

Κεφάλαιο 3. Διαχείριση Συνθηματικών και Επιθέσεις

Σύνοψη

Η εργαστηριακή δραστηριότητα, που παρουσιάζεται στο κεφάλαιο αυτό, αφορά τη διαχείριση συνθηματικών και την προστασία τους από επιθέσεις ανάκτησης συνθηματικών με χρήση τριών διαφορετικών μεθοδολογιών. Αν και η πλατφόρμα στην οποία θα υλοποιηθεί η δραστηριότητα είναι το Λ.Σ. Windows 2008 Server, οι βασικές αρχές που θα παρουσιαστούν εφαρμόζονται σε κάθε υπολογιστικό σύστημα. Μετά το πέρας της εργαστηριακής δραστηριότητας, ο φοιτητής θα είναι σε θέση να αναγνωρίζει τις κακές και να επιλέγει καλές πρακτικές για την επιλογή ανθεκτικών συνθηματικών.

Προαπαιτούμενη γνώση

Δεν απαιτείται κάποια ιδιαίτερη γνώση, πέρα από τη βασική δυνατότητα χρήσης ενός υπολογιστικού συστήματος με λειτουργικό σύστημα Windows.

3.1 Προεργασία

Για την υλοποίηση αυτής της δραστηριότητας, θα απαιτηθεί η χρήση ενός υπολογιστικού συστήματος με Λ.Σ. Windows. Μπορεί να χρησιμοποιηθεί το image που δημιουργήσατε στο Κεφάλαιο 1 για την υπηρεσία Okeanos, ή οποιοδήποτε υπολογιστικό σύστημα με Λ.Σ. Windows 7, 2008 ή νεότερα.

Αρχικά, θα πρέπει να γίνει σύνδεση με λογαριασμό administrator σε μια τοπική ή απομακρυσμένη κονσόλα του συστήματος και η δημιουργία τεσσάρων λογαριασμών χρήστη. Για το σκοπό αυτό, εκκινήστε την κονσόλα διαχείρισης του συστήματος (Server Manager) με έναν από τους παρακάτω τρόπους:

- Από το εικονίδιο στη γραμμή εργασιών



Εικόνα 3.1 Εικονίδιο εκκίνησης Server Manager

- Πατώντας Start και κάνοντας δεξί κλικ στην επιλογή Computer, από όπου επιλέγετε κατόπιν το Manage.
- Εκτελώντας διαδοχικά: **Start → Run → ServerManager.msc**
- Εκτελώντας διαδοχικά: **Control Panel → System and Security → Administrative Tools → Server Manager**
- Στο αριστερό μέρος του παραθύρου του Server Manager, ακολουθήστε τη διαδρομή:

Server Manager → Configuration → Local Users and Groups

και επιλέξτε Users, όπως φαίνεται στην ακόλουθη Εικόνα 3.2:



Εικόνα 3.2 Επιλογή χρηστών

Στο δεξί μέρος της οθόνης, βλέπετε τους υπάρχοντες λογαριασμούς χρήστη στο σύστημά σας. Εκτελούμε εναλλακτικά:

- Από το μενού Action, επιλογή New User
- Δεξί κλικ στο κενό του δεξιού μέρους και επιλογή New User
- Δεξί κλικ στο Users του αριστερού μέρους και επιλογή New User

Ως αποτέλεσμα, εμφανίζεται η φόρμα καθορισμού νέου λογαριασμού χρήστη:

A screenshot of the 'New User' dialog box. It contains the following fields and options:

- User name:** A text input field.
- Full name:** A text input field.
- Description:** A text input field.
- Password:** A password input field.
- Confirm password:** A password input field.
- ☒ **User must change password at next logon**
- ☐ **User cannot change password**
- ☐ **Password never expires**
- ☐ **Account is disabled**

At the bottom, there are three buttons: 'Help', 'Create', and 'Close'.

Εικόνα 3.3 Φόρμα καθορισμού νέου λογαριασμού χρήστη

Δημιουργήστε τέσσερις (4) νέους λογαριασμούς χρήστη, σύμφωνα με τα στοιχεία που παρουσιάζονται στον Πίνακα 3.1:

Όνομα χρήστη	Συνθηματικό	Ομάδα Χρήστη
user31	passMe1	Users
user32	Abc123	Guests
user33	Hockey1	Users
user34	1ep#%B#4	Administrator

Πίνακας 3.1 Στοιχεία λογαριασμών χρήστη προς δημιουργία

Από τον ιστότοπο του βιβλίου, κατεβάστε το αρχείο lab3-utils.zip που βρίσκεται στη διεύθυνση: <http://infosec.uom.gr/Study/LAB/ISS/6519/lab3-utils.zip> και αποσυμπίστε το στην επιφάνεια εργασίας (Desktop). Θα δημιουργηθεί ο κατάλογος (folder) ISS_Chapter3, με υλικό που θα χρησιμοποιήσουμε στη συνέχεια.

3.2 Ανάκτηση Συνόψεων Συνθηματικών

Σε αυτό το σημείο, θα χρειαστεί να εργαστούμε με τη βάση δεδομένων στην οποία το λειτουργικό σύστημα διατηρεί (αποθηκεύει) τα συνθηματικά των χρηστών. Για να εντοπίσουμε τη βάση δεδομένων και να εξετάσουμε το περιεχόμενό της, θα χρησιμοποιήσουμε το πρόγραμμα fgdump.

Από τον κατάλογο ISS_Chapter3\fgdump εκτελέστε το αρχείο fgdump.exe. Μετά την εκτέλεση θα παραχθούν τρία αρχεία. Το αρχείο με το οποίο θα ασχοληθούμε στη συνέχεια είναι αυτό με το όνομα: 127.0.0.1.pwdump.

Από τον κατάλογο ISS_Chapter3\notepad++ εκτελέστε το αρχείο Notepad++Portable και με αυτό ανοίξτε (Open) το αρχείο ISS_Chapter3\fgdump\127.0.0.1.pwdump. Παρατηρούμε ότι στο αρχείο υπάρχουν τόσες γραμμές, όσοι και οι λογαριασμοί χρηστών του συστήματος. Η μορφολογία της κάθε γραμμής (γραμμογράφηση) είναι:

Username : SID : LM Hash : NTLM Hash

- Μπορείτε να εντοπίσετε τους λογαριασμούς χρηστών;
- Τι παρατηρείτε για τον τρόπο αποθήκευσης των συνθηματικών;
- Μπορείτε να εντοπίσετε στη βιβλιογραφία υλικό σχετικό με τον όρο «Hash»;

Προτείνεται να εξετάσετε τις διαφορές μεταξύ των περιεχομένων της στήλης «LM Hash» και της στήλης «NTLM Hash».

3.3 Επίθεση Λεξικού

Η πρώτη επίθεση για την ανάκτηση αποθηκευμένων συνθηματικών, που θα εξετάσουμε, είναι η επίθεση λεξικού (Dictionary Attack). Η επίθεση αυτή βασίζεται στην υπόθεση ότι πολλοί χρήστες επιλέγουν για συνθηματικό μια συνηθισμένη ακολουθία χαρακτήρων (όπως π.χ. abc, 123, abc123, password, access κοκ), που είναι εύκολο να απομνημονευθεί. Έτσι, ο επιτιθέμενος δημιουργεί ή εντοπίζει λίστες (λεξικά) με τα πιθανά συνθηματικά και τα δοκιμάζει για να συνδεθεί στο σύστημα έχοντας γνωστό το όνομα χρήστη ενός λογαριασμού.

Από τον κατάλογο ISS_Chapter3\cain_abel εκτελέστε το αρχείο ca_install.exe για να εγκατασταθεί η εφαρμογή Cain & Abel. Αποδεχτείτε τις προτροπές του συστήματος για εγκατάσταση και του λογισμικού WinPcap, αφήνοντας ίδιες, σε κάθε περίπτωση, τις προεπιλεγμένες ρυθμίσεις.

Μετά την ολοκλήρωση της εγκατάστασης, θα εμφανιστεί στην επιφάνεια εργασίας το εικονίδιο της εφαρμογής (Εικόνα 3.4).



