



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ  
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

UNIVERSITY OF THE AEGEAN  
DEPARTMENT OF INFORMATION AND COMMUNICATION SYSTEMS ENGINEERING

**321-3404**

**Ασφάλεια Πληροφοριακών και Επικοινωνιακών  
Συστημάτων**

Διδάσκων: Στεργιόπουλος Γεώργιος

---

**1<sup>η</sup> Εργαστηριακή Άσκηση**

---

Εργαστηριακοί Συνεργάτες: Δούμα Αναστασία, Μπαζάκας Αθανάσιος

3212018107 Κυριαζής Ιωάννης

3212018161 Παπαδόπουλος Παναγιώτης

Σάμος, Δευτέρα 22 Μαρτίου, 2021



321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

## Κατάλογος Περιεχομένων

<b><u>ΚΕΦΑΛΑΙΟ 1</u></b>	Αρχική εγκατάσταση και βασική παραμετροποίηση του ΛΣ.....σελ. 03
<b><u>ΚΕΦΑΛΑΙΟ 2</u></b>	Εγκατάσταση Υπηρεσιών και Ενδυνάμωση .....σελ. 17
<b><u>ΚΕΦΑΛΑΙΟ 3</u></b>	Αυτοματοποίηση Διαδικασιών.....σελ. 48
<b><u>ΚΕΦΑΛΑΙΟ 4</u></b>	Συμπεράσματα.....σελ. 51
<b><u>ΚΕΦΑΛΑΙΟ 5</u></b>	Βιβλιογραφία / Πηγές πληροφόρησης .....σελ. 53



321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

## **ΚΕΦΑΛΑΙΟ 1**

Αρχική εγκατάσταση και βασική παραμετροποίηση του ΛΣ



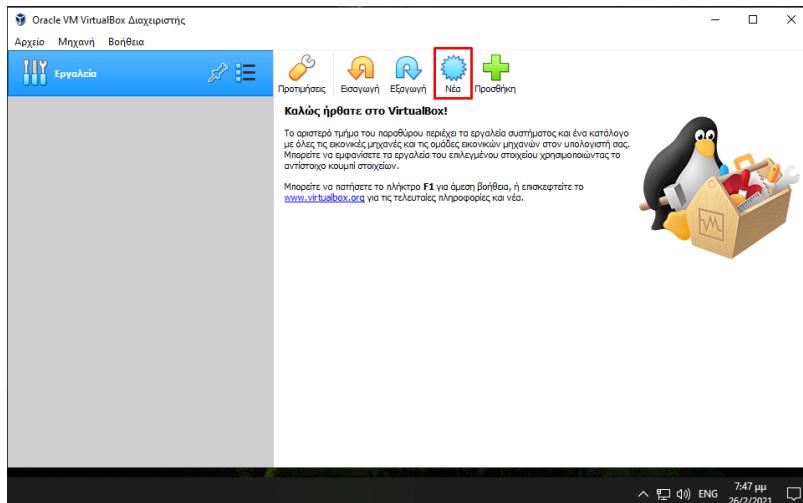
321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

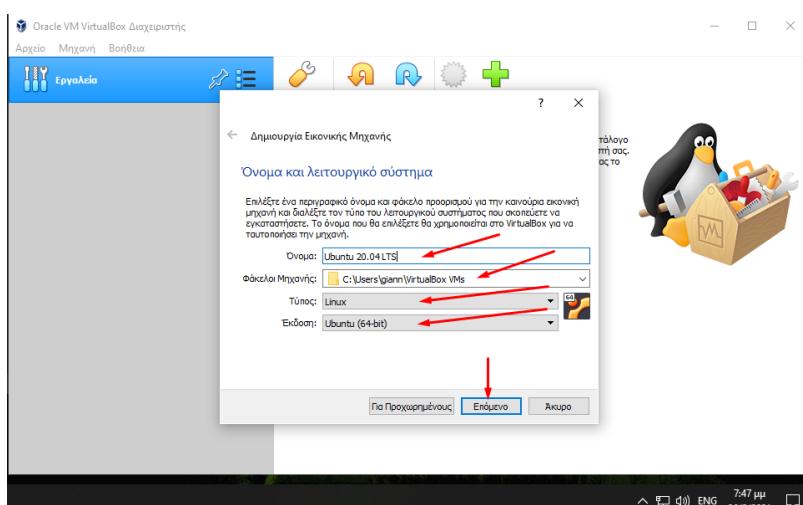
Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

