
Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Αναφορά 1ης Εργαστηριακής Άσκησης
– Μέρος Πρώτο –
Υλοποίηση Εξυπηρετητή Linux

Αυλακιώτης Χρήστος – 321/2012015
Κατσιβέλης Κων/νος – 321/2011063
Φιωτάκης Γιώργος – 321/2013220

A1. Αρχικά δημιουργήσαμε ένα virtual machine και εγκαταστήσαμε το λειτουργικό Ubuntu 12.04.5 LTS

A2. Κάναμε εγκατάσταση του ssh server με την εντολή:

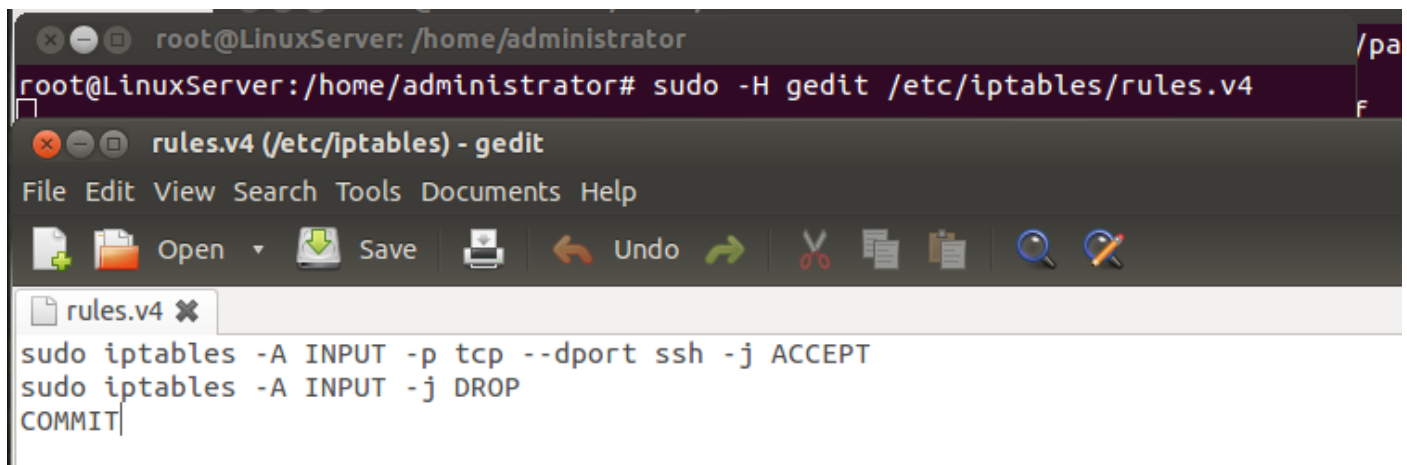
```
sudo apt-get install openssh-server
```

Έπειτα κάναμε εγκατάσταση των iptables persistent με την εντολή:

```
sudo apt-get install iptables-persistent
```

ώστε να μπορούμε να παραγοντοποιήσουμε τους κανόνες και να αποθηκεύσουμε τις ρυθμίσεις αυτές .

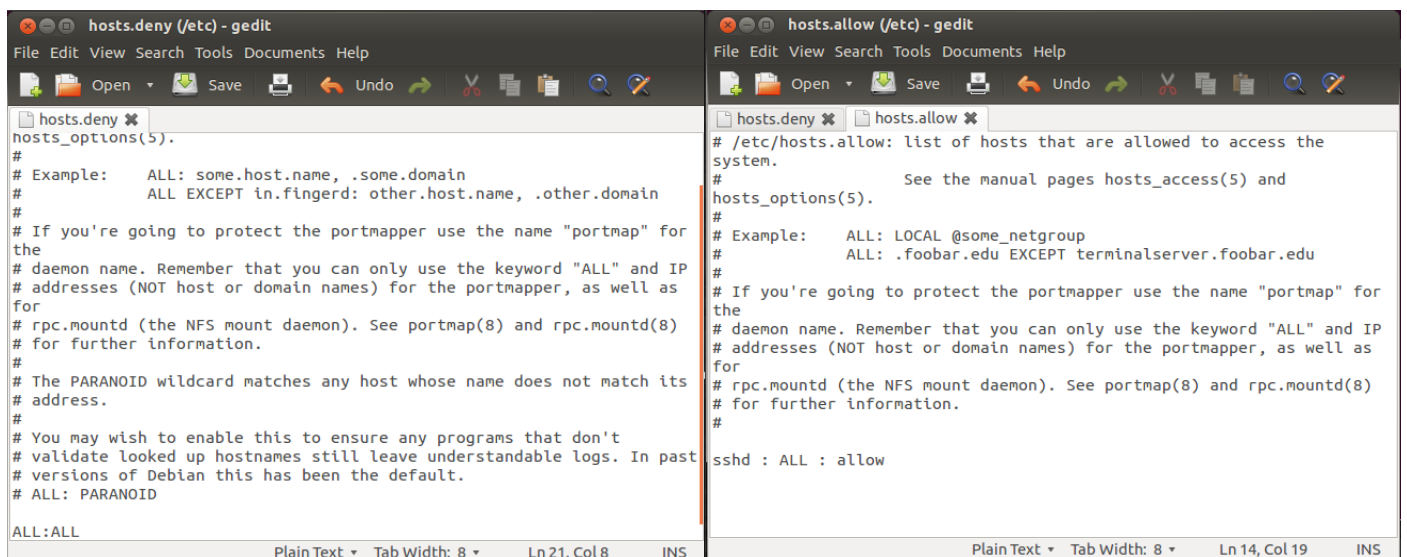
Επιετά προσθέσαμε του δυο παρακάτω κανόνες στο αρχείο /etc/iptables/rules.v4 ώστε να απαγορεύονται όλες οι συνδέσεις που γίνονται προς τον εξυπηρετητή εκτός από τις ssh



```
root@LinuxServer: /home/administrator
root@LinuxServer:/home/administrator# sudo -H gedit /etc/iptables/rules.v4

rules.v4 (/etc/iptables) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT
sudo iptables -A INPUT -j DROP
COMMIT
```

Επίσης απαγορέψαμε όλες τις συνδέσεις εκτός από τις ssh στα αρχεία hosts.deny και hosts.allow:



```
hosts.deny (/etc) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
hosts_options(5).
# Example: ALL: some.host.name, .some.domain
# ALL EXCEPT in.fingerd: other.host.name, .other.domain
# 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.
# 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
ALL:ALL

hosts.allow (/etc) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
# /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 : ALL : allow
```

Και για μεγαλύτερη ασφάλεια πήγαμε στο αρχείο /etc/ssh/sshd_config και προσθέσαμε/αλλάξαμε τις γραμμές:

- PermitRootLogin no
- DebianBanner no
- AllowUsers administrator,ftpadmin,professor,seics12015,secis11063,seics13220

