



Πανεπιστήμιο Αιγαίου

**Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών
Συστημάτων**

321-3404 Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Διδάσκων: Καρύδα Μαρία , Καμπουράκης Γεώργιος

Μελέτη βασικών μηχανισμών ασφάλειας των λειτουργικών συστημάτων Windows Server & Linux

Εργαστηριακοί Συνεργάτες : Νίκος Αλεξίου & Αλέξανδρος Φακής

Μέλη Ομάδας

Αντωνιάδης Χαράλαμπος icsd10011

Ευκαρπίδης Κωνσταντίνος icsd15051

Ζιώζας Γεώργιος icsd15058

Σάμος, 18/3, 2018



Περιεχόμενα

1	ΕΙΣΑΓΩΓΗ.....	3
2	ΜΕΡΟΣ 1^ο - ΔΙΑΧΕΙΡΙΣΗ ΧΡΗΣΤΩΝ ΚΑΙ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ.....	4
2.1	ΔΗΜΙΟΥΡΓΙΑ ΧΡΗΣΤΩΝ, ΟΜΑΔΩΝ ΚΑΙ ΣΥΝΘΗΜΑΤΙΚΩΝ	4
2.2	ΚΑΘΟΡΙΣΜΟΣ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ.....	7
2.3	ΈΛΕΓΧΟΣ ΕΝΕΡΓΟΠΟΙΗΣΗΣ ΚΑΘΟΡΙΣΜΕΝΩΝ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ.....	9
2.4	ΕΡΩΤΗΜΑΤΑ 1 ^{ΟΥ} ΜΕΡΟΥΣ	11
3	ΜΕΡΟΣ 2^ο - ΔΙΑΧΕΙΡΙΣΗ ΣΥΝΘΗΜΑΤΙΚΩΝ & ΜΕΛΕΤΗ ΕΠΙΘΕΣΕΩΝ.....	13
3.1	ΈΛΕΓΧΟΣ ΔΥΝΑΜΙΚΟΤΗΤΑΣ ΣΥΝΘΗΜΑΤΙΚΩΝ	13
3.2	ΦΥΛΑΞΗ ΛΟΓΑΡΙΑΣΜΩΝ & ΣΥΝΘΗΜΑΤΙΚΩΝ.....	15
3.3	ΕΠΙΘΕΣΕΙΣ ΜΕ ΧΡΗΣΗ PASSWORD CRACKER	16
3.4	ΕΡΩΤΗΜΑΤΑ 2 ^{ΟΥ} ΜΕΡΟΥΣ.....	22
4	ΜΕΡΟΣ 3^ο - ΈΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ ΠΟΡΩΝ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ	23
4.1	ΔΗΜΙΟΥΡΓΙΑ ΟΜΑΔΩΝ & ΠΡΟΣΩΠΙΚΟΥ ΧΩΡΟΥ.....	23
4.2	ΚΑΘΟΡΙΣΜΟΣ ΕΠΙΠΕΔΩΝ ΠΡΟΣΒΑΣΗΣ.....	27
4.3	ΕΡΩΤΗΜΑΤΑ 3 ^{ΟΥ} ΜΕΡΟΥΣ	27
5	ΜΕΡΟΣ 4^ο - ΚΑΤΑΓΡΑΦΗ & ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΕΝΕΡΓΕΙΩΝ ΧΡΗΣΤΗ	32
5.1	ΜΗΧΑΝΙΣΜΟΙ ΚΑΤΑΓΡΑΦΗΣ ΣΥΜΒΑΝΤΩΝ	32
5.2	ΧΡΗΣΗ SYSLOG DAEMON & ΈΛΕΓΧΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΜΕ ΠΑΡΑΔΕΙΓΜΑ	34
5.3	ΕΝΕΡΓΟΙ ΧΡΗΣΤΕΣ & ΠΡΟΣΠΑΘΕΙΑ ΕΙΣΒΟΛΗΣ ΩΣ ROOT	34
6	ΜΕΡΟΣ 5^ο - ΣΥΓΚΡΙΣΗ ΤΩΝ ΔΥΟ ΛΕΙΤΟΥΡΓΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ	35
6.1	ΠΟΣΟ ΔΙΑΦΟΡΕΤΙΚΟΙ ΘΕΩΡΕΙΤΕ ΌΤΙ ΕΙΝΑΙ ΟΙ ΜΗΧΑΝΙΣΜΟΙ ΚΑΙ ΤΟ ΕΠΙΠΕΔΟ ΑΣΦΑΛΕΙΑΣ ΠΟΥ ΠΑΡΕΧΟΝΤΑΙ ΣΕ ΈΝΑ LINUX ΣΥΣΤΗΜΑ ΣΕ ΣΧΕΣΗ ΜΕ ΈΝΑ Λ.Σ. WINDOWS; ΣΦΑΛΜΑ! ΔΕΝ ΕΧΕΙ ΟΡΙΣΤΕΙ ΣΕΛΙΔΟΔΕΙΚΤΗΣ.	
6.2	ΠΟΣΟ ΔΙΑΦΟΡΕΤΙΚΗ ΕΙΝΑΙ Η ΔΙΑΧΕΙΡΙΣΗ ΤΩΝ ΜΗΧΑΝΙΣΜΩΝ ΑΥΤΩΝ ΣΤΑ WINDOWS, ΣΕ ΣΥΓΚΡΙΣΗ ΜΕ ΤΗ ΔΙΑΧΕΙΡΙΣΗ ΣΕ LINUX ΣΥΣΤΗΜΑ; ΣΦΑΛΜΑ! ΔΕΝ ΕΧΕΙ ΟΡΙΣΤΕΙ ΣΕΛΙΔΟΔΕΙΚΤΗΣ.	
6.3	ΠΟΙΟ ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΘΑ ΛΕΓΑΤΕ ΌΤΙ ΕΙΝΑΙ ΕΥΚΟΛΟΤΕΡΟ ΓΙΑ ΈΝΑΝ ΔΙΑΧΕΙΡΙΣΤΗ; ΠΟΙΟ ΘΕΩΡΕΙΤΑΙ ΌΤΙ ΕΙΝΑΙ ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΕΡΟ ΓΙΑ ΤΑ ΣΕΝΑΡΙΑ ΠΟΥ ΜΕΛΕΤΗΣΑΤΕ; ΣΦΑΛΜΑ! ΔΕΝ ΕΧΕΙ ΟΡΙΣΤΕΙ ΣΕΛΙΔΟΔΕΙΚΤΗΣ.	
7	ΒΙΒΛΙΟΓΡΑΦΙΑ.....	38



321-3404 Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: Μελέτη βασικών μηχανισμών ασφάλειας των λειτουργικών συστημάτων Windows Server & Linux

Αντωνιάδης Χαράλαμπος icsd10011 , Ευκαρπίδης Κωνσταντίνος icsd15051 , Ζιώζας Γεώργιος icsd15058



1 Εισαγωγή

Κατά την παρουσίαση της 1^{ης} εργαστηριακής άσκησης , σε πρώτο στάδιο συζητήθηκε η μορφή του εργαστηρίου. Σε δεύτερη φάση, τέθηκε ο στόχος της άσκησης, ο οποίος είναι να εξερευνήσουμε τους μηχανισμούς που μας παρέχουν τα λειτουργικά συστήματα Linux & Windows Server. Οι μηχανισμοί αυτοί , όπου αποτελούν σε συνδυασμό με μία πληθώρα ερωτημάτων τα μέρη της εργασίας , αφορούν την διαχείριση των χρηστών και την αυθεντικοποίηση τους , την διαχείριση των συνθηματικών και δυνατοί τρόποι επίθεσης αυτών, τους μηχανισμούς ελέγχου πρόσβασης και τέλος την καταγραφή αρχείων για κινήσεις του χρήστη. Στο τέλος της αναφοράς ακολουθεί και μία μικρή σύγκριση μεταξύ των δύο λειτουργικών συστημάτων. Η εγκατάσταση των λειτουργικών έγινε στο εικονικό περιβάλλον της Oracle (Oracle VM VirtualBox).

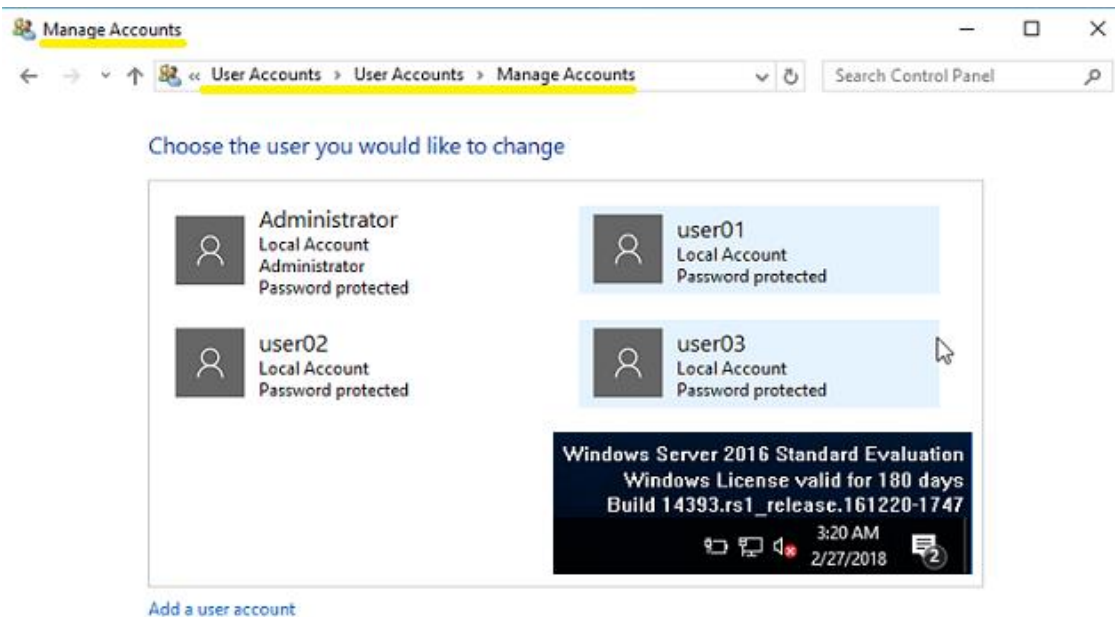


2 Μέρος 1^ο - Διαχείριση Χρηστών και Αυθεντικοποίηση

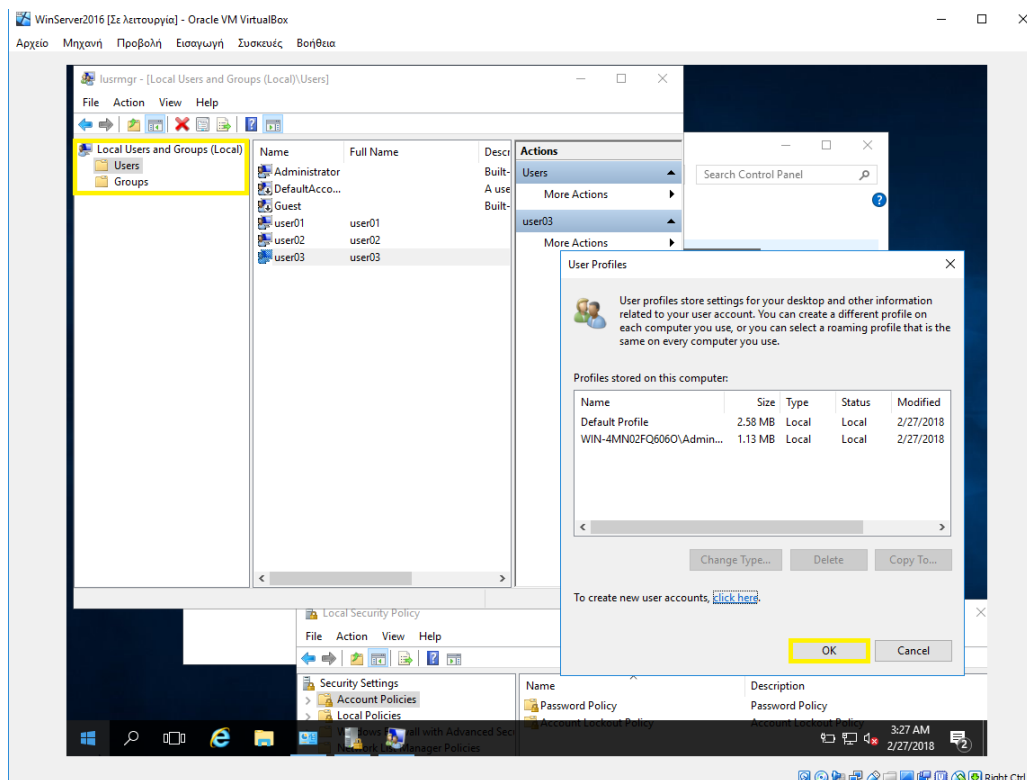
Στο πρώτο μέρος της εργασίας ασχολούμαστε με την διαχείριση των χρηστών και με ποιους μηχανισμούς αυθεντικοποιούνται. Συγκεκριμένα καλούμαστε να δημιουργήσουμε τέσσερις χρήστες από τους οποίους οι τρεις θα είναι απλοί users και ο ένας διαχειριστής. Η πολυπλοκότητα των κωδικών των χρηστών πρέπει να διαφέρει. Ακολούθως μελετάμε τις πολιτικές ασφαλείας και καθορίζουμε τις πιο βασικές από αυτές. Εν συνεχεία ελέγχουμε την εγκυρότητα τους και απαντάμε στα δοθέντα ερωτήματα.

2.1 Δημιουργία χρηστών, ομάδων και συνθηματικών

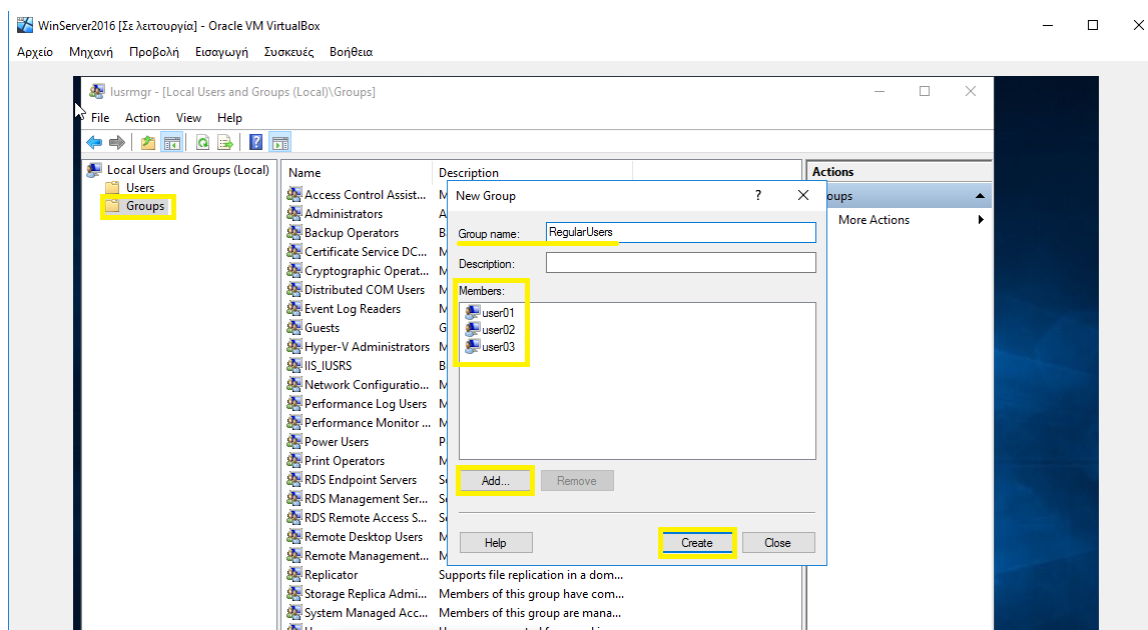
- Για την δημιουργία χρηστών στον περιβάλλον «Windows» ακολουθούμε το μονοπάτι που φαίνεται στο στιγμιότυπο (Εικόνα 2.1.1) και έπειτα δημιουργούμε όσους χρήστες χρειαζόμαστε. Έπειτα ανοίγουμε το «Computer Management», είτε από την αναζήτηση είτε από την έναρξη, και μετά επιλέγουμε «Local Users and Groups». Επιλέγουμε groups και δημιουργούμε καινούριο όπου θα προσθέσουμε και τους 3 απλούς χρήστες μας.
- Αντίστοιχα, από την πλευρά του Ubuntu επιλέξαμε να ακολουθήσουμε την τακτική «terminal». Για την δημιουργία χρήστη τρέχουμε «`sudo adduser user_name`» και στην συνέχεια πληκτρολογούμε έναν κωδικό πρόσβασης και προαιρετικά λοιπά στοιχεία του χρήστη. Η διαδικασία αυτή διαφέρει ελάχιστα σε περίπτωση που θέλουμε να φτιάξουμε έναν διαχειριστή. Πάλι όπως και πριν δημιουργούμε έναν χρήστη απλά μετέπειτα πρέπει να των προσθέσουμε στο «`sudo group`» όπου παίρνει αυτόματα τα ανάλογα δικαιώματα.



Εικόνα 2.1.1 : Δημιουργία users (Windows Server)



Εικόνα 2.1.2 : Επιβεβαίωση δημιουργίας χρήστη



Εικόνα 2.1.3 : Δημιουργία group & προσθήκη users



```
Terminal
myadmintest@myadmin-VirtualBox: /home/myadmin
myadmintest@myadmin-VirtualBox:~$ adduser user01
adduser: Only root may add a user or group to the system.
myadmintest@myadmin-VirtualBox:~$ sudo adduser user01
Adding user 'user01' ...
Adding new group 'user01' (1001) ...
Adding new user 'user01' (1001) with group 'user01' ...
The home directory '/home/user01' already exists. Not copying from '/etc/skel'.
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for user01
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] Y
myadmintest@myadmin-VirtualBox:~$
```

Εικόνα 2.1.4 : Δημιουργία users (Ubuntu)

```
Terminal
myadmin@myadmin-VirtualBox: ~
myadmin@myadmin-VirtualBox:~$ groupadd -g 3 RegularUsers
groupadd: GID '3' already exists
myadmin@myadmin-VirtualBox:~$ groupadd -g 666 RegularUsers
groupadd: Permission denied.
groupadd: cannot lock /etc/group; try again later.
myadmin@myadmin-VirtualBox:~$ sudo groupadd -g 666 RegularUsers
myadmin@myadmin-VirtualBox:~$
```

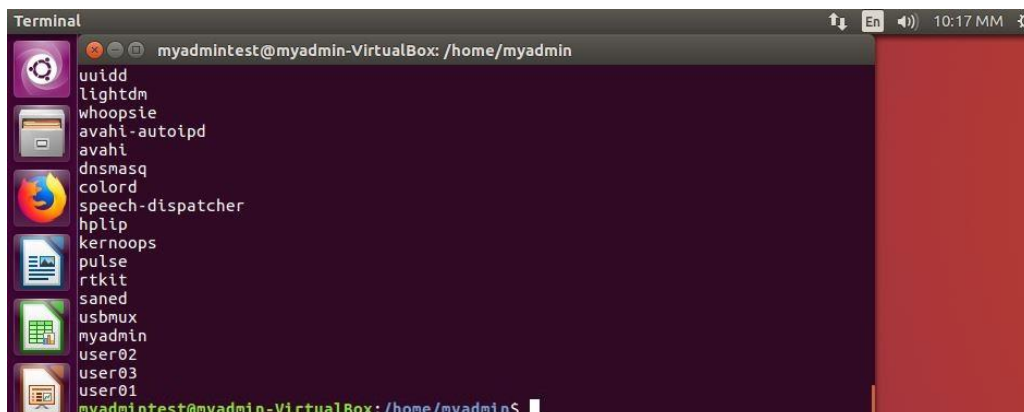
Εικόνα 2.1.5 : Δημιουργία Group

```
Terminal
myadmintest@myadmin-VirtualBox: /home
myadmintest@myadmin-VirtualBox:~$ sudo usermod -a -G NewRegularUsers user10
myadmintest@myadmin-VirtualBox:~$ sudo usermod -a -G NewRegularUsers user11
myadmintest@myadmin-VirtualBox:~$ sudo usermod -a -G RegularUsers user01
myadmintest@myadmin-VirtualBox:~$ sudo usermod -a -G RegularUsers user02
myadmintest@myadmin-VirtualBox:~$ sudo usermod -a -G RegularUsers user03
```

Εικόνα 2.1.6 : Προσθήκη users στα ζητούμενα groups

```
Terminal
myadmin@myadmin-VirtualBox: ~
option to relax this check or reconfigure NAME_REGEX.
myadmin@myadmin-VirtualBox:~$ sudo adduser myadmintest
Adding user 'myadmintest' ...
Adding new group 'myadmintest' (1004) ...
Adding new user 'myadmintest' (1004) with group 'myadmintest' ...
Creating home directory '/home/myadmintest' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for myadmintest
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] Y
myadmin@myadmin-VirtualBox:~$ sudo usermod -aG sudo myadmintest
myadmin@myadmin-VirtualBox:~$
```

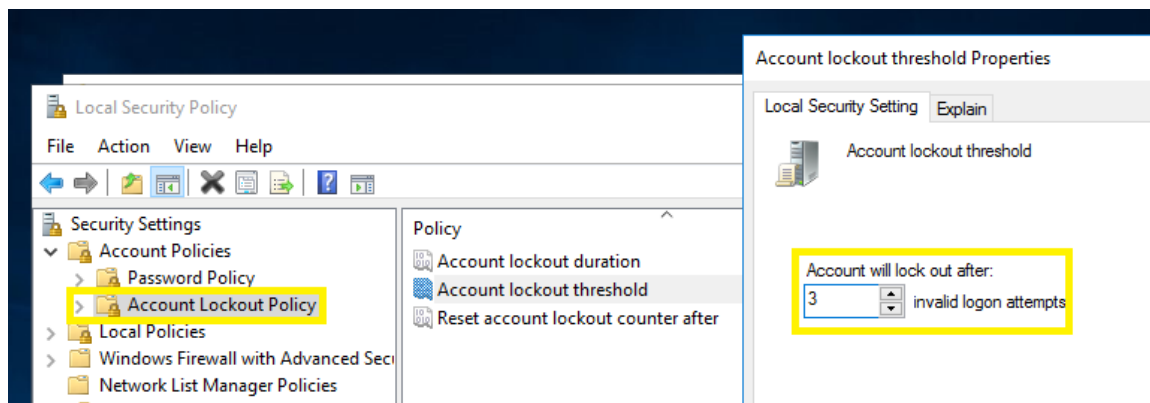
Εικόνα 2.1.7 : Καταχώρηση ενός χρήστη ως administrator



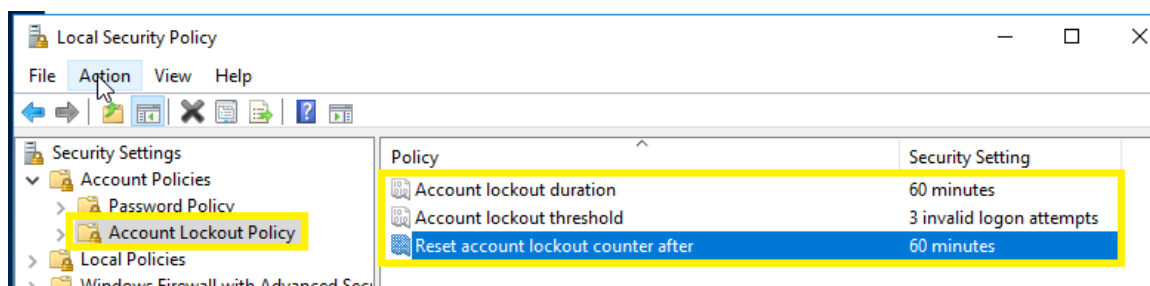
Εικόνα 2.1.8 : Επιβεβαίωση δημιουργίας χρηστών

2.2 Καθορισμός πολιτικών ασφαλείας

Στο σύστημα των Windows οι πολιτικές ασφαλείας καθορίζονται από την ενότητα «Local Security Policy». Στο «Account Policies», το οποίο μας απασχολεί, περιέχει και πολιτικές κωδικών αλλά και λογαριασμών. Όμοια και στα Ubuntu οι οριοθετήσεις αυτές γίνονται μέσα από δύο ξεχωριστά αρχεία με όνομα “common-auth” & “common-password”. Για το άνοιγμα αυτών των αρχείων χρησιμοποίησαν τον editor gedit. Οι επιλογές των παραμέτρων που ορίσαμε φαίνονται παρακάτω στα στιγμιότυπα.



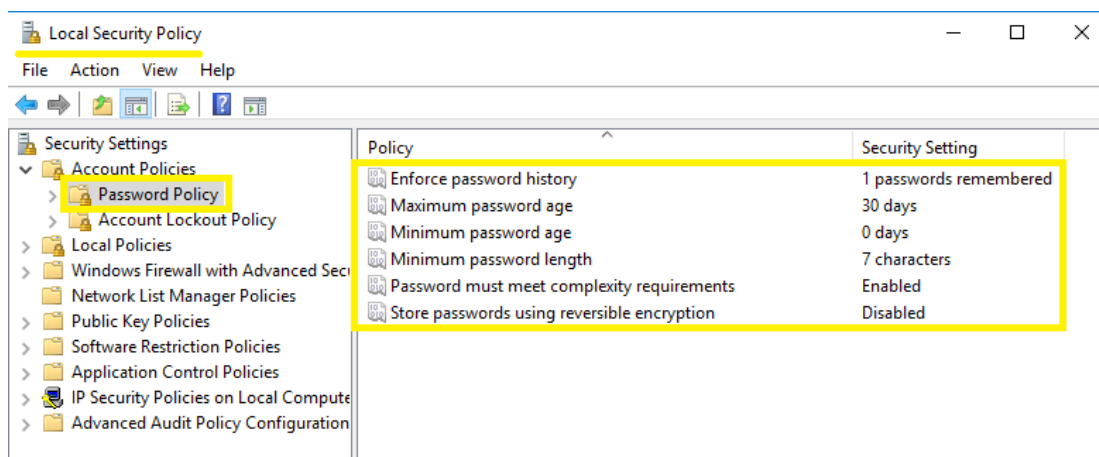
Εικόνα 2.2.1 : Καθορισμός αριθμού αποτυχημένων προσπαθειών



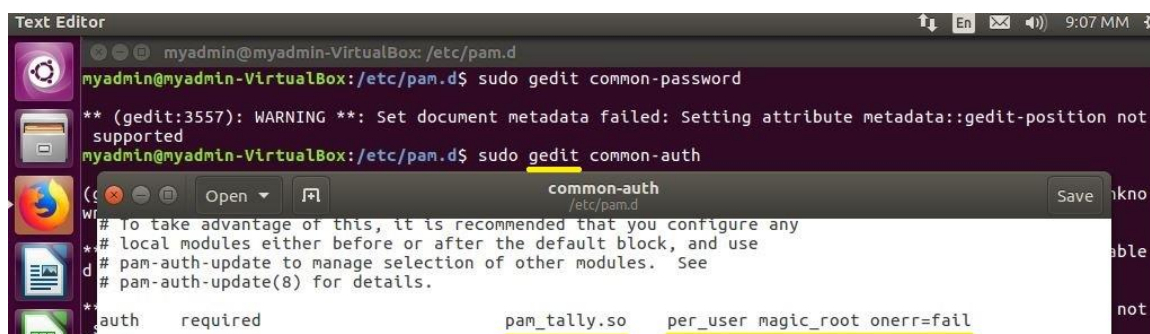
Εικόνα 2.2.2 : Καθορισμός όλων των δυνατών πολιτικών



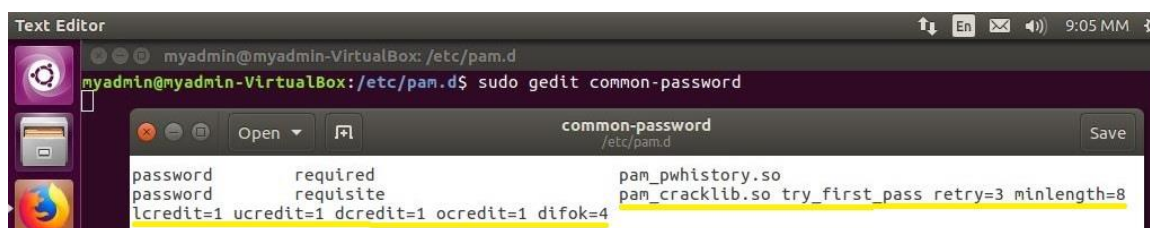
Στο σημείο αυτό θα παρατηρήσουμε μια διαφορά μεταξύ Windows Server και Linux. Στα windows ενεργοποιείς το complexity και έχει από default ρυθμίσεις σε αντίθεση με τα Ubuntu όπου εσύ ρυθμίζεις στην ουσία το πόσο περίπλοκος θες να είναι για όλους τους χρήστες.



Εικόνα 2.2.3 : Καθορισμός πολιτικών ασφαλείας κωδικών



Εικόνα 2.2.4 : Παραμετροποίηση αρχείου common-auth

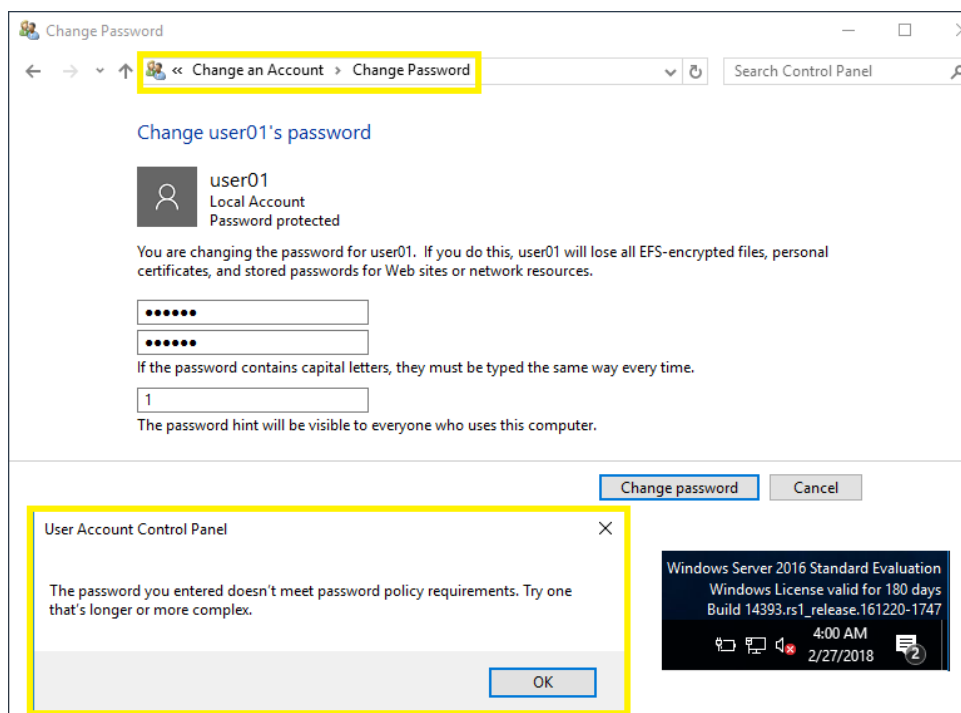


Εικόνα 2.2.5 : Παραμετροποίηση αρχείου common-password

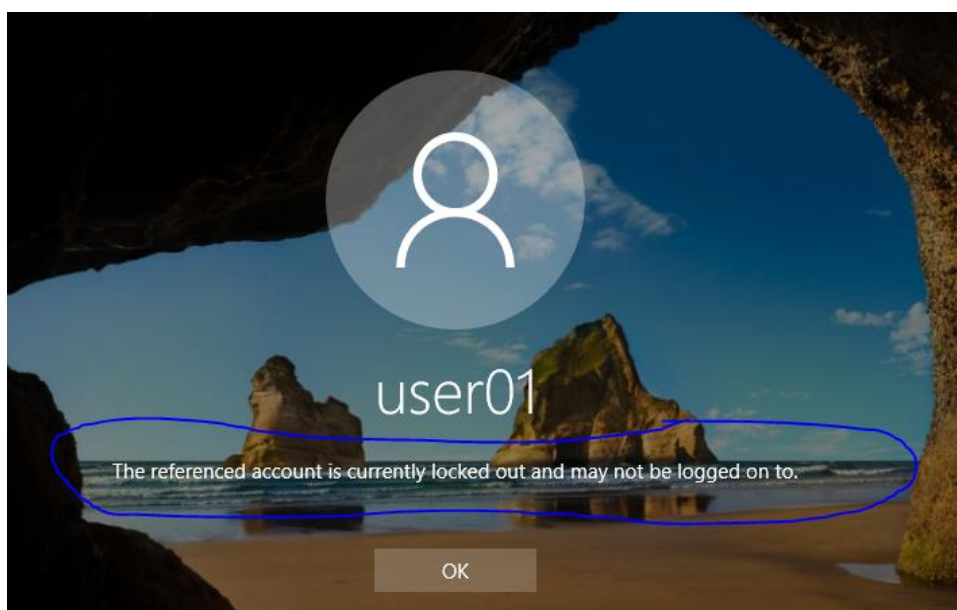


2.3 Έλεγχος ενεργοποίησης καθορισμένων πολιτικών ασφαλείας

Αφού ενεργοποιήσαμε τις πολιτικές ασφαλείας και στα 2 λειτουργικά συστήματα ήρθε η ώρα να ελέγξουμε την εγκυρότητα τους. Και στα 2 λειτουργικά πραγματοποιείτε προσπάθεια αλλαγής κωδικού που δεν πληρεί την πολυπλοκότητα.



Εικόνα 2.3.1 : Προσπάθεια αλλαγής κωδικού με μικρότερη πολυπλοκότητα



Εικόνα 2.3.2 : Κλείδωμα λογαριασμού μετά από 3 αποτυχημένες προσπάθειες



```
Terminal
myadmintest@myadmin-VirtualBox: /etc/pam.d
myadmintest@myadmin-VirtualBox:/etc/pam.d$ su user01
Password:
su: Authentication failure
myadmintest@myadmin-VirtualBox:/etc/pam.d$ su user01
Password:
su: Authentication failure
myadmintest@myadmin-VirtualBox:/etc/pam.d$ su user01
Password:
su: Authentication failure
myadmintest@myadmin-VirtualBox:/etc/pam.d$ su user01
Account locked due to 4 failed logins
Password: 
```

Εικόνα 2.3.3 : Κλείδωμα λογαριασμού μετά από 3 αποτυχημένες προσπάθειες

```
Terminal
myadmintest@myadmin-VirtualBox: /
myadmintest@myadmin-VirtualBox:/ $ faillog -m 3 -l 10
faillog: Cannot open /var/log/faillog: Permission denied
myadmintest@myadmin-VirtualBox:/ $ sudo faillog -m 3 -l 10
myadmintest@myadmin-VirtualBox:/ $ su user01
Account locked due to 13 failed logins
Password:
su: Authentication failure
myadmintest@myadmin-VirtualBox:/ $ faillog -u user01 -r
faillog: Cannot open /var/log/faillog: Permission denied
myadmintest@myadmin-VirtualBox:/ $ sudo faillog -u user01 -r
myadmintest@myadmin-VirtualBox:/ $ su user01
Password:
su: Authentication failure
myadmintest@myadmin-VirtualBox:/ $ su user01
Account temporary locked (1 seconds left)
Password:
su: Authentication failure
myadmintest@myadmin-VirtualBox:/ $ su user01
Password:
su: Authentication failure
myadmintest@myadmin-VirtualBox:/ $ su user01
Account locked due to 4 failed logins
```

Εικόνα 2.3.4 : Εμφάνιση υπολειπόμενου χρόνου μέχρι επόμενη προσπάθεια & ξεκλείδωμα χρήστη

```
Terminal
myadmintest@myadmin-VirtualBox: /
myadmintest@myadmin-VirtualBox:/ $ faillog -a | tail -5
myadmin      0      3  02/26/18 23:40:01 +0200 /dev/pts/17 [10s lock]
user02       0      3  01/01/70 02:00:00 +0200 [10s lock]
user03       3      3  02/26/18 23:35:32 +0200 /dev/pts/17 [10s lock]
myadmintest  0      3  01/01/70 02:00:00 +0200 [10s lock]
user01       4      3  02/26/18 23:51:08 +0200 /dev/pts/17 [10s lock]
myadmintest@myadmin-VirtualBox:/ $
```

Εικόνα 2.3.5 : Εμφάνιση αρχείου καταγραφής αποτυχημένων προσπαθειών

```
myadmintest@myadmin-VirtualBox:/home/myadmin$ passwd
Changing password for myadmintest.
(current) UNIX password:
New password:
Retype new password:
BAD PASSWORD: it is too simplistic/systematic
New password:
BAD PASSWORD: it is WAY too short
New password:
BAD PASSWORD: it is WAY too short
passwd: Have exhausted maximum number of retries for service
passwd: password unchanged
myadmintest@myadmin-VirtualBox:/home/myadmin$ 
```

Εικόνα 2.3.6 : Δοκιμή αλλαγής κωδικού με έναν πιο απλό



2.4 Ερωτήματα 1^{ου} μέρους

Θεωρείτε ότι είναι χρήσιμη η καταγραφή (auditing) των γεγονότων σε ένα λειτουργικό σύστημα; Είναι χρήσιμο να καταγράφονται τα πάντα σε ένα ή περισσότερα αρχεία καταγραφής;

Η καταγραφή (auditing) των γεγονότων σε ένα λειτουργικό σύστημα αποτελεί μια πολύ σημαντική και κρίσιμη λειτουργία η οποία στοχεύει στον καλύτερο και πιο αποτελεσματικό τρόπο αντιμετώπισης προβλημάτων από τον System Administrator. Υπάρχουν αρκετά είδη (log files) ώστε να καλύπτουν το όλο το εύρος των διαφορετικών λειτουργιών και ενεργειών που παίρνουν μέρος στο σύστημα. Οι κατηγορίες των log files και για τα 2 λειτουργικά αφορούν :

- Account logon events
- Account management
- Directory service access
- Logon events
- Object access
- Policy change
- Privilege use
- Process tracking
- System events

Έτσι το κάθε log file αποθηκεύεται στην κατηγορία η οποία αντιπροσωπεύει τη λειτουργία του. Με αυτό το τρόπο ο System Administrator έχοντας ενεργοποιήσει την auditing λειτουργία ασφάλειας είναι σε θέση μεταβαίνοντας στην κατηγορία που επιθυμεί να ελέγξει το log file που επιθυμεί. Η επιλογή μαζικής αποθήκευσης των log files σε ένα ενιαίο αρχείο δεν προτιμάται αφότου δεν είναι καθόλου πρακτική και ασφαλής. Το κύριο μέλημα κάθε λειτουργικού συστήματος εκτός από την λειτουργικότητα είναι η πρακτικότητα και η όσο δυνατόν μεγαλύτερη ευκολία χρήσης των λειτουργιών αυτού από τον χρήστη. Τέλος το auditing αποτελεί ένα πολύ σημαντικό εργαλείο στην αντιμετώπιση επιθέσεων προς τον χρήστη καθώς με σωστή χρήση του ο διαχειριστής είναι ικανός να καταλάβει και να σταματήσει τον κίνδυνο πριν να είναι πολύ αργά.

Θεωρείτε ότι είναι σημαντική η λειτουργία του κλειδώματος λογαριασμού μετά από συγκεκριμένο αριθμό προσπαθειών σύνδεσης; Ποσό σημαντική είναι η διάρκεια του κλειδώματος που κληθήκατε να καθορίσετε;

Η λειτουργία του κλειδώματος λογαριασμού μετά από συγκεκριμένο αριθμό προσπαθειών σύνδεσης είναι ιδιαίτερα σημαντική σε αρκετές περιπτώσεις. Αρχικά το κλείδωμα ενός λογαριασμού μετά από X>1 προσπάθειες στοχεύει στην αντιμετώπιση των κακόβουλων επιθέσεων από hackers. Συγκεκριμένα, σε μια BruteForce επίθεση όπου ο hacker μέσω ειδικών



εργαλείων χρησιμοποιεί εκατομμύρια κωδικούς ,ώστε με λίγη τύχη κάποια στιγμή να βρει τον κωδικό του χρήστη. Ο μηχανισμός κλειδώματος καθιστά την μέθοδο επίθεσης που διάλεξε ΜΗ-αποτελεσματική (το όριο προσπαθειών είναι 999-windows). Έπειτα υπάρχει και η επιλογή να τεθεί ο αριθμός κλειδώματος στον αριθμό "0" , δηλαδή να μην υπάρχει περίπτωση κλειδώματος του λογαριασμού όσες φορές και αν ο χρήστης πληκτρολογήσει λανθασμένα το συνθηματικό του. Βέβαια υπάρχουν και παραδείγματα όπου το κλείδωμα λογαριασμών μπορεί να αποβεί μοιραίο. Για παράδειγμα σε επίθεση DDOS όπου ο χρήστης στέλνει συνεχείς αιτήματα πρόσβασης στους υπολογιστές-μέλη του δικτύου, εάν όλοι οι υπολογιστές έχουν ενεργοποιημένη την λειτουργία κλειδώμα λογαριασμού μετά από $X > 1$ προσπάθειες τότε όλοι οι λογαριασμοί θα καθιστούν "άχρηστοι" αφού θα κλειδωθούν άμεσα. Όσον αφορά τον αριθμό τον οποίο θέτω σαν όριο κλειδώματος εξαρτάται από την εταιρεία-χρήστη, τις πολιτικές και το μέγεθος ρίσκου που είναι έτοιμες να πάρουν. Ένας γενικός κανόνας είναι ότι ο αριθμός θα πρέπει να κυμαίνεται μεταξύ 4 και 10. Έτσι, η επιλογή ασφαλείας κλειδώματος είναι ένα μείζονος σημασίας «feature», αλλά για να λειτουργήσει αποτελεσματικά χρειάζεται σωστή χρήση και προσαρμογή στα "θέλω και πρέπει" της εκάστοτε εταιρείας-χρήστη. Για παράδειγμα, θέτοντας το όριο lock στο μηδέν, διαβεβαιώνουμε ότι δεν πρόκειται να κλειδωθεί ο λογαριασμός αλλά από την άλλη δεν αποκλείουμε μια BruteForce επίθεση. Σε μια τέτοια περίπτωση για να αποφύγουμε όσο το δυνατόν πιο αποτελεσματικά μια τέτοια είδους επίθεση θα πρέπει να θέσουμε στο χρήστη αναγκαστικά να θέσει ένα περίπλοκο κωδικό με κατώτερο όριο πχ 9 χαρακτήρες ή να θέσουμε διάρκεια κλειδώματος. Με την τελευταία μέθοδο υποχρεώνουμε τον χρήστη να περιμένει ,ίσως για να σκεφτεί περισσότερο, για να ξαναπροσπαθήσει.

Τι προσφέρει η δυνατότητα του Λ.Σ. να διατηρεί ιστορικό συνθηματικών για κάθε χρήστη;

Η δυνατότητα του Λ.Σ. να διατηρεί ιστορικό συνθηματικών για κάθε χρήστη ανοίγει τους ορίζοντες για μια αρκετά μεγάλη γκάμα επιλογών. Με αυτό το τρόπο μπορούμε να θέσουμε επιπλέον όρια στον χρήστη όπως το να μην χρησιμοποιεί τον ίδιο κωδικό για πάνω από X φορές (σε μια προσπάθεια να αποφύγουμε τις επιβλαβείς επιθέσεις). Επιπλέον μπορούμε να θέσουμε ανώτατο και κατώτατο όριο του μεγέθους του κωδικού. Επιπρόσθετα το password history log είναι αρκετά χρήσιμο καθώς σου δίνει την δυνατότητα να παρακολουθείς το ΠΟΤΕ συνδέθηκες στο μηχάνημα, αρκετά σημαντικό για να εντοπιστούν επιβλαβείς ενέργειες κατά του λογαριασμού του χρήστη μας.

Η προεπιλεγμένη ρύθμιση στα Λ.Σ. των Windows και Linux επιτρέπει τη διατήρηση του ίδιου συνθηματικού χρήστη για συγκεκριμένο χρονικό διάστημα ή ο χρήστης είναι ικανός να διατηρήσει μόνιμα το ίδιο συνθηματικό?

- Όσον αφορά το λειτουργικό σύστημα Windows η προκαθορισμένη (default) τιμή για domain controllers οι οποίοι χρησιμοποιούν κάποια έκδοση του Windows Server 2003 είναι 24. Για domain controllers οι οποίοι χρησιμοποιούν κάποια έκδοση των Windows 2000 είναι 3. Ενώ για όλες τις υπόλοιπες εκδόσεις των Windows η προκαθορισμένη τιμή είναι 0.
- Από την άλλη πλευρά στο λειτουργικό Ubuntu η default τιμή είναι 0 και σου επιτρέπει να τον διατηρείς μόνιμα αλλά υπάρχει δυνατότητα παραμετροποίησης ,υποχρεωτικής αλλαγής , ώστε να τον αλλάζει ο χρήστης ανά όσες μέρες του έχει οριστεί από το σύστημα.



3 Μέρος 2^ο - Διαχείριση συνθηματικών & Μελέτη επιθέσεων

Στο δεύτερο μέρος της άσκησης ζητείται η αλληλεπίδραση σε θέματα όπως διαχείριση συνθηματικών ,τρόποι φύλαξης και μέθοδοι δημιουργίας ασφαλέστερων κωδικών ώστε να προστατεύονται από επιθέσεις ανάκτησης τους.

3.1 Έλεγχος δυναμικότητας συνθηματικών

Αρχικά πρέπει να ελέγξουμε τις δυναμικότητες των κωδικών που είχαμε ορίσει παραπάνω σε κάποιο από τα site που μας δόθηκαν.



Εικόνα 3.1.1 : Κωδικός που ανήκει στους 5 πιο δημοφιλείς



Εικόνα 3.1.2 : Κωδικός χαμηλής πολυπλοκότητας



Εικόνα 3.1.3 : Κωδικός καλής πολυπλοκότητας



Εικόνα 3.1.4 : Κωδικός που δεν ανακτάται



Αναλύοντας τα παραπάνω στιγμιότυπα βγάζουμε κάποια συμπεράσματα σχετικά με τις παραμέτρους που οριοθετούν την πολυπλοκότητα ενός συνθηματικού. Οι παράγοντες αυτοί είναι ο αριθμός της συμβολοσειράς που πρέπει να είναι τουλάχιστον 8, η διαφορετικότητα (να περιέχει πεζά, κεφαλαία, σύμβολα, αριθμούς) καθώς και το να μην είναι διαδοχικά μεταξύ τους. Περιοχή φύλαξης λογαριασμών χρηστών & συνθηματικών

3.2 Φύλαξη λογαριασμών & συνθηματικών

- Ένα προφίλ χρήστη (Windows) αποτελείται από τα ακόλουθα στοιχεία: Μια ομάδα μητρώου. Η ομάδα μητρώου είναι το αρχείο **NTuser.dat**. Το μητρώο φορτώνεται από το σύστημα κατά τη σύνδεση του χρήστη και αντιστοιχεί στο κλειδί μητρώου **HKEY_CURRENT_USER**. Η ομάδα μητρώου χρήστη διατηρεί τις προτιμήσεις και τη διαμόρφωση των μητρώων του χρήστη σε ένα σύνολο φακέλων προφίλ αποθηκευμένων στο σύστημα αρχείων. Τα αρχεία προφίλ χρήστη αποθηκεύονται στον κατάλογο Προφίλ, σε ένα φάκελο ανά χρήστη. Ο φάκελος προφίλ χρήστη είναι ένα κοντέινερ για εφαρμογές και άλλα στοιχεία του συστήματος που συμπληρώνονται με υποφακέλους και δεδομένα ανά χρήστη, όπως έγγραφα και αρχεία ρυθμίσεων. Η «Εξερεύνηση των Windows» χρησιμοποιεί εκτενώς τους φακέλους προφίλ χρήστη για στοιχεία όπως το φάκελο του Desktop, του μενού "Εναρξη" και "Εγγραφα" του χρήστη. Στα windows κυρίως αποθηκεύονται στο path C:\users\username\AppData\Roaming\Microsoft\credentials και στο C:\users\username\AppData\Roaming\Microsoft\Vault. Επειδή όμως αυτοί οι φάκελοι πρέπει να είναι ασφαλείς μόνο ο χρήστης και ο διαχειριστής συστήματος μπορούν να έχουν πρόσβαση και επίσης τα ευαίσθητα δεδομένα είναι κρυπτογραφημένα. Όσον αφορά τους κωδικούς πρόσβασης στα Windows τα στοιχεία των λογαριασμών αποθηκεύονται στην registry SAM. Αποθηκεύει κωδικούς χρησιμοποιώντας one-way-hash (LM HASH ή NTLM hash). Το αρχείο SAM της registry είναι αποθηκευμένο στην διεύθυνση %WinDir%\system32\config\SAM και αυτή η διαδρομή είναι προσβάσιμη ΜΟΝΟ στους διαχειριστές, ώστε να μην υπάρχει κίνδυνος παραβίασης τους.
- Στην Ubuntu πλευρά οι λογαριασμοί αποθηκεύονται στον φάκελο home. Για την ακρίβεια όταν δημιουργείτε έναν λογαριασμό δημιουργείτε και ο προσωπικός του χώρος, όπου αυτόματα δημιουργούνται και άλλοι υποφακέλοι. Τα συνθηματικά αποθηκεύονται στο αρχείο /etc/passwd το οποίο ανοίγει με "nano". Ο κωδικός όλων εκεί, προφανώς και είναι κρυφός, και έχει το ίδιο σύμβολο "x". Η κρυπτογράφηση αυτού του κωδικού μπορεί να πραγματοποιηθεί με κρυπτογράφηση MD5, SHA-256, SHA-512 καθώς και Blowfish για μερικές διανομές.



Εικόνα 3.2.1 : Χώρος φύλαξης λογαριασμών



```
Terminal
myadmin@myadmin-VirtualBox: /home
GNU nano 2.5.3 File: /etc/passwd Modified
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127:,:/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
myadmin:x:1000:1000:pipis,,,:/home/myadmin:/bin/bash
user02:x:1002:1002:,,,:/home/user02:/bin/bash
user03:x:1003:1003:,,,:/home/user03:/bin/bash
myadmintest:x:1004:1004:,,,:/home/myadmintest:/bin/bash
user01:x:1001:1001:,,,:/home/user01:/bin/bash
```

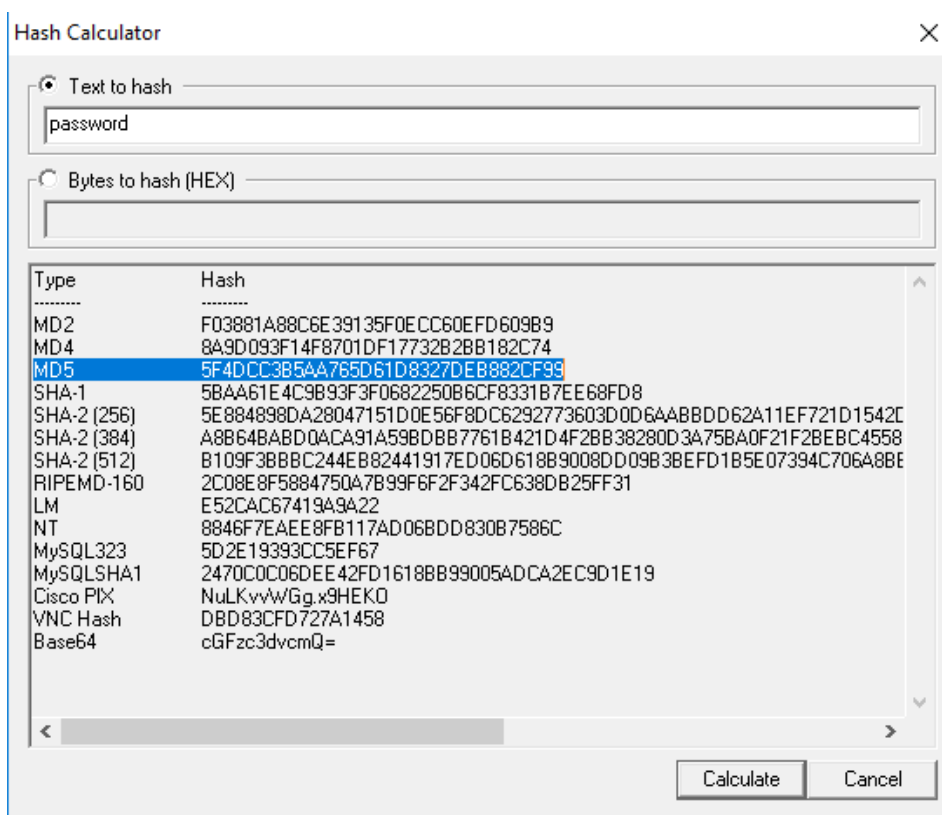
Εικόνα 3.2.2 : Το σύμβολο x αναπαριστά τον κρυμμένο κωδικό

Όσον αφορά τον όρο **hash**, ένα hash είναι μια σειρά τυχαίων χαρακτήρων που μονοσήμαντα τα δεδομένα, όπως το δακτυλικό αποτύπωμα. Μπορούμε να κάνουμε hashing οποιαδήποτε δεδομένα, είτε πρόκειται για ένα αρχείο (όπως ένα μουσικό MP3 ή spreadsheet) είτε απλά μια σειρά χαρακτήρων (όπως ένας κωδικός πρόσβασης). Κάθε φορά που κάνετε hash generating τα ίδια δεδομένα, θα έχετε την ίδια ακριβώς τιμή κατακερματισμού ως αποτέλεσμα. Χρησιμοποιούμε το hashing για να αποκρύψουμε τα αποθηκεύσουμε δεδομένα. Ο πιο ασφαλής τρόπος για να αποθηκευτούν ευαίσθητα δεδομένα όπως κωδικοί πρόσβασης είναι να τους μετατρέψεις σε hash έτσι ώστε και να προσπαθήσει να κλέψει δεδομένα το μόνο που θα βρει είναι το hash key το οποίο δεν είναι εύκολο να αντιστραφεί από κάποιον. Η διαδικασία της αναζήτησης σε μια Βάση Δεδομένων μέσω του hashing γίνεται πιο γρήγορη. Επίσης με τη μέθοδο του hash μπορούμε να σιγουρευτούμε για την γνησιότητα ενός αρχείου. Για παράδειγμα όταν κατεβάζουμε από το internet κάποιο αρχείο προτού το ανοίξουμε μπορούμε να τρέξουμε το αρχείο μέσω μιας hash generator και να ελέγξουμε το hash που παρήγαγε με το hash που δίνει ο official κατασκευαστής.

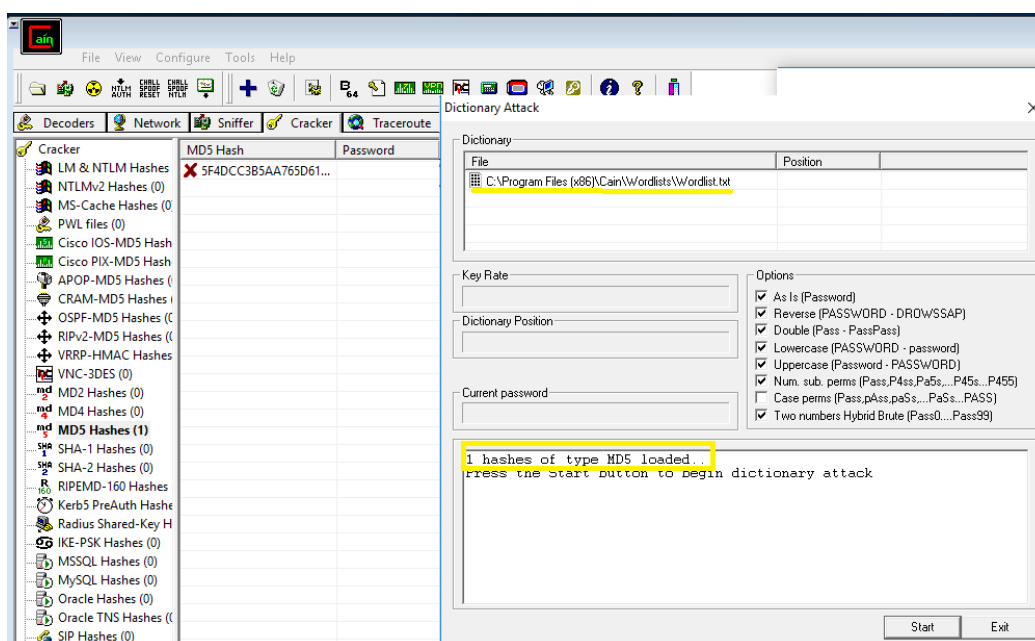
3.3 Επιθέσεις με χρήση Password Cracker

Ως password cracker χρησιμοποιήσαμε το Cain & Abel για τα Windows και το “John the ripper” για τα Ubuntu.

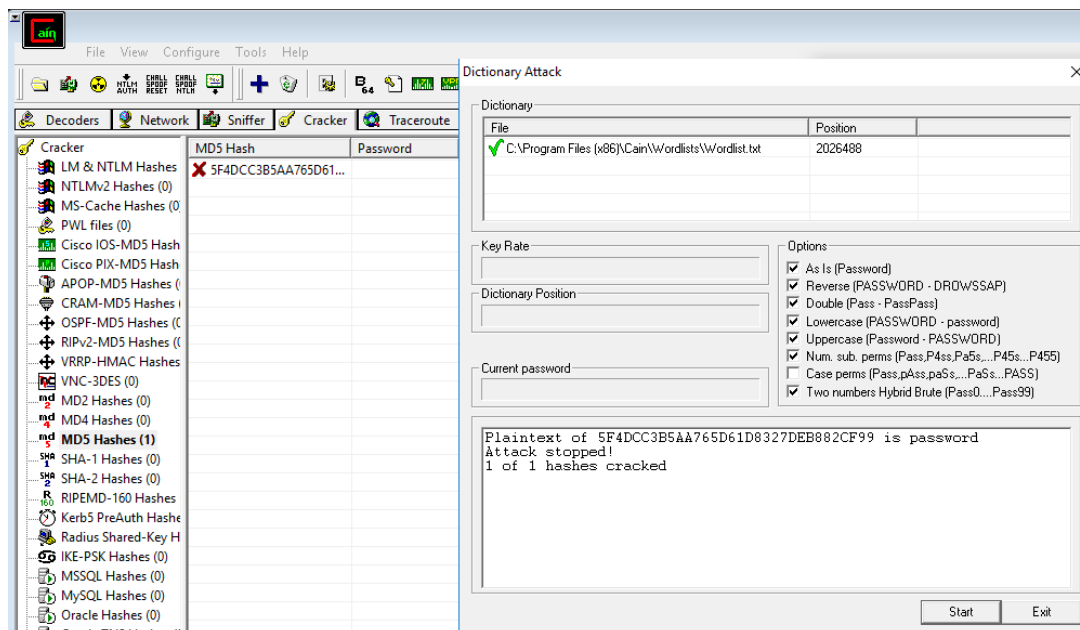
- Στο «cain & abel» ανοίγουμε το hash generator που μας παρέχει και εισάγουμε το συνθηματικό που θέλουμε να μας χασάρει και μας εμφανίζει τα hash που αντιστοιχούν στην κάθε κρυπτογράφηση. Στην 1^η προσπάθεια κάνουμε επίθεση με λεξικό. Όπως θα δούμε καταλαβαίνει το είδος της κρυπτογράφησης μέσω του hash ,ανακτεί το κωδικό πολύ γρήγορα και μας τον εμφανίζει. Στην επόμενη περίπτωση που χρησιμοποιήσαμε περίπλοκο συνθηματικό " !@Georgezias123456 " τότε αναγκαστήκαμε να σταματήσουμε την προσπάθεια καθώς μετά από αρκετή ώρα δεν είχε καμία απολύτως πρόοδο ή επιτυχία.
- Για να κατεβάσουμε το “john the ripper” από το τερματικό γράφουμε “sudo snap install john-the-ripper. Αφού το εγκαταστήσουμε και προτού ξεκινήσουμε τις δοκιμές πάμε να αλλάξουμε από το αρχείο common-password την κρυπτογράφηση κωδικών σε MD5 ώστε να είναι πιο εύκολο το σπάσιμο του συνθηματικού έναντι του SHA-512. Κατεβάσαμε ένα έτοιμο λεξικό και προσθέσαμε μέσα τον κωδικό του user03. Στην συνέχεια τρέχουμε “sudo john -w:/test/rockyou.txt pass. Pass είναι το αρχείο που δημιουργεί με τα επιτυχημένα αποτελέσματα. Για να τα δούμε γράφουμε “sudo john – show pass”.



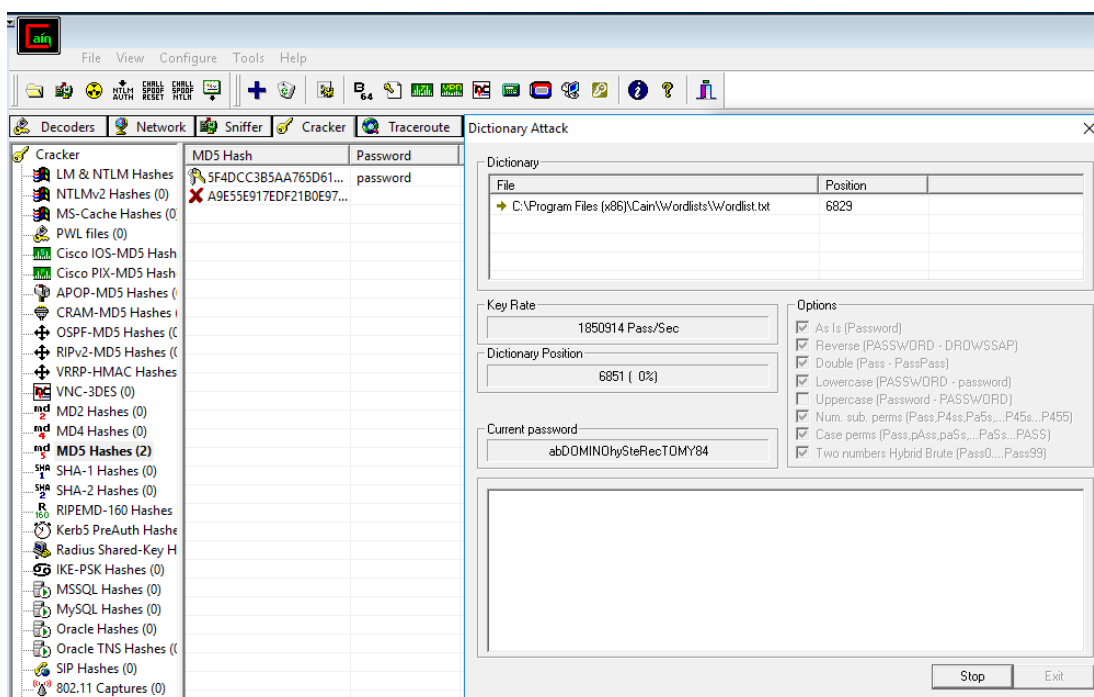
Εικόνα 3.3.1 : Hash Generator



Εικόνα 3.3.2 : Μεταφόρτωση λεξικού και εκκίνηση επίθεσης



Εικόνα 3.3.3 : Επιτυχής επίθεση & εμφάνιση κωδικού



Εικόνα 3.3.4 : Πολύωρη ανεπιτυχής επίθεση



```
myadmin@myadmin-VirtualBox: /test
GNU nano 2.5.3 File: /etc/pam.d/common-password Modified

# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

password      required          pam_pwhistory.so
password      requisite         pam_cracklib.so try_first_pass retry=3 minlength=8 l$

# here are the per-package modules (the "Primary" block)
password      [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass md5
```

Εικόνα 3.3.5 : Αλλαγή κρυπτογράφησης κωδικών σε md5

```
Terminal
root@myadmin-VirtualBox: /test
GNU nano 2.5.3 File: rockyou.txt Modified

123456
12345
123456789
password
iloveyou
princess
1234567
Hom@#3e# <-- kwdikos user03 gia euresi apo john
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
```

Εικόνα 3.3.6 : Εισαγωγή κωδικού δικού μας χρήστη στο λεξικό

```
root@myadmin-VirtualBox:/test# sudo john -w:/test/rockyou.txt pass
Loaded 5 password hashes with 5 different salts (crypt, generic crypt(3) [?/64])
Remaining 4 password hashes with 4 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
Hom@#3e# (user03)
```

Εικόνα 3.3.7 : Επιτυχής ανάκτηση κωδικού

```
root@myadmin-VirtualBox:/test# sudo john --show pass
user02:user02:1002:1002:,,,:/home/user02:/bin/bash
user03:Hom@#3e#:1003:1003:,,,:/home/user03:/bin/bash

2 password hashes cracked, 3 left
root@myadmin-VirtualBox:/test#
```

Εικόνα 3.3.8 : Εμφάνιση κωδικού που ανακτήθηκε

Στο στιγμιότυπο 3.3.8 βλέπουμε ότι μας εμφανίζει τις γραμμές με τις ίδιες πληροφορίες που είχε το αρχείο /etc/passwd με την διαφορά ότι τώρα έχουμε στην θέση του συμβόλου x τον πραγματικό κωδικό.



Για την εξέταση της ανάκτησης με την μέθοδο των rainbow tables χρειάστηκε να εγκαταστήσουμε την εφαρμογή rcrack. Τρέχοντας λοιπόν ,μετά την εγκατάσταση , ./ και το όνομα του script (rcrack,rtgen,rtsort) μας ανοίγει η αρχική οθόνη του προγράμματος. Έτσι βλέπουμε το πώς συντάσσετε η εντολή και από τι παραμέτρους εξαρτάται. Αρχικά πρέπει να τρέξουμε το rtgen ώστε να δημιουργήσουμε τα rainbow tables. Έπειτα μπορούμε να κάνουμε sort ώστε να επιταχύνουμε την διαδικασία αφού ταξινομεί τα tables. Και τέλος το rcrack ώστε να γίνει η επίθεση με το υλικό που έχουμε φτιάξει.

```
myadmin@myadmin-VirtualBox: ~/Downloads/rainbowcrack-1.5/amd64
myadmin@myadmin-VirtualBox:~/Downloads/rainbowcrack-1.5/amd64$ ./rcrack
RainbowCrack 1.5
Copyright 2003-2010 RainbowCrack Project. All rights reserved.
Official Website: http://project-rainbowcrack.com/

usage: rcrack rt_files [rt_files ...] -h hash
       rcrack rt_files [rt_files ...] -l hash_list_file
       rcrack rt_files [rt_files ...] -f pwdump_file
       rcrack rt_files [rt_files ...] -n pwdump_file
rt_files:      path to the rainbow table(s), wildchar(*, ?) supported
-h hash:      load single hash
-l hash_list_file: load hashes from a file, each hash in a line
-f pwdump_file: load lanmanager hashes from pwdump file
-n pwdump_file: load ntlm hashes from pwdump file

hash algorithms implemented in alglib0.so:
lm, plaintext_len limit: 0 - 7
ntlm, plaintext_len limit: 0 - 15
md5, plaintext_len limit: 0 - 15
sha1, plaintext_len limit: 0 - 20
mysqlsha1, plaintext_len limit: 0 - 20
halflmchall, plaintext_len limit: 0 - 7
ntlmchall, plaintext_len limit: 0 - 15
oracle-SYSTEM, plaintext_len limit: 0 - 10
md5-half, plaintext_len limit: 0 - 15

example: rcrack *.rt -h 5d41402abc4b2a76b9719d911017c592
         rcrack *.rt -l hash.txt
myadmin@myadmin-VirtualBox:~/Downloads/rainbowcrack-1.5/amd64$
```

Εικόνα 3.3.9 : Παράδειγμα προβολής οδηγού rcrack

Το συγκεκριμένο rainbow table θα ανακτούσε συνθηματικά μέχρι 7 ψηφίων με μήκος αλυσίδας 3800 και αριθμό αλυσίδων 100000. Το index αλλάζει από 0 σε 1 επειδή σπάει σε 2 parts το table.

```
myadmin@myadmin-VirtualBox: ~/Downloads/rainbowcrack-1.5/amd64
myadmin@myadmin-VirtualBox:~/Downloads/rainbowcrack-1.5/amd64$ ./rtgen md5 loweralpha-numeric 1 7 0 3800 100000 0
rainbow table md5_loweralpha-numeric#1-7_0_3800x100000_0.rt parameters
hash algorithm:      md5
hash length:        16
charset:             abcdefghijklmnopqrstuvwxyz0123456789
charset in hex:      61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 30 31 32 33 34 35 36
37 38 39
charset length:      36
plaintext length range: 1 - 7
reduce offset:       0x00000000
plaintext total:     80603140212

sequential starting point begin from 0 (0x0000000000000000)
generating...
65536 of 100000 rainbow chains generated (0 m 38.4 s)
100000 of 100000 rainbow chains generated (0 m 20.3 s)
myadmin@myadmin-VirtualBox:~/Downloads/rainbowcrack-1.5/amd64$ ./rtgen md5 loweralpha-numeric 1 7 1 3800 100000 0
rainbow table md5_loweralpha-numeric#1-7_1_3800x100000_0.rt parameters
```

Εικόνα 3.3.10 : Παραγωγή rainbow table 7 ψηφίων

Έπειτα κάνουμε sort μεταξύ όλων αυτών των παραδειγμάτων που φτιάξαμε. Τέλος δοκιμάζουμε την αποτελεσματικότητα για τον χρόνο που του διαθέσαμε.



```
myadmin@myadmin-VirtualBox: ~/Downloads/rainbowcrack-1.5/amd64
myadmin@myadmin-VirtualBox:~/Downloads/rainbowcrack-1.5/amd64$ ./rtsort *.rt
md5_loweralpha#1-2_0_3800x3_0.rt:
1709903872 bytes memory available
loading rainbow table...
sorting rainbow table by end point...
writing sorted rainbow table...

md5_loweralpha#1-6_0_3800x3_0.rt:
1709903872 bytes memory available
loading rainbow table...
sorting rainbow table by end point...
writing sorted rainbow table...

md5_loweralpha#1-7_0_1000x1000_0.rt:
1709903872 bytes memory available
loading rainbow table...
sorting rainbow table by end point...
writing sorted rainbow table...

md5_loweralpha-numeric#1-7_0_3800x100000_0.rt:
1709903872 bytes memory available
loading rainbow table...
sorting rainbow table by end point...
writing sorted rainbow table...

md5_loweralpha-numeric#1-7_0_3800x5000_0.rt:
1709580288 bytes memory available
loading rainbow table...
sorting rainbow table by end point...
writing sorted rainbow table...
```

Εικόνα 3.3.11 : Ταξινόμηση των τραπέζιων

```
myadmin@myadmin-VirtualBox: ~/Downloads/rainbowcrack-1.5/amd64
myadmin@myadmin-VirtualBox:~/Downloads/rainbowcrack-1.5/amd64$ ./rcrack *.rt -h 80c9ef0fb86369cd25f90af27ef53a9e
1679925248 bytes memory available
20 x 1600000 bytes memory allocated for table buffer
60800 bytes memory allocated for chain traverse
disk: md5_loweralpha#1-2_0_3800x3_0.rt: 48 bytes read
disk: md5_loweralpha#1-6_0_3800x3_0.rt: 48 bytes read
disk: md5_loweralpha#1-7_0_1000x1000_0.rt: 16000 bytes read
disk: md5_loweralpha-numeric#1-7_0_3800x100000_0.rt: 1600000 bytes read
disk: md5_loweralpha-numeric#1-7_0_3800x5000_0.rt: 80000 bytes read
disk: md5_loweralpha-numeric#1-7_10_3800x5000_0.rt: 80000 bytes read
disk: md5_loweralpha-numeric#1-7_1_3800x100000_0.rt: 1600000 bytes read
disk: md5_loweralpha-numeric#1-7_1_3800x5000_0.rt: 80000 bytes read
disk: md5_loweralpha-numeric#1-7_2_3800x100000_0.rt: 1600000 bytes read
disk: md5_loweralpha-numeric#1-7_2_3800x5000_0.rt: 80000 bytes read
disk: md5_loweralpha-numeric#1-7_3_3800x100000_0.rt: 1600000 bytes read
disk: md5_loweralpha-numeric#1-7_3_3800x5000_0.rt: 80000 bytes read
disk: md5_loweralpha-numeric#1-7_4_3800x100000_0.rt: 1600000 bytes read
disk: md5_loweralpha-numeric#1-7_4_3800x5000_0.rt: 80000 bytes read
disk: md5_loweralpha-numeric#1-7_5_3800x100000_0.rt: 1600000 bytes read
disk: md5_loweralpha-numeric#1-7_5_3800x5000_0.rt: 80000 bytes read
disk: md5_loweralpha-numeric#1-7_6_3800x5000_0.rt: 80000 bytes read
disk: md5_loweralpha-numeric#1-7_7_3800x5000_0.rt: 80000 bytes read
disk: md5_loweralpha-numeric#1-7_8_3800x5000_0.rt: 80000 bytes read
disk: md5_loweralpha-numeric#1-7_9_3800x5000_0.rt: 80000 bytes read
searching for 1 hash...
disk: finished reading all files
searching for 1 hash...
searching for 1 hash...
searching for 1 hash...
plaintext of 80c9ef0fb86369cd25f90af27ef53a9e is a123

statistics
-----
plaintext found:                1 of 1
total time:                     5.37 s
  time of chain traverse:       3.35 s
  time of alarm check:         1.96 s
  time of wait:                 0.00 s
  time of other operation:      0.07 s
time of disk read:              0.01 s
hash & reduce calculation of chain traverse: 22147600
hash & reduce calculation of alarm check: 16637369
number of alarm:                9987
speed of chain traverse:        6.61 million/s
speed of alarm check:          8.50 million/s

result
-----
80c9ef0fb86369cd25f90af27ef53a9e a123 hex:61313233
myadmin@myadmin-VirtualBox:~/Downloads/rainbowcrack-1.5/amd64$
```

Εικόνα 3.3.12 : Αναζήτηση ανάκτησης κωδικού “a123”



Στη τελευταία γραμμή φαίνεται ότι έχει βρει τον παραπάνω εύκολο κωδικό. Στην συνέχεια δοκιμάσαμε να φτιάξουμε μεγαλύτερα tables που θα ήταν αποτελεσματικά για πιο πραγματικές συνθήκες σε πιο πολύπλοκα συνθηματικά αλλά λόγω της μεγάλης διάρκειας που απαιτούσε να φτιαχτεί το σταματήσαμε χωρίς να πάρουμε αποτέλεσμα.

3.4 Ερωτήματα 2ου μέρους

Για κάθε λογαριασμό χρήστη στα δύο Λ.Σ. , αποθηκεύεται το κρυπτογραφημένο συνθηματικό, η κρυπτογραφική σύνοψή του, ή το κλειδί κρυπτογράφησης του συνθηματικού;

Και στα 2 λειτουργικά αποθηκεύεται το κρυπτογραφημένο συνθηματικό.

Τι απαιτείται για να επιτύχει μια επίθεση λεξικού και τι για να επιτύχει μια επίθεση εξαντλητικής αναζήτησης;

- Για να επιτύχει μια επίθεση λεξικού χρειάζεται μεγάλη υπολογιστική ισχύ καθώς το υπολογιστικό σύστημα θα πρέπει να τρέχει για πάρα πολλές ώρες κάνοντας όσον το δυνατόν περισσότερους υπολογισμούς μπορεί να αντέξει.
- Για να επιτύχει μια επίθεση εξαντλητικής αναζήτησης (BruteForce) χρειάζεται επίσης ικανοποιητική υπολογιστική δύναμη αλλά και έναν έξυπνο αλγόριθμο παραγωγής κλειδιών για έλεγχο ώστε να υπάρξουν τα επιθυμητά για τον "διαρρήκτη" αποτελέσματα.

Ποια τεχνική θα επιλέγατε για την ταχύτερη αποκάλυψη ενός πολύπλοκου συνθηματικού και γιατί;

Για την ταχύτερη αποκάλυψη ενός πολύπλοκου συνθηματικού θα χρησιμοποιούσα την μέθοδο rainbow table attack καθώς είναι πάρα πολύ αποτελεσματική απέναντι σε δύσκολους και πολύπλοκους κωδικούς. Τα τραπέζια ουράνιου τόξου είναι βασικά τεράστια σύνολα πινάκων γεμάτους με τιμές κατακερματισμού που είναι προ-αντιστοιχισμένοι σε πιθανούς κωδικούς πρόσβασης plaintext. Οι πίνακες ουράνιου τόξου επιτρέπουν ουσιαστικά στους χάκερς να αντιστρέψουν τη λειτουργία κατακερματισμού για να καθορίσουν ποιος μπορεί να είναι ο κωδικός πρόσβασης. Η χρήση των Rainbow Tables επιτρέπει τη δημιουργία ραγισμένων κωδικών σε πολύ σύντομο χρονικό διάστημα σε σύγκριση με τις μεθόδους BruteForce, ωστόσο, ο συμβιβασμός είναι ότι απαιτεί πολύ χώρο αποθήκευσης (μερικές φορές Terabytes) για να συγκρατήσει τους ίδιους τους πίνακες Rainbow. Συνεπώς αν διαθέτεις τα χρήματα για να αγοράσεις έτοιμους σκληρούς που περιέχουν τα rainbow tables ,και δεν παίζεις σ' αυτήν την ατελείωτη διαδικασία να τα παράξεις ,τότε η ανάκτηση έγινε «παιχνιδάκι».

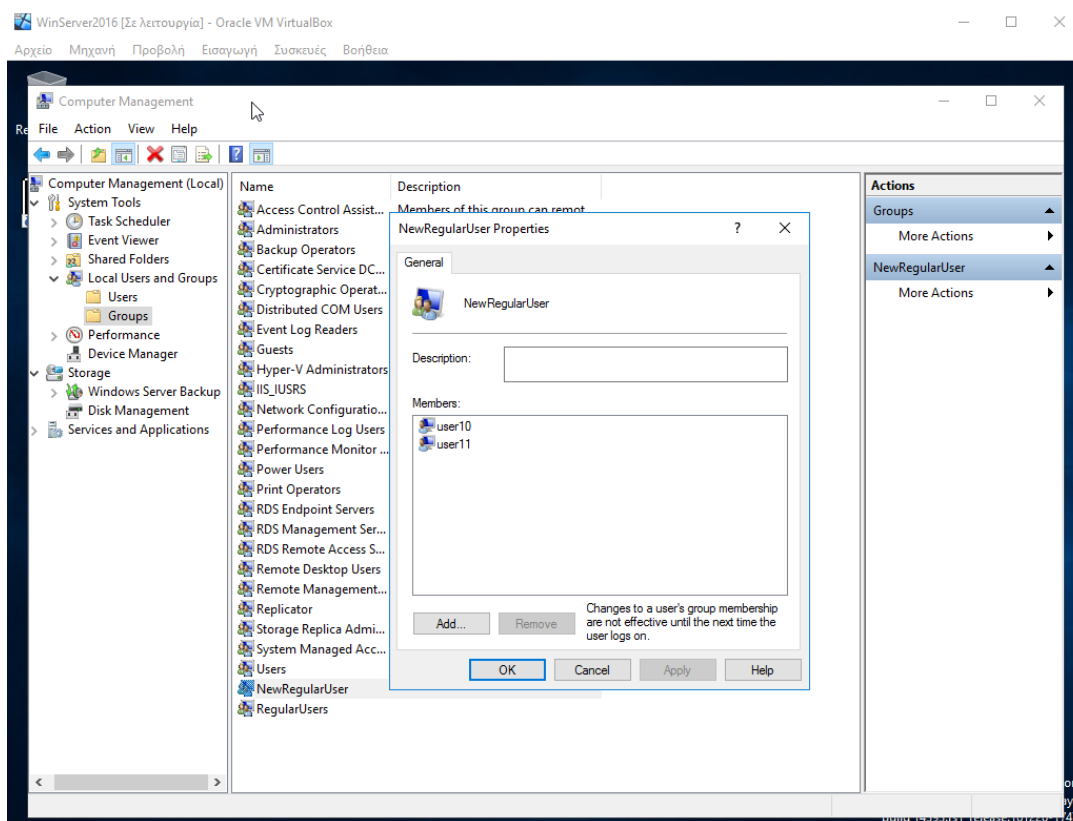


4 Μέρος 3^ο - Έλεγχος πρόσβασης πόρων Λειτουργικού Συστήματος

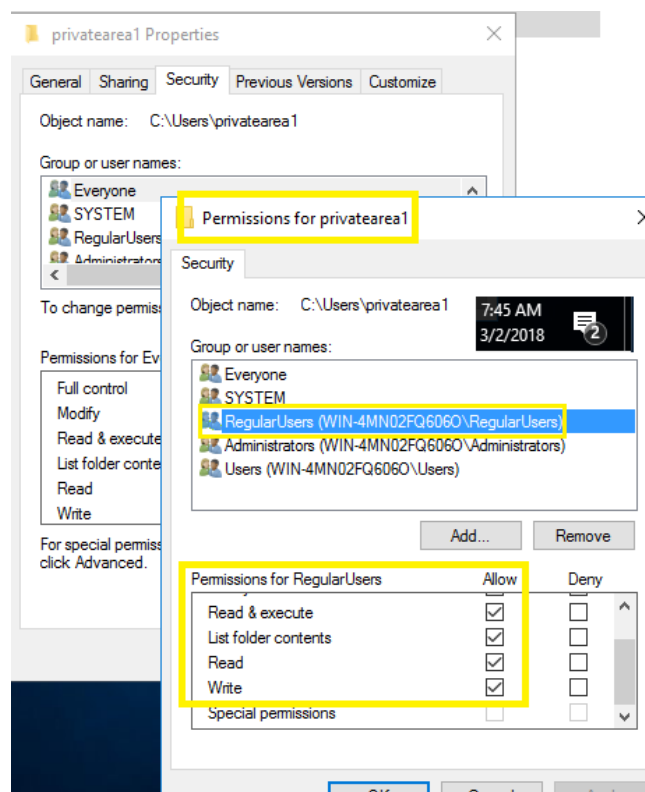
Στο τρίτο μέρος της άσκησης καλούμαστε να ασχοληθούμε με τους μηχανισμούς ελέγχου πρόσβασης και των δύο λειτουργικών συστημάτων. Επίσης θα εξετάσουμε και το πώς γίνεται έλεγχος πρόσβασης στους πόρους (αρχεία, φάκελοι) του συστήματος.

4.1 Δημιουργία ομάδων & προσωπικού χώρου

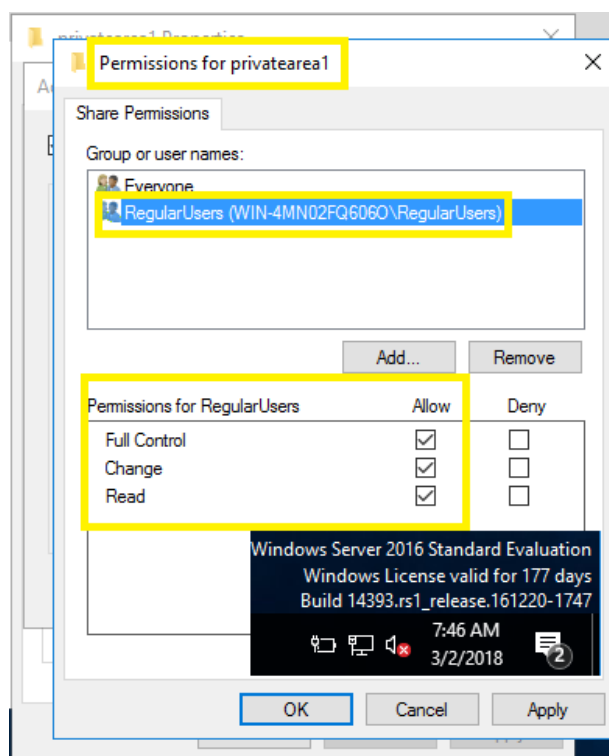
Ως πρώτο τμήμα του ερωτήματος χρειάζεται να φτιάξουμε το παρακάτω σενάριο. Αρχικά δημιουργήσουμε δύο καινούργιους χρήστες user10 & user11 και τους προσθέσουμε στο καινούριο group “NewRegularUsers” που πρέπει να φτιάξουμε. Έπειτα δημιουργούμε 2 περιοχές με όνομα privateArea1 (1^η ομάδα) & privateArea2 (2^η ομάδα) όπου μόνο τα μέλη της ίδιας ομάδας έχουν πλήρη δικαιώματα και όλοι οι άλλοι κανένα. Μετέπειτα άλλες 2 περιοχές publicArea1 (1^η ομάδα) & publicArea2 (2^η ομάδα) όπου όλοι οι χρήστες του συστήματος μπορούν να προσθέσουν αρχεία και να διαβάσουν αλλά μόνο οι ιδιοκτήτες μπορούν να το τροποποιούν ή να το διαγράψουν.



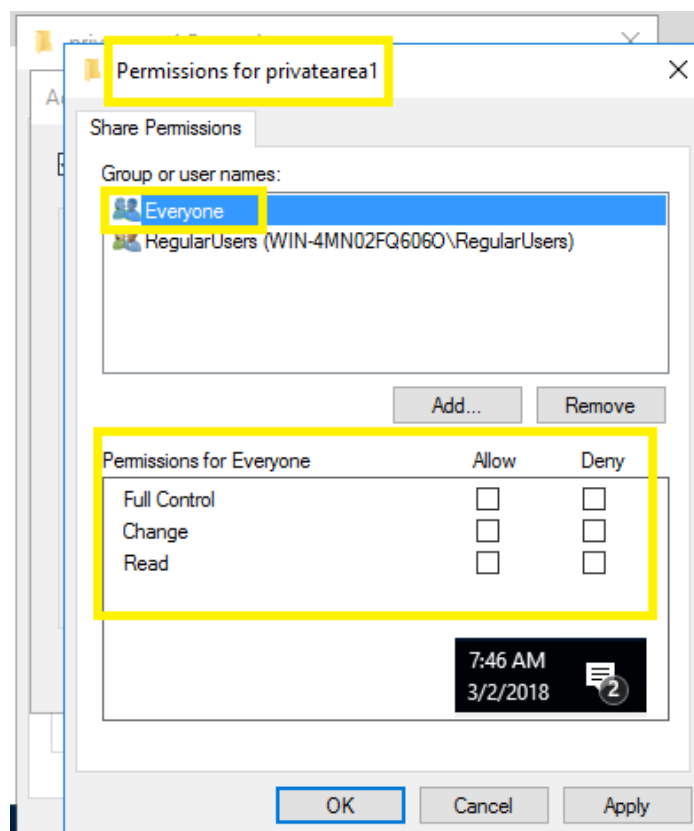
Εικόνα 4.1.1 : Δημιουργία group και πρόσθεση χρηστών σ αυτό



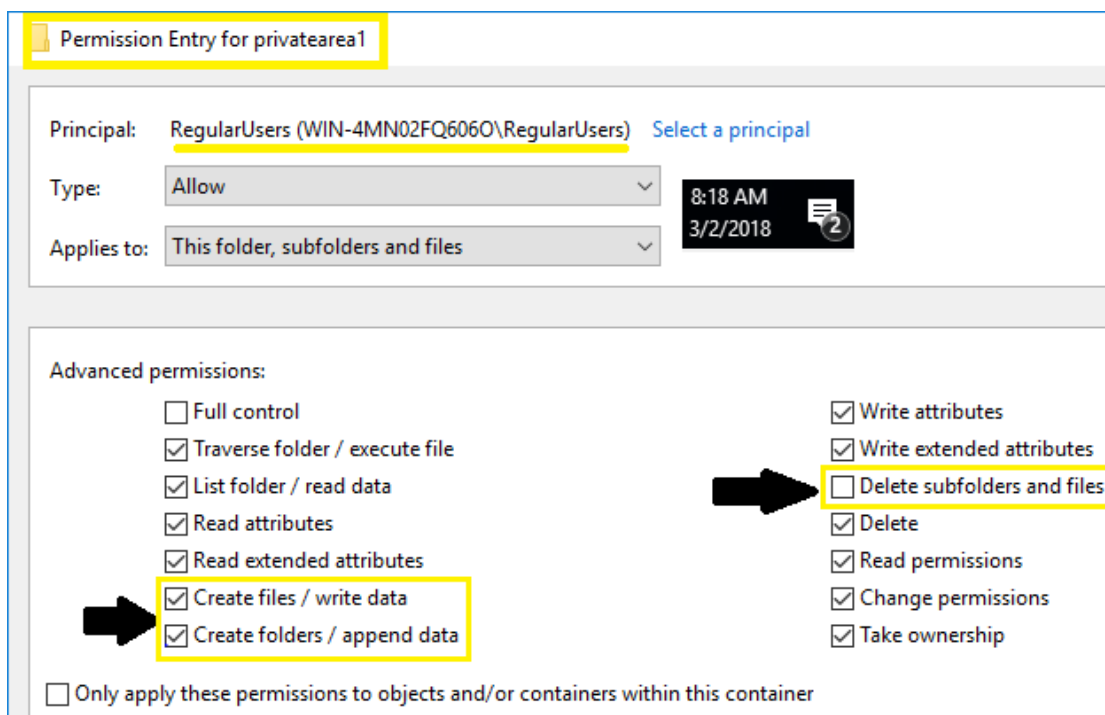
Εικόνα 4.1.2 : Καταχώρηση δικαιωμάτων για RegularUsers στην privateArea1



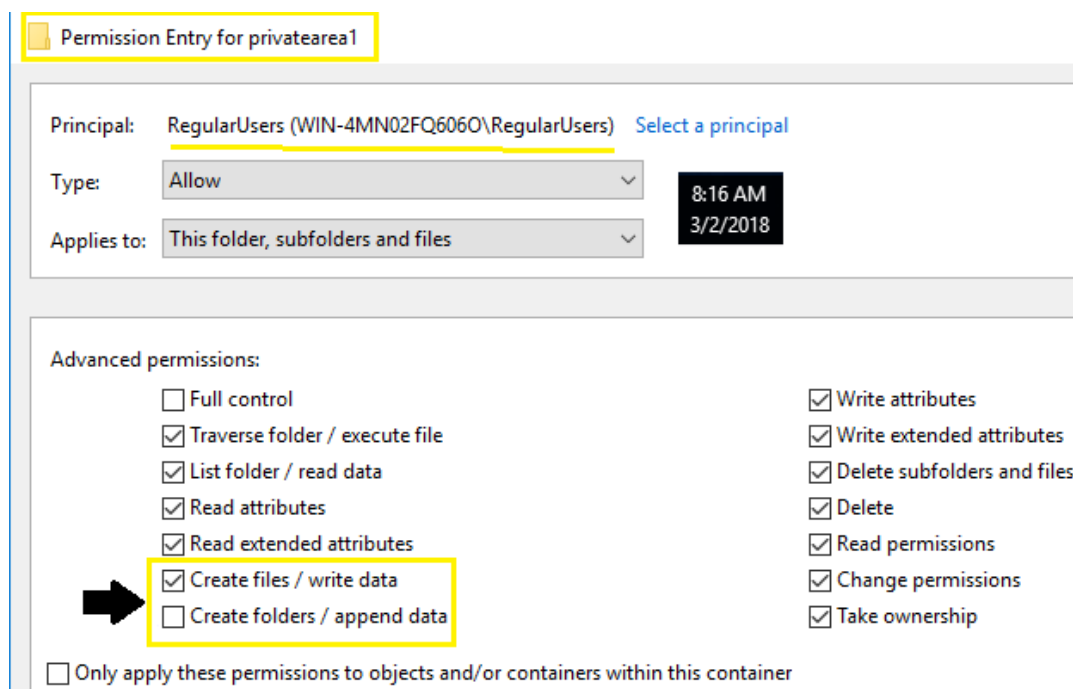
Εικόνα 4.1.3 : Απομόνωση δικαιωμάτων μόνο για RegularUsers



Εικόνα 4.1.4 : Καταχώρηση δικαιωμάτων για όλους στην privateArea1

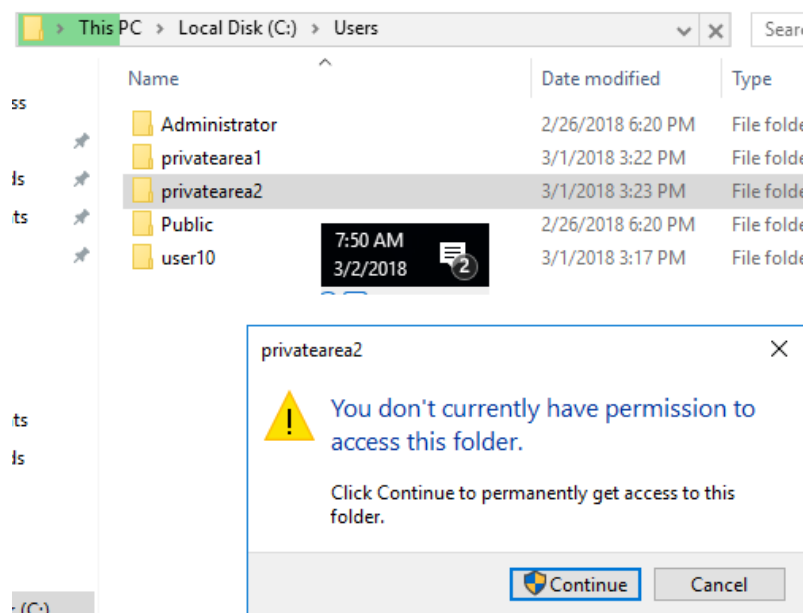


Εικόνα 4.1.5 : Απαγόρευση διαγραφής φακέλων



Εικόνα 4.1.6 : Απαγόρευση δημιουργίας φακέλου

Ακολουθούμε ακριβώς την ίδια διαδικασία για τη privateArea2 και το group NewRegularUsers.



Εικόνα 4.1.7 : Έλεγχος προσβασιμότητας



```
myadmintest@myadmin-VirtualBox: /home
myadmintest@myadmin-VirtualBox: /home$ sudo mkdir PrivateArea1
myadmintest@myadmin-VirtualBox: /home$ sudo mkdir PrivateArea2
myadmintest@myadmin-VirtualBox: /home$ sudo mkdir PublicArea1
myadmintest@myadmin-VirtualBox: /home$ sudo mkdir PublicArea2
myadmintest@myadmin-VirtualBox: /home$ ls
asd123  myadmintest  PrivateArea2  PublicArea2  user02  user10  usertest
myadmin PrivateArea1 PublicArea1  user01      user03  user11
myadmintest@myadmin-VirtualBox: /home$
```

Εικόνα 4.1.8 Δημιουργία φακέλων Groups

```
myadmintest@myadmin-VirtualBox: /home
myadmintest@myadmin-VirtualBox: /home$ sudo chown -R user01:RegularUsers PrivateArea1
myadmintest@myadmin-VirtualBox: /home$ sudo chown -R user01:RegularUsers PublicArea1
myadmintest@myadmin-VirtualBox: /home$ sudo chown -R user10:NewRegularUsers PublicArea2
myadmintest@myadmin-VirtualBox: /home$ sudo chown -R user10:NewRegularUsers PrivateArea2
myadmintest@myadmin-VirtualBox: /home$
```

Εικόνα 4.1.9 : Καθορισμός ιδιοκτήτη περιοχών

4.2 Καθορισμός επιπέδων πρόσβασης

Ο μηχανισμός με τον οποίο οι διανομές Unix καθορίζουν τα δικαιώματα σε περιοχές και αρχεία είναι το “**chmod**”. Οι 3 αριθμοί που ακολουθούν, χαρακτηρίζει ο καθένας τους από 3 πράγματα. Ο αριθμός 7 είναι ο μέγιστος και αυτό προκύπτει από το άθροισμα $4 + 2 + 1$. Κάθε ένας από τους 3 είναι ένα δικαίωμα. Το 1^ο είναι το read, το 2^ο το write (περιλαμβάνει και delete) και το 3^ο είναι το execute (τρέξιμο εφαρμογών). Αυτό για τον έναν από τους 3 αριθμούς του chmod. Ο κάθε ένας δείχνει σε ποιο group χρηστών αναφέρετε. Η πρώτη ομάδα είναι ο creator, η δεύτερη τα άτομα που ανήκουν στο group και τέλος οι υπόλοιποι (others). Με την εντολή “**chown**” καθορίζουμε δημιουργό.

```
myadmintest@myadmin-VirtualBox: /home
myadmintest@myadmin-VirtualBox: /home$ sudo chmod -R 770 PrivateArea1
myadmintest@myadmin-VirtualBox: /home$ sudo chmod -R 770 PrivateArea2
myadmintest@myadmin-VirtualBox: /home$
```

Εικόνα 4.2.1 : Καθορισμός δικαιωμάτων ομάδων

```
myadmintest@myadmin-VirtualBox: /home
myadmintest@myadmin-VirtualBox: /home$ sudo chmod -R 700 user01
myadmintest@myadmin-VirtualBox: /home$ sudo chmod -R 700 user02
myadmintest@myadmin-VirtualBox: /home$ sudo chmod -R 700 user03
myadmintest@myadmin-VirtualBox: /home$ sudo chmod -R 700 user10
myadmintest@myadmin-VirtualBox: /home$ sudo chmod -R 700 user11
myadmintest@myadmin-VirtualBox: /home$
```

Εικόνα 4.2.2 : Καθορισμός δικαιωμάτων για τους χρήστες του συστήματος



```
myadmintest@myadmin-VirtualBox: /home
user02@myadmin-VirtualBox:/home/PublicArea1$ su myadmintest
Password:
myadmintest@myadmin-VirtualBox:/home/PublicArea1$ cd ..
myadmintest@myadmin-VirtualBox:/home$ sudo chmod -R 777 PublicArea1
myadmintest@myadmin-VirtualBox:/home$ sudo chmod -R 777 PublicArea2
myadmintest@myadmin-VirtualBox:/home$ sudo chmod +t PublicArea1
myadmintest@myadmin-VirtualBox:/home$ sudo chmod +t PublicArea2
myadmintest@myadmin-VirtualBox:/home$ ls -la
total 56
drwxr-xr-x 14 root      root      4096 Μάρ  4 20:01 .
drwxr-xr-x 25 root      root      4096 Μάρ  2 22:17 ..
drwxr-xr-x  2          1005      4096 Φεβ 26 22:14 asd123
drwxr-xr-x 20 myadmin   myadmin   4096 Μάρ  4 18:29 myadmin
drwxr-xr-x 17 myadmintest myadmintest 4096 Μάρ  2 20:15 myadmintest
drwxrwx---  2 user01     RegularUsers 4096 Μάρ  4 20:06 PrivateArea1
drwxrwx---  2 user10     NewRegularUsers 4096 Μάρ  4 19:44 PrivateArea2
drwxrwxrwt  2 user01     RegularUsers 4096 Μάρ  4 20:05 PublicArea1
drwxrwxrwt  2 user10     NewRegularUsers 4096 Μάρ  4 20:24 PublicArea2
drwx----- 17 user01     user01      4096 Μάρ  4 20:05 user01
drwx-----  2 user02     user02      4096 Φεβ 27 00:00 user02
drwx-----  2 user03     user03      4096 Φεβ 26 22:01 user03
drwx-----  2 user10     user10      4096 Μάρ  4 19:22 user10
drwx-----  2 user11     user11      4096 Μάρ  4 19:26 user11
myadmintest@myadmin-VirtualBox:/home$
```

Εικόνα 4.2.3 : Προβολή τελικής εικόνας δικαιωμάτων ανά ομάδα

Τι θα αλλάζατε στα δικαιώματα πρόσβασης αν για κάποιο λόγο ο χρήστης user11 που ανήκει στην ομάδα NewRegularUsers θα έπρεπε προσωρινά να αποκλειστεί εντελώς από την πρόσβαση στην «αυστηρά ελεγχόμενη περιοχή εργασίας» της ομάδας του;

- Εάν για κάποιο λόγο ο χρήστης user11 ο οποίος ανήκει στην ομάδα NewRegularUsers χρειαστεί να αποκλειστεί τότε θα προσθέσω μια νέα ειδική ρύθμιση απευθύνοντας μόνο στον user11 και δεν θα του έδωνα δικαίωμα πρόσβασης στο αρχείο για κάποιο χρονικό διάστημα. (deny all).
- Στο Ubuntu θα τρέξουμε την εντολή “**setfacl -m u:user11:000 /home/privateArea2**”.Έπειτα μπαίνουμε ως user11 και ελέγχουμε την προσβασιμότητα του στην ομάδα όπου αποκλείστηκε.

```
user10@myadmin-VirtualBox: /home/PrivateArea2
user10@myadmin-VirtualBox:/home/PrivateArea2$ setfacl -m u:user11:000 /home/PrivateArea2
user10@myadmin-VirtualBox:/home/PrivateArea2$ su user11
Password:
user11@myadmin-VirtualBox:/home/PrivateArea2$ cd ..
user11@myadmin-VirtualBox:/home$ cd PrivateArea2
bash: cd: PrivateArea2: Permission denied
user11@myadmin-VirtualBox:/home$ logout
bash: logout: not login shell: use 'exit'
user11@myadmin-VirtualBox:/home$ exit
exit
user10@myadmin-VirtualBox:/home/PrivateArea2$ setfacl -x u:user11:000 /home/PrivateArea2
```

Εικόνα 4.2.4 : Ban user11 & έλεγχος προσβασιμότητας



Σε φακέλους στους οποίους έχουν αποκλειστική πρόσβαση μόνο τα μέλη της κάθε ομάδας, επιτρέπεται η δημιουργία μεμονωμένων υποφακέλων ή ακόμα και αρχείων στα οποία επιτρέπεται η πρόσβαση (ανάγνωση/εγγραφή) από χρήστες οι οποίοι δεν είναι μέλη της ομάδας; Περιγράψτε τη διαδικασία αν θεωρείτε ότι κάτι τέτοιο είναι δυνατό.

Στο Λ.Σ. Ubuntu κάτι τέτοιο είναι εφικτό. Ως δημιουργοί (user10) φτιάχνουμε έναν φάκελο με όνομα “folder” και του δίνουμε δικαιώματα με την εντολή «**chmod -R 777 folder**». Έπειτα με ένα “**ls -la**” εμφανίζονται όλα τα αρχεία και οι φάκελοι καθώς και τα δικαιώματα αυτών. Όπως φαίνεται και στο στιγμιότυπο παρακάτω ο φάκελος “folder” είναι προσβάσιμος σε όλους.

```
user10@myadmin-VirtualBox: /home/PrivateArea2
user10@myadmin-VirtualBox: /home/PrivateArea2$ mkdir folder
user10@myadmin-VirtualBox: /home/PrivateArea2$ ls -la
total 12
drwxrwx---+ 3 user10 NewRegularUsers 4096 Μάρ  4 20:51 .
drwxr-xr-x 14 root root 4096 Μάρ  4 20:01 ..
drwxrwxr-x 2 user10 user10 4096 Μάρ  4 20:51 folder
user10@myadmin-VirtualBox: /home/PrivateArea2$ chmod -R 777 folder
user10@myadmin-VirtualBox: /home/PrivateArea2$ ls -la
total 12
drwxrwx---+ 3 user10 NewRegularUsers 4096 Μάρ  4 20:51 .
drwxr-xr-x 14 root root 4096 Μάρ  4 20:01 ..
drwxrwxrwx 2 user10 user10 4096 Μάρ  4 20:51 folder
user10@myadmin-VirtualBox: /home/PrivateArea2$
```

Εικόνα 4.2.5 : Έλεγχος δικαιωμάτων δημιουργημένου φακέλου μετά τον καθορισμό τους.

```
user10@myadmin-VirtualBox: /home/PrivateArea2/folder$ chmod -R 777 test.txt
user10@myadmin-VirtualBox: /home/PrivateArea2/folder$ su user01
```

Εικόνα 4.2.6 : Καθορισμός δικαιωμάτων αρχείου

```
user01@myadmin-VirtualBox: /home$ cd PrivateArea2
bash: cd: PrivateArea2: Permission denied
user01@myadmin-VirtualBox: /home$ more PrivateArea2/folder/test.txt
more: stat of PrivateArea2/folder/test.txt failed: Permission denied
user01@myadmin-VirtualBox: /home$
```

Εικόνα 4.2.7 : Απόρριψη ανοίγματος αρχείου

4.3 Ερωτήματα 3^{ου} μέρους

Υπάρχει τρόπος να αποτραπεί η πρόσβαση σε μια συγκεκριμένη περιοχή από τους διαχειριστές του συστήματος (System Administrator); Υπάρχει η δυνατότητα ο διαχειριστής να παρακάμψει τα δικαιώματα πρόσβασης που έχουν οριστεί; Περιγράψτε αντίστοιχο σενάριο και για τα 2 Λ.Σ.

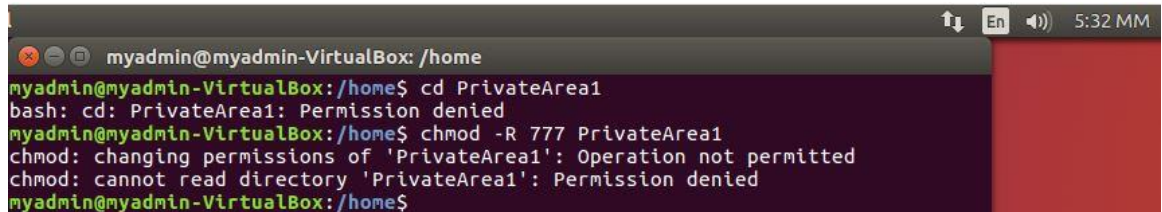
- Είναι εφικτό κάποιος χρήστης να αποκλείσει την πρόσβασή από τον Administrator σε κάποιο αρχείο του αλλά αυτό είναι προσωρινό. Έτσι μπορεί βέβαια στο tab-> security να αφαιρέσει όλα τα μέλη από την λίστα δικαιωμάτων και να αφήσει μέσα μόνο τον εαυτό του. Παρόλα αυτά ο διαχειριστής χάρη στην ιεραρχία που κατέχει στο σύστημα μπορεί οποιαδήποτε στιγμή να μπει στον φάκελο παίρνοντας δικαιώματα διαχειριστή και να αλλάξει τα δικαιώματα πρόσβασης από το tab security του φακέλου.



- Για τα ubuntu συνδεόμαστε με τον user01 που γνωρίζουμε ότι είναι ο δημιουργός της περιοχής privateArea1. Αποκλείουμε τον χρήστη myadmin (διαχειριστής) και ξανασυνδεόμαστε ως myadmin. Βλέπουμε ότι η προσπέλαση της περιοχής είναι αδύνατη. Εξετάζουμε λοιπόν και την περίπτωση να μπορεί να αλλάξει τα δικαιώματα του φακέλου, αλλά δεν επιτρέπεται επίσης.

```
user01@myadmin-VirtualBox:/home$ setfacl -m u:myadmin:000 /home/PrivateArea1
```

Εικόνα 4.3.1 : Αποκλεισμός διαχειριστή από την περιοχή privateArea1



Εικόνα 4.3.2 : Έλεγχος αποκλεισμού & προσπάθεια ανάκτησης πρόσβασης

Τι δικαιώματα πρέπει να δώσετε σε ένα φάκελο έτσι ώστε:

α) να μην μπορεί κάποιος να δημιουργήσει νέους υποφακέλους αλλά μόνο αρχεία.

β) να μην είναι ικανός κάποιος να σβήσει αρχεία ή υποφακέλους, αλλά μόνο να προσθέσει ή να δημιουργήσει νέα αρχεία και νέους υποφακέλους.

- Για τα windows και το ερώτημα α η απάντηση είναι στο στιγμιότυπο 4.1.6. Για το ερώτημα β αντίστοιχα στο 4.1.5.
- Για τα ubuntu φαίνεται στο στιγμιότυπο 4.2.3 με την τεχνική “*sticky bit*”. Χαρακτηρίζεται από το χαρακτήρα “*t*” στο τέλος της συμβολοσειράς δικαιωμάτων όπου αντικατέστησε το x.

Ποια είναι η χρησιμότητα των πρόσθετων ειδικών δικαιωμάτων που παρέχονται σε ένα Λ.Σ. Linux, δηλαδή των δικαιωμάτων Set User ID (SUID), Set Group ID (SGID), και Sticky bit (STB); Περιγράψτε και εφαρμόστε κατάλληλα πραγματικά σενάρια στα οποία να είναι απαραίτητη η χρήση των συγκεκριμένων δικαιωμάτων πρόσβασης.

- Το SUID είναι ένας ειδικός τύπος δικαιωμάτων που δίνονται σε ένα αρχείο. Συγκεκριμένα όταν ένα πρόγραμμα εκτελείτε κληρονομεί τα δικαιώματα του χρήστη που είναι συνδεδεμένος στο σύστημα. Οπότε είναι μία προσωρινή κατάσταση καταχώρησης δικαιωμάτων στο χρήστη που είναι συνδεδεμένος με τα δικαιώματα του δημιουργού και όχι αυτού που το τρέχει. Για παράδειγμα θέλουμε να αλλάξουμε τον κωδικό μας με την χρήση της εντολής “*passwd*” (δημιουργός root). Η ενέργεια αυτή θα επηρεάσει περισσότερο το ενός αρχείου χωρίς την γνώση του χρήστη ,αρχεία που σε καμία περίπτωση δεν μπορεί να διαβάσει τροποποιήσει με άλλο τρόπο ο χρήστης (εφόσον δεν είναι root). Καταλήγουμε στο γεγονός ότι αν αφαιρούσαμε την επιλογή που μας δίνει το SUID δεν ήταν δυνατή η πραγματοποίηση της αλλαγής του κωδικού αφού δεν θα γίνονταν οι αλλαγές που δεν είναι εμφανής στο user. Αφορά την πρώτη ομάδα δικαιωμάτων από τις 3.
- Αντίστοιχα και το SGID είναι το ίδιο πράγμα αλλά αφορά groups και όχι user μεμονωμένα. Από αυτό απορρέει ότι αλλάζεις την δεύτερη ομάδα δικαιωμάτων.



321-3404 Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: Μελέτη βασικών μηχανισμών ασφάλειας των λειτουργικών συστημάτων Windows Server & Linux

Αντωνιάδης Χαράλαμπος icsd10011 , Ευκαρπίδης Κωνσταντίνος icsd15051 , Ζιώζας Γεώργιος icsd15058

- Το sticky bit αφορά τον περιορισμό στο σβήσιμο φακέλων. Όταν αυτό είναι ενεργοποιημένο τότε οι χρήστες σχεδόν πλήρη δικαιώματα. Δηλαδή μπορούν να διαβάσουν αρχεία ,να εκτελέσουν εφαρμογές, να δημιουργήσουν και να τροποποιήσουν αρχεία μέσα στο φάκελο για τον οποίο ισχύει το sticky bit , αλλά σε καμία περίπτωση δεν μπορούν να διαγράψουν αρχεία από το φάκελο και προφανώς τον ίδιο το φάκελο.

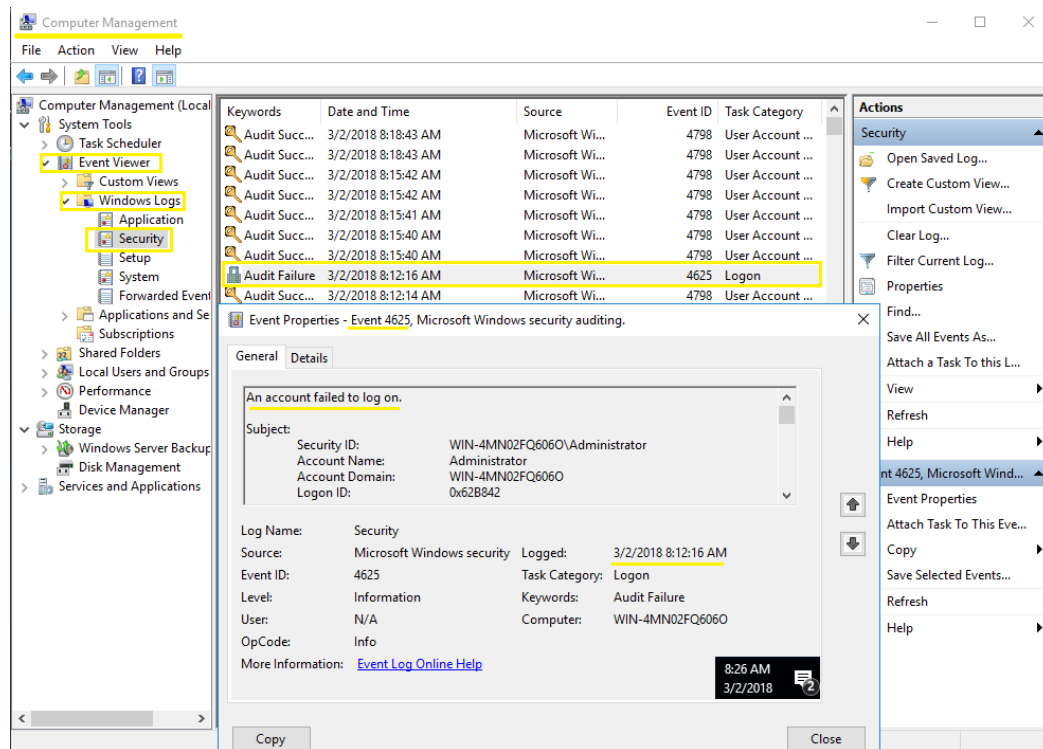


5 Μέρος 4^ο - Καταγραφή & παρακολούθηση ενεργειών χρήστη

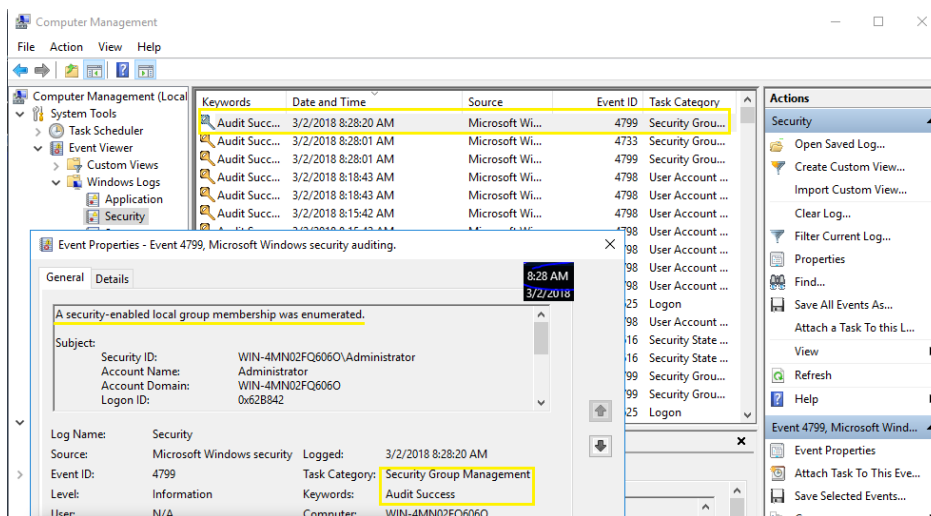
Στο τέταρτο κομμάτι της εργασίας ασχολούμαστε με τους μηχανισμούς καταγραφής συμβάντων των δύο Λ.Σ.

5.1 Μηχανισμοί καταγραφής συμβάντων

- Για το λειτουργικό Windows υπάρχει ως μηχανισμός καταγραφής συμβάντων το Security Log, το οποίο υπάρχει στην εφαρμογή “Computer Management” στην ενότητα “Event Viewer”. Έπειτα στην υποενότητα “Windows Logs” και “Security”. Με δύο στιγμιότυπα έχουμε αποθανάτισει ένα συμβάν αποτυχημένης προσπάθειας εισόδου και ένα event απαρίθμησης των μελών ενός group με δυνατότητα ασφαλείας.



Εικόνα 5.1.1 : Λεπτομέρειες καταγεγραμμένου συμβάντος



Εικόνα 5.1.2 : Συμβάν που προκαλέσαμε

- Στα ubuntu υπάρχει μία πιο επαρκής λίστα μηχανισμών καταγραφής των γεγονότων αλλά με λιγότερο κατανοητά logs. Επίσης υπάρχουν αρχεία τα οποία δεν ανοίγουν με κάποιον edit αλλά με έτοιμα scripts. Να πούμε ότι ανά κάποιες παραμέτρους (ανάλογα το είδος του log) δημιουργείτε νέο πακέτο logs την μορφής πχ. access_log.2.gz. Για να αποφύγουμε την εκτενή και κουραστική εμφάνιση 20 στιγμιότυπων φτιάξαμε έναν πίνακα με τα όνομα των αρχείων, το που βρίσκονται καθώς και τον τρόπο εκτέλεσης.

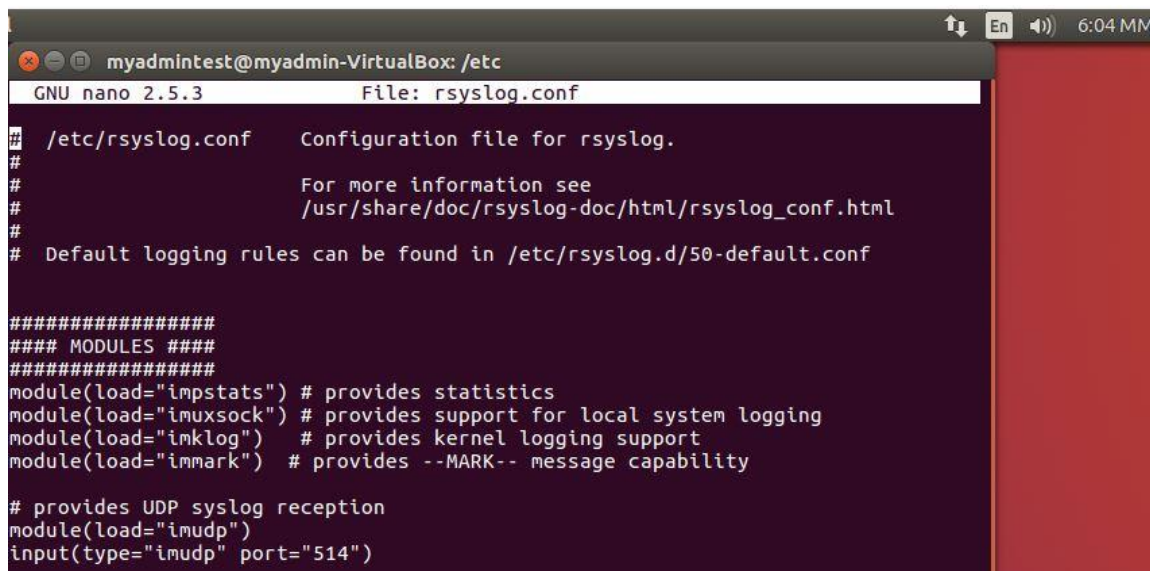
Όνομα Αρχείου	Περιοχή	Τρόπος αναπαράστασης
access_log	/var/log/cups	“more”
kern_log	/var/log	“more”
history_log	/var/log/apt	“more”
term_log	/var/log/apt	“more”
dpkg_log	/var/log	“more”
chasper_log	/var/log/installer	“more”
X.org_log	/var/log	“more”
auth_log	/var/log	“more”
lightdm_log	/var/log/lightdm	“gedit”
seat0_greeter_log	/var/log/lightdm	“gedit”
apport_log	/var/log	“gedit”
error_log	/var/log/cups	“nano”
wtmp	/var/log	“last”

Πίνακας 5.1.3 : Αρχεία καταγραφής συμβάντων



5.2 Χρήση Syslog Daemon & έλεγχος λειτουργίας με παράδειγμα

Ο δαίμονας syslog είναι πάρα πολύ χρήσιμος για τους χρήστες του συστήματος. Δίνει την δυνατότητα παραμετροποίησης του βασικού αρχείου που χρησιμοποιεί ως οδηγό ο δαίμονας. Με αυτό τον τρόπο μπορούμε να φτιάξουμε δικά μας scripts καταγραφής γεγονότων που θα του ορίσουμε. Από default έχει προκαθορισμένους μηχανισμούς χωρίς να χρειάζεται να του ορίσουμε εμείς, όπως καταγραφή εισόδου χρηστών στο σύστημα, αποτυχημένων προσπαθειών, updates, upgrades, kernel κινήσεις, και πάρα πολλά ακόμη. Για να αλλάξουμε τις πολιτικές αυτού του δαίμονα έπρεπε να ανοίξουμε με nano το αρχείο `/etc/rsyslog.conf`. Έπειτα ενεργοποιήσαμε το module `"immark"`.



```
myadmintest@myadmin-VirtualBox: /etc
GNU nano 2.5.3 File: rsyslog.conf

# /etc/rsyslog.conf Configuration file for rsyslog.
#
# For more information see
# /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf

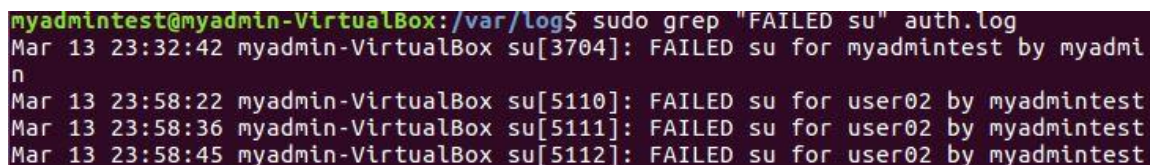
#####
### MODULES ###
#####
module(load="imstats") # provides statistics
module(load="imuxsock") # provides support for local system logging
module(load="imklog") # provides kernel logging support
module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")
```

Εικόνα 5.2.1 : Παραμετροποίηση rsyslog αρχείου

5.3 Ενεργοί χρήστες & προσπάθεια εισβολής ως root

Για να ενημερωθούμε για τους ενεργούς χρήστες του συστήματος και το ποιοι έχουν συνδεθεί και για πόσο πληκτρολογούμε στο τερματικό `"w"` & `"who"`. Επίσης για να δούμε ποιοι χρήστες έχουν αποτύχει να συνδεθούν στο σύστημα μας τρέχουμε `"faillog -a"`. Όσων αφορά το ερώτημα για καταγραφή αποτυχημένων προσπαθειών εισόδου χρηστών ως διαχειριστές η απάντηση είναι ναι. Η πληροφορία αυτή εμπεριέχεται στο αρχείο `auth.log` το οποίο τρέχουμε με την εντολή `"sudo grep 'FAILED su' auth.log"`. Του ζητάμε δηλαδή να μας εμφανίσεις τις αποτυχημένες su προσπάθειες. Βλέπουμε ότι ο user02 προσπάθησε να συνδεθεί 3 φορές ως διαχειριστής.



```
myadmintest@myadmin-VirtualBox: /var/log$ sudo grep "FAILED su" auth.log
Mar 13 23:32:42 myadmin-VirtualBox su[3704]: FAILED su for myadmintest by myadmi
n
Mar 13 23:58:22 myadmin-VirtualBox su[5110]: FAILED su for user02 by myadmintest
Mar 13 23:58:36 myadmin-VirtualBox su[5111]: FAILED su for user02 by myadmintest
Mar 13 23:58:45 myadmin-VirtualBox su[5112]: FAILED su for user02 by myadmintest
```

Εικόνα 5.3.1 : Αποτυχημένες προσπάθειες χρηστών σύνδεσης ως root



6 Μέρος 5^ο - Σύγκριση των δύο Λειτουργικών Συστημάτων

Η σύγκριση των δύο λειτουργικών αποτελεί το τελευταίο κομμάτι της 1^{ης} εργαστηριακής άσκησης.

Πόσο διαφορετικοί θεωρείτε ότι είναι οι μηχανισμοί και το επίπεδο ασφαλείας που παρέχονται σε ένα Linux σύστημα σε σχέση με ένα Λ.Σ. Windows;

Και τα δύο λειτουργικά παρέχουν πληθώρα μηχανισμών που μπορούμε να πούμε ότι πλησιάζουν αρκετά. Η διαφορά σ' αυτό το κομμάτι είναι ότι η κάθε εταιρία χρησιμοποιεί τον δικό της μηχανισμό όπως UAC για τα Windows και DAC, MAC για τα Ubuntu. Μία άλλη διαφορά είναι στα windows τα περισσότερα εργαλεία, αν όχι όλα, είναι ήδη εγκατεστημένα ενώ στα ubuntu πρέπει να κατεβάσεις πολύ υλικό.

Πόσο διαφορετική είναι η διαχείριση των μηχανισμών αυτών στα Windows, σε σύγκριση με τη διαχείριση σε Linux σύστημα;

Στα windows οποιαδήποτε παραμετροποίηση γίνεται εύκολα μέσω του γραφικού περιβάλλοντος σε αντίθεση με τα ubuntu στα οποία παρά το γραφικό περιβάλλον ορισμένες αλλαγές πραγματοποιούνται μόνο στο τερματικό. Αυτό έχει ως αποτέλεσμα το Λ.Σ. Windows Server να είναι πιο προσιτό και φιλικό προς τον χρήστη. Αντίθετα τα ubuntu απαιτούν να έχεις μία πιο σημαντική εξοικείωση.

Ποιο σύστημα διαχείρισης θα λέγατε ότι είναι ευκολότερο για έναν διαχειριστή; Ποιο θεωρείται ότι είναι αποτελεσματικότερο για τα σενάρια που μελετήσατε;

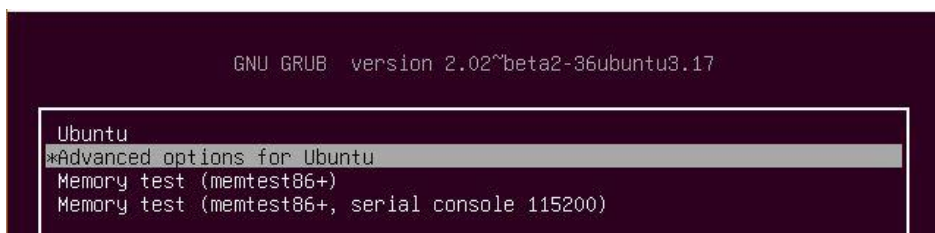
Όπως αναφέραμε και παραπάνω η πραγματοποίηση παραμετροποιήσεων μέσω GUI διευκολύνει πολύ την δουλειά ενός διαχειριστή, συνεπώς θα προτείνουμε Windows Server. Για τα σενάρια που μελετήσαμε αφού πραγματοποιούνται και στα 2 Λ.Σ. εξαρτάται από την εξοικείωση του χρήστη με το κάθε λειτουργικό.

Τέλος, να επισημάνουμε πως το Linux σύστημα είναι ανοιχτού κώδικα (open source), που σημαίνει πως όλη η παραμετροποίηση ασφαλείας είναι ανοιχτή στο καθένα να την ελέγξει και πολλοί συμφωνούν πως γίνονται σωστά όλες οι διαδικασίες για την καλύτερη δυνατή ασφάλεια. Ενώ στα Windows ο κώδικας είναι κρυφός (Security by Obscurity) και δεν έχουν ελεγχθεί μαζί τα μέτρα ασφαλείας από πλευράς κώδικα, με αποτέλεσμα να υπάρχει πιθανό κενό ασφαλείας που να μην έχει βρεθεί ακόμα, ή ακόμα χειρότερα να το εκμεταλλεύονται τρίτοι εν αγνοία της ίδιας της εταιρίας.

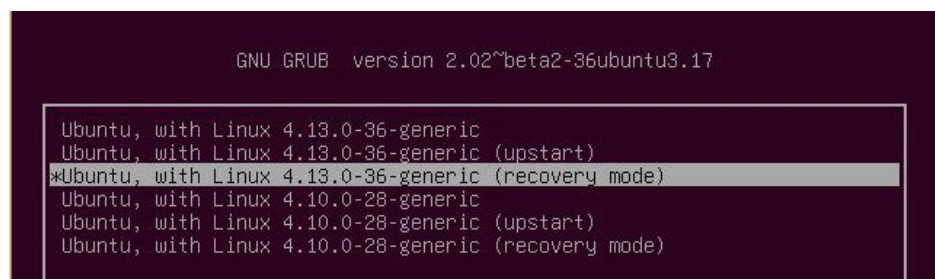


7 Recovery Mode

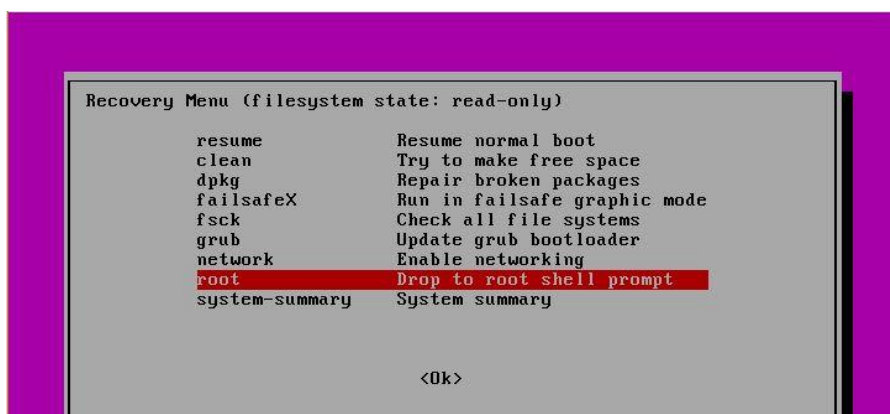
Κατά την υλοποίηση της εργασίας στο Λ.Σ. Ubuntu αντιμετωπίσαμε ένα πρόβλημα με το κλείδωμα των λογαριασμών των διαχειριστών. Έτσι λοιπόν δεν μπορούσαμε να πραγματοποιήσουμε “sudo” εντολές και αυτό είχε ως συνέπεια να έπρεπε να ξανασετάρουμε από την αρχή το λειτουργικό. Για να αποφύγουμε αυτήν την «επίπονη» διαδικασία βρήκαμε ότι μπορείς να μπεις σε ένα μηχανισμό των Linux ,εν ονόματι **GNU GRUB** το οποίο περιέχει και το recovery mode, και να συνδεθείς ως root χωρίς κωδικό. Αν φτάναμε σε εκείνο το στάδιο μετά έμενε μόνο να ξεκλειδώσουμε τους users ,κάτι το οποίο θα ήταν εφικτό που θα είχαμε δικαιώματα διαχειριστή. Για να μεταβούμε στην οθόνη 7.1 πρέπει να κρατήσεις πατημένο το shit κατά το boot του machine και πριν την εμφάνιση του ubuntu logo με τα 4 dots.



Εικόνα 7.1 : Advanced options



Εικόνα 7.2 : Επιλογή πιο πρόσφατης έκδοσης recovery mode



Εικόνα 7.3 : Επιλογή σύνδεσης ως root



```
Press Enter for maintenance
(or press Control-D to continue):
root@myadmin-VirtualBox:~# mount -o remount,rw /
root@myadmin-VirtualBox:~# faillog -u myadmin -r
[ TIME ] Timed out waiting for device dev-di...
x2dbe6f\x2d707a4b8f885c.device.
[DEPEND] Dependency failed for /dev/disk/by-...6b1-5e52-4e43-be6f-707a4b8f885c.
[DEPEND] Dependency failed for Swap.

root@myadmin-VirtualBox:~# faillog -u myadmin -r
root@myadmin-VirtualBox:~# faillog -u myadmin -r
root@myadmin-VirtualBox:~#
```

Εικόνα 7.4 : Επιλογή mount για read & write στο δίσκο , ξεκλείδωμα λογαριασμών

Θεωρήσαμε σημαντικό να επισυνάψουμε αυτήν την διαδικασία.



8 Βιβλιογραφία

- ~Science Buddies. “MD5 encryption”. 2002. <<http://www.md5online.org/md5-encrypt.html>>.
- ~Ubuntu. “dpkg – Package Management”. 2017. <<https://help.ubuntu.com/its/serverguide/dpkg.html>>.
- ~Jackbravo. “Linux Log Files”. 23 January 2015. <<https://help.ubuntu.com/community/LinuxLogFiles>>.
- ~Unknown. “Faillog – the log of failed login attempts”. 2010. <<https://linux.die.net/man/8/faillog>>.
- ~Amo-ej1. “X.org.0.log file and information”. 25 August 2008. <<https://ubuntuforums.org/showthread.php?t=900245>>.
- ~Rinzwind. “GPU manager”. 18 August 2016. <<https://askubuntu.com/questions/813826/what-does-gpu-manager-do>>.
- ~Rsyslog. “Tools – Config Builder”. 2018. <<https://www.rsyslog.com/rsyslog-configuration-builder/>>.
- ~Gibson Research. “Remote system event logging”. 2016. <https://www.grc.com/port_514.html>.
- ~Oli. “Login history location”. 13 December 2013. <<https://askubuntu.com/questions/390201/how-to-see-login-history>>.
- ~Pavlos G. “Users connected to the system”. 7 June 2011. <<https://askubuntu.com/questions/45238/how-can-i-know-the-username-connected-to-my-system>>.
- ~Dustin Puryear. “Comparing Access Control in Windows and Linux”. 8 June 2010. <<https://www.networkworld.com/article/2230977/microsoft-subnet/comparing-access-control-in-windows-and-linux.html>>.
- ~Vasudevan Nagendra & Yaohui Chen. “Access Control Lists in Linux & Windows”. 2014. <https://compas.cs.stonybrook.edu/~nhonarmand/courses/fa14/cse506.2/slides/ACLs-Vasu_and_Yaohui.pdf>.
- ~Mikel. “Encryption methods for /etc/passwd file”. 26 February 2016. <<https://unix.stackexchange.com/questions/8229/what-methods-are-used-to-encrypt-passwords-in-etc-passwd-and-etc-shadow>>.
- ~Surendra Anne. “Sticky Bit, SUID & SGID”. 1 Jan 2012. <<https://www.linuxnix.com/sticky-bit-set-linux/>>.
- ~TechNet. Microsoft. “Security Account Manager (SAM)”. 11 April 2014. <[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server2003/cc756748\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server2003/cc756748(v=ws.10))>.



~ Eli the Computer Guy. “File and Share Permissions”. 16 April 2013.

< <https://www.youtube.com/watch?v=fJHFmt6F0Rc&t=1297s>>.

~Brian Lich & Justinha. “Security Options”. 8 January 2017. < <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/security-options>>.

~Microsoft. “Security Configuration Tool Set”. 12 September 2009.

<[https://docs.microsoft.com/enus/previousversions/windows/itpro/windowsserver2000/bb742512\(v=technet.10\)](https://docs.microsoft.com/enus/previousversions/windows/itpro/windowsserver2000/bb742512(v=technet.10))>.

~Microsoft. “Configuring User Right”. 2000. < <https://technet.microsoft.com/en-us/library/dd277404.aspx>>.

~Andrei Miroshnikov & Justinha. “A security-enabled local group membership was enumerated”. 19 April 2017. <<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4799>>.

~David Schuetz. “Rainbow Tables for Unix DES Crypt (3) Hashes”. 22 December 2010. <<https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2010/december/rainbow-tables-for-unix-des-crypt3-hashes/>>.

~OpenWall.com. “John the Ripper”. 29 May 2013. <<http://www.openwall.com/john/doc/EXAMPLES.shtml>>.

~Justin Ellingwood. “System Users in Linux on Ubuntu”. 5 September 2013. <<https://www.digitalocean.com/community/tutorials/how-to-view-system-users-in-linux-on-ubuntu>>.

~Vivek Gite. “Faillog in Linux: Display Records of Login Failure”. 26 April 2011. <<https://www.cyberciti.biz/faq/faillog-in-linux-command/>>.

~ Michael Boelen. “File permissions of the /etc/shadow password file”. 21 January 2016. <<https://linux-audit.com/file-permissions-of-the-etc-shadow-password-file/>>.