## A1.

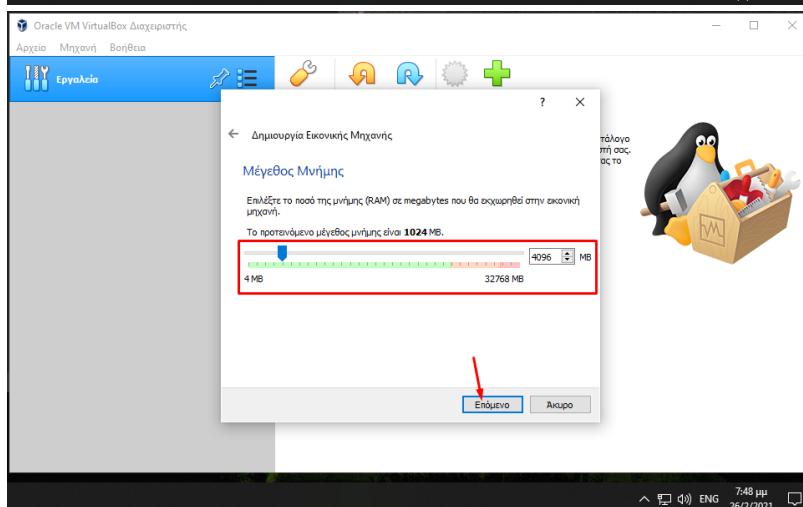
Για να φτιάξουμε τον ζητούμενο σέρβερ, χρησιμοποιήσαμε τον λειτουργικό Ubuntu LTS 20.04. Προκειμένου να το διαχειριστούμε, το εγκαταστήσαμε σε μία virtual machine που ονομάζεται VirtualBox.



Δημιουργήσαμε μία νέα εικονική μηχανή.



Δίνουμε όνομα, τον φάκελο που θα αποθηκευτεί, τον τύπο του λειτουργικού καθώς και την έκδοση.



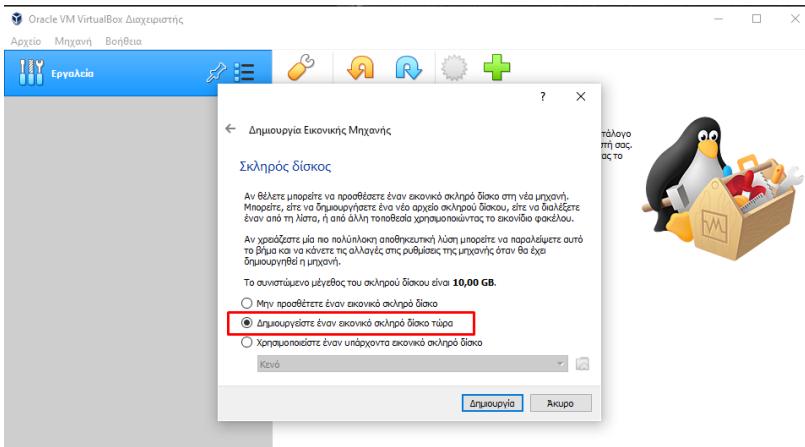
Δίνουμε την χωρητικότητα σε μνήμη RAM.



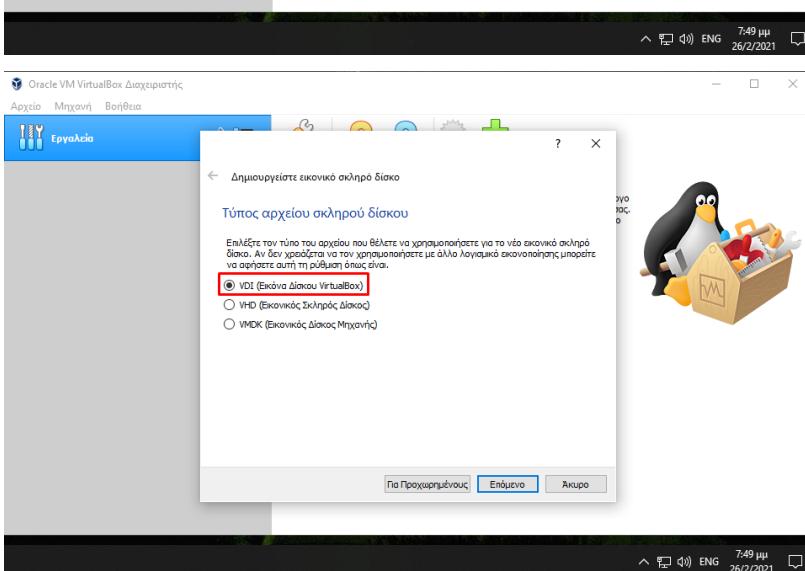
## 321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