Και δοκιμάσαμε σύνδεση sash από άλλον υπολογιστή

```
root@kali:~/Desktop# ssh administrator@192.168.1.108
The authenticity of host '192.168.1.108 (192.168.1.108)' can't be established.
ECDSA key fingerprint is SHA256:B45E9f2/h8l1hdXKa/ekhnRoqD3qCoYPkIXi5W5AL0Q.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.108' (ECDSA) to the list of known hosts.
administrator@192.168.1.108's password:
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2017.

Last login: Mon Mar 28 08:01:29 2016 from viki.local
administrator@LinuxServer:~$ sudo su
[sudo] password for administrator:
root@LinuxServer:/home/administrator#
```

B1. Για την απενεργοποίηση των services εγκαταστήσαμε το [rcconf](#) με την εντολή:

```
sudo apt-get install rcconf
```

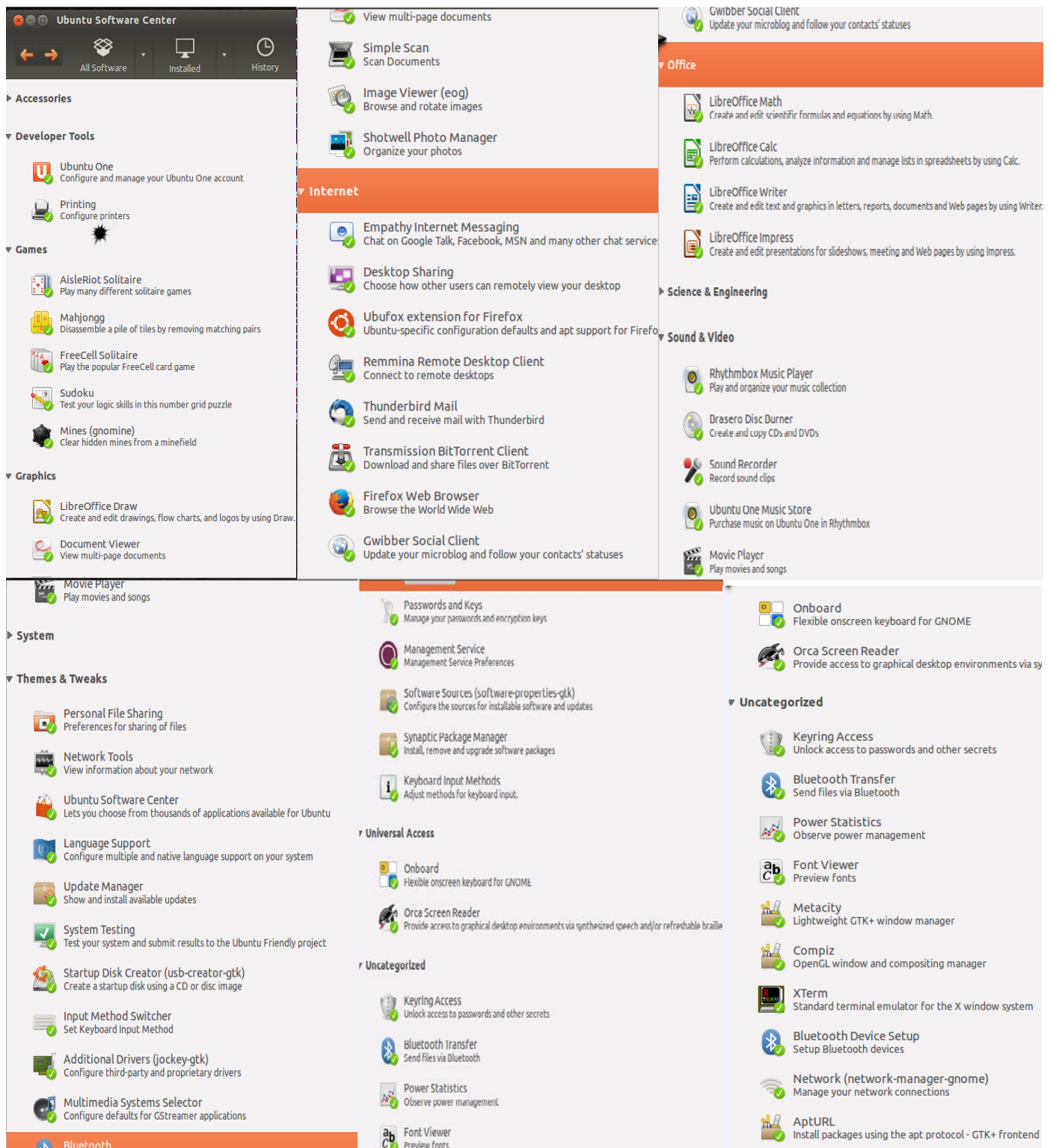
Για να δούμε τη λίστα με τις υπηρεσίες τρέξαμε την εντολή:

```
rcconf --list --expert
```

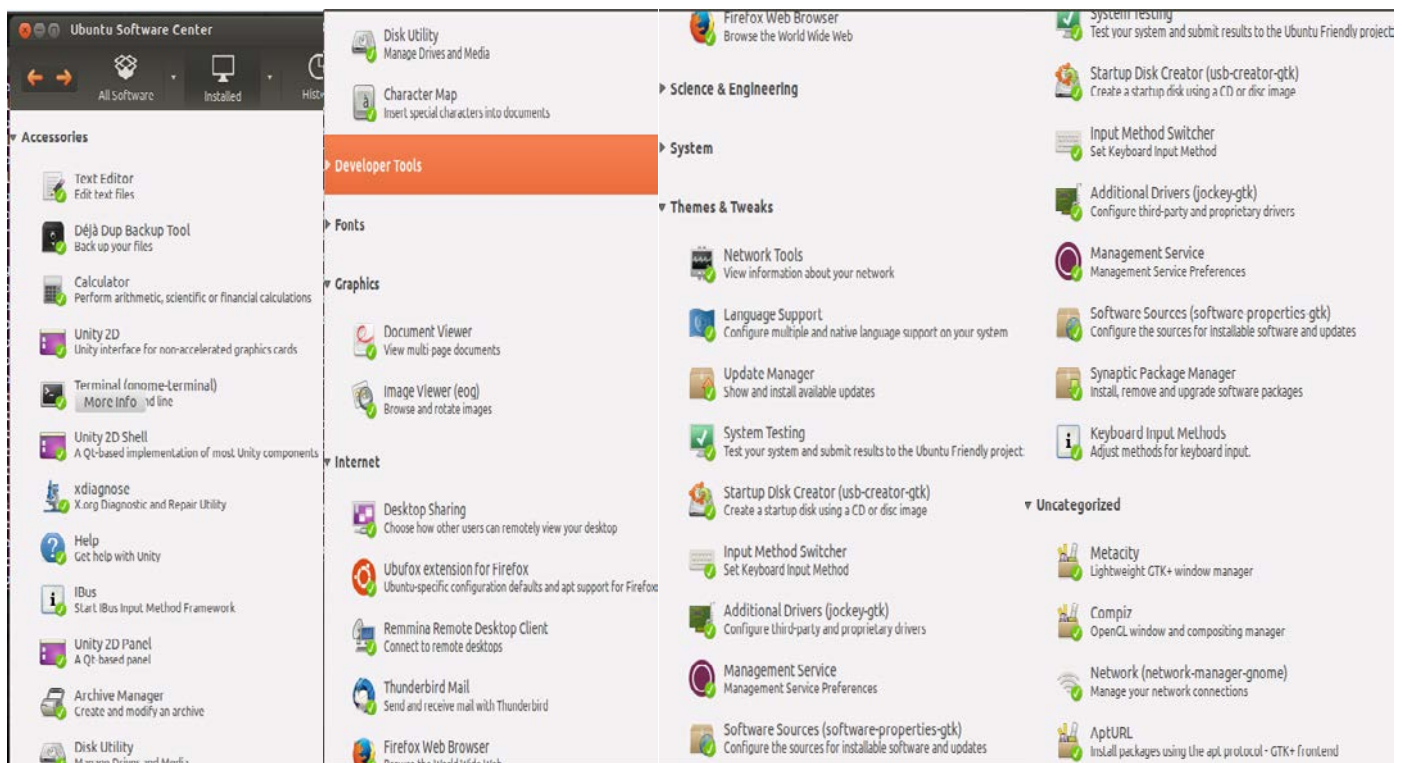
Από τις υπηρεσίες, κρίναμε πως δε θέλουμε στο σύστημα μας την [speech-dispatcher](#) την οποία αποκαταστήσαμε με την εντολή: `rcconf --off speech-dispatcher`

```
root@LinuxServer:/home/administrator# rcconf --off speech-dispatcher
update-rc.d: warning: speech-dispatcher start runlevel arguments (none) do not match LSB Default
-Start values (2 3 4 5)
update-rc.d: warning: speech-dispatcher stop runlevel arguments (0 1 2 3 4 5 6) do not match LSB
Default-Stop values (0 1 6)
Adding system startup for /etc/init.d/speech-dispatcher ...
/etc/rc0.d/K00speech-dispatcher -> ../init.d/speech-dispatcher
/etc/rc1.d/K00speech-dispatcher -> ../init.d/speech-dispatcher
/etc/rc2.d/K00speech-dispatcher -> ../init.d/speech-dispatcher
/etc/rc3.d/K00speech-dispatcher -> ../init.d/speech-dispatcher
/etc/rc4.d/K00speech-dispatcher -> ../init.d/speech-dispatcher
/etc/rc5.d/K00speech-dispatcher -> ../init.d/speech-dispatcher
/etc/rc6.d/K00speech-dispatcher -> ../init.d/speech-dispatcher
root@LinuxServer:/home/administrator# rcconf --list --expert
ondemand on
apparmor on
killprocs on
rsync on
urandom on
iptables-persistent on
vboxadd-service on
cryptdisks on
x11-common on
umountnfs.sh on
saned on
pulseaudio on
mountnfs on
```