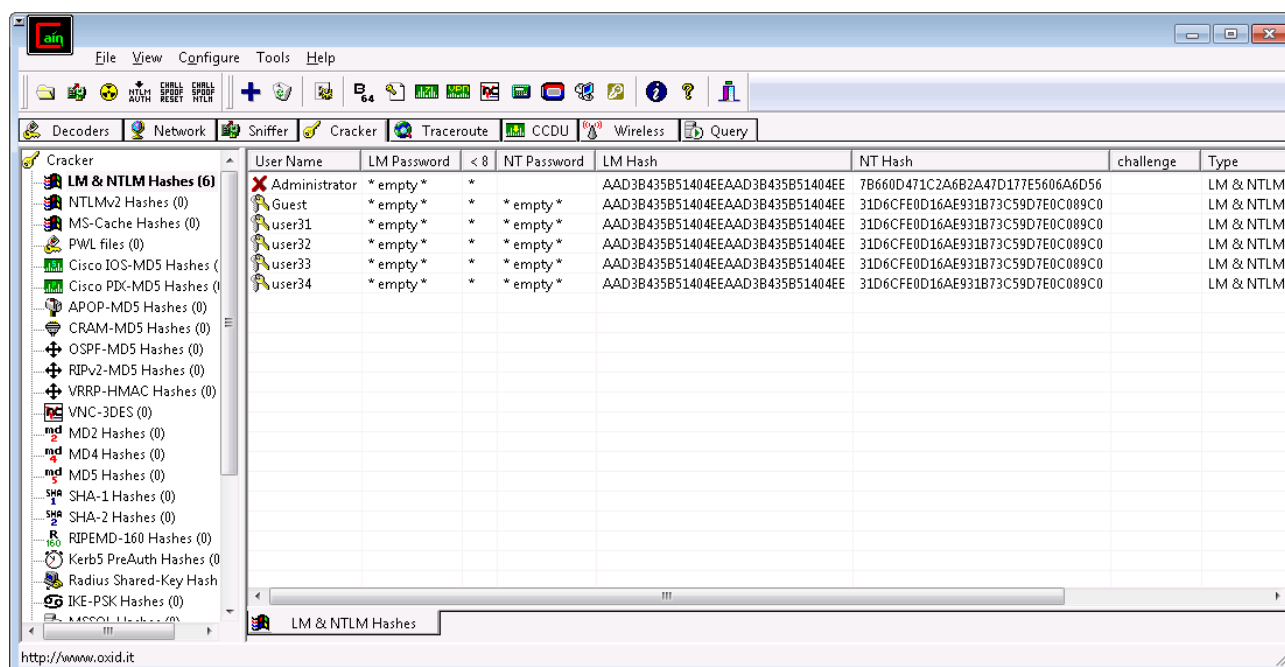
Cain

Εικόνα 3.4 Εικονίδιο εφαρμογής Cain&Abel

Εκτελέστε την εφαρμογή Cain & Abel, κάνοντας διπλό κλικ στο εικονίδιο αυτό. Αν εμφανιστεί προειδοποίηση για την ύπαρξη του Windows Firewall, πατήστε OK. Από τις καρτέλες (tabs) που εμφανίζονται στη διεπιφάνεια της εφαρμογής, επιλέξτε την καρτέλα Cracker.

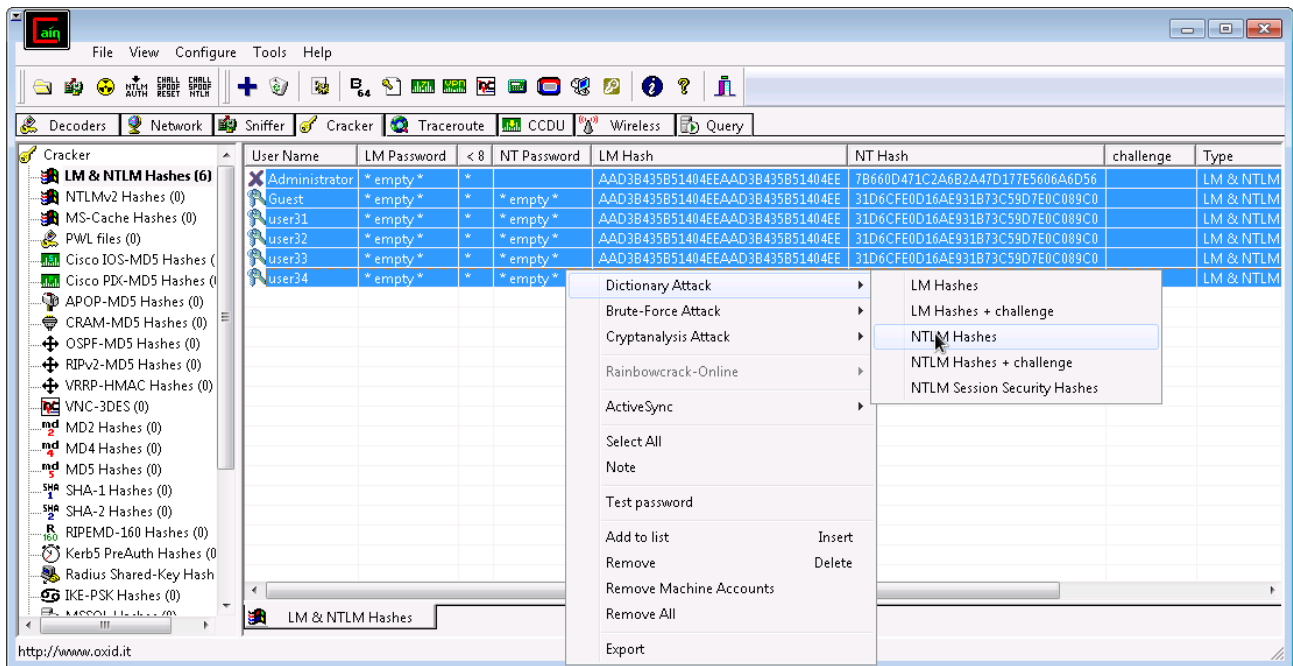
Στην ελεύθερη περιοχή, που βρίσκεται στο δεξί μέρος, κάντε δεξί κλικ και επιλέξτε Add to List ή πατήστε το πλήκτρο Insert.

Στο νέο παράθυρο που θα εμφανιστεί, επιλέξτε “Import Hashes From Local System” και πατήστε Next. Ως αποτέλεσμα, θα εμφανιστούν όλοι οι λογαριασμοί χρηστών του συστήματος, ενώ στις στήλες LM Hash και NT Hash εμφανίζονται οι συνόψεις (hash) των λογαριασμών χρηστών.



Εικόνα 3.5 Hash των λογαριασμών χρηστών

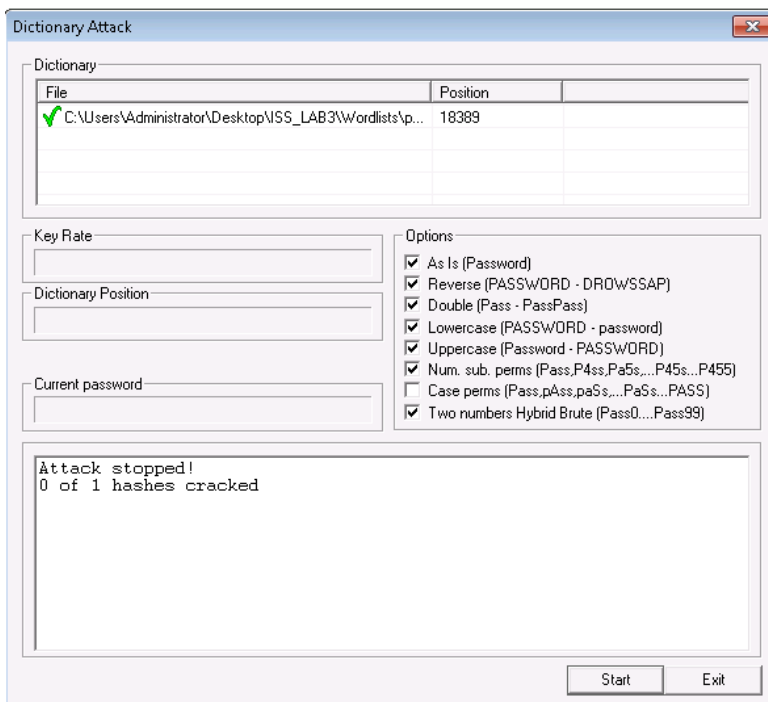
Στην περιοχή όπου εμφανίζονται οι πληροφορίες των λογαριασμών, κάντε δεξί κλικ και επιλέξτε Select All. Επάνω στις επιλεγμένες γραμμές, κάντε εκ νέου δεξί κλικ και επιλέξτε Dictionary Attack και κατόπιν επιλέξτε NTLM Hashes.



Εικόνα 3.6 Επιλογή επίθεσης Dictionary Attack

Στη συνέχεια, θα πρέπει να εισαχθούν τα αρχεία λεξικών που θα χρησιμοποιηθούν κατά την επίθεση. Στην ελεύθερη (κενή) περιοχή του πεδίου Dictionary, κάντε δεξί κλικ και επιλέξτε Add to list. Επιλέξτε το αρχείο passwords.txt που θα βρείτε στον κατάλογο ISS_Chapter3\Wordlist. Το αρχείο αυτό δημιουργήθηκε στις 2/12/1998 (άρα δεν είναι ιδιαίτερα πρόσφατο) για το Openwall Project και περιέχει μία ταξινομημένη λίστα με τα 2289 πιο συχνά χρησιμοποιούμενα συνθηματικά σε UNIX συστήματα, στα μέσα της δεκαετίας του 1990.

Στη συνέχεια, πατήστε Start.



Εικόνα 3.7 Αποτέλεσμα επίθεσης λεξικού

- Πόσα συνθηματικά ανακτήθηκαν;
- Θα μπορούσαμε να σκεφτούμε κάτι διαφορετικό ώστε να ανακτήσουμε περισσότερα συνθηματικά;
- Ποιες εναλλακτικές επιλογές παρατηρήσατε ότι παρέχονται στις επιλογές (Options) αναζήτησης;

Πατήστε δεξί κλικ στο αρχείο `passwords.txt` στη λίστα και επιλέξτε `Reset initial file position`, ώστε η αναζήτηση να ξεκινήσει από την αρχή. Απενεργοποιήστε όλες τις επιλογές (Options) αναζήτησης και ενεργοποιήστε μόνο την επιλογή `Case perms`. Πατήστε `Start` και παρατηρήστε την αναφορά με τα συνθηματικά που ανακτήθηκαν. Κατόπιν, πατήστε `Exit`.

Ανοίξτε το αρχείο `passwords.txt` με το `notepad++` (το πρόγραμμα βρίσκεται στα αρχεία που κατεβάσατε νωρίτερα) και αναζητήστε (`Ctrl+F`) τις λέξεις `Abc123` και `Hockey1`. Στη συνέχεια, αναζητήστε εκ νέου τις ίδιες λέξεις με επιλεγμένη την επιλογή `Match Case`.

- Τι παρατηρείτε κατά την επίθεση, σε σχέση και με τις επιλογές που κάνατε νωρίτερα;
- Πόσα συνθηματικά ανακτήθηκαν;
- Ποιοι παράγοντες επηρεάζουν κυρίως την επιτυχία μιας επίθεσης λεξικού;

3.4 Επίθεση Εξαντλητικής Αναζήτησης

Η δεύτερη επίθεση που θα μελετηθεί είναι και αυτή που εφαρμόζεται συχνότερα. Στην επίθεση εξαντλητικής αναζήτησης (`brute-force attack`), ο επίδοξος εισβολέας προσπαθεί να δοκιμάσει κάθε πιθανό συνθηματικό ως συνδυασμό αλφαριθμητικών χαρακτήρων. Η εξαντλητική αναζήτηση είναι ιδιαίτερα χρονοβόρα, αλλά αναμένεται να δώσει πάντα αποτέλεσμα, εφόσον για το αλφάβητο (`predefined charset`) επιλεγούν όλοι οι χαρακτήρες που υπάρχουν στο συνθηματικό. Όμως ο χρόνος που θα απαιτηθεί για να γίνει κάτι τέτοιο πιθανώς να είναι (όπως συμβαίνει συνήθως) απαγορευτικά μεγάλος.

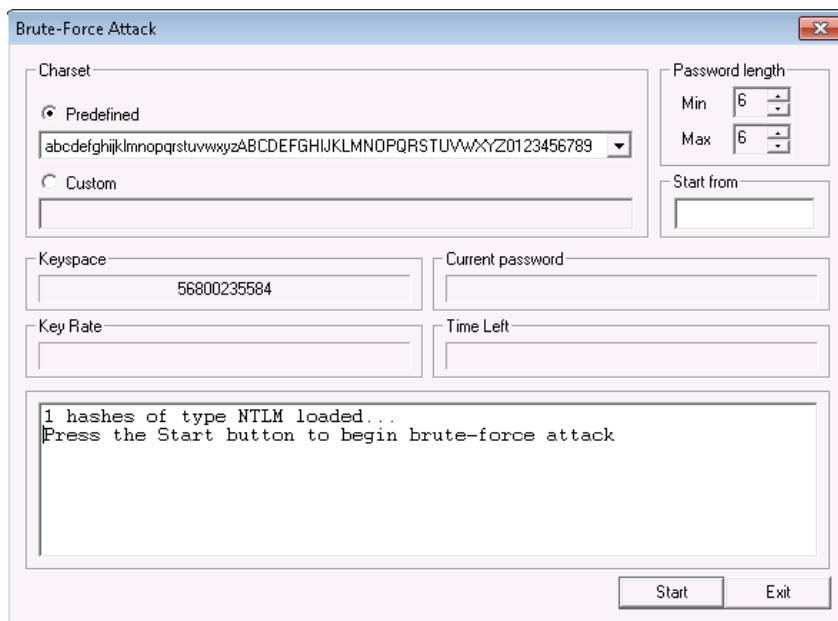
Στην ελεύθερη περιοχή, που βρίσκεται στο δεξί μέρος του παραθύρου `Cracker`, κάντε δεξί κλικ και επιλέξτε `Remove All` για να ‘καθαρίσετε’ τα αποτελέσματα της προηγούμενης αναζήτησης. Στη συνέχεια, στην ίδια περιοχή, κάντε δεξί κλικ και επιλέξτε `Add to List` ή πατήστε το πλήκτρο `Insert`.

Στο νέο παράθυρο, επιλέξτε `“Import Hashes From Local System”` και πατήστε `Next`. Ως αποτέλεσμα, θα εμφανιστούν όλοι οι λογαριασμοί χρηστών του συστήματος. Κάντε δεξί κλικ στο λογαριασμό χρήστη `user32`, ενώ στη συνέχεια επιλέξτε `brute force attack` και κατόπιν επιλέξτε `NTLM hashes`.

Στο παράθυρο που εμφανίζεται, μπορείτε να μεταβάλλετε τα προεπιλεγμένα σύνολα χαρακτήρων, καθώς και το ελάχιστο και το μέγιστο μήκος συνθηματικού. Ως αποτέλεσμα αυτών των αλλαγών, μπορείτε να παρατηρήσετε τις μεταβολές που προκαλούνται στο χώρο αναζήτησης (`keyspace`).

Ας υποθέσουμε το σενάριο ότι ο επιτιθέμενος, καθώς βρίσκεται πίσω από τον χρήστη που κατέχει τον λογαριασμό χρήστη με όνομα `user32`, κατάφερε να διαπιστώσει κατά την πληκτρολόγηση ότι το μήκος του συνθηματικού του ήταν 6 χαρακτήρες, γράμματα και αριθμοί χωρίς σημεία στίξης ή άλλα σύμβολα. Δυστυχώς, δεν μπορεί να είναι σίγουρος αν τα γράμματα ήταν πεζά ή κεφαλαία, ούτε ακριβώς ποια νούμερα πληκτρολόγησε ο χρήστης. Ως αποτέλεσμα, οι παραπάνω πληροφορίες τον οδηγούν στην απόφαση να κάνει τις ακόλουθες επιλογές:

- `predefined charset: abcdef....xyzABC....XYZ0123456789`
- μήκος: από 6 ως 6 χαρακτήρες



Εικόνα 3.8 Προετοιμασία επίθεσης Brute-Force

Επιλέξτε Start και παρατηρήστε πως, ακόμη και για το απλό συνθηματικό Abc123, απαιτείται αρκετός χρόνος, παρότι δοκιμάζονται αρκετά μεγάλος αριθμός συνθηματικών ανά δευτερόλεπτο (πόσα;). Διακόψτε την αναζήτηση (Stop) και αφού ‘καθαρίσετε’ το περιεχόμενο του πεδίου Start from, εισάγετε το Custom charset: abcdABCD1234 και πατήστε Start.

- Εντοπίστηκε το συνθηματικό;
- Παρατηρήσατε ότι η μείωση του χώρου αναζήτησης έφερε και μείωση στο χρόνο;

Επιλέξτε Stop και Exit. Επιλέξτε το λογαριασμό χρήστη user34 και δοκιμάστε να εφαρμόσετε μια νέα επίθεση Brute-Force με την τελευταία επιλογή από τη λίστα των Predefined Charset (όπου εμφανίζονται όλοι οι πιθανοί χαρακτήρες), για συνθηματικά με μήκος από 1 ως 16 χαρακτήρες (λογικό σενάριο για πραγματικές συνθήκες).

- Ποια η γνώμη σας για μια τέτοια επίθεση;
- Πώς και υπό ποιες προϋποθέσεις θα ήταν αποτελεσματική;

3.5 Επίθεση με Πίνακες Ουράνιου Τόξου

Οι πίνακες ουράνιου τόξου (rainbow tables) λειτουργούν αποθηκεύοντας «αλυσίδες» (chains) από προϋπολογισμένες συνόψεις (hashes), όπου για τη n -οστή συνόψιση ισχύει:

$$h_n = H(R_n(h_{n-1}))$$

όπου:

- h_n είναι το αποτέλεσμα της εφαρμογής για το βήμα n της συνάρτησης κατακερματισμού H πάνω σε ένα πιθανό συνθηματικό,
- R_n είναι το αποτέλεσμα της εφαρμογής για το βήμα n της συνάρτησης απομείωσης (reduction function) που θα μετατρέψει τη συνόψιση του προηγούμενου βήματος σε ένα πιθανό συνθηματικό.

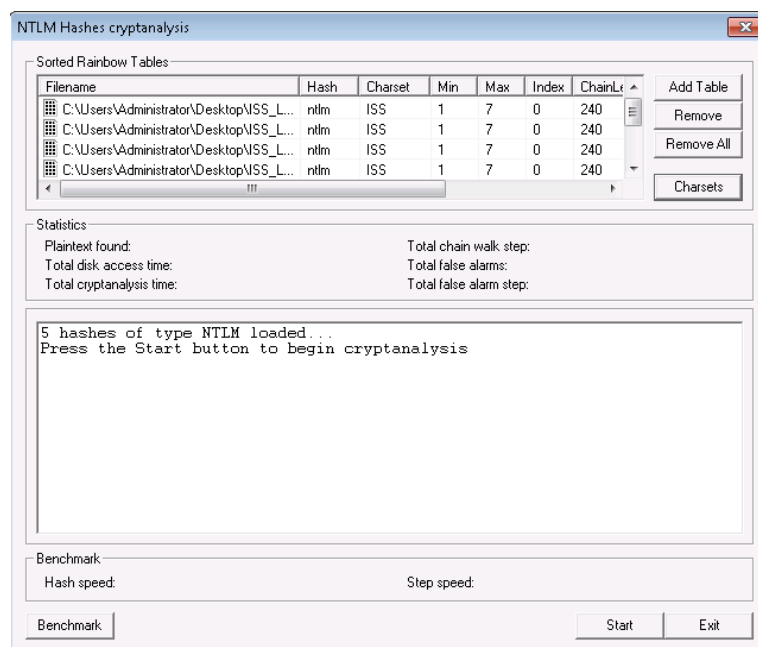
Οι επιθέσεις με χρήση rainbow tables είναι πολύ γρήγορες κατά την εκδήλωσή τους, αλλά προϋποθέτουν τη διαθεσιμότητα κατάλληλα προϋπολογισμένων πινάκων, οι οποίοι είναι ιδιαίτερα χρονοβόροι στην κατασκευή τους, όπως θα φανεί στη συνέχεια.

Στην ελεύθερη περιοχή που βρίσκεται στο δεξί μέρος του παραθύρου Cracker, κάντε δεξί κλικ και επιλέξτε Remove All για να ‘καθαρίσετε’ τα αποτελέσματα της προηγούμενης αναζήτησης. Στη συνέχεια, στην ίδια περιοχή, κάντε δεξί κλικ και επιλέξτε Add to List ή πατήστε το πλήκτρο Insert.

Στο νέο παράθυρο, επιλέξτε “Import Hashes From Local System” και πατήστε Next. Θα πρέπει να εμφανιστούν όλοι οι λογαριασμοί χρηστών του συστήματος. Κάντε δεξί κλικ και επιλέξτε Select All. Πάνω στους επιλεγμένους λογαριασμούς χρηστών, κάντε δεξί κλικ και επιλέξτε Cryptanalysis Attack. Κατόπιν, επιλέξτε NTLM Hashes και μετά επιλέξτε via Rainbow Tables (RainbowCrack).

Στο παράθυρο που θα εμφανιστεί, πατήστε το πλήκτρο Charsets και, στη συνέχεια, επιλέξτε και ανοίξτε το αρχείο charset.txt από τον κατάλογο ISS_Chapter3\Rainbow_Tables. Στη συνέχεια, επιλέξτε Add Table και προσθέστε τα έξι (6) .rt αρχεία του καταλόγου ISS_Chapter3\Rainbow_Tables:

```
ntlm_ISS#1-7_0_240x400000_oxid#00[0-5].rt
```



Εικόνα 3.9 Ετοιμασία επίθεσης με rainbow tables

Σημειώνεται πως οι πίνακες έχουν δημιουργηθεί για NTLM hashes και μήκος plain text από 1 ως 7 χαρακτήρες.

- Με βάση αυτή την παραδοχή, ποια συνθηματικά αναμένετε να ανακτηθούν;
- Εάν γνωρίζατε πως το charset είναι ABCMabcedesp1234, τότε σε ποια συνθηματικά θα περιορίζατε την εκτίμησή σας;

Πατήστε το κουμπί Start και μόλις ολοκληρωθεί η διαδικασία πατήστε το κουμπί Exit.

- Ποια συνθηματικά ανακτήθηκαν;

3.6 Δημιουργία των Rainbow Tables

Είναι χρήσιμο να ασχοληθούμε με τη δημιουργία των rainbow tables, που χρησιμοποιήθηκαν στην προηγούμενη επίθεση.

Στον κατάλογο εγκατάστασης του Cain & Abel, υπάρχει ο κατάλογος Winrtgen (C:\Program Files (x86)\Cain\Winrtgen). Μεταβείτε στον κατάλογο αυτό και εντοπίστε τα αρχεία winrtgen.exe και charsets.txt. Ανοίξτε με το notepad++ και μελετήστε το περιεχόμενο του αρχείου charsets.txt. Το αρχείο αυτό περιέχει τα πιθανά σύνολα χαρακτήρων που μπορούμε να χρησιμοποιήσουμε για τη δημιουργία των πινάκων. Φυσικά, μπορούμε να προσθέσουμε και τα δικά μας σύνολα χαρακτήρων.

Εκτελέστε το winrtgen.exe και πατήστε Add Table.

Εικόνα 3.10 Δημιουργία πινάκων rainbow

Παρατηρήστε τις παραμέτρους:

- **Hash:** Οι τύποι συνόψεων για τις οποίες θα δημιουργηθούν οι πίνακες.
- **Min Len:** Το ελάχιστο μήκος των συνθηματικών.
- **Max Len:** Το μέγιστο μήκος των συνθηματικών.
- **Index:** Το διακριτικό του πίνακα. Μπορούμε να έχουμε πολλαπλά αρχεία για έναν πίνακα.
- **Chain Len:** Το μήκος της αλυσίδας που προκύπτει από τις συναρτήσεις hashing και reduction και αφορά το πλήθος των συνόψεων που αναπαριστώνται στην αλυσίδα, παρόλο ότι αποθηκεύονται μόνον η αρχική και η τελική συνόψιση.
- **Chain Count:** Το πλήθος των αλυσίδων σε κάθε αρχείο.
- **No of tables:** Ο αριθμός των αρχείων (μεγέθους μέχρι 2GB) που θα παραχθούν για το τρέχον table index.
- **Charset:** Το σύνολο χαρακτήρων που θα χρησιμοποιηθούν με τυχαία επιλογή για την παραγωγή του χώρου ορισμού των συνθηματικών (key space).

Μεταβάλλοντας τις τιμές παραμέτρων, παρατηρήστε πως αλλάζουν το key space, το μέγεθος του χώρου στο δίσκο, αλλά και η πιθανότητα επιτυχίας!

Δημιουργήστε τους δικούς σας πίνακες rainbow, επιλέγοντας ως charset το numeric και δίνοντας τις ακόλουθες τιμές στις παραμέτρους:

- Hash: ntlm
- Min Len: 1
- Max Len: 8
- Index: 0
- Chain Len: 240
- Chain Count: 1000000
- No of tables: 1

Πατήστε OK και παρατηρείστε το αρχείο που δημιουργήθηκε. Σε ποια περίπτωση θα μπορούσε να χρησιμοποιηθεί;

Βιβλιογραφία

Bosworth, S., Kabay, M. E., & Whyne, E. (2014). Computer Security Handbook, Set. John Wiley & Sons.