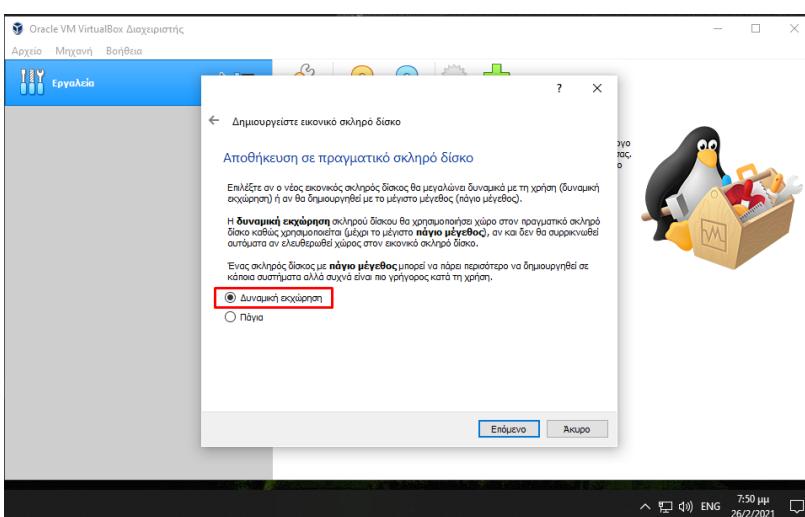
Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης



Επιλέγουμε να δημιουργήσουμε έναν νέο σκληρό δίσκο.



Επιλέγουμε Εικόνα Δίσκου VirtualBox.



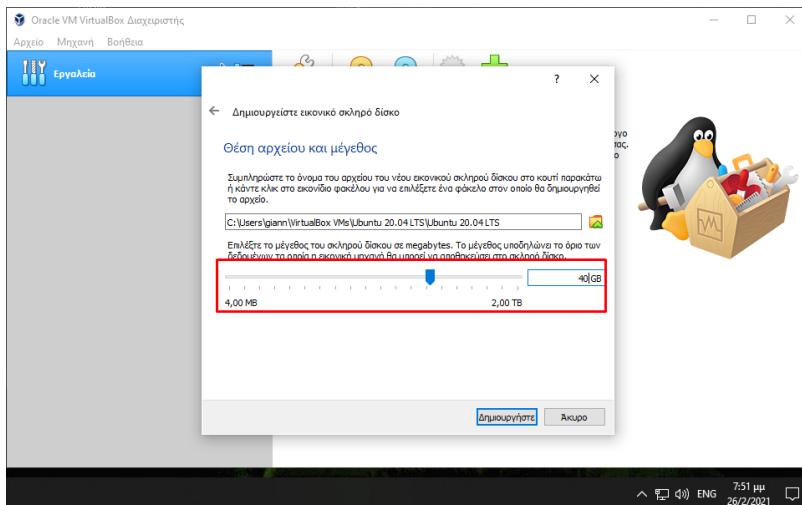
Επιλέγουμε Δυναμική Εκχώρηση.



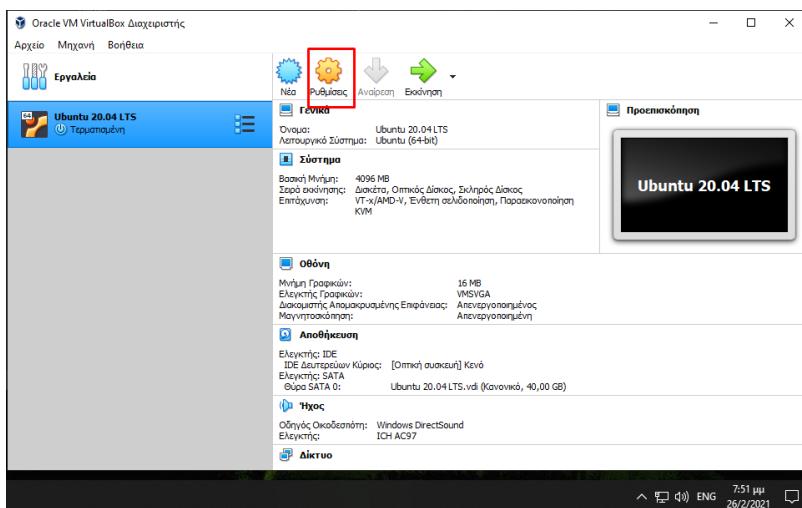
## 321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

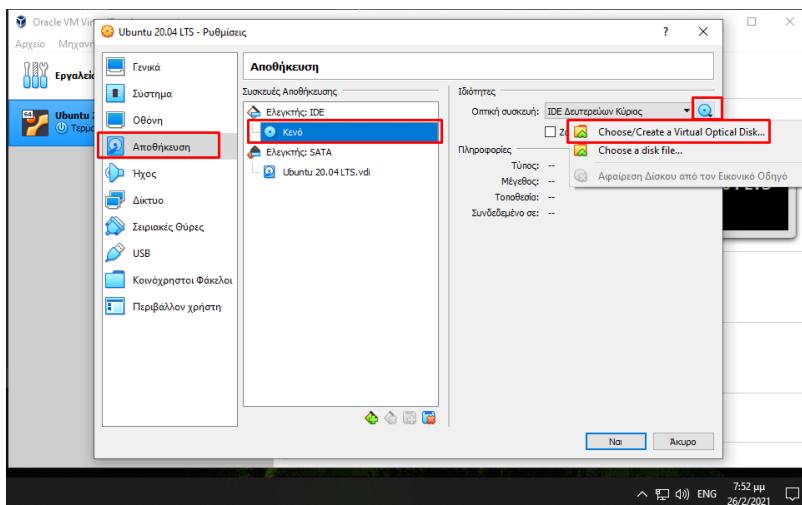
Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης



Δίνουμε το μέγεθος  
του σκληρού δίσκου  
που θα  
χρησιμοποιηθεί.



Επιλέγουμε  
Ρυθμίσεις



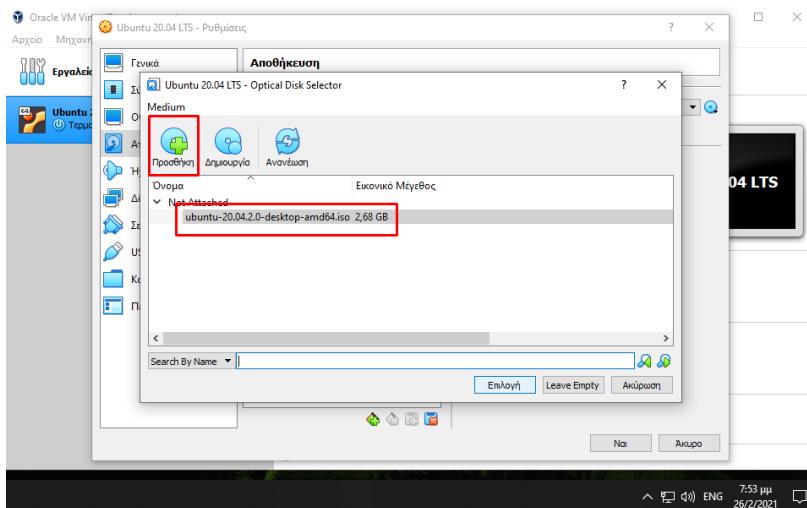
Επιλέγουμε να  
προσθέσουμε έναν  
ήδη υπάρχον οπτικό  
δίσκο του  
λειτουργικού.



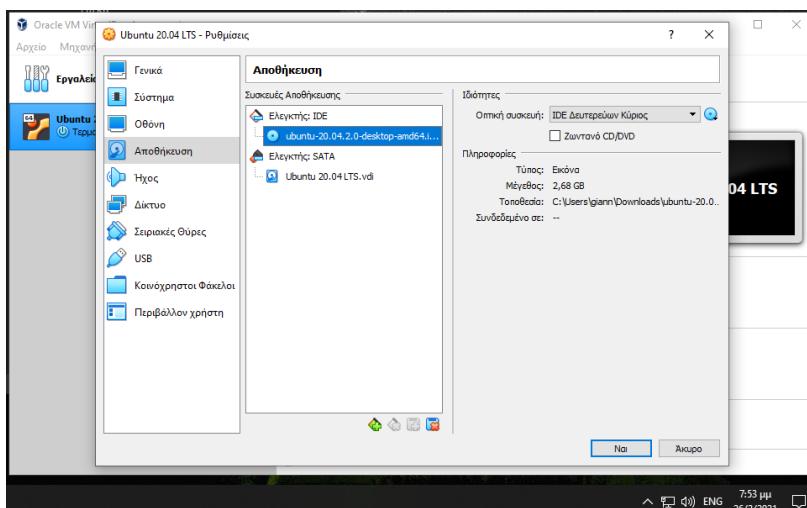
## 321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

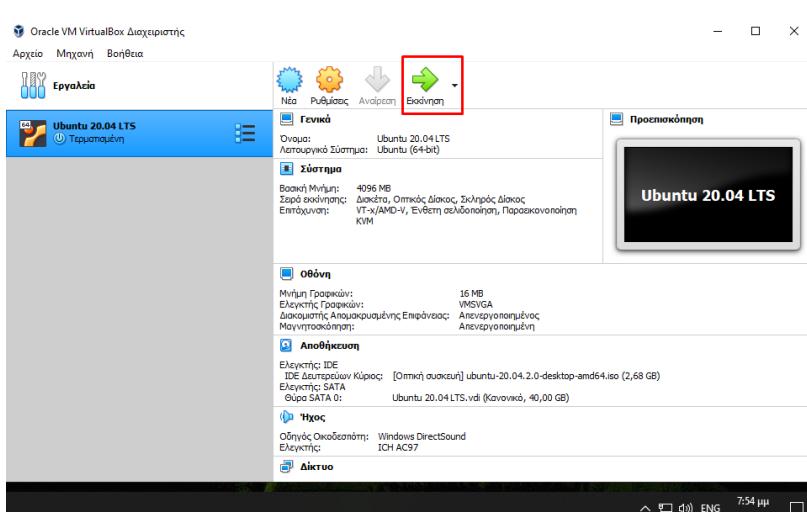
Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης



Επιλέγουμε τον ψηφιακό δίσκο που έχουμε κατεβάσει.