B2. Για να απενεργοποιήσουμε τα προγράμματα που δε χρειαζόμαστε πήγαμε στο πρόγραμμα Ubuntu Software Center στη καρτέλα Installed όπου βρήκαμε πολλές άχρηστες εφαρμογές που εγκαταστάθηκαν με το λειτουργικό σύστημα.



Από αυτές αποκαταστήσαμε αρκετές και αφήσαμε μόνο τις απαραίτητες

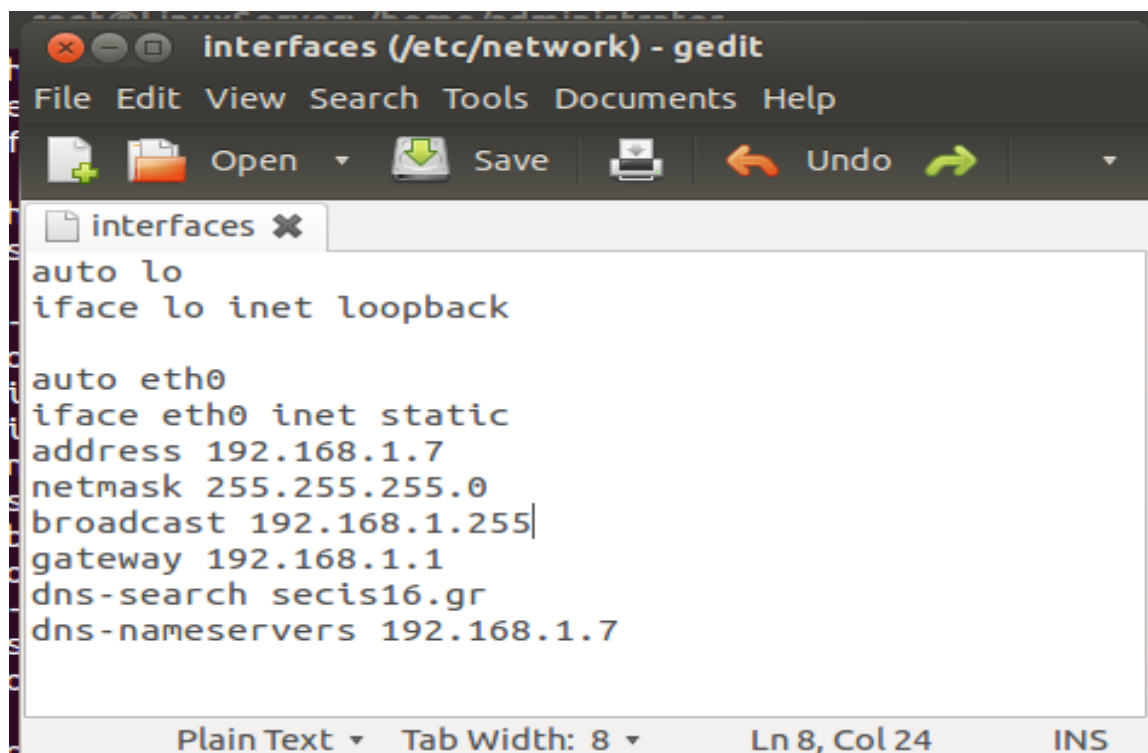


B3.

Υπηρεσία DNS:

Εγκαταστήσαμε το bind9 με την εντολή:

```
sudo apt-get install bind9
```




```
named.conf.local (/etc/bind) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
interfaces x named.conf.local x
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "secis16.gr" {
    type master;
    file "/etc/bind/db.secis16";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.secis16.rev";
};
```

```
db.secis16 (/etc/bind) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
interfaces x named.conf.local x db.secis16 x
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      www.secis16.gr. root.www.secis16.gr. (
                                2           ; Serial
                                604800      ; Refresh
                                86400       ; Retry
                                2419200     ; Expire
                                604800 )    ; Negative Cache TTL
;
@         IN      NS       www.secis16.gr.
@         IN      A        192.168.1.7
www.secis16.gr  IN      A        192.168.1.7
```

```
db.secis16.rev (/etc/bind) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
interfaces x named.conf.local x db.secis16 x db.secis16.rev x

;
; BIND data file for local loopback interface
;
$TTL      604800
@          IN      SOA      www.secis16.gr. root.www.secis16.gr. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;

1.168.192.om-addr.arpa.      IN      NS       www.secis16.gr
1                             IN      PTR      www.secis16.gr
```

```
resolv.conf (/etc) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
interfaces x named.conf.local x db.secis16 x db.secis16.rev x resolv.conf x

# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.1.7
search secis16.gr
```

