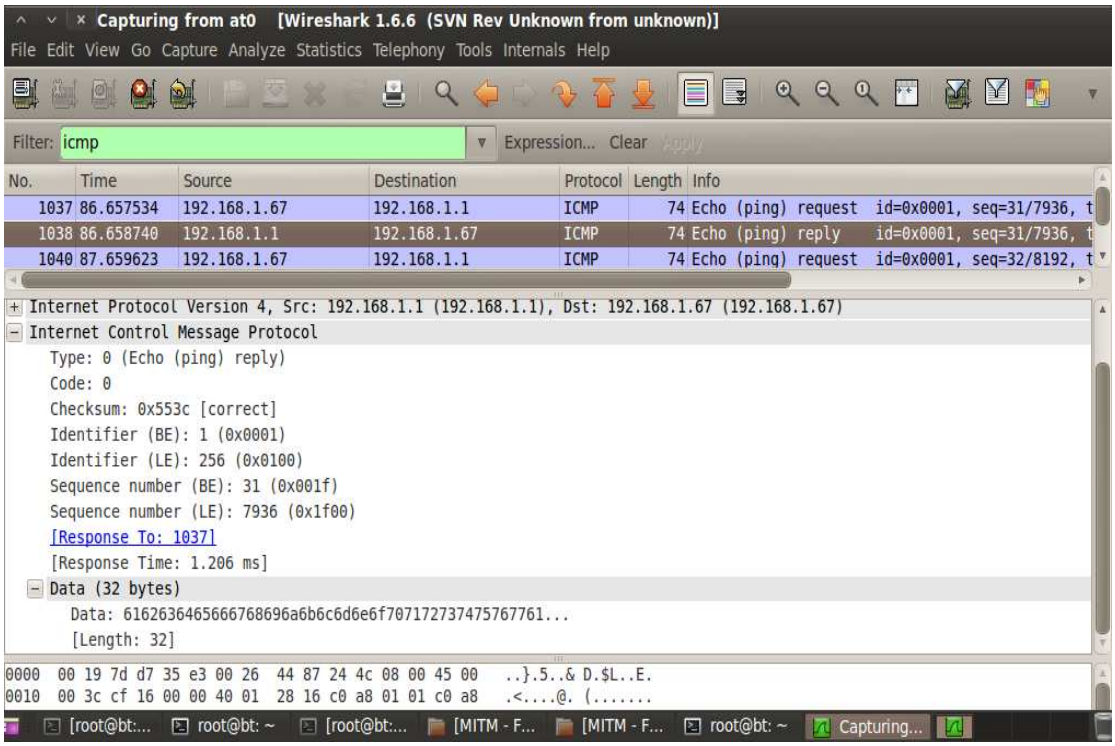
Εικόνα 161. Η σύνδεση του client με το software AP και κατ' επέκταση με το gateway επιβεβαιώνεται και από το ότι του έχει εκχωρηθεί IP address

Η επιβεβαίωση του client με το software AP φαίνεται και από το παράθυρο του terminal όπου τρέχει το airbase-ng.

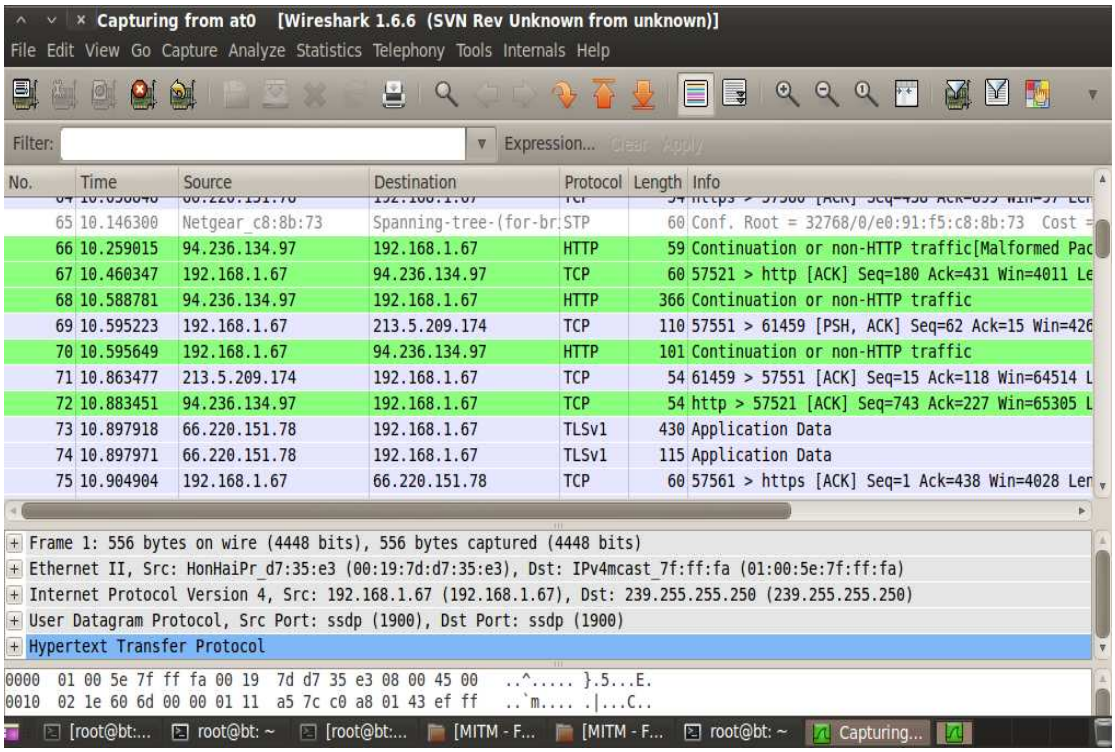


Εικόνα 162. Επιβεβαίωση σύνδεσης και μέσω airbase-ng

Αφού είδατε πως δημιουργείται ένα είδος επίθεσης man in the middle μπορείτε να χρησιμοποιήσετε κάποιο πρόγραμμα για την υποκλοπή δεδομένων του client. Ένα αρκετά γνωστό πρόγραμμα για sniffing πακέτων μεταξύ client και software access point είναι το wireshark. Με αυτό μπορείτε να κάνετε capture πακέτα τα οποία μπορεί να περιέχουν hashes κωδικών και usernames για κάποια sites και με το ανάλογο πρόγραμμα να τα αποκρυπτογραφήσετε και να τα υποκλέψετε.



Εικόνα 163. Πακέτα ICMP από το ping του client θύματος στο gateway



Εικόνα 164. Capture *πακέτων από το soft AP στο at0 interface*

6. Κεφάλαιο – Επιθέσεις σε WLAN κρυπτογράφηση

6.1 Τρόποι μετάδοσης δεδομένων και κρυπτογράφηση

Είναι αυτονόητο αλλά πρέπει να τονιστεί, πως οποιαδήποτε επικοινωνία πραγματοποιείται χωρίς κρυπτογράφηση, είναι διαθέσιμη σε οποιονδήποτε θέλει και έχει πρόσβαση στο μέσο μεταφοράς της. Μέσα μεταφοράς είναι οι αγωγοί χαλκού και οι οπτικές ίνες για τις ενσύρματες επικοινωνίες, ενώ για τις ασύρματες επικοινωνίες έχουμε τα ραδιοκύματα και τους παλμούς φωτός. Για την υποκλοπή ενσύρματων επικοινωνιών απαιτείται η προσέγγιση του χώρου του «θύματος», οπότε, πρακτικά είναι πολύ πιο δύσκολο σε σχέση με την υποκλοπή μιας ασύρματης επικοινωνίας που χρησιμοποιεί τα ραδιοκύματα ως μέσο μετάδοσης, και μπορεί να πραγματοποιηθεί ακόμα κι από μεγάλη απόσταση, τέτοια ώστε αυτός που θα την πράξει να μην γίνει αντιληπτός. Αυτός ακριβώς είναι ο τρόπος λειτουργίας ενός ασύρματου router, και μία τέτοια συσκευή μπορεί να μεταδώσει δεδομένα σε αρκετά μεγάλες αποστάσεις. Με τον κατάλληλο εξοπλισμό (πχ. κατευθυντική κεραία υψηλής απολαβής) απ' την πλευρά του υποκλοπέα, η απόσταση μπορεί να φτάσει σε αρκετά χιλιόμετρα στην περίπτωση οπτικής επαφής υποκλοπέα και router, ενώ ανάμεσα στα κτίρια μιας πόλης πέφτει σε μερικές εκατοντάδες μέτρα.

6.2 Τρόποι κρυπτογράφησης ασύρματων δικτύων

Οι πρώτες ασύρματες συσκευές που κυκλοφόρησαν, διέθεταν κρυπτογράφηση WEP. Αυτή υλοποιήθηκε με μια απλοϊκή και λανθασμένη χρήση του αλγορίθμου RC4[27], δηλαδή αναφερόμαστε σε μια κρυπτογραφικά αδύναμη κωδικοποίηση, και σύντομα φάνηκαν οι αδυναμίες της. Σήμερα θεωρείται εντελώς αποτυχημένη, ενώ με προγράμματα που κυκλοφορούν ελεύθερα, μπορεί να αποκτήσει κάποιος το κλειδί κρυπτογράφησης μέσα σε λίγα λεπτά. Στη συνέχεια έκαναν την εμφάνισή τους συσκευές που διόρθωναν τα λάθη του WEP, ενώ σε πολλές περιπτώσεις οι κατασκευαστές δημιούργησαν firmware για την αναβάθμιση των παλαιότερων συσκευών, στην μέθοδο κρυπτογράφησης TKIP[28] που χρησιμοποιούσε πλέον με σωστό τρόπο και με όλες τις απαραίτητες δικλείδες ασφαλείας τον αλγόριθμο RC4. Οι συσκευές που τηρούν τις προδιαγραφές του TKIP, φέρουν την πιστοποίηση WPA. Η τελευταία πιστοποίηση είναι η WPA2 και χρησιμοποιεί μια παραλλαγή του αλγορίθμου AES που ονομάζεται CCMP. Ο αλγόριθμος αυτός θεωρείται σήμερα απολύτως ασφαλής, ενώ είναι πολλές τάξεις ανώτερος του προηγούμενου από κρυπτογραφική άποψη. Οι νεότερες συσκευές στην πλειοψηφία τους έρχονται με την πιστοποίηση WPA2. Παρ' όλα αυτά, για λόγους συμβατότητας υποστηρίζουν και τους παλαιότερους τρόπους κρυπτογράφησης.

Οι πιο διαδεδομένοι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται για την ασφάλεια των ασύρματων δικτύων είναι οι παρακάτω:

- **Wired Equivalent Privacy (WEP):** Η WEP είναι μια παλαιότερη μέθοδος ασφαλείας δικτύου που εξακολουθεί να είναι διαθέσιμη για να υποστηρίζει παλαιότερες συσκευές, αλλά δεν συνιστάται πια. Κατά την ενεργοποίηση της

[27] http://en.wikipedia.org/wiki/RC4
[28] http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol

WEP, ρυθμίζετε ένα κλειδί ασφαλείας δικτύου. Αυτό το κλειδί κρυπτογραφεί τις πληροφορίες, τις οποίες κάποιος υπολογιστής στέλνει σε κάποιον άλλον μέσα στο δίκτυο. Ωστόσο η ασφάλεια WEP είναι σχετικά εύκολο να παραβιαστεί.[29]

- **Wi-Fi Protected Access (WPA) και Wi-Fi Protected Access II (WPA2):** Η WPA κρυπτογραφεί πληροφορίες, ενώ ταυτόχρονα εκτελεί ελέγχους, ώστε να εξασφαλίσει ότι το κλειδί ασφαλείας δικτύου δεν έχει τροποποιηθεί. Επιπλέον, η WPA ελέγχει την ταυτότητα των χρηστών και εξασφαλίζει ότι μόνον εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στο δίκτυο.

  Υπάρχουν δύο τύποι ελέγχου ταυτότητας WPA: Η WPA και η WPA2. Η WPA σχεδιάστηκε για να είναι συμβατή με όλους τους προσαρμογείς ασύρματου δικτύου, αλλά ενδέχεται να μην είναι συμβατή με παλαιότερους δρομολογητές ή σημεία πρόσβασης. Η WPA2 είναι ασφαλέστερη από την WPA, αλλά δεν είναι συμβατή με ορισμένους παλαιότερους προσαρμογείς δικτύου. Η WPA σχεδιάστηκε για χρήση με διακομιστές ελέγχου ταυτότητας 802.1X, οι οποίοι διανέμουν διαφορετικά κλειδιά σε κάθε χρήστη. Ο έλεγχος αυτός ονομάζεται WPA-Εταιρικό ή WPA2-Εταιρικό. Επιπλέον, μπορεί να χρησιμοποιηθεί στην κατάσταση λειτουργίας ήδη κοινόχρηστου κλειδιού (PSK), όπου όλοι οι χρήστες λαμβάνουν την ίδια φράση πρόσβασης.[30]

6.3 Σκοπός

Στο κεφάλαιο αυτό θα επικεντρωθούμε με το να δείξουμε πως γίνεται να κάνουμε Sniffing καθώς και πως μπορούμε να “σπάσουμε” τους αλγορίθμους WEP και WPA που χρησιμοποιούν όλα τα router . Το πρόγραμμα που θα χρησιμοποιήσουμε είναι το Aircrack 1.1 σε περιβάλλον Backtrack 5 R2 (Linux) και Windows.

6.4 Υλοποίηση επιθέσεων για ανάκτηση κωδικών WEP και WPA

Παρακάτω λοιπόν θα δείξουμε πως μπορούμε να κάνουμε επίθεση σε ένα ασύρματο δίκτυο που χρησιμοποιεί αλγόριθμο κρυπτογράφησης WEP και WPA αντίστοιχα με σκοπό την ανάκτηση του κλειδιού του δικτύου και την πρόσβαση σε αυτό.

6.4.1 Υλοποίηση επίθεσης σε δίκτυο που κάνει χρήση ασφάλειας WEP

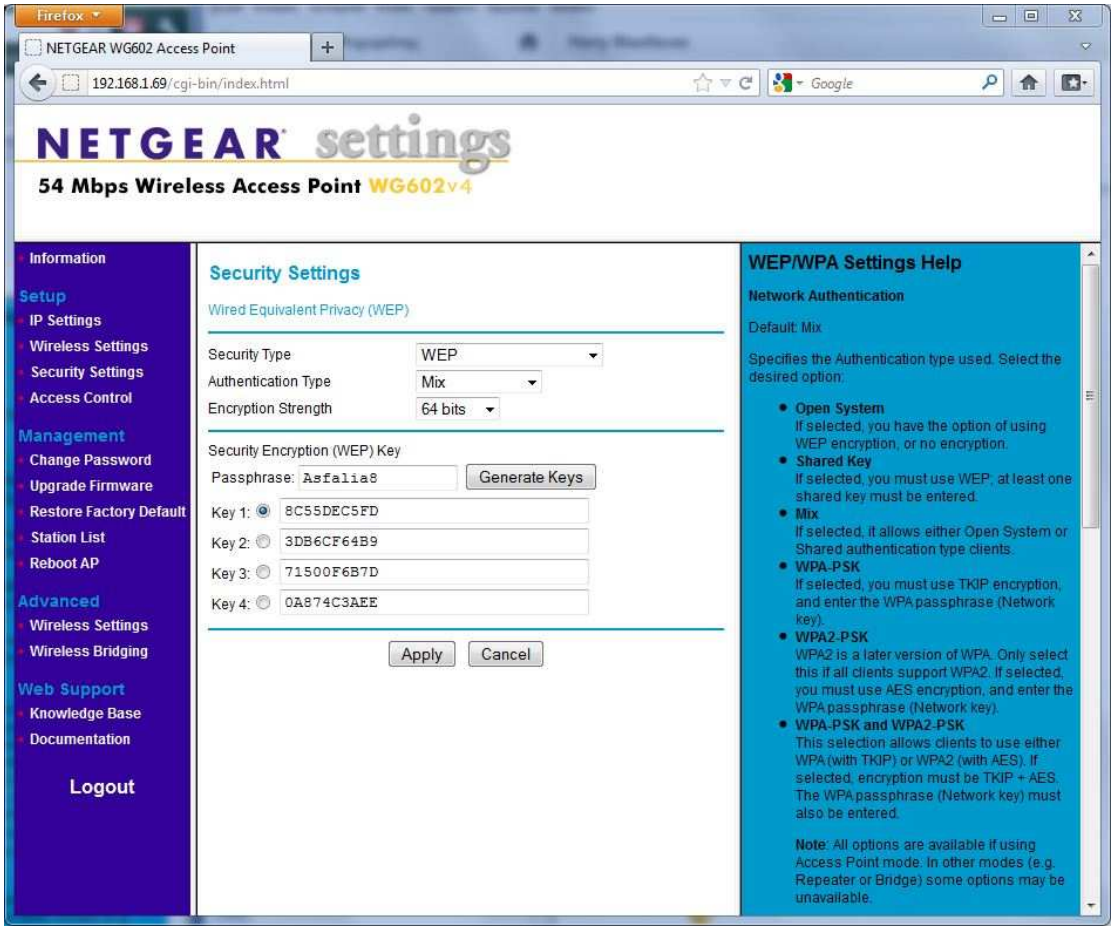
Όπως έχουμε αναφέρει και στην εισαγωγή ο αλγόριθμος κρυπτογράφησης WEP είναι μια παλαιότερη μέθοδος ασφαλείας δικτύου που εξακολουθεί να είναι διαθέσιμη για να υποστηρίζει παλαιότερες συσκευές. Για αυτό και θεωρείτε ως ένα

[29] http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
[30] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

αδύναμος αλγόριθμος που προσφέρει σχετικά μικρά επίπεδα ασφάλειας σε αντίθεση με το μεταγενέστερο του WPA και WPA2.

Αυτό λοιπόν θα εξετάσουμε και παρακάτω σε τέσσερα (4) απλά βήματα. Θα κάνουμε επίθεση σε ένα Access Point με SSID "**Wireless Security**" που κάνει χρήση του αλγορίθμου κρυπτογράφησης WEP με τη χρήση μιας εξωτερικής ασύρματης κάρτας. Τα προϊόντα που χρησιμοποιήσαμε είναι της εταιρείας NETGEAR και συγκεκριμένα το Wireless-G 54 Access Point και τον USB Adapter N150 Wireless.

Ξεκινώντας λοιπόν προχωρήσαμε στην ρύθμιση του Access Point όπως μπορείτε να δείτε και παρακάτω. Συγκεκριμένα στην καρτέλα Security Settings επιλέξαμε τύπο ασφαλείας: WEP, Authentication Type: Mix, και Encryption Strength: 64 bits. Στην συνέχεια και συγκεκριμένα στο Security / Encryption (WEP) key στη λέξη ασφαλείας δώσαμε τον κωδικό **Asfalia8** και πατώντας το κουμπί Generate Keys μας δημιούργησε τέσσερα (4) διαφορετικά κλειδιά όπου μπορούμε να διαλέξουμε πιο θα χρησιμοποιηθεί για την επαλήθευση των στοιχείων όταν χρειαστεί να συνδεθούμε στο συγκεκριμένο Access Point. Ας δούμε λοιπόν τα βήματα που μπορεί να ακολουθήσει κάποιος προκειμένου να καταφέρει να "σπάσει" ένα τέτοιο δίκτυο με την χρήση του Backtrack 5 R2 και της σουίτας Aircrack-ng.



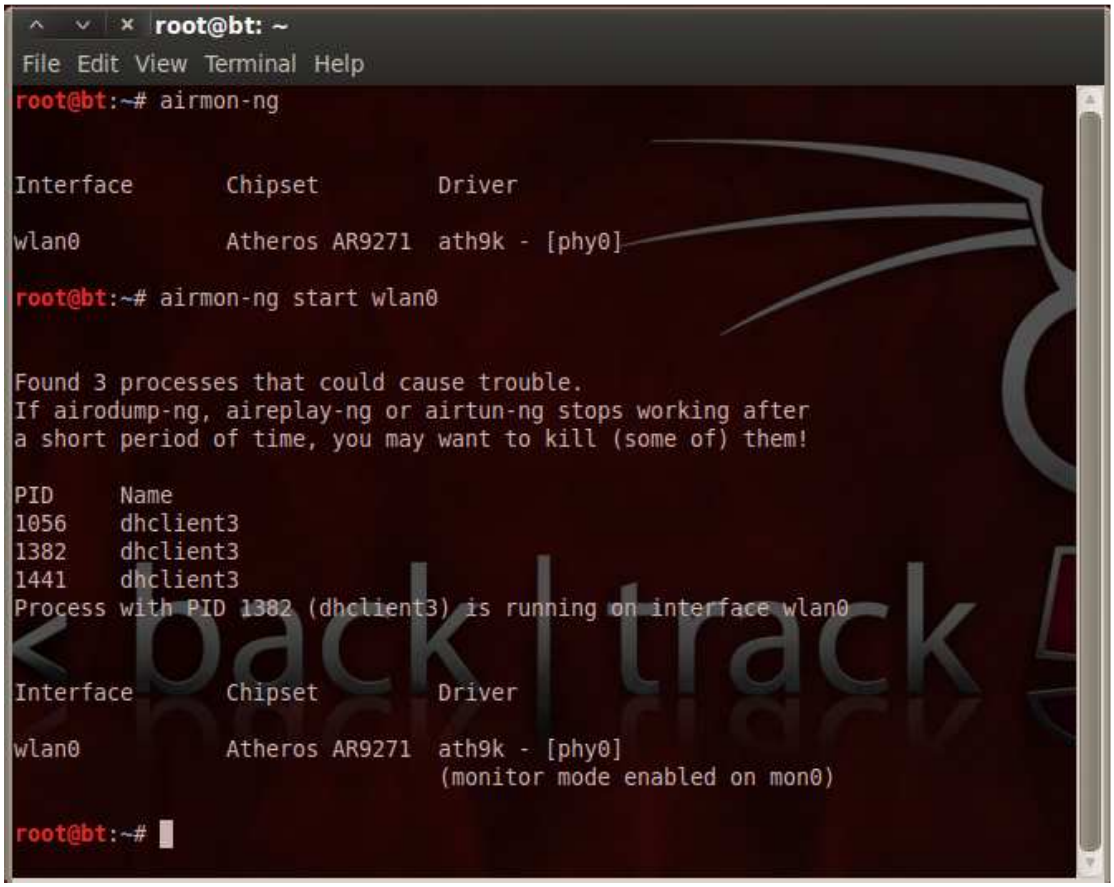
Εικόνα 165. Netgear Access Point - Configuration Settings

Βήμα 1^{ο} – Ανίχνευση και καταγραφή πακέτων

Πριν από τον εντοπισμό των διαθέσιμων δικτύων πρέπει να τεθεί η κάρτα σε monitor mode. Στο monitor mode η κάρτα μπορεί να λάβει όλα τα πακέτα που διακινούνται στο ασύρματο δίκτυο αντί μόνο αυτών που προορίζονται για τον συγκεκριμένο υπολογιστή. Επίσης κατ' αυτόν τον τρόπο δίνεται η δυνατότητα στον χρήστη να ενεργοποιήσει την λειτουργία injection έτσι ώστε να αυξηθεί η κίνηση πακέτων στο δίκτυο και να ολοκληρωθεί γρηγορότερα η όλη διαδικασία.

Για να τεθεί η κάρτα δικτύου σε monitor mode ανοίγετε ένα τερματικό και πληκτρολογείτε τα εξής:

- **airmon-ng**
- **airmon-ng start wlan0**



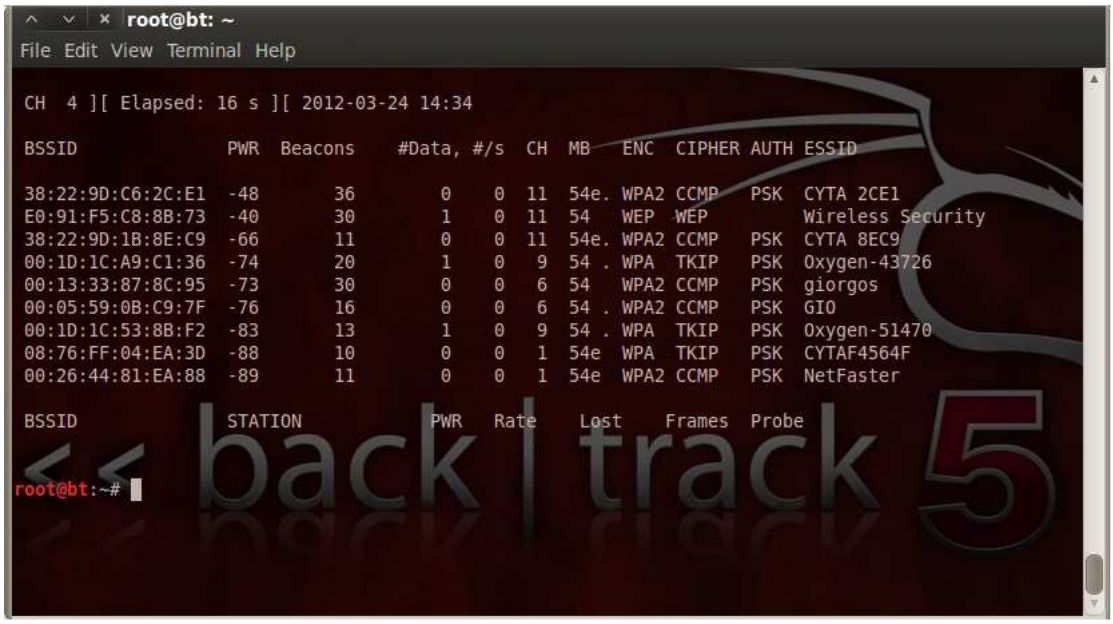
Εικόνα 166. Ενεργοποίηση Monitor mode

Όπως μπορείτε να προσέξετε και παραπάνω η ασύρματη κάρτα έχει τεθεί σε λειτουργία monitor mode (mon0).

Έχοντας φέρει την ασύρματη κάρτα σας σε κατάσταση monitor mode, μπορείτε να χρησιμοποιήσετε πια το εργαλείο airodump-ng που διαθέτει η σουίτα Aircrack-ng για τον εντοπισμό των Access Point. Για να εντοπίσετε τα διαθέσιμα ασύρματα δίκτυα στο ίδιο terminal που βρίσκεστε θα πρέπει να πληκτρολογήσετε την εντολή:

- **airodump-ng mon0**

Αν το Airodump-ng συνδεθεί με την συσκευή WLAN, θα εμφανιστεί το παρακάτω παράθυρο:

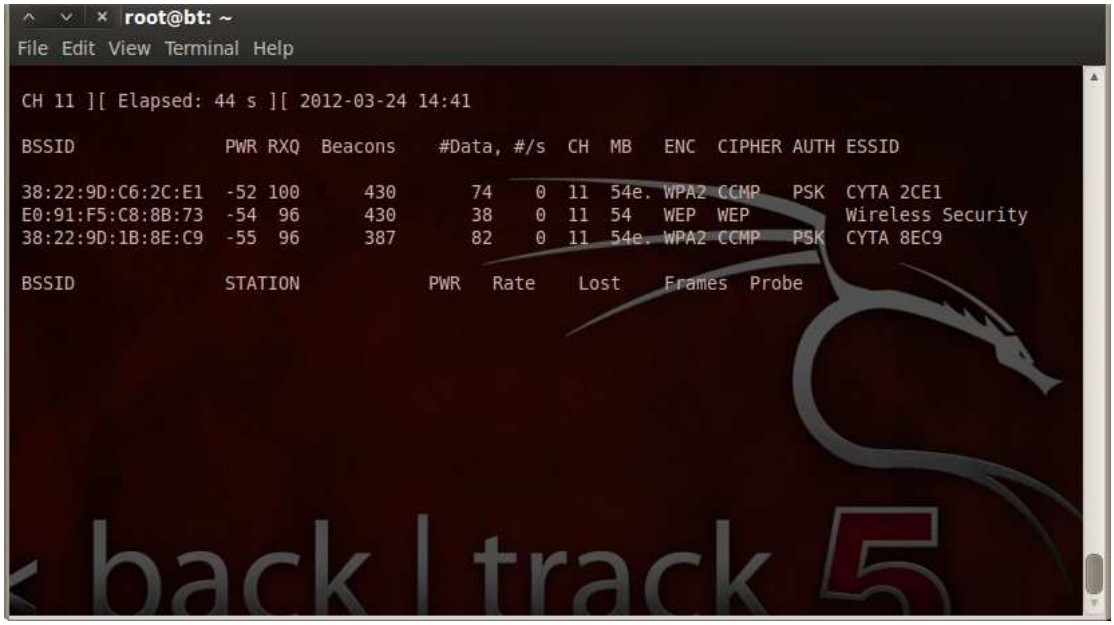


Εικόνα 167 Ενεργοποίηση Airodump-ng

Το airodump-ng κάνει αναζήτηση για AP από τα οποία μπορεί να δεχτεί πακέτα δεδομένων σε όλα τα κανάλια. Μετά από κάποιο χρονικό διάστημα κάποια AP και οι συνδεδεμένοι σε αυτά clients θα εμφανιστούν.

Στην συνέχεια θα πρέπει να εισάγετε κάποιες παραμέτρους στο airodump-ng έτσι ώστε να εστιάσει στο επιθυμητό δίκτυο και να ξεκινήσει την καταγραφή πακέτων. Για να γίνει αυτό, θα πρέπει να διακόψετε την αναζήτηση δικτύων πατώντας Ctrl+C και στο terminal που βρίσκεστε να πληκτρολογήσετε την παρακάτω εντολή:

- **airodump-ng –c 11 –w crack –b BSSID mon0**



Εικόνα 168. Airodump-ng - Capture Packets

- Με την παράμετρο -c το airodump-ng συντονίζεται στο συγκεκριμένο κανάλι ενώ η παράμετρος -w δηλώνει τα network dumps που αποθηκεύονται στον σκληρό. Η παράμετρος --bssid (αλλιώς -b) σε συνδυασμό με τη διεύθυνση MAC του AP περιορίζει την αναζήτηση σε ένα συγκεκριμένο.

Μπορείτε ακόμη να προσθέσετε την παράμετρο ivs η οποία αποθηκεύει μόνο τις αναγκαίες πληροφορίες από τα πακέτα δεδομένων που λαμβάνει η κάρτα ασύρματου δικτύου, εξοικονομώντας έτσι αρκετό χώρο στο σκληρό δίσκο.

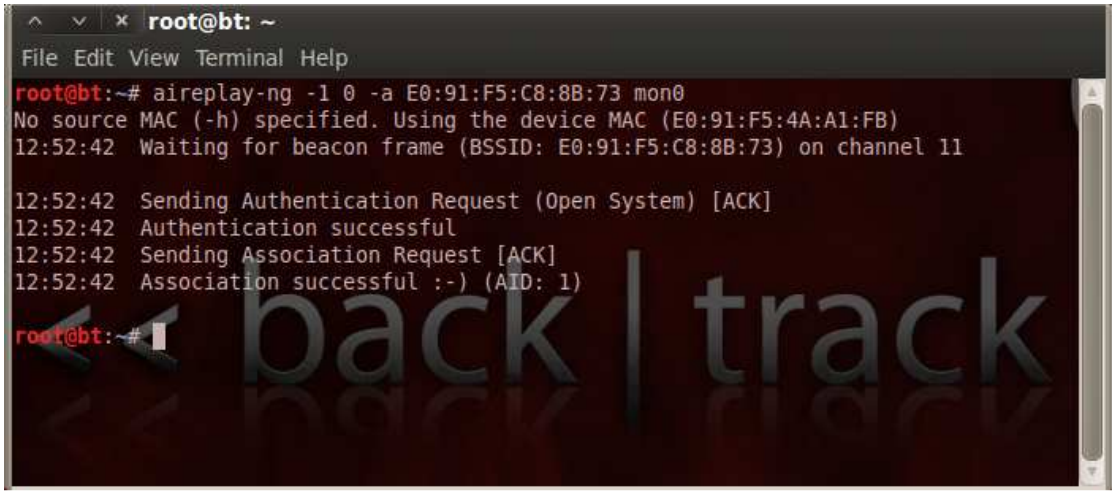
Για να μπορέσετε να "σπάσετε" ένα κλειδί WEP συνήθως χρειάζονται 30.000 με 50.000 διαφορετικά IVs (Initialization Vectors). Κάθε πακέτο δεδομένων περιέχει ένα IV. Ένα IV μπορεί να ξαναχρησιμοποιηθεί, γι' αυτό συνήθως ο αριθμός των IVs είναι μικρότερος από τον αριθμό των πακέτων δεδομένων που λαμβάνονται.

Βήμα 2^0 – Packet Injection

Στην συνέχεια θα χρησιμοποιήσετε την λειτουργία του Packet injection. Η κύρια λειτουργία του είναι να **δημιουργήσουμε κυκλοφορία πακέτων** ώστε να καταγράφουμε πολύ περισσότερα πακέτα από αυτά που ανταλλάσσονται πραγματικά στο δίκτυο. Απαραίτητο στοιχείο είναι το BSSID του AP. Στην συνέχεια προσπαθούμε να συνδεθούμε με το AP χρησιμοποιώντας το εργαλείο aireplay-ng με την εξής εντολή σε ένα καινούργιο terminal:

- **aireplay-ng -1 0 –a BSSID mon0**

Η τιμή μετά την παράμετρο -a είναι το BSSID του AP, το -1 είναι ο τύπος της επίθεσης (fake authentication) και το 0 δηλώνει την καθυστέρηση (delay) στο οποίο θα περιμένει ο client την απάντηση από το AP. Αν το injection επιτύχει θα δείτε το παρακάτω:



Εικόνα 169. Aireplay-ng - Packet Injection

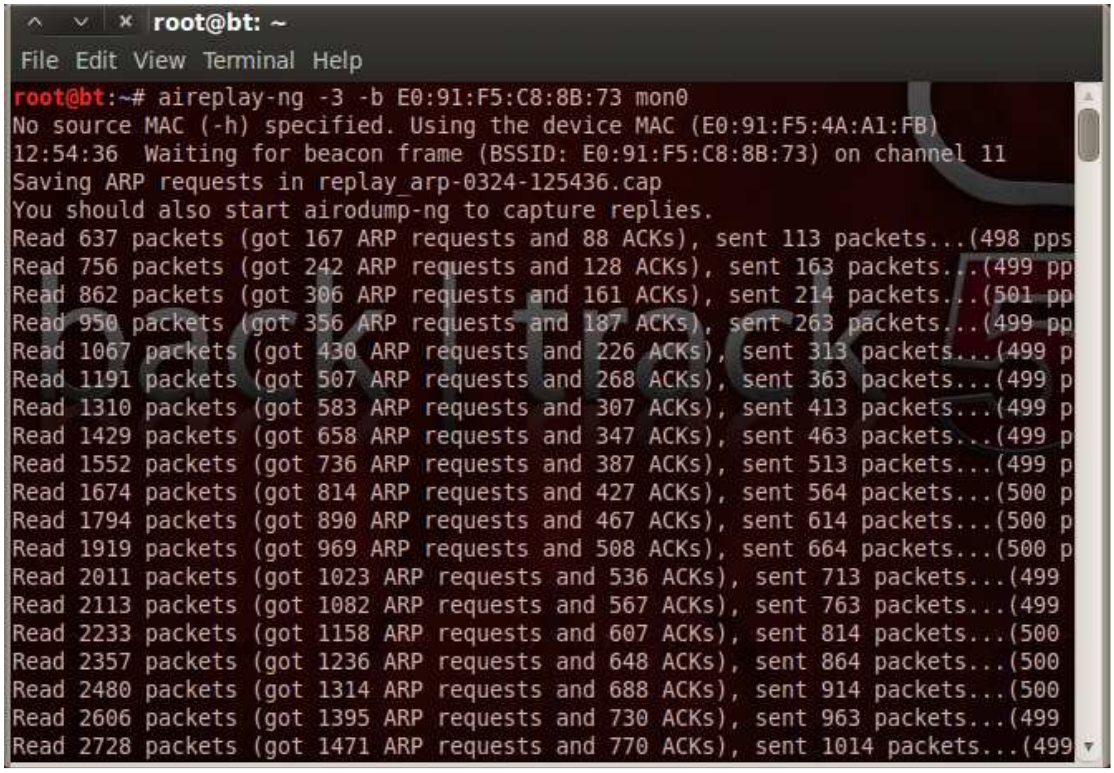
Βήμα 3ο – Αύξηση ταχύτητας καταγραφής πακέτων (ARP replay)

Στην ουσία αυτό που κάνουμε κατά κύριο λόγο με το aireplay-ng είναι να στέλνουμε σήματα στο AP κάνοντας τον να στέλνει περισσότερα πακέτα δεδομένων στον client. Ακόμη μπορούμε να δημιουργήσουμε έναν εικονικό client ο οποίος δεν είναι απευθείας συνδεδεμένος με το AP ωστόσο μπορεί να αυξήσει σημαντικά την κίνηση πακέτων δεδομένων στο δίκτυο και ως αποτέλεσμα να συγκεντρώνουμε γρηγορότερα τα απαραίτητα IVs.

Έχοντας διαπιστώσει ότι λειτουργεί το injection μπορείτε να αυξήσετε δραματικά τον ρυθμό συλλογής IVs.[31] Ανοίξτε λοιπόν ένα νέο τερματικό και πληκτρολογήστε την εντολή:

- **aireplay-ng -3 –b BSSID mon0**

Η τιμή μετά την παράμετρο -b είναι το BSSID του AP, το -3 είναι ο τύπος της επίθεσης (ARP request replay attack). Αν επιτευχθεί θα δείτε το παρακάτω:



Εικόνα 170. Αύξηση ταχύτητας καταγραφής πακέτων

Βήμα 4ο – Εύρεση WEP key

Αφού συγκεντρωθούν αρκετά IVs μπορείτε να ξεκινήσετε τη διαδικασία εύρεσης του WEP key σε ένα νέο terminal:

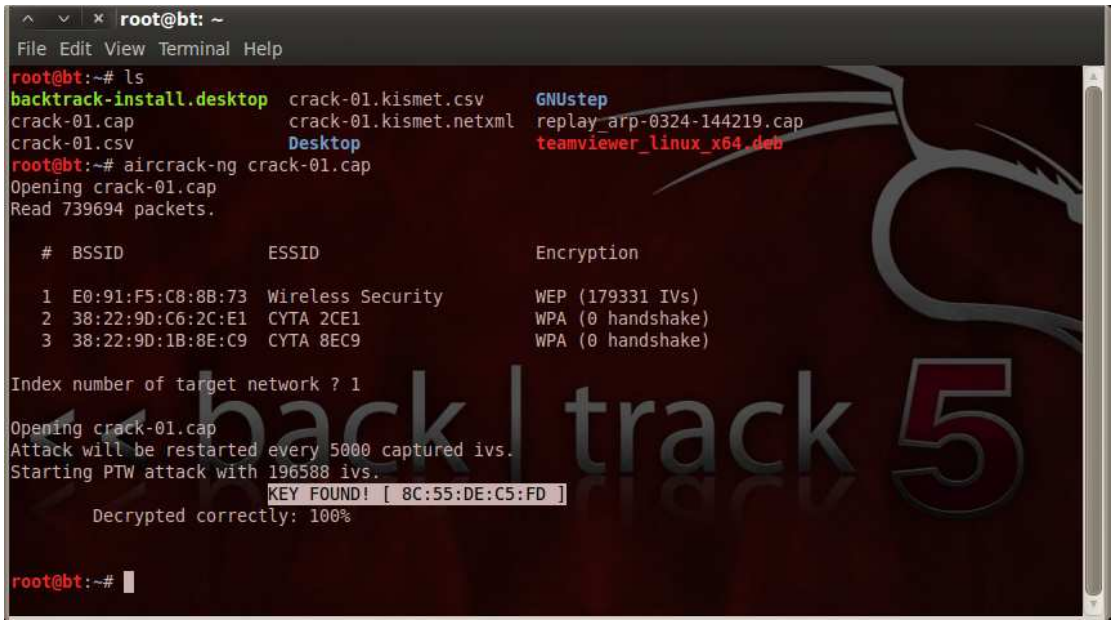
- **aircrack-ng crack-01.cap (όνομα αρχείου όπου έχουν καταγράφει τα πακέτα)**

[31] http://www.aircrack-ng.org/doku.php?id=arp-request_reinjection&DokuWiki=53eb6b9217af02fe9b51a4659a201092

Ωστόσο ενδέχεται κατά την ώρα της καταγραφής των πακέτων από το AP που έχετε επιλέξει, η ασύρματη κάρτα σας να έχει καταγράψει και μερικά πακέτα από κάποιο άλλο AP. Όταν λοιπόν θα χρησιμοποιήσετε την aircrack-ng θα σας ζητήσει να επιλέξετε τα πακέτα όπου θέλετε να αποκρυπτογραφήσετε. Έτσι εσείς αρκεί να δώσετε τον αριθμό που έχει μπροστά το δίκτυό σας. Στο δικό μας παράδειγμα είναι το 1 όπου και έχουμε το AP Wireless Security.

Εικόνα 171. Packet selection for cracking

Μετά το πέρας της αποκωδικοποίησης θα εμφανιστεί το εξής παράθυρο που θα σας δείχνει το WEP κλειδί:



Εικόνα 172. Επιτυχής εύρεση κωδικού ασφαλείας

6.4.2 Υλοποίηση επίθεσης σε δίκτυο που κάνει χρήση ασφάλειας WPA

Όπως έχουμε αναφέρει και στην εισαγωγή ο αλγόριθμος κρυπτογράφησης WPA κρυπτογραφεί πληροφορίες, ενώ ταυτόχρονα εκτελεί ελέγχους, ώστε να εξασφαλίσει ότι το κλειδί ασφαλείας δικτύου δεν έχει τροποποιηθεί. Επιπλέον, η WPA ελέγχει την ταυτότητα των χρηστών και εξασφαλίζει ότι μόνον εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στο δίκτυο. Είναι αυτό όμως η πραγματική αλήθεια;

Για να "σπάσει" το WPA/WPA2 PSK θα πρέπει να συλλάβετε το «Handshake». Δηλαδή θα πρέπει να έχει **ήδη** γίνει ανταλλαγή πακέτων handshake μεταξύ κάποιου client και του ασύρματου δικτύου στόχο, ώστε να μπορέσει να ολοκληρωθεί επιτυχώς η επίθεση. Ο καλύτερος τρόπος γι' αυτό το πακέτο ο εισβολέας θα πρέπει να αποσυνδέσει έναν συνδεδεμένο πελάτη από το AP που είναι συνδεδεμένο κάνοντας χρήση της επίθεσης Deauthentication. Η επίθεση αυτή στέλνει πακέτα αποσυσχέτισης (disasociate) σε έναν ή περισσότερους clients οι οποίοι είναι συνδεδεμένοι στο ασύρματο δίκτυο στόχο. Η αποσυσχέτιση κάποιου client μας βοηθάει να:

- δημιουργηθούν πακέτα ARP requests κατά την αποσυσχέτιση τα οποία θα τα καταγράψουμε και στη συνέχεια θα τα χρησιμοποιήσουμε κάνοντάς τα inject.
- καταγράψουμε το WPA/WPA2 handshake κάνοντας τον client που αποσυσχετίσαμε να ξανασυσχετιστεί με το AP.

Μόλις το κλειδί / πακέτο έχει συλληφθεί, είναι καιρός να ξεκινήσετε μια επίθεση Dictionary.

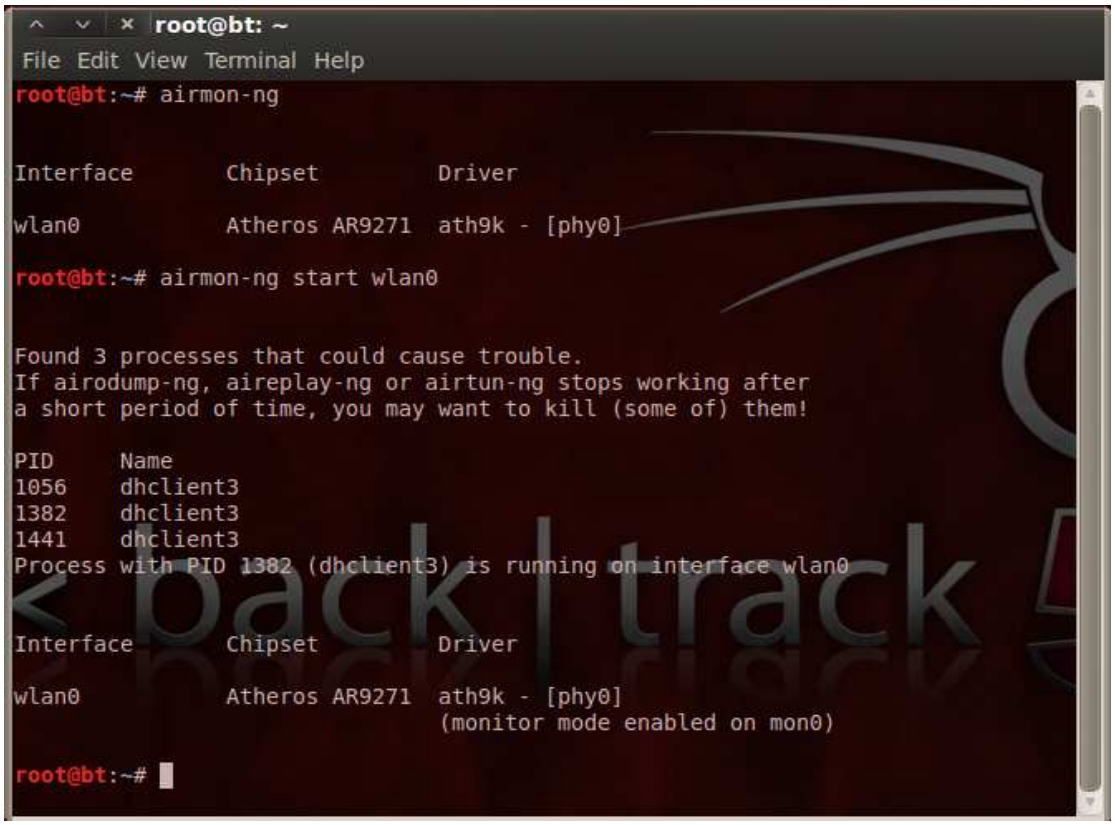
Αυτό λοιπόν θα εξετάσουμε και παρακάτω, πως σε τρία (3) απλά βήματα μπορείτε να “χτυπήσετε” ένα δίκτυο που κάνει χρήση του αλγορίθμου κρυπτογράφησης WPA. Θα κάνουμε επίθεση στο ίδιο Access Point με SSID “**Wireless Security**”. Όπως θα δείτε και παρακάτω το πρώτο βήμα είναι το ίδια με της κρυπτογράφησης WEP.

Βήμα 1^{ο} – Ανίχνευση και καταγραφή πακέτων

Πριν από τον εντοπισμό των διαθέσιμων δικτύων πρέπει να τεθεί η κάρτα σε monitor mode. Στο monitor mode η κάρτα μπορεί να λάβει όλα τα πακέτα που διακινούνται στο ασύρματο δίκτυο αντί μόνο αυτών που προορίζονται για τον συγκεκριμένο υπολογιστή. Επίσης κατ’ αυτόν τον τρόπο δίνεται η δυνατότητα στον χρήστη να ενεργοποιήσει την λειτουργία injection έτσι ώστε να αυξηθεί η κίνηση πακέτων στο δίκτυο και να ολοκληρωθεί γρηγορότερα η όλη διαδικασία.

Για να τεθεί η κάρτα δικτύου σε monitor mode ανοίγετε ένα τερματικό και πληκτρολογείτε τα εξής:

- **airmon-ng**
- **airmon-ng start wlan0**



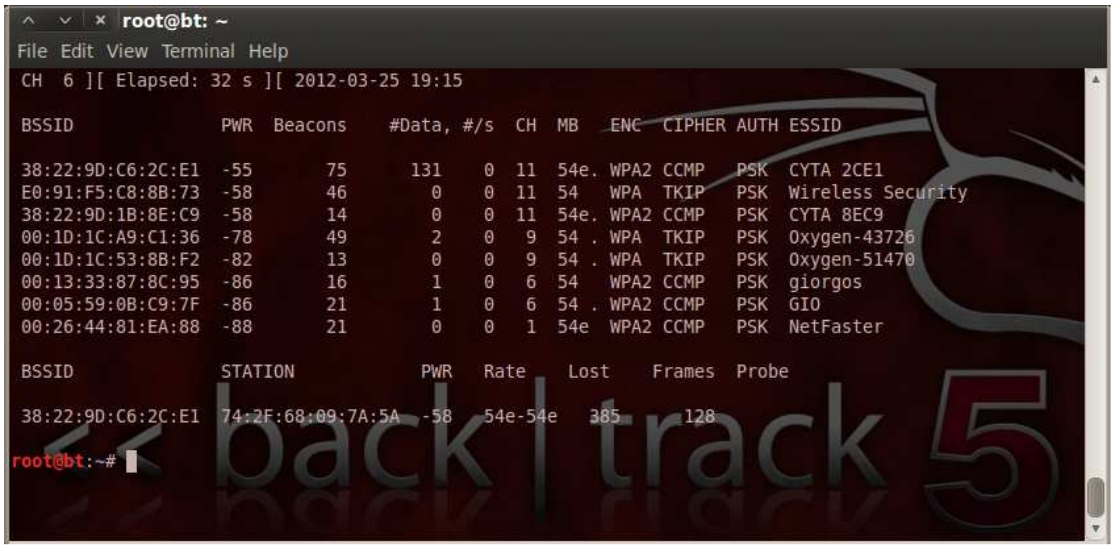
Εικόνα 173. Ενεργοποίηση Monitor Mode

Όπως μπορείτε να προσέξετε και παραπάνω η ασύρματη κάρτα έχει τεθεί σε λειτουργία monitor mode (mon0).

Έχοντας φέρει την ασύρματη κάρτα σας σε κατάσταση monitor mode, μπορείτε να χρησιμοποιήσετε πια το εργαλείο airodump-ng που διαθέτει η σουίτα Aircrack-ng για τον εντοπισμό των Access Point. Για να εντοπίσετε τα διαθέσιμα ασύρματα δίκτυα στο ίδιο terminal που βρίσκεστε θα πρέπει να πληκτρολογήσετε την εντολή:

- **airodump-ng mon0**

Αν το Airodump-ng συνδεθεί με την συσκευή WLAN, θα εμφανιστεί το παρακάτω παράθυρο:



Εικόνα 174. Ενεργοποίηση Airodump-ng

Το airodump-ng κάνει αναζήτηση για AP από τα οποία μπορεί να δεχτεί πακέτα δεδομένων σε όλα τα κανάλια. Μετά από κάποιο χρονικό διάστημα κάποια AP και οι συνδεδεμένοι σε αυτά clients θα εμφανιστούν.

Αφού βρείτε το δίκτυο που θέλετε πατάμε CTRL+C για να σταματήσετε το scan και δίνετε την εντολή:

- **airodump-ng -c (channel) -w (file name) --bssid (AP bssid) (interface)**

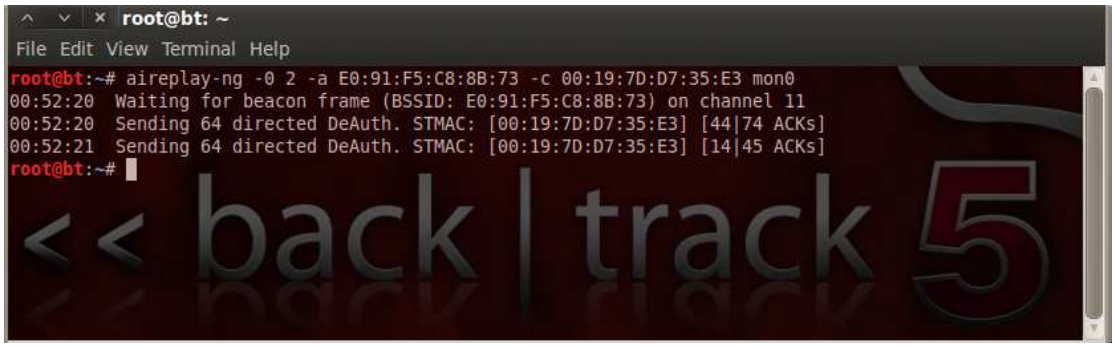
(Όπου channel το κανάλι που είναι το ασύρματο, όπου file name ένα όνομα που θέλετε εσείς και όπου AP bssid η MAC address του "θύματος") για να αρχίσετε την συλλογή του authentication handshake.

Βήμα 2ο – Capture 4-way Authentication Handshake

Στην συνέχεια ανοίγετε ένα δεύτερο terminal και δίνετε την εντολή:

- **aireplay-ng -0 2 -a (bssid AP) -c (bssid Client) (interface)**

για να αρχίσετε να συλλάβετε το 4-way authentication handshake από το AP (Όπου bssid Client η MAC address του πελάτη που είναι συνδεδεμένος με το AP).



Εικόνα 175. 4-way Authentication Handshake

Όταν λάβετε το WPA handshake τότε επάνω αριστερά θα σας εμφανίσει κάτι

σαν το παρακάτω παράθυρο:

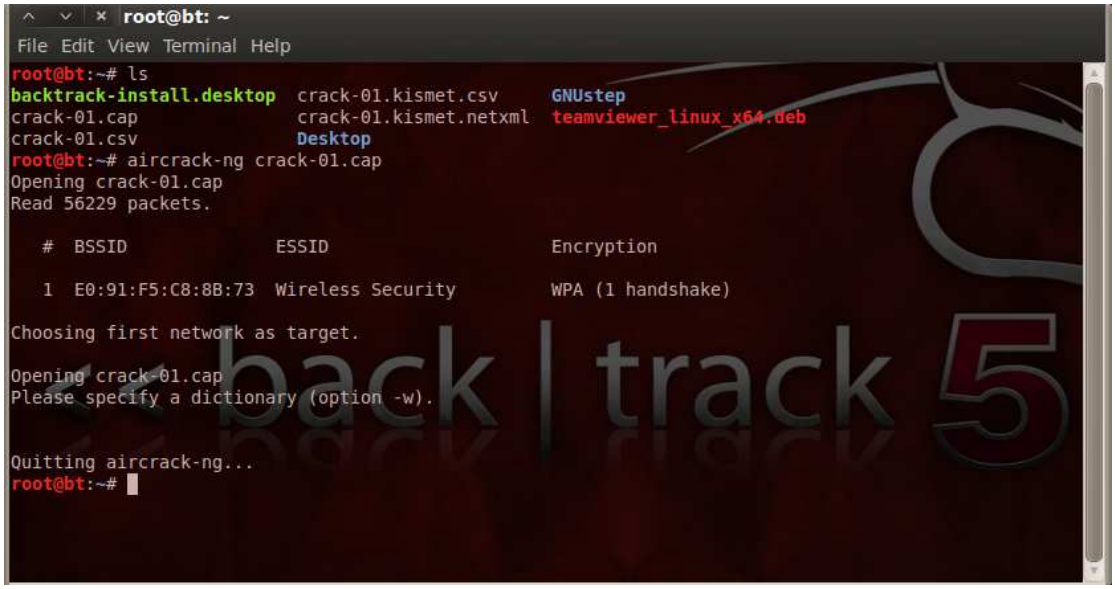
Εικόνα 176. WPA Handshake packet capture

Βήμα 3^{ο} – Εύρεση WPA key

Όταν πάρετε το WPA Handshake τότε ήσαστε στο τελευταίο βήμα. Απλά ανοίγετε ένα τρίτο terminal και δίνετε τις εντολές:

- **aircrack-ng crack-01.cap**
- **aircrack-ng -w (wordlist) -b (bssid AP) (file name)*.cap**

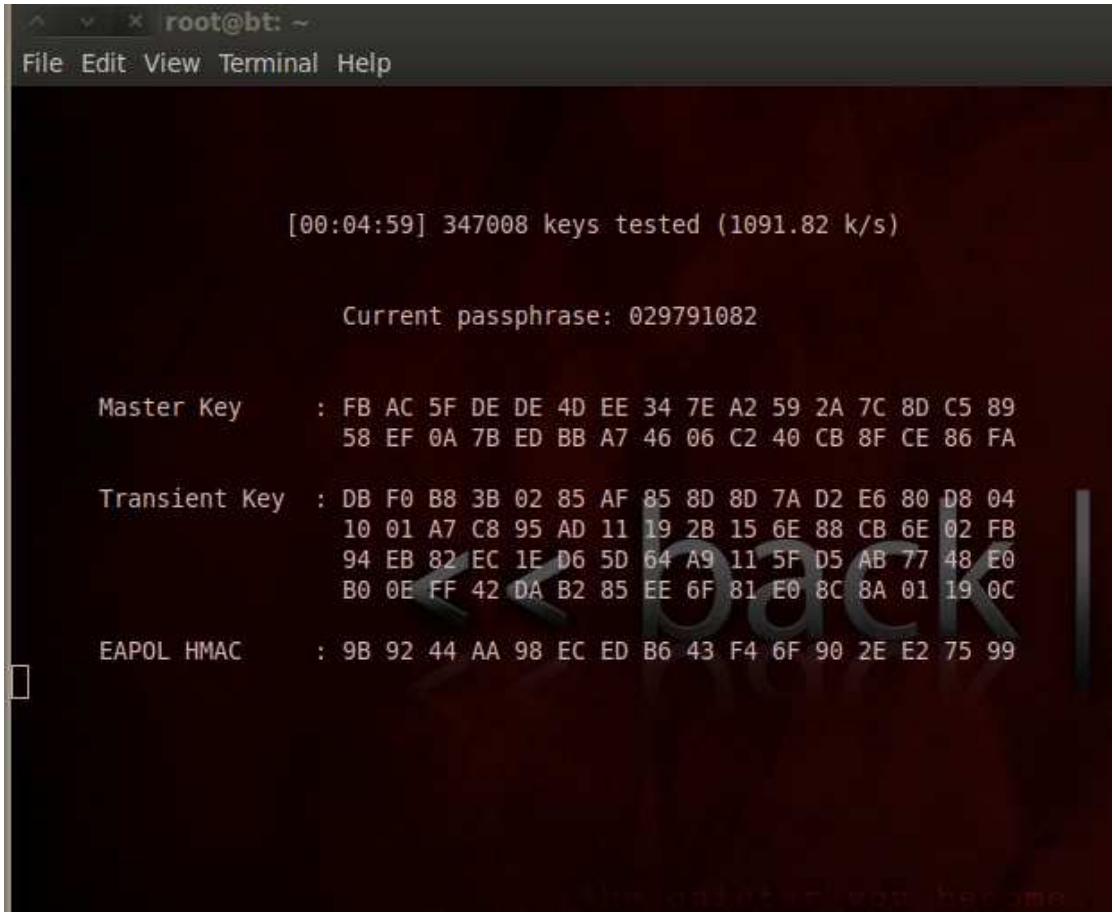
για να "σπάσετε" το pre-shared key. Σημαντικό είναι να καθορίσετε την λίστα με τους κωδικούς που έχετε στην κατοχή σας προκειμένου να γίνει μια προσπάθεια για την εύρεση του WPA key.



Εικόνα 177. Καθορισμός αρχείου για την εύρεση του WPA key

Εικόνα 178. Χρήση της Wordlist (uniq.txt) στο αρχείο crack-01.cap

Τέλος όπως μπορείτε να δείτε και παρακάτω, το πρόγραμμα ξεκίνησε να διατρέχει την λίστα (uniq.txt) για να βρει το κλειδί του δικτυού. Στο σημείο αυτό πρέπει να πούμε ότι δεν είναι απόλυτα σίγουρο ότι το WPA key θα βρεθεί από το πρόγραμμα. Για να γίνει αυτό πρέπει ο κωδικός του δικτύου να βρίσκετε μέσα στην καθορισμένη λίστα.



Εικόνα 179. Προσπάθεια εύρεσης WPA key

Εικόνα 180. Επιτυχής εύρεση WPA key

Επίλογος

Από την εργασία αυτή επιβεβαιώνεται ότι όλα τα μέτρα προστασίας πληροφοριακών συστημάτων και δικτύων παρέχουν ένα σχετικό και όχι απόλυτο βαθμό ασφαλείας. Κατά συνέπεια δε θα πρέπει ποτέ κανείς διαχειριστής να αγνοεί κανένα κίνδυνο και να αρκείται στην εφαρμογή ενός μόνο μέτρου ασφάλειας.

Ο συνδυασμός πολλών μέτρων ασφαλείας και η συνεχής αλλαγή κωδικών είναι ο καλύτερος τρόπος για να περιορίζεται στο ελάχιστο η τέλεση μιας κυβερνοεπίθεσης εναντίον ενός δικτύου ή ενός πληροφοριακού συστήματος.

Αν το παραπάνω θεωρείται πολυτέλεια σε ένα οικιακό δίκτυο ή οικιακό πληροφοριακό σύστημα με ευθύνη του ιδιοκτήτη τους, σε επιχειρηματικά πληροφοριακά και δικτυακά περιβάλλοντα εργασίας, είναι υποχρέωση του διαχειριστή να λάβει τα καλύτερα δυνατά μέτρα προστασίας τους από εσωτερικές και εξωτερικές επιθέσεις. Άλλωστε κανείς χρήστης ή διαχειριστής δεν πρέπει να ξεχνάει τη φράση…

Ό,τι κλειδώνει, ξεκλειδώνει!

7. Βιβλιογραφία

Abraham Silberschatz et al, Λειτουργικά Συστήματα, Ίων, 2005

Chris Brenton et al, Ασφάλεια δικτύων, Γκιούρδας, 2003

Manzuik Steve et al,Network security assessment: from vulnerability to patch, Rockland, Syngress, 2004

Mcclure et al, Ασφάλεια δικτύων, Γκιούρδας, 2009

Pejman Roshan, Jonathan Leary, 802.11 Wireless LAN fundamentals, Indianapolis, Cisco Press, 2004

Rappaport, Theodore, Ασύρματες επικοινωνίες, Γκιούρδας, 2006

Ross, John, Εισαγωγή στην ασύρματη δικτύωση, Κλειδάριθμος, 2009

Scambray Joel et al, Hacking exposed: web applications: web application security secrets and solutions, New York, McGraw-Hill, 2011

Stallings, William, Βασικές αρχές ασφάλειας δικτύων, Κλειδάριθμος, 2008

Stallings, William, Κρυπτογραφία και ασφάλεια δικτύων, Ίων, 2011

Tanenbaum A. S., Δίκτυα Υπολογιστών, Κλειδάριθμος, 2003

Tanenbaum A. S., Σύγχρονα Λειτουργικά Συστήματα, 2002

Καμπουράκης, Γιώργος, Ασφάλεια ασυρμάτων και κινητών δικτύων επικοινωνιών, Παπασωτηρίου, 2006

Κάτσικας Σ. et al, Ασφάλεια Πληροφοριακών Συστημάτων, Νέες Τεχνολογίες, 2004

Νικοπολιτίδης Π. et al, Ασύρματα δίκτυα, Κλειδάριθμος, 2006

Παπαδόπουλος Γ – Στεργιάκης Α, Κατασκευή Ασφαλούς Ασύρματου Σημείου Πρόσβασης και εγκατάσταση στο τμήμα Πληροφορικής, ΣΤΕΦ, ΤΕΙ Θεσσαλονίκης, 2006

Σουρής, Ανδρέας, Ασφάλεια της πληροφορίας, Νέες Τεχνολογίες, 2004

Πηγές διαδικτύου

https://forum.ubuntu-gr.org/viewtopic.php?f=9&t=3899

http://osix.net/modules/article/?id=455

http://en.wikipedia.org/wiki/Password_strength

http://www.aircrack-ng.org/doku.php

http://www.openwall.com

http://www.backtrack-linux.org/wiki/index.php/Main_Page

http://www.backtrack-linux.org/tutorials/