Πατάμε «Ναι»



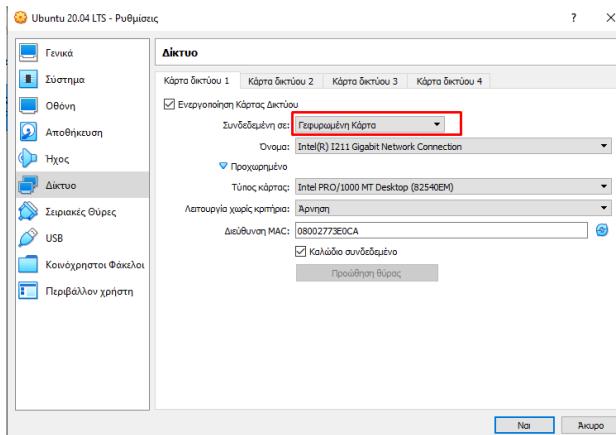
Εκκινούμε την εικονική μηχανή.



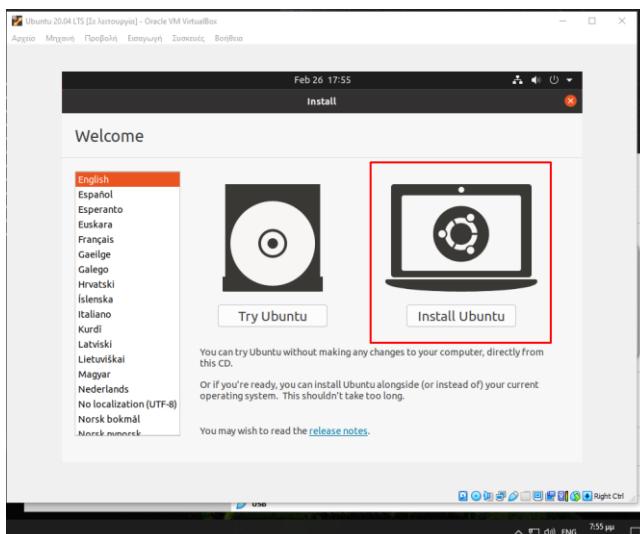
## 321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

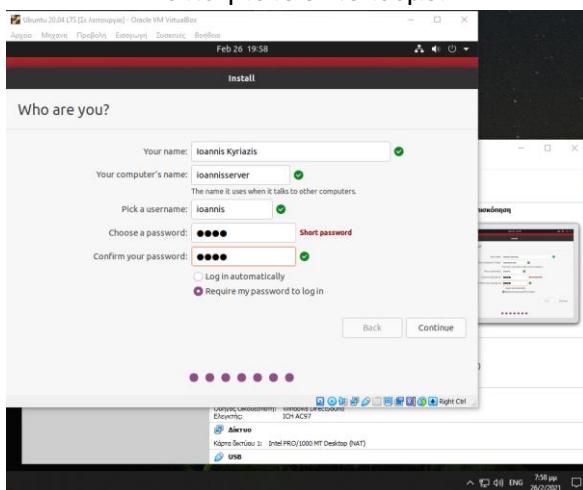


Όσον αφορά το Δίκτυο, θα επιλέξουμε να έχουμε «Γεμισμένη Κάρτα» διότι θέλουμε να υπάρχει διαφορετική διεύθυνση IP για τον σέρβερ μας.

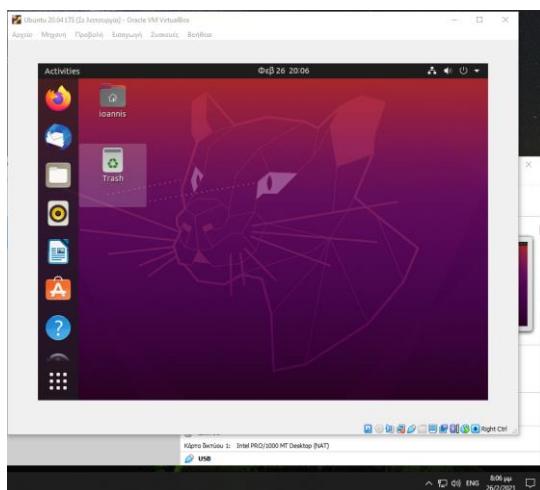


Επιλέγουμε την εγκατάσταση του λειτουργικού.