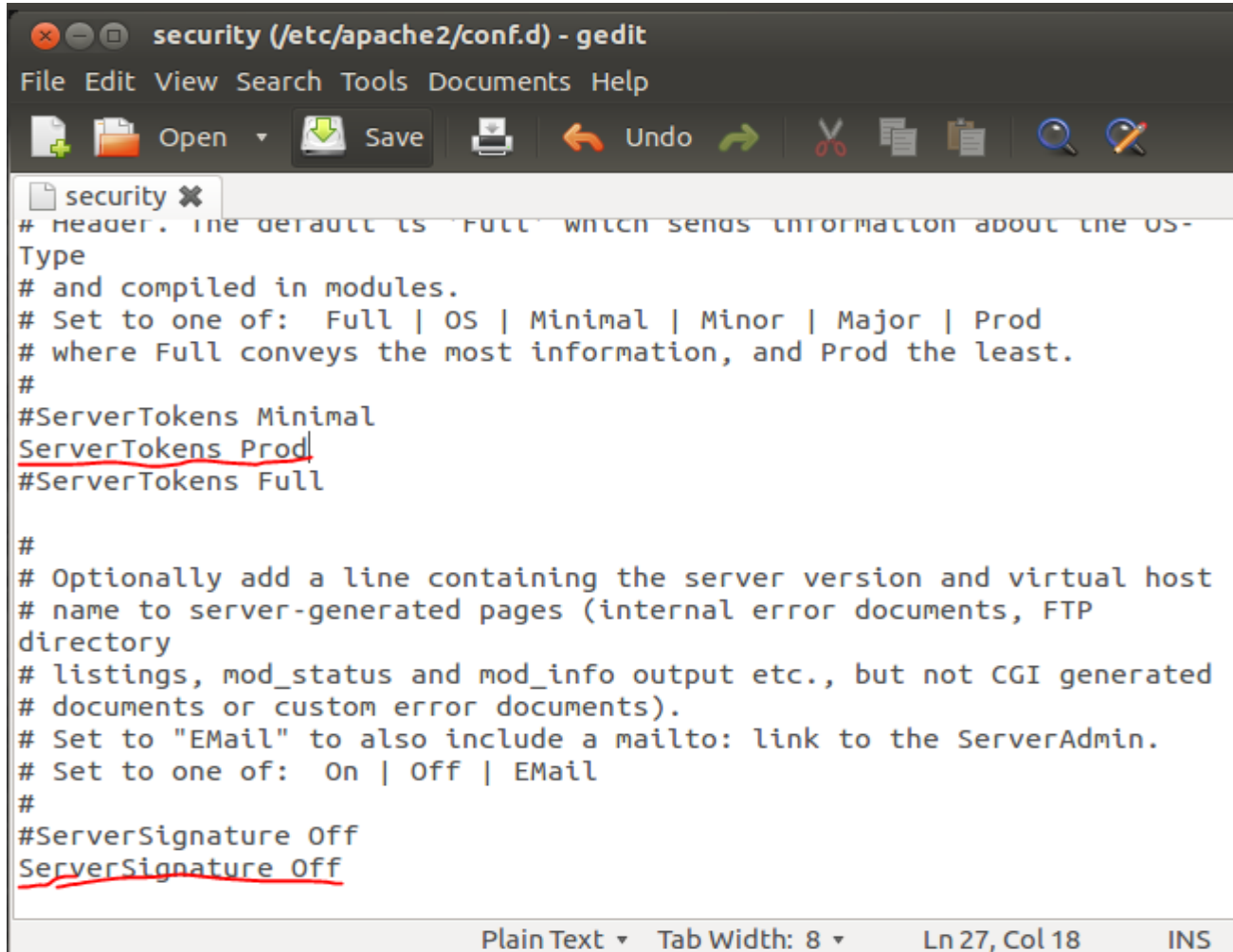
Υπηρεσία IIS:

Κάναμε εγκατάσταση τον apache server με την εντολή:

```
sudo apt-get install apache2
```



Για να τον κάνουμε πιο ασφαλές πήγαμε στο αρχείο /etc/apache2/conf.d/security και αλλάξαμε τις γραμμές:

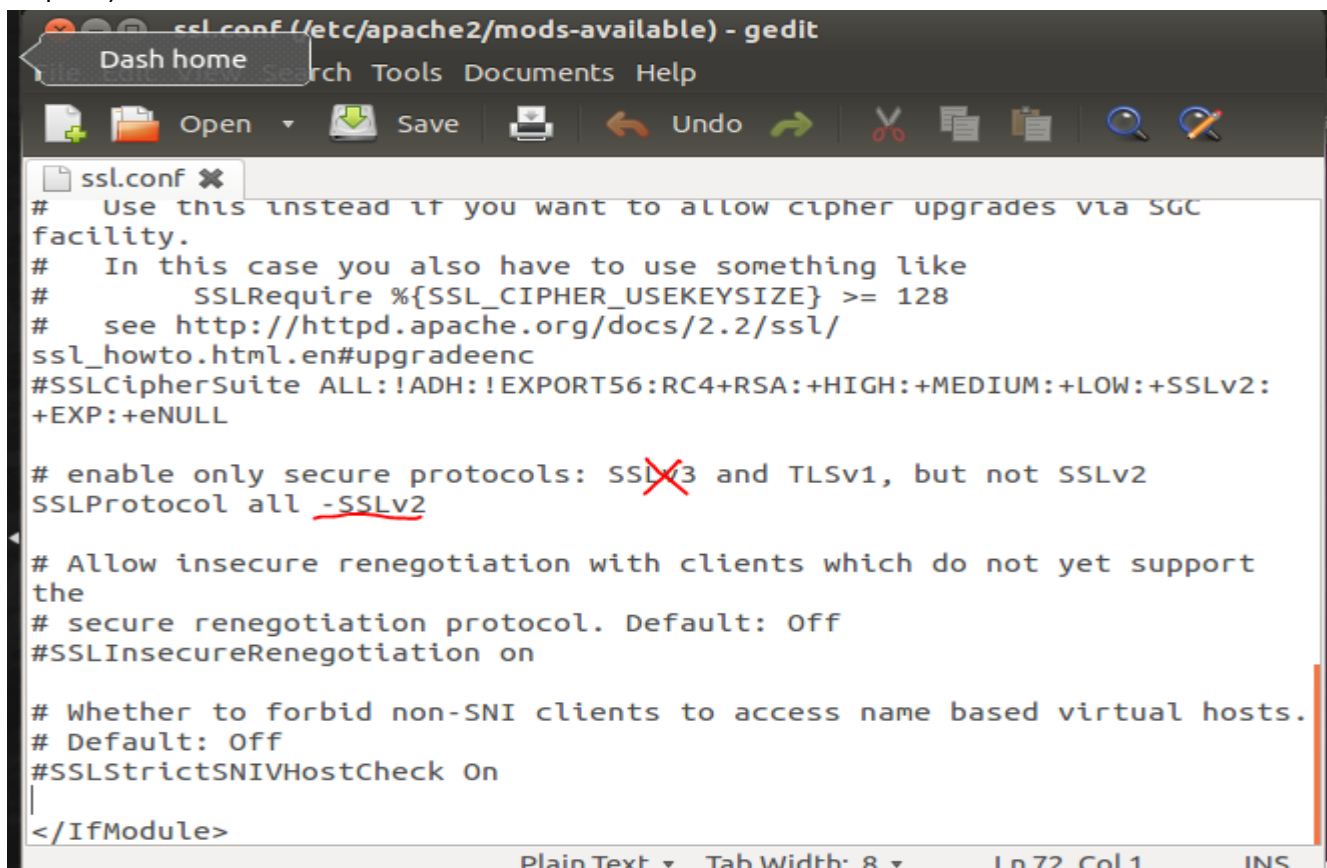


```
security (/etc/apache2/conf.d) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
security x
# header. The default is "Full" which sends information about the OS-
Type
# and compiled in modules.
# Set to one of: Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#
#ServerTokens Minimal
ServerTokens Prod
#ServerTokens Full

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP
directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "Email" to also include a mailto: link to the ServerAdmin.
# Set to one of: On | Off | Email
#
#ServerSignature Off
ServerSignature Off

Plain Text Tab Width: 8 Ln 27, Col 18 INS
```