Marechal, S. (2008). Advances in password cracking. Journal in Computer Virology, 4(1), 73–81.
<http://doi.org/10.1007/s11416-007-0064-y>

Κριτήρια αξιολόγησης

Ερωτήσεις κατανόησης

Απαντήστε στις ακόλουθες ερωτήσεις. Κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Στο σύστημα που μελετήσατε, για κάθε λογαριασμό χρήστη αποθηκεύεται:

- α) Το κρυπτογραφημένο συνθηματικό
- β) Τα κωδικοποιημένο συνθηματικό
- γ) Η συνόψιση του συνθηματικού
- δ) Το κλειδί κρυπτογράφησης του συνθηματικού

2. Ένα NTLM hash έχει υπολογιστεί με τη χρήση της συνάρτησης κατακερματισμού:

- α) MD4
- β) MD5
- γ) SHA1
- δ) SHA256

3. Για να επιτύχει μια επίθεση λεξικού πρέπει:

- α) Οι χρήστες να χρησιμοποιούν παλιά συνθηματικά
- β) Να έχουμε κατάλληλα λεξικά πιθανών συνθηματικών
- γ) Τα συνθηματικά να αποθηκεύονται ως ανοιχτό κείμενο (clear text)
- δ) Τα συνθηματικά να είναι ως 7 χαρακτήρες

4. Από τα αποτελέσματα της επίθεσης λεξικού σε λειτουργικό σύστημα Windows, παρατηρήσαμε ότι:

- α) Τα συνθηματικά είναι case sensitive
- β) Τα συνθηματικά είναι case insensitive
- γ) Το λεξικό θα πρέπει περιέχει τα NTLM hashes

δ) Το λεξικό θα πρέπει να περιέχει τα συνθηματικά

5. Μια brute-force attack:

- α) Είναι συνήθως γρήγορη
- β) Είναι συνήθως χρονοβόρα
- γ) Απαιτεί τη γνώση κάποιων ιδιοτήτων του αναζητούμενου συνθηματικού
- δ) Πετυχαίνει μόνο σε περιπτώσεις με απλά συνθηματικά

6. Για να πετύχει μια brute-force attack πρέπει:

- α) Τα συνθηματικά να είναι case insensitive
- β) Τα συνθηματικά να είναι απλοϊκά
- γ) Ο έλεγχος να γίνεται για περιορισμένο χρόνο
- δ) Να επιλεγεί σωστά το σύνολο χαρακτήρων (charset)

7. Για τους πίνακες rainbow ισχύει ότι:

- α) Η δημιουργία τους είναι συνήθως γρήγορη και η χρήση τους χρονοβόρα
- β) Η δημιουργία τους είναι συνήθως χρονοβόρα και η χρήση τους γρήγορη
- γ) Η δημιουργία και η χρήση τους είναι εξίσου γρήγορες
- δ) Η δημιουργία και η χρήση τους είναι συνήθως εξίσου χρονοβόρες

8. Ποιο είναι το πλεονέκτημα μιας επίθεσης με πίνακες rainbow έναντι μιας επίθεσης brute-force:

- α) Η μεγάλη ταχύτητα αναζήτησης
- β) Ο μεγάλος χώρος αποθήκευσης
- γ) Το ποσοστό επιτυχίας
- δ) Το μέγεθος των αρχείων

9. Για την ταχύτερη ανακάλυψη ενός συνθηματικού με πολλούς χαρακτήρες που ακολουθεί σύνθετους κανόνες πολυπλοκότητας θα επιλέγατε:

- α) Dictionary Attack
- β) Brute-Force Attack
- γ) Rainbow Tables Attack
- δ) Οποιαδήποτε από τις παραπάνω

10. Ποια από τα παρακάτω ισχύουν:

- α) Η επιλογή του χώρου αναζήτησης (key space) είναι σημαντική για την επιτυχία της επίθεσης
- β) Η brute-force attack, χωρίς περιορισμό χρόνου, είναι σίγουρο ότι θα επιτύχει.
- γ) Το μέγεθος ενός rainbow table εξαρτάται μόνο από το μήκος της αλυσίδας
- δ) Η επιτυχία μιας επίθεσης με rainbow tables δεν εξαρτάται από το πώς δημιουργήθηκαν οι πίνακες
- ε) Σε ένα συνθηματικό είναι πιο σημαντικό το μήκος του παρά το σύνολο χαρακτήρων (charset) που χρησιμοποιήθηκε
- στ) Για την αποκάλυψη ενός συνθηματικού, η γνώση του μήκους του είναι χρήσιμη
- ζ) Ένα ισχυρό συνθηματικό πρέπει να χρησιμοποιεί ευρύ σύνολο χαρακτήρων (charset)

Συγκριτική αξιολόγηση

Συγκρίνετε τις τρεις επιθέσεις που παρουσιάστηκαν στο κεφάλαιο (Dictionary attack, Brute-Force attack, Rainbow Tables) ως προς το χρόνο και το χώρο που απαιτείται για την προετοιμασία και εφαρμογή τους, αλλά και ως προς την αποτελεσματικότητά τους και εξηγήστε σε ποια περίπτωση θα επιλέγατε κάθε μία από αυτές.