Προσθέτουμε τα στοιχεία. Για κωδικό βάλαμε έναν εύκολο για ευκολία και ταχύτητα σε οτιδήποτε εκτελούμε.



Το λειτουργικό είναι έτοιμο προς χρήση και τροποποίηση.





## A2.

```
Activities Terminal Map 2 10:28
loannis@ioannissserver:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd 00:00:00:00:00:00 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 192.168.1.11 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86323sec preferred_lft 86323sec
    inet6 fe80::192:168.1.11%enp0s3 brd ff:ff:ff:ff:ff:ff scope link noprefixroute
        valid_lft 864725sec preferred_lft 86152sec
    inet 192.168.1.11 brd 192.168.1.255 scope global dynamic mngtmpad
        valid_lft 604770sec preferred_lft 86370sec
        valid_lft forever preferred_lft forever
loannis@ioannissserver:~$ ls /etc/netplan
01-network-manager-all.yaml
loannis@ioannisserver:~$ sudo cp /etc/netplan/01-network-manager-all.yaml 01-network-manager-all.yaml.bak
[sudo] password for ioannis:
loannis@ioannisserver:~$
```

- Με την εντολή "ip a" βλέπουμε την διεύθυνση ip του συστήματός μας (192.168.1.11). Προεπιλεγμένα, η διεύθυνση του υπολογιστή μας ρυθμίζεται αυτόματα με τον DHCP που υπάρχει. Εμείς θα ρυθμίσουμε στατικά την διεύθυνση ip για να μας διευκολύνει στις παραμετροποιήσεις.

- Με την εντολή "ls /etc/netplan" βλέπουμε το αρχείο που περιέχει τις ρυθμίσεις του δικτύου.

- Με την τελευταία εντολή δημιουργούμε ένα backup για το αρχείο του δικτύου διότι πρόκειται να το τροποποιήσουμε.

```
Activities Terminal Map 2 10:33
loannis@ioannissserver:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 192.168.1.11 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86323sec preferred_lft 86323sec
    inet6 fe80::192:168.1.11%enp0s3 brd ff:ff:ff:ff:ff:ff scope link noprefixroute
        valid_lft 864725sec preferred_lft 86152sec
    inet 192.168.1.11 brd 192.168.1.255 scope global dynamic mngtmpad
        valid_lft 604770sec preferred_lft 86370sec
        valid_lft forever preferred_lft forever
loannis@ioannisserver:~$ ls /etc/netplan
01-network-manager-all.yaml
loannis@ioannisserver:~$ sudo cp /etc/netplan/01-network-manager-all.yaml 01-network-manager-all.yaml.bak
[sudo] password for ioannis:
loannis@ioannisserver:~$ sudo nano /etc/netplan/01-network-manager-all.yaml
loannis@ioannisserver:~$ sudo netplan try
Do you want to keep these settings?
Press ENTER before the timeout to accept the new configuration

Changes will revert in 118 seconds
Configuration accepted.
loannis@ioannisserver:~$ sudo netplan apply
loannis@ioannisserver:~$
```

```
Activities Terminal Map 2 10:32
loannis@ioannisserver:~$ nano /etc/netplan/01-network-manager-all.yaml
GNU nano 4.8 /etc/netplan/01-network-manager-all.yaml Modified
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.1.155/24
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

- Με την πρώτη εντολή τροποποιούμε το αρχείο δικτύου σε ένα txt form.

- Με την εντολή "sudo netplan try" ελέγχουμε την σωστή λειτουργία του τροποποιημένου αρχείου δικτύου.

- Με την τελευταία εντολή εφαρμόζουμε το πλάνο μας. Έτσι πλέον έχουμε στατική διεύθυνση ip.

- Τροποποιούμε το αρχείο του δικτύου.

- Επιλέγουμε να μην έχουμε dhcp δυνατότητα και δηλώνουμε την στατική ip διεύθυνση που θέλουμε να έχουμε (192.168.1.155). Δηλώνουμε μεγάλη για να να μην έχουμε προβλήματα με άλλες συσκευές.

- Πληκτρολογούμε την default gateway του ρούτερ μας.

- Πληκτρολογούμε τους DNS servers της google οι οποίοι είναι γρήγοροι και αξιόπιστοι.



## 321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

```
ork-manager-all.yaml.bak
[sudo] password for ioannis:
[ioannis@ioannissERVER:~] $ sudo nano /etc/netplan/01-network-manager-all.yaml
[ioannis@ioannissERVER:~] $ sudo netplan try
Do you want to keep these settings?

Press ENTER before the timeout to accept the new configuration

Changes will revert in 118 seconds
Configuration accepted.

[ioannis@ioannissERVER:~] $ sudo netplan apply
i: interface: BACK,UP,LOWER_UP: mtu 65536 qdisc noqueue state UNKNOWN group default
    link:[loopback]:0 brd 0:0:0:0:0:0 brd 0:0:0:0:0:0
    inet [127.0.0.1/8] brd 0:0:0:0:0:0 scope host lo
        valid_lft forever preferred_lft forever
    inet ::/128 scope host
        valid_lft forever preferred_lft forever
        valid_lft forever preferred_lft forever
2: enp0s3: MTU: 1500 qdisc mq state UP qlen 1000
    link/ether 00:0c:27:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.155/24 brd 192.168.1.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
        inet fe80::0c27:feff:fe73:c0a/64 scope link
            valid_lft forever preferred_lft forever
[ioannis@ioannissERVER:~]
```

```
[ioannis@ioannissERVER:~] $ sudo apt update
Hit:1 http://gr.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:3 http://gr.archive.ubuntu.com/ubuntu focal-updates InRelease
Reading package lists...
Building dependency tree
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
[ioannis@ioannissERVER:~] $ sudo apt install openssh-server
Reading package lists... done
Building dependency tree
Reading state information... done
The following additional packages will be installed:
  curses-term openssh-sftp-server ssh-import-id
Suggested packages:
  policy-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  curses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
Need to get 688 kB of archives.
After this operation, 6010 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://gr.archive.ubuntu.com/ubuntu focal/main amd64 ncurses-term all 6.2-0ubuntu2 [249 kB]
Get:2 http://gr.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-sftp-server amd64 1:8.2p1-4ubuntu0.1 [51.5 kB]
Get:3 http://gr.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-server amd64 1:8.2p1-4ubuntu0.1 [377 kB]
[ioannis@ioannissERVER:~]
```

```
stend/system/sh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
Setting up ssh-import-id (5.10-Buubuntu1) ...
Attempting to convert /etc/ssh/sshd import_id
Setting up ncurses-term (6.2-0ubuntu2) ...
Processing triggers for systemd (245.4-4ubuntu3.4) ...
Processing triggers for man-db (2.9.1-1) ...
[ioannis@ioannissERVER:~] $ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: en
   Active: active (running) since Tue 2021-03-02 10:37:21 EET; 28s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
           Main PID: 2655 (sshd)
             Tasks: 1 (limit: 4654)
           Memory: 1.1M
          CGroup: /system.slice/ssh.service
                  └─2655 sshd: /usr/sbin/sshd -D [listener] @ of 10-100 startups

Map 02 10:37:21 ioannissERVER systemd[1]: Starting OpenBSD Secure Shell server...
Map 02 10:37:21 ioannissERVER sshd[2655]: Server listening on 0.0.0.0 port 22.
Map 02 10:37:21 ioannissERVER sshd[2655]: Server listening on :: port 22.
Map 02 10:37:21 ioannissERVER systemd[1]: Started OpenBSD Secure Shell server.
[lines 1-15/15 (END)]
[1]+ Stopped                  sudo systemctl status ssh
[ioannis@ioannissERVER:~]
```

```
Map 02 10:37:21 ioannissERVER sshd[2655]: Server listening on 0.0.0.0 port 22.
Map 02 10:37:21 ioannissERVER sshd[2655]: Server listening on :: port 22.
Map 02 10:37:21 ioannissERVER systemd[1]: Started OpenBSD Secure Shell server.
[lines 1-15/15 (END)]
[1]+ Stopped                  sudo systemctl status ssh

[ioannis@ioannissERVER:~] $ sudo ufw status
Status: inactive
[ioannis@ioannissERVER:~] $ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
[ioannis@ioannissERVER:~] $ sudo ufw allow openSSH
Rules updated
[ioannis@ioannissERVER:~] $ sudo ufw enable
Firewall is active and enabled on system startup
[ioannis@ioannissERVER:~] $ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To           Action      From
----        --          --
22/tcp (OpenSSH) ALLOW IN  Anywhere
22/tcp (OpenSSH (v6)) ALLOW IN  Anywhere (v6)

[ioannis@ioannissERVER:~]
```

Με την εντολή "ip a" ελέγχουμε την τρέχουσα διεύθυνση ή μετά την αλλαγή που κάναμε. Άρα η διεύθυνσή μας πλέον είναι 192.168.1.155.

- Με την πρώτη εντολή ενημερώνουμε το λειτουργικό μας στην τελευταία έκδοση.

- Με την δεύτερη εντολή εγκαθιστούμε τον openssh server που είναι ο πιο ασφαλής τρόπος για να έχουμε ssh λειτουργία στον σέρβερ μας.

Με την εντολή "sudo systemctl status ssh" βλέπουμε την τρέχουσα κατάσταση της ssh λειτουργίας (ενεγοποιημένη).

- Με την πρώτη εντολή βλέπουμε την τρέχουσα κατάσταση του firewall του συστήματός μας (απενεργοποιημένο).

- Με την δεύτερη εντολή λέμε στο firewall να απορρίπτει όλες τις εισερχόμενες αιτήσεις για σύνδεση στον σέρβερ μας (κλείνει όλες τις ανοιχτές πόρτες του συστήματος).

- Με την τρίτη εντολή επιτρέπουμε το openssh (ssh server) στο firewall.

- Με την τέταρτη εντολή ενεργοποιούμε το firewall.

- Με την τελευταία εντολή βλέπουμε την τρέχουσα κατάσταση του firewall μετά τις τροποποιήσεις.



## 321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

The screenshot shows two terminal windows. The left window displays the output of `sudo ufw enable` and `sudo ufw status verbose`, indicating that the firewall is active and enabled on system startup. The right window shows the configuration file `/etc/ssh/sshd\_config` with the port `Port 2200` highlighted. The command `sudo nano /etc/ssh/sshd\_config` and `service ssh restart` are also visible.

- Με την πρώτη εντολή τροποποιούμε το αρχείο που περιέχει τις ssh πληροφορίες. Το κάνουμε για να αλλάξουμε την εξ' ορισμού θύρα ssh όπως μας ζητείται.

- Με την τελευταία εντολή κάνουμε restart την ssh λειτουργία του σερβερ μας.

- Τροποποιούμε την πόρτα ssh.

- Την θέτουμε 2200.

- Όσον αφορά την ημερομηνία, είχαμε ξεχάσει να βγάλουμε την «#» μπροστά από την εντολή με αποτέλεσμα να μην απαντήσουμε ορθώς στην ζητούμενη ερώτηση. Παρόλα αυτά το διορθώσαμε.

The screenshot shows two terminal windows. The top window runs `sudo grep Port /etc/ssh/sshd\_config` and `netstat -tulpn | grep ssh` to find the current port. The bottom window shows the addition of a new rule with `sudo ufw deny 22/tcp` and the removal of an old rule with `sudo ufw allow 22000/tcp`.

- Με την πρώτη εντολή βλέπουμε αν έχει οριστεί η πόρτα που δώσαμε.

- Με την δεύτερη εντολή βλέπουμε που τρέχει το ssh (στην πόρτα 22000).

- Με την τρίτη εντολή κλείνουμε την πόρτα 22 που ήταν η εξ' ορισμού πόρτα του ssh.

- Με την τέταρτη εντολή ανοίγουμε την πόρτα 22000 που έχουμε θέσει ως ssh πόρτα

The screenshot shows a terminal window displaying the output of `sudo ufw status`. It lists various ports and their status (Allow or Deny) from both IPv4 and IPv6 perspectives. The port `22000/tcp (v6)` is shown as ALLOWed.

- Με την εντολή "sudo ufw status" βλέπουμε ότι άνοιξε η πόρτα 22000.

- Λόγω του προβλήματος που αναφέραμε πιο πάνω, είχαμε προχωρήσει παρακάτω στην άσκηση γι' αυτό βλέπουμε αρκετές θύρες ανοιχτές.



```
loannis@ioannisserver:~$ sudo ufw status
Status: active
To                         Action      From
...                         ALLOW       Anywhere
OpenSSH                     ALLOW       Anywhere
Apache Full                 ALLOW       Anywhere
53                         ALLOW       Anywhere
53/udp                     ALLOW       Anywhere
80/tcp                      ALLOW      192.168.1.10
80                         ALLOW      192.168.1.10
443/tcp                     ALLOW      192.168.1.10
443                         ALLOW      192.168.1.10
Nginx Full                  ALLOW      192.168.1.10
53/tcp                      ALLOW      192.168.1.10
53/udp                     ALLOW      192.168.1.10
5353/tcp                    ALLOW      192.168.1.10
5353                         ALLOW      192.168.1.10
22/tcp                      DENY      Anywhere
22000/tcp                   ALLOW      Anywhere
OpenSSH (v6)                ALLOW      Anywhere (v6)
Apache Full (v6)             ALLOW      Anywhere (v6)
80 (v6)                     ALLOW      Anywhere (v6)
443/tcp (v6)                ALLOW      Anywhere (v6)
443                         ALLOW      Anywhere (v6)
Nginx Full (v6)              ALLOW      Anywhere (v6)
53/tcp (v6)                 ALLOW      Anywhere (v6)
53/udp (v6)                 ALLOW      Anywhere (v6)
5353/tcp (v6)               ALLOW      Anywhere (v6)
5353                         ALLOW      Anywhere (v6)
22/tcp (v6)                 DENY      Anywhere (v6)
22000/tcp (v6)              ALLOW      Anywhere (v6)

loannis@ioannisserver:~$
```

Ανοίγουμε την εφαρμογή PuTTY για να ελέγχουμε ότι λειτουργεί το ssh από την αλλαγή πόρτας που επιