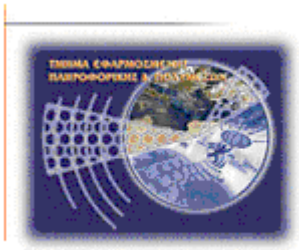
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Τίτλος: PASSWORD CRACKING

ΟΡΦΑΝΟΥΔΑΚΗΣ
ΦΑΝΟΥΡΙΟΣ ΑΜ 1756
E-mail: fdefrag@yahoo.gr

Ηράκλειο 13/03/2009

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

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

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή και επόπτη μου για την συγκεκριμένη πτυχιακή εργασία, τον κύριο Μανιφάβα καθώς η βοήθειά του στην διεκπεραίωση της συγκεκριμένης πτυχιακής έπαιξε σημαντικό ρόλο.

Εισαγωγή

Η πτυχιακή εργασία αναφέρεται στην χρησιμοποίηση κωδικών πρόσβασης σε υπολογιστικά συστήματα και τονίζει τον τρόπο χρησιμοποίησης τους ορθά και σωστά για την αποφυγή υποκλοπής τους. Σε καθημερινή βάση οι χρήστες των υπολογιστών χρησιμοποιούν τους κωδικούς τους ώστε να έχουν πρόσβαση σε mail, λογαριασμούς χρηστών, συναλλαγές με τράπεζες,, πιστωτικές κάρτες κτλ. Η ασφάλεια, όπως είναι φυσικό, είναι ένας πολύ σημαντικός παράγοντας για την διατήρηση και την χρήση αυτών των κωδικών . Θα αναφερθούμε αναλυτικότερα στην δημιουργία των λογαριασμών χρηστών με χρήση ασφαλών κωδικών στα λειτουργικά συστήματα Windows και Linux.
Επίσης γίνεται χρήση κάποιων κρυπτογραφικών εργαλείων ώστε να γίνει κατανοητό αφενός το πώς λειτουργούν αυτά τα προγράμματα και αφετέρου για να επισημανθεί το επίπεδο ασφάλειας των κωδικών.

ΕΥΧΑΡΙΣΤΙΕΣ **3**

ΕΙΣΑΓΩΓΗ **4**

ΚΕΦΑΛΑΙΟ 1 : **7**

ΕΙΣΑΓΩΓΗ ΣΤΟΥΣ ΚΩΔΙΚΟΥΣ ΠΡΟΣΒΑΣΗΣ **7**

1.1 Τι ειναι ο κωδικος 7
1.2 Passphrase & passcode 7
1.3 Παραγοντες για ασφαλεια κωδικου 8
προσβασης ενος συστηματος 8
1.4 Κυριες μεθοδοι επιθεσης 9
1.4.1 Αδύναμη κρυπτογράφηση (weak encryption) *9*
1.4.2 Κρυπτογράφηση από υποθέσεις (Guessing) *9*
1.5 Πως μπορω να βρω τους κωδικους προσβασης που αποθηκευονται στον υπολογιστη μου; 10
1.5.1 Που υπάρχουν τα Password file *10*
1.5.2 Cracks & Hacks *11*
1.6 Keyloggers 11

ΚΕΦΑΛΑΙΟ 2 : WINDOWS PASSWORDS: **13**

2.1 Αρχειο Κωδικων των WIN XP/2000 (SAM FILE) 13
2.2 Λογαριασμοι Χρηστων ενος Υπολογιστη. 14
Δημιουργια ενος Λογαριασμου Χρηστη. 14
2.3 Ανακτηση κωδικων στα XP/2000 20
2.3.1 Διαγραφή κωδικού χρήστη *20*
2.3.2 Αλλαγή κωδικού χρήστη μέσω του safe mode *24*
2.3.3 Δημιουργία δισκέτας μηδενισμού του κωδικού των XP *27*
2.3.4 Πρόσβαση σαν Administrator *30*

ΚΕΦΑΛΑΙΟ 3 LINUX PASSWORDS **32**

3.1 SHADOW PASSWORDS 33
3.1.1 Ενεργοποίηση Shadow passwords *33*
3.1.2 Πρόσβαση σαν root (Administrator) *36*
3.2 Ηλικια Password 39
3.3 Ορθη χρηση/τακτικη κωδικου προσβασης για την αποφυγη υποκλοπης του 40
3.3.1 Σωστή διαχείριση κωδικών *40*
3.3.2 Remember my Password *41*
3.4 ΠΕΡΙΕΧΟΜΕΝΑ ΤΩΝ PASSWD ΚΑΙ SHADOW FILES 43
3.4.1 /etc/passwd File *44*
3.4.2 /etc/shadow File *46*
3.5 PASSWORD LONGEVITY 47
3.6 Το menu GRUB 48
3.7. Ανακτηση κωδικου στα Linux (Ubuntu) 49
3.7.1 Reset root Password *49*
3.7.2 Ανάκτηση κωδικών root με Recovery Mode *53*
3.8 Η εντολη passwd 55

ΚΕΦΑΛΑΙΟ 4 PASSWORD STRENGTH **57**

4.1 BIT STRENGTH 57
4.2 Οδηγιες για δυνατους κωδικους 58
4.3 ΜΕΘΟΔΟΙ ΕΛΕΓΧΟΥ ΔΥΝΑΜΗΣ ΤΟΥ PASSWORD 60
4.3.1 PASSWORDMETER *60*
4.3.1 MICROSOFT PASSWORD CHECKER *62*
4.4 STRONG PASSWORD GENERATOR 63
4.5 ΚΛΕΙΔΩΜΑ ΑΡΧΕΙΩΝ & ΑΣΦΑΛΕΙΑ ΚΩΔΙΚΩΝ 64
4.5.1 PASSWORD SAFE *64*
4.5.2 Microsoft Private Folder *67*
4.6 Ασφαλεια κωδικων στο Διαδικτυο- Mozilla Firefox 69
4.6.1 Προστασία αποθηκευμένων κωδικών πρόσβασης χρησιμοποιώντας ένα κύριο κωδικό πρόσβασης (master password) *69*
4.6.2 Cracking Master Password *72*

ΚΕΦΑΛΑΙΟ 5 PASSWORD POLICY 74

5.1 ΜΗΚΟΣ ΚΑΙ ΣΧΗΜΑΤΙΣΜΟΣ ΤΟΥ PASSWORD 74
5.2 ΚΥΡΩΣΕΙΣ 74
5.3 ΕΠΙΛΟΓΗ ΕΝΟΣ ΚΑΤΑΛΛΗΛΟΥ PASSWORD POLICY 75
5.4 ΕΚΤΙΜΗΣΕΙΣ ΧΡΗΣΙΜΟΠΟΙΗΣΗΣ 76
5.5 ΠΑΡΑΔΕΙΓΜΑΤΑ PASSWORD POLICIES 77
5.5.1 Yahoo mail Policy 77
5.5.1 Hotmail Policy 78
5.6 PASSWORD POLICY 79
5.6.1 Επιβολή μιας πολιτικής (Policy) 79
5.6.2 Password Policy Enforcer 79

ΚΕΦΑΛΑΙΟ 6 ΧΡΗΣΗ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΕΡΓΑΛΕΙΩΝ 82

6.1 JOHN THE RIPPER 83
6.1.1 Single mode 85
6.1.2 Wordlist mode 85
6.1.3 Incremental mode 87
6.2 LOGIN ACCOUNTS ΣΤΑ UBUNTU: ΑΝΑΚΤΗΣΗ USERNAMES ΚΑΙ ΚΩΔΙΚΩΝ 89
6.3 OPHCRACK 96
6.4 CAIN & ABEL 102
6.4.1 ΕΓΚΑΤΑΣΤΑΣΗ ΣΕ WINDOWS 102
6.4.2 Εγκατάσταση Cain 103
6.4.3 Εγκατάσταση Abel 106
6.5 ΑΝΑΚΤΗΣΗ ΚΩΔΙΚΩΝ ΜΕΣΩ ΤΟΥ CAIN & ABEL 107
6.5.1 DICTIONARY ATTACK 109
6.5.2 BRUTE FORCE ATTACK 111
6.5.3 CRYPTANALYSIS ATTACK 114

ΚΕΦΑΛΑΙΟ 7 ΣΥΜΠΕΡΑΣΜΑΤΑ 115

ΒΙΒΛΙΟΓΡΑΦΙΑ 116

ΚΕΦΑΛΑΙΟ 1 :

ΕΙΣΑΓΩΓΗ ΣΤΟΥΣ ΚΩΔΙΚΟΥΣ ΠΡΟΣΒΑΣΗΣ

1.1 Τι είναι ο κωδικός

Ένας κωδικός πρόσβασης είναι μια λέξη ή μια σειρά χαρακτήρων που εισάγονται, συχνά μαζί με ένα όνομα χρήστη (user name), σε ένα υπολογιστικό σύστημα έτσι ώστε να μπορεί να συνδεθεί ο χρήστης ή να αποκτήσει πρόσβαση σε κάποιο πόρο. Οι κωδικοί πρόσβασης είναι μια κοινή μορφή επικύρωσης. Για πλήρης ασφάλεια απαιτείται ο κωδικός πρόσβασης να κρατιέται μυστικός από χρήστες στους οποίους δεν έχει δοθεί πρόσβαση.

Η χρήση των κωδικών πρόσβασης υπήρχε από τα αρχαία χρόνια. Οι σκοποί που φρουρούσαν μια θέση γνώριζαν έναν κωδικό πρόσβασης ή ένα σύνθημα που τους είχε δοθεί.. Θα επέτρεπαν πρόσβαση μόνο σε πρόσωπα τα οποία ήξεραν τον κωδικό. Στα σύγχρονα χρόνια, οι κωδικοί πρόσβασης χρησιμοποιούνται για να ελέγξουν την πρόσβαση σε προστατευμένα λειτουργικά συστήματα υπολογιστών, σε κινητά τηλέφωνα, σε αποκωδικοποιητές καλωδιακής τηλεόρασης, σε αυτοματοποιημένες μηχανές αφηγητών (ATMs), κ.λπ. Ένας χαρακτηριστικός χρήστης υπολογιστών μπορεί να χρειάζεται τους κωδικούς πρόσβασης για πολλούς λόγους: για να έχει πρόσβαση σε λογαριασμούς λειτουργικών συστημάτων, για να ανακτά το ηλεκτρονικό ταχυδρομείο από τους κεντρικούς υπολογιστές, να έχει πρόσβαση σε προγράμματα, σε βάσεις δεδομένων, σε δίκτυα, σε ιστοχώρους, ακόμη και να διαβάζει την εφημερίδα on-line.

Παρά το όνομα, δεν είναι αναγκαίο για τους κωδικούς πρόσβασης να είναι πραγματικές λέξεις. Οι κωδικοί πρόσβασης που δεν είναι πραγματικές λέξεις είναι πιο δύσκολο να βρεθούν από κακόβουλους χρήστες. Μερικοί κωδικοί πρόσβασης αποτελούνται από πολλές λέξεις και λέγονται passphrases. Ο όρος Passcode χρησιμοποιείται όταν οι μυστικές πληροφορίες προστατεύονται από αριθμούς, όπως ο προσωπικός αριθμός αναγνώρισης (PIN) που χρησιμοποιείται συνήθως για την πρόσβαση σε ATM. Οι κωδικοί πρόσβασης είναι γενικά σύντομοι ώστε να μπορούν να απομνημονευθούν.

1.2 Passphrase & passcode

Παρά το όνομα, δεν είναι αναγκαίο για τους κωδικούς πρόσβασης να είναι πραγματικές λέξεις. Οι κωδικοί πρόσβασης που δεν είναι πραγματικές λέξεις είναι πιο δύσκολο να βρεθούν από κακόβουλους χρήστες. Μερικοί κωδικοί πρόσβασης αποτελούνται από πολλές λέξεις και λέγονται passphrases. Ο όρος Passcode χρησιμοποιείται όταν οι μυστικές πληροφορίες προστατεύονται από αριθμούς, όπως ο προσωπικός αριθμός αναγνώρισης (PIN) που χρησιμοποιείται συνήθως για την πρόσβαση σε ATM. Οι κωδικοί πρόσβασης είναι γενικά σύντομοι ώστε να μπορούν να απομνημονευθούν.

Οι Passphrases χρησιμοποιούνται γενικά για την πιστοποίηση του δημόσιου/ιδιωτικού κλειδιού. Ένα σύστημα δημόσιου/ιδιωτικού κλειδιού καθορίζει την μαθηματική σχέση μεταξύ των δημόσιο κλειδί που είναι γνωστό σε όλους, και το ιδιωτικό κλειδί, το οποίο είναι γνωστό μόνο σε έναν χρήστη. Χωρίς την Passphrases για να ξεκλειδώσει το ιδιωτικό κλειδί, ο χρήστης δεν μπορεί να αποκτήσει πρόσβαση.

Οι Passphrases δεν χρησιμοποιούνται με τον ίδιο τρόπο όπως τα passwords. Μία Passphrase είναι μία εκτενέστερη έκδοση ενός password, και κατ' επέκταση είναι πιο ασφαλής. Μία Passphrase τυπικά αποτελείται από πολλαπλές λέξεις. Εξαιτίας αυτού, μία Passphrase είναι πιο ασφαλής ενάντια στις "dictionary attacks".

Μία καλή Passphrase είναι σχετικά μακριά και περιέχει ένα συνδυασμό κεφαλαίων και μικρών γραμμάτων και αριθμητικών και συμβολικών χαρακτήρων. Ένα παράδειγμα μίας καλής Passphrase είναι το εξής:
"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

Ένα passphrase είναι μια ακολουθία λέξεων ή άλλο κείμενο που χρησιμοποιείται για να ελέγξει την πρόσβαση σε ένα υπολογιστικό σύστημα, πρόγραμμα ή αρχείο. Το passphrase είναι παρόμοιο με έναν κωδικό πρόσβασης στη χρήση, αλλά είναι γενικά μακρύτερο και δυσκολότερο για επιπλέον ασφάλεια. Χρησιμοποιείται για να ελέγχει την πρόσβαση και τη λειτουργία σε κρυπτογραφικά προγράμματα και συστήματα. Το Passphrases χρησιμοποιείται ιδιαίτερα σε συστήματα που χρησιμοποιούν το passphrase ως κλειδί κρυπτογράφησης. Η σύγχρονη έννοια των passphrases θεωρείται για να έχει εφευρεθεί από τον Sigmund N. το 1982.

1.3 Παράγοντες για ασφάλεια κωδικού πρόσβασης ενός συστήματος

Η ασφάλεια ενός συστήματος που προστατεύεται από κωδικό πρόσβασης εξαρτάται από διάφορους παράγοντες. Το σύστημα πρέπει να σχεδιαστεί για την υγιή ασφάλεια, με την προστασία ενάντια στους ιούς υπολογιστών και την προστασία από κακόβουλους χρήστες. Εδώ είναι μερικά συγκεκριμένα διοικητικά ζητήματα κωδικού πρόσβασης που πρέπει να εξεταστούν, όπως ο βαθμός στο οποίο ένας επιτιθέμενος μπορεί να μαντέψει κωδικούς πρόσβασης

Ο βαθμός στον οποίο ένας επιτιθέμενος μπορεί να μαντέψει κωδικούς πρόσβασης του συστήματος είναι ένας βασικός παράγοντας της ασφάλειας συστημάτων. Μερικά συστήματα επιβάλλουν έναν χρόνο από αρκετά δευτερόλεπτα μετά από έναν μικρό αριθμό (π.χ., τρία) αποτυχημένων προσπαθειών εισόδων κωδικού πρόσβασης. Υπό άλλες συνθήκες όμως, τέτοια συστήματα μπορούν να είναι αρκετά ασφαλή με σχετικά απλούς κωδικούς πρόσβασης, εάν έχουν επιλεχτεί καλά και δεν μπορούν να μαντευτούν εύκολα..

Πολλά συστήματα αποθηκεύουν ή διαβιβάζουν κρυπτογραφικό hash του κωδικού πρόσβασης με έναν τρόπο που καθιστά τη hash αξία προσιτή σε έναν επιτιθέμενο. Όταν αυτό γίνεται, ένας επιτιθέμενος μπορεί να εργαστεί εκτός σύνδεσης, εξετάζοντας τους υποψήφιους κωδικούς ώστε να βρει τον πραγματικό κωδικό πρόσβασης. στην του αληθινού κωδικού πρόσβασης

Οι κωδικοί που χρησιμοποιούνται για να παράγουν κρυπτογραφικά κλειδιά, (π.χ. disk encryption ή ασφάλεια WI-FI) μπορούν επίσης να μαντευτούν εύκολα. Οι κατάλογοι κοινών κωδικών πρόσβασης είναι ευρέως διαθέσιμοι και μπορούν να καταστήσουν τις επιθέσεις κωδικού πρόσβασης πολύ αποδοτικές. Η ασφάλεια σε τέτοιες καταστάσεις εξαρτάται από την πολυπλοκότητα των κωδικών πρόσβασης ή passphrases που κάνει μια

τέτοια επίθεση υπολογιστικά ανέφικτη για τον επιτιθέμενο. Μερικά συστήματα, όπως PGP και Wi_Fi WPA εφαρμόζουν υπολογισμός-εντατικό hash στον κωδικό πρόσβασης για να επιβραδύνουν τέτοιες επιθέσεις.

Το Password cracking στην ουσία είναι η διαδικασία ανάκτησης κωδικών από αρχεία/δεδομένα που έχουν αποθηκευτεί σε ένα υπολογιστικό σύστημα. Μια κοινή προσέγγιση είναι να μαντεύονται συνεχώς κωδικοί με σκοπό την ταυτοποίηση και εύρεση του αναζητούμενου κωδικού πρόσβασης.. Σκοπός αυτού μπορεί να είναι η ανάκτηση ενός ξεχασμένου password από ένα χρήστη για να έχει πρόσβαση σε ένα σύστημα, για να ελέγξει τους εύκολα «σπασμένους» κωδικούς πρόσβασης.

1.4 Κύριες μέθοδοι επίθεσης

Υπάρχουν διάφορες μέθοδοι επίθεσης σε ένα υπολογιστικό σύστημα με σκοπό την υποκλοπή κωδικών ή την κακόβουλη μεταχείριση από άλλους χρήστες. Μερικές μέθοδοι είναι:

1.4.1 Αδύναμη κρυπτογράφηση (weak encryption)

Εάν ένα σύστημα χρησιμοποιεί μια αντιστρέψιμη λειτουργία για να αποκρύβει αποθηκεμένους κωδικούς, κάποιος κακόβουλος χρήστης μπορεί να εκμεταλλευτεί την αδυναμία αυτή και να μπορέσει να ανακτήσει ακόμη και τους δυνατούς κωδικούς πρόσβασης του συστήματος

1.4.2 Κρυπτογράφηση από υποθέσεις (Guessing)

Πολλοί κωδικοί πρόσβασης μπορούν να μαντευτούν είτε από ανθρώπους είτε από cracking programs που ενισχύονται με λεξικά και τις προσωπικές πληροφορίες του χρήστη.

Πολλοί χρήστες χρησιμοποιούν αδύνατους κωδικούς πρόσβασης, συνήθως κάτι σχετικό με τον εαυτό τους π.χ ημερομηνία γέννησης όνομα επίθετο κτλ. Όπως καταλαβαίνουμε αυτό αποτελεί εύκολη λεία για τα password cracking programs τα οποία δεν δυσκολεύονται να βρουν τον κωδικό.

Μερικοί χρήστες παραμελούν να αλλάξουν τον κωδικό πρόσβασης που τους δόθηκε με την αγορά μιας υπολογιστικής μονάδας ή μιας σύνδεσης κτλ.. Επίσης μερικές εταιρίες παραμελούν να αλλάξουν τους προεπιλεγμένους κωδικούς πρόσβασης παρέχονται από τον προμηθευτή λειτουργικών συστημάτων ή τον προμηθευτή υλικού. Ένα παράδειγμα είναι η χρήση FieldService με όνομα χρήστη την λέξη ‘’Guest” ως κωδικό πρόσβασης. Αν αυτός ο κωδικός παραμείνει σε ένα υπολογιστικό σύστημα τότε ένας τυχαίος χρήστης που θα έχει ασχοληθεί με τέτοια συστήματα θα έχει σπάσει ένα κωδικό πρόσβασης. Οι κατάλογοι προεπιλεγμένων κωδικών πρόσβασης είναι διαθέσιμοι στο διαδίκτυο και μπορεί ανά πάσα στιγμή να τους δει οποιοσδήποτε.

Τα προσωπικά στοιχεία ατόμων είναι πλέον διαθέσιμα από διάφορες πηγές, συνήθως από το internet, και συχνά λαμβάνονται από κάποιο άτομο που ασχολείται με την ασφάλεια αυτών

(πχ ελεγκτής ελέγχου ασφαλείας). Κάποιος που γνωρίζει το άτομο αυτό μπορεί να μαντέψει τον κωδικό του με αποτέλεσμα να δει και όλα τα προσωπικά στοιχεία που κατέχει το άλλο άτομο. Έπειτα μπορεί να χρησιμοποιήσει κάποιο cracking program το οποίο θα δεχτεί τις πληροφορίες σχετικά με τον επιτιθέμενο χρήστη και θα παράγει κοινές παραλλαγές των στοιχείων του ώστε να καταφέρει να βρει τους κωδικούς του.

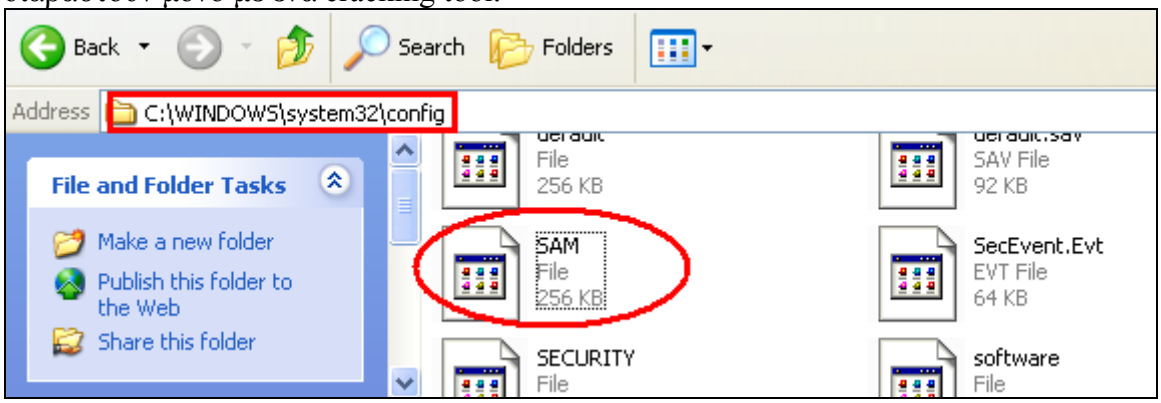
1.5 Πώς μπορώ να βρω τους κωδικούς πρόσβασης που αποθηκεύονται στον υπολογιστή μου;

Όλοι στηρίζονται σε κωδικούς πρόσβασης στον υπολογιστή μας, και επίσης να έχουμε πρόσβαση σε διάφορες υπηρεσίες στο Διαδίκτυο. Είτε πρόκειται για έναν κωδικό πρόσβασης σε έναν από τους λογαριασμούς ηλεκτρονικού ταχυδρομείου είτε για κάτι πιο σημαντικό, για παράδειγμα αυτό που μας δίνει πρόσβαση σε χρηματοοικονομικές πληροφορίες αν χαθεί ο κωδικός, μπορεί να είναι πολύ ενοχλητικό.

Ένας από τους καλύτερους τρόπους για να ανακτήσει κάποιος τον κωδικό πρόσβασης είναι η χρήση λογισμικού κατά τη δημιουργία κωδικών πρόσβασης που παρακολουθεί, έτσι ώστε αν τους χάσει, να μπορεί να τους ανακτήσει. Δυστυχώς, οι περισσότεροι άνθρωποι δεν έχουν καμία σχέση με αυτό το λογισμικό μέχρι να χαθεί ή να ξεχαστεί το password που έχουν χρησιμοποιήσει. Προγράμματα που διατίθενται για την ανάκτηση των κωδικών πρόσβασης περιλαμβάνουν: MDW Recovery, MSN Password Recovery ακόμα και χρησιμοποίηση του Password Manager του Firefox. Τέτοια προγράμματα μπορούν να βρεθούν στις παρακάτω διευθύνσεις:
http://www.nirsoft.net/password_recovery_tools.html
http://www.download3000.com/download_10777.html
http://www.sofotex.com/download/Security/Password_Recovery/

1.5.1 Που υπάρχουν τα Password file

Σε όλα τα λειτουργικά συστήματα, τα στοιχεία αποθηκεύονται σε μια βάση δεδομένων με συγκεκριμένο όνομα και σε συγκεκριμένη θέση μέσα στο filesystem. Η δομή των αρχείων αυτών είναι συγκεκριμένη ώστε να μπορούν όλα τα προγράμματα να έχουν πρόσβαση σε αυτή τη βάση, όποτε χρειαστεί.Το αρχείο που αποθηκεύονται όλοι οι κωδικοί λέγεται SAM file και βρίσκεται στο C:\WINDOWS\system32\config\sam.
Όλοι οι κωδικοί που βρίσκονται σε αυτό το αρχείο είναι κρυπτογραφημένοι και μπορούν να διαβαστούν μόνο με ένα cracking tool.



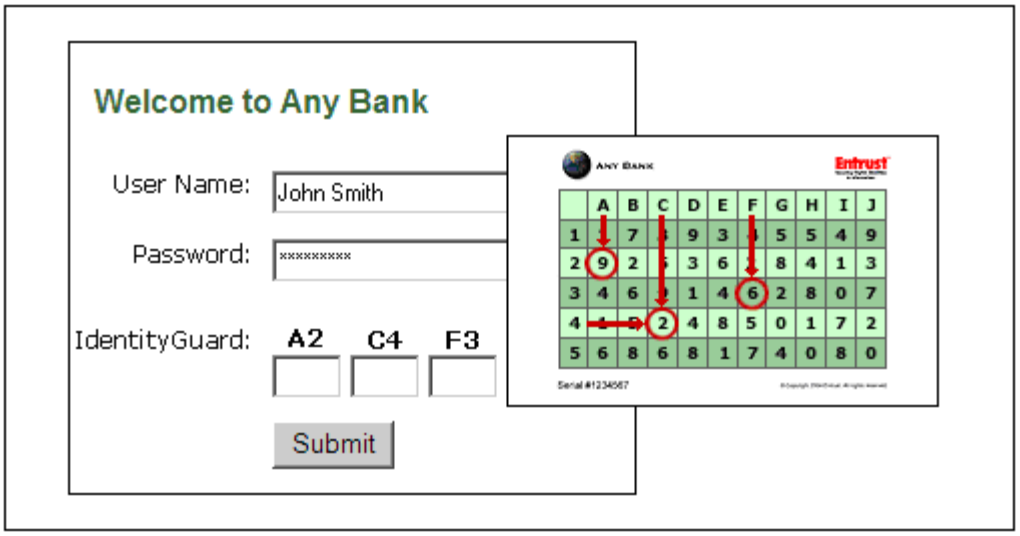
1.5.2 Cracks & Hacks

Οι μέθοδοι αυτές είναι συνήθως παράνομες, ειδικά αν κάποιος προσπαθεί να βρει κάποιους κωδικούς πρόσβασης που δεν είναι δικοί του. Ενώ το Internet προσφέρει αυτό το είδος λογισμικού, αυτό πρέπει να χρησιμοποιείται σωστά και με ενημέρωση για τον χρήστη. Συχνά, αυτά τα cracks και κατεβάζοντας διάφορα hacks μπορεί επίσης να είναι είδη «δούρειων ίππων», είτε virus, κ.λπ.
Η διαφορά σε αυτούς τους δύο όρους (cracking και hacking) δεν είναι γνωστή στη μεγαλύτερη μερίδα του πληθυσμού. Στην ουσία το cracking είναι εκείνο το οποίο έχει καταστροφικές διαθέσεις. Ένας hacker δεν εστιάζει στο να υποκλέψει κωδικούς και πληροφορίες ώστε να τα χρησιμοποιήσει εναντίον κάποιου. Αντίθετα μάλιστα, hacker είναι κάποιος που συλλέγει γνώση για ένα λογισμικό, κερδίζει πρόσβαση σε σημεία που ένας χρήστης δεν ξέρει ή δεν μπορεί να έχει και βάση των γνώσεών του το επεκτείνει δίνοντας του νέες δυνατότητες ή επεκτείνοντας τα προβλήματά του (bugs). Από την άλλη πλευρά cracker είναι κάποιος που κερδίζει πρόσβαση παράνομα, ξεπερνώντας συστήματα ασφαλείας με σκοπό να βλάψει το λογισμικό ή το σύστημα το οποίο έχει στοχεύσει.

1.6 Keyloggers

Ένας άλλος τρόπος για να ανακτηθεί ένας αποθηκευμένος κωδικός πρόσβασης από τον υπολογιστή είναι να χρησιμοποιηθεί ένας keylogger. Τα keylogger λειτουργούν στο παρασκήνιο, και μπορεί ο χρήστης να επιστρέψει και να δει τον κωδικό πρόσβασης. Στην ουσία βλέπουν τον κωδικό τον οποίο πληκτρολόγησε ο χρήστης μέσω των κουμπιών του πληκτρολογίου τα οποία πάτησε. Καταγράφουν όλες τις πληροφορίες που πληκτρολογεί ένας χρήστης και στη συνεχεία στέλνουν αυτές τις πληροφορίες. Είναι πολύ επικίνδυνα και μπορούν να χρησιμοποιηθούν για να κλέψουν προσωπικά στοιχεία όπως ο αριθμός πιστωτικής κάρτας, καθώς και τους κωδικούς πρόσβασης. Τα Keyloggers είναι ιδιαιτέρα επικίνδυνα για όλους όσους χρησιμοποιούν ηλεκτρονικούς δικτυακούς τόπους μέσω των οποίων γίνονται χρηματικές συναλλαγές.

-Παράδειγμα keylogger-



Η Ανίχνευση ενός keylogger δεν είναι εύκολη υπόθεση. Μπορεί να εγκατασταθεί σε πάρα πολλές θέσεις στον υπολογιστή και συνήθως βρίσκεται σε ένα από τα αρχεία του συστήματος. Ωστόσο, υπάρχει ένας εύκολος τρόπο για να βρεθεί αν ένα keylogger είναι σε λειτουργία η όχι. Κάνοντας δεξί κλικ στη γραμμή μενού και έπειτα στο Task Manager. Εξετάζοντας όλες τις διεργασίες που εκτελούνται εκείνη τη στιγμή προσπαθούμε να βρούμε αν κάποια διεργασία μας φαίνεται ύποπτη. Φυσικά αυτό προϋποθέτει την γνώση των διεργασιών του υπολογιστή μας . Υπάρχει ένα πρόγραμμα που ονομάζεται Security Task Manager το οποίο ελέγχει τις διεργασίες που εκτελούνται στον υπολογιστή. Αυτό μπορεί να ειδοποιήσει τιν χρήστη για τις ύποπτες κινήσεις που βλέπει στο task manager. Το εν λόγω πρόγραμμα μπορεί να βρεθεί στην διεύθυνση:
http://www.neuber.com/taskmanager/index.html

Επίσης υπάρχει ένα άλλο πρόγραμμα το οποίο εξασφαλίζει πλήρη προστασία από κάθε γνωστό και άγνωστο keylogger. Αντί να τα κυνηγάει βάσει ενημερώσεων και πάλι να μην ξέρει τα εντελώς καινούργια, αποκλείει τους τρόπους λειτουργίας των keyloggers.
Έτσι με το να προστατεύει την γραμμή μετάδοσης της πληροφορίας, από το πληκτρολόγιο ως το μόνιτορ, αποκλείει την δράση κάθε keylogger που μπορεί να έχει ο υπολογιστής. Λειτουργεί σε όλα τα windows. εκτός των vista . Το εν λόγω πρόγραμμα μπορεί να βρεθεί στη παρακάτω διεύθυνση σε trial έκδοση:

http://www.amictools.com/download/AntiKeyloggerShieldSetup.exe

-Anti keylogger-

ΚΕΦΑΛΑΙΟ 2 : Windows Passwords:

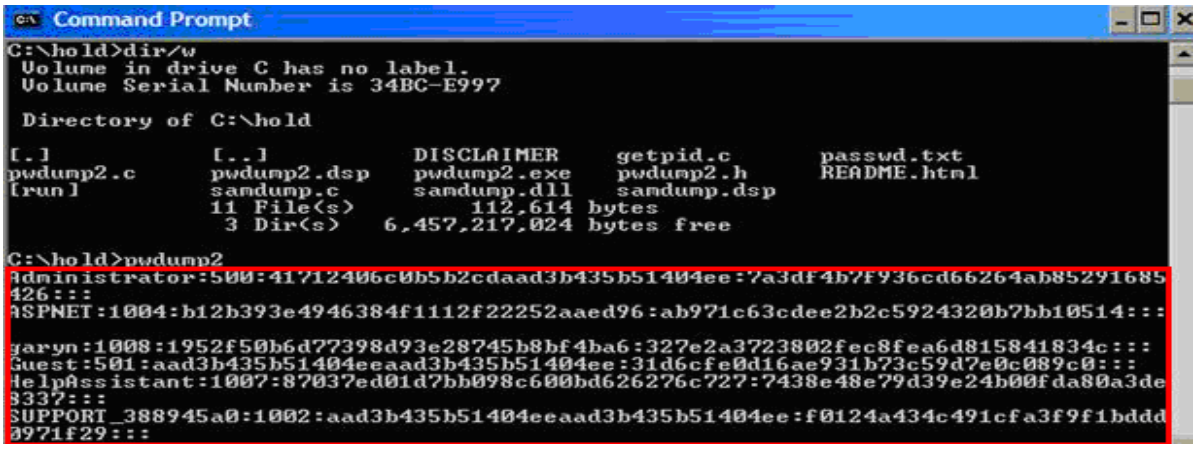
2.1 Αρχείο Κωδικών των WIN XP/2000 (SAM FILE)

Τα windows από την γενιά των 2000 και έπειτα αποθηκεύουν τους κωδικούς των χρηστών (πχ administrator , userX , guest) σε ένα αρχείο που καλείται sam file (Security Accounts Manager). Το εν λόγω αρχείο βρίσκεται στους φακέλους του συστήματος των windows και δεν μπορεί να διαβαστεί παρά μόνο με την χρήση κάποιων cracking tools. Επίσης δεν μπορεί να αντιγραφεί ή να αποκοπεί όση ώρα λειτουργούν τα Windows, ούτε από τον Adminstrator.Μπορεί να βρεθεί στη διαδρομή C:\WINDOWS\system32\config\sam. Εκτός αυτού μπορεί να υπάρξει και στο φάκελο C:\WINDOWS\repair εάν έχει χρησιμοποιηθεί το NT Repair Disk Utility και δεν το έχει διαγράψει ο administrator. Για να διαβάσει κάποιος τα παραπάνω αρχείο, πρέπει με κάποιο τρόπο να αποκτήσει πρόσβαση στον δίσκο. Ο καλύτερος τρόπος για να γίνει αυτό είναι πχ να χρησιμοποιηθεί κάποια δισκέτα η CD που κάνει απευθείας εκκίνηση τον H/Y (bootable) παρακάμπτοντας τελείως το φάκελο εκκίνησης των Windows. Συνήθως , αυτή η δισκέτα στηρίζεται στης διαδικασίες boot από κάποιο λειτουργικό σύστημα open source , (πχ Linux).Τα περιεχόμενα του sam, σε περίπτωση που μπορεί να έχει κάποιος πρόσβαση σε αυτό θα είναι κάπως έτσι:

```
Administrator:500:73CC402BD3E791756C3D3B817E02809D:C7E2622D76D3F001CF08B0753646BBCC:::

fredc:1011:3466C2B0487FE39A417EAF50CFAC29C3:80030E356D15FB1942772DCFD7DD3234:::

Guest:1000:89D42A44E77140AAAAD3B435B51404EE:C5663434F963BE79C8FD99F535E7AAD8:::

william:1012:DBC5E5CBA8028091B79AE2610DD89D4C:6B6E0FB2ED246885B98586C73B5BFB77:::
```

Αυτό μας δείχνει ότι το αρχείο μπορεί να περιέχει τους κωδικούς των accounts αλλά είναι όλοι κωδικοποιημένοι και έτσι ακόμα και σε περίπτωση που ανοιχτεί δεν μπορεί να γίνει κατανοητό το περιεχόμενό του χωρίς την χρήση κάποιου cracking tool.

-Παράδειγμα περιεχομένων SAM FILE-



2.2 Λογαριασμοί Χρηστών ενός Υπολογιστή.

Δημιουργία ενός Λογαριασμού Χρήστη.

Πολλές φορές έναν υπολογιστή τον χρησιμοποιούν περισσότεροι του ενός χρήστες. Τότε είναι δυνατόν τα αρχεία του ενός να μπλέκονται με τα αρχεία του άλλου ή ο ένας να μην θέλει να βλέπει ο άλλος τα αρχεία που δημιουργεί. Το πρόβλημα αυτό λύνεται με την δημιουργία «λογαριασμών» των χρηστών. Έτσι για κάθε έναν χρήστη δημιουργείται ένα περιβάλλον σαν να είναι μοναδικός χρήστης του υπολογιστή. Η εναλλαγή των χρηστών είναι εύκολη και ο ένας δεν μπορεί να μπει στο περιβάλλον του άλλου αν δεν γνωρίζει το όνομα χρήστη και τον κωδικό πρόσβασης, εάν βεβαίως έχει δημιουργηθεί. Το όνομα χρήστη πρέπει να είναι μοναδικό για τον υπολογιστή. Δηλαδή δεν επιτρέπεται δύο χρήστες να έχουν το ίδιο όνομα. Επίσης τον ίδιο ισχύει και για τον κωδικό πρόσβασης. Κάθε χρήστης έχει τον δικό του κωδικό τον οποίο πρέπει να πληκτρολογεί για να μπει στο λειτουργικό σύστημα.

Κατά την εγκατάσταση των Windows XP αυτόματα δημιουργείται ένας λογαριασμός του Administrator(του διαχειριστή). Πολλές φορές καθορίζεται κωδικός πρόσβασης για τον διαχειριστή κατά την εγκατάσταση. Εάν δεν ορισθεί τέτοιος κωδικός, τότε όταν γίνεται εκκίνηση του υπολογιστή μπαίνουμε αυτόματα στο λειτουργικό σύστημα του υπολογιστή, διαφορετικά πρέπει να τον πληκτρολογήσουμε. Ο συγκεκριμένος λογαριασμός μας παρέχει την δυνατότητα πρόσβασης στις ρυθμίσεις του υπολογιστή, των προγραμμάτων αλλά και των περιεχομένων του υπολογιστή.

Εκτός από τον λογαριασμό του **Administrator** στον υπολογιστή υπάρχει και ο λογαριασμός του **τοπικού χρήστη (Local User).** Και αυτός ο λογαριασμός δημιουργείται από τον διαχειριστή κατά την εγκατάσταση. Αφού δημιουργηθεί ο λογαριασμός ορίζουμε τα αρχεία και ο τους φακέλους στα οποία ο χρήστης θα έχει πρόσβαση. Λογαριασμούς χρηστών μπορεί να δημιουργεί μόνον ο Administrator και να ορίζει τον τύπο κάθε ενός λογαριασμού. Τύποι λογαριασμών υπάρχουν δύο, ο Computer Administrator και ο Limited. Ο λογαριασμός Computer Administrator μας παρέχει τις εξής δυνατότητες:

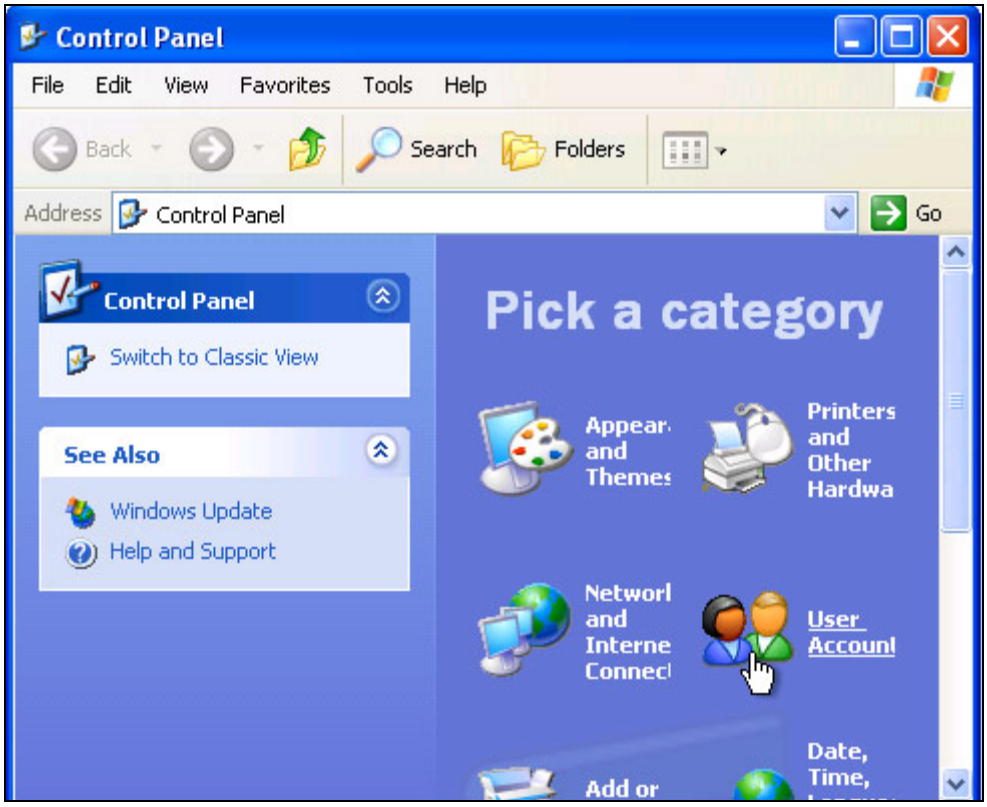
- Να δημιουργούμε και να διαγράφουμε λογαριασμούς χρηστών.
- Να ορίζουμε κωδικούς πρόσβασης για άλλους λογαριασμούς χρηστών.
- Να αλλάζουμε τα ονόματα, τις εικόνες και τους κωδικούς πρόσβασης άλλων χρηστών αλλά και τον τύπο του λογαριασμού τους.
- Δεν μπορούμε να αλλάξουμε τον τύπο του λογαριασμού μας από Computer Administrator σε Limited εκτός αν υπάρχει και άλλος λογαριασμός με τύπο Computer Administrator.
- Ο λογαριασμός με τύπο Limited μας παρέχει τις εξής δυνατότητες:

- Μπορούμε να αλλάξουμε την εικόνα του λογαριασμού μας και να ορίσουμε ή να αλλάξουμε τον κωδικό μας πρόσβασης.
- Δεν μπορούμε να εγκαταστήσουμε προγράμματα ή νέο Hardware.
- Δεν μπορούμε να αλλάξουμε το όνομα και τον τύπο του λογαριασμού μας.

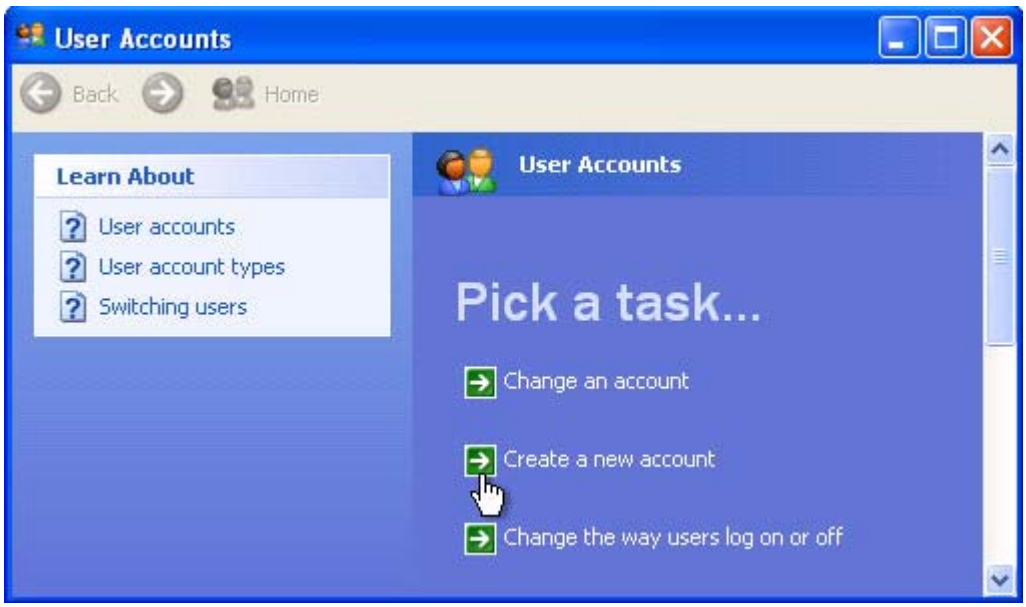
Όπως σε κάθε ενέργεια στα Windows έτσι και για τη δημιουργία χρήστη υπάρχουν πολλοί τρόποι. Ένας από αυτούς ο πιο απλός είναι ο εξής:

- Ανοίγουμε το παράθυρο του **Control Panel.**

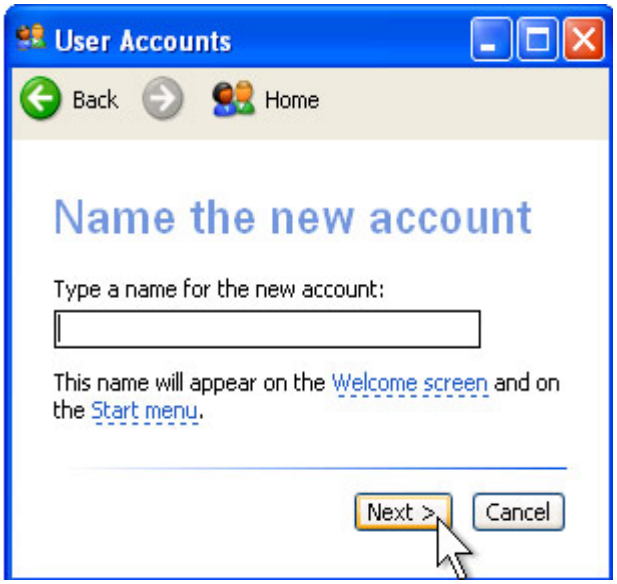
- Από την κατηγορία **Pick a category** επιλέγουμε την **User Accounts**.



- Από την ενότητα **Pick a task…** επιλέγουμε την **Create a new account**.



- Ανοίγει το παράθυρο **Name the new account** στο οποίο υπάρχει η θέση όπου θα γράψουμε το όνομα χρήστη του λογαριασμού που δημιουργούμε. Και αφού το γράψουμε πατάμε **Next.**



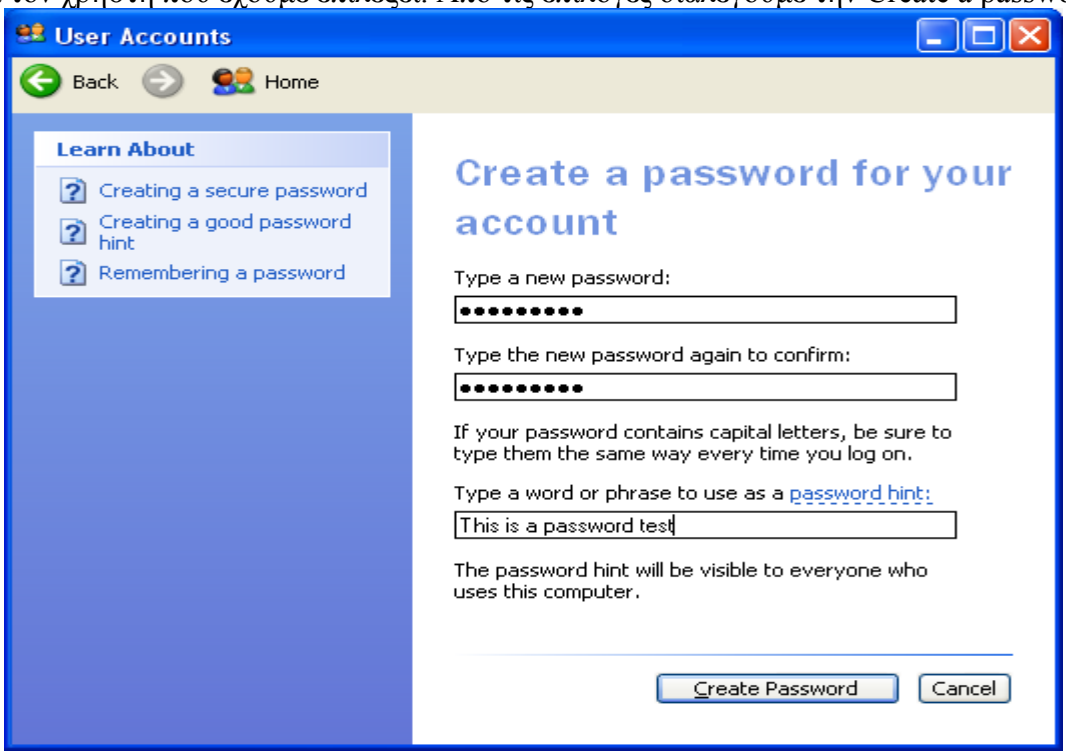
- Στο νέο παράθυρο **Pick an account type** επιλέγουμε τον τύπο του λογαριασμού, κάνοντας κλικ στον κύκλο δίπλα στον αντίστοιχο τύπο.

- Κατόπιν πατάμε στο πλήκτρο **Create Account.**
- Τέλος κλείνουμε το παράθυρο του **User Accounts** και το παράθυρο του **Control Panel.**

Όπως βλέπουμε με τη δημιουργία του νέου λογαριασμού δεν μας ζητήθηκε να ορίσουμε κωδικό πρόσβασης. Αυτός καθορίζεται μετά τη δημιουργία του λογαριασμού.

Η διαδικασία καθορισμού του κωδικού πρόσβασης είναι η εξής:
Από το παράθυρο User Accounts του Control Panel και στην κατηγορία or pick an account to change επιλέγουμε τον λογαριασμό χρήστη. Εμφανίζεται το παράθυρο What do you want to change about account?

Για τον χρήστη που έχουμε επιλέξει. Από τις επιλογές διαλέγουμε την Create a password.



Τότε ανοίγει το παράθυρο **Create a password for account** .Γράφουμε τον κωδικό που θέλουμε στο πρώτο πλαίσιο, τον επαναλαμβάνουμε στο δεύτερο και για να ολοκληρώσουμε τη διαδικασία πατάμε στο πλήκτρο **Create Password** και κλείνουμε το παράθυρο. Για να εναλλάξουμε τους χρήστες ενός υπολογιστή αρκεί να κάνουμε κλικ στην **Έναρξη (Start)** και να επιλέξουμε **Log off**. Στο παράθυρο **Log Off Windows** επιλέγουμε **Switch User** και από εκεί επιλέγουμε το λογαριασμό που επιθυμούμε. Γράφουμε τον κωδικό πρόσβασης και πατάμε το πλήκτρο **Enter** του πληκτρολογίου για να μπούμε στο λογαριασμό.

Γενικά τα passwords δεν αποθηκεύονται κάπου ώστε να μπορεί κάποιος να τα βρει. Τα passwords και οι ρυθμίσεις του λογαριασμού μας, αποθηκεύονται στο c:\windows\system32\configure\sam σαν SAM αρχεία. Αυτός ο φάκελος περιέχει hashed κώδικες οι οποίοι δεν έχουν κάποιον αλγόριθμο αποκρυπτογράφησης. Όσο τρέχει το λειτουργικό σύστημα δεν μπορούμε να μετακινήσουμε ή να αλλάξουμε αυτό το φάκελο.

Εάν ένας κωδικός πρόσβασης είναι αδύνατος, μπορεί μερικές φορές να ανακτηθεί χρησιμοποιώντας μια dictionary attack- δηλ., παράγοντας ασφαλή hashes ενός μεγάλου καταλόγου λέξεων και ελέγχοντας εάν οποιοιδήποτε από αυτούς αντιστοιχούν στο SAM Το εν λόγω αρχείο είναι ορατό , μόνο όταν ξεκινάνε τα windows. Μετά το login , όχι απλώς παραμένει κρυφό , άλλα πραγματικά εξαφανίζεται τελείως από το σκληρό μας δίσκο.

2.3 Ανάκτηση κωδικών στα XP/2000

Υπάρχουν οι εξής επιλογές για τον χρήστη.

1. Να διαγραφεί τελείως ο κωδικός του (password resetting)
2. Να γίνει πλήρη ανάκτηση του κωδικού.(password retrieval)

Η διαφορές των δύο μεθόδων είναι προφανείς. Η πιο σημαντική διαφορά όμως είναι ότι στον πρώτο τρόπο γίνεται επέμβαση στο Sam File των Windows , που συνεπάγεται τροποποίηση του αρχείου , δηλαδή ο χρήστης το δοκιμάζει με δική του ευθύνη. Αντίθετα στην δεύτερη περίπτωση γίνεται απλώς ανάγνωση του αρχείου κωδικών , για να ακολουθήσει η αποκωδικοποίηση αυτών με προγράμματα τρίτων κατασκευαστών που κυκλοφορούν

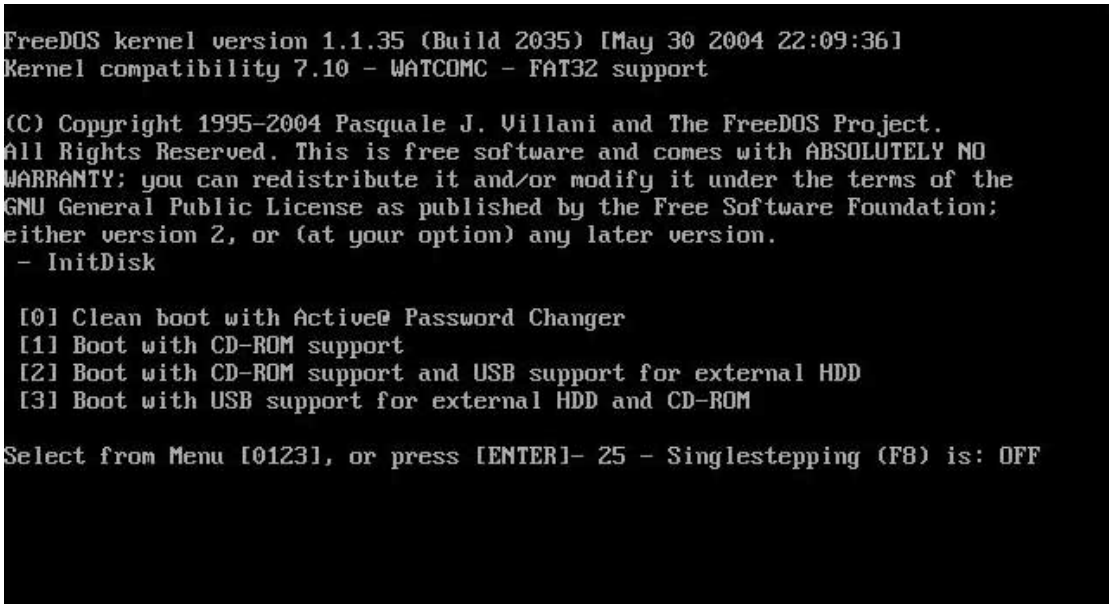
Σε πολλές περιπτώσεις ο χρήστης μπορεί να ξεχάσει τον κωδικό πρόσβασής του λογαριασμού του και έτσι να μην έχει πρόσβαση στα αρχεία του.

Υπάρχουν διάφοροι τρόποι οι οποίοι μπορούν να χρησιμοποιηθούν για την ανάκτηση του κωδικού. Μερικοί από αυτούς περιγράφονται παρακάτω.

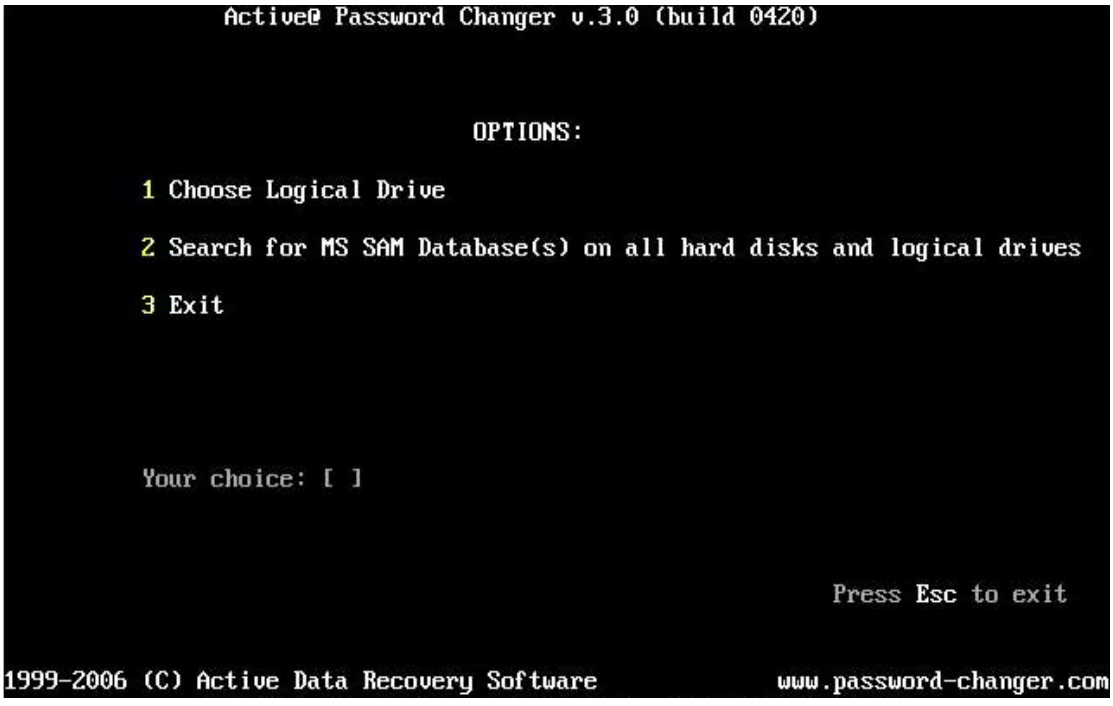
2.3.1 Διαγραφή κωδικού χρήστη

Για να γίνει αυτό , πρέπει να εκκινήσουμε τον Η/Υ με κάποιο CD η δισκέτα που δεν είναι βασισμένη στα windows. Ένα αρκετά δημοφιλές πρόγραμμα είναι το Active Password Changer (http://www.password-changer.com/). Αφού κατεβάσουμε το αρχείο το γράφουμε σε ένα CD ώστε να είναι bootable (μπορεί δηλαδή να εκκινήσει τον Η/Υ από μόνο του).

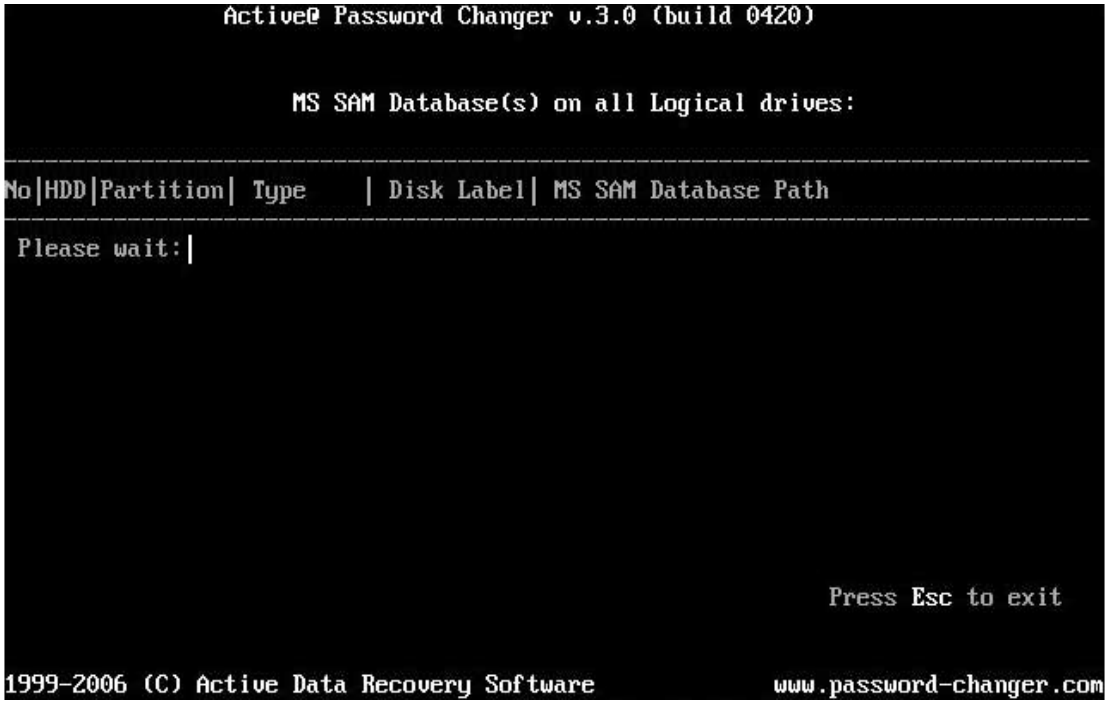
Μετά την εκκίνηση του Η/Υ (και ενώ ακόμα είμαστε σε dos mode) τρέχει αυτόματα η εφαρμογή «Active Password Changer».



Πατάμε τα 0 ώστε ο υπολογιστής μας να bootάρει από το Active Password Changer. Έπειτα μας εμφανίζονται 3 επιλογές:

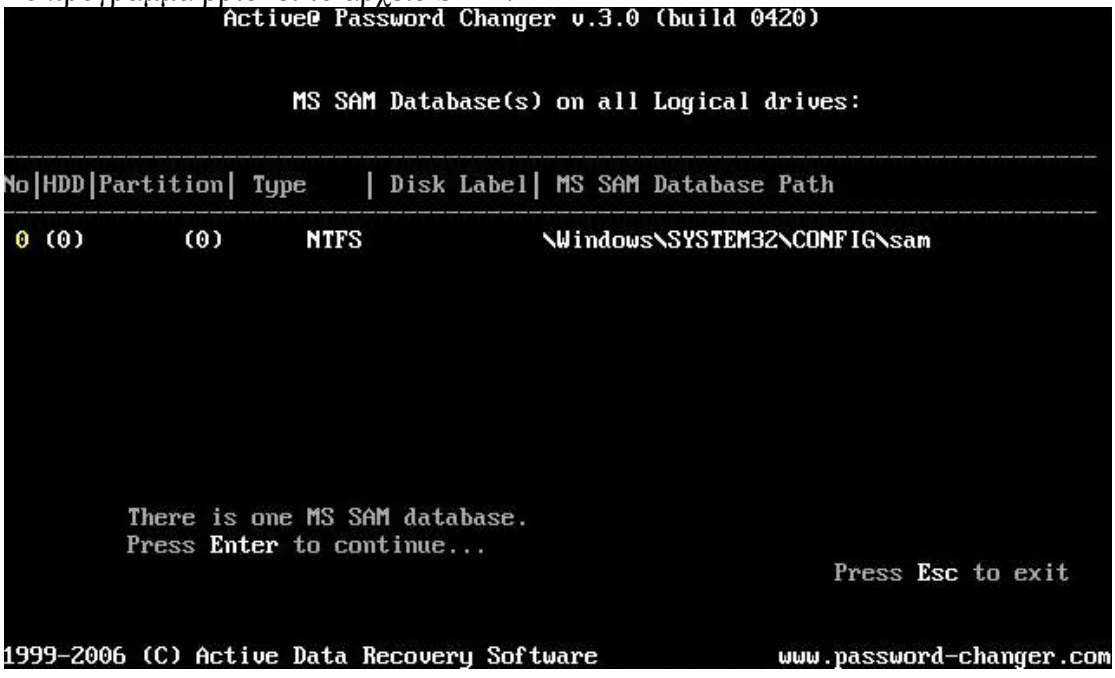


Από αυτές, επιλέγοντας την 2η, ο υπολογιστής μας αρχίζει να ψάχνει τις βάσεις δεδομένων αρχείων SAM, στις οποίες είναι καταχωρημένες οι πληροφορίες για τον λογαριασμό του χρήστη.



Σε περίπτωση που έχουμε παραπάνω από ένα λειτουργικά εγκατεστημένα στον υπολογιστή, τότε το πρόγραμμα θα μας εμφανίσει περισσότερα sam files.

Το πρόγραμμα βρίσκει το αρχείο SAM:



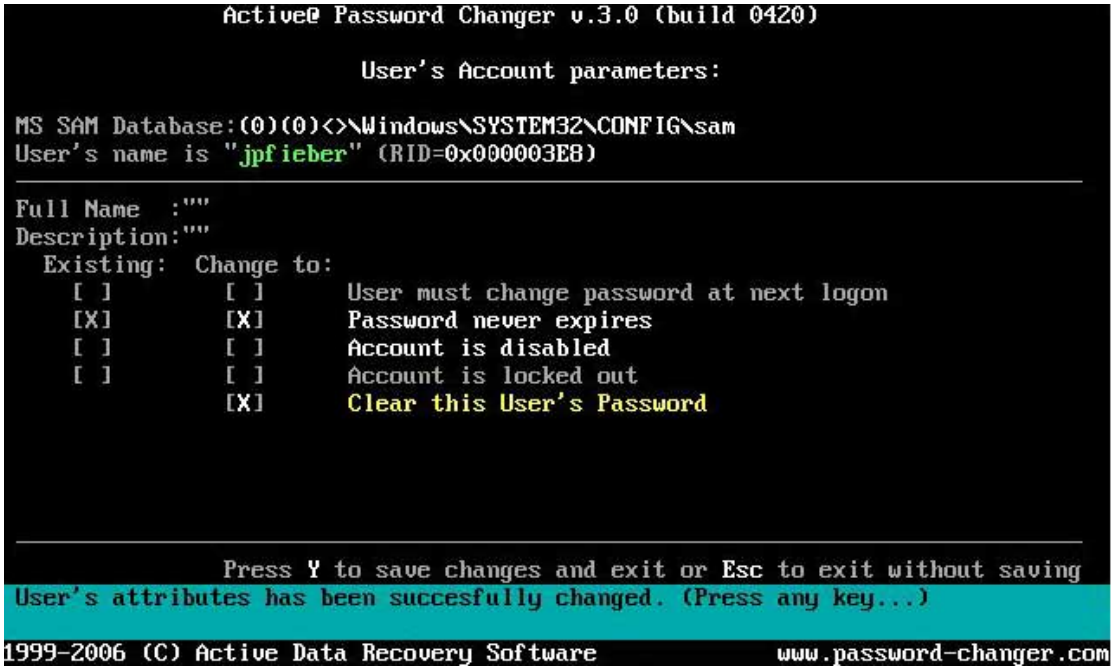
Έπειτα δείχνει στον χρήστη τους λογαριασμούς χρηστών οι οποίοι υπάρχουν στη βάση δεδομένων του συγκεκριμένου αρχείου SAM:

Σε περίπτωση που στον υπολογιστή υπάρχει ένας μόνο λογαριασμός χρήστη, τότε στη οθόνη θα μας εμφανίσει 3 λογαριασμούς: του Administrator, του Guest και τον δικό μας.

Το πρόγραμμα μας δίνει την δυνατότητα είτε να κάνουμε reset τον κωδικό του χρήστη που επιλέξαμε είτε να τον αλλάξουμε, βάζοντας ένα "X" στην επιλογή που θέλουμε.

Το πρόγραμμα θα αλλάξει τον λογαριασμό του χρήστη, απλά «καθαρίζοντας» τον κωδικό του:

Μόλις τελειώσει η διαδικασία, το πρόγραμμα θα μας ενημερώσει ότι έγινε η αλλαγή και ότι ο κωδικός είναι κενός.

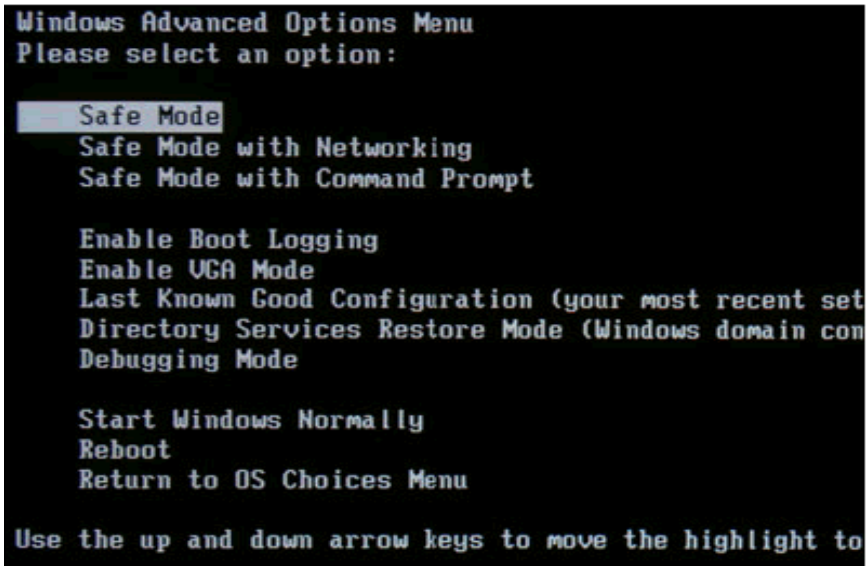


Είναι προτιμότερο να γίνεται reset του κωδικού (Clear this user password) και ο νέος κωδικός να εισάγεται από τα Windows , αφού κάνουμε login, για λόγους ασφαλείας.

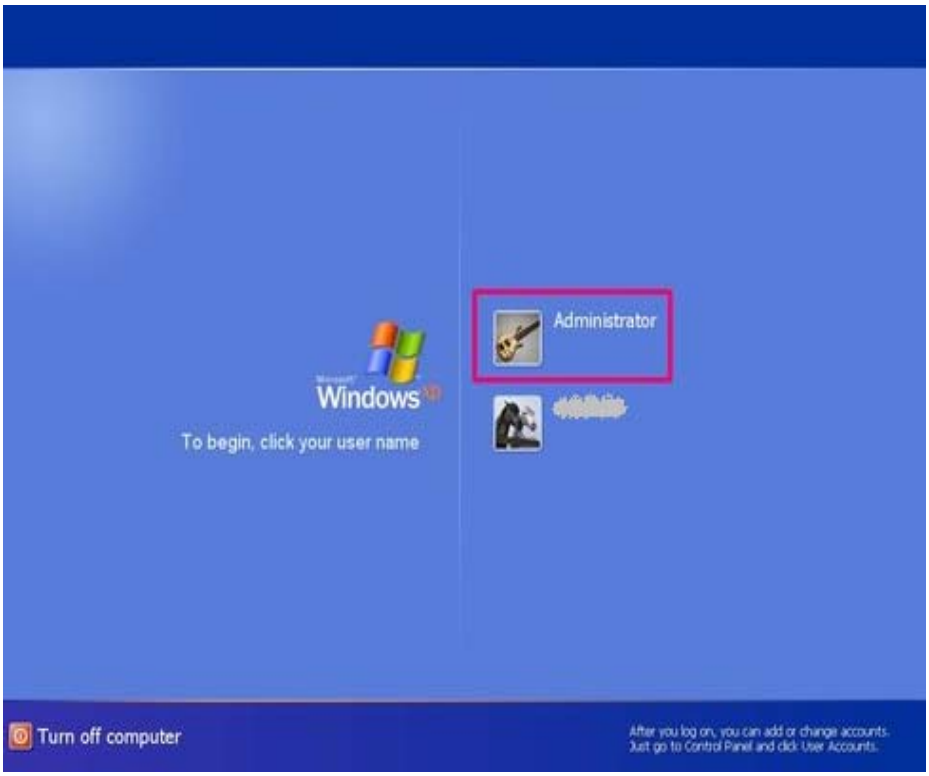
2.3.2 Αλλαγή κωδικού χρήστη μέσω του safe mode

Σε περίπτωση που θέλουμε να εισέλθουμε σε ένα σύστημα και δεν έχουμε τον κωδικό πρόσβασης μπορούμε να κάνουμε τα εξής:

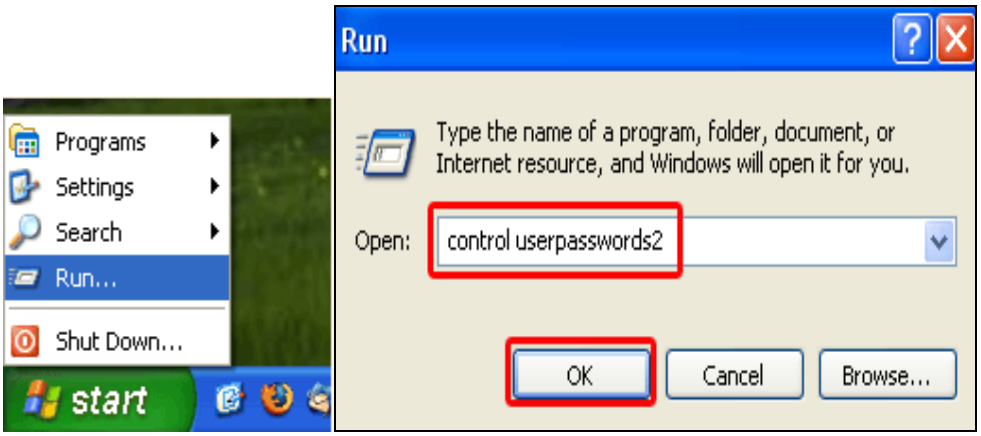
- Κάνουμε Επανεκκίνηση του υπολογιστή
- Όταν bootάρει στην αρχή πατάμε F8 και επιλέγουμε "**Safe Mode**"



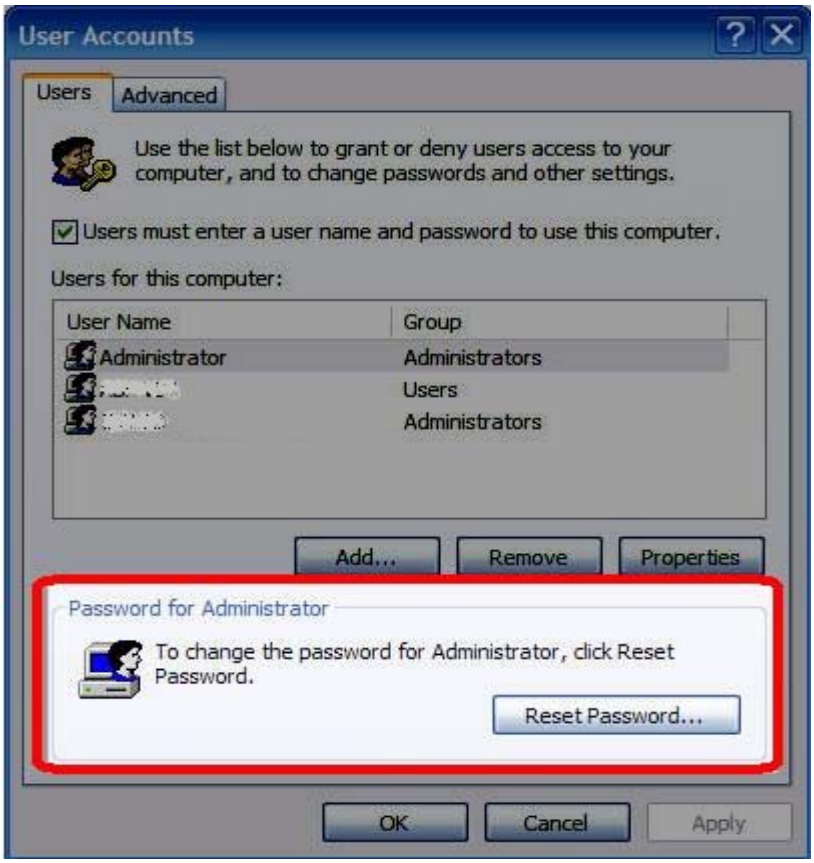
1. Αφού εισέλθουμε στο login menu συνδεόμαστε σαν Administrator και παρατηρούμε ότι δε μας ζητάει κωδικό



2. Πατάμε Έναρξη>Εκτέλεση και πληκτρολογούμε cmd. Μας εμφανίζεται το command prompt των Windows. Γράφουμε control userpasswords2



3. Επιλέγουμε το account του Administrator και πατάμε το Reset Password.

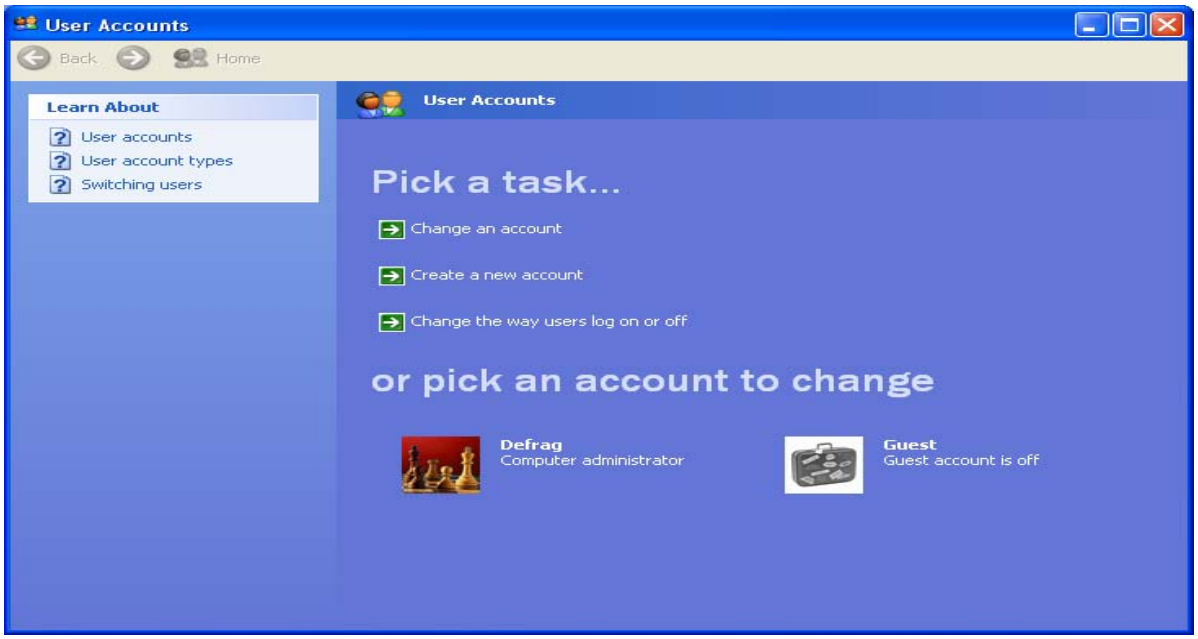


4. Πληκτρολογούμε τον καινούργιο κωδικό που θέλουμε στο New Password και Confirm New Password και πατάμε οκ.

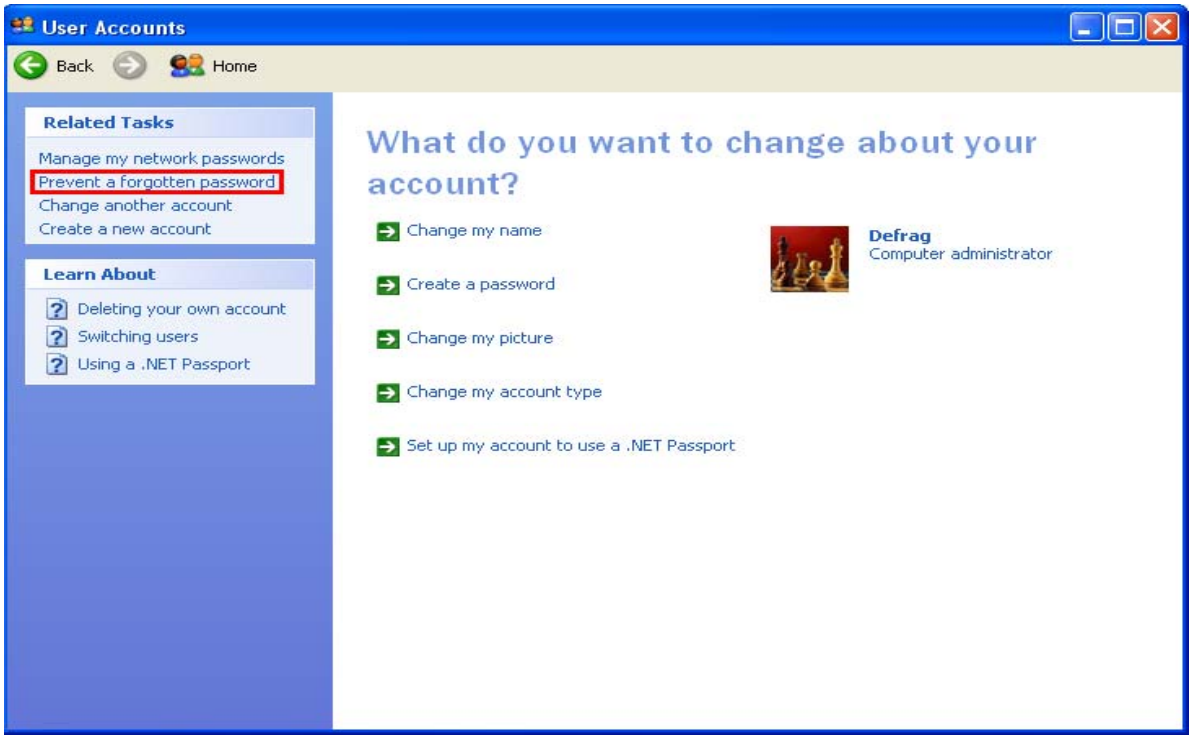
5. Κάνουμε restart και πλέον μπορούμε να συνδεθούμε στο σύστημα αφού αλλάξαμε τον κωδικό που θέλαμε.

2.3.3 Δημιουργία δισκέτας μηδενισμού του κωδικού των XP

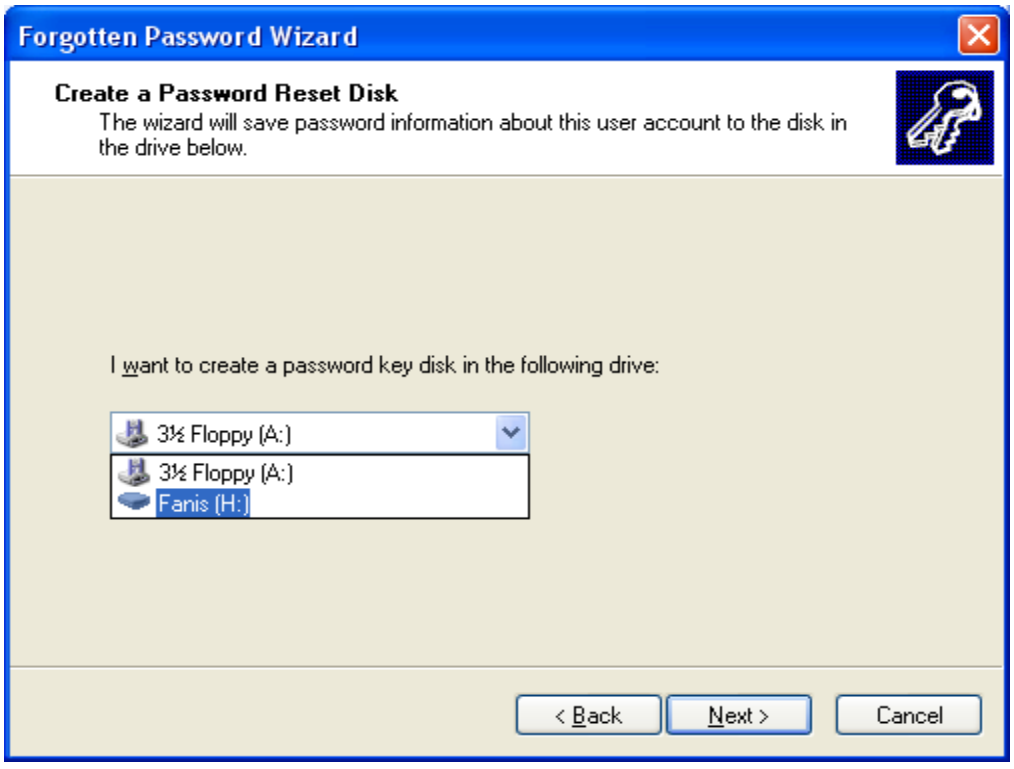
Μια πολύ καλή λύση σε περίπτωση που έχει ξεχάσει κάποιος τον κωδικό του είναι η δημιουργία δισκέτας μηδενισμού του κωδικού. Σε αυτήν την περίπτωση το άτομο πρέπει να έχει προνοήσει και να έχει δημιουργήσει μια δισκέτα πριν χάσει/ξεχάσει τον κωδικό του.
Αρχικά πρέπει να γίνει είσοδος σαν administrator στο σύστημα και έπειτα να εισέλθει στην καρτέλα του Πίνακα Ελέγχου όπου γράφει Λογαριασμοί Χρηστών.



Έπειτα πρέπει να επιλεχτεί η καρτέλα που γράφει "Αλλαγή Λογαριασμού". Προσοχή όμως, για να είναι εφικτή η συγκεκριμένη διαδικασία πρέπει η παρουσίαση να είναι σε "Προβολή Κατηγοριών" και όχι "Κλασσική Προβολή". Η σχετική επιλογή παρουσιάζεται στο αριστερό πλαίσιο του "Πίνακα Ελέγχου". Επιλέγουμε την πρόταση που γράφει "Αποτροπή ξεχασμένου κωδικού πρόσβασης" ("Prevent a forgotten password").

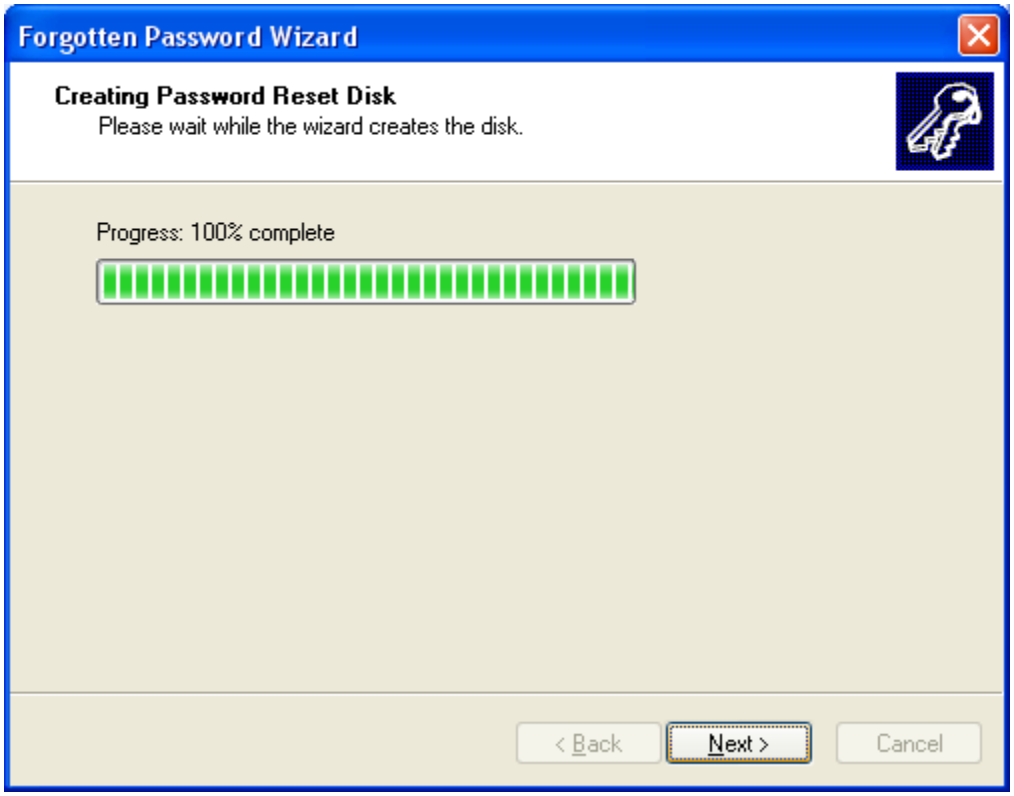


Ακολουθώντας τα βήματα εισάγουμε ένα USB Drive στον υπολογιστή ή μια δισκέτα αντίστοιχα και δημιουργούμε μια δισκέτα επαναφοράς του κωδικού πρόσβασης.



Μας εμφανίζεται μια εικόνα όπου μας ζητείται ο κωδικός πρόσβασής μας.

Αφού εισάγουμε τον κωδικό η διαδικασία ξεκινάει και η δισκέτα επαναφοράς του κωδικού πρόσβασης είναι έτοιμη!



Με την συγκεκριμένη μέθοδο είναι αδύνατο για κάποιον ενώ έχει χάσει τον κωδικό του να μην μπορέσει να εισέλθει στο σύστημα μιας και θα έχει τρόπο να τον ανακτήσει.

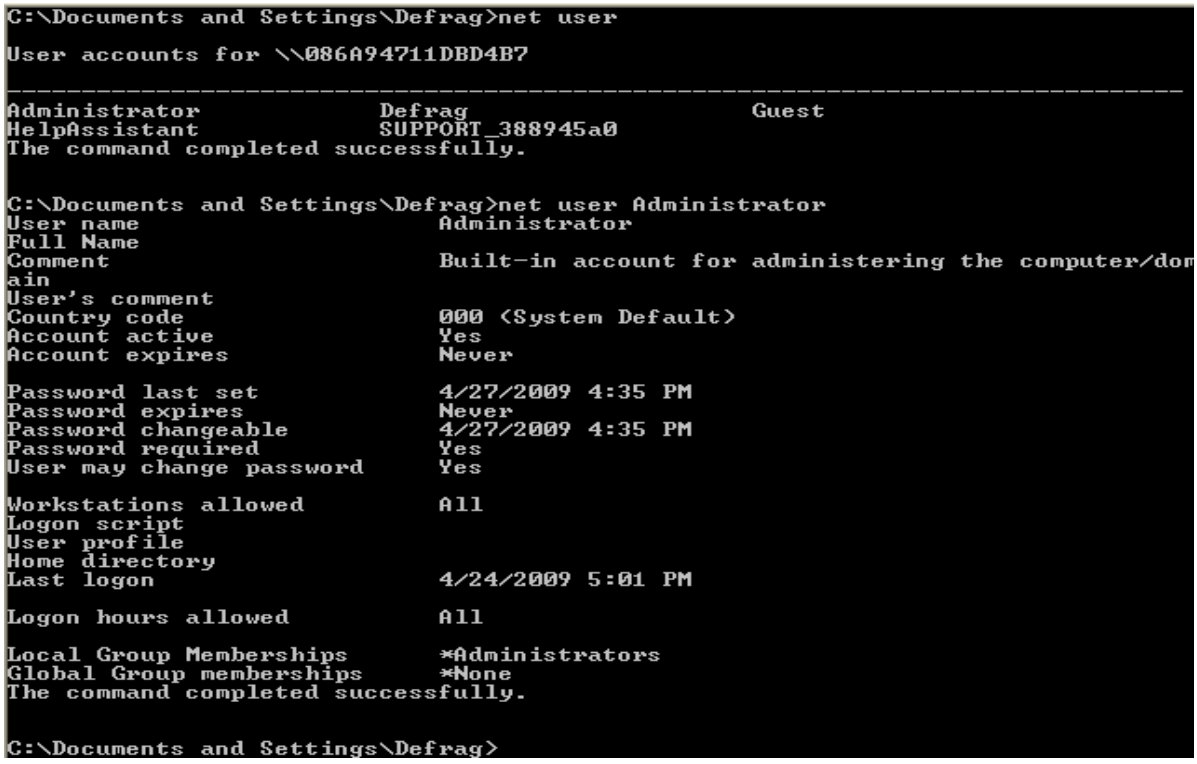
2.3.4 Πρόσβαση σαν Administrator

Αφού αποκτήσουμε πρόσβαση σε έναν οποιονδήποτε λογαριασμό χρήστη στον υπολογιστή και ανοίξουμε ένα παράθυρο DOS (“Εναρξη” -> “Εκτέλεση” -> “CMD”) γράφουμε τις παρακάτω εντολές:

net user: Η συγκεκριμένη εντολή μας δείχνει όλα τα accounts που υπάρχουν στον υπολογιστή μας

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

C:\Documents and Settings\Defrag>net user

User accounts for \\086A94711DBD4B7

-------------------------------------------------------------------------------
Administrator            Defrag                   Guest
HelpAssistant            SUPPORT_388945a0
The command completed successfully.


C:\Documents and Settings\Defrag>_
```

Έπειτα πατώντας **net user Administrator** μας δείχνει πληροφορίες σχετικά με το Administrator account.



Γράφοντας **net user Administrator** 123 (όπου 123 είναι ο νέος κωδικός) αυτό αλλάζει τον κωδικό του Administrator και πλέον μπορούμε να έχουμε πρόσβαση.

ΚΕΦΑΛΑΙΟ 3 LINUX PASSWORDS

Στην συγκεκριμένη περίπτωση χρησιμοποιήσαμε την έκδοση Ubuntu μέσα από μια πληθώρα επιλογών που μας προσφέρουν τα UNIX.
Κατά την είσοδο στα Ubuntu ζητείται το username του χρήστη.

Πληκτρολογώντας το username μας ζητείται το κατάλληλο password ώστε να εισέλθουμε στο σύστημα.

Σχεδόν σε όλες τις διανομές Linux οι πληροφορίες χρηστών αποθηκεύονται σε /etc/passwd, ένα αρχείο κειμένου που περιέχει :

- το login του χρήστη
- τον κρυπτογραφημένο κωδικό πρόσβασής του
- ένα μοναδικό αριθμητικό user-id (αποκαλούμενο uid)
- μια αριθμητική ταυτότητα ομάδας (αποκαλούμενη gid)
- ένα προαιρετικός comment field (συνήθως περιέχουν τέτοια στοιχεία όπως το πραγματικούς όνομα, τηλεφωνικό τον αριθμό τους, κ.λπ.)
- τον εγχώριο κατάλογός τους (home directory),

Μια χαρακτηριστική είσοδος στο /etc/passwd είναι κάπως έτσι:

```
  pete:K3xcO1Qnx8LFN:1000:1000:Peter Hernberg,,,1-800-
FOOBAR:/home/pete:/bin/bash
```

3.1 SHADOW PASSWORDS

3.1.1 Ενεργοποίηση Shadow passwords

Το πρόβλημα με αυτό το σχέδιο είναι ότι με τη σημερινή τεχνολογία, εάν κάποιος πάρει ένα αντίγραφο του κρυπτογραφημένου κωδικού πρόσβασης, είναι θέμα χρόνου μέχρι να μπορεί να βρει τον αρχικό κωδικό πρόσβασης. Αυτός ο στόχος γίνεται ακόμα ευκολότερος όταν ταιριάζει ο κωδικός πρόσβασης του χρήστη μια λέξη λεξικών. Για να αντιμετωπιστεί αυτό το πρόβλημα, το πιο πρόσφατο Unix και τα συστήματα που μοιάζουν με Unix χρησιμοποιούν τους κωδικούς πρόσβασης «σκιών» (shadow passwords). Οι κρυπτογραφημένοι κωδικοί πρόσβασης δεν αποθηκεύονται στο /etc/password, αλλά αντί αυτού σε ένα μη αναγνώσιμο αρχείο που λέγεται /etc/shadow. Υπάρχουν λίγοι λόγοι ώστε να μην χρησιμοποιούνται οι κωδικοί πρόσβασης shadow. Ο αρχικός είναι ότι εάν χρησιμοποιούνται τα NIS (Network Information System- επιτρέπει πολλούς υπολογιστές σε ένα δίκτυο να μοιράζονται πληροφορίες σχετικά με ρυθμίσεις και αρχεία κωδικών) για να συγχρονιστούν οι λογαριασμοί και οι κωδικοί γύρω από μια περιοχή, οι κωδικοί πρόσβασης που θέλουμε να μοιραστούμε δεν μπορούν να σκιαστούν.

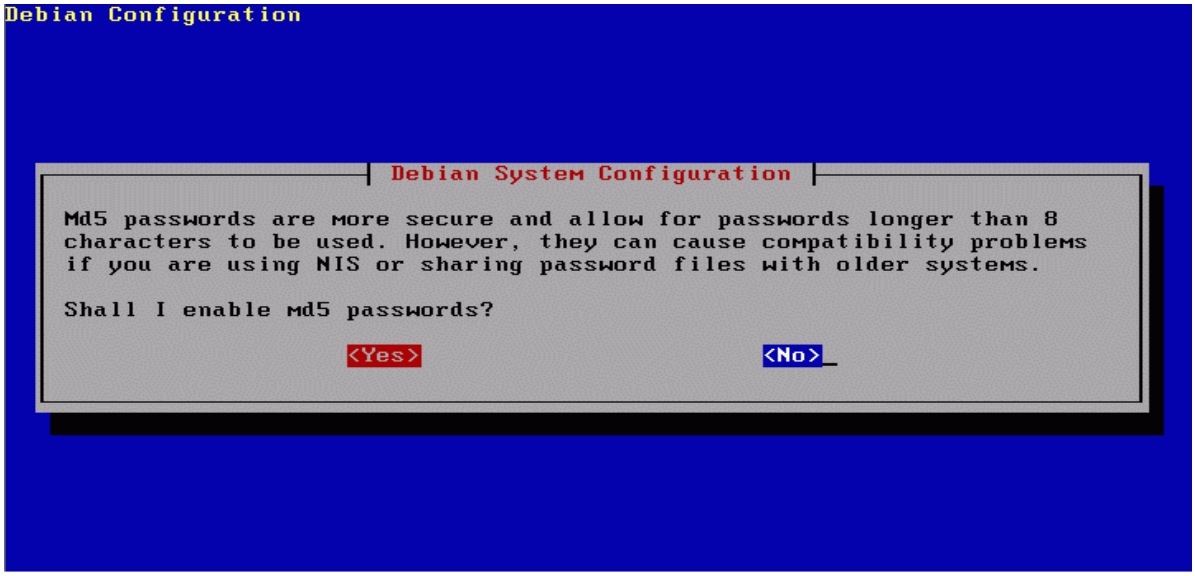
Στα σύγχρονα συστήματα UNIX πέρα από το αρχείο password, που περιέχει πληροφορίες σχετικά με τους χρήστες, υπάρχει και το αρχείο shadow, το οποίο περιέχει τα username και τα password των χρηστών.

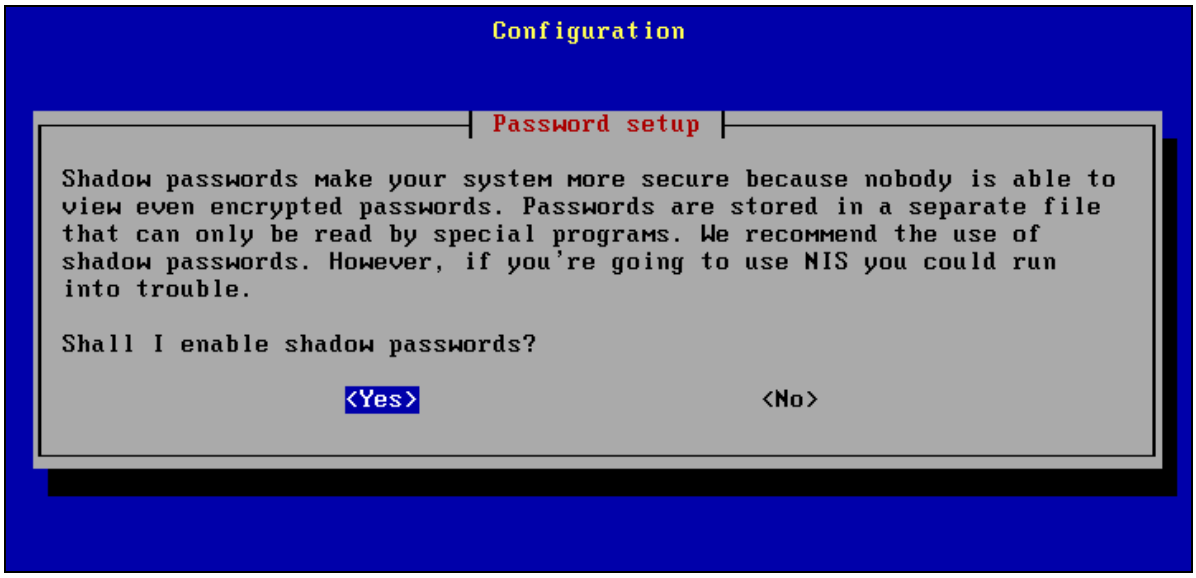
Για τους άλλους χρήστες ειδικά για αυτούς που χρησιμοποιούν redhat και mandrake η χρησιμοποίηση κωδικών πρόσβασης σκιών είναι αρκετά απλή: πληκτρολογούμε setup και έπειτα πάμε στο Auth Configuration… Επιλέγουμε να χρησιμοποιήσουμε το shadow, και για περισσότερη ασφάλεια επιλέγουμε το MD5 επίσης. Μόλις γίνει αυτό, κάνουμε login σαν root και πληκτρολογούμε passed για να αλλάξουμε τους κωδικούς μας είτε οποιουδήποτε άλλου account που υπάρχει στον υπολογιστή μας.

Σε κάποιες περιπτώσεις για να ενεργοποιηθούν τα shadow passwords πρέπει να συνδεθούμε σαν root (administrator) του συστήματος και έπειτα να πληκτρολογήσουμε στο terminal την εντολή pwconv. Έτσι θα ενεργοποιηθεί το αρχείο /etc/shadow. Η διαφορά μεταξύ του /etc/passwd και του /etc/shadow είναι όσο αφορά την ασφάλεια των κωδικών. Το αρχείο /etc/passwd μπορεί να διαβαστεί (να πάρει κάποιος τα hashes των κωδικών) από οποιοδήποτε σε αντίθεση με το /etc/shadow το οποίο μπορεί να το διαβάσει μόνο ο root. Επίσης το /etc/shadow περιέχει το username, το password και κάποιες ακόμα πληροφορίες όπως το πότε λήγει το account κτλ. Σε περίπτωση που δεν θέλουμε να χρησιμοποιούμε shadow passwords το μόνο που χρειάζεται να κάνουμε είναι να πληκτρολογήσουμε την εντολή pwunconv στο terminal και πλέον οι πληροφορίες των accounts του συστήματος θα αποθηκεύονται στο passwd file.

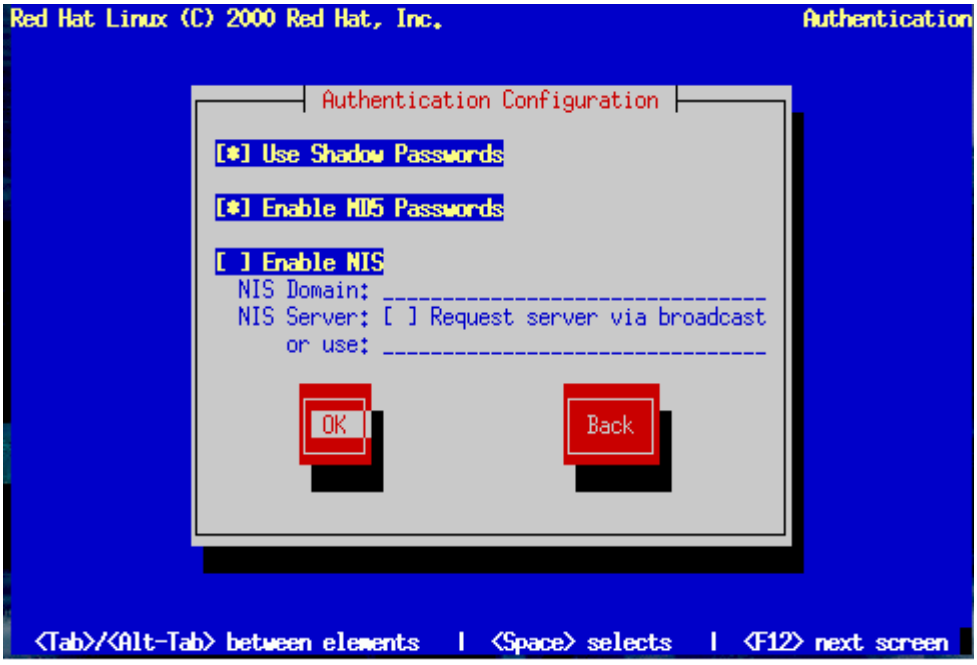
Σε κάποιες άλλες εκδόσεις των UNIX (πχ DEBIAN,REDHAT)μας ζητείται κατά την διάρκεια της εγκατάστασης αν θέλουμε να ενεργοποιήσουμε τα shadow passwords. Έτσι πρέπει να επιλέξουμε αρχικά να μην ενεργοποιηθούν τα MD5 passwords και έπειτα να επιλέξουμε τα shadow:

-Shadow passwords σε DEBIAN-

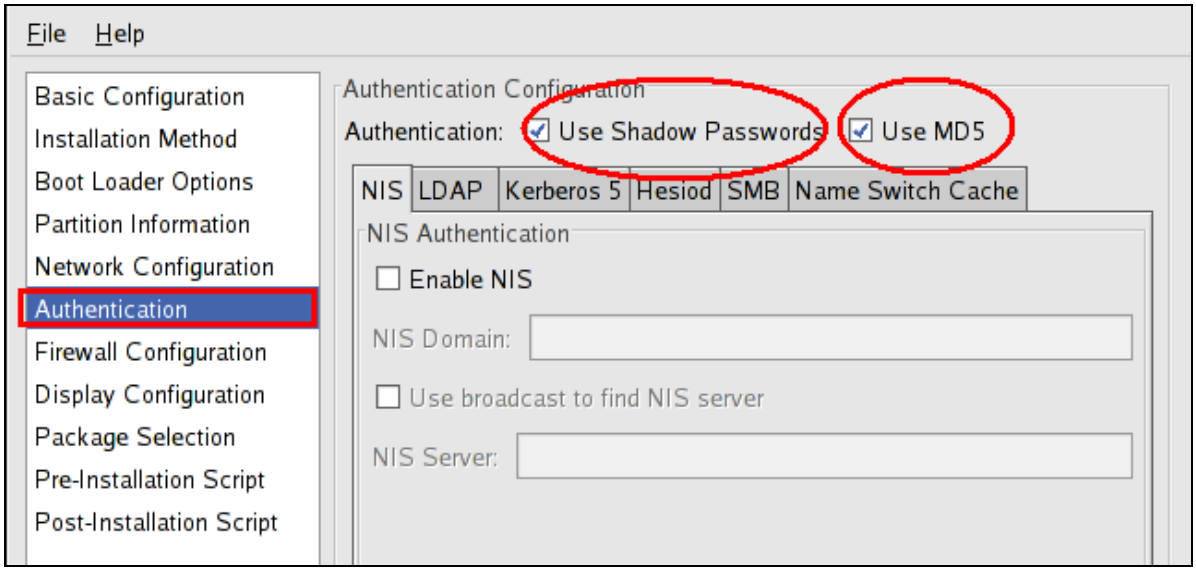




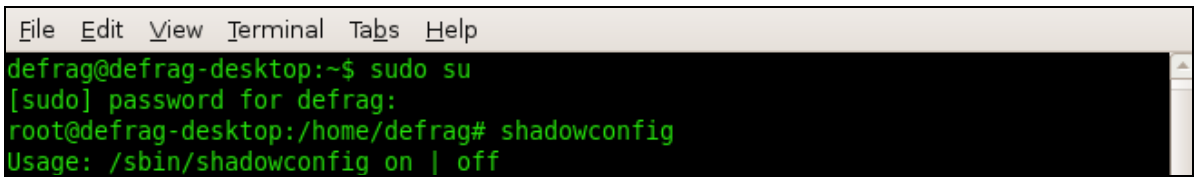
-Shadow Passwords σε REDHAT μέσω εγκατάστασης -



Σε κάποιες διανομές επίσης δίνεται η δυνατότητα ενεργοποίησης των shadow passwords μέσω του Authentication window:



Στις νεότερες εκδόσεις UNIX, τα shadow passwords είναι εγκατεστημένα εξαρχής οπότε δεν χρειάζεται να προβούμε σε ενέργειες εγκατάστασης. Ένας ακόμα τρόπος και ο πιο απλός είναι να τα εγκαταστήσουμε με την εντολή shadowconfig.



Σε αυτή την περίπτωση απλώς πληκτρολογούμε shadowconfig on στο terminal και ενεργοποιούνται τα shadow passwords.

```
root@defrag-desktop:/home/defrag# shadowconfig on
Shadow passwords are now on.
root@defrag-desktop:/home/defrag#
```

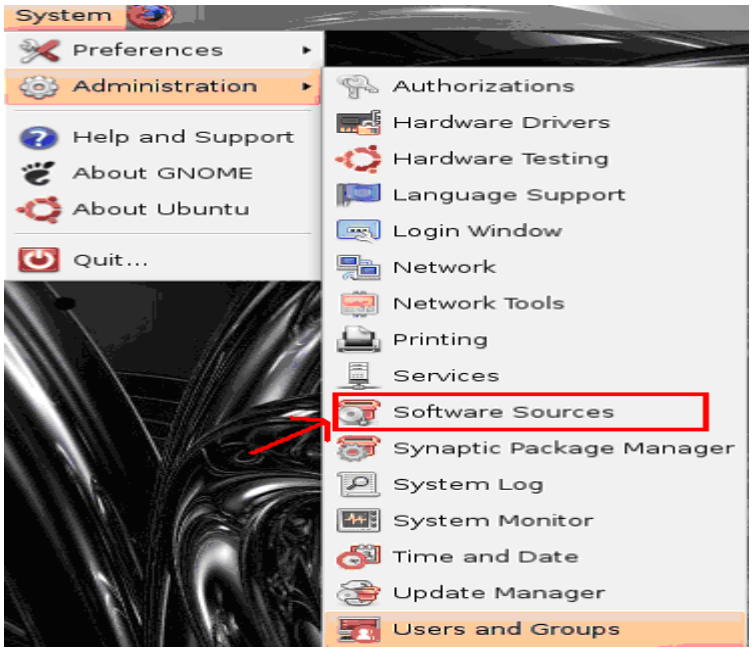
Σε περίπτωση που θέλουμε να τα απενεργοποιήσουμε πληκτρολογούμε την ενοτλή shadowconfig off.

```
root@defrag-desktop:/home/defrag# shadowconfig on
Shadow passwords are now on.
root@defrag-desktop:/home/defrag#
```

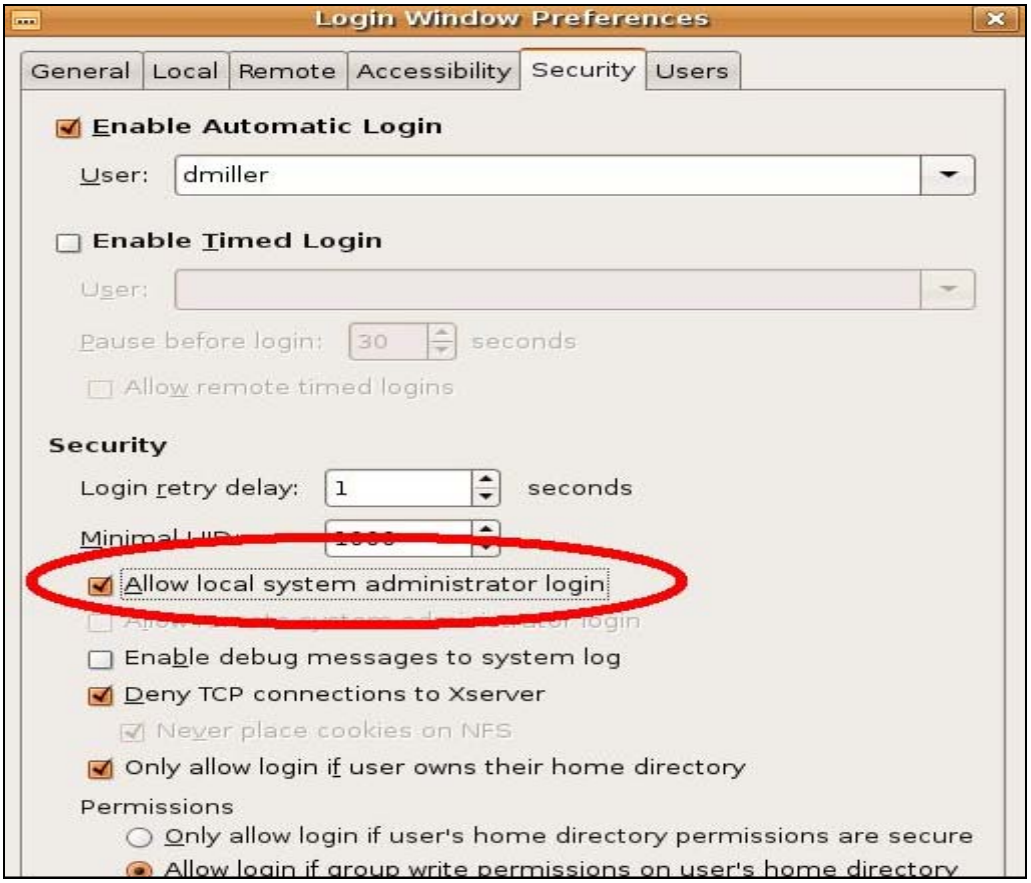
Πρέπει να σημειωθεί ότι το να χρησιμοποιείται αυτή η εντολή (shadowconfig on) ενώ είναι ενεργοποιημένα τα shadow passwords βλάπτει το σύστημα και επίσης ότι χρησιμοποιώντας αυτή την εντολή χάνονται όλες οι πληροφορίες του κωδικού όσο αφορά το password aging.

3.1.2 Πρόσβαση σαν root (Administrator)

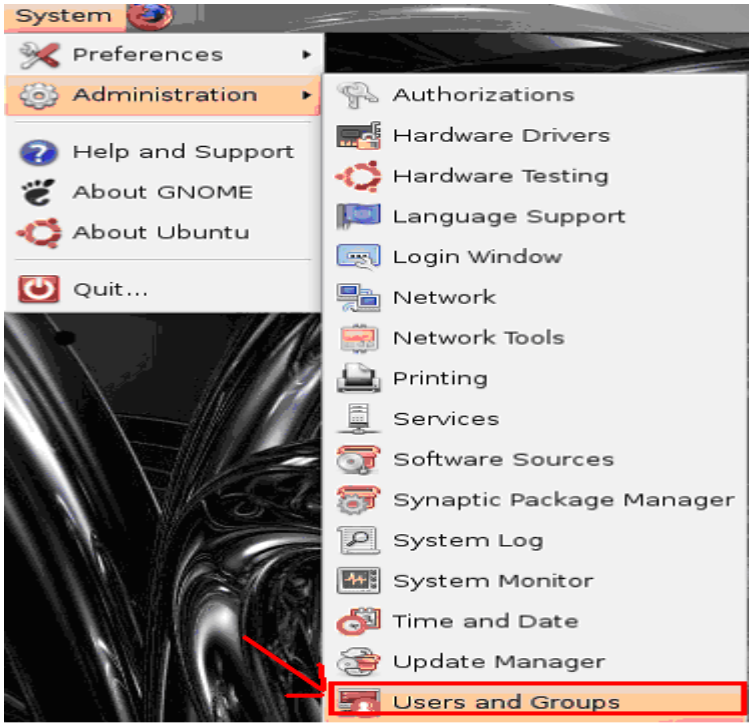
Για να να μπορούμε να κάνουμε login σαν administrator του συστήματος πάμε αρχικά **System > Administration > Software Sources**



Έπειτα απλά πατάμε την καρτέλα που γράφει ¨ασφάλεια¨ (security) και επιλέγουμε το «Allow local system Administrator login». Το προκαθορισμένο username και password για την διανομή των Ubuntu είναι root και root αντίστοιχα και μπορεί να αλλαχθεί ότι ώρα το επιθυμεί ο χρήστης.

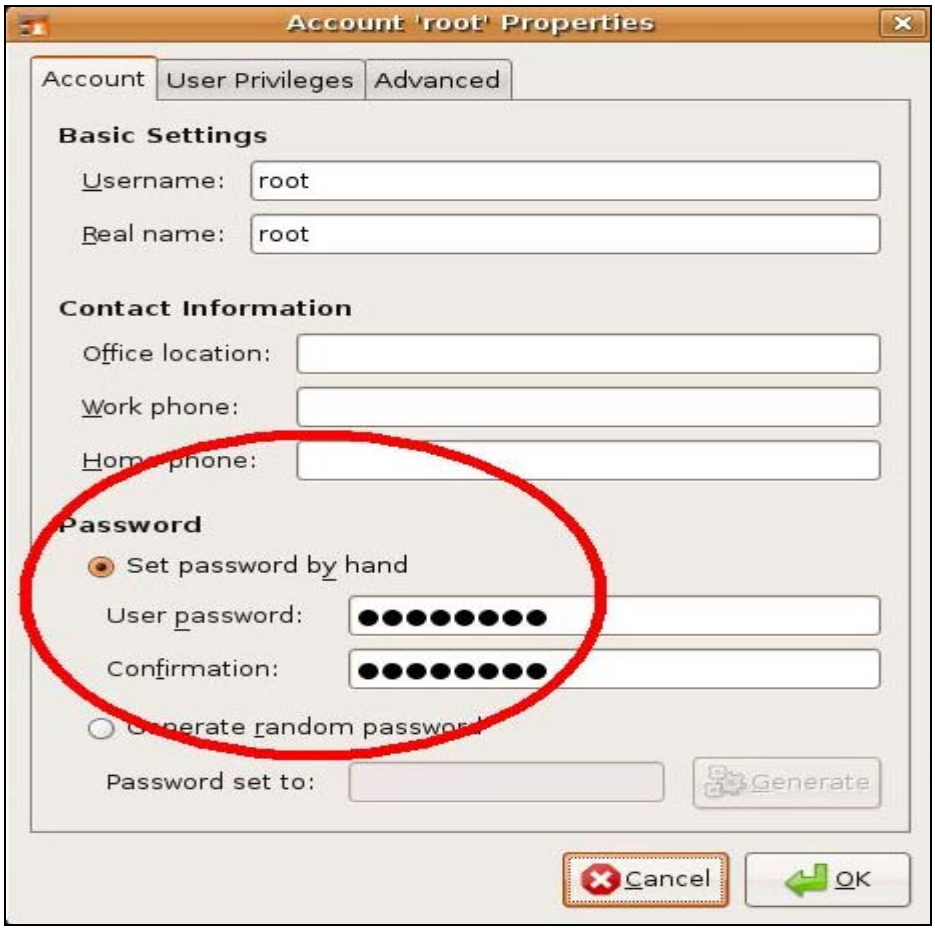


Για να αλλάξουμε τον κωδικό του root πηγαίνουμε System --> Administration --> User and Groups.



Εκεί βλέπουμε το χρήστη root ---> κάνουμε δεξι κλικ πάνω του ---> properties.

Εκεί στο πεδίο **password** θα έχει δημιουργηθεί ένας κωδικός τον οποίο σβήνουμε και βάζουμε αυτόν που επιθυμούμε . Θέλει προσοχή όμως γιατί ο κωδικός που θα μπει πρέπει να είναι ο ίδιος που χρησιμοποιείται από τον απλό user λογαριασμό. Αν μπει διαφορετικός , θα αλλάξει και ο το pass για τον κανονικό χρήστη (και θα γίνει ίδιος με αυτόν του root).

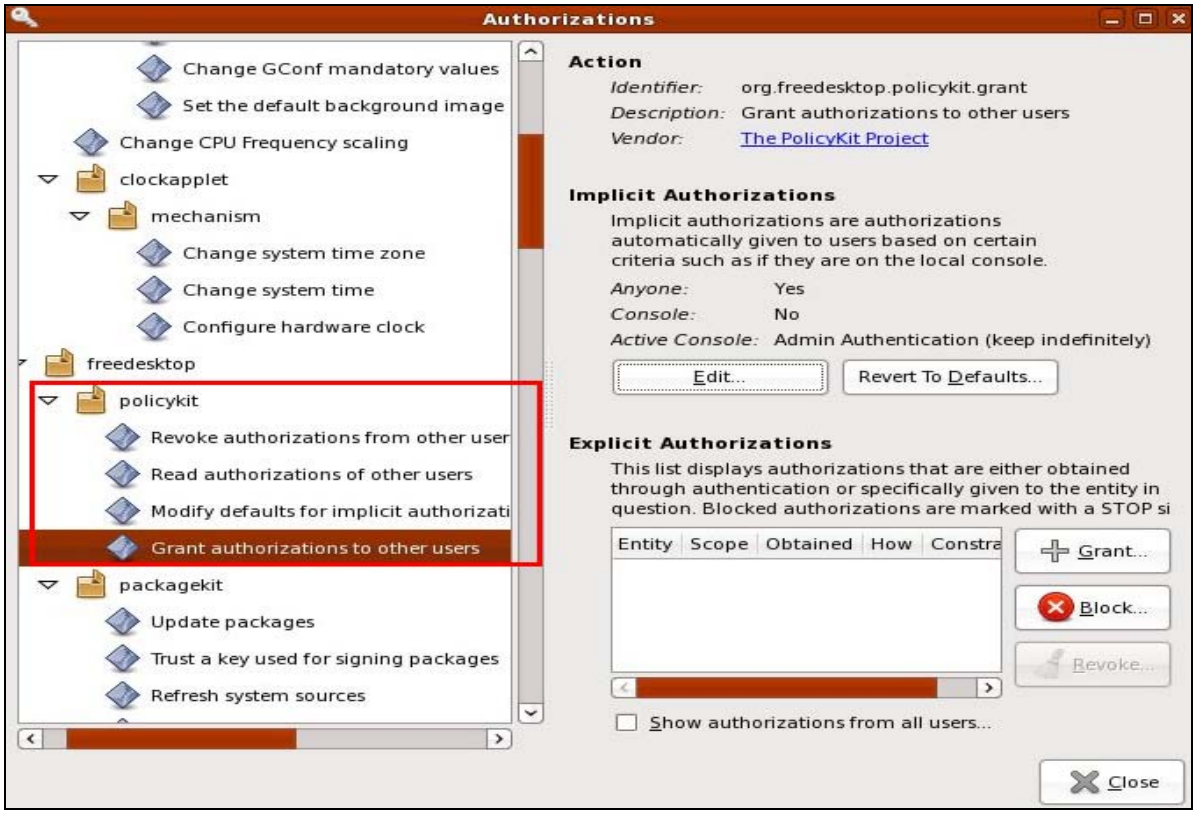


3.2 Ηλικία Password

Στις διανομές linux η ηλικία προεπιλογής που επιτρέπεται για έναν κωδικό πρόσβασης είναι 99999 ημέρες, μετά από αυτήν την περίοδο ο κωδικός πρόσβασης πρέπει να αλλάξει. Όπως καταλαβαίνουμε αυτή η χρονική περίοδος είναι μεγάλη και καθιστά το password ανασφαλές. Η αλλαγή αυτού του χρονικού περιθωρίου μπορεί να γίνει από το /etc/login.defs. Η γραμμή που πρέπει να αλλαχτεί στο /etc/login.defs μοιάζει με το PASS_MAX_DAYS 99999
Το password aging κρατάει τους κωδικούς πρόσβασης φρέσκους, αλλά και απενεργοποιεί τους εκτός λειτουργίας λογαριασμούς χρηστών (accounts) που μπορούν και να αντιπροσωπεύουν κινδύνους ασφαλείας.

Στο λειτουργικό σύστημα Ubuntu μπορούμε να δούμε το Policy Kit επιλέγοντας SystemAdministration—Authorizations

Απ'το παράθυρο που θα εμφανιστεί μπορεί ο χρήστης να διακρίνει το policykit των Ubuntu.



Μερικά policies απαιτούν από τους χρήστες να αλλάζουν τους κωδικούς τους περιοδικά πχ κάθε 90 ή 180 μέρες. Τα συστήματα που εφαρμόζουν τέτοιες πολιτικές αποτρέπουν στους χρήστες να επιλέξουν κάποιο κωδικό πρόσβασης σχεδόν ίδιο με κάποιον προεπιλεγμένο. Αυτή η πολιτική μπορεί συχνά να αποτύχει. Δεδομένου ότι είναι δύσκολο να βρεθούν καλοί και δυνατοί κωδικοί πρόσβασης τους οποίους θα πρέπει να θυμάται ο χρήστης και να χρειάζεται να τους αλλάζουν, η κατάληξη είναι να χρησιμοποιούνται αδύναμους κωδικούς πρόσβασης. Επίσης αν η πολιτική αυτή αποτρέπει τον χρήστη από το να επαναλάβει ένα χρησιμοποιημένο κωδικό, αυτό σημαίνει ότι υπάρχει μία βάση δεδομένων η οποία περιέχει όλους τους τωρινούς κωδικούς (ή τα hashes τους) αντί να σβήνονται οι παλιοί κωδικοί από τη μνήμη. Χρησιμοποιώντας έναν πολύ ισχυρό κωδικό πρόσβασης και χωρίς την απαίτηση να τον αλλάζουν συχνά είναι αρκετά καλύτερο. Εντούτοις έχει ένα σημαντικό μειονέκτημα: εάν κάποιος αποκτά έναν κωδικό πρόσβασης, εάν δεν αλλάζει, μπορεί να υπάρξει μακροπρόθεσμη πρόσβαση.

Είναι απαραίτητο να υπολογίζονται αυτοί οι παράγοντες:

- η πιθανότητα ότι κάποιος μπορεί να υποθέτει έναν κωδικό πρόσβασης που είναι αδύναμος
- η πιθανότητα ότι κάποιος θα προσπαθήσει να κλέψει ή αλλιώς να αποκτήσει χωρίς να χρειαστεί να μαντέψει ένα κωδικός πρόσβασης.
- Και τέλος η πιθανότητα να αποκτήσει τον κωδικό χωρίς να χρειαστεί να μαντέψει καν

3.3 Ορθή χρήση/τακτική κωδικού πρόσβασης για την αποφυγή υποκλοπής του

3.3.1 Σωστή διαχείριση κωδικών

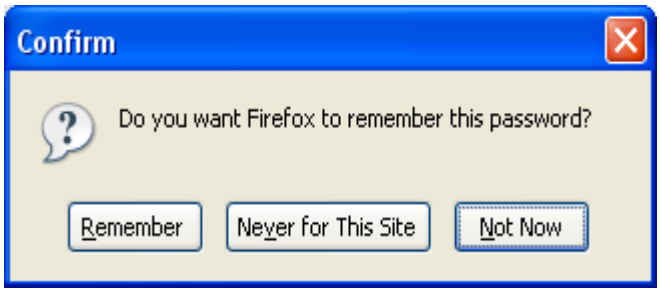
Συχνά τα password policies συμπεριλαμβάνουν συμβουλές για την σωστή διαχείριση ενός κωδικού όπως για παράδειγμα:

- Ποτέ να μην μοιράζεται ο κωδικός
- Ποτέ να μην χρησιμοποιείται ο ίδιος κωδικός για περισσότερους από ένα λογαριασμούς χρηστών
- ποτέ να μην λέγεται ο κωδικός σε κανένα, συμπεριλαμβανομένου ανθρώπων που ισχυρίζονται ότι είναι από το τμήμα εξυπηρέτησης πελατών ή της ασφάλειας
- ποτέ να μην γράφεται ο κωδικός σε χαρτί
- ποτέ να μην δίνεται ο κωδικός μέσω τηλεφώνου, e-mail η instant messaging
- να γίνεται log off μετά την χρήση του υπολογιστή
- να αλλάζεται ο κωδικός σε περίπτωση που υπάρχουν υποψίες

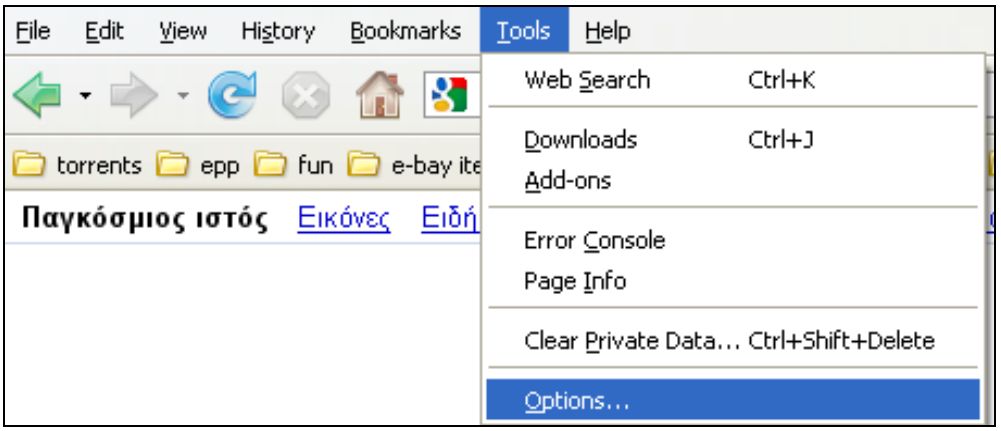
- οι κωδικοί των windows και των εφαρμογών τους να είναι διαφορετικοί
- οι κωδικοί να περιέχουν γράμματα και νούμερα ταυτόχρονα
- μην αποκαλύπτεται το password σε ΚΑΝΕΝΑ άτομο, ούτε ακόμα και σε εμπιστοσύνης άτομα.

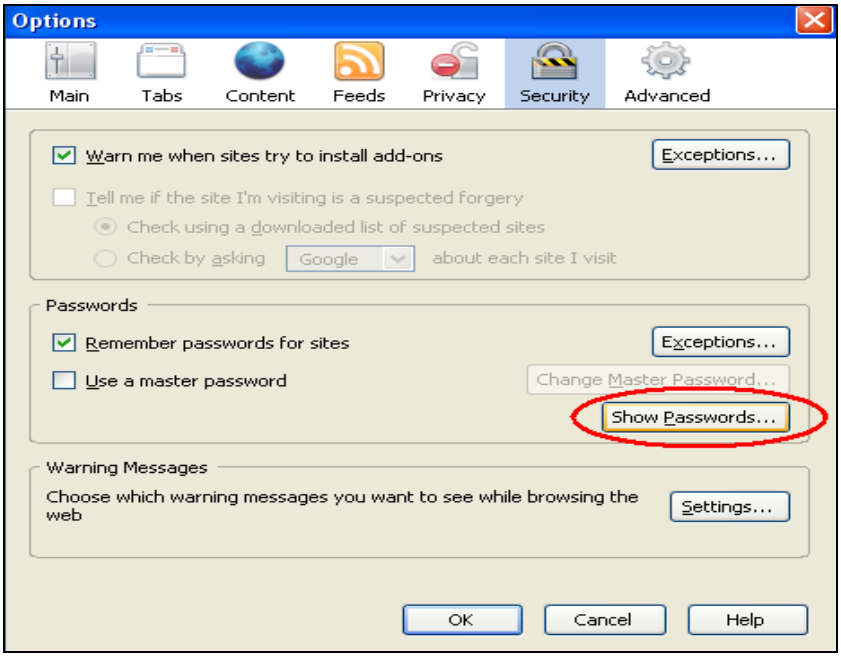
3.3.2 Remember my Password

Επίσης ένα σημαντικό κομμάτι που θα πρέπει να προσέξουμε είναι η Επιλογή "Remember Password" η οποία χρησιμοποιείται για να αποθηκεύεται ο κωδικός μας και να μην χρειάζεται να τον πληκτρολογούμε κάθε φορά. Αυτή η τεχνική κρύβει πολλούς κινδύνους μιας και ο κωδικός αποθηκεύεται στον σκληρό δίσκο του υπολογιστή σαν cookie και είναι πολύ εύκολο να αποκτήσει κάποιος πρόσβαση σε αυτό το αρχείο και να τον ανακτήσει.

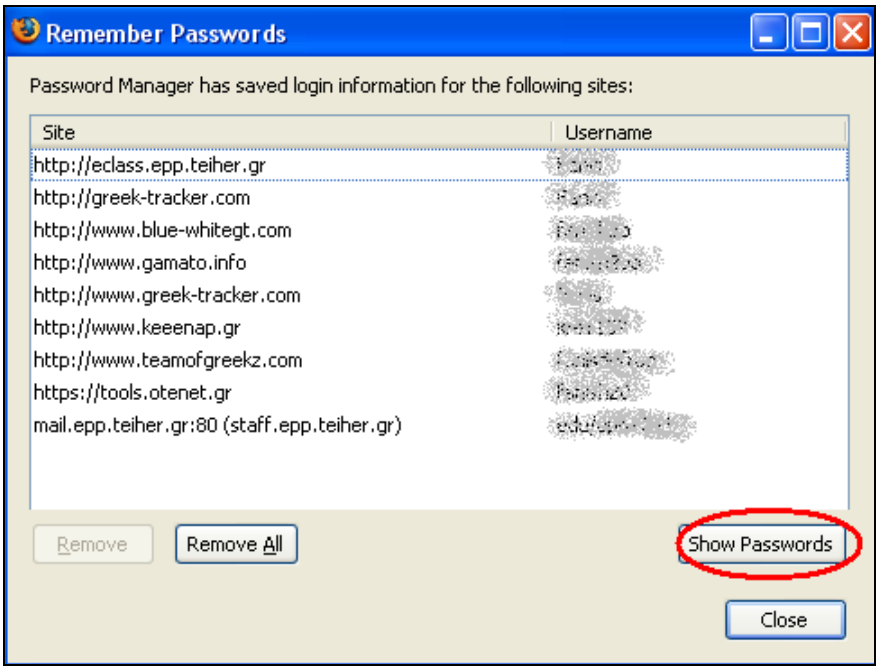


Σε αυτή την περίπτωση οι κωδικοί αποθηκεύονται με την μορφή cookies στον σκληρό μας δίσκο. Έτσι απλά επιλέγοντας αργότερα μπορεί ο οποιοσδήποτε να δει τους κωδικούς που έχουμε αποθηκεύσει.

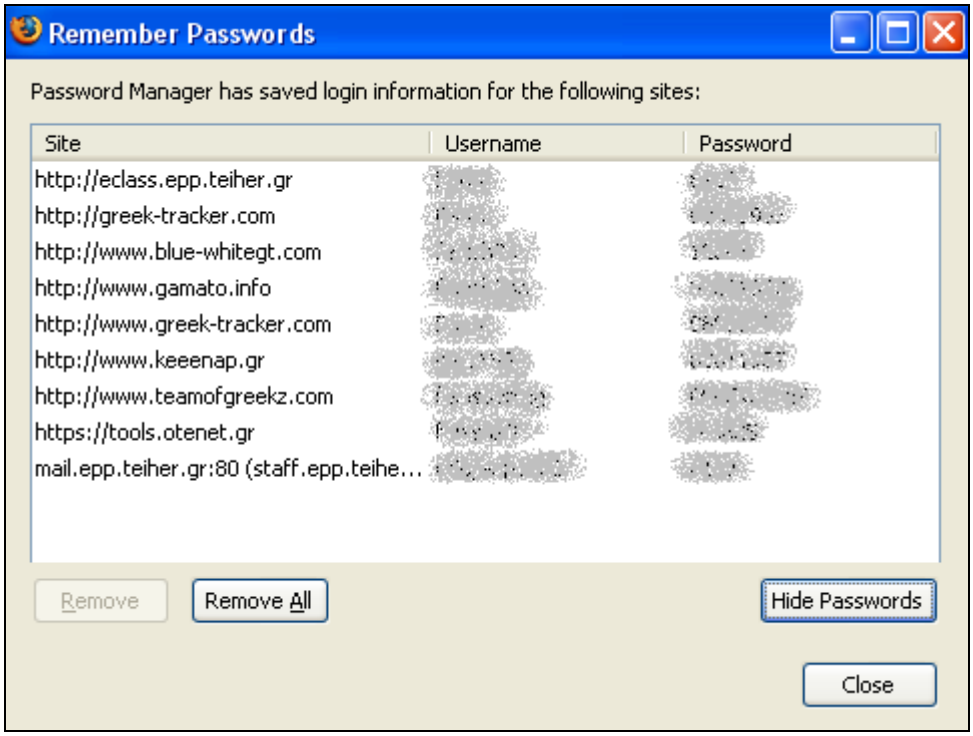




Μας εμφανίζεται το παρακάτω παράθυρο όπου μπορούμε να δούμε τα usernames των account που υπάρχουν στον υπολογιστή.



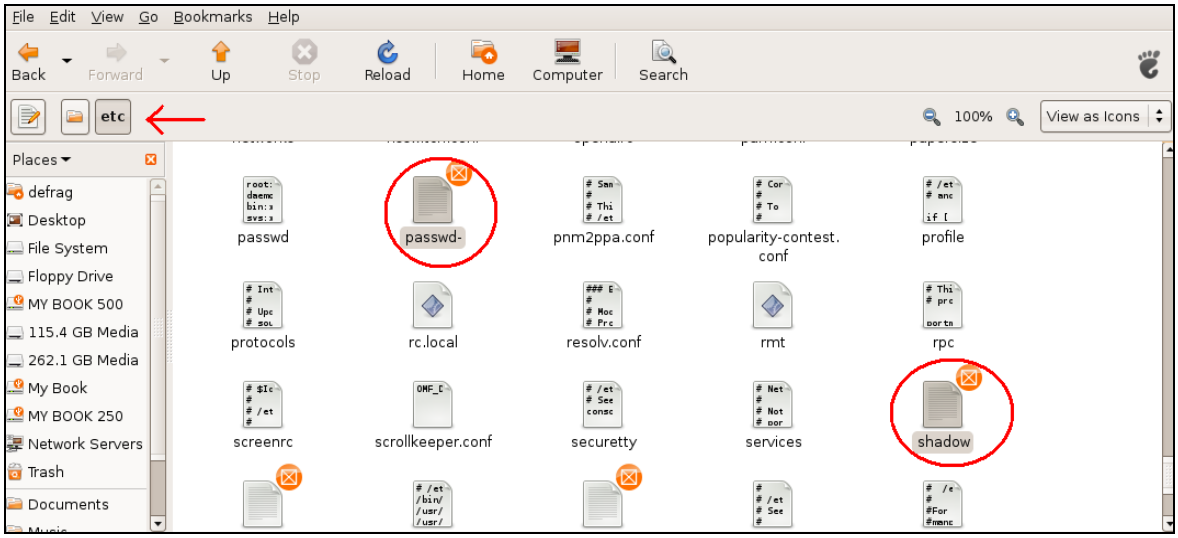
Επιλέγοντας το “Show passwords” μας εμφανίζονται οι κωδικοί για τον κάθε ιστοχώρο που έχουμε επιλέξει να αποθηκευτεί το password.



Στα συστήματα UNIX είναι εφικτό να χρησιμοποιούνται τα */etc/passwd* και */etc/shadow*, χωρίς τη χρήση των στοιχείων του password aging. Παρόλαυτά τα πλεονεκτήματα που προσφέρονται σε συνδυασμό με το password aging είναι πολλά και με τις κατάλληλες τιμές password aging μπορεί να δημιουργηθεί σε ένα σύστημα ένα ιδανικό password policy με εναλλαγή των κωδικών , μειώνοντας έτσι το ρίσκο ότι οι χρήστες θα κλειδωθούν έξω από τα account τους.

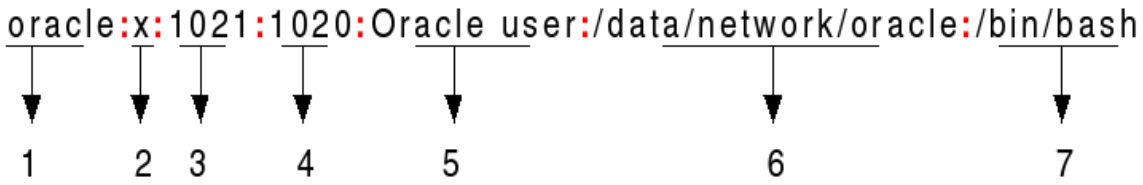
3.4 ΠΕΡΙΕΧΟΜΕΝΑ ΤΩΝ PASSWD KAI SHADOW FILES

Τα δύο αυτά αρχεία βρίσκονται μέσα στο filesystem στο αρχείο /etc.



3.4.1 /etc/passwd File

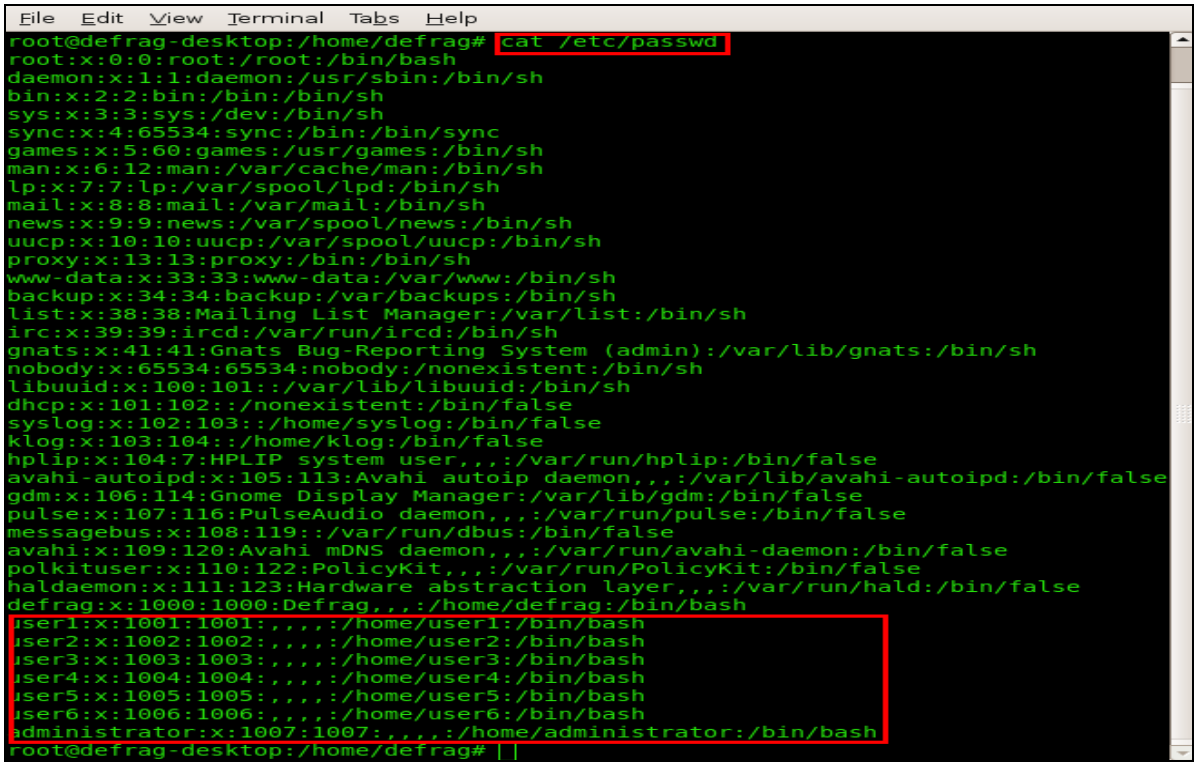
Το /etc/passwd File περιέχει μία είσοδο ανά σειρά για κάθε χρήστη (ή λογαριασμό χρήστη) του συστήματος. Τα πεδία του είναι 7 και χωρίζονται από ένα σύμβολο (:).Το format ενός τέτοιου αρχείου θα μοιάζει με το παρακάτω:



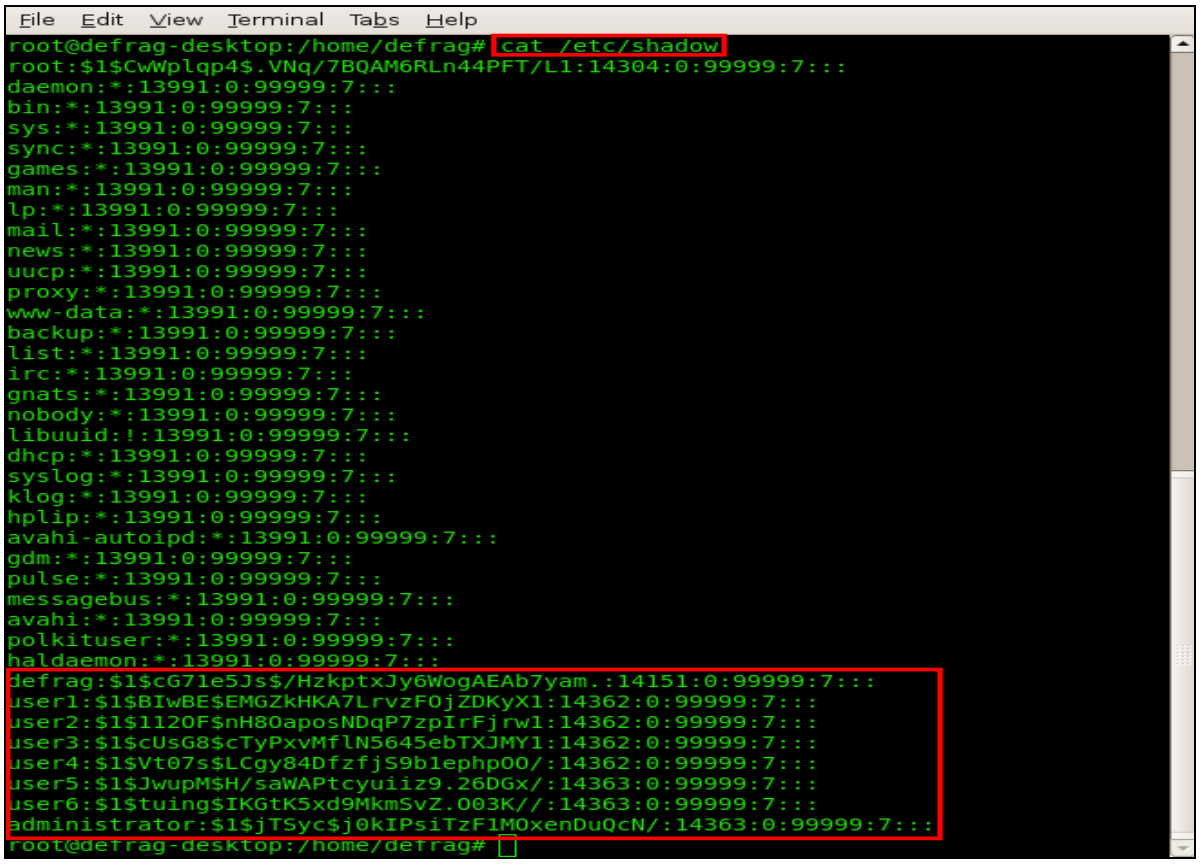
1. **Username:**Το πρώτο πεδίο χρησιμοποιείται όταν συνδέονται οι χρήστες. Είναι μεταξύ 1 και 32 χαρακτήρων.
2. **Password:**Αν υπάρχει το σύμβολο X σημαίνει ότι ο κωδικός έχει αποθηκευτεί στο /etc/shadow file.
3. **User ID (UID):**Κάθε χρήστης πρέπει να έχει μια User Id. Το UID 0 χρησιμοποιείται για τον root και οι τιμές 1-99 χρησιμοποιούνται για τους άλλους προκαθορισμένους λογαριασμούς. Οι UID με τιμές από 100-999 έχουν κατοχυρωθεί από το σύστημα για administrative λογαριασμούς ή λογαριασμούς χρηστών του συστήματος.
4. **Group ID (GID):**Το αρχικό group ID. Αποθηκεύεται στο /etc/group file.
5. **User ID Info:** Το πεδίο για τα σχόλια. Επιτρέπει να προστεθούν κάποιες επιπλέον πληροφορίες για τον χρήστη για παράδειγμα το ονοματεπώνυμο του χρήστη ή το τηλέφωνό του κτλ.
6. **Home Directory:**Το απόλυτο μονοπάτι στο οποίο θα βρίσκεται ο χρήστης όταν κάνει login. Αν αυτός ο κατάλογος δεν υπάρχει τότε το πεδίο διαδρομής του χρήστη γίνεται ¨/¨.
7. **Command/shell:** Το απόλυτο μονοπάτι μιας εντολής η ενός shell (/bin/bash). Τυπικά αυτό είναι ένα shell.

Το /etc/passwd χρησιμοποιείται για τοπικούς χρήστες μόνο. Για να δούμε όλη την λίστα από τους χρήστες πρέπει να πληκτρολογήσουμε:

```
cat /etc/passwd
```



Στην συγκεκριμένη περίπτωση έχουμε shadow passwords, όπως μπορούμε να καταλάβουμε από το παραπάνω screenshot. Οπότε αντί για /etc/passwd θα βάζουμε /etc/shadow



Για να ψάξουμε για ένα username με το όνομα User1 γράφουμε:

grep User1 /etc/passwd

```
File  Edit  View  Terminal  Tabs  Help
root@defrag-desktop:/home/defrag# grep user1 /etc/shadow
user1:$1$BIwBE$EMGZkHKA7LrvzFOjZDKyX1:14362:0:99999:7:::
root@defrag-desktop:/home/defrag#
```

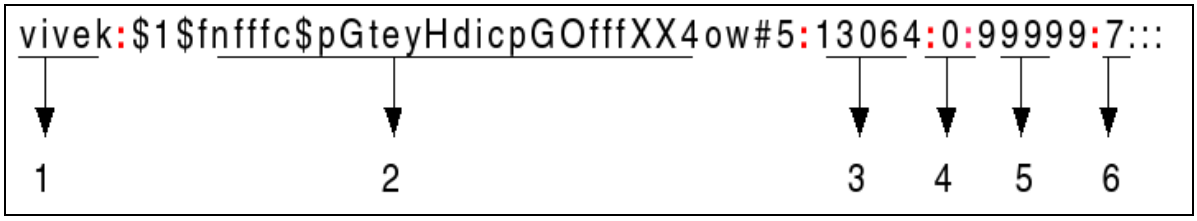
Η άδεια στο /etc/passwd πρέπει να διαβάζεται μόνο από τον χρήστη και ο ιδιοκτήτης πρέπει να είναι ο root.

ls –l /etc/passwd

```
File  Edit  View  Terminal  Tabs  Help
root@defrag-desktop:/home/defrag# ls -l /etc/shadow
-rw-r----- 1 root shadow 1321 2009-04-29 17:20 /etc/shadow
root@defrag-desktop:/home/defrag#
```

3.4.2 /etc/shadow File

Για να καταλάβουμε το πώς δουλεύει το password aging σε ένα σύστημα UNIX, πρέπει να κατανοήσουμε το format του /etc/shadow file. Κάθε χωρισμένη εγγραφή μοιάζει κάπως έτσι



1. Το πρώτο πεδίο όπως φαίνεται ξεκάθαρα είναι το username.
2. Το επόμενο είναι το password του account κωδικοποιημένο.
3. Το επόμενο πεδίο είναι η ημερομηνία κατά την οποία ο κωδικός άλλαξε τελευταία φορά εκφρασμένη ως ο αριθμός των ημερών από τις 1 Ιανουαρίου 1970.
4. Το πεδίο **min** είναι ο ελάχιστος αριθμός των ημερών που χρειάζεται ώστε να μπορεί κάποιος χρήστης να αλλάξει τον κωδικό. Αυτό χρησιμοποιείται για να αποτρέψει τους χρήστες από το να αλλάζουν τους κωδικούς τους και μετά αμέσως να τους ξαναναλλάζουν στην προηγούμενη τιμή που είχαν (ακυρώνοντας έτσι την προοριζόμενη ασφάλεια).
5. Το πεδίο **max** αντιπροσωπεύει τον μέγιστο αριθμό ημερών οπου μπορεί να χρησιμοποιηθεί ένας κωδικός πριν τη λήξη του. Αν για παράδειγμα ένας administrator θέλει αυστηρά να αλλάζουν οι χρήστες τους κωδικούς τους κάθε 30 ημέρες θα ορίσει και τα δύο αυτά πεδία με την τιμή 30.Γενικά όμως το πεδίο max λαμβάνει συνήθως μια μεγαλύτερη τιμή από το πεδίο min.
6. Το πεδίο warn διευκρινίζει τον αριθμό ημερών κατά τον οποίο ένας χρήστης ειδοποιήθηκε στο τελευταίο του login ότι ο κωδικός του θα λήξει. Αυτό δεν πρέπει να είναι μια πάρα πολύ μικρή περίοδος χρόνου από την στιγμή που πολλοί χρήστες δεν συνδέονται καθημερινά και το μήνυμα μπορεί εύκολα να

αγνοηθεί στα login messages.Στο συγκεκριμένο παράδειγμα δεν υπάρχει τέτοιος ορισμός.

7. Το πεδίο inactive ορίζει των αριθμό των ημερών οπου μπορεί ένας λογαριασμός να είναι ανενεργός. Αυτό το πεδίο μπορεί να βοηθήσει αποτρέποντας τους αδρανείς λογαριασμούς από το να παραβιαστούν.
8. Τέλος ,το πεδίο expire ορίζει την απόλυτη μέρα (εκφρασμένη ως ο αριθμός των ημερών από τις 1 Ιανουαρίου 1970) οπου θα λήξει ο κωδικός. Το πεδίο flag δεν χρησιμοποιείται.

Σε περίπτωση που δεν έχει ενεργοποιηθεί το password aging τότε το αρχείο shadow θα είναι κάπως έτσι:
sbob:dZlJpUNyyusab:12345:::::

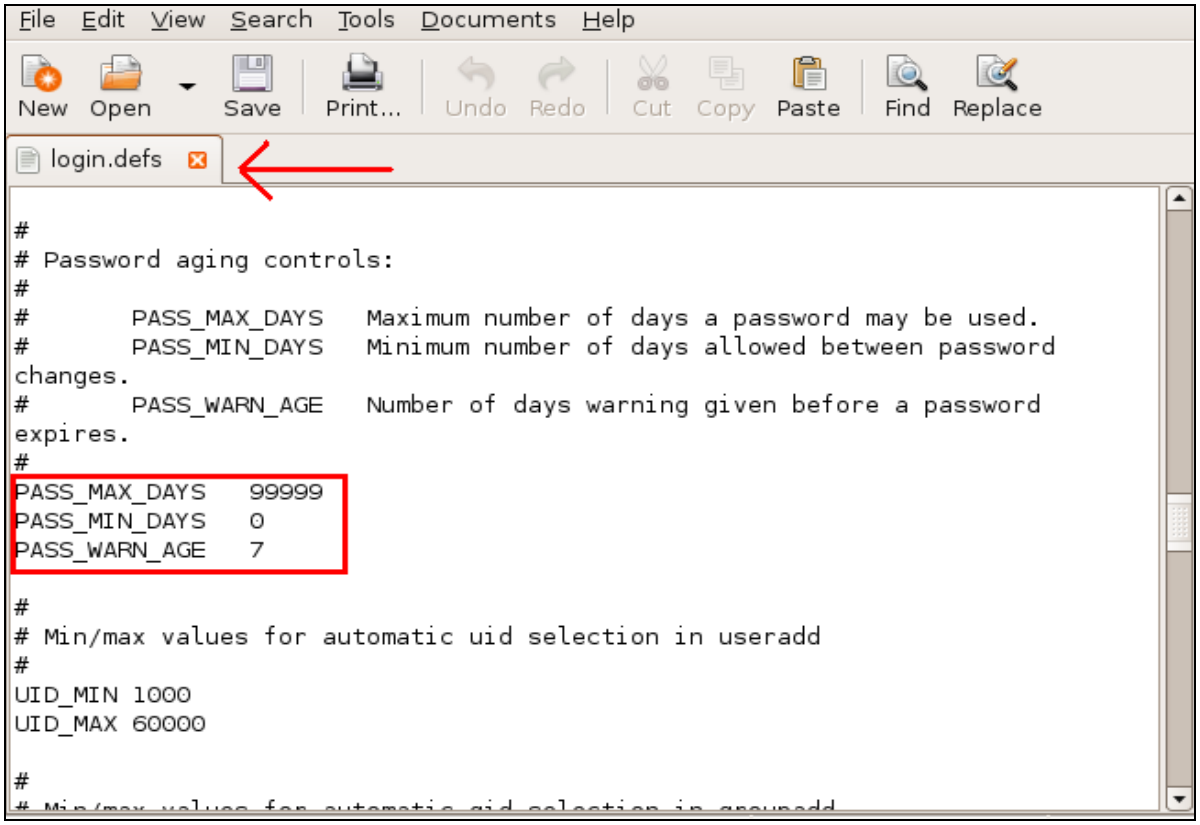
Αν ο λογαριασμός είναι κλειδωμένος (δηλαδή έχει κλειδωθεί από τον administrator του συστήματος) τότε θα μοιάζει σαν το παρακάτω:
dumbo:*LK*:::::::

Σε ένα shadow αρχείο είναι εφικτοί γενικά διάφοροι συνδυασμοί.
Για παράδειγμα:
jdoe:w0qjde84kr%p0:13062:60:::::

Το παραπάνω αρχείο shadow υπονοεί ότι ο χρήστης πρέπει να κρατάει ένα κωδικό για 60 μέρες αφότου τον αλλάξει αλλά δεν απαιτείται καμία αλλαγή του κωδικού πρόσβασης.

3.5 PASSWORD LONGEVITY

Όπως είπαμε το password aging είναι ένα χαρακτηριστικό γνώρισμα μερικών υπολογιστικών συστημάτων το οποίο εξαναγκάζει τους χρήστες να αλλάζουν τους κωδικούς τους συχνά με την πρόθεση ότι ένας κωδικός αργά ή γρήγορα θα πέσει σε χέρια τρίτου και θα παραβιαστεί καθιστώντας τον έτσι άχρηστο. Τέτοιες πολιτικές προκαλούν συνήθως στην καλύτερη περίπτωση την διαμαρτυρία των χρηστών και στην χειρότερη ακόμα και την εχθρότητα. Οι χρήστες ανακαλύπτουν συνήθως καινούργιες πατέντες ώστε να απομνημονεύουν τους κωδικούς τους. Σε οποιαδήποτε περίπτωση όμως ,το να ανακτήσει ένας επιτιθέμενος τον κωδικό που επιθυμεί είναι θέμα χρόνου, σε περίπτωση που αυτός ο κωδικός δεν αλλάζει συχνά. Εκτός από αυτό όμως, αν ένας επιτιθέμενος καταφέρει να ¨σπάσει¨ τον κωδικό και να αποκτήσει πρόσβαση σε ένα σύστημα, τότε μπορεί να ¨πειράξει¨ κάποιες παραμέτρους του υπολογιστή ώστε να του επιτραπεί η μελλοντική πρόσβαση ακόμα και αν ο κωδικός αυτός έχει λήξει (rootkit).
Όσο αφορά τα passwords στα συστήματα UNIX και σχετικά με το longevity του καθενός αυτό μπορεί να αλλάξει μέσα από κάποιες παραμετροποιήσεις στο αρχείο /etc/login.defs. Ανοίγοντας το συγκεκριμένο αρχείο εμφανίζεται ένας κώδικας στην οθόνη. Ψάχνοντας βρίσκουμε τις εξής παραμέτρους σε κάποιο σημείο του κώδικα:



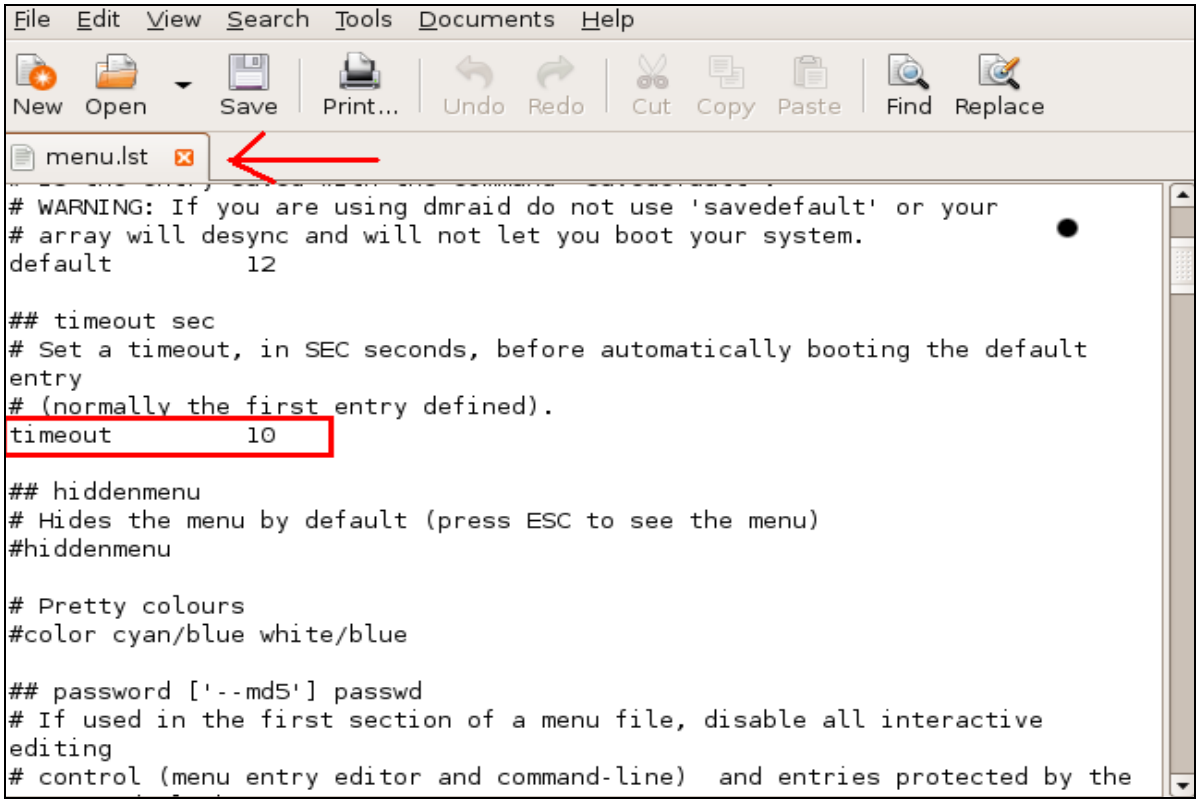
Το πεδίο PASS_MAX_DAYS υποδεικνύει το χρονικό όριο σε μέρες οπου πρέπει να αλλάξει ο κωδικός. Έτσι αν για παράδειγμα το θέταμε ίσο με 60 τότε το σύστημα θα υποχρέωνε το χρήστη να αλλάζει κωδικό κάθε 2 μήνες.

Το πεδίο PASS_MIN_DAYS δείχνει πόσες μέρες χρειάζεται να περάσουν πρίν επιτραπεί στον χρήστη να αλλάξει τον κωδικό από την προηγούμενη αλλαγή που έκανε.

Το τελευταίο πεδίο PASS_WARN_AGE δείχνει πόσες μέρες πρίν από την λήξη του κωδικού θα στέλνονται στον χρήστη προειδοποιητικά μηνύματα (όταν κάνουν login).

3.6 Το menu GRUB

Το GRUB είναι ένας boot loader δηλαδή ένα λογισμικό που βλέπει ένας υπολογιστής όταν ξεκινάει. Είναι υπεύθυνος για τη φόρτωση και την μεταφορά ελέγχου στον kernel (κεντρικό τμήμα) ενός λειτουργικού συστήματος. Με τη σειρά του ο kernel, αρχικοποιεί το υπόλοιπο του λειτουργικού συστήματος.
Ο GNU GRUB είναι ένας πολύ ισχυρός boot loader και μπορεί να φορτώσει τόσο λειτουργικά συστήματα ελεύθερου λογισμικού, όσο και κλειστού (με τη χρήση της λειτουργίας chain loading).
Όταν κάνουμε boot με τον GRUB, μπορούμε να χρησιμοποιήσουμε είτε γραμμή εντολών, είτε μενού. Με την γραμμή εντολών εισάγουμε χειροκίνητα τον σκληρό δίσκο και το όνομα του αρχείου του kernel. Με το μενού, απλά επιλέγουμε ένα λειτουργικό σύστημα χρησιμοποιώντας τα βελάκια. Το μενού βασίζεται σε ένα αρχείο ρυθμίσεων, το **menu.lst**



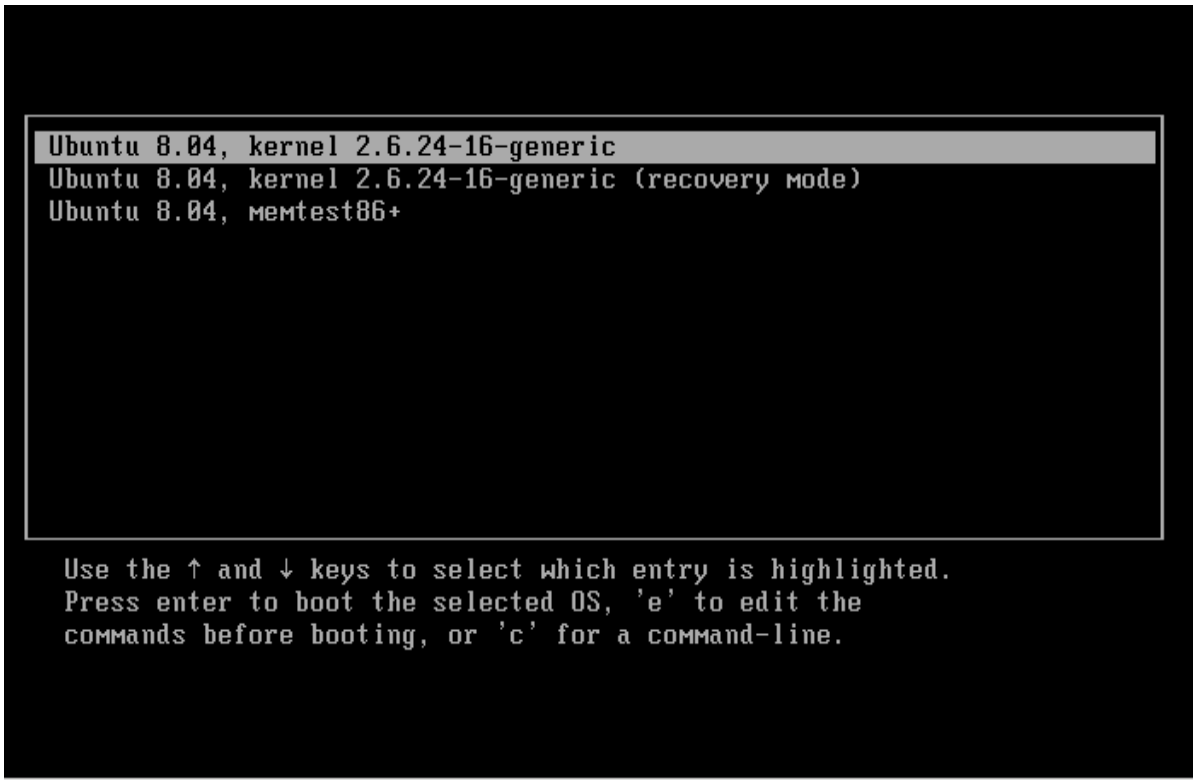
Σε περίπτωση που θέλουμε να απενεργοποιήσουμε το GRUB θέτουμε το timeout (αντιστοιχεί σε δευτερόλεπτα) ίσο με 0 στο αρχείο /boot/grub/menu.lst . Σε περίπτωση που θέλουμε να το ξαναενεργοποιήσουμε απλά βάζουμε ένα LIVE CD των Linux και μπαίνοντας στο filesystem στο ίδιο αρχείο το ξαναθέτουμε ίσο με 10 ή κάποια άλλη τιμή της επιλογής μας..

3.7. Ανάκτηση κωδικού στα Linux (Ubuntu)

Σε περίπτωση που θέλουμε να κάνουμε ανάκτηση του κωδικού μας στα Linux, αντικαθιστώντας τον με τον ίδιο ή κάποιον άλλο κωδικό κάνουμε τα εξής βήματα:

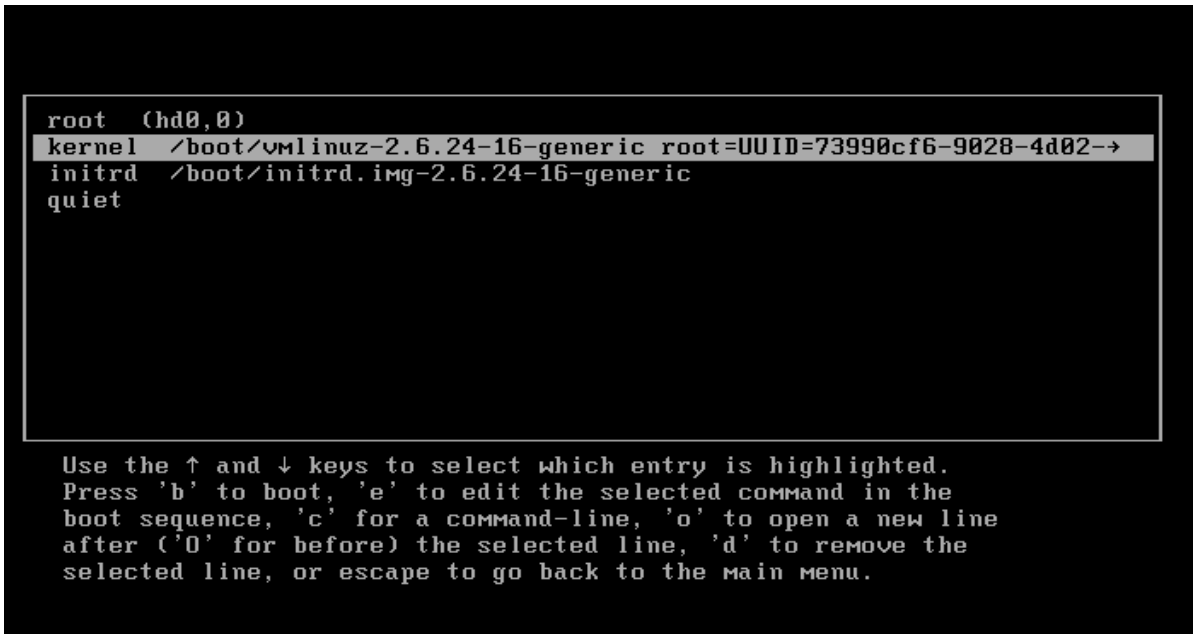
3.7.1 Reset root Password

Ανοίγοντας τον υπολογιστή μας εμφανίζεται στην οθόνη το grub menu για να επιλέξουμε σε πιο λειτουργικό σύστημα θέλουμε να αποκτήσουμε πρόσβαση. Σε περίπτωση που δεν εμφανίζεται απλά πατάμε το πλήκτρο “Esc” και μας εμφανίζεται το παρακάτω:



--GrubBootmenu—

Έπειτα προσπαθούμε να επεξεργαστούμε τα δεδομένα από το boot menu.Πατάμε ¨e¨ για να αρχίσουμε την επεξεργασία του μενού και έπειτα πάμε στην kernel line.



Πατώντας ¨e¨ ξανά και έπειτα αφαιρούμε τον κομμάτι κώδικα που γράφει ***quiet splash*** και γράφουμε στη θέση του ***init=/bin/bash***.

```
      [ Minimal BASH-like line editing is supported.   For
        the   first   word,  TAB  lists  possible  command
        completions.  Anywhere else TAB lists the possible
        completions of a device/filename.  ESC at any time
        exits. ]

<6-9028-4d02-9a46-defececc107d ro init=/bin/bash_
```

Έπειτα πατώντας Enter θα μας εμφανιστεί το παρακάτω:

```
 root  (hd0,0)
 kernel  /boot/vmlinuz-2.6.24-16-generic root=UUID=73990cf6-9028-4d02-→
 initrd  /boot/initrd.img-2.6.24-16-generic
 quiet

   Use the ↑ and ↓ keys to select which entry is highlighted.
   Press 'b' to boot, 'e' to edit the selected command in the
   boot sequence, 'c' for a command-line, 'o' to open a new line
   after ('O' for before) the selected line, 'd' to remove the
   selected line, or escape to go back to the main menu.
```

Έπειτα είμαστε έτοιμοι να εισέλθουμε στο λειτουργικό σύστημα. Πατάμε b ώστε να κανει boot και θα μας βγάλει το παρακάτω παράθυρο εντολών:

```
[  661.733026] scsi1 : ata_piix
[  661.733444] scsi2 : ata_piix
[  661.733506] ata1: PATA max UDMA/33 cmd 0x1f0 ctl 0x3f6 bmdma 0x1050 irq 14
[  661.733557] ata2: PATA max UDMA/33 cmd 0x170 ctl 0x376 bmdma 0x1058 irq 15
[  662.047874] ata2.00: ATAPI: VMware Virtual IDE CDROM Drive, 00000001, max U
A/33
[  662.202812] ata2.00: configured for UDMA/33
[  662.203591] scsi 2:0:0:0: CD-ROM            NECVMWar VMware IDE CDR10 1.00
: 0 ANSI: 5
[  662.203760] scsi 2:0:0:0: Attached scsi generic sg1 type 5
[  662.212401] Driver 'sr' needs updating - please use bus_type methods
[  662.216385] sr0: scsi3-mmc drive: 1x/1x xa/form2 cdda tray
[  662.216631] Uniform CD-ROM driver Revision: 3.20
[  666.103943] kjournald starting.  Commit interval 5 seconds
[  666.104310] EXT3-fs: sda1: orphan cleanup on readonly fs
[  666.105570] EXT3-fs: sda1: 1 orphan inode deleted
[  666.105622] EXT3-fs: recovery complete.
[  671.268246] EXT3-fs: mounted filesystem with ordered data mode.
Begin: Running /scripts/local-bottom ...
Done.
Done.
Begin: Running /scripts/init-bottom ...
Done.
root@(none):/# _
```

Με την παραπάνω διαδικασία διαμορφώσαμε το λειτουργικό σύστημα ώστε να μην έχει root (administrator) με αποτέλεσμα να μας ζητήσει να ορίσουμε ένα νέο με νέο όνομα και κωδικό.

Σε μερικά συστήματα linux μπορεί να χρειάζεται να κάνουμε στα partitions mount/ και /proc. Αυτό γίνεται με πληκτρολογώντας :

```
mount –o remount,rw /
```

```
mount –o remount,rw /proc
```

```
root@(none):/# mount -o remount,rw /
[  884.976778] EXT3 FS on sda1, internal journal
root@(none):/# mount -o remount,rw /proc
root@(none):/# _
```

Σε οποιαδήποτε περίπτωση που δεν είμαστε σίγουροι αν τα partitions του σκληρού μας δίσκου έχουν γίνει mount καλό θα είναι να τρέξουμε τις παραπάνω εντολές αλλιώς μπορεί να μην είναι εφικτό να αλλάξουμε το κωδικό του root. Σε μια τέτοια περίπτωση θα μας εμφανίσει ένα κομμάτι error στην οθόνη μας:

```
passwd: Authentication token lock busy
```

το οποίο δεν μας αφήνει να ορίσουμε ένα νέο κωδικό για τον λογαριασμό του root ή να ανακτήσουμε τον παλιό.

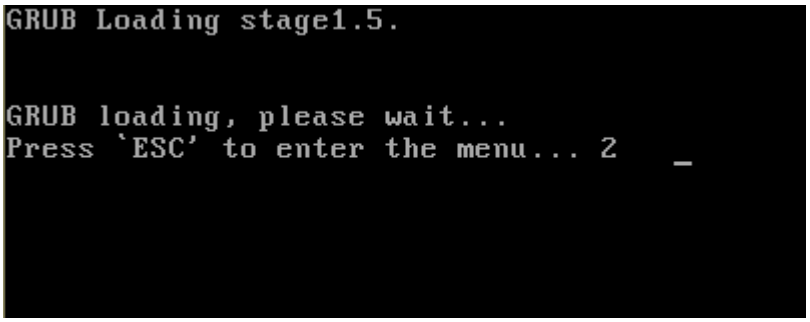
Έπειτα πληκτρολογώντας απλά ¨**passwd**¨ μας ζητείται να δώσουμε ένα νέο κωδικό για τον root.

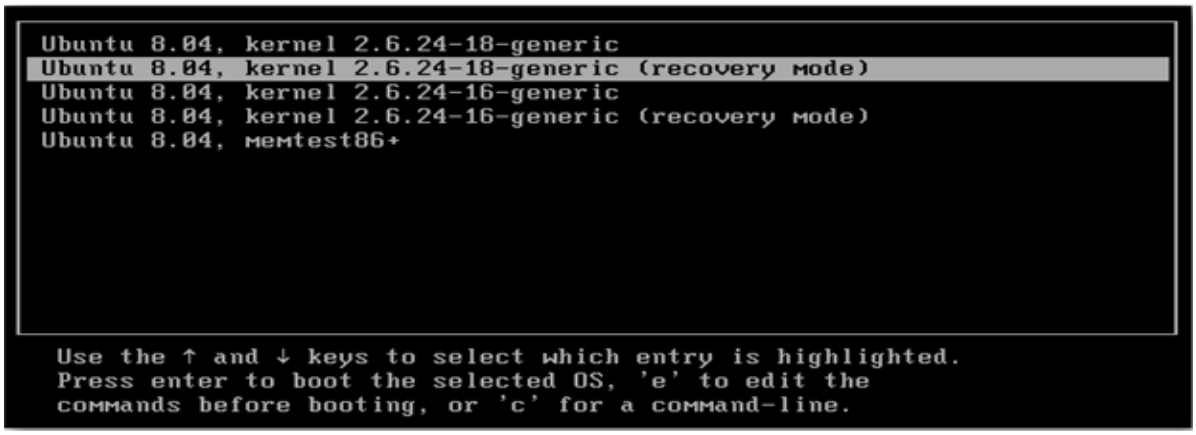
```
Done.
root@(none):/# mount -o remount,rw /
[  884.976778] EXT3 FS on sda1, internal journal
root@(none):/# mount -o remount,rw /proc
root@(none):/# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@(none):/# _
```

Απλά κάνουμε reboot και ο νέος κωδικός έχει καταχωρηθεί!

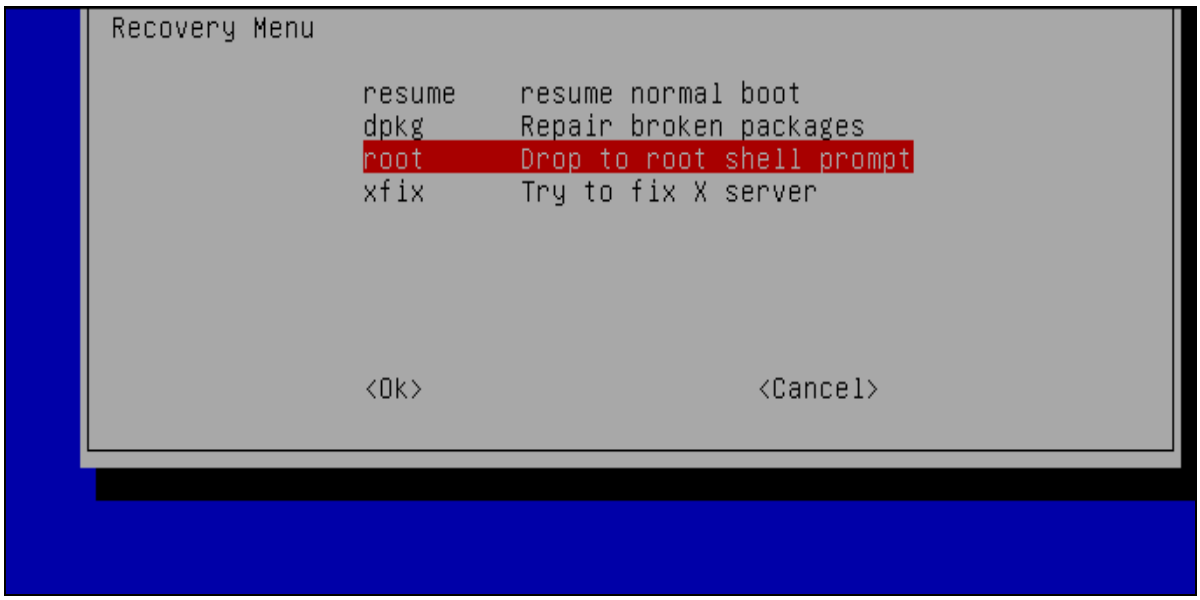
3.7.2 Ανάκτηση κωδικών root με Recovery Mode

Αρχικά ανοίγοντας τον υπολογιστή, επιλέγουμε να εισέλθει με το recovery mode.





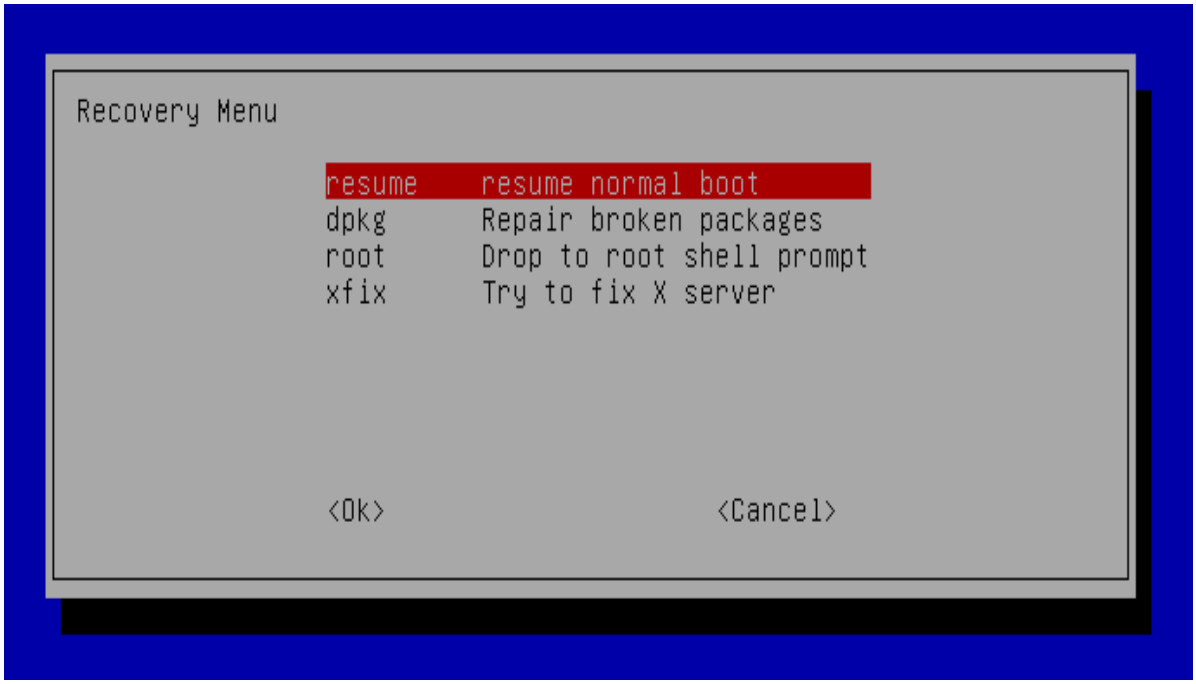
Μετά αφού έχουμε επιλέξει το recovery mode,περιμένουμε λίγο ώστε να τελειώσουν οι διεργασίες που εκτελούνται και έπειτα εμφανίζονται κάποιες επιλογές. Επιλέγουμε την επιλογή ¨*Drop to root shell prompt*¨ , και το σύστημα εισέρχεται στο κομμάτι κώδικα του root (ΠΡΟΣΟΧΗ: Ο λογαριασμός root έχει τα απόλυτα δικαιώματα administrator στο λειτουργικό σύστημα και μπορεί ακόμα και να διαγράψει τα πάντα, οπότε εφίσταται αρκετή προσοχή).



Πληκτρολογούμε τα εξής:

```
root@ubuntu:~# ls /home
linda
root@ubuntu:~# passwd linda
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@ubuntu:~# exit
```

όπου το ¨linda¨ είναι το όνομα του νέου μας account (σε περίπτωση που δεν θυμόμαστε το όνομα του παλιού).Θα μας δοθεί η ευκαιρία να επιλέξουμε ένα νέο κωδικό για τον συγκεκριμένο λογαριασμό. Κατά την διάρκεια που πληκτρολογείτε ο κωδικός, δεν φαίνονται αυτά που τυπώνονται. Παρόλαυτα πληκτρολογώντας τον και πατώντας Enter ο κωδικός γράφεται κανονικά. Ο κωδικός αλλάζει επιτυχώς και έπειτα πατάμε τις εντολή exit.



Γυρνάμε στο αρχικό recovery menu και επιλέγουμε το resume normal boot ώστε να ξεκινήσει κανονικά το λειτουργικό σύστημα, έχοντας ορίσει πλέον τον νέο κωδικό. Σε μερικές εκδόσεις Linux, δεν υπάρχει recovery menu. Από την στιγμή που θα επιλεχθεί το recovery mode οδηγούμαστε απευθείας στο κομμάτι κώδικα. Εκεί πληκτρολογούμε τις εντολές που αναφέρθηκαν παραπάνω και στο τέλος πληκτρολογούμε reboot ώστε να κάνει επανεκκίνηση το σύστημα και να εισέλθουμε κανονικά.

3.8 Η εντολή passwd

Με την χρήση της συγκεκριμένης εντολής μπορούμε να αλλάξουμε τον κωδικό ενός χρήστη. Επίσης μπορεί να χρησιμοποιηθεί για διάφορες παραμέτρους που μπορεί να κάνει ένας administrator σε ένα σύστημα.

Χρήση της εντολής:

$ passwd – Φτιάχνει ένα καινούργιο κωδικό

passwd user1 –Ζητάει καινούργιο κωδικό για τον User1.

passwd -l user1 –Κλειδώνει τον συγκεκριμένο χρήστη.

passwd -u user1 -- Ξεκλειδώνει τον συγκεκριμένο χρήστη.

passwd -d user1 – Αφαιρεί τον κωδικό του χρήστη.

passwd -S user1 –Δείχνει κάποιες πληροφορίες για τον κωδικό του χρήστη.

passwd -n 30 user1 – Θέτει σαν όριο τις 30 μέρες μέχρι να λήξει ο κωδικός του χρήστη

passwd -e user1 – Λήγει τον κωδικό για το συγκεκριμένο account

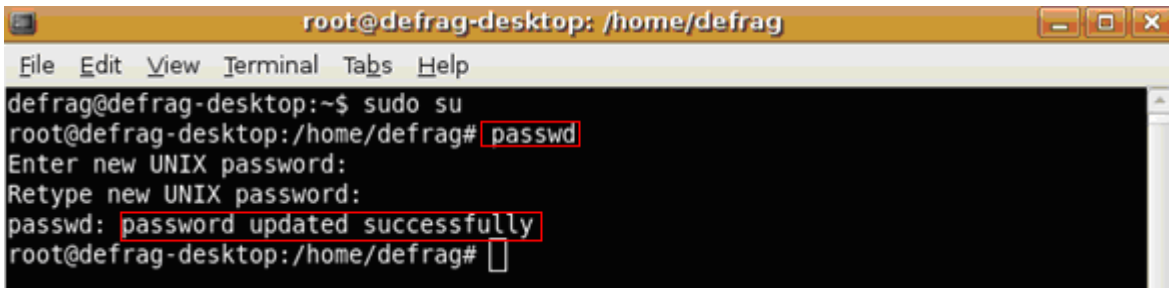
passwd –k –Αλλάζει τον κωδικό μόνο αν έχει λήξει.

passwd –i user1 –θέτει ένα λογαριασμό ανενεργό αφού έχει λήξει

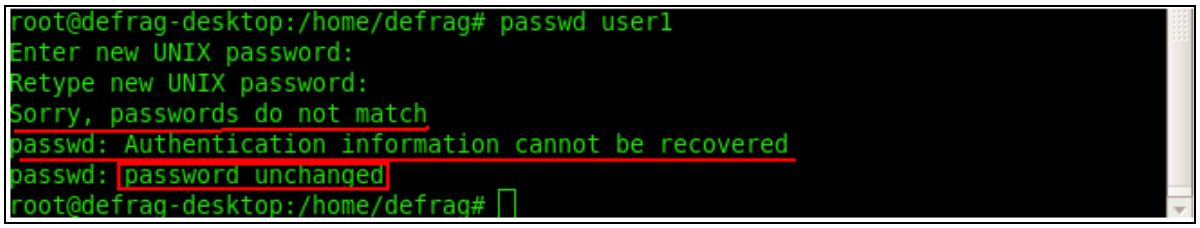
passwd -S user1 – Δείχνει την κατάσταση του συγκεκριμένου λογαριασμού.

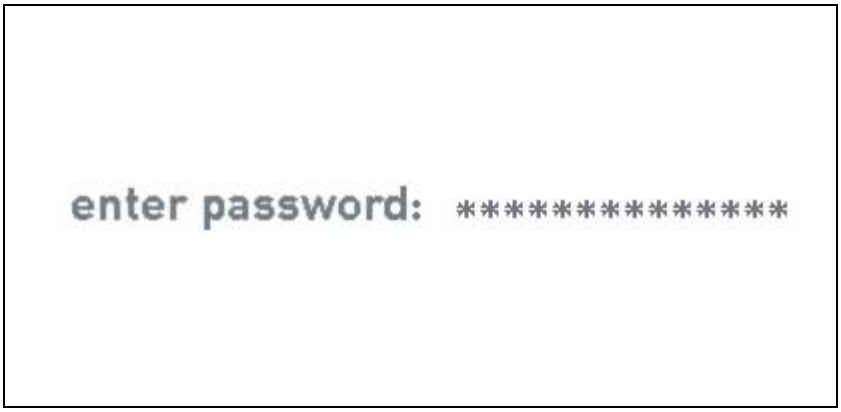
```
File  Edit  View  Terminal  Tabs  Help
Usage: passwd [options] [LOGIN]

Options:
  -a, --all                     report password status on all accounts
  -d, --delete                  delete the password for the named account
  -e, --expire                  force expire the password for the named account
  -h, --help                    display this help message and exit
  -k, --keep-tokens             change password only if expired
  -i, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -l, --lock                    lock the named account
  -n, --mindays MIN_DAYS        set minimum number of days before password
                                change to MIN_DAYS
  -q, --quiet                   quiet mode
  -r, --repository REPOSITORY   change password in REPOSITORY repository
  -S, --status                  report password status on the named account
  -u, --unlock                  unlock the named account
  -w, --warndays WARN_DAYS      set expiration warning days to WARN_DAYS
  -x, --maxdays MAX_DAYS        set maximim number of days before password
                                change to MAX_DAYS

root@defrag-desktop:/home/defrag#
```

Έτσι αν θέλουμε να αλλάξουμε τον κωδικό ενός χρήστη πατάμε απλά την εντολή passwd. Μας ζητείται να εισάγουμε τον νέο κωδικό και έπειτα μια επιβεβαίωση.



Σε περίπτωση που πληκτρολογεί άλλος κωδικός στην επιβεβαίωση τότε ό κωδικός δεν αλλάζει και εμφανίζεται το παρακάτω μήνυμα:





ΚΕΦΑΛΑΙΟ 4 PASSWORD STRENGTH

Η δύναμη κωδικού πρόσβασης είναι μια μέτρηση του πόσο αποτελεσματικός μπορεί να είναι ένας κωδικός πρόσβασης ως πιστοποιητικό επικύρωσης. Η δύναμη ενός κωδικού πρόσβασης είναι μια λειτουργία μήκους πολυπλοκότητας, και τύχης

Αν και οι κωδικοί πρόσβασης εξυπηρετούν έναν ουσιαστικό ρόλο στην ασφάλεια υπολογιστών, πρέπει επίσης να είναι λογικοί και λειτουργικοί για τον χρήστη. Οι κωδικοί πρόσβασης που είναι πολύ δυνατοί τις περισσότερες φορές θα γραφτούν σε χαρτί, το οποίο θεωρείται επίσης ως ένας κίνδυνος ασφάλειας.. Αντίθετα, άλλοι υποστηρίζουν ότι ο καταναγκασμός των χρηστών να θυμηθεί τους κωδικούς πρόσβασης απαιτεί τους αδύνατους κωδικούς πρόσβασης, και θέτει έτσι έναν πολύ μεγαλύτερο κίνδυνο ασφάλειας.

Χρησιμοποιώντας ισχυρούς κωδικούς πρόσβασης μειώνεται ο κίνδυνος παραβίασης της ασφάλειας αλλά οι ίδιοι οι κωδικοί δεν αντικαθιστούν την ανάγκη για άλλους ελέγχους ασφαλείας. Οι κίνδυνοι διατίθενται με διάφορα μέσα όσο αφορά την ασφάλεια των υπολογιστών τα οποία δεν σχετίζονται με την δύναμη των κωδικών και το πόσο ισχυροί είναι. Μερικά τέτοια μέσα είναι:

- software vulnerabilities
- phishing
- keystroke logging
- social engineering
- dumpster diving

4.1 BIT STRENGTH

Τα κοινά κριτήρια για την ανάλυση δύναμης ενός κωδικού πρόσβασης είναι να υπολογιστεί η «δύναμη των bit του», η οποία χρησιμοποιείται επίσης στον υπολογισμό της δύναμης των κλειδιών κρυπτογράφησης. Η δύναμη των bit (Bit Strength) είναι ο συνολικός αριθμός

πιθανών μετέπειτα αλλαγών σε έναν κωδικό πρόσβασης. Παραδείγματος χάριν, ένας κωδικός πρόσβασης με 8-bit δύναμη έχει 256 διαφορετικές δυνατότητες (δηλ., 2^8).Οι κωδικοί πρόσβασης αποτελούνται συνήθως από χαρακτήρες ASCII . Το σύνολο αυτών των εκτυπώσιμων χαρακτήρων περιλαμβάνει τα πεζά και κεφαλαία γράμματα, εκτός από τα ψηφία και τα σύμβολα(συμπεριλαμβανομένης και της στίξης). Αν και τα περισσότερα πληκτρολόγια παράγουν 8-bit χαρακτήρες, στους πιο συγχρόνους υπολογιστές οι χαρακτήρες που χρησιμοποιούνται στους κωδικούς πρόσβασης χρησιμοποιούν σπάνια 8-bit. Ο λόγος είναι ότι δεν είναι όλες οι 8bitες εκδόσεις ASCII ίδιες, ενώ όλες έχουν τους ίδιους χαρακτήρες στους πρώτους 128 (δηλ., 7-bit) θέσεις. Αυτό παράγει 7 μπιτ «δύναμη» το μέγιστο.
Για παράδειγμα, ας υποθέσουμε ότι έχουμε ένα κωδικό 8 χαρακτήρων (και ότι χρησιμοποιούμε αγγλικούς χαρακτήρες). Το αγγλικό αλφάβητο αποτελείτε από 26 γράμματα,οι αριθμοί που μπορούν να χρησιμοποιηθούν είναι 10 (0-9) και τα σύμβολα 33.Αν αυτός ο κωδικός αποτελείτε μόνο από γράμματα τότε θα έχει 26^8 πιθανές τιμές (περίπου 38 bit). Παρακάτω καταγράφονται πόσα bit αντιστοιχούν σε διάφορους συνδιασμούς (το N είναι ο αριθμός των πιθανών χαρακτήρων από το keyboard)

Symbol set	N	bits
Μόνο αριθμοί (0-9)	10	3,32
Μικρά γράμματα (a-z)	26	4,7
Μικρά γράμματα & αριθμοί (a-z,0-9)	36	5,17
Μικρά,κεφαλαία γράμματα & αριθμοί (a-z,A-Z,0-9)	62	5,95
Όλοι οι χαρακτήρες ASCII του keyboard	94	6,55

Από τα παραπάνω καταλαβαίνουμε ότι όσο περισσότερους χαρακτήρες αποτελείται ο κωδικός τόσο μεγαλύτερο bit strength έχει. Επιπρόσθετα, η πολυπλεξία χαρακτήρων αλλα και το μήκος του παίζουν σημαντικό ρόλο ώστε να μην μπορέσει να αποκαλυφθεί ο κωδικός. Ένας 9ψήφιος κωδικός έχει το κατάλληλο bit strenth και σε συνδυασμό με γράμματα και σύμβολα, αυξάνεται το bit strenth του με αποτέλεσμα να τον καθιστά αρκετά ισχυρό.

4.2 Οδηγίες για δυνατούς κωδικούς

Τα ισχυρά passwords έχουν τα ακόλουθα χαρακτηριστικά:

- Περιέχουν κεφαλαία και μικρούς χαρακτήρες
- Περιέχουν αριθμούς, γράμματα και σύμβολα
- Έχουν μήκος τουλάχιστον δεκαπέντε αλφαριθμητικών χαρακτήρων
- Δεν υφίστανται ως λέξεις σε οποιαδήποτε γλώσσα
- Δεν βασίζονται σε προσωπικές πληροφορίες, ονόματα κτλ.
- Τα passwords δεν θα πρέπει ποτέ να γράφονται ή να αποθηκεύονται on-line
- Αποφυγή χρησιμοποίησης λέξεων ή χαρακτήρων που αντιστοιχούν σε usernames, λέξεις λεξικών, ακολουθίες χαρακτήρων ή αριθμών ή βιογραφικές πληροφορίες όπως ονόματα ή ημερομηνίες.

Αντίστοιχα ένας αδύναμος κωδικός έχει τα παρακάτω χαρακτηριστικά:

- Το password περιέχει λιγότερους από δεκαπέντε χαρακτήρες.
- Το password είναι μία λέξη που υπάρχει σε λεξικό.
- Το password είναι μία λέξη κοινής χρήσης όπως:
    - Όνομα οικογένειας, κατοικίδιων ζώων, φίλων, συναδέλφων, χαρακτήρων φαντασίας κτλ.
    - Όρους και ονόματα υπολογιστών, εντολών, sites, εταιριών, λογισμικού
    - Το όνομα του οργανισμού
    - Γενέθλια και άλλη προσωπική πληροφορία, όπως διευθύνσεις ή τηλεφωνικοί αριθμοί.
    - Λέξεις ή αριθμοί όπως aaabbb, qwerty, zyxwvuts, 123321 κτλ.
    - Λέξεις στις οποίες προηγείται ή ακολουθεί ένας ακέραιος (πχ. Secret1, 1secret)

Μερικά παραδείγματα αδύνατων κωδικών που επιλέγουν συνήθως οι χρήστες είναι:

- κενό
- οι λέξεις "password", "passcode", "admin" και παράγωγά τους
- το username
- μια λέξη από λεξικό
- ένα όνομα μιας προσωπικότητας ή διασημότητας που συμπαθούν
- την πινακίδα του αυτοκινήτου τους
- μια σειρά από γράμματα από ένα τυποποιημένο σχεδιάγραμμα πληκτρολογίου πχ asdfg ή qwertyuiop

Μερικά passwords τα οποία χρησιμοποιούνται αρκετά συχνά είναι:

123456	Password	12345678	qwerty	asdfgh
xxxxxxx	pass	null	wordpass	lol
qweasd	112233	king	freedom	secret
121212	hello	chelsea	money	aaaaaa
player	booboo	cocacola	666666	john
abc123	mike	diablo	god	111111
love	stupid	gordon	helpme	admin
test	access	1234	killer	enter

Λίστες με τέτοια passwords υπάρχουν στα παρακάτω links:

http://www.whatsmypass.com/?p=415

http://tech.yahoo.com/blog/hughes/11844

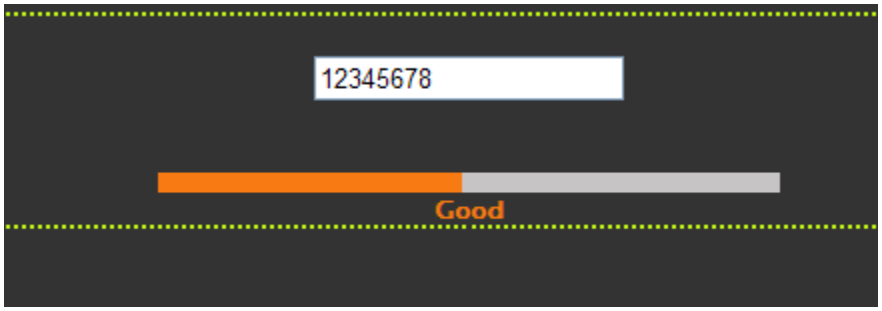
http://www.thenetworkadministrator.com/passwords.htm

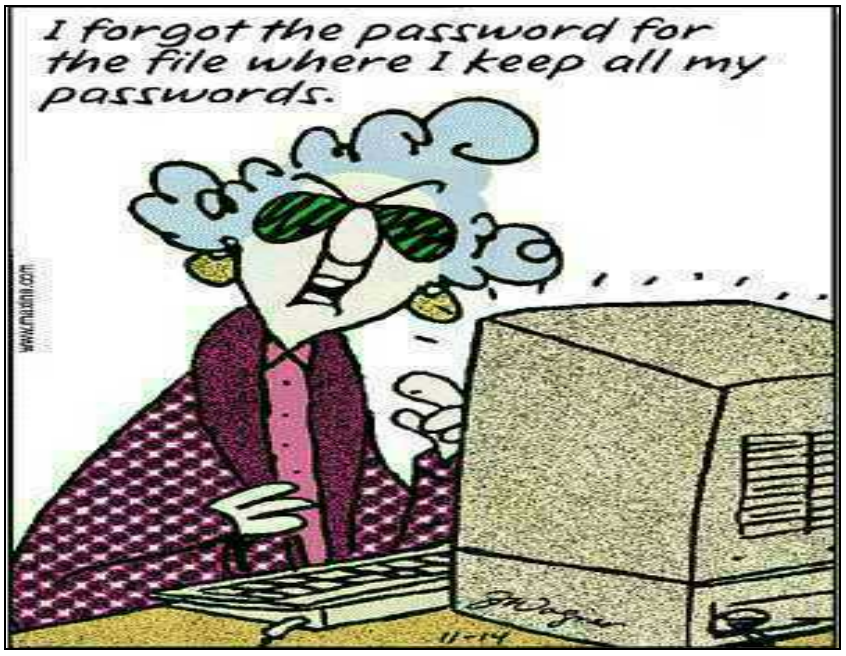
4.3 ΜΕΘΟΔΟΙ ΕΛΕΓΧΟΥ ΔΥΝΑΜΗΣ ΤΟΥ PASSWORD

4.3.1 PASSWORDMETER

Υπάρχουν διάφοροι τρόποι και μέσα ώστε να μπορέσει κάποιος να ελέγξει το πόσο δυνατός και ασφαλής είναι ο κωδικός που χρησιμοποιεί. Στην ιστοσελίδα www.passwordmeter.com/ έχουμε την δυνατότητα να το ελέγξουμε βάζοντας απλά το password μας και το πρόγραμμα θα μας δείξει αν όντως ο κωδικός μας είναι δυνατός και πόσο ασφαλής είναι. Μας εμφανίζει ένα box το οποίο δείχνει τι χρησιμοποιήσαμε στον κωδικό (γράμματα, αριθμούς, κεφαλαία κτλ) και επισημαίνει τι κάνει τον κωδικό μας αδύναμο. Αν για παράδειγμα έχουμε χρησιμοποιήσει πολλές φορές ένα γράμμα τότε το πρόγραμμα θα μας το δείξει και έτσι εμείς θα γνωρίζουμε την αδυναμία του κωδικού μας ώστε να μπορέσουμε να τον αλλάξουμε και να τον κάνουμε πιο ασφαλή.

Γενικότερα δεν είναι καλό να χρησιμοποιούμε το web γιατί δεν υπάρχει αρκετή ασφάλεια και οι κωδικοί καταγράφονται.. Παρόλαυτά τα συγκεκριμένα προγράμματα μπορούν να δοκιμαστούν ώστε μέσα από αυτά να καθοδηγηθεί ο χρήστης και να καταλάβει την σωστή δημιουργία ενός κατάλληλου κωδικού.





The Password Meter

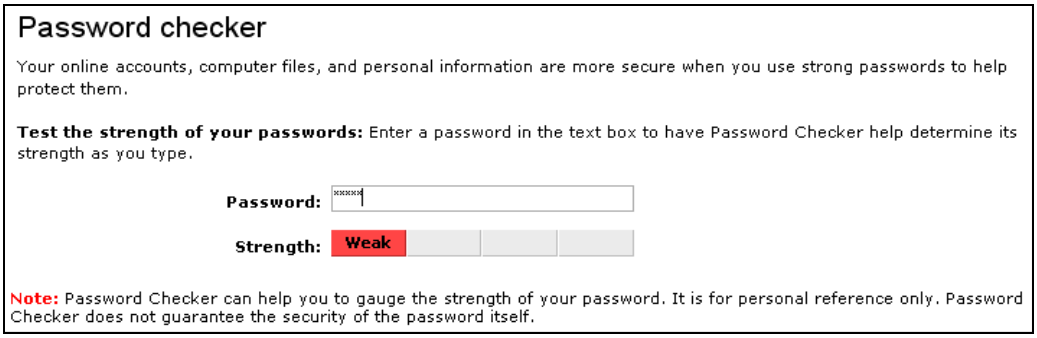
Test Your Password		Minimum Requirements
Password:	*********	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	88%	
Complexity:	Very Strong	

Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	9	+ 36
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 16
✓	Lowercase Letters	Cond/Incr	+((len-n)*2)	5	+ 8
✓	Numbers	Cond	+(n*4)	1	+ 4
✓	Symbols	Flat	+(n*6)	2	+ 12
✓	Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
✓	Requirements	Flat	+(n*2)	5	+ 10
Deductions					
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Incr	-(n(n-1))	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	2	- 4
✓	Consecutive Numbers	Flat	-(n*2)	0	0
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0

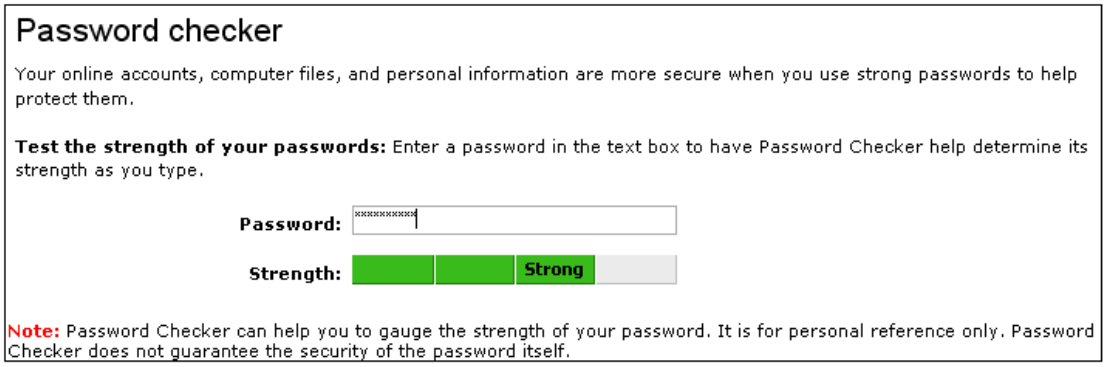
Χρησιμοποιώντας το παραπάνω πρόγραμμα μπορεί ο χρήστης να δει τι περιέχεται στον κωδικό του και αν αυτό προσμετράτε θετικά ή αρνητικά.Για παράδειγμα αν χρησιμοποιούνται μόνο μικροί χαρακτήρες το πρόγραμμα θα το καταγράψει και θα το μετρήσει αρνητικά ως προς τη δομή του κωδικού. Θα αναλύσει τον κωδικό και θα υποδείξει στο χρήστη πόσο δυνατός είναι με ένα δείκτη %. Παραπάνω βάλαμε ένα 8 ψήφιο κωδικό και το πρόγραμμα μας υπέδειξε τα θετικά και τα αρνητικά του.Στην προκειμένη περίπτωση ο κωδικός ήταν αρκετά ισχυρός και τα θετικά υπερτερούσαν των αρνητικών με αποτέλεσμα ο κωδικός να αποδειχθεί 88% ισχυρός.

4.3.1 MICROSOFT PASSWORD CHECKER

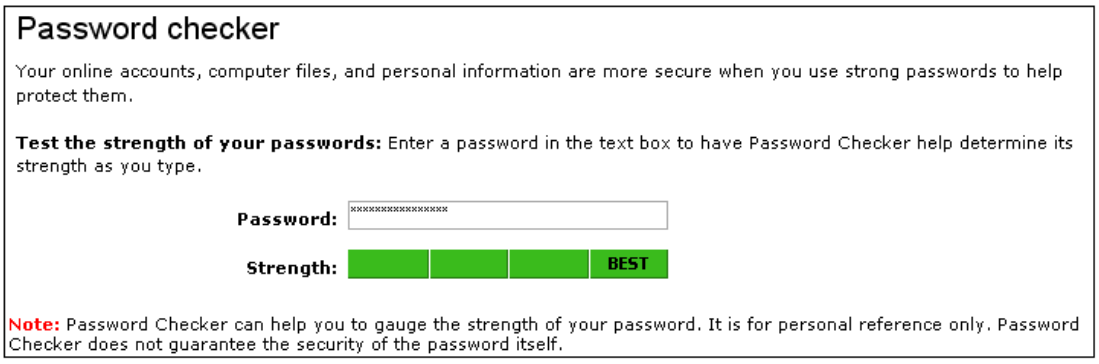
Ένα άλλο URL για τον έλεγχο του κωδικού μας είναι το http://www.microsoft.com/protect/yourself/password/checker.mspx. Το συγκεκριμένο πρόγραμμα είναι πιο απλό και απλά ενημερώνει τον χρήστη για την δύναμη του κωδικού και τίποτα περεταίρω. Αν ο κωδικός για παράδειγμα είναι αδύναμος τότε θα έχουμε την ένδειξη "weak" όπως φαίνεται παρακάτω:



Στην περίπτωση που ο κωδικός μας είναι δυνατός (αλλά και πάλι όχι αρκετά δυνατός) τότε θα μας επισημάνει ότι ο κωδικός μας είναι εντάξει («strong»):

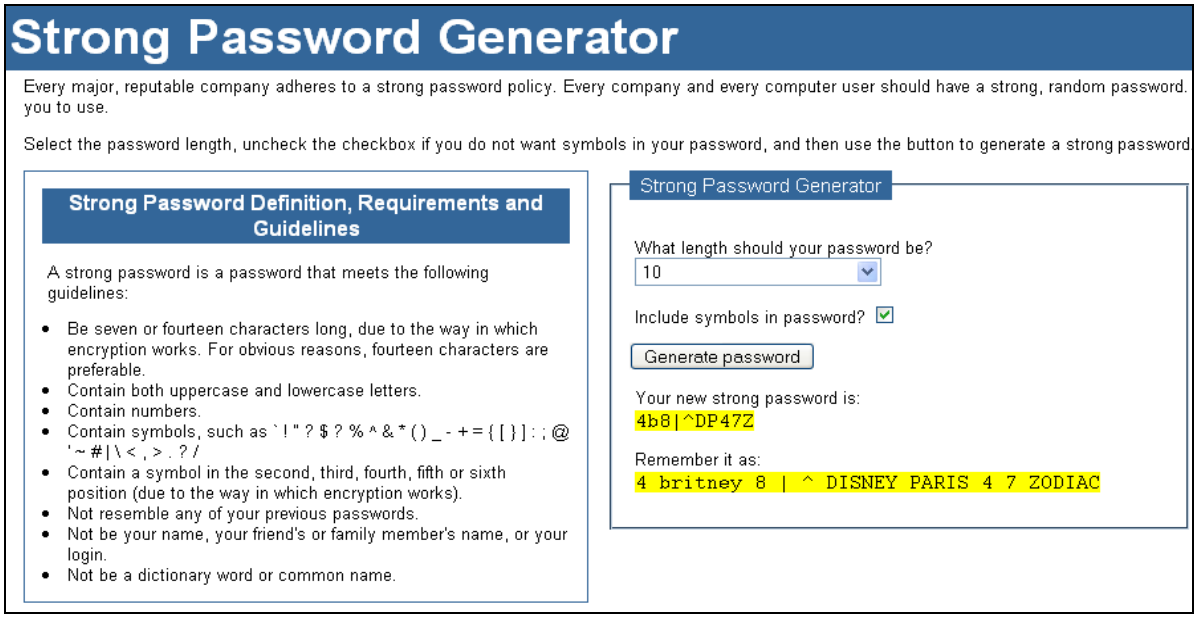


Αν τελικά έχουμε χρησιμοποιήσει κάποιο κωδικό ώστε να είναι αρκετά δυνατός και σχεδόν αδύνατο να σπάσει τότε το πρόγραμμα θα μας βγάλει το παρακάτω επισημαίνοντας ότι ο κωδικός που χρησιμοποιήσαμε είναι πάρα πολύ καλός:



4.4 STRONG PASSWORD GENERATOR

Το συγκεκριμένο εργαλείο χρησιμοποιείται για την δημιουργία ισχυρών κωδικών. Είναι αρκετά χρήσιμο στο να φτιάχνει κωδικούς αρκετά πολύπλοκους και προσπαθεί επίσης να δώσει κάποια βοήθεια ώστε να μπορεί ο χρήστης να τον απομνημονεύσει ευκολότερα.



Παρατηρούμε ότι το πρόγραμμα μας δίνει την δυνατότητα να επιλέξουμε από πόσους χαρακτήρες θα αποτελείτε ο κωδικός μας και αν θέλουμε να περιλαμβάνει σύμβολα. Σαφώς με την χρήση συμβόλων ο κωδικός θα είναι αρκετά ισχυρότερος, αυτό όμως δεν σημαίνει ότι και χωρίς κανένα σύμβολο δεν θα είναι δυνατός. Επίσης στο αριστερό μέρος της οθόνης μας έχει ένα password policy το οποίο μας υποδεικνύει την σωστή χρήση κάποιων παραμέτρων ώστε να φτιαχτεί ένας ισχυρός κωδικός και τι πρέπει να περιέχει.

Το παραπάνω πρόγραμμα το βρήκα στην διεύθυνση:
http://strongpasswordgenerator.com/

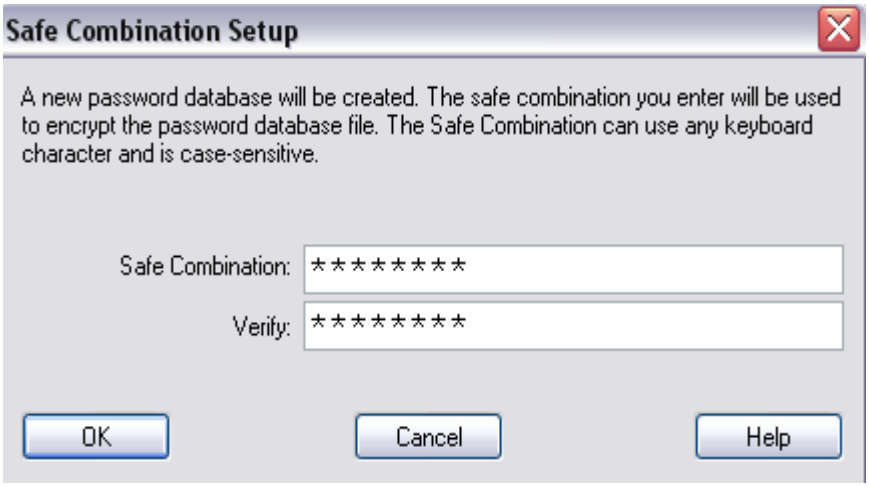
4.5 ΚΛΕΙΔΩΜΑ ΑΡΧΕΙΩΝ & ΑΣΦΑΛΕΙΑ ΚΩΔΙΚΩΝ

Παρ'όλη την ασφάλεια που μπορεί να παρέχουν κάποιοι κωδικοί η απομνημόνευσή τους μπορεί να φαντάζει δύσκολη για κάποιους χρήστες είτε για την πολυπλοκότητά τους είτε γιατί το να θυμάται κάποιος ένα σωρό κωδικούς από mail,credit cards, paypal cards δεν είναι κάτι το εύκολο. Γιαυτούς τους λόγους κατασκευάστηκαν κάποια προγράμματα τα οποία επέτρεπαν στο χρήστη να κρατάει τους κωδικούς του ασφαλείς σε ένα μόνο αρχείο και να θυμάται μόνο ένα κύριο κωδικό ώστε να έχει πρόσβαση σε όλους τους άλλους.

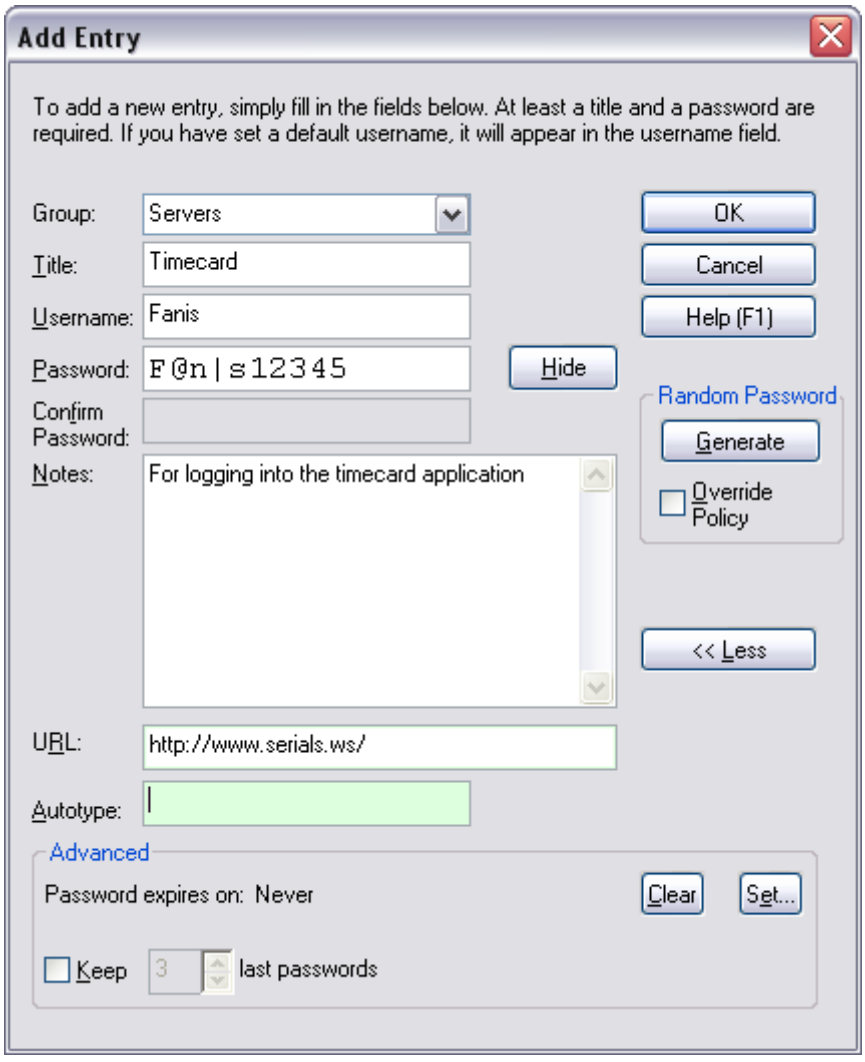
4.5.1 PASSWORD SAFE

Το Password safe είναι ένα πρόγραμμα ανάκτησης κωδικών των Windows. Αφού ο χρήστη συμπληρώσει τον master password που έχει επιλέξει, έχει πρόσβαση σε όλα τα στοιχεία λογαριασμών τα οποία έχει αποθηκεύσει στο πρόγραμμα. Τα δεδομένα μπορούν να οργανωθούν ανά κατηγορίες, να ταξινομηθούν και να αναζητηθούν. Με το Password Safe υπάρχει η επιλογή να οργανωθούν τα δεδομένα ανάλογα τις προτιμήσεις του χρήστη –για παράδειγμα οργανωμένα κατά ID'S, κατηγορίες, ιστοσελίδες, τοποθεσίες κ.α. Το user interface του είναι αρκετά εύχρηστο και πρακτικό και ο χρήστης εξοικειώνεται γρήγορα μαζί του.
Κατά τη εκκίνηση εμφανίζεται η παρακάτω οθόνη

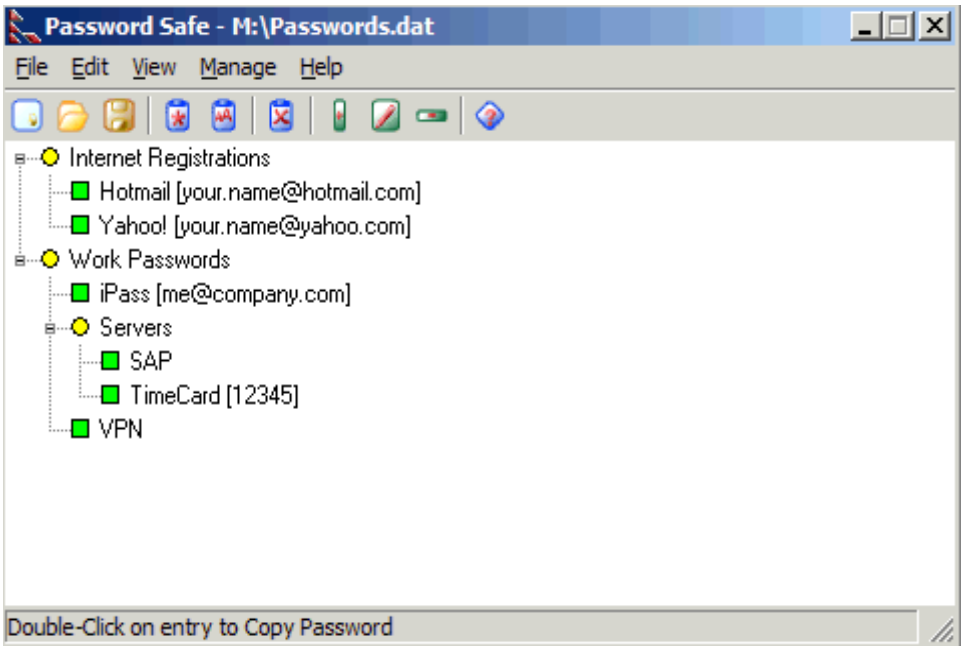
Επιλέγουμε το New Database και δημιουργούμε μία καινούργια βάση δεδομένων για να αποθηκεύονται τα δεδομένα του. Μόλις το αποθηκεύσουμε μας εμφανίζεται ένα παράθυρο στο οποίο μας ζητείται να εισάγουμε τον master password που θέλουμε.



Από το μενού επιλέγουμε Edit>Add Entry και γράφουμε τα στοιχεία τα οποία θέλουμε να καταχωρηθούν στο Password Safe.



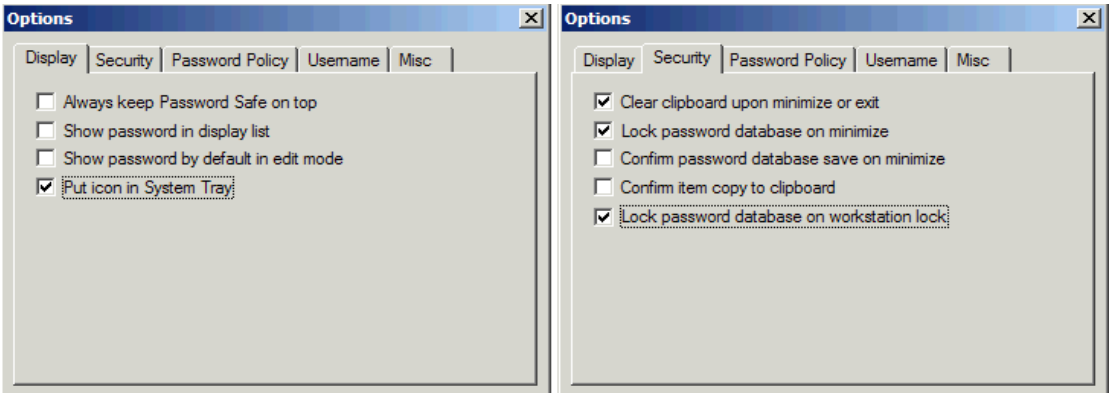
Μπορούμε να βάλουμε πολλά στοιχεία και να τα κατατάξουμε ανάλογα τις προτιμήσεις μας. Για παράδειγμα παρακάτω αναγράφονται στοιχεία λογαριασμών από mails, κωδικούς καρτών, servers και διάφορα άλλα.



Για την ανάκτηση των κωδικών απλώς πατάμε διπλό κλικ στην επιλογή που θέλουμε. Αυτό αντιγράφει τον κωδικό και έπειτα μπορούμε να το επικολλήσουμε σε ένα κατάλληλο pass field για παράδειγμα στο Word.

Αυτή είναι μια αρκετά έξυπνη επιλογή του Password Safe αφού για παράδειγμα αν δουλεύουμε μαζί με κάποιο άλλο άτομο και θέλουμε να δούμε κάποιο κωδικό, ο οποίος μπορεί να περιέχει κάποιο χρήσιμο URL ή άλλου είδους χρήσιμες πληροφορίες, θα το επιλέξουμε χωρίς να αποκαλυφθεί ο κωδικός στην πραγματικότητα.

Για μεγαλύτερη ασφάλεια του προγράμματος, επιλέγουμε Manage>Options και από το security window κάνουμε τις παρακάτω ρυθμίσεις, με τις οποίες ο κωδικός δεν θα μπορεί να αντιγραφεί από την στιγμή που θα κλείσει το πρόγραμμα, το πρόγραμμα όταν ελαχιστοποιείται θα ζητείται κωδικός μετά, για την επαναφορά του και να κλειδώνει η βάση δεδομένων του προγράμματος κάθε φορά που κλείνει το πρόγραμμα.



Το παραπάνω πρόγραμμα μπορεί να βρεθεί στη παρακάτω διεύθυνση:

http://passwordsafe.sourceforge.net/

4.5.2 Microsoft Private Folder

Ένας άλλος τρόπος ώστε να μπορούμε να κρατάμε ένα αρχείο με κωδικούς ή κάποια αρχεία ασφαλή και να μην μπορεί κάποιος τρίτος να έχει πρόσβαση είναι με την ιδιότητα να τα έχουμε σε ένα φάκελο ο οποίος θα είναι private και θα έχει κάποιο master password.. Ένα παράδειγμα είναι το Microsoft private Folder το οποίο μας δίνει τη δυνατότητα να αποθηκεύσουμε ότι αρχεία θέλουμε σε ένα φάκελο και να μην επιτρέπεται από άλλους η χρήση αυτών των αρχείων. Το εν λόγω πρόγραμμα μπορεί να βρεθεί στην ηλεκτρονική διεύθυνση http://fileforum.betanews.com/detail/Microsoft_Private_Folder/1152200243/1 .

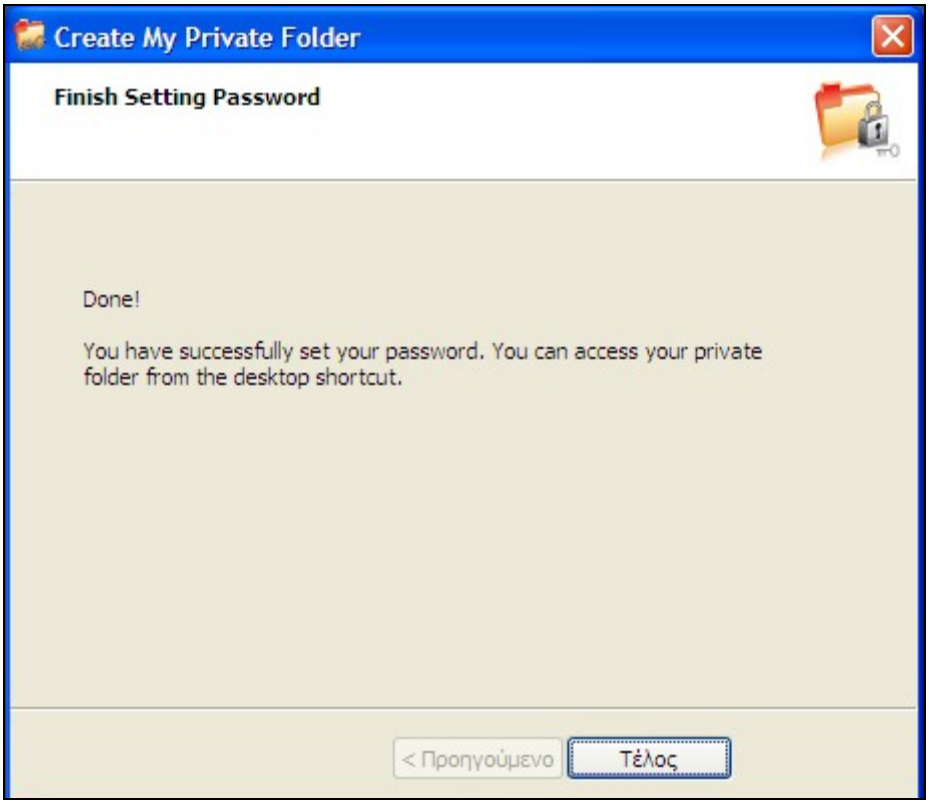
Μετά τη λήψη του αρχείου και την εγκατάσταση της εφαρμογής, δημιουργείται ένα εικονίδιο στην Επιφάνεια Εργασίας με όνομα *My Private Folder*.

Στην πραγματικότητα δημιουργείται ο φάκελος στη διαδρομή:
c:\documents and settings\username\My Private Folder

Στη συνέχεια με διπλό κλικ στο εικονίδιο τρέχει ο οδηγός δημιουργίας του προσωπικού φακέλου και το κλείδωμά του με κωδικό πρόσβασης.

Έπειτα μας ζητείται να εισάγουμε ένα master password

Αφού εισάγουμε τον κωδικό το πρόγραμμα μας ειδοποιεί ότι όλα είναι εντάξει και ότι ο φάκελος είναι έτοιμος.



Πλέον, με διπλό κλικ ζητείται ο κωδικός πρόσβασης στο φάκελο και με το σωστό κωδικό ο φάκελος ξεκλειδώνει. Εμφανίζεται επίσης και στο tray (γραμμή ειδοποιήσεων) εικονίδιο της εφαρμογής με επιπλέον επιλογές και **επιλογή για κλείδωμα του φακέλου.**
Στην επιλογή Options -> Idle Time Before Auto-Lock μας δίνεται η δυνατότητα αυτόματου κλειδώματος του φακέλου μετά από xxx λεπτά χωρίς πρόσβαση σε κάποιο αρχείο του (αδράνεια).

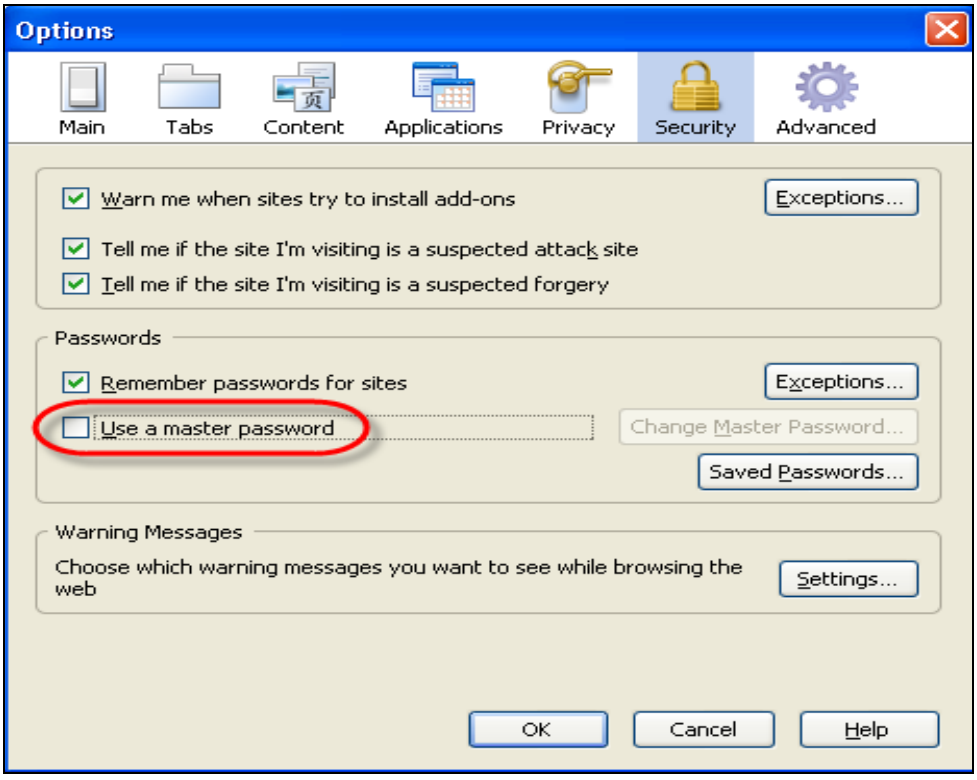
4.6 Ασφάλεια κωδικών στο Διαδίκτυο- Mozilla Firefox

4.6.1 Προστασία αποθηκευμένων κωδικών πρόσβασης χρησιμοποιώντας ένα κύριο κωδικό πρόσβασης (master password).

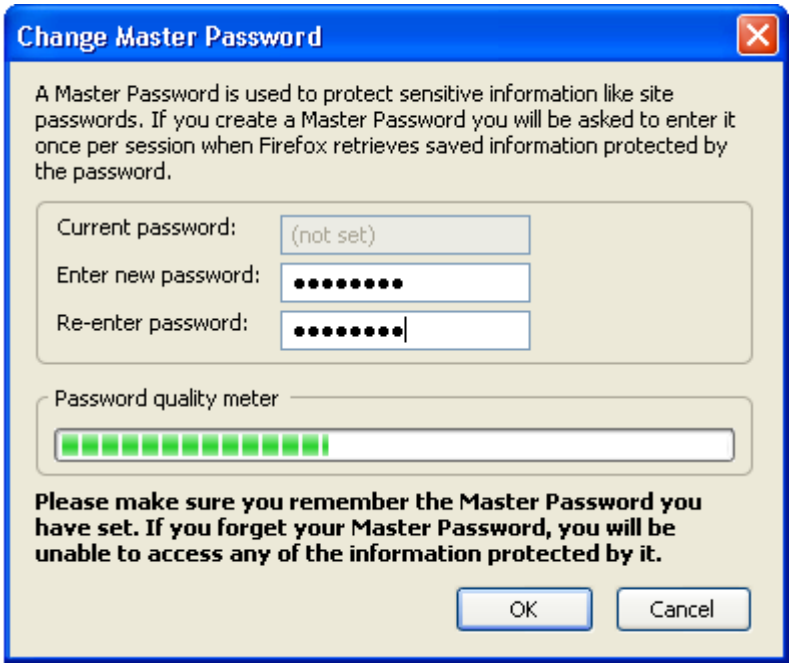
Όπως άλλες μηχανές αναζήτησης, ο Firefox μπορεί να αποθηκεύσει τα ονόματα χρήστη και τους κωδικούς πρόσβασης που χρησιμοποιούνται είτε στο ηλεκτρονικό ταχυδρομείο είτε σε υπηρεσίες online συναλλαγών, όπως η ιστοσελίδα μιας τράπεζας. Δεδομένου ότι αυτά τα στοιχεία αποθηκεύονται σε φακέλους στον υπολογιστή του χρήστη, αντιπροσωπεύουν έναν κίνδυνο ασφάλειας και πρέπει να προστατευθούν. Χρησιμοποιώντας την ιδιότητα του Master Password μπορούν να προστατευθούν όλα τα usernames και τα passwords με ένα κύριο κωδικό (master). Όταν εισέλθει ο χρήστης σε κάποιο λογαριασμό του που έχει το username του τότε εκτός από το password του, ζητείται και το master password το οποίο είναι κοινό προς όλα τα accounts.

Ο Firefox δεν χρησιμοποιεί master passwords κατά την πρώτη εκκίνησή του. Ο χρήστης πρέπει να ενεργοποιήσει μόνος του την επιλογή του master password:

1. Από το μενού του Firefox επιλέγουμε Tools>Options
2. Επιλέγουμε το Security Icon και τσεκάρουμε το **Use a master password**.

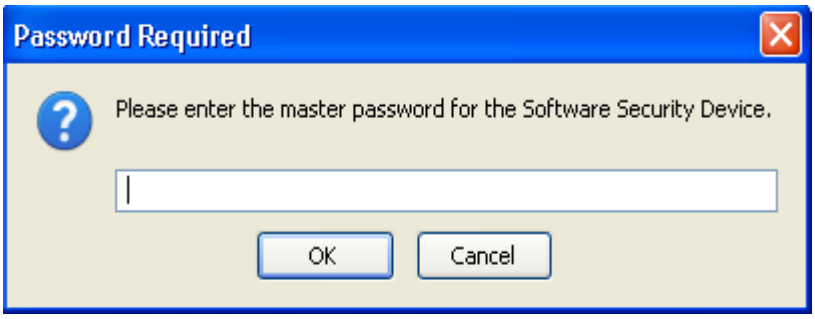


Εμφανίζεται το παράθυρο για την εισαγωγή του κωδικού. Όσο εισάγεται ο κωδικός υπάρχει ένα password meter το οποίο καταγράφει και βρίσκει το επίπεδο δυσκολίας του κωδικού και το πόσο δυνατός είναι.

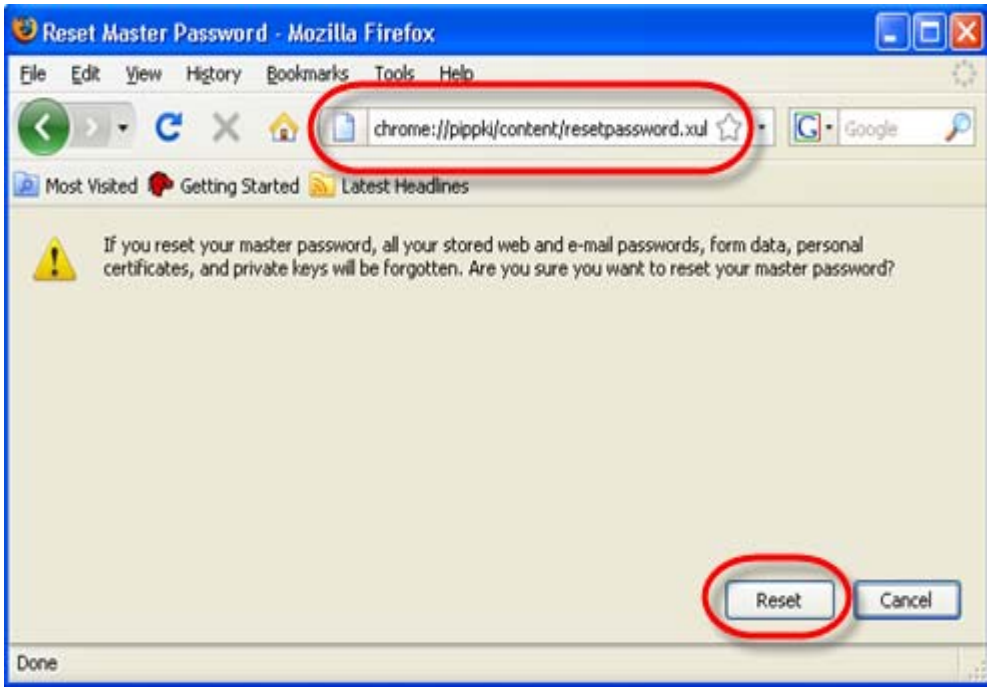


Ο κωδικός πρέπει να γραφεί 2 φορές ώστε να επιβεβαιωθεί ότι γράφτηκε σωστά.

Πλέον ο master password θα ζητείται κάθε φορά που θα επισκεπτόμαστε μια ιστοσελίδα και θα χρησιμοποιείται το username μας.



Σε περίπτωση που ξεχαστεί ο κύριος κωδικός, πληκτρολογούμε στο παράθυρο του URL *chrome://pippki/content/resetpassword.xul* και πατάμε Enter. Θα εμφανιστεί μία σελίδα η οποία λέγεται Reset Master Password, και απλά θα επιλέξουμε να μας κάνει reset το Master Password με την υποσημείωση όμως ότι θα αφαιρέσει και όλα τα usernames και passwords τα οποία έχουν σωθεί.



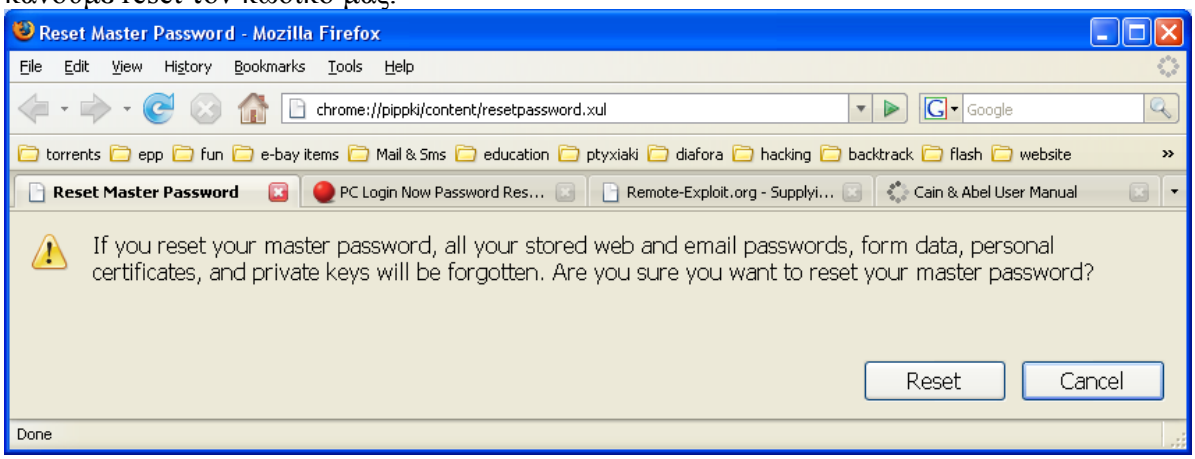
Σε περίπτωση που θέλουμε να αλλάξουμε τον κύριο κωδικό

1. Από το μενού του Firefox πάμε Tools>Options
2. Επιλέγουμε το Security Icon
3. Πατάμε Change Master Password και αλλάζουμε τον κωδικό.

4.6.2 Cracking Master Password

Μπορεί ένας master password να προσφέρει αρκετή ασφάλεια στον υπολογιστή όμως για κάποιον που ξέρει είναι εύκολο να ανακτήσει τον κωδικό έστω και αν δεν τον γνωρίζει, από την στιγμή που αποκτήσει πρόσβαση στον υπολογιστή μας..
Αρχικά ανοίγοντας τον browser, γράφουμε πάνω στο link το εξής:
chrome://pippki/content/resetpassword.xul

Θα μας εμφανιστεί ένα παράθυρο οπου θα μας ζητείται επιβεβαίωση αν θέλουμε να κάνουμε reset τον κωδικό μας.



Πατώντας reset ο κωδικός παύει να υπάρχει και έτσι οποιοσδήποτε μπορεί να δει πλέον τους κωδικούς.

Επίσης υπάρχουν αρκετά cracking tools στην αγορά τα οποία υποστηρίζουν ότι μπορούν να σπάσουν τους κωδικούς του browser, όπως το Mozilla Password recovery,το IE Passview,το Firekeeper και άλλα πολλά. Παρόλαυτά όμως κανένα από αυτά δεν μπορεί να σπάσει το master password ή και να μπορεί θα του πάρει άπειρο χρόνο. Συνοψίζοντας η ασφάλεια που μπορεί να σου προσφέρει ένα master password είναι αρκετά υψηλή και ο μόνος τρόπος να υποκλέψει κάποιος τους κωδικούς είναι να έχει πρόσβαση στο σύστημά.

ΚΕΦΑΛΑΙΟ 5 PASSWORD POLICY

Το password policy είναι ένα σύνολο κανόνων με σκοπό να ενισχύσουν την ασφάλεια υπολογιστών ενθαρρύνοντας τους χρήστες να υιοθετήσουν ισχυρούς κωδικούς πρόσβασης και να τους χρησιμοποιήσουν κατάλληλα. Ένα password policy είναι συχνά ένα μέρος των επίσημων κανονισμών μιας οργάνωσης και μπορεί να διδαχθεί ως κομμάτι μιας συνειδητοποιημένης ασφάλειας. Το password policy μπορεί είτε να είναι συμβουλευτικό είτε εξουσιοδοτημένο από τεχνικά μέσα.

Τα κύρια χαρακτηριστικά ενός password policy περιλαμβάνουν:

5.1 Μήκος και σχηματισμός του password

Πολλά policies απαιτούν ένα ελάχιστο μήκος κωδικού πρόσβασης, συνήθως 6 με 8 χαρακτήρες. Μερικά συστήματα επιβάλλουν ένα μέγιστο μήκος κωδικού για συμβατότητα με άλλα συστήματα.

Μερικά policies επίσης, προτείνουν ή επιβάλλουν απαιτήσεις σε τι τύπου κωδικό μπορεί ένας χρήστης να επιλέξει, όπως:

- τη χρήση κεφαλαίων και μικρών γραμμάτων
- την ενσωμάτωση ενός ή περισσοτέρων αριθμητικών ψηφίων
- την ενσωμάτωση ειδικών χαρακτήρων (σημεία στίξης κτλ)
- την απαγόρευση λέξεων που βρίσκονται σε ένα λεξικό η είναι σχετικές με προσωπικά στοιχεία του χρήστη
- την απαγόρευση κωδικών που ταιριάζουν με ημερολογιακές ημερομηνίες, με
- αριθμούς πινακίδων κυκλοφορίας ή άλλους κοινούς αριθμούς
- Άλλα συστήματα δημιουργούν τον κωδικό πρόσβασης για τους χρήστες ή αφήνουν το χρήστη να επιλέξει ένα από έναν περιορισμένο αριθμό κωδικών.

5.2 ΚΥΡΩΣΕΙΣ

Τα password policies μπορούν να περιλαμβάνουν προοδευτικές κυρώσεις, ξεκινώντας από προειδοποιήσεις και καταλήγοντας σε πιθανή απώλεια των δικαιωμάτων ενός υπολογιστή ή τον τερματισμό της συνεργασίας. Όπου η εμπιστευτικότητα εξουσιοδοτείται από το νόμο πχ με ταξινομημένες πληροφορίες, μια παραβίαση ενός password policy μπορεί να είναι και ένα ποινικό αδίκημα. Μερικοί θεωρούν μια πειστική εξήγηση της σπουδαιότητας της ασφάλειας περισσότερο αποτελεσματική παρά τις απειλές των κυρώσεων.

5.3 ΕΠΙΛΟΓΗ ΕΝΟΣ ΚΑΤΑΛΛΗΛΟΥ PASSWORD POLICY

Το επίπεδο δύναμης ενός κωδικού πρόσβασης εξαρτάται, εν μέρει, από τον τρόπο με τον οποίο μπορεί εύκολα ένας επιτιθέμενος να μαντέψει τον κωδικό με διάφορα μέσα και τρόπους. Μερικά συστήματα περιορίζουν σε ένα συγκεκριμένο αριθμό το πόσες φορές μπορεί ο χρήστης να εισάγει ένα λάθος κωδικό, προτού να επιβληθεί μια καθυστέρηση ή να παγώσει ο λογαριασμός. Από την άλλη μεριά όμως μερικά συστήματα παρέχουν μια ειδικά hashed έκδοση του κωδικού πρόσβασης έτσι ώστε να μπορεί ο καθένας να ελέγξει την ισχύ του. Όταν γίνει αυτό, ένας επιτιθέμενος μπορεί να δοκιμάσει κωδικούς πολύ γρήγορα και για αυτό το λόγο χρειάζονται πολύ ισχυρότεροι κωδικοί για μια ικανοποιητική ασφάλεια. Πιο αυστηρές απαιτήσεις είναι επίσης κατάλληλες για λογαριασμούς με μεγαλύτερα προνόμια, όπως οι root ή οι διαχειριστές συστήματος (system administrators).

5.4 Εκτιμήσεις χρησιμοποίησης

Τα password policies είναι συνήθως μια ανταλλαγή μεταξύ θεωρητικής ασφάλειας και πρακτικότητας της ανθρώπινης συμπεριφοράς. Για παράδειγμα:

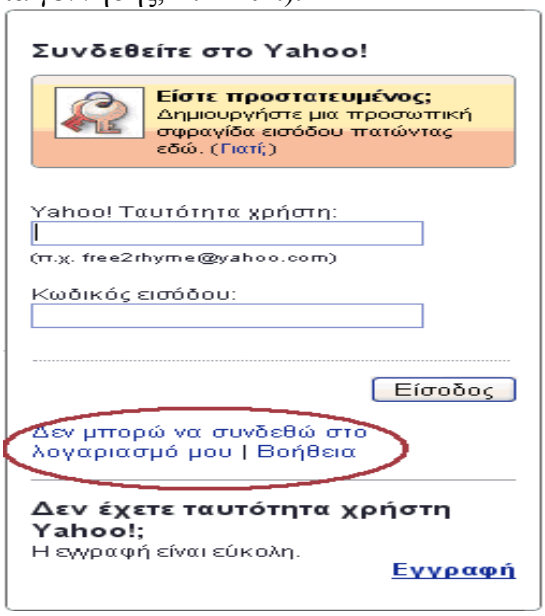
1) Η απαίτηση των υπερβολικά σύνθετων passwords και ο καταναγκασμός να αλλάζονται συχνά αναγκάζουν τους χρήστες να γράφουν τους κωδικούς σε μέρη τα οποία είναι εύκολο για κάποιον ανεπιθύμητο να τα βρει, όπως για παράδειγμα σε ένα post-it δίπλα στον υπολογιστή ή σε ένα Rolodex.
2) Οι χρήστες έχουν συχνά δεκάδες κωδικούς τους οποίους διαχειρίζονται. Θα ήταν πιο ρεαλιστικό να προτεινόταν ένας απλός κωδικός για όλες τις εφαρμογές χαμηλής ασφάλειας όπως για παράδειγμα το διάβασμα μιας on-line εφημερίδας ή την πρόσβαση σε ιστοχώρους ψυχαγωγίας.
3) Παρομοίως, η απαίτηση να μην γράφουν οι χρήστες ποτέ τους κωδικούς τους μπορεί να μην είναι ρεαλιστικό και να ωθεί τους χρήστες να επιλέγουν αδύναμα passwords. Μια εναλλακτική λύση είναι να κρατάνε τους κωδικούς τους γραμμένους σε ένα ασφαλές μέρος όπως ένα χρηματοκιβώτιο ή ένα κρυπτογραφημένο κύριο αρχείο. Γράφοντας ένα κωδικό πρόσβαση μπορεί να είναι πρόβλημα εάν οι πιθανοί επιτιθέμενοι έχουν πρόσβαση στο ασφαλές σύστημα. Εάν η απειλή είναι μακρινοί επιτιθέμενοι που δεν έχουν πρόσβαση στο σύστημα τότε αυτό μπορεί να είναι μια πολύ ασφαλής μέθοδος.
4) Ο συνυπολογισμός ειδικών χαρακτήρων μπορεί να είναι ένα πρόβλημα αν κάποιος χρήστης θέλει να συνδεθεί σε ένα υπολογιστή σε μια διαφορετική χώρα. Μερικοί ειδικοί χαρακτήρες μπορεί να είναι δύσκολοι ή αδύνατο να βρεθούν σε πληκτρολόγια σχεδιασμένα για άλλες γλώσσες.
5) Μερικά συστήματα διαχείρισης ταυτότητας (identity management systems) επιτρέπουν το Self Service Password Reset κατά το οποίο ο χρήστης μπορεί να προσπεράσει την ασφάλεια απαντώντας σε μια η περισσότερες ερωτήσεις όπως “Που γεννήθηκες”, “Ποια είναι η αγαπημένη σου ταινία” κτλ. Συχνά οι απαντήσεις σε αυτές τις ερωτήσεις μπορούν να βρεθούν εύκολα από μια απλή έρευνα είτε με phishing.

Παρακάτω αναφέρουμε μερικά παραδείγματα από password policies τα οποία χρησιμοποιούνται σε σελίδες με mail πχ. Yahoo,hotmail κτλ.

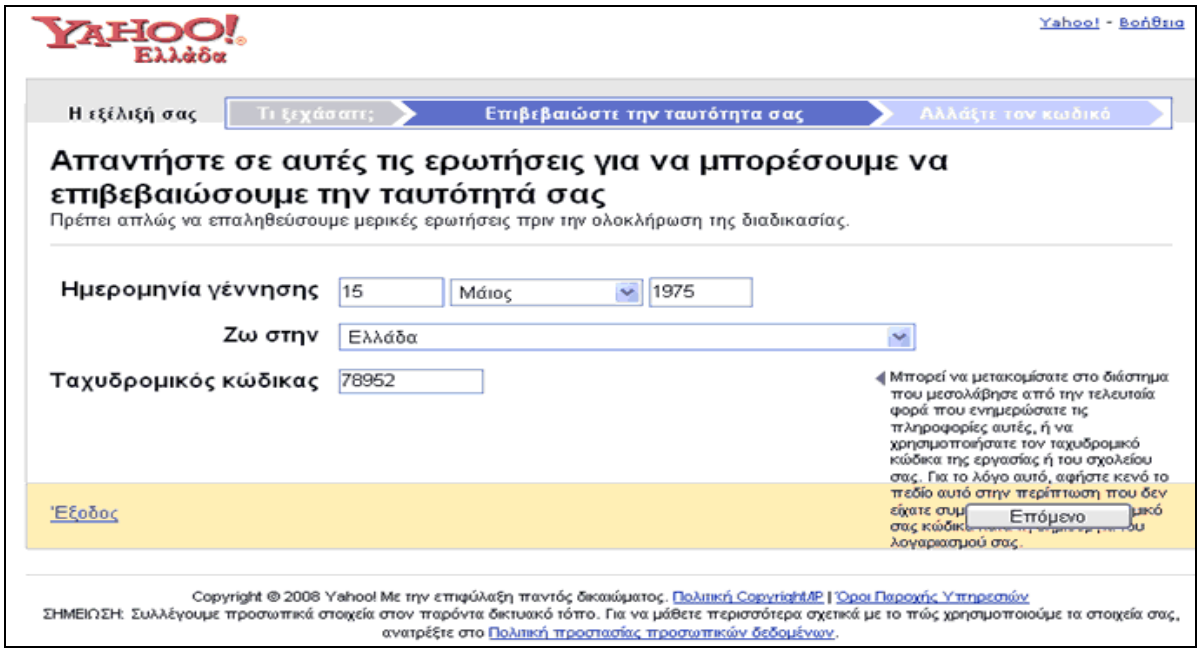
5.5 ΠΑΡΑΔΕΙΓΜΑΤΑ PASSWORD POLICIES

5.5.1 Yahoo mail Policy

Σε αυτή την περίπτωση η δημιουργία ενός yahoo mail μας δίνει την δυνατότητα σε περίπτωση που ξεχάσουμε τον κωδικό να μπορέσουμε να τον ανακτήσουμε. Αυτό επιτυγχάνεται με κάποιες ερωτήσεις που μας υποβάλλονται κατά την δημιουργία του λογαριασμού. (ημερομηνία γέννησης, Τ.Κ κτλ.).



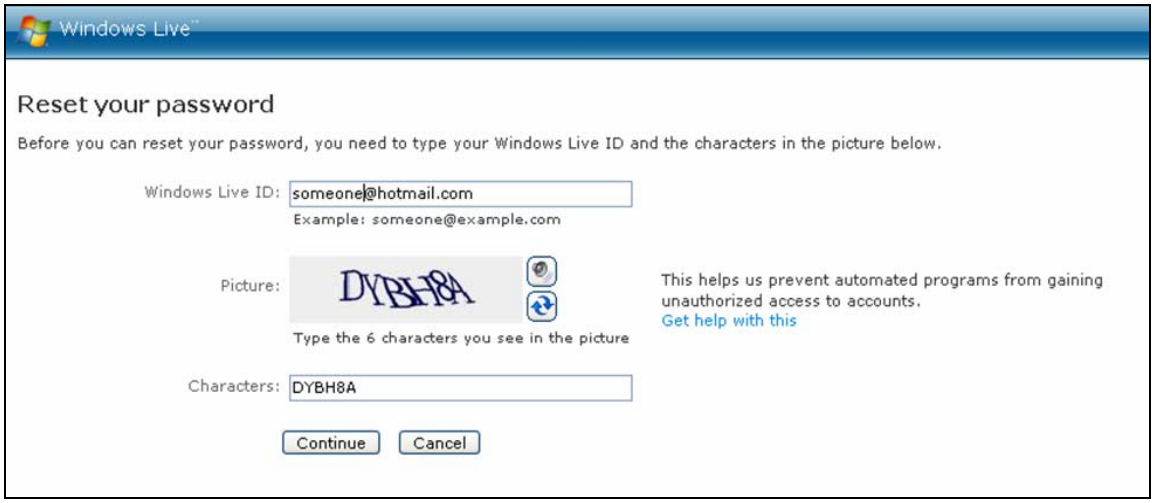
Έτσι σε περίπτωση που κάποιος θέλει να ανακτήσει τον κωδικό του πρέπει πρώτα να απαντήσει στις ερωτήσεις που θα του εμφανιστούν σχετικά με κάποια προσωπικά στοιχεία. Αν είναι κάποιος ο οποίος δεν γνωρίζει τις απαντήσεις τότε δεν μπορεί και να αλλάξει τον κωδικό ή να τον ανακτήσει.



-Σχετικό link: http://gr.yahoo.com/ -

5.5.1 Hotmail Policy

Με τον ίδιο τρόπο όπως το yahoo mail,το hotmail προσφέρει το ίδιο επίπεδο ασφαλείας. Σε περίπτωση απώλειας του κωδικού μπορεί ο χρήστης να τον ανακτήσει απαντώντας σε κάποιες ερωτήσεις ώστε να επιβεβαιωθεί η ταυτότητά του.



Στην συγκεκριμένη περίπτωση ο χρήστης κατά τη δημιουργία του λογαριασμού του έχει θέσει μία ερώτηση και γνωρίζει αυτός μόνο την απάντηση. Αυτή η ερώτηση του υποβάλετε όταν θελήσει να ανακτήσει τον κωδικό του. Ο συγκεκριμένος τρόπος είναι πολύ καλός και αυξάνει την ασφάλεια του λογαριασμού που έχει δημιουργήσει.

-Σχετικό link: http://www.hotmail.com -

Άλλες προσεγγίσεις είναι διαθέσιμες και θεωρούνται ότι είναι πιο ασφαλείς από τους απλούς κωδικούς. Αυτές περιλαμβάνουν την χρήση ενός συμβολικού ή one-time συστήματος κωδικού όπως το S/Key.

5.6 PASSWORD POLICY

5.6.1 Επιβολή μιας πολιτικής (Policy)

Η επιβολή ενός policy που δημιουργήθηκε μπορεί να είναι το πραγματικό ζήτημα σε οποιαδήποτε ρύθμιση δικτύων. Οι διαχειριστές ασφάλειας (security administrators) μπορούν να εξουσιοδοτήσουν ένα σύνολο κανόνων προς τους τελικούς χρήστες.

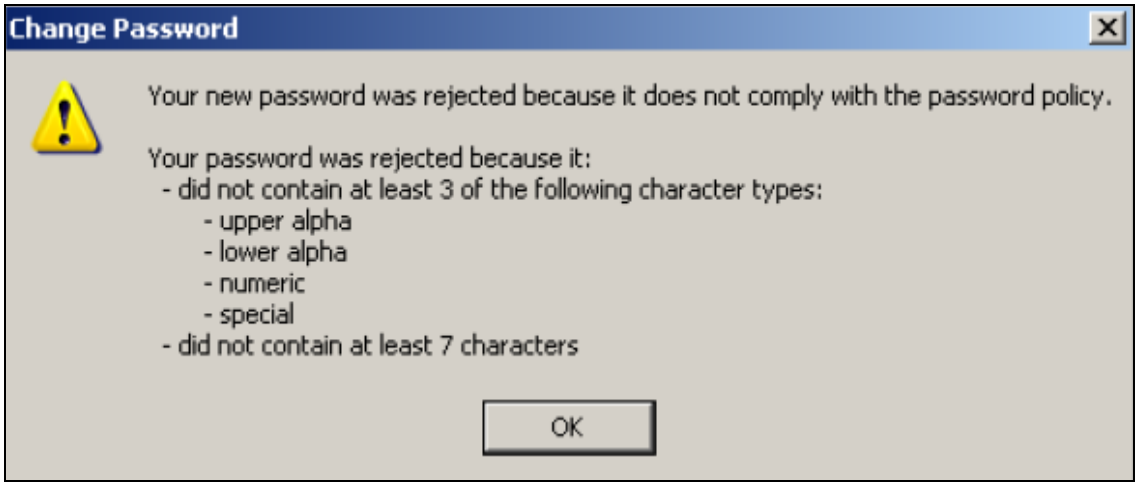
Με την προφορική προσέγγιση- Πολλές εταιρίες απλά επιβάλλουν τις πολιτικές τους προφορικά, με το στόμα. Δηλαδή δηλώνουν ακριβώς την πολιτική που χρησιμοποιούν για τους κωδικούς και αναμένουν τους χρήστες του δικτύου να ακολουθήσουν τους κανόνες

Με την δημιουργία Passfilt- Για πολλούς administrators υπάρχει η επιλογή να δημιουργήσει ο χρήστης τη δική του άδεια εισόδου (Passfilt). Πρέπει να υπάρχει όμως προσοχή γιατί μπορεί να αποδειχτεί περίπλοκο και να προκαλέσει πολλούς πονοκεφάλους.

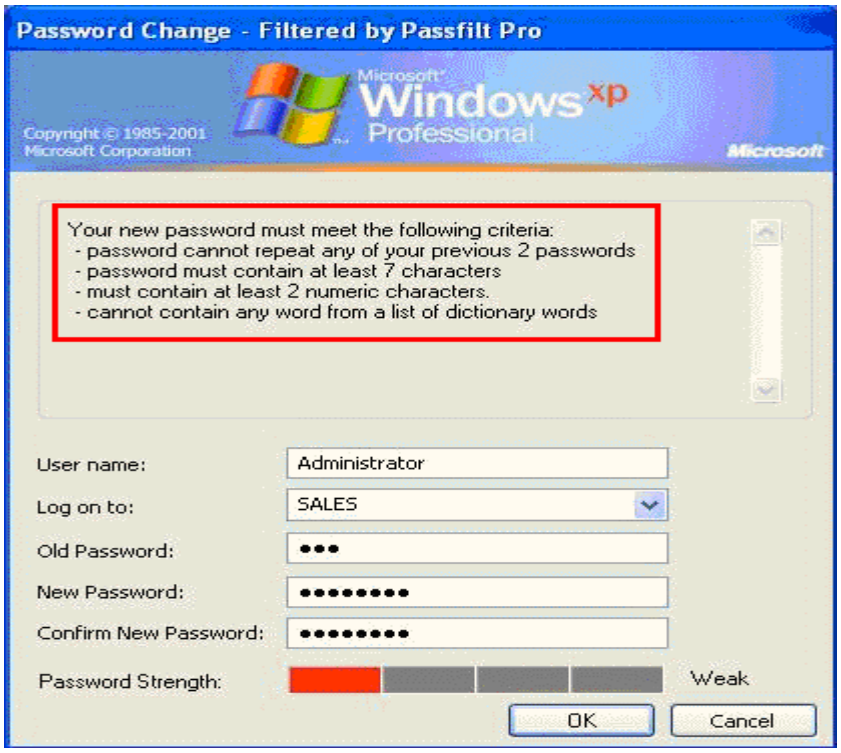
Αν βρεθεί υπάλληλος που έχει παραβιάσει κάποια πολιτική, υπόκειται σε πειθαρχική πράξη μέχρι και σε τερματισμό της σύμβασης εργασίας.

5.6.2 Password Policy Enforcer

Ένα καλό παράδειγμα passfilt είναι το πρόγραμμα Password Policy Enforcer. Το συγκεκριμένο πρόγραμμα βοηθάει σε περίπτωση που στηθεί ένας server, να αποτρέπετε στους χρήστες να χρησιμοποιούν απλούς κωδικούς και τους προτρέπει στην δημιουργία δυνατών κωδικών. Σε περίπτωση που κάποιος προσπαθήσει να χρησιμοποιήσει ένα απλό κωδικό το πρόγραμμα αρνείται να τον δεχτεί και του εμφανίζει το παρακάτω μήνυμα.

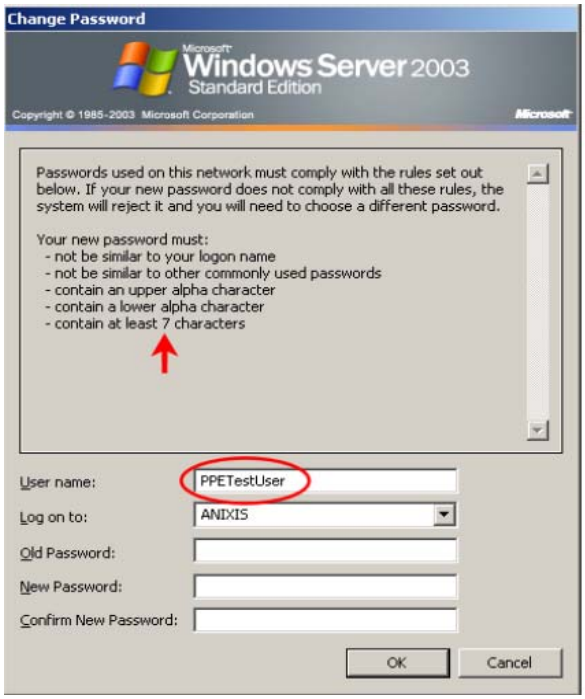


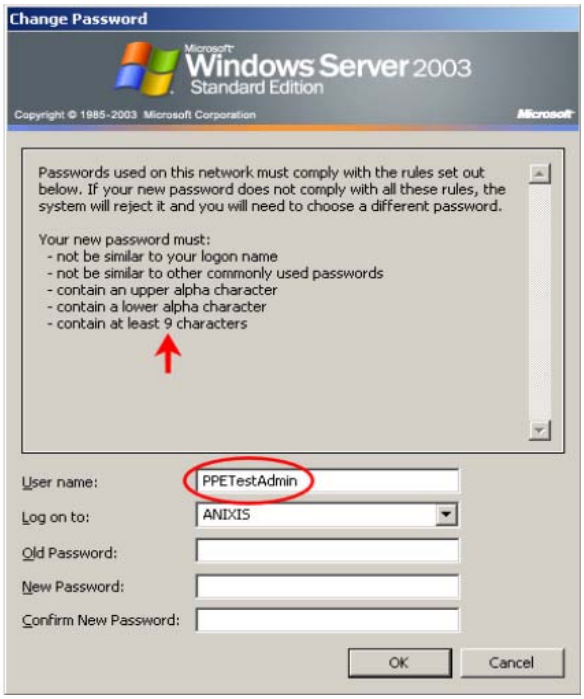
Αφού εγκατασταθεί το πρόγραμμα στον υπολογιστή μπορούμε να δοκιμάσουμε να αλλάξουμε τον κωδικό. Συνήθως για να αλλάξουμε τον κωδικό πατάμε ταυτόχρονα τα κουμπιά CTRL-ALT-DEL και μας εμφανίζεται το Task Manager. Επιλέγουμε να αλλάξουμε τον κωδικό και μας εμφανίζεται το παρακάτω παράθυρο.



Παρατηρούμε ότι το συγκεκριμένο παράθυρο έχει αλλάξει αφού εγκαταστήσουμε το Password Policy Enforcer στον υπολογιστή μας. Πλέον ο χρήστης πρέπει να ακολουθήσει τα παραπάνω κριτήρια για την δημιουργία του κωδικού του. Σε περίπτωση που ο κωδικός δεν πληρεί τα παραπάνω θα το εμφανιστεί το παράθυρο ότι ο κωδικός του απορρίπτεται και ότι πρέπει να εισάγει ένα καινούργιο password

Κάνοντας τις κατάλληλες παραμέτρους στο πρόγραμμα μπορούμε να φτιάξουμε το policy όπως επιθυμούμε. Για παράδειγμα μπορούμε να του δώσουμε την εντολή να δέχεται συγκεκριμένο αριθμό χαρακτήρων ή ο ελάχιστος αριθμός χαρακτήρων του να είναι παραπάνω από π.χ. 7 ή 9.





Το πρόγραμμα όπως και παραπάνω πληροφορίες σχετικά με αυτό μπορούν να βρεθούν στην ιστοσελίδα http://anixis.com/ . Επίσης στο συγκεκριμένο site μπορεί να βρεθεί και το πρόγραμμα Anixis Password Reset το οποίο μπορεί να επαναφέρει ένα χαμένο κωδικό πρόσβασης. Εκεί παρέχονται αρκετές πληροφορίες και για τα δύο προγράμματα σε περίπτωση που ενδιαφέρεται κάποιος για να τα χρησιμοποιήσει.

ΚΕΦΑΛΑΙΟ 6 ΧΡΗΣΗ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΕΡΓΑΛΕΙΩΝ

Παρακάτω θα μελετηθούν κάποια προγράμματα τα οποία χρησιμοποιούνται για το "σπάσιμο" των κωδικών. Υπάρχουν πάρα πολλών ειδών τέτοια προγράμματα και αν κάποιος ψάξει στο διαδίκτυο θα μείνει έκπληκτος από το πόσο ευάλωτος μπορεί να είναι ο υπολογιστής και οι κωδικοί του, μέσα από το σύνολο αυτών των προγραμμάτων.

Παρουσιάζονται στον παρακάτω πίνακα τα κορυφαία 10 προγράμματα για το σπάσιμο των passwords και θα αναλύσουμε τα 3 καλύτερα.

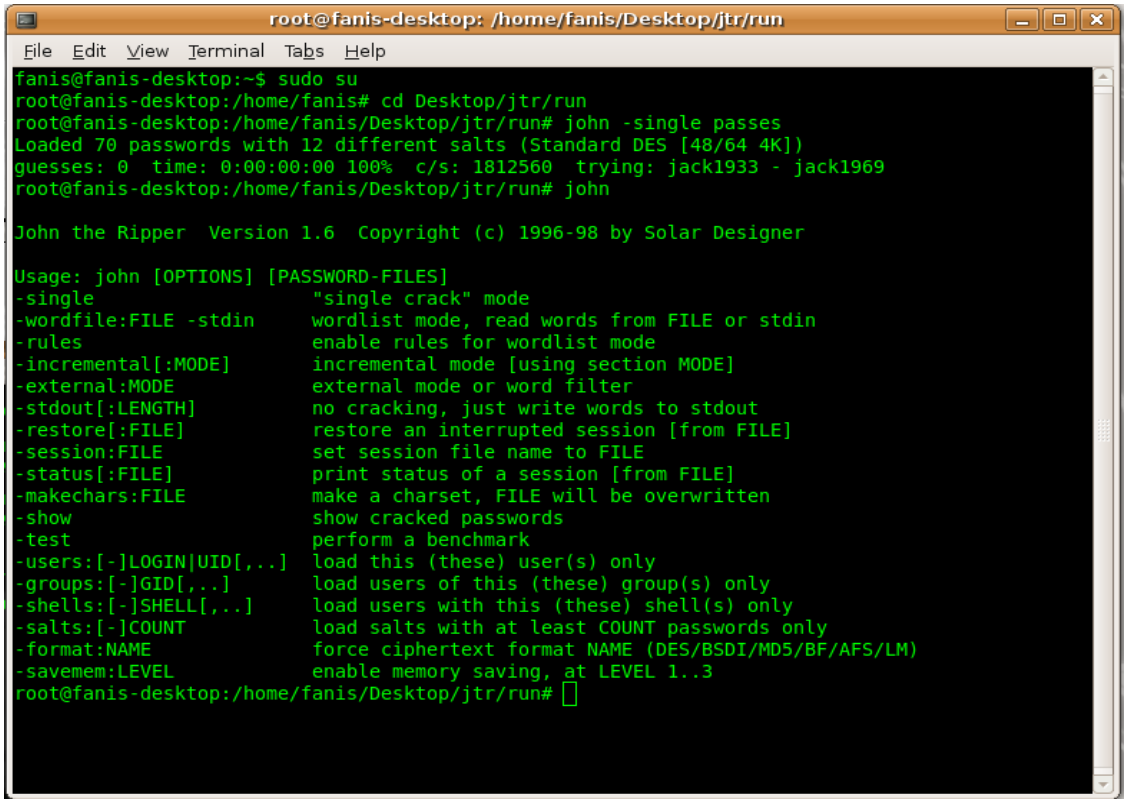
	Logo	free	Linux	Windows	Mac Os X	Command Line Interface	Point & Click Interface	Code for further inspection
Cain & Abel		✓		✓			✓	
John the Ripper		✓	✓	✓	✓	✓		✓
THC Hydra		✓	✓	✓	✓	✓	✓	✓
Aircrack		✓	✓	✓	✓	✓		✓
LOphtcrack				✓			✓	
Airsnort / Aircrack		✓	✓	✓	✓	✓		✓
Solar winds				✓			✓	

Pwdump		✓		✓		✓		✓
Rainbowcrack		✓	✓	✓	✓	✓		✓
Brutus				✓			✓	

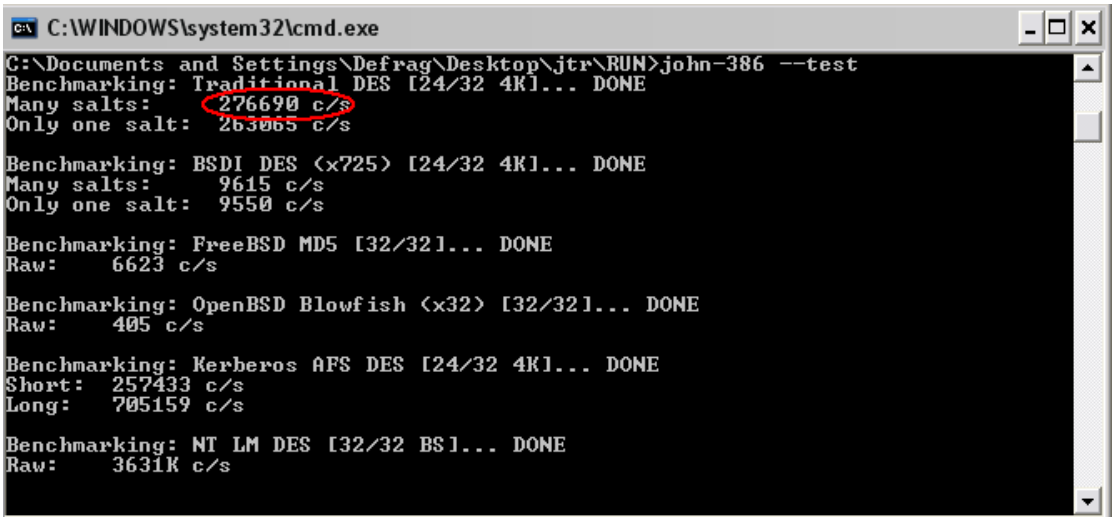
6.1 JOHN THE RIPPER

Το πρόγραμμα John the Ripper είναι ένα δωρεάν εργαλείο cracking ανοιχτού κώδικα. Αρχικά δημιουργήθηκε για το λειτουργικό σύστημα Unix αλλά με τον καιρό αναπτύχτηκε και πλέον τρέχει σε 15 διαφορετικές πλατφόρμες (11 οι οποίες είναι βασισμένες στην αρχιτεκτονική του UNIX, DOS, Win32, Beos και OpenVMS). Είναι ένα από τα δημοφιλέστερα προγράμματα «σπασίματος» κωδικών και συνδυάζει ένα αριθμό από password crackers σε ένα πακέτο, εντοπίζει αυτόματα τύπους hash κωδικών και περιλαμβάνει ένα ειδικό cracker. Μπορεί να λειτουργήσει ενάντια σε διαφόρων ειδών κρυπτογραφημένους κωδικούς και επιπλέον με κάποια πρόσθετα χαρακτηριστικά έχει τη δυνατότητα να συμπεριλαμβάνει password hashes βασισμένα σε MD4 και κωδικούς αποθηκεμένους σε LDAP, MySQL και άλλα. Χρησιμοποιούμε την πλατφόρμα Ubuntu (Linux) για να τρέξουμε το John the Ripper. Αρχικά για να μπορέσουμε να τρέξουμε το πρόγραμμα συνδεόμαστε σαν root έτσι ώστε να έχουμε δικαιώματα. Αυτό το επιτυγχάνουμε πληκτρολογώντας sudo su. Έπειτα πατώντας john βλέπουμε όλες τις πιθανές ενέργειες που μπορούμε να κάνουμε στο πρόγραμμα

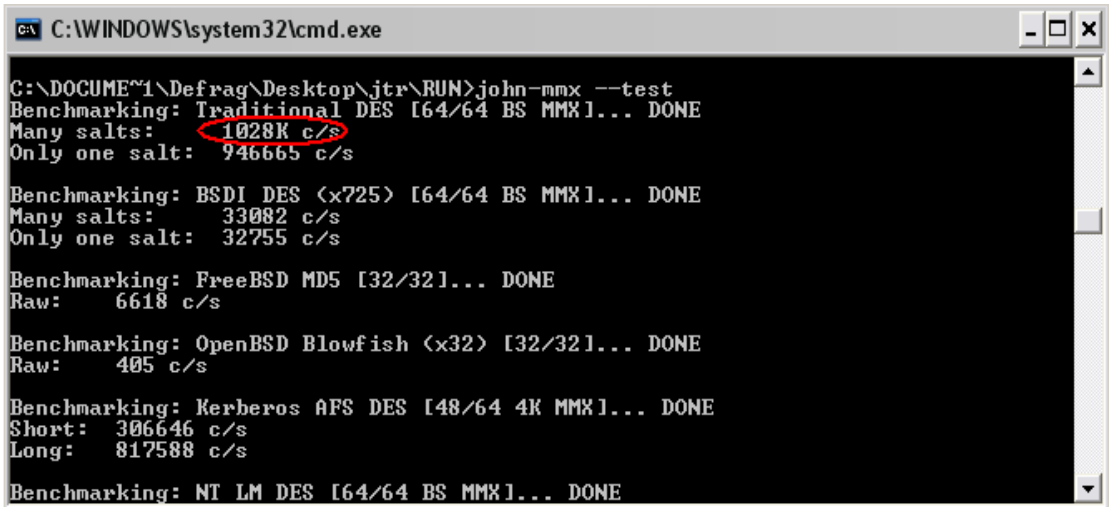
.



Στο λειτουργικό σύστημα windows δοκιμάσαμε το John με την εντολή *john-386 –test*. Στο σύστημά μας, το Traditional DES[24/32 4k] μας ενημέρωσε ότι μπορεί να κρυπτογραφεί 276690 χαρακτήρες το δευτερόλεπτο.



Επανέλαβα τη διαδικασία για την έκδοση MMX του προγράμματος, η οποία συμπεριλαμβάνετε μέσα στο John 1.7. Πατώντας *john-mmx --test* εμφανίστηκαν τα παρακάτω αποτελέσματα:



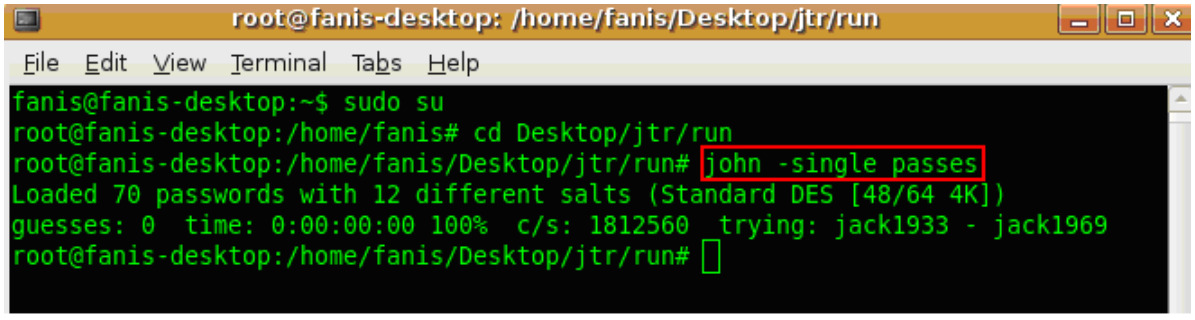
Όπως βλέπουμε, με το john-mmx το Traditional Des[64/64 BS MMX] μας ενημέρωσε ότι το σύστημα μπορεί να κρυπτογραφεί με 1028 εκατομμύρια χαρακτήρες ανά δευτερόλεπτο ανά πυρήνα.
Σαφώς η έκδοση MMX του John αποδεικνύεται πολύ ταχύτερη από την απλή στην συγκεκριμένη περίπτωση.

Παρακάτω θα αναλυθούν οι μέθοδοι που χρησιμοποιεί το John the Ripper και έπειτα θα δοκιμαστούν αναλυτικά μία-μία στο λειτουργικό σύστημα των Unix.

6.1.1 Single mode

Η μέθοδος αυτή δοκιμάζει ως πιθανά passwords τα userIDs των χρηστών, τα ονόματα τους καθώς και τα ονόματα των "home directory" των χρηστών. Αν βρει κάποιο password το δοκιμάζει για όλους τους users του αρχείου passwd για την περίπτωση που έχει χρησιμοποιηθεί και από άλλον χρήστη.

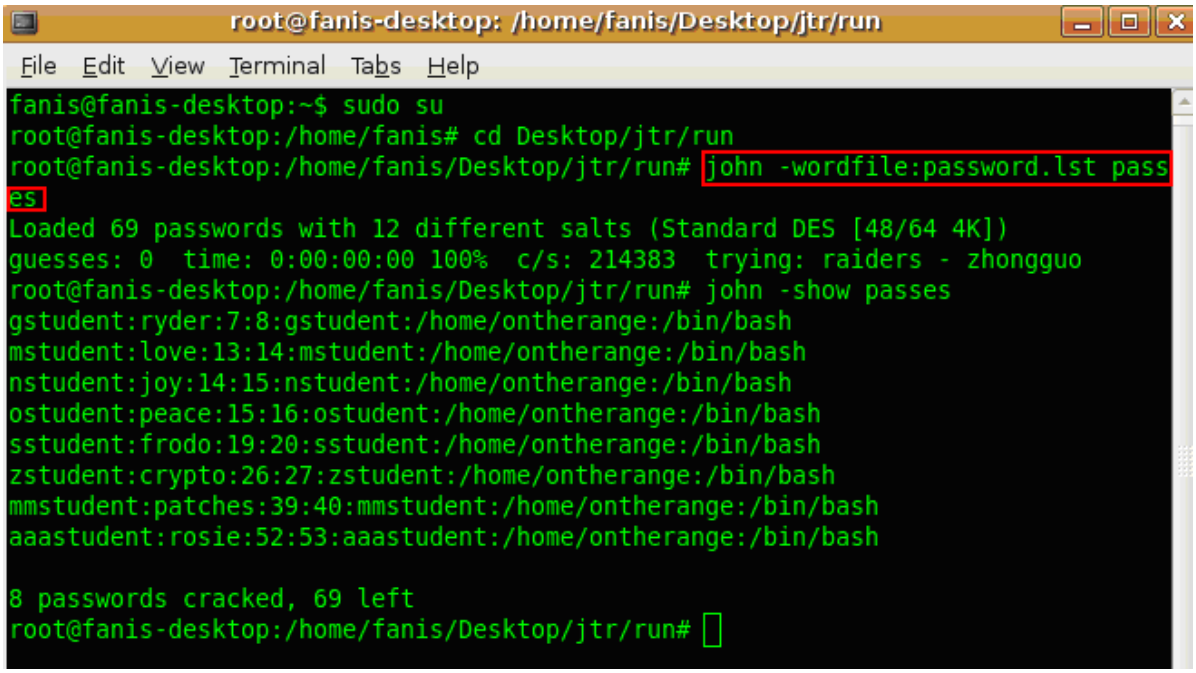
-Παράδειγμα single mode-



6.1.2 Wordlist mode

Η μέθοδος αυτή χρησιμοποιεί ένα text αρχείο το οποίο περιέχει λέξεις που θα μπορούσαν να αποτελούν password. Κάθε λέξη από αυτό το αρχείο δοκιμάζεται με τα κωδικοποιημένα passwords που αναζητούμε. Το πρόγραμμα μάλιστα έχει τη δυνατότητα να παράγει λέξεις που δεν υπάρχουν στο αρχείο-λεξικό αλλά προέρχονται από αυτό χρησιμοποιώντας κάποιους κανόνες (mangling rules). Το αρχείο με το λεξικό θα πρέπει να περιέχει κάθε λέξη μια φορά ώστε να αποφευχθεί η σπατάλη υπολογιστικού χρόνου. Επίσης έχει διαπιστωθεί ότι το πρόγραμμα θα δώσει γρηγορότερα κάποιο αποτέλεσμα (αν αυτό είναι δυνατό) αν η λίστα με τα υποψήφια password είναι ταξινομημένη με σειρά από το πιο πιθανό προς το πιο απίθανο password. Αν η ταξινόμηση αυτή δεν είναι δυνατή, είναι προτιμότερο να ταξινομηθεί αλφαβητικά γιατί η εφαρμογή λειτουργεί γρηγορότερα αν κάθε λέξη διαφέρει από την προηγούμενη σε λίγους χαρακτήρες.

-Παράδειγμα wordlist mode-



Μερικά χρήσιμα URLs στα οποία μπορεί κανείς να βρει λεξικά με πιθανούς κωδικούς είναι:

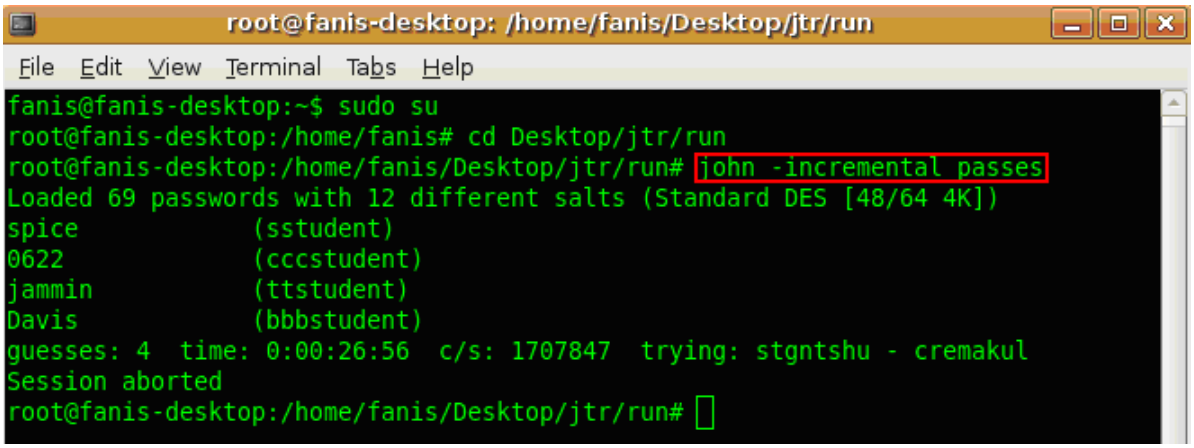
- ftp://ftp.openwall.com/pub/wordlists
- http://ftp.cerials.purdue.edu/pub/dict/dictionaries
- http://ftp.cerials.purdue.edu/pub/dict/wordlists

6.1.3 Incremental mode

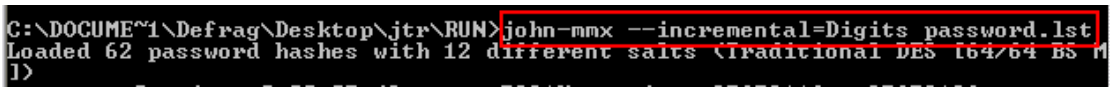
Η μέθοδος αυτή είναι και η πιο αποτελεσματική γιατί δημιουργεί και δοκιμάζει λέξεις συνδυάζοντας όλους τους πιθανούς χαρακτήρες που θα μπορούσε να έχει κάποιο password. Η μέθοδος αυτή θα μπορούσε θεωρητικά να σπάσει όλα τα password. Για να το κάνει όμως αυτό θα χρειαστεί τεράστιος υπολογιστικός χρόνος. Αυτό είναι εύκολο να διαπιστωθεί αν υπολογίσουμε τον αριθμό των λέξεων που μπορούν να προκύψουν αν συνδυάσουμε 5 μόνο χαρακτήρες από μικρά και κεφαλαία γράμματα, αριθμούς και σημεία στίξης. Η πολυπλοκότητα και αντίστοιχα ο υπολογιστικός χρόνος αυξάνονται εκθετικά αν θελήσουμε να δοκιμάσουμε λέξεις έξι ή περισσότερων χαρακτήρων. Ειδικότερα σε περιπτώσεις που έχουμε παραπάνω από 14 χαρακτήρες το John the Ripper και γενικά όλα τα cracking tools είναι υπερβολικά δύσκολο να βρουν τους κωδικούς.

Το πρόγραμμα μας παρέχει τη δυνατότητα να περιορίσουμε τους χαρακτήρες που θα χρησιμοποιηθούν (π.χ. μόνο στους αριθμούς (--Incremental:Digits), ή μόνο στα γράμματα (--Incremental:alpha)). Έχουμε επίσης τη δυνατότητα να ορίσουμε το ελάχιστο και το μέγιστο μήκος των λέξεων που θα ελεγχθούν καθώς και το μέγιστο αριθμό διαφορετικών χαρακτήρων που μπορούν να χρησιμοποιηθούν ώστε να προκύψει το υποψήφιο password.

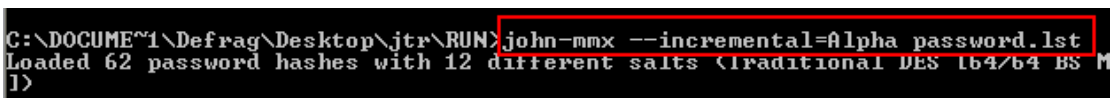
Το πρόγραμμα διακόπτεται (με ctrl-C) όταν θέλουμε να σταματήσει την περαιτέρω αναζήτηση passwords.



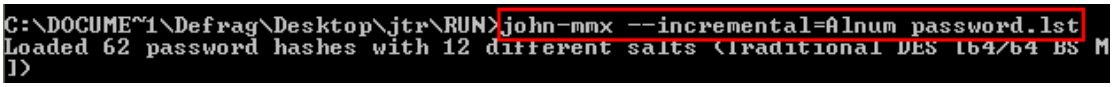
Μπορούμε επίσης να περιορίσουμε την αναζήτησή μας μόνο σε νούμερα πληκτρολογώντας:



είτε μόνο γράμματα:



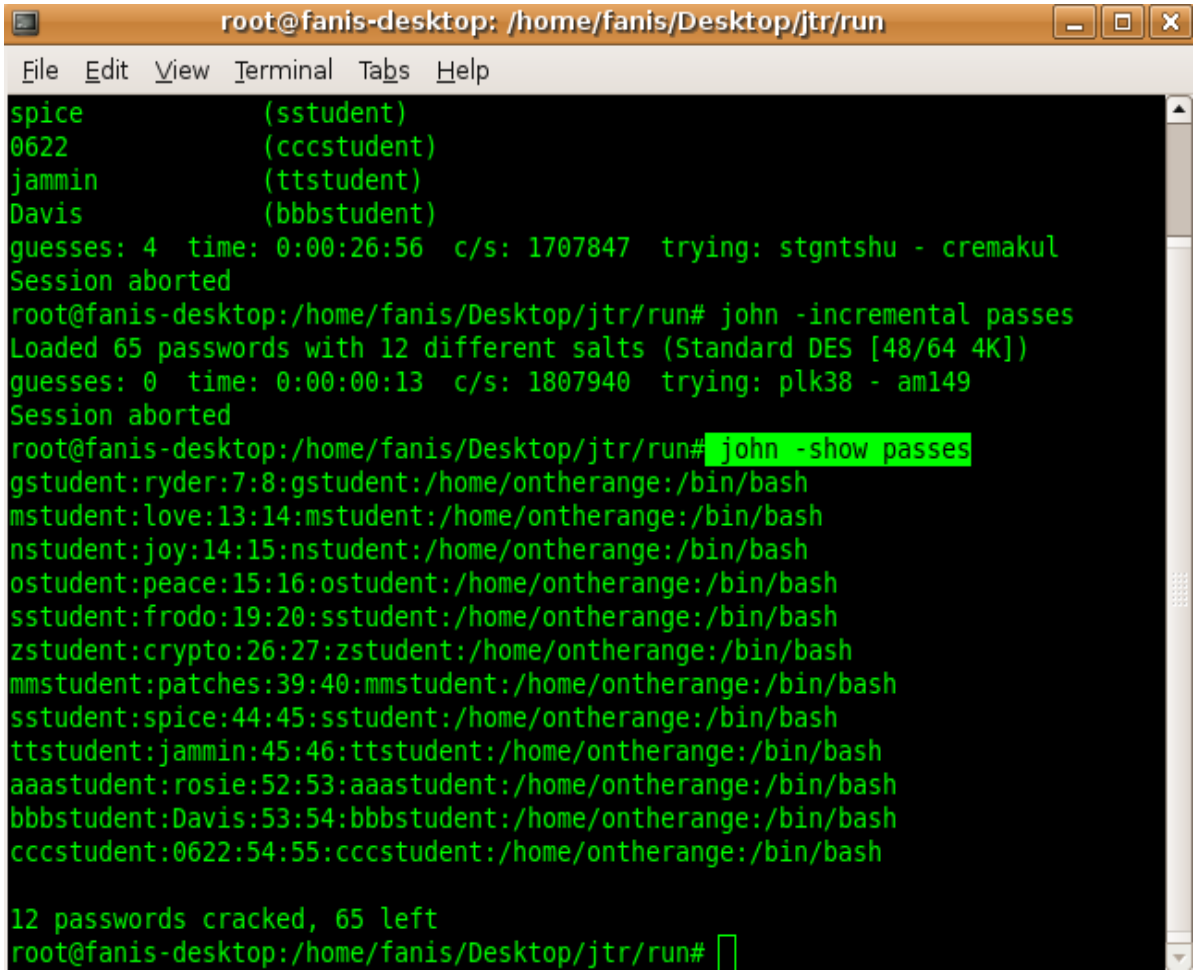
είτε κάποιο συνδυασμό τους:



http://www.openwall.com/john/

Όταν σταματήσει το πρόγραμμα, δίνεται η δυνατότητα να εμφανιστούν όλοι οι κωδικοί τους οποίους μπόρεσε να σπάσει το john χρησιμοποιώντας τις διάφορες μεθόδους του. Αυτό επιτυγχάνεται πληκτρολογώντας john –show passes. Παρακάτω δίνεται το παράδειγμα στο οποίο βλέπουμε ότι το john μπόρεσε να σπάσει 12 κωδικούς (τους οποίους και μας τους δείχνει ποιοι είναι και από ποιον χρήστη) και έμειναν άλλοι 65.

-Παράδειγμα incremental mode-



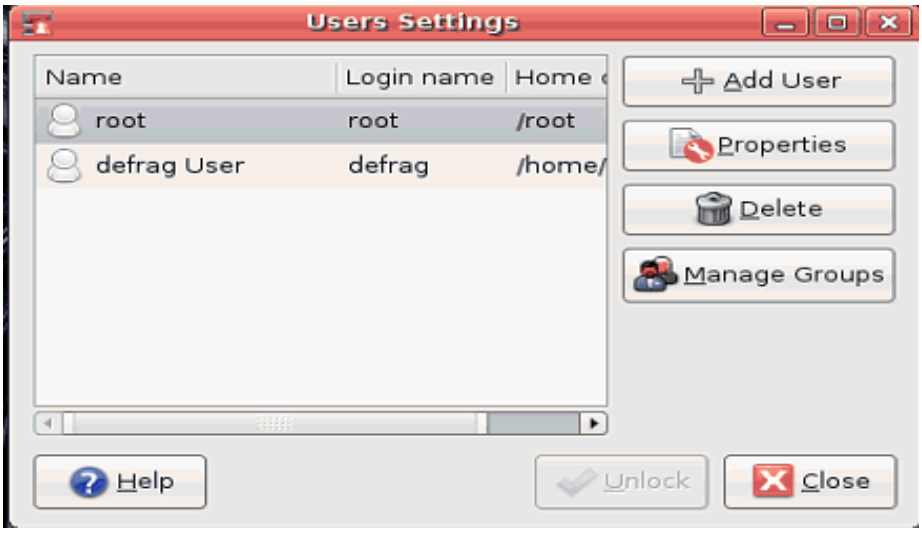
6.2 LOGIN ACCOUNTS ΣΤΑ UBUNTU: ΑΝΑΚΤΗΣΗ USERNAMES ΚΑΙ ΚΩΔΙΚΩΝ

Για να δούμε το John the ripper αναλυτικότερα φτιάξαμε μερικά accounts στο λειτουργικό σύστημα των Linux κα δοκιμάσαμε να τα σπάσουμε. Για την δημιουργία τους μπορούμε να πατήσουμε στο command line το εξής σαν παράδειγμα:

Useradd user1

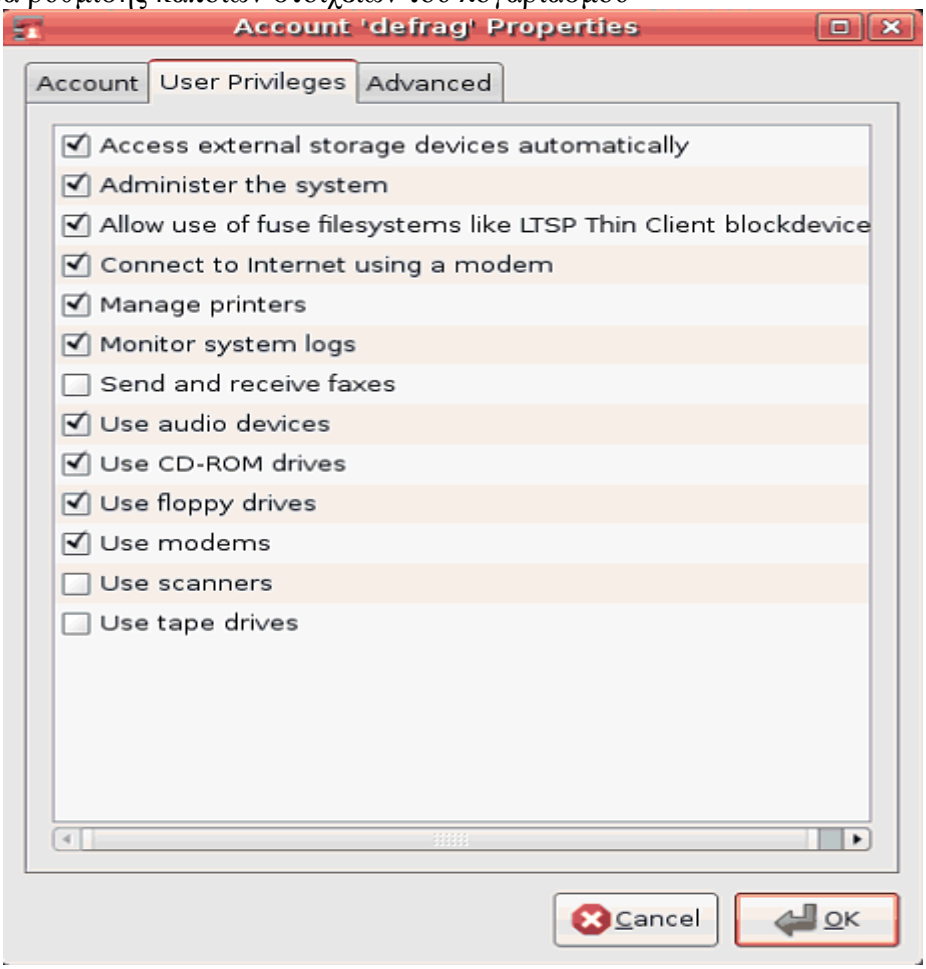
Passwd 12345 ή αλλιώς:

Απο την επιφάνεια εργασίας επιλέγουμε System-Administration και έπειτα “Users and Groups”.



Μας εμφανίζεται το παρακάτω παράθυρο στο οποίο πρέπει να έχουμε Administration privileges για να προσθέσουμε ένα user. Πατώντας Unclock και πληκτρολογώντας τον κωδικό, συνδεόμαστε πλέον σαν root και έχουμε τα administration privileges.

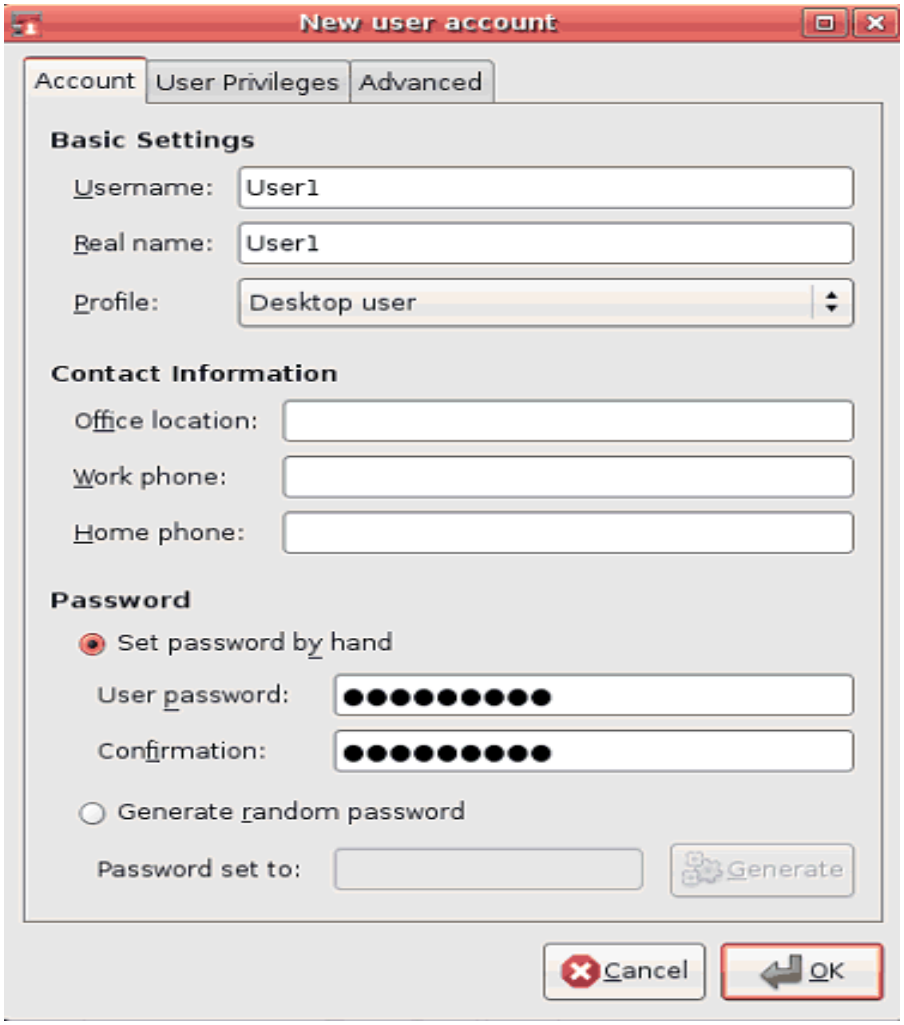
Πατώντας την επιλογή Add User μας εμφανίζεται ένα παράθυρο σχετικά με τις πληροφορίες του νέου account που θέλουμε να δημιουργήσουμε. Επίσης δίνεται η δυνατότητα ρύθμισης κάποιων στοιχείων του λογαριασμού

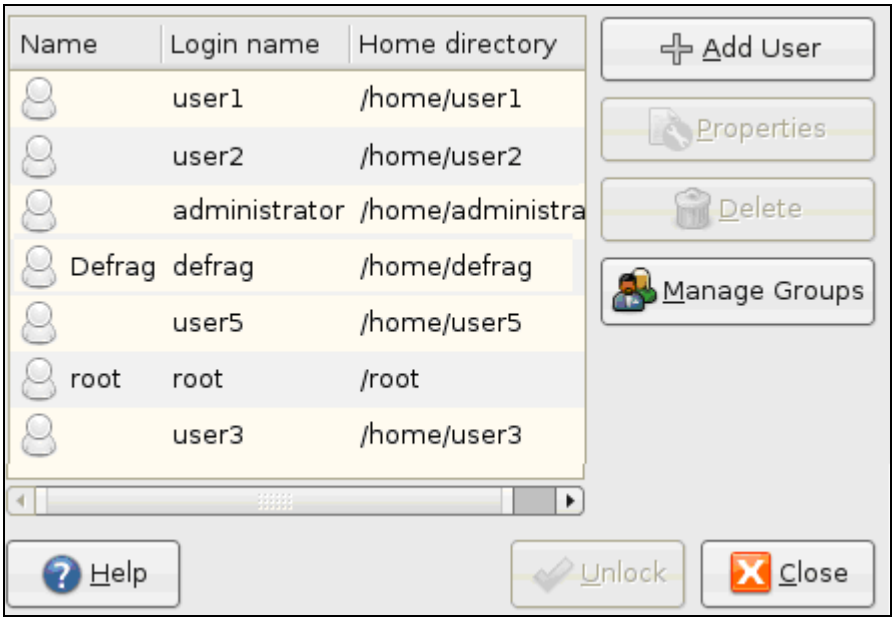


Δημιουργήσαμε τους εξής users με τους αντίστοιχους κωδικούς:

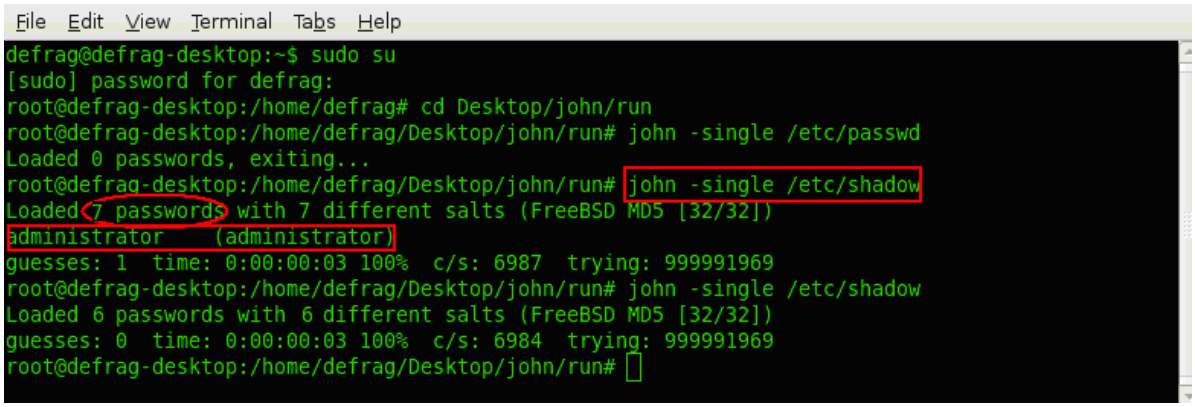
root	@dmin|str@t0R
defrag	8TryToCr@ckTh|s
user1	123456
user2	abcdef
user3	123abc
user5	123456789
administrator	administrator

και αλλάξαμε τον κωδικό του defrag(τον λογαριασμό που χρησιμοποιούμε) σε 8TryToCr@ckTh|s. Όπως και του root σε @dmin|str@t0R.



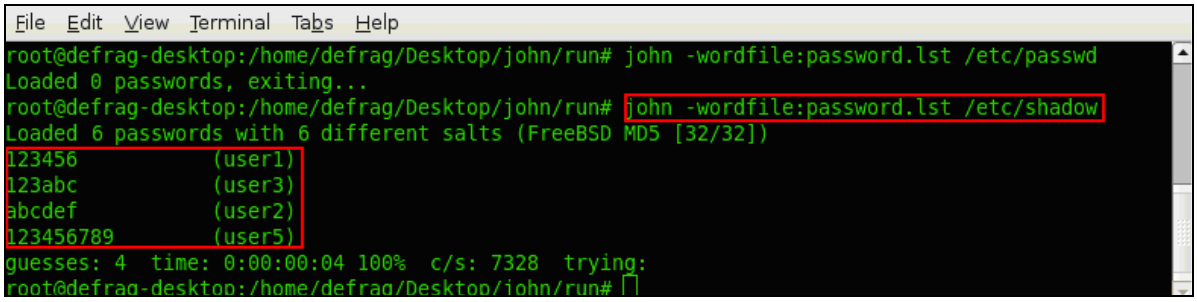


Προσπαθήσαμε να σπάσουμε αυτά τα login passwords χρησιμοποιώντας το John the ripper με την απλή μέθοδο (single method)Q



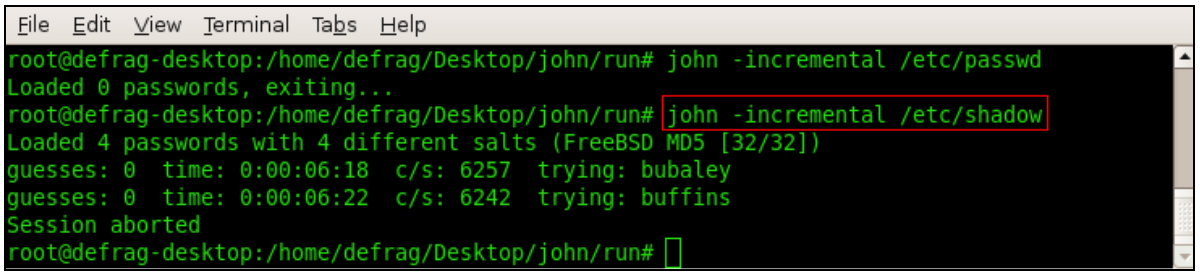
Το πρόγραμμα μας ενημερώνει ότι βρήκε 7 accounts με τους κωδικούς τους και χρησιμοποιώντας την εντολή john –single /etc/shadow κατάφερε να σπάσει ένα από αυτούς, τον λογαριασμό του administrator οπου είχε και το αντίστοιχο password. Στους άλλους 6 λογαριασμούς δεν κατάφερε να βρει τους κωδικούς με αυτή την μέθοδο.

Έπειτα προχωρήσαμε σε περαιτέρω αναζήτηση για το σπάσιμο των άλλων κωδικών χρησιμοποιώντας την μέθοδο wordfile. Το John έχει από μόνο του ένα .txt file οπου περιέχει αρκετά default passwords. Εμείς αυτό που καναμε ήταν απλά να ενισχύσουμε αυτή την λίστα προσθέτωντας ακόμα περισσότερα default passwords τα οποία βρήκαμε στο internet και συγκεκριμένα στις διευθύνσεις http://www.maxalbums.com/password_list.php και http://isc.sans.org/presentations/ircbot_pwlist.txt .

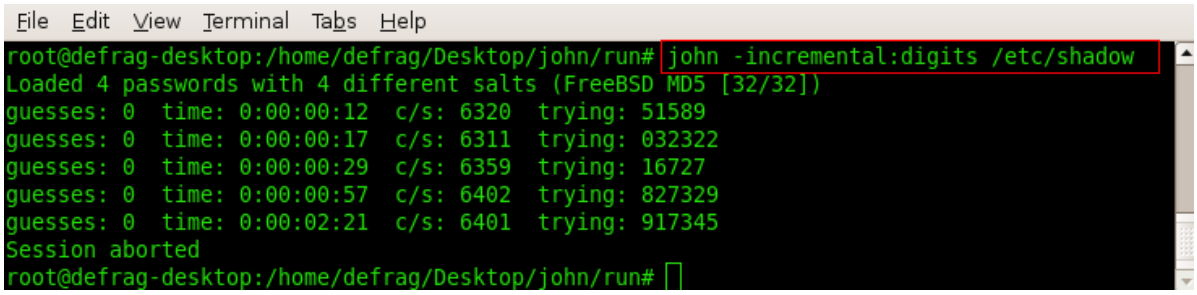


Με αυτή τη μέθοδο το John κατάφερε να σπάσει άλλους 4 κωδικούς, τους user1, user2, user3 και user5 αντίστοιχα.

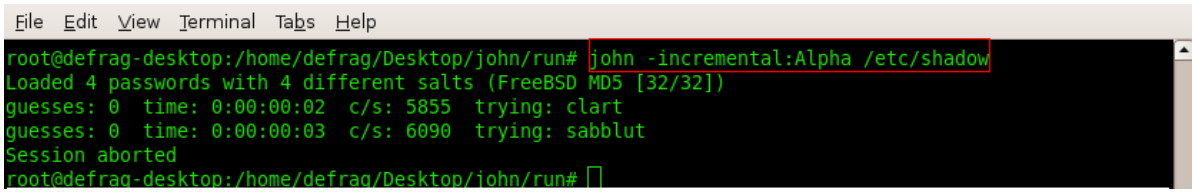
Πλέον, έχοντας σπάσει 5 κωδικούς από τους 7 με τις 2 παραπάνω μεθόδους, single method και wordfile method, μένει να χρησιμοποιήσουμε ακόμα την incremental method η οποία θεωρείται και η πιο ισχυρή.



Περιορίσαμε την αναζήτηση ώστε το John να ψάχνει μόνο συνδιασμούς αριθμών γράφοντας john –incremental:digits /etc/shadow



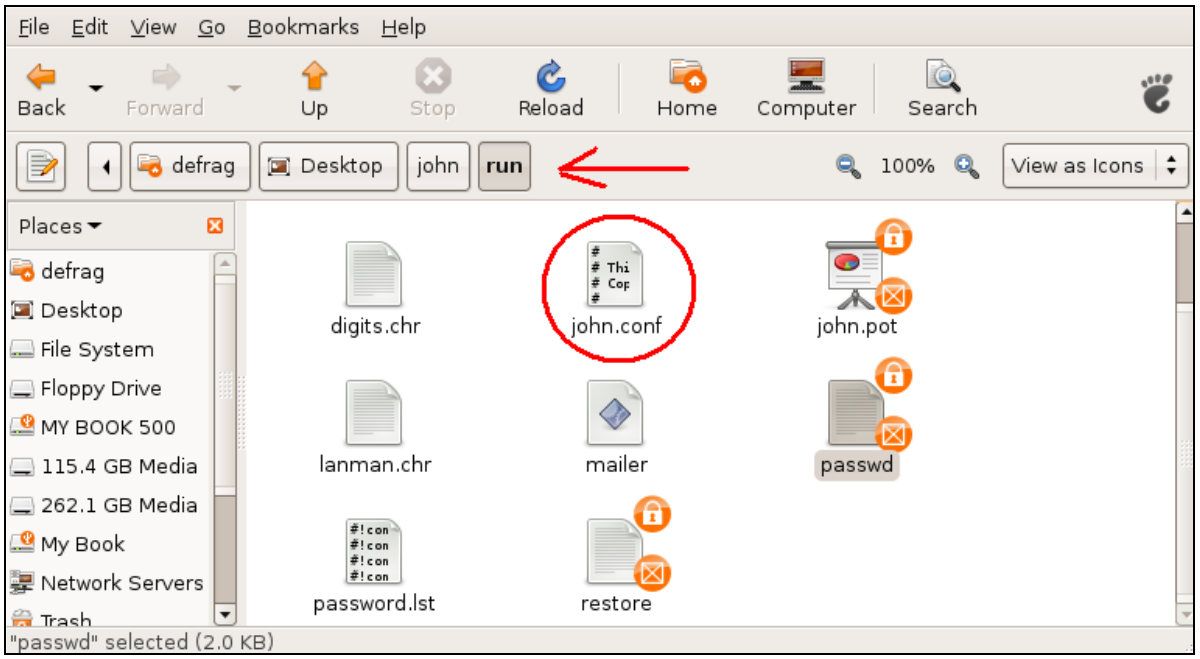
και έπειτα μόνο γράμματα:

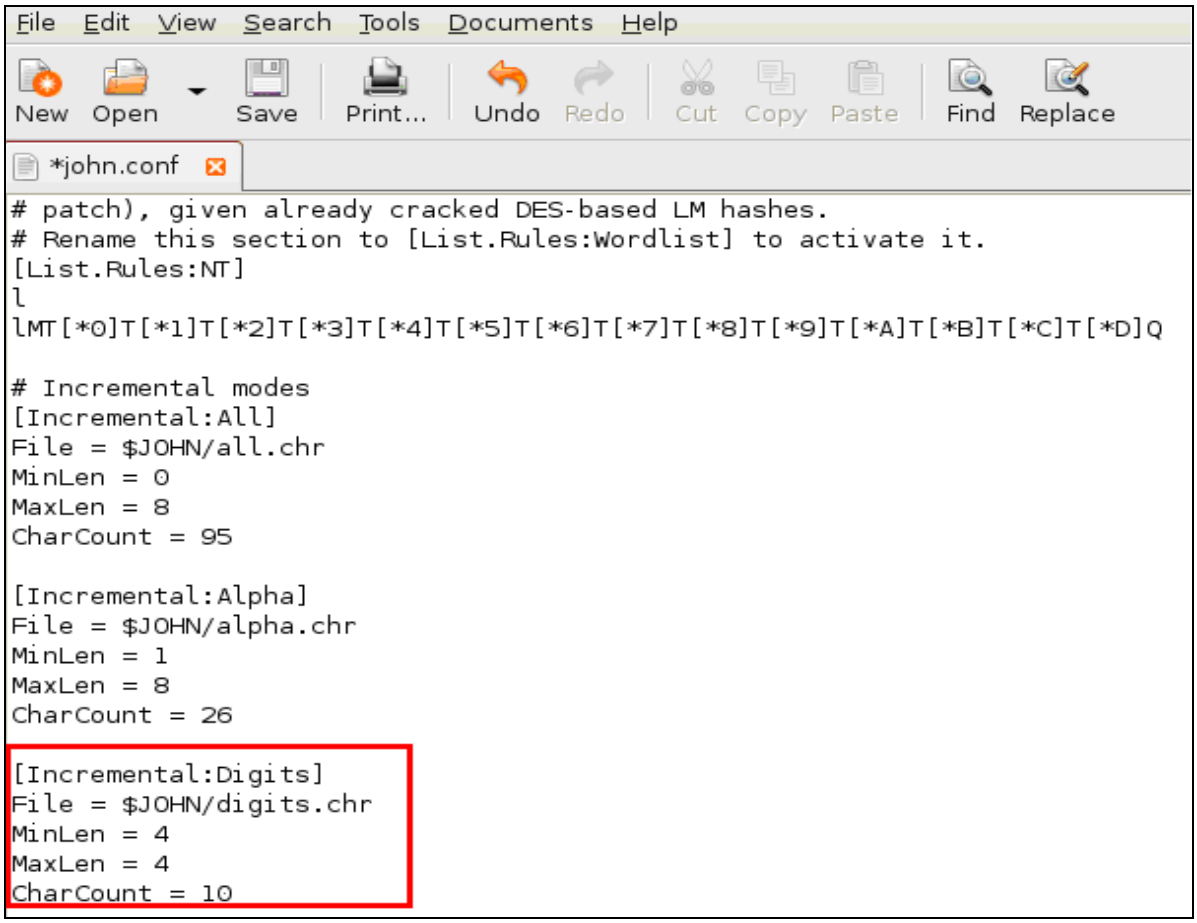


ή και συνδυασμούς γραμμάττων με αριθμούς με την εντολή john –incremental:alnum /etc/shadow χωρίς κάποιο αποτέλεσμα.

Γενικότερα η μέθοδος incremental θεωρείται και η πιο ισχυρή αλλά μπορεί να πάρει υπερβολικά αρκετό χρόνο.

Αλλάξαμε κάποιες παραμέτρους στο αρχείο john.conf το οποίο βρίσκεται στο φάκελο /john/run,σχετικά με το incremental mode και το κάναμε να ψάχνει για 4 χαρακτήρες. Εκεί ορίσαμε το MinLenEN και το MaxLen της παραμέτρου Incremental:Digits ίσο με 4.





Οποιαδήποτε αλλαγή στις παραπάνω παραμέτρους μπορούσε να γίνει αποδεκτή από το John και να περιορίσει/διευκολύνει την αναζήτησή μας.

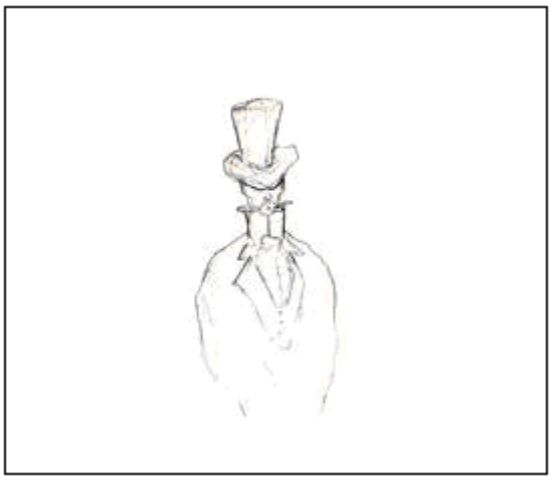
Το αποτέλεσμα παρέμεινε ίδιο λόγω του ότι οι υπόλοιποι κωδικοί που έμειναν ήταν αρκετά ισχυροί και δεν μπορούσαν να σπάσουν. Λογικά αν αφήναμε το John the Ripper με την μέθοδο incremental θα κατάφερνε να σπάσει τους κωδικούς αλλά αυτή η ενέργεια μπορεί και να έπαιρνε μήνες ακόμα και χρόνια.

Με την εντολή john –show /etc/shadow μπορέσαμε να δούμε τους κωδικούς που κατάφερε να σπάσει το JohnQ

```
root@defrag-desktop:/home/defrag/Desktop/john/run# john -show /etc/shadow
user1:123456:14364:0:99999:7:::
user2:abcdef:14364:0:99999:7:::
user3:123abc:14364:0:99999:7:::
user5:123456789:14364:0:99999:7:::
administrator:administrator:14364:0:99999:7:::

5 passwords cracked, 2 left
root@defrag-desktop:/home/defrag/Desktop/john/run#
```

Η αναζήτηση διακόπηκε με Ctrl-C και καταφέραμε να σπάσουμε 5 από τα 7 Login Accounts τα οποία δημιουργήσαμε.Όπως ήταν αναμενόμενο το John κατάφερε να σπάσει 5 από τους 7 κωδικούς σε μικρό χρονικό διάστημα. Αφήσαμε το John για κάποιες μέρες μήπως μπορέσει και ανακτήσει τους άλλους 2 κωδικούς, χωρίς όμως αποτέλεσμα, μιας και οι κωδικοί ήταν αρκετά δυνατοί.

Το John the Ripper δίκαια θεωρείται ένα από τα καλύτερα cracking tools όπως είδαμε. Κατάφερε μέσα σε λίγο χρονικό διάστημα να σπάσει αρκετούς κωδικούς και σίγουρα με την πιο ισχυρή του μέθοδο (incremental method) αν το αφήσουμε θα καταφέρει να σπάσει τους περισσότερους κωδικούς που υπάρχουν σε ένα υπολογιστικό σύστημα. Παρόλο που η συγκεκριμένη μέθοδος είναι αρκετά χρονοβόρα και σε συνδιασμό με τις άλλες μεθόδους του John καταφέρνει να κάνει το πρόγραμμα από τα καλύτερα στο είδος του.

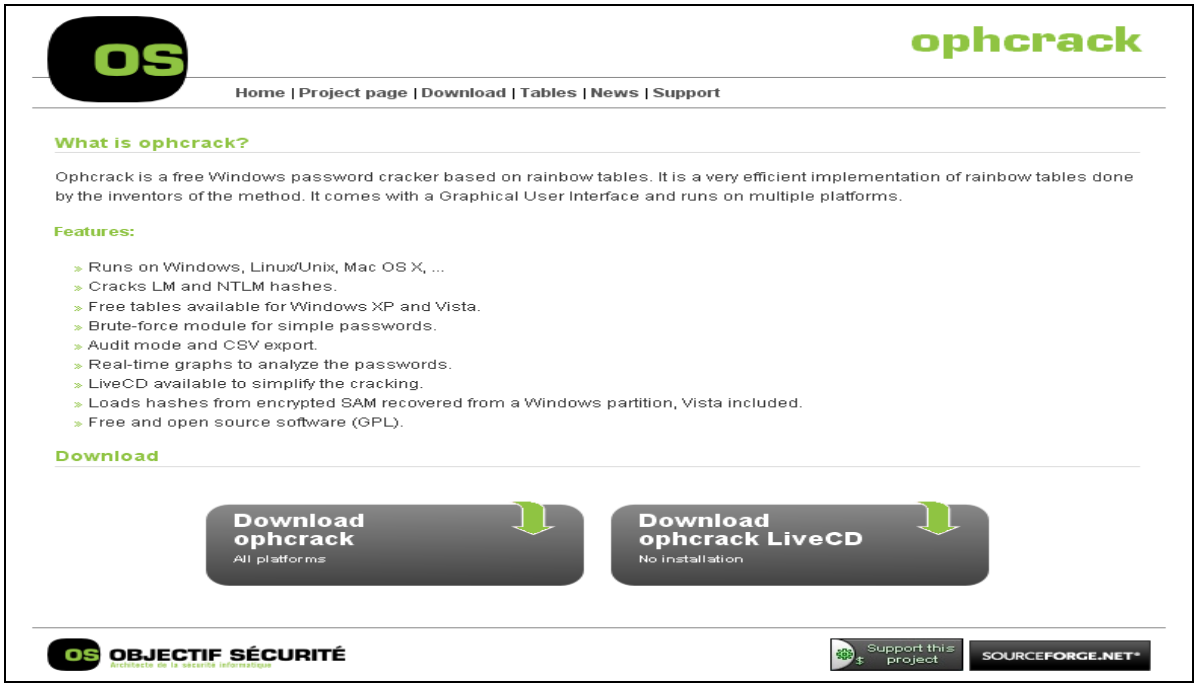


6.3 OPHCRACK

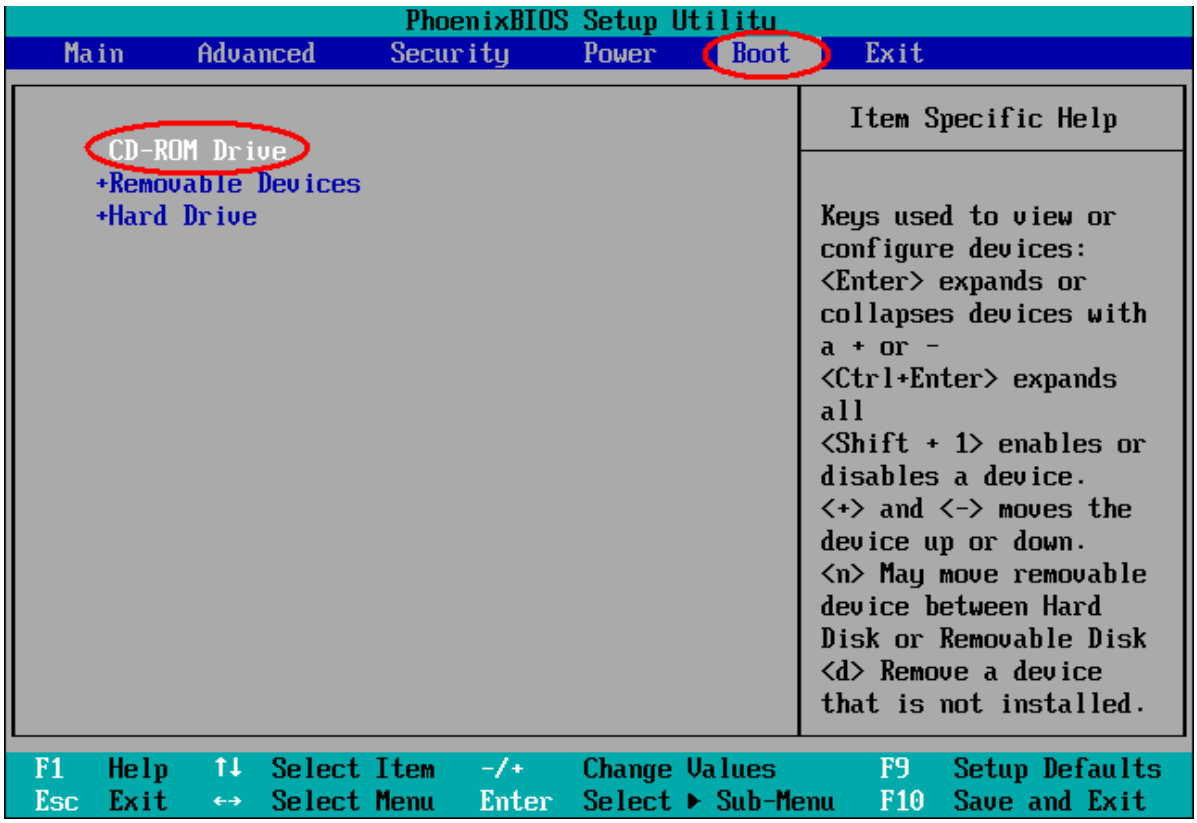
Το Ophcrack είναι ένα πρόγραμμα open source το οποίο έχει την δυνατότητα να βρίσκει τους κωδικούς σε ένα σύστημα χρησιμοποιώντας LM Hashes μέσα από rainbow tables. Έχει Graphical User Interface και τρέχει σε Windows,Linux και MAC OS. Το πρόγραμμα μπορεί να εξάγει τα hashes ενός υπολογιστή και πιο συγκεκριμένα τα αρχεία sam στα οποία περιέχονται οι κωδικοί του συστήματος. Μπορεί να σπάσει 99.9% κωδικούς οι οποίοι αποτελούνται από γράμματα και αριθμούς και έχουν μήκος μέχρι 14 χαρακτήρες, μέσα σε λίγα λεπτά.

Τα Rainbow Tables για τα LM Hashes κωδικών οι οποίοι αποτελούνται από γράμματα και νούμερα δίνονται δωρεάν από τους δημιουργούς του Ophcrack. Παρακάτω θα χρησιμοποιήσουμε το Ophcrack Live CD ώστε να καταφέρουμε να σπάσουμε τους κωδικούς του συστήματος.
Το LM hash (LAN Manager) είναι ένα από τα format των Microsoft Lan Manager και των Windows το οποίο χρησιμοποιείτε για να αποθηκεύουν οι χρήστες κωδικούς μικρότερους από 15 χαρακτήρες. Το συγκεκριμένο format είναι το μοναδικό το οποίο χρησιμοποιείτε στον Windows Lan Manager. Μπορεί να ¨σπάσει¨ εύκολα εξαιτίας 2 λόγων. Ο πρώτος είναι ότι οι κωδικοί οι οποίοι είναι πάνω από 7 χαρακτήρες χωρίζονται σε δύο κομμάτια και το κάθε κομμάτι έχει διαφορετικό hash. Ο $2^{ος}$ λόγος είναι ότι όλα τα μικρά γράμματα που περιέχει ο κωδικός μετατρέπονται σε μεγάλα πριν κωδικοποιηθεί.
Το Ophcrack χρησιμοποίησε αρχικά το 2003 τα rainbow tables, μια διαδικασία η οποία στόχευε στις αδυναμίες της κωδικοποίησης LM. Αργότερα υιοθέτησαν αυτή την ιδέα και άλλα cracking tools με αποτέλεσμα την γρήγορη εύρεση κωδικών ακόμα και μέσα σε λίγα δευτερόλεπτα.

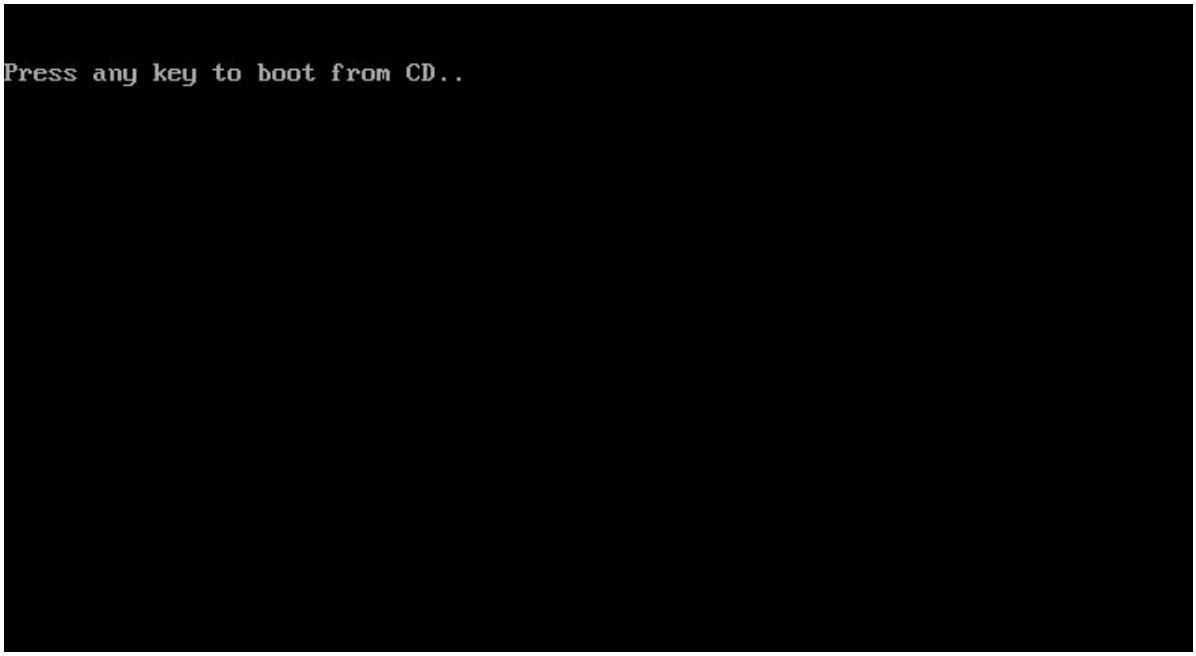
Το Live CD μπορεί να βρεθεί στην διεύθυνση:
http://ophcrack.sourceforge.net

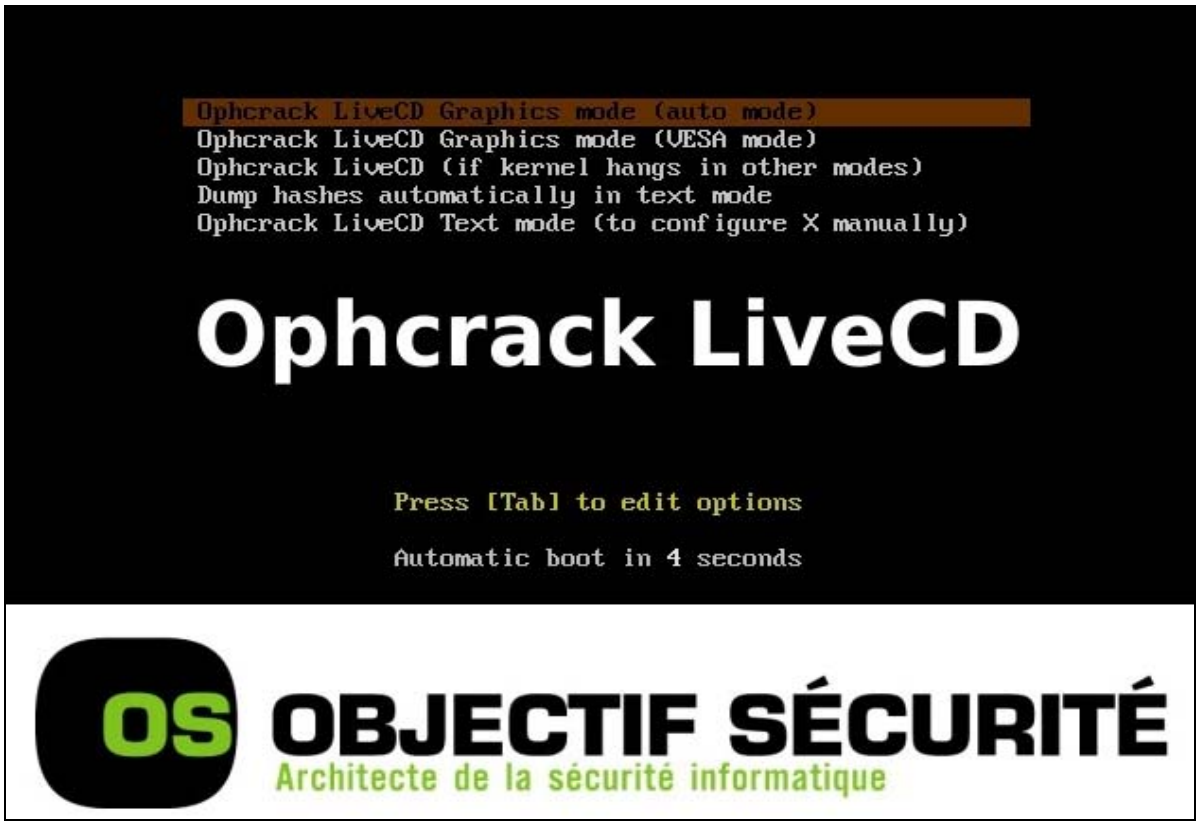


Αφού κατεβάσουμε την έκδοση του Ophcrack από το παραπάνω url πρέπει να επιλέξουμε το σύστημά μας όταν ξεκινάει να κάνει boot από το cd ώστε να τρέξει το Ophcrack. Αυτό το επιτυγχάνουμε πατώντας DEL κατά την εκκίνηση του υπολογιστή ώστε να μπούμε στις ρυθμίσεις του BIOS. Αφού εισέλθουμε επιλέγουμε από τις ρυθμίσεις του BIOS σαν πρώτη επιλογή όταν ξεκινήσει ο υπολογιστής να κάνει boot πρώτα από το cd.



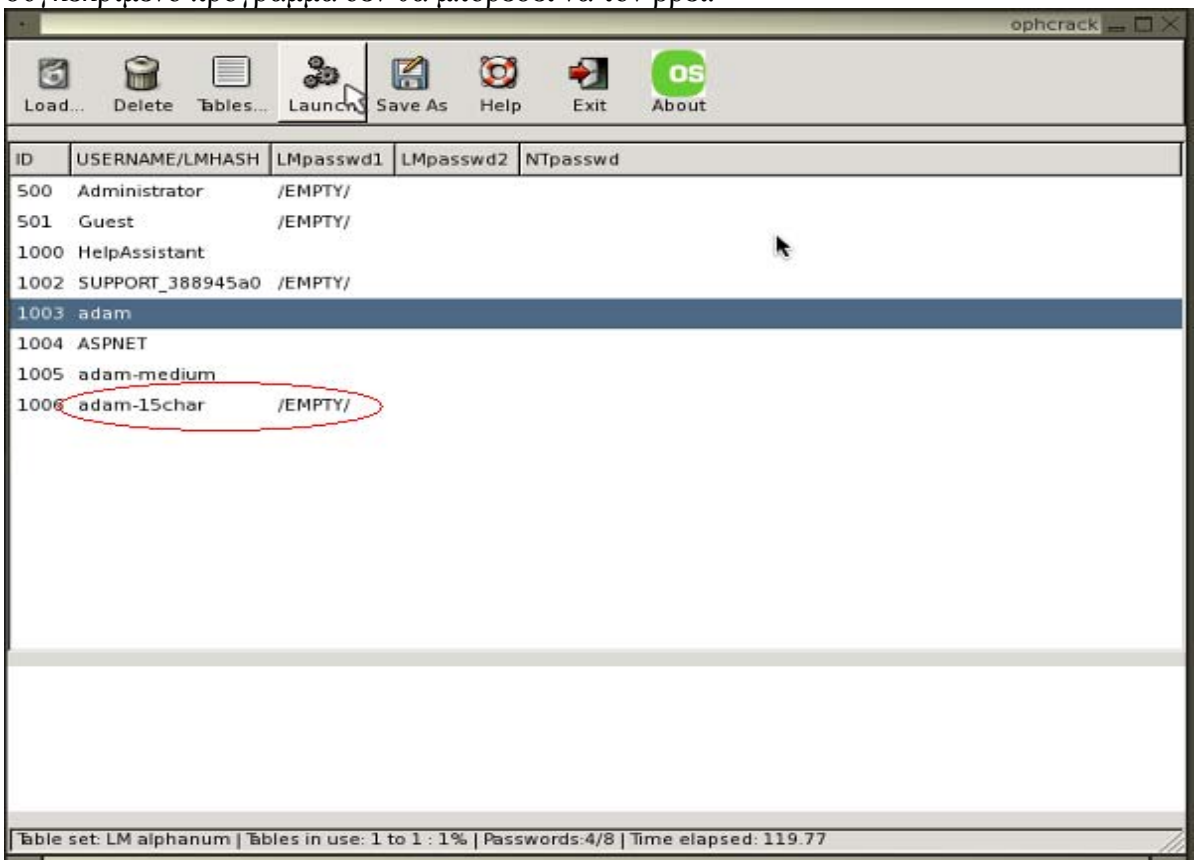
Έπειτα πατάμε EXIT και αποθηκεύουμε τις ρυθμίσεις που κάναμε. Κατά την εκκίνηση του υπολογιστή μας εμφανίζεται το παρακάτω μήνυμα και μας ζητάει να πατήσουμε ένα οποιοδήποτε πλήκτρο ώστε το σύστημα να ξεκινήσει να διαβάζει από το cd.





Στην συγκεκριμένη περίπτωση δημιουργήσαμε 3 λογαριασμούς χρηστών. Στον πρώτο αποδόθηκε ο κωδικός ¨easypass¨, στον δεύτερο ένα κωδικό αποτελούμενο από χαρακτήρες σύμβολα και αριθμούς και στον τρίτο λογαριασμό ένας κωδικός μεγαλύτερος από 14 χαρακτήρες.

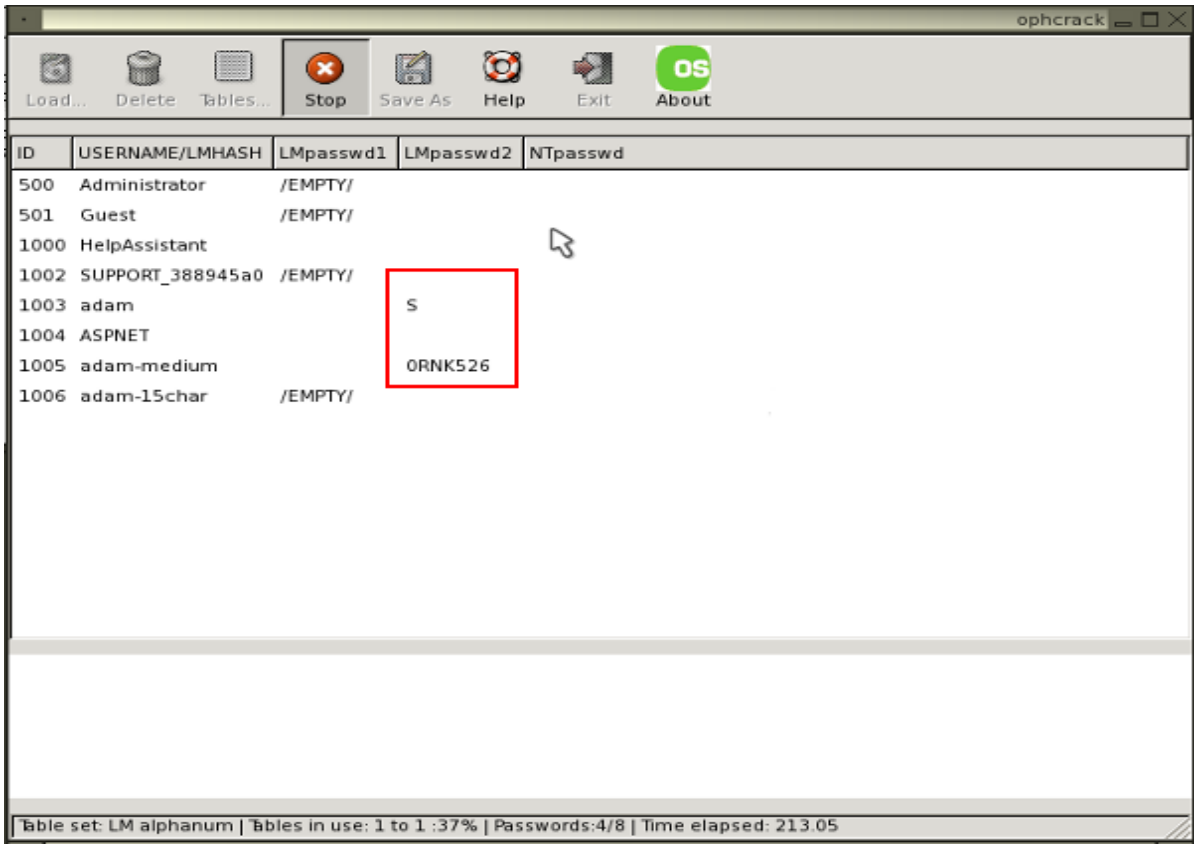
Αφού πλέον έχουμε εισέλθει με το Ophcrack μας εμφανίζεται μια λίστα με όλα τα accounts που υπάρχουν στο σύστημα. Πατώντας το "Launch"ξεκινάει η προσπάθεια ανεύρεσης των κωδικών. Στο παράδειγμά μας τα usernames είναι τα adam(με τον απλό κωδικό), το adam-medium (τον δυνατό κωδικό) και τον adam-15chars (με κωδικό που αποτελείται πάνω από 14 χαρακτήρες). Καθώς ξεκινάει το πρόγραμμα, δεν μας εμφανίζεται καν ο 3^{ος} κωδικός ο οποίος αποτελείται πάνω από 15 χαρακτήρες.. Αυτό σημαίνει ότι ο κωδικός είναι αρκετά ισχυρό και ότι σε περίπτωση που αποτελείτε πάνω από 14 χαρακτήρες τότε το συγκεκριμένο πρόγραμμα δεν θα μπορέσει να τον βρεί.

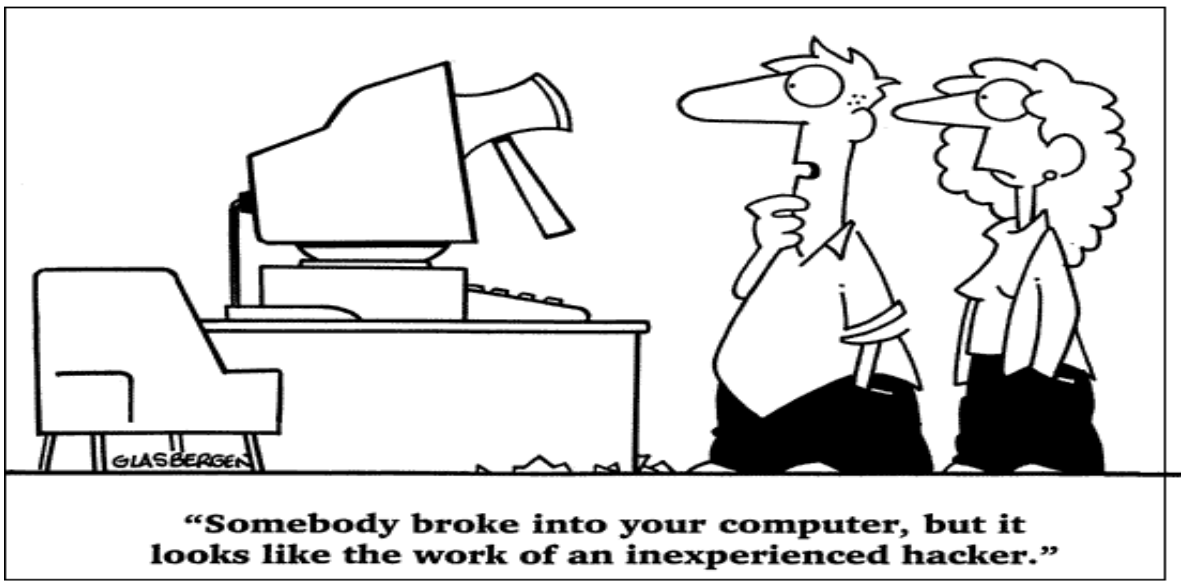


Όταν ξεκινήσει να δουλεύει το πρόγραμμα θα εμφανίζονται στην οθόνη διάφοροι συνδυασμοί γραμμάτων, στα πεδία LMpasswd1 και LMpasswd2.

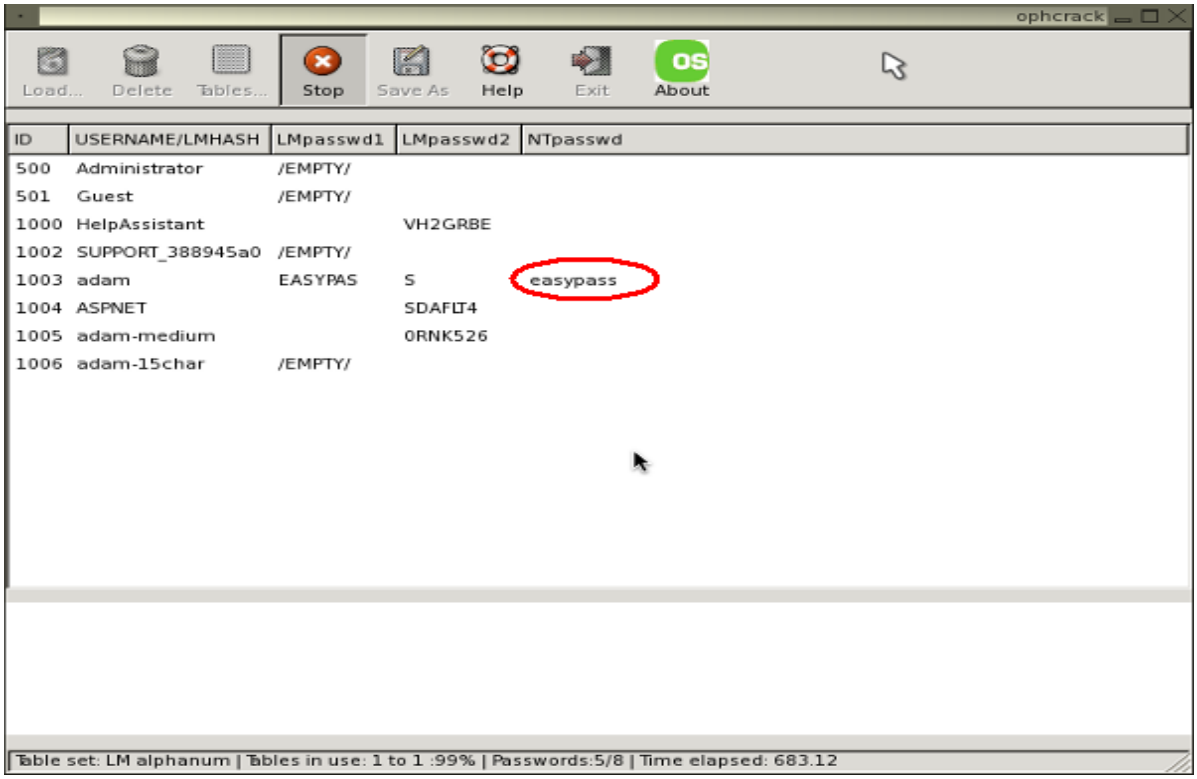
Έπειτα από 5 λεπτά το Ophcrack καταφέρνει να σπάσει τον εύκολο κωδικό easypass. Επίσης σε περίπτωση που ο κωδικός αποτελείτε μέχρι και 13 γράμματα το Ophcrack καταφέρνει να τον σπάσει σχετικά γρήγορα.

--Αναζήτηση κωδικών--

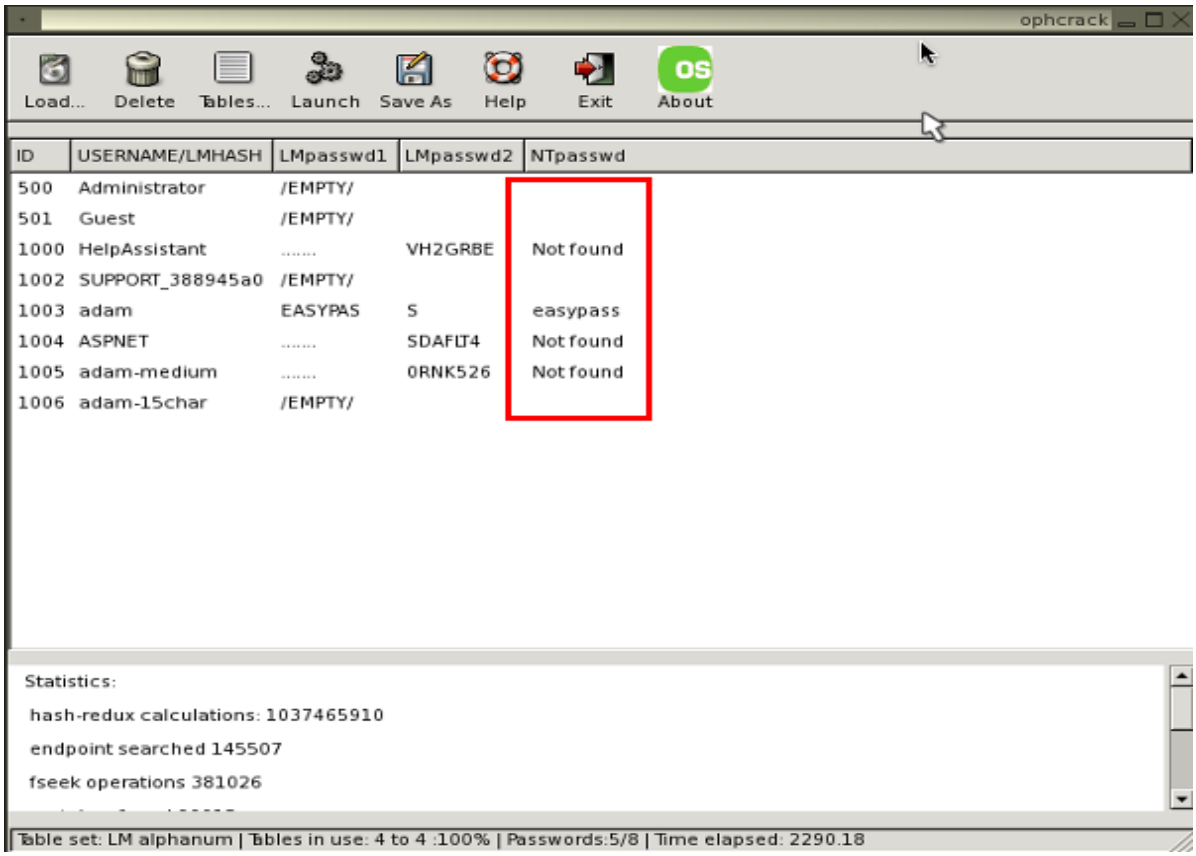




--Εύρεση κωδικών--



Έπειτα από 30 λεπτά το Ophcrack σταματάει τις προσπάθειες εύρεσης των άλλων κωδικών αποτυγχάνοντας να σπάσει τον μέτριο κωδικό που ορίσαμε.



6.4 CAIN & ABEL

Το Cain και Abel είναι ένα δωρεάν εργαλείο κωδικών πρόσβασης για τα windows. Θεωρείτε οτι είναι το κορυφαίο εργαλείο ανάκτησης κωδικών πρόσβασης για τους χρήστες Unix και χειρίζεται μια μεγάλη ποικιλία στόχων. Μπορεί να ανακτήσει πολλά είδη κωδικών πρόσβασης χρησιμοποιώντας μεθόδους όπως packet sniffing, διασπώντας διάφορα hashes κωδικών πρόσβασης με μεθόδους όπως οι dictionary attacks, brute force ακόμα και επιθέσεις cryptanalysis, καταγράφοντας συνομιλίες VoIP, αποκρυπτογραφώντας πολύπλοκους κωδικούς, αποκαλύπτοντας κουτιά κωδικών, ξεσκεπάζοντας κωδικούς καταχωρημένους στην μνήμη και αναλύοντας πρωτόκολλα δρομολόγησης. Οι επιθέσεις cryptanalysis γίνονται μέσω των rainbow tables που μπορούν να παραχθούν με το πρόγραμμα winrtgen.exe που παρέχεται με το Cain.

6.4.1 ΕΓΚΑΤΑΣΤΑΣΗ ΣΕ WINDOWS

ΑΠΑΙΤΗΣΕΙΣ

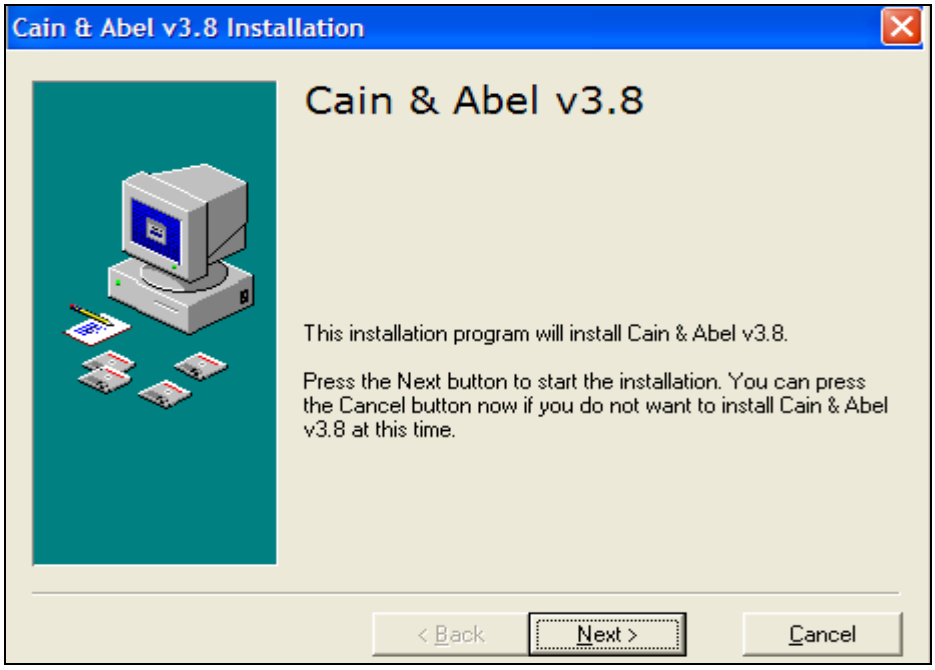
Η έκδοση του Cain & Abel απαιτεί τα παρακάτω:

- 10Mb ελεύθερο χώρο στο σκληρό δίσκο
- Λειτουργικό σύστημα Microsoft Windows 2000/XP/2003
- Winpcap Packet Driver(v2.3 ή μεγαλύτερη)
- Airpcap Packet Driver (για παθητικές ασύρματες sniffer / WEP επιθέσεις).

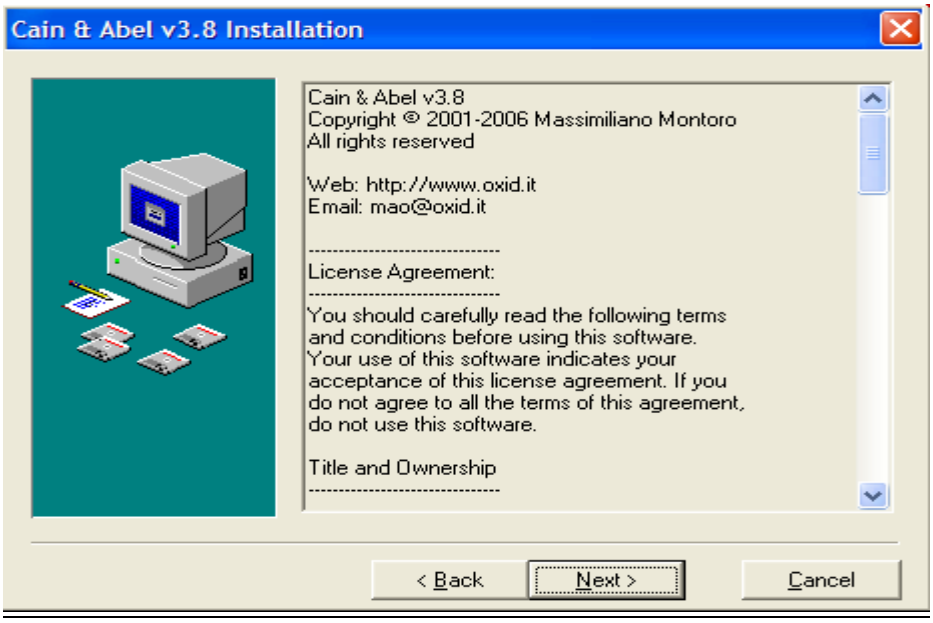
6.4.2 Εγκατάσταση Cain

Επισκεφτήκαμε την ιστοσελίδα www.oxid.it/cain.html και κατεβάσαμε το Cain & Abel το οποίο διανέμεται σαν ένα εκτελέσιμο αρχείο self-installing ονομαζόμενο "ca_setup.exe". Το Cain (Cain.exe) είναι η κύρια εφαρμογή GUI, ενώ το Abel είναι μια υπηρεσία των Windows που αποτελείτε από δύο αρχεία: το Abel.exe και το Abel.dll…Αφού κατεβάσουμε το πρόγραμμα από την παραπάνω διεύθυνση ξεκινάμε την εγκατάσταση η οποία είναι πολύ απλή. Αρχικά μας εμφανίζεται η παρακάτω οθόνη:

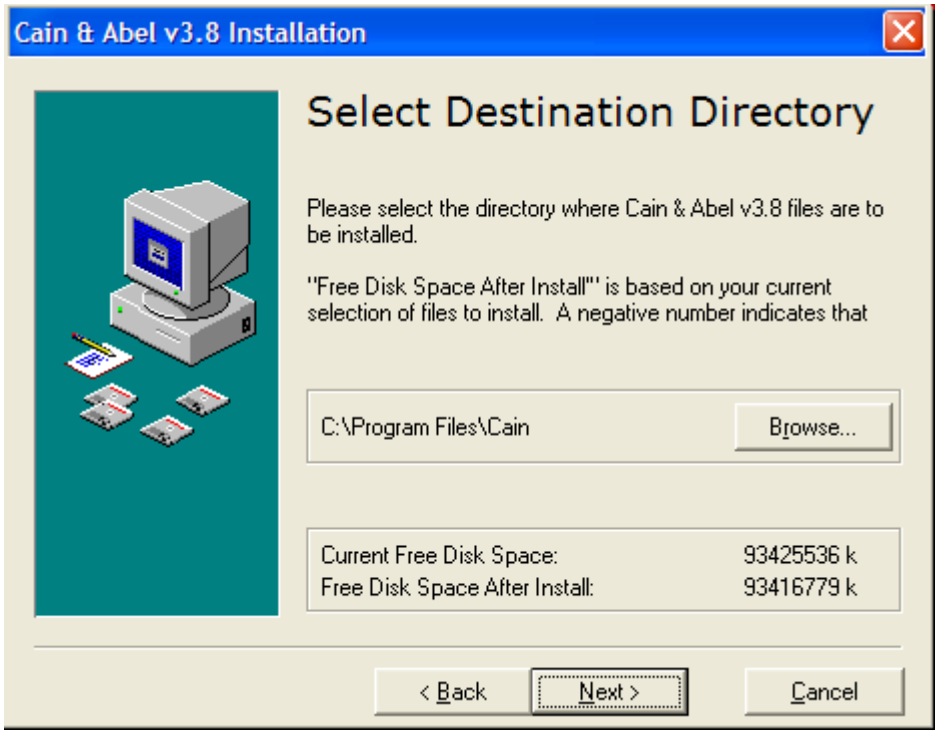
-Εικόνα 1-



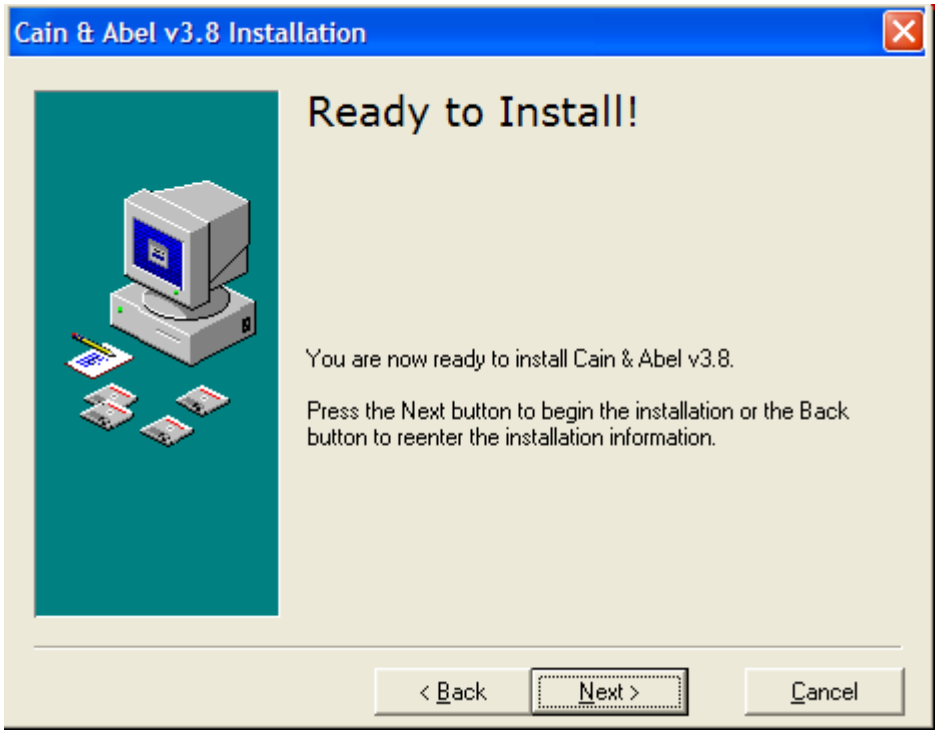
-Εικόνα 2-



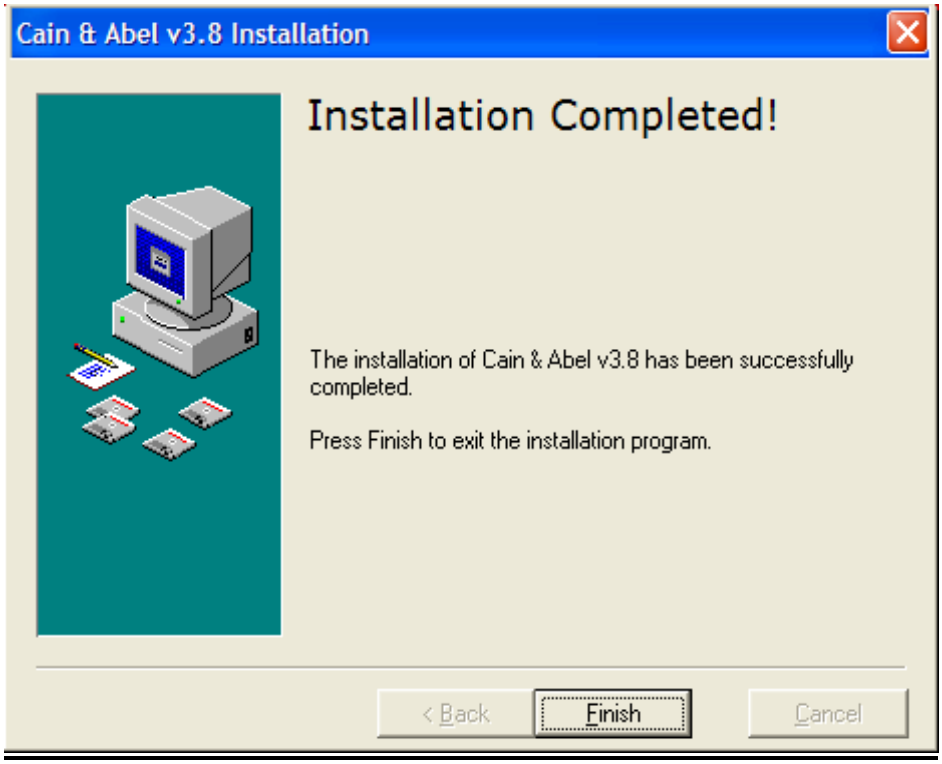
-Εικόνα 3-



-Εικόνα 4-

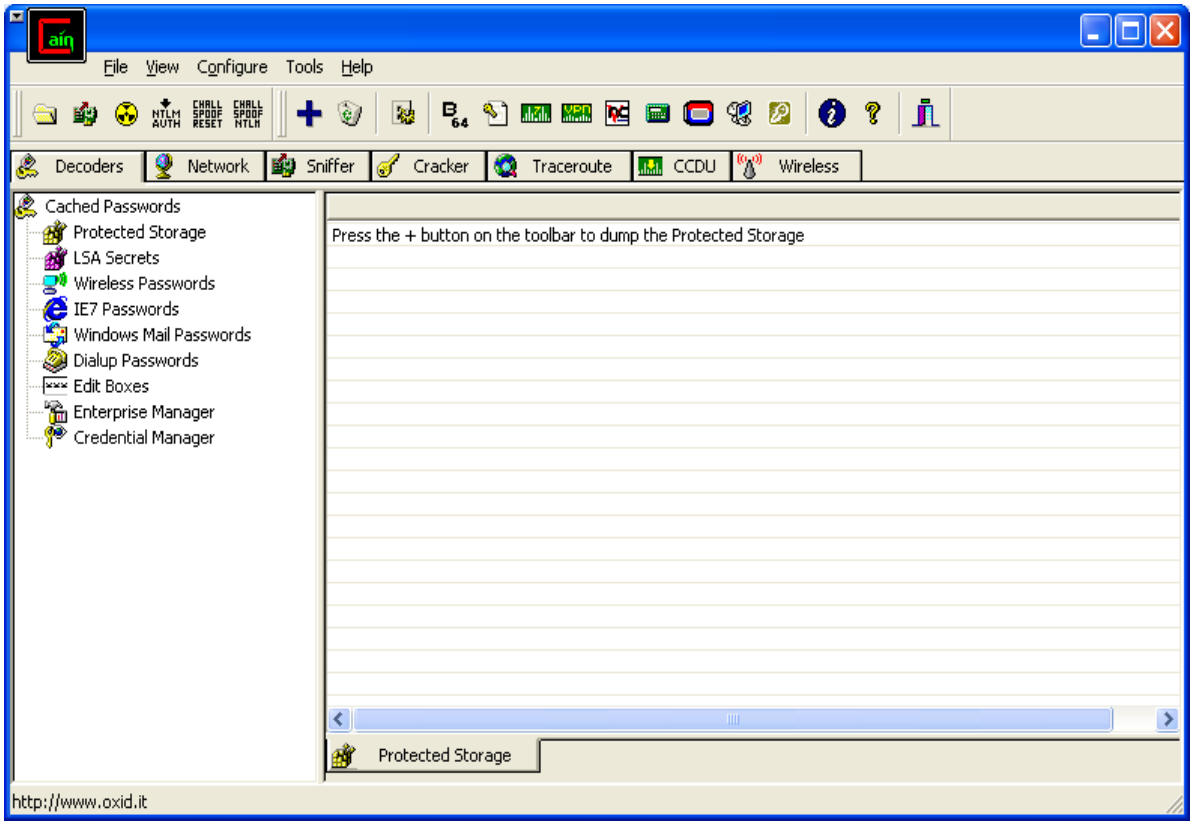


-Εικόνα 5-



Πλέον το πρόγραμμα έχει εγκατασταθεί και είμαστε έτοιμοι να το τρέξουμε.

-Εικόνα 6-

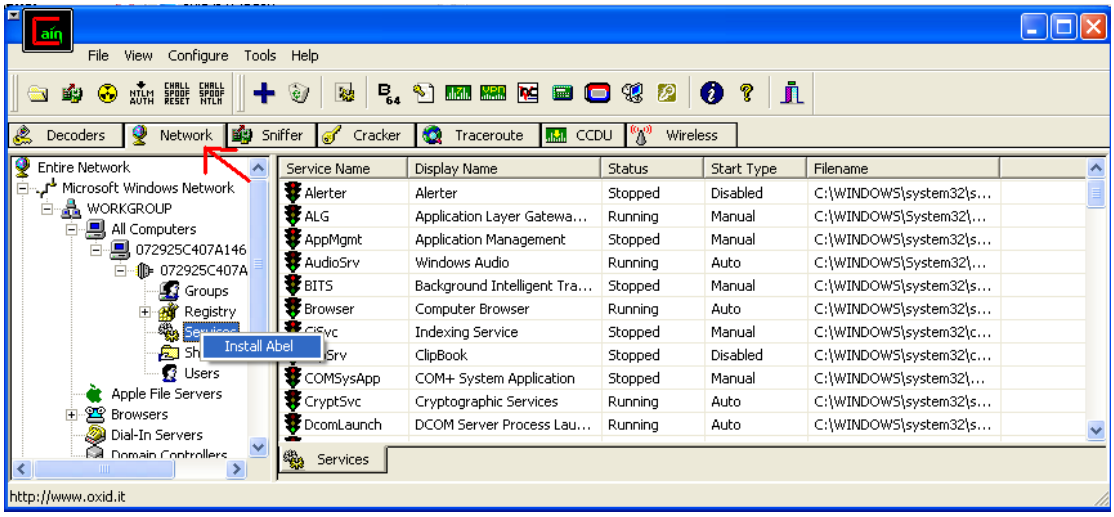


6.4.3 Εγκατάσταση Abel

Το Abel είναι μια υπηρεσία των Windows NT που αποτελείτε από δύο αρχεία, τα "Abel.exe" και το "Abel.dll". Αυτά τα αρχεία αποθηκεύονται κατά την εγκατάσταση στο φάκελο του προγράμματος αλλά δεν αποθηκεύονται αυτόματα στο σύστημα Το Abel μπορεί να εγκατασταθεί είτε με την βοήθεια του command prompt είτε μέσω του Cain, και απαιτεί προνόμια Administrator στο μηχάνημα το οποίο δουλεύει.

♠ Με το command prompt

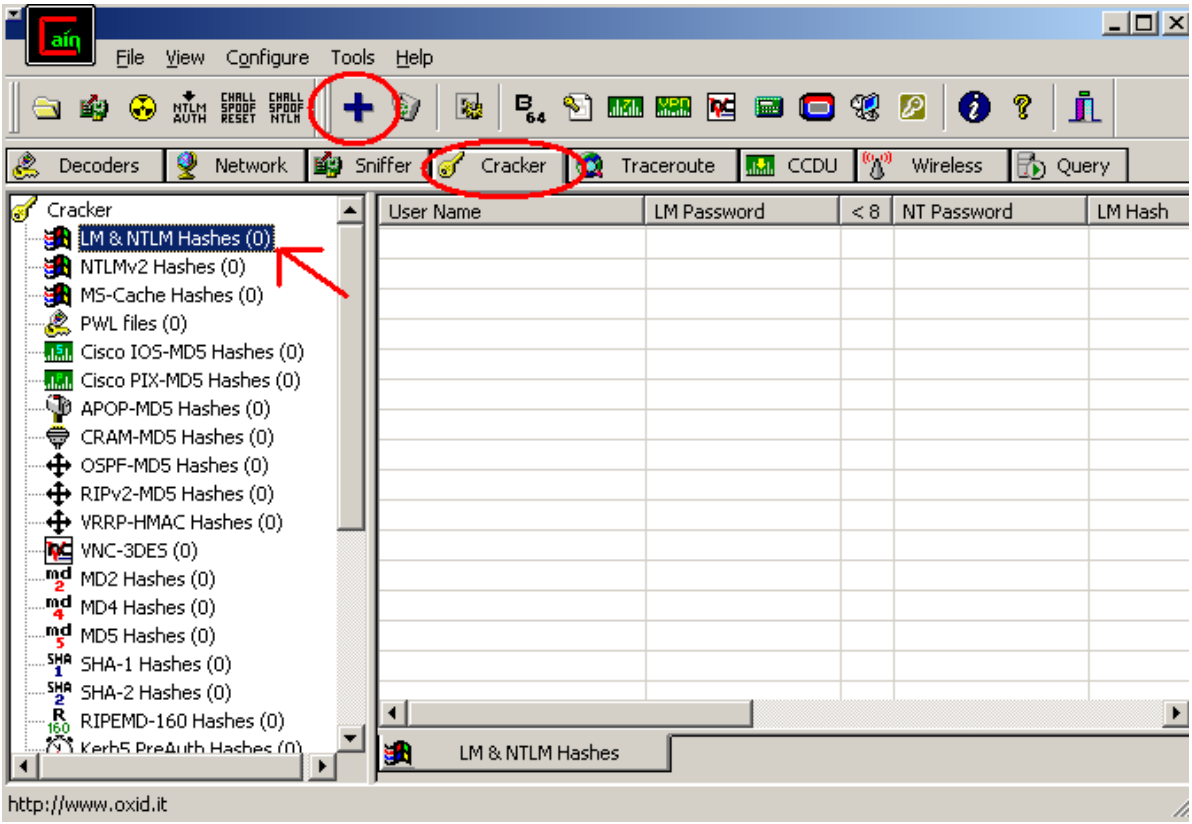
♠Μέσω του Cain



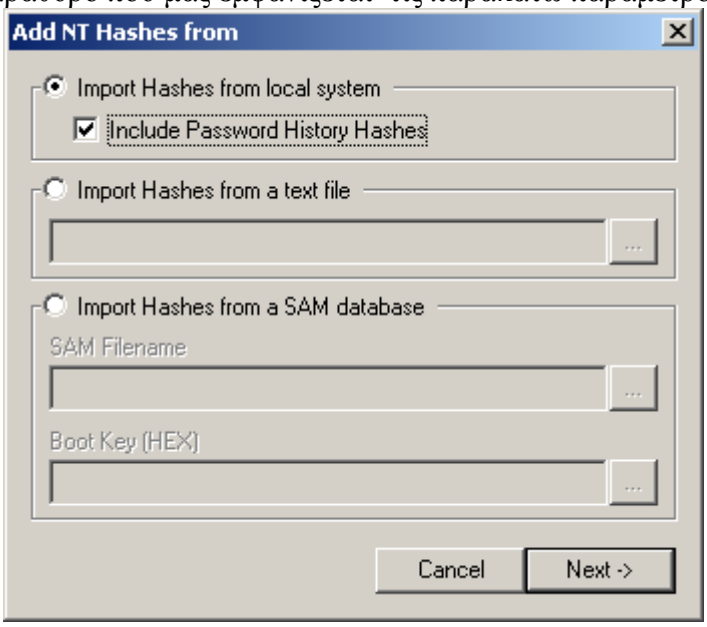
Το Abel επικοινωνεί με το Cain χρησιμοποιώντας τη «σωλήνα» των Windows *\\computername\pipe\abel* και δέχεται συνδέσεις από πολλούς hosts ταυτόχρονα. Όλα τα δεδομένα τα οποία μεταφέρονται μέσω αυτού του σωλήνα είναι κρυπτογραφημένα χρησιμοποιώντας τον αλγόριθμο συμμετρικής κρυπτογράφησης RC4 και το σταθερό κλειδί "Cain & Abel". Αυτό γίνεται για να ανακατωθεί η κίνηση η οποία στέλνεται στο διαδίκτυο και όχι για να «κρυφτούν» οι προθέσεις του προγράμματος.

6.5 ΑΝΑΚΤΗΣΗ ΚΩΔΙΚΩΝ ΜΕΣΩ ΤΟΥ CAIN & ABEL

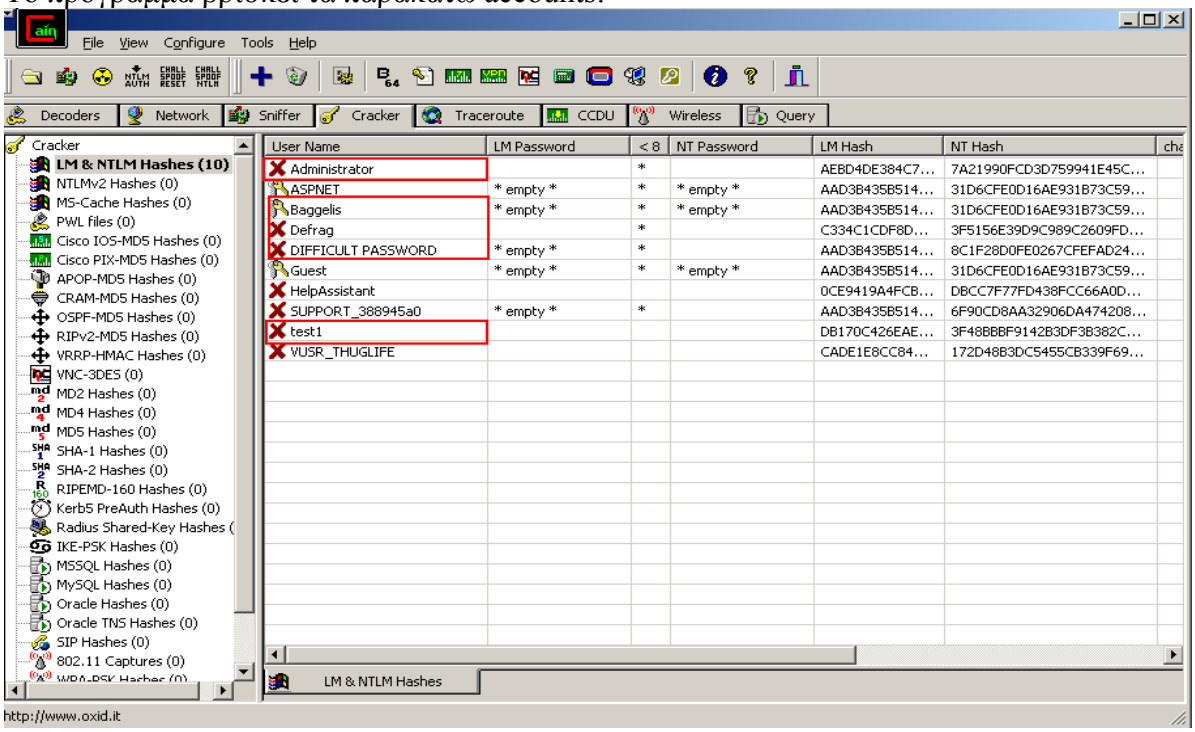
Παρακάτω θα επιχειρήσουμε να σπάσουμε τους κωδικούς των λογαριασμών χρηστών που βρίσκονται στο σύστημα. Έχοντας επιλέξει στην καρτέλα Cracker την κατηγορία LM & NTLM Hashes πατάμε το κουμπί  ώστε να εμφανίσουμε τα διαθέσιμα accounts.



Επιλέγουμε στο παράθυρο που μας εμφανίζεται τις παρακάτω παραμέτρους:



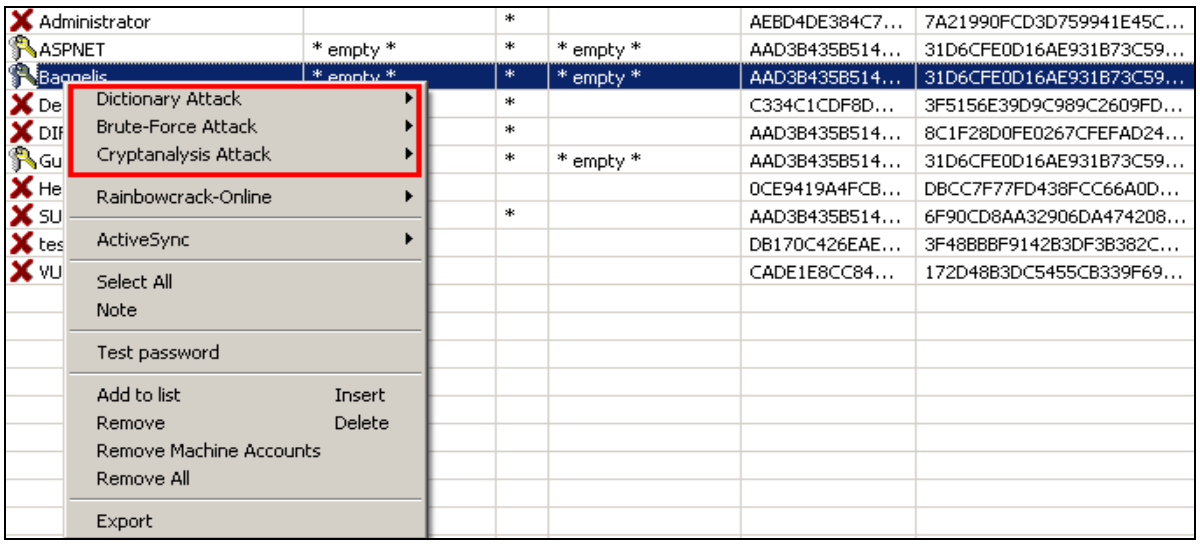
Το πρόγραμμα βρίσκει τα παρακάτω accounts:



Οι κωδικοί οι οποίοι χρησιμοποιήθηκαν για τα παραπάνω accounts ώστε να δοκιμάσουμε το Cain & Abel είναι οι :

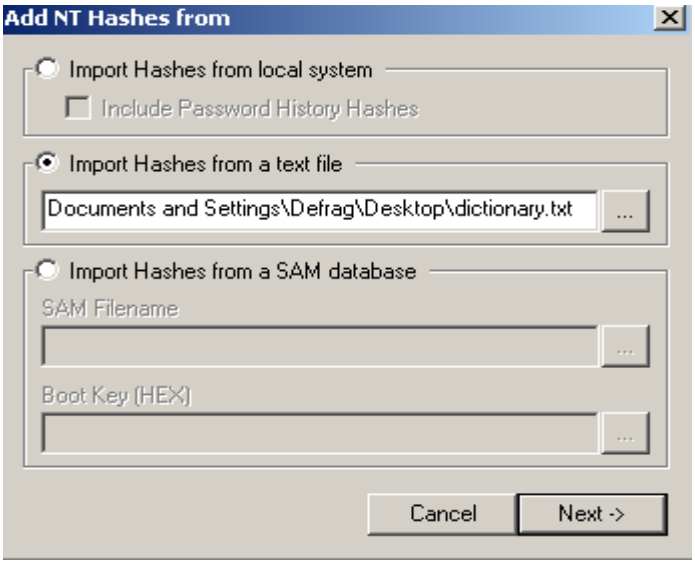
Administrator	12345
Baggelis	@123
Defrag	abcde
Test1	a1b2c3
DIFFICULT PASSWORD	!q@w#e$r%t67890

Κάνοντας δεξί κλικ σε ένα από τα accounts μας εμφανίζονται μεταξύ κάποιων άλλων ιδιοτήτων, οι 3 κύριες διαθέσιμες μέθοδοι αποκρυπτογράφησης κωδικών: Η επίθεση Brute Force, η επίθεση με την χρήση λεξικού (Dictionary Attack) και η Cryptalanalysis Attack η οποία χρησιμοποιεί Rainbow Tables για την ανεύρεση κωδικών.

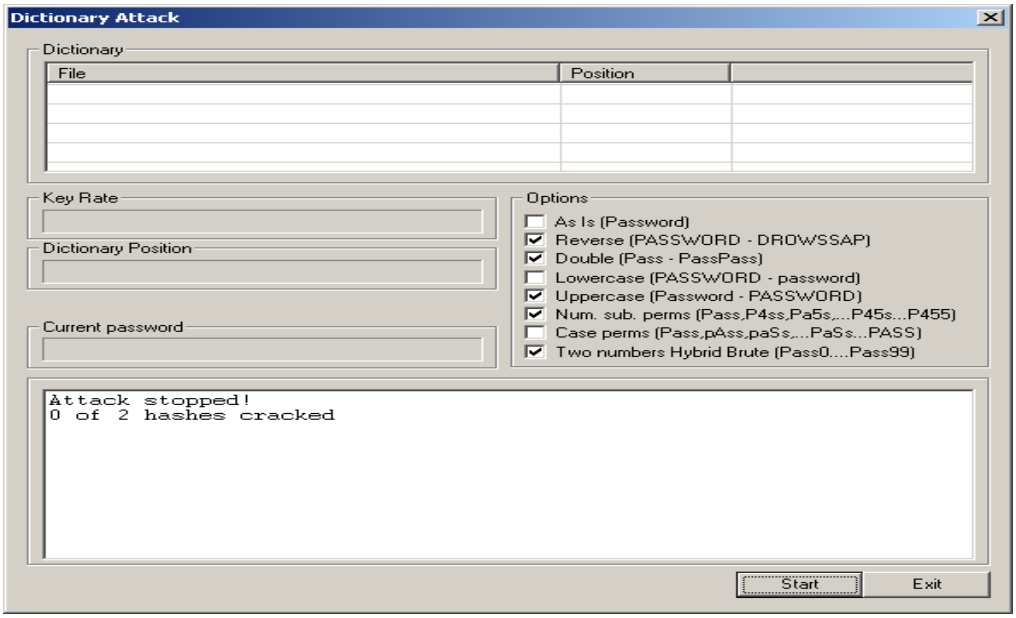


6.5.1 DICTIONARY ATTACK

Η μέθοδος του λεξικού χρησιμοποιεί μια έτοιμη λίστα από λέξεις (ή γενικότερα συνδυασμούς χαρακτήρων) τις οποίες κρυπτογραφεί με τον ίδιο αλγόριθμο που έχει δημιουργήσει τον κωδικό, ελέγχοντας αν το κρυπτογραφημένο κείμενο που δημιουργείται, είναι ίδιο με την κρυπτογραφημένη μορφή κωδικού. Το Cain παρέχει από μόνο του ένα μέσου μεγέθους λεξικό της τάξης των 3,30MB) το οποίο, όμως, μπορεί να αλλάξει με κάποιο λεξικό δικής μας προτίμησης το οποίο έχουμε φτιάξει εμείς ή έχουμε βρει έτοιμο από το Internet. Για την προσθαφαίρεση κάποιου λεξικού απλά θα επιλέξουμε από τις παραμέτρους που μας εμφανίζονται, όταν κάνουμε δεξί κλικ σε ένα account την ιδιότητα ¨Add to list¨ και θα προσθέσουμε το λεξικό:

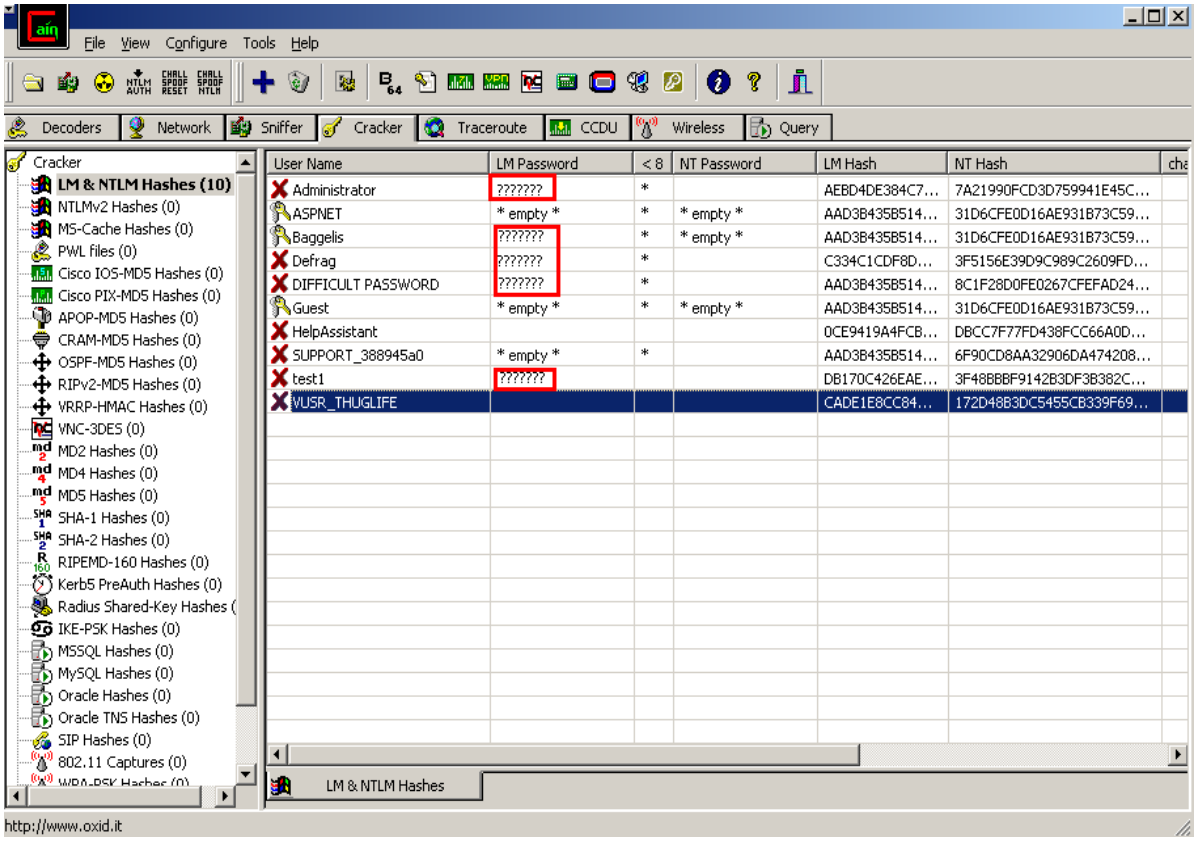


Πατάμε Start για να ξεκινήσει η ¨επίθεση¨ :



Στο λεξικό μας δεν βρισκόταν κανένας από τους παραπάνω κωδικούς, οπότε η προσπάθειά μας για την ανάκτηση κάποιου κωδικού, απέτυχε με αυτή τη μέθοδο.

Δοκιμάσαμε αντίστοιχα και στους άλλους λογαριασμούς χρηστών αλλά το αποτέλεσμα ήταν το ίδιο.



Η μέγιστη πιθανή διάρκεια της συγκεκριμένης επίθεσης εξαρτάται από το συνολικό μέγεθος των λεξικών που χρησιμοποιούνται. Η ταχύτητα, όμως, είναι κατά πολύ χαμηλότερη (δοκιμάζει περίπου σαράντα χιλιάδες κωδικούς ανά δευτερόλεπτο) από αυτήν της Brute Force επίθεσης η οποία δοκιμάζει περίπου ενάμιση εκατομμύριο κωδικούς ανά δευτερόλεπτο.

Η χρήση της συγκεκριμένης επίθεσης μπορεί να χαρακτηριστεί αρκετά αποδοτική με την χρήση ενός ισχυρού λεξικού. Τέτοια λεξικά μπορούν να βρεθούν στις παρακάτω διευθύνσεις :

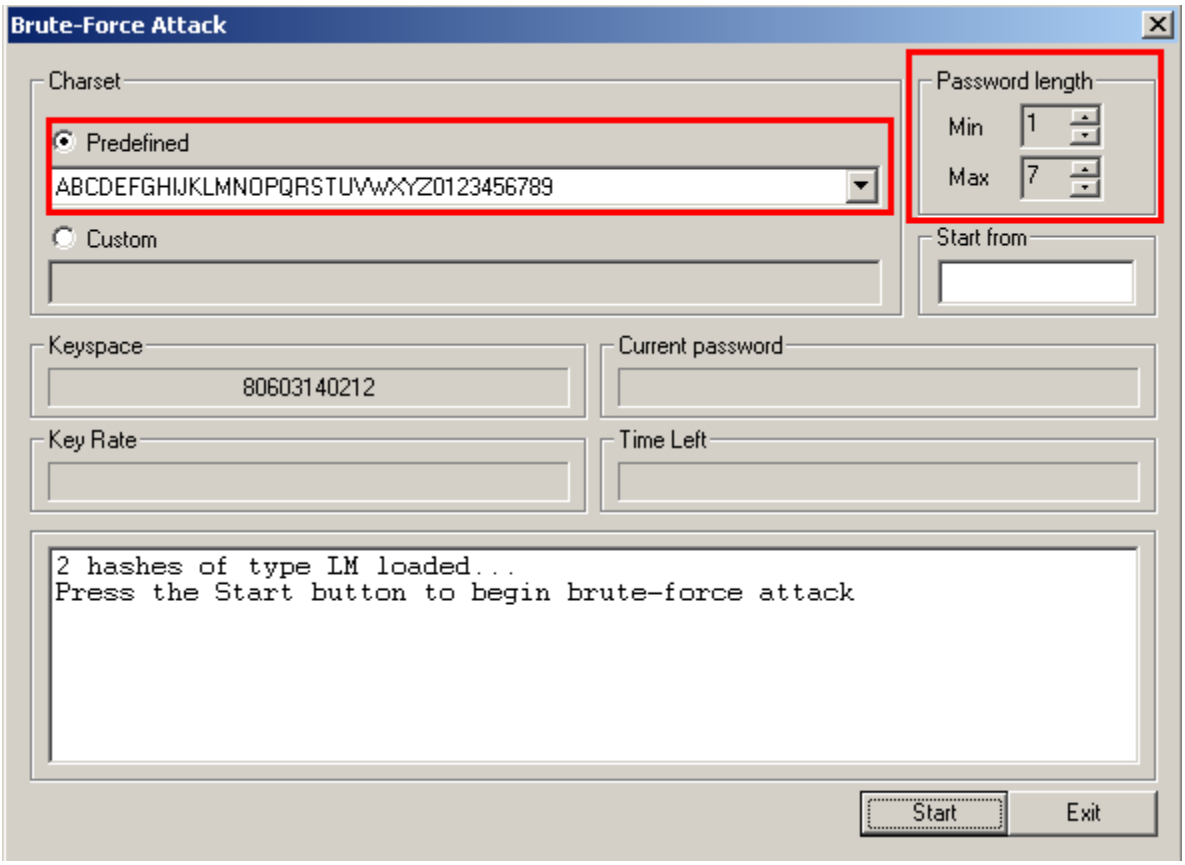
- http://www.lastbit.com/dict.asp
- http://www.outpost9.com/files/WordLists.html
- http://www.phreak.org/html/wordlists.shtml
- http://www.cotse.com/tools/wordlists1.htm
- ftp://ftp.ox.ac.uk/pub/wordlists/
- http://packetstormsecurity.org/Crackers/wordlists/

6.5.2 BRUTE FORCE ATTACK

Η μέθοδος της Brute Force επίθεσης (κυριολεκτικά: επίθεση με την χρήση ¨ωμής βίας¨) είναι ο πιο γνωστός και διαδεδομένος τρόπος αποκρυπτογράφησης κωδικών, αφού για την χρήση τους δεν απαιτείται τίποτε περισσότερο από την κατοχή του κρυπτογραφημένου κειμένου και τη γνώση του αλγόριθμου με τον οποίο έχει κρυπτογραφηθεί. Το Cain υλοποιεί ένα εξελιγμένο υποσύστημα Brute Force αποκρυπτογράφησης, το οποίο είναι προσβάσιμο από την αντίστοιχη επιλογή, που εμφανίζεται κάνοντας δεξί κλικ πάνω σε ένα account.

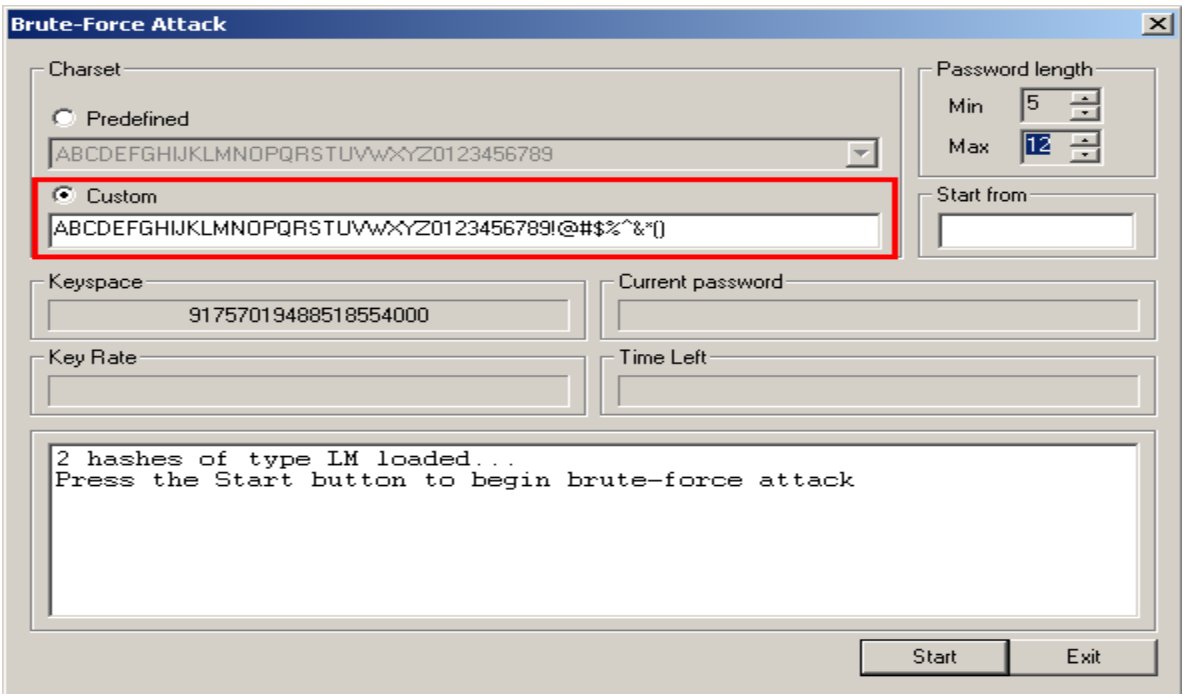
Από το παράθυρο διαλόγου Brute Force Attack μπορούν να οριστούν κάποιοι παράμετροι προτού ξεκινήσει το σπάσιμο των κωδικών. Μπορούμε να επιλέξουμε (από το πεδίο Predefined) το σύνολο των χαρακτήρων (Charset) που περιέχει όλους τους χαρακτήρες που - πιθανώς - περιέχονται στην αρχική, μη κρυπτογραφημένη μορφή του κωδικού. Η πολυπλοκότητα της διαδικασίας αυξάνεται ανάλογα προς το μέγεθος του Character set που χρησιμοποιείται. Από την άλλη, ένα σύνολο χαρακτήρων που περιέχει, για παράδειγμα, μόνο τα πεζά γράμματα του λατινικού αλφαβήτου, πιθανώς να μην δημιουργήσει τον κατάλληλο συνδυασμό για την αποκρυπτογράφηση του κωδικού.

Από την περιοχή Password length μπορούμε να επιλέξουμε το ελάχιστο (πεδίο Min) και το μέγιστο (πεδίο Max) μήκος των κωδικών που θα δοκιμαστούν. Ομοίως προς το Character set, το μέγεθος του κωδικού είναι μια παράμετρος που καθορίζει την πολυπλοκότητα του εγχειρήματος, οπότε και την πιθανή μέγιστη διάρκεια τις επίθεσης.

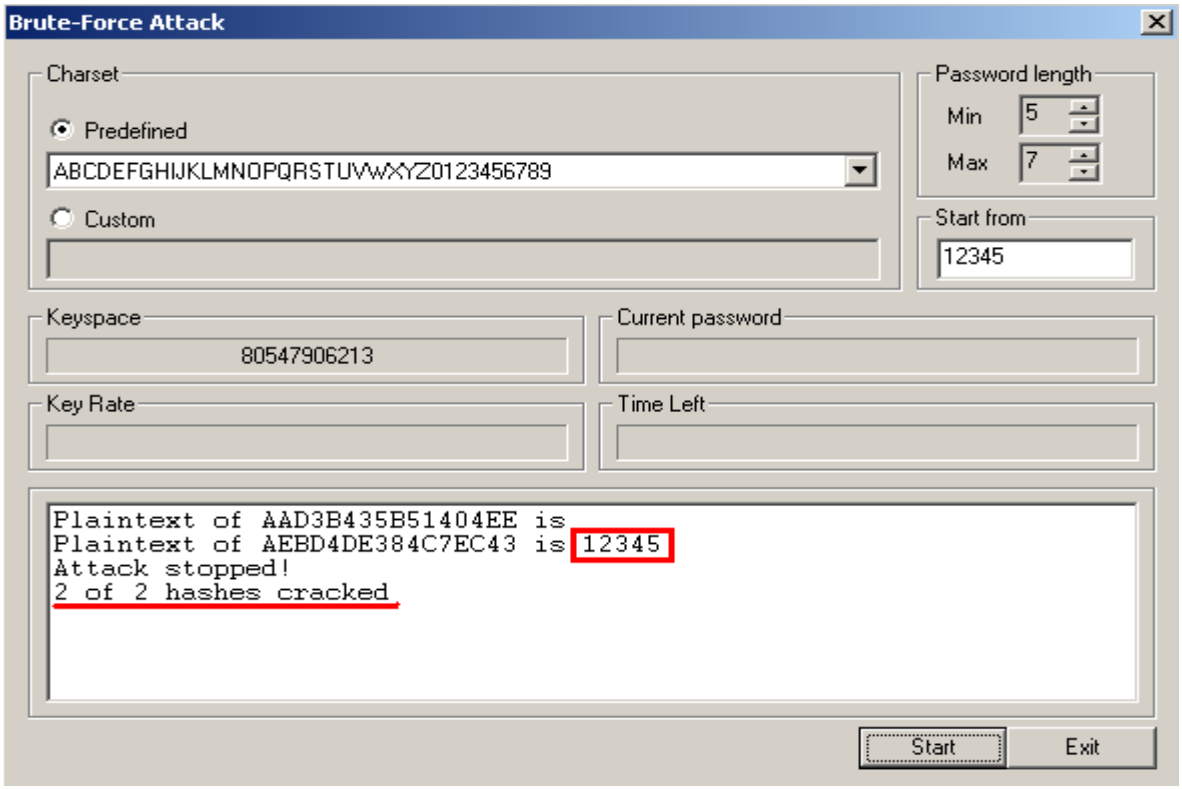


Σε περίπτωση που θέλουμε να χρησιμοποιήσουμε χαρακτήρες που δεν υπάρχουν στα ήδη παρεχόμενα σύνολα χαρακτήρων, θα πρέπει να εισάγουμε ένα δικό μας, ενεργοποιώντας το

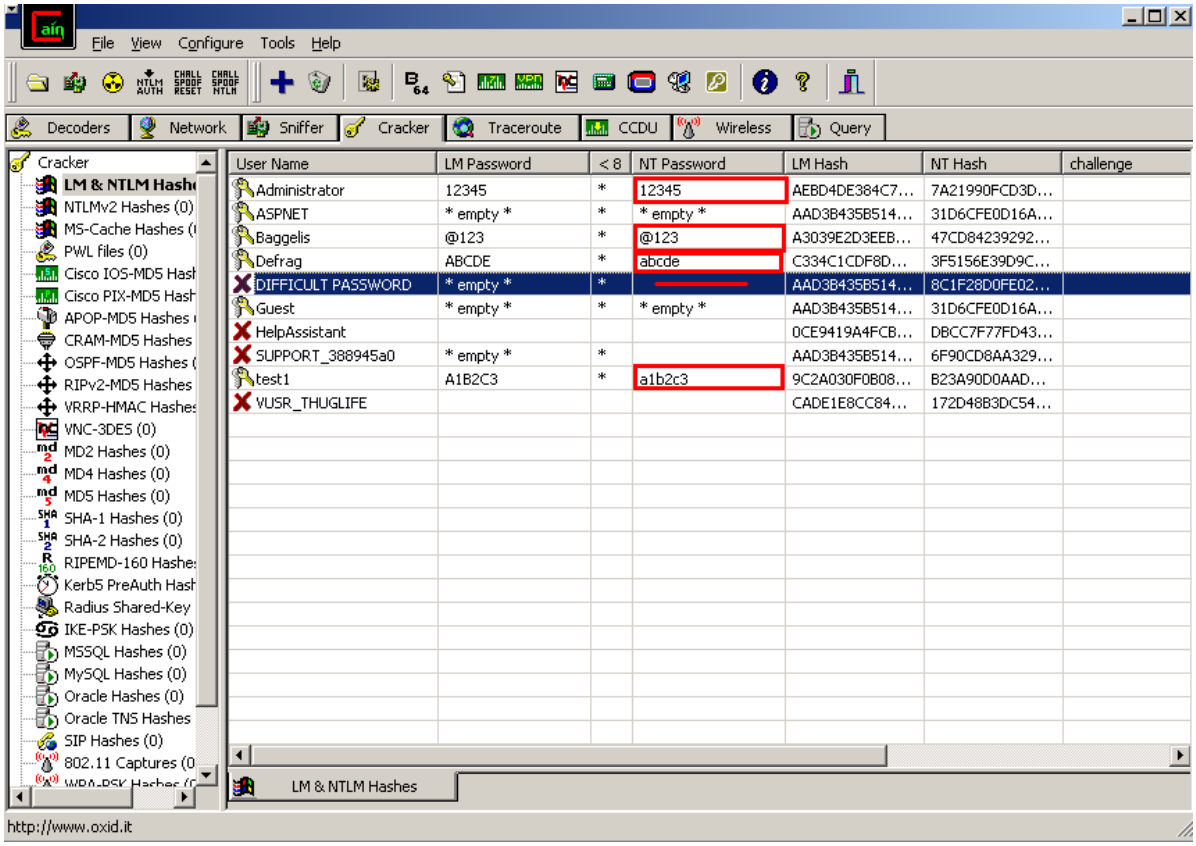
πεδίο ¨Custom¨ στην περιοχή Charset. Δεν αρκεί να εισάγουμε μόνο τους επιπλέον χαρακτήρες. Μόλις έχουμε ολοκληρώσει την παραμετροποίηση της επίθεσης, πατάμε το κουμπί Start και περιμένουμε μέχρι να ανευρεθεί ο κωδικός.



Ξεκινώντας το σπάσιμο καταφέραμε να βρούμε τον κωδικό του Administrator ο οποίος ήταν ¨12345¨.



Αντίστοιχα, κάναμε το ίδιο και με τους άλλους κωδικούς καταφέρνοντας να σπάσουμε επιτυχώς 4 από τους 5.



Στην περίπτωση του DIFFICULT PASSWORD ήταν αδύνατο να σπάσει ο κωδικός μιας και για την ανάκτησή του το σύστημα μας δεν αναγνώρισε καν ότι υπάρχει κωδικός, πράγμα απολύτως φυσιολογικό αφού το μήκος του ξεπερνούσε τους 13 χαρακτήρες.

Στον παρακάτω πίνακα παρουσιάζονται κάποια νούμερα από την παραδοχή ότι ένα cracking tool δοκιμάζει ένα εκατομμύριο συνδυασμούς το δευτερόλεπτο, σε ένα τυπικό σύστημα.

Μέγεθος Password	Ένα σετ χαρακτήρων (26) Όλα πεζά ή όλα κεφαλαία	Δύο σετ χαρακτήρων (52) Πεζά και κεφαλαία	Τρία σετ χαρακτήρων (62) Πεζά, κεφαλαία και νούμερα	Όλα τα σετ χαρακτήρων (92) Πεζά, κεφαλαία, νούμερα και σύμβολα
3 χαρακτήρες	0,01 δευτερόλεπτα	0,14 δευτερόλεπτα	0,22 δευτερόλεπτα	0,77 δευτερόλεπτα
4 χαρακτήρες	0,45 δευτερόλεπτα	7,3 δευτερόλεπτα	14,7 δευτερόλεπτα	71 δευτερόλεπτα
5 χαρακτήρες	11,8 δευτερόλεπτα	6,3 λεπτά	15,2 λεπτά	1,8 ώρες
6 χαρακτήρες	5,1 λεπτά	5,4 ώρες	15,7 ώρες	1 εβδομάδα
7 χαρακτήρες	2,2 ώρες	11 μέρες	40 μέρες	1,7 χρόνια
8 χαρακτήρες	2,4 μέρες	1,6 χρόνια	6,9 χρόνια	1,62 αιώνες
9 χαρακτήρες	2 μήνες	88 χρόνια	4,29 αιώνες	14,9 χιλιετηρίδες
10 χαρακτήρες	4,4 χρόνια	4,5 χιλιετηρίδες	26,6 χιλιετηρίδες	1.377 χιλιετηρίδες

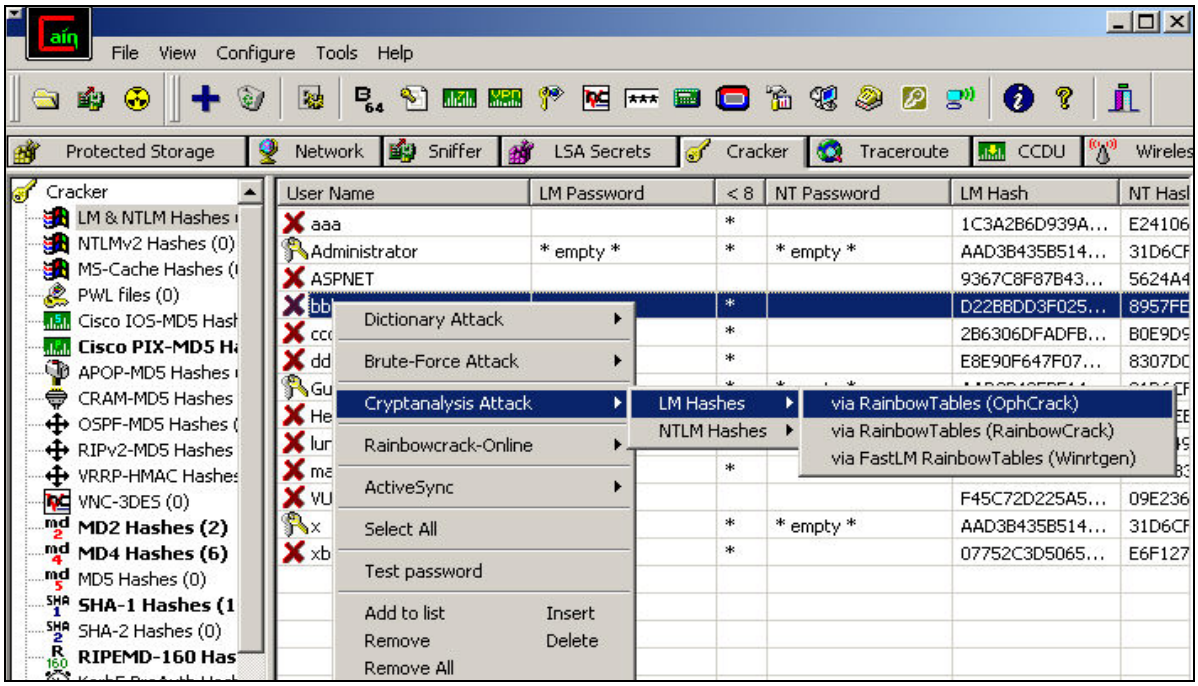
6.5.3 CRYPTANALYSIS ATTACK

Η συγκεκριμένη τακτική είναι αρκετά γρήγορη παρολαυτά όμως είναι χρήσιμη στο να σπάει μόνο μερικά είδη κρυπτογραφημένων κωδικών. Χρησιμοποιεί ένα σέτ από μεγάλα tables από προ-υπολογισμένους κρυπτογραφημένους κωδικούς (Rainbow Tables), ώστε να βελτιώσει τις μεθόδους ανταλλαγής οι οποίες είναι γνωστές σήμερα και για να ανακτήσει γρηγορότερα διάφορους κωδικούς.

Είναι συμβατό με το RainbowCrack, και υποστηρίζει Rainbow Tables για τους εξής αλγόριθμους:

- LM
- FastLM,
- NTLM
- CiscoPIX
- MD2, MD4, MD5
- SHA-1, SHA-2 (256), SHA-2 (384), SHA-2 (512),
- MySQL (323), MySQL (SHA1),
- RIPEMD160

Η Cryptanalysis Attack δεν είναι συμβατή με το να σπάει hashes κωδικών τα οποία αιχμαλωτίζονται σε ένα δίκτυο, αντιθέτως είναι αρκετά αποτελεσματική να σπάει hashes τα οποία συχνά χρησιμοποιούνται για να υποθηκεύσουν κρυπτογραφημένους κωδικούς τοπικά.



Γενικότερα, το Cain & Abel είναι ένα πανίσχυρο εργαλείο και οι δυνατότητες του δεν περιορίζονται μόνο στην εύρεση κωδικών λογαριασμών χρηστών. Δυστυχώς μπορεί να χρησιμοποιηθεί μόνο σε Windows και όχι σε Unix συστήματα ώστε να μπορέσει να διαβάσει το /etc/passwd file. Μπορεί να χρησιμοποιηθεί σε πάρα πολλές περιπτώσεις εύρεσης-ανάκτησης κωδικών γενικότερα, ασφάλειας ,ως διαγνωστικό σύστημα για τον εντοπισμό δικτυακών προβλημάτων, όπως, επίσης, ως σύστημα απομακρυσμένης διαχείρισης των Windows υπολογιστών τοπικών δικτύων. Για περισσότερες πληροφορίες σχετικά με το ισχυρό αυτό cracking tool υπάρχουν στην διεύθυνση:
http://www.oxid.it/

ΚΕΦΑΛΑΙΟ 7 ΣΥΜΠΕΡΑΣΜΑΤΑ

Η παραπάνω αναφορά μας βοηθάει να κατανοήσουμε την σημασία των κωδικών στην καθημερινή τους χρήση. Η ασφάλεια είναι ένας σημαντικός παράγοντας ώστε να κρατάμε τα προσωπικά μας δεδομένα και όχι μόνο. Στόχος μας είναι η αποφυγή υποκλοπής δεδομένων από κακόβουλους χρήστες και η πλήρης θωράκιση αυτών των δεδομένων. Αυτό μπορεί να επιτευχθεί με την ορθή και σωστή χρήση των κωδικών πρόσβασης.

Το όνομα χρήστη και ο κωδικός είναι τα πιο σημαντικά στοιχεία που αποδεικνύουν την άδεια πρόσβασής σε ένα σύστημα. Για να αποτρέψουμε επίδοξους εισβολείς ή απλά περίεργους να αποκτήσουν πρόσβαση στις δικές μας υπηρεσίες όπως email, forum κλπ, χρειαζόμαστε ένα ισχυρό κωδικό. Η ανάγκη αυτή γίνεται ακόμα πιο έντονη όταν οι κωδικοί μας είναι πολύτιμα κλειδιά σε υπηρεσίες φιλοξενίας ιστοσελίδων, σε διακομιστές, πίνακες ελέγχου φόρουμ, λογαριασμοί σε τράπεζες ή ακόμα και στο ίντρανετ της επιχείρησης μας.

Η δυνατότητες των cracking tools που κυκλοφορούν είναι απεριόριστες και όσο προχωρά η τεχνολογία, σε συνδυασμό με την ελλιπής γνώση, δημιουργούν αρκετά κενά στους απλούς χρήστες υπολογιστικών συστημάτων. Ζητήματα όπως η ακεραιότητα και η εμπιστευτικότητα πρέπει να τονίζονται ιδιαίτερα όσο αφορά το κομμάτι της ασφάλειας των κωδικών οι οποίοι αποτελούν πλέον κομμάτι της προσωπικής μας ζωής.

ΒΙΒΛΙΟΓΡΑΦΙΑ

URL'S

http://www.gtsamis.gr/

http://support.mozilla.com/en-US/kb/

http://techrepublic.com.com/2001-10875-0.html

http://www.linuxconfig.org/Main_Page

http://www.psychocats.net/ubuntu/

http://lifehacker.com/

http://www.cyberciti.biz/

http://www.instructables.com/

http://techgurulive.com/

http://www.pcstats.com/

http://www.nothing2hide.net/

http://www.labtestproject.com/

http://www.instructables.com/

http://pcsupport.about.com/

http://www.gohacking.com/

http://www.insomnia.gr

http://awesome-tech.blogspot.com/

http://en.wikipedia.org/wiki

http://passwordsafe.sourceforge.net/

http://www.darknet.org.uk/

http://www.oxid.it/

http://www.happyhacker.org/

http://mechanicshell.wordpress.com/

http://www.ethicalhacker.net/

http://sectools.org/crackers.html

http://foracamp.gr/

http://www.openwall.com/john/

http://www.computeractive.gr/

http://www.cgomag.gr/

http://www.pcw.gr/

http://www.ubuntu.com/

http://pctrela.blogspot.com/

http://www.thelab.gr/

ΒΙΒΛΙΑ

HACKING UBUNTU *ΣΥΓΓΡΑΦΕΑΣ WILEY AND SONS LTD*

ΕΡΓΑΛΕΙΟΘΗΚΗ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΧΑΚΕΡ
ΣΥΓΓΡΑΦΕΑΣ JONES,KEITH J.

HACKING FOR DUMMIES *ΣΥΓΓΡΑΦΕΑΣ MCCLURE, STUART*

ΑΣΦΑΛΕΙΑΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΣΤΟΥΣ ΥΠΟΛΟΓΙΣΤΕΣ, ΣΤΟ ΙΝΤΕΡΝΕΤ, ΣΤΗΝ ΚΑΘΗΜΕΡΙΝΗ ΜΑΣ ΖΩΗ *ΣΥΓΓΡΑΦΕΑΣ ΣΟΥΡΗΣ ΑΝΔΡΕΑΣ*

ΟΙ ΧΑΚΕΡ ΕΠΙΤΙΘΕΝΤΑΙ *ΣΥΓΓΡΑΦΕΑΣ MANSFIELD, RICHARD*

ΜΗΝΙΑΙΑ ΕΛΛΗΝΙΚΑ ΠΕΡΙΟΔΙΚΑ

TOTAL XAKER
COMPUTER ΓΙΑ ΟΛΟΥΣ
RAM
PC WORLD
COMPUTER ACTIVE