Στο αρχείο /etc/apache2/mods-available/ssl.conf και απενεργοποιήσαμε το πρωτόκολλο SSLv3 καθώς θεωρείται μη ασφαλές



```
ssl.conf (/etc/apache2/mods-available) - gedit
Dash home
File Edit View Search Tools Documents Help
Open Save Undo
ssl.conf x
# Use this instead if you want to allow cipher upgrades via SGC
facility.
# In this case you also have to use something like
# SSLRequire %{SSL_CIPHER_USEKEYSIZE} >= 128
# see http://httpd.apache.org/docs/2.2/ssl/
ssl_howto.html.en#upgradeenc
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:
+EXP:+eNULL

# enable only secure protocols: SSLv3 and TLSv1, but not SSLv2
SSLProtocol all -SSLv2

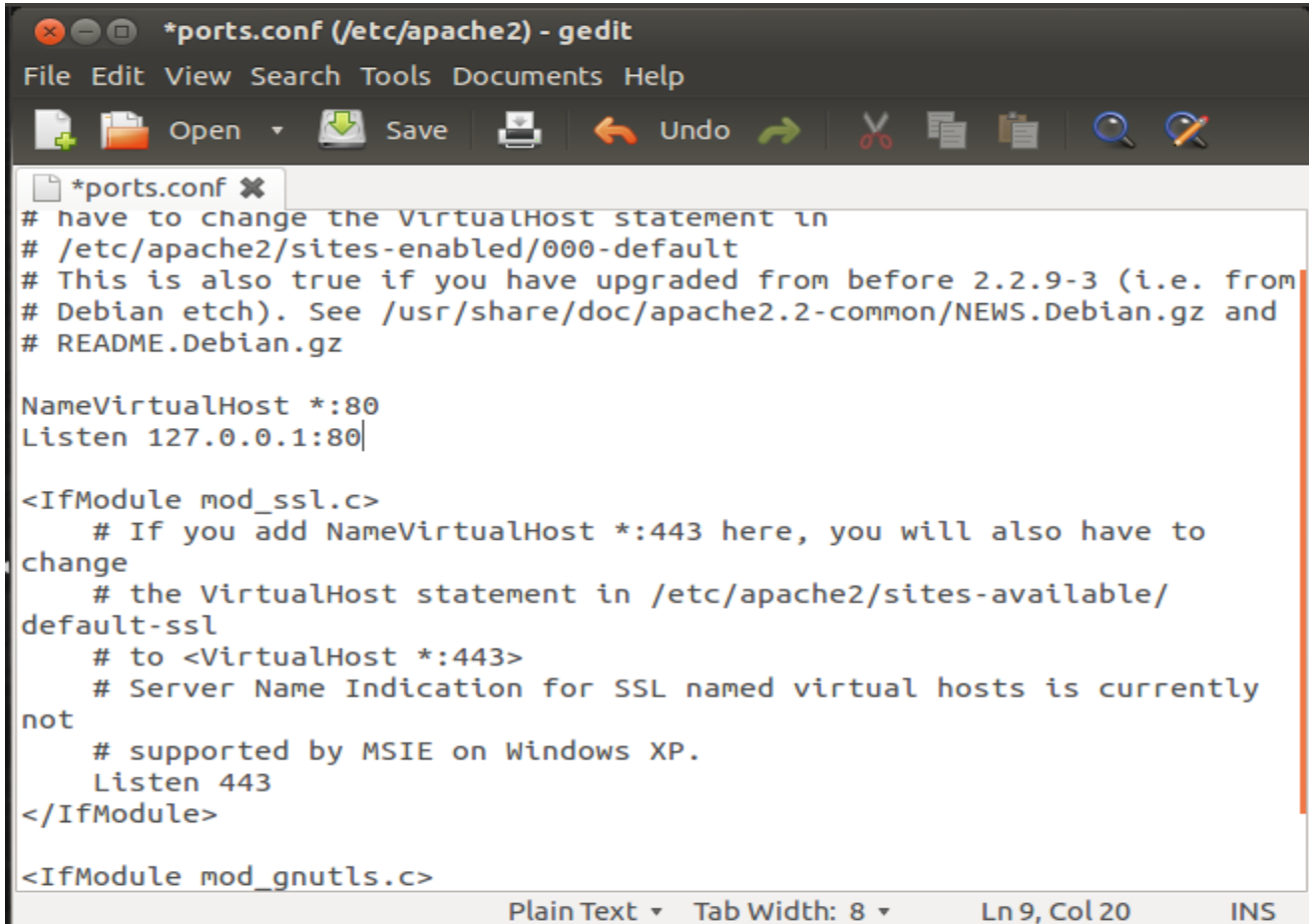
# Allow insecure renegotiation with clients which do not yet support
the
# secure renegotiation protocol. Default: Off
#SSLInsecureRenegotiation on

# Whether to forbid non-SNI clients to access name based virtual hosts.
# Default: Off
#SSLStrictSNIVHostCheck On

</IfModule>

Plain Text Tab Width: 8 Ln 72, Col 1 INS
```


Και στο αρχείο /etc/apache2/ports.conf και θέσαμε μοναδικό server τον δικό μας



```
*ports.conf (/etc/apache2) - gedit
File Edit View Search Tools Documents Help

# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default
# This is also true if you have upgraded from before 2.2.9-3 (i.e. from
# Debian etch). See /usr/share/doc/apache2.2-common/NEWS.Debian.gz and
# README.Debian.gz

NameVirtualHost *:80
Listen 127.0.0.1:80

<IfModule mod_ssl.c>
    # If you add NameVirtualHost *:443 here, you will also have to
change
    # the VirtualHost statement in /etc/apache2/sites-available/
default-ssl
    # to <VirtualHost *:443>
    # Server Name Indication for SSL named virtual hosts is currently
not
    # supported by MSIE on Windows XP.
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
```

Υπηρεσία FTP:

Εγκαταστήσαμε την υπηρεσία FTP με την εντολή:

```
sudo apt-get vsftpd
```

Έπειτα πήγαμε στο αρχείο /etc/vsftpd.conf και προσθέσαμε/αλλάξαμε τις παρακάτω γραμμές:

```
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
```

```
anonymous_enable=NO
```

```
# Uncomment this to allow local users to log in.
```

```
local_enable=YES
```

```
# Uncomment this to enable any form of FTP write command.
```

```
write_enable=YES
```

```
#Enable Logging
```

```
xferlog_enable=YES
```

```
xferlog_std_format=NO
```

```
xferlog_file=/var/log/vsftpd.log
```

```
log_ftp_protocol=YES
```

```
debug_ssl=YES
```

Έπειτα προσπαθήσαμε να συνδεθούμε στον FTP Server άλλα πρόέκυψε το παρακάτω σφάλμα

```
root@LinuxServer: /home/administrator
root@LinuxServer:/home/administrator# ftp
ftp> open localhost
Connected to localhost.
220 Welcome, to SECIS16 FTP Service!
Name (localhost:administrator): secis12015
331 Please specify the password.
Password:
500 OOPS: vsftpd: refusing to run with writable root inside chroot()
Login failed.
ftp>
```

Το λύσαμε κατεβάζοντας την τελευταία έκδοση του vsftpd με τις εντολές:

```
sudo add-apt-repository ppa:thefrontiergroup/vsftpd
```

```
sudo apt-get update
```

```
sudo apt-get install vsftpd
```

Και προσθέτοντας στο vsftpd.conf τη γραμμή:

```
# Keep non-chroot listed users jailed
```

```
allow_writeable_chroot=YES
```

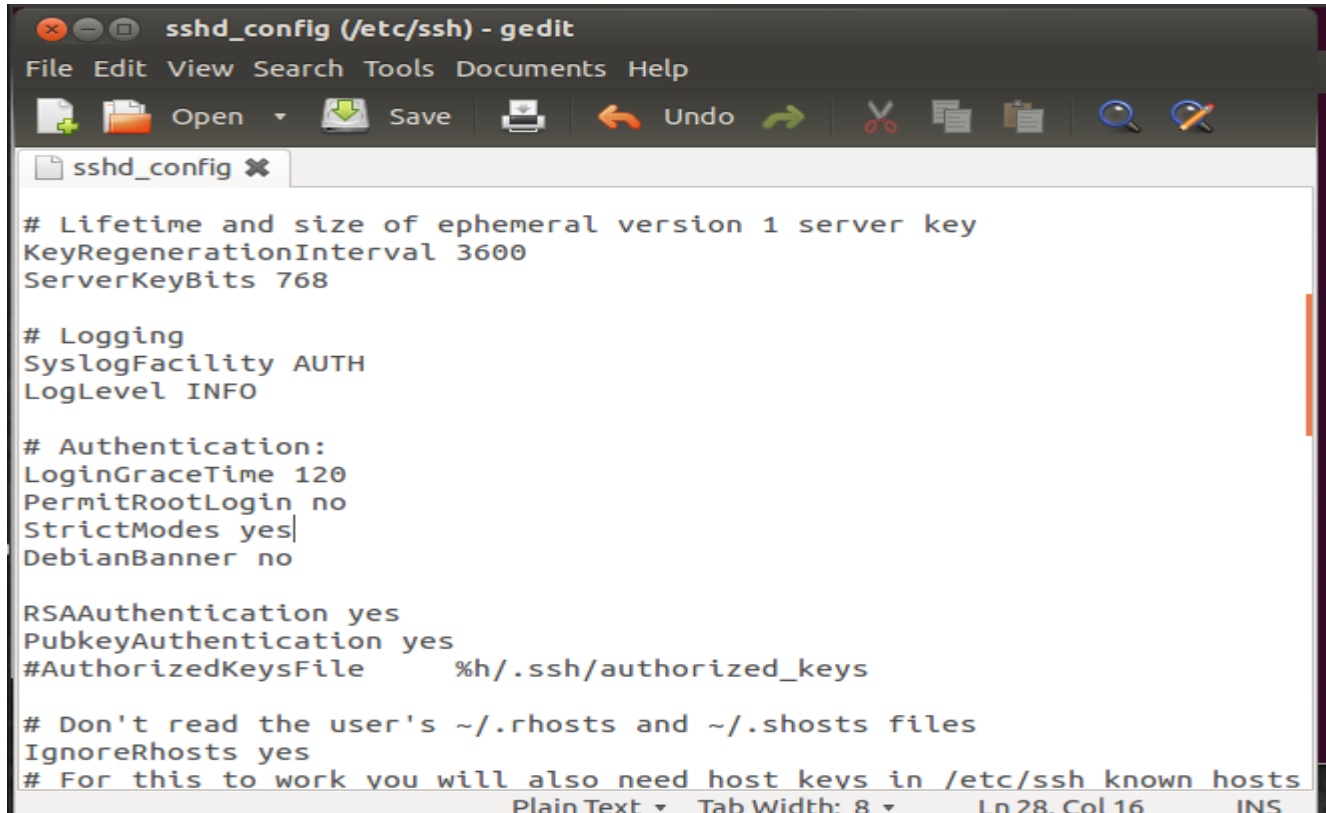
```
root@LinuxServer: /home/administrator
root@LinuxServer:/home/administrator# ftp
ftp> open localhost
Connected to localhost.
220 Welcome, to SECIS16 FTP Service!
Name (localhost:administrator): secis12015
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 1001 1001 8445 Mar 28 17:11 examples.desktop
226 Directory send OK.
ftp>
```

B6. Δημιουργήσαμε 3 groups και 6 χρηστές με την τον παρακάτω τρόπο

```
root@LinuxServer: /home/administrator
root@LinuxServer:/home/administrator# groupadd special
root@LinuxServer:/home/administrator# groupadd proffessors
root@LinuxServer:/home/administrator# groupadd students
root@LinuxServer:/home/administrator# sudo adduser secis12015 --home /usr/local/secis12015 --ingroup s
tudents
Adding user `secis12015' ...
Adding new user `secis12015' (1003) with group `students' ...
Creating home directory `/usr/local/secis12015' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for secis12015
Enter the new value, or press ENTER for the default
Full Name []: Χρήστος Αυλακιώτης
Room Number []:
Work Phone []:
Home Phone []:
Other []:
chfn: name with non-ASCII characters: 'Χρήστος Αυλακιώτης'
Is the information correct? [Y/n] y
root@LinuxServer:/home/administrator# printf 'USERS MADE:\n'; id administrator; id ftpadmin; id proffe
ssor; id secis12015; id secis11063; id secis13220
USERS MADE:
uid=1000(administrator) gid=1000(administrator) groups=1000(administrator),4(adm),24(cdrom),27(sudo),3
0(dip),46(plugdev),109(lpadmin),124(sambashare)
uid=1004(ftpadmin) gid=1001(special) groups=1001(special)
uid=1005(proffessor) gid=1002(proffessors) groups=1002(proffessors)
uid=1003(secis12015) gid=1003(students) groups=1003(students)
uid=1001(secis11063) gid=1003(students) groups=1003(students)
uid=1002(secis13220) gid=1003(students) groups=1003(students)
root@LinuxServer:/home/administrator#
```

B7.

Για να αποτρέψουμε τη δυνατότητα σύνδεσης στον εξυπηρετητή με τον λογαριασμό root από απομακρυσμένους υπολογιστές πήγαμε στο αρχείο `/etc/ssh/sshd_config` και αλλάξαμε τη γραμμή `PermitRootLogin` σε `no`

A screenshot of a gedit window titled 'sshd_config (/etc/ssh) - gedit'. The window shows the configuration file for the SSH daemon. The content includes comments and settings for key regeneration, logging, authentication, and host key management. The 'PermitRootLogin' setting is set to 'no'. The status bar at the bottom indicates 'Plain Text', 'Tab Width: 8', 'Ln 28, Col 16', and 'INS' mode.

```
# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

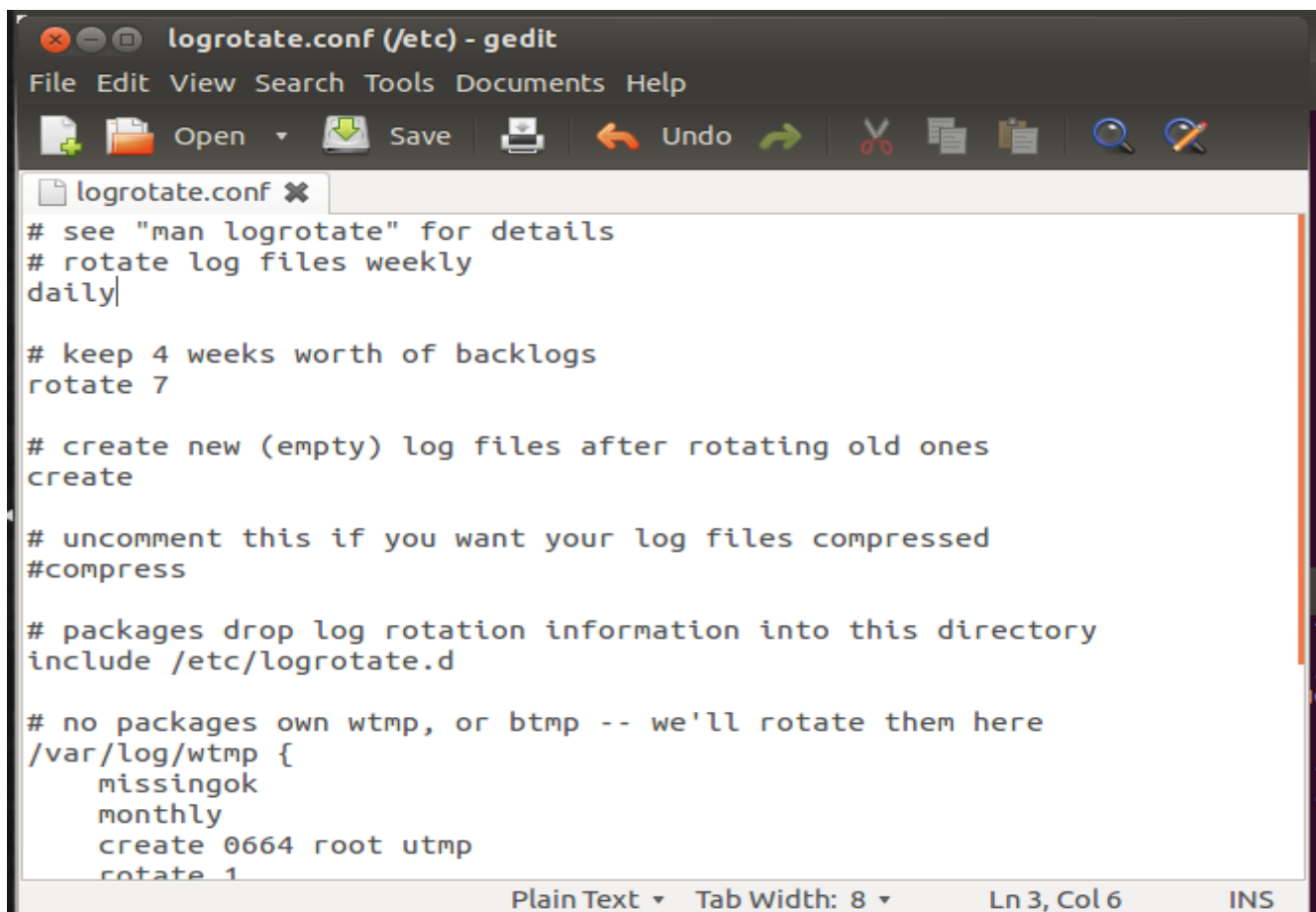
# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes
DebianBanner no

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile          %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh/known_hosts
```

B9. Πήγαμε στο αρχείο `/etc/logrotate` και κάναμε τις παρακάτω ρυθμίσεις

A screenshot of a gedit window titled 'logrotate.conf (/etc) - gedit'. The window shows the configuration file for log rotation. The content includes comments and settings for log file rotation frequency, retention, compression, and directory inclusion. The status bar at the bottom indicates 'Plain Text', 'Tab Width: 8', 'Ln 3, Col 6', and 'INS' mode.

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

# keep 4 weeks worth of backlogs
rotate 7

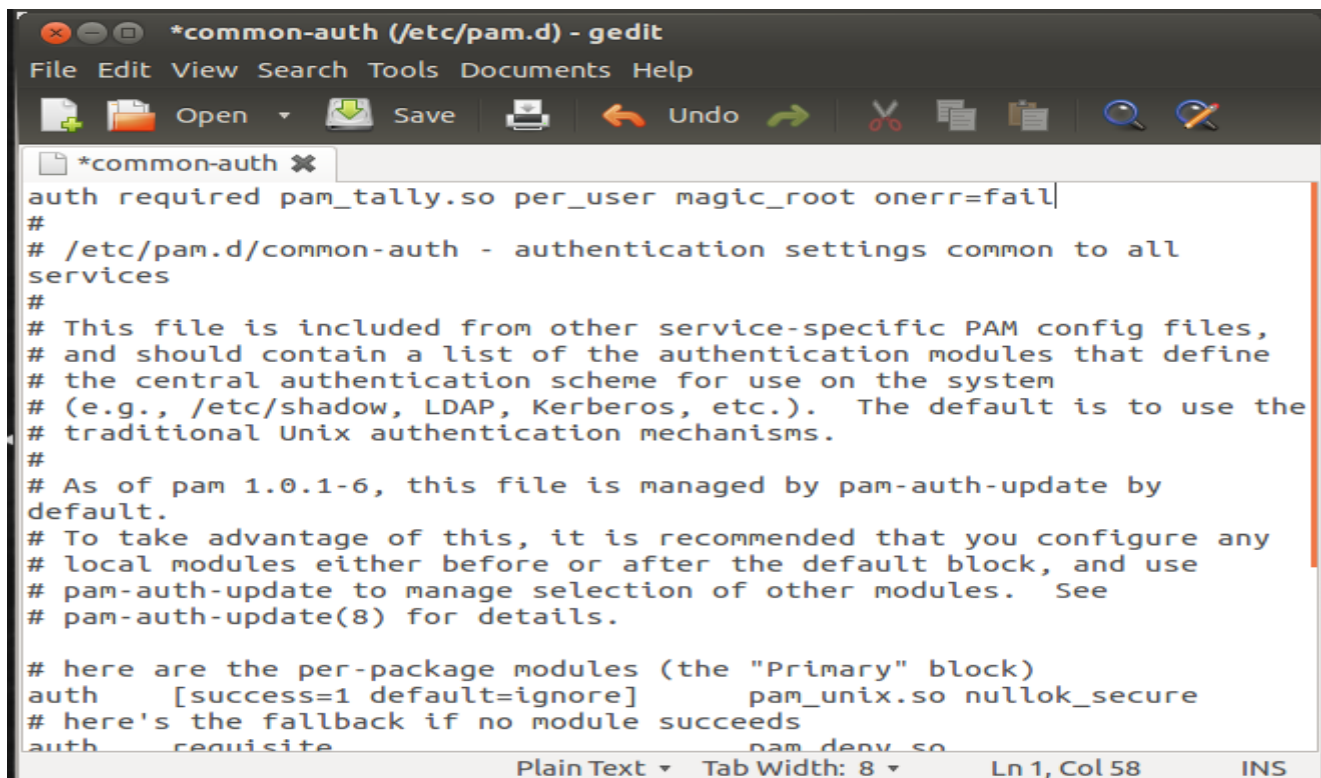
# create new (empty) log files after rotating old ones
create

# 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
    create 0664 root utmp
    rotate 1
```

B11. α) για να επιτύχουμε το ζητούμενο πήγαμε στο αρχείο /etc/pam.d/common-auth και στην αρχή



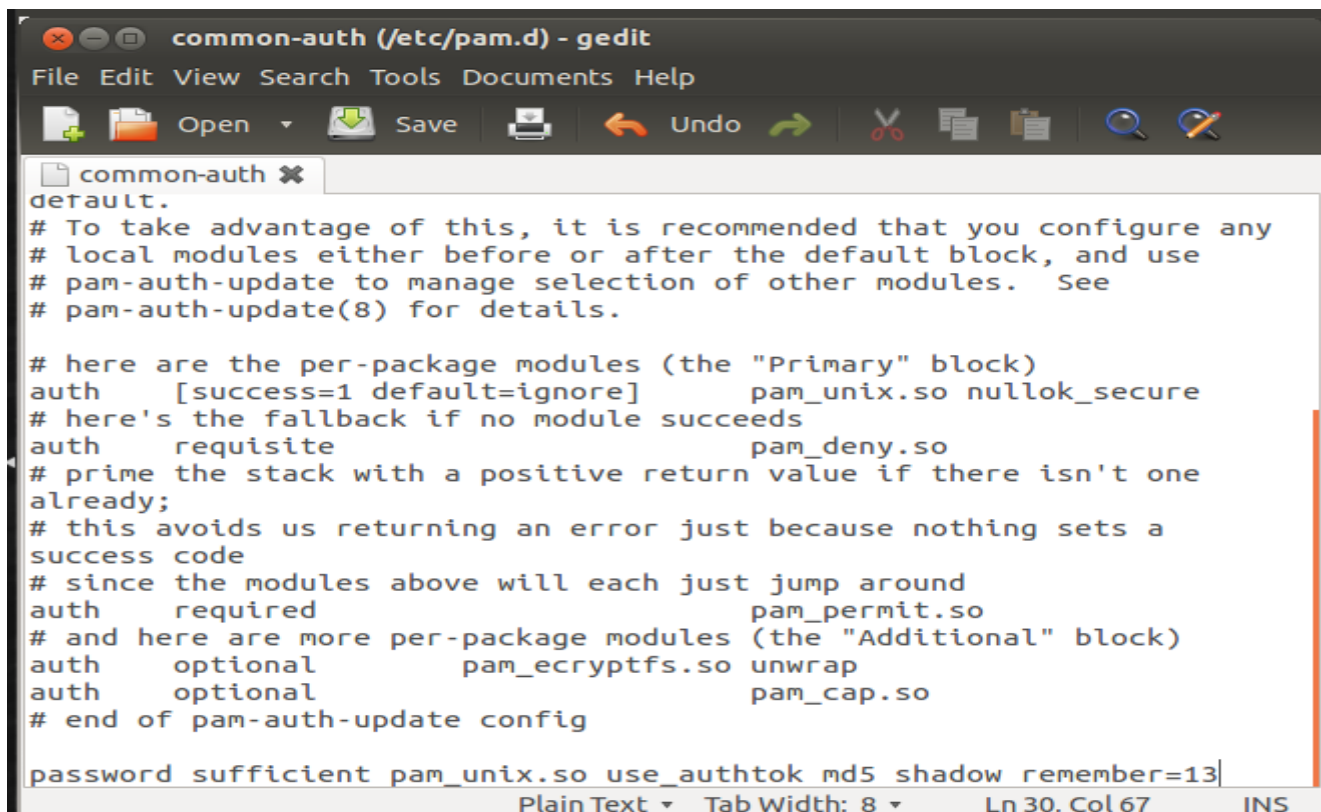
```
*common-auth (/etc/pam.d) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
*common-auth x
auth required pam_tally.so per_user magic_root onerr=fail
#
# /etc/pam.d/common-auth - authentication settings common to all
# services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.). The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by
# default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
auth [success=1 default=ignore] pam_unix.so nullok_secure
# here's the fallback if no module succeeds
auth requisite pam_deny.so
Plain Text Tab Width: 8 Ln 1, Col 58 INS
```

Στη συνέχεια τρέξαμε την εντολή:

```
faillog -m 7 -l 3600
```

Όπου -m ορίζουμε τις αποτυχημένες προσπάθειες μέχρι το κλειδωμα και στο -l το χρόνο κλειδωματος

Β) για να επιτύχουμε το ζητούμενο πήγαμε στο αρχείο /etc/pam.d/common-auth και στο τέλος προσθέσαμε την ακόλουθη γραμμή



```
common-auth (/etc/pam.d) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
common-auth x
default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
auth [success=1 default=ignore] pam_unix.so nullok_secure
# here's the fallback if no module succeeds
auth requisite pam_deny.so
# prime the stack with a positive return value if there isn't one
# already;
# this avoids us returning an error just because nothing sets a
# success code
# since the modules above will each just jump around
auth required pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth optional pam_ecryptfs.so unwrap
auth optional pam_cap.so
# end of pam-auth-update config
password sufficient pam_unix.so use_authtok md5 shadow remember=13
Plain Text Tab Width: 8 Ln 30, Col 67 INS
```

B12.

Για την εύρεση των αρχείων αυτών τρέξαμε τις εντολές:

```
sudo find / -perm -4000 -print
```

 (SUID)

```
sudo find / -perm -2000 -print
```

 (SGID)

Πηγές

<https://www.thefanclub.co.za/how-to/how-secure-ubuntu-1204-lts-server-part-1-basics>

<http://www.cyberciti.biz/tips/linux-security.html>

<http://www.tecmint.com/linux-server-hardening-security-tips/>

<http://askubuntu.com/>

<http://manpages.ubuntu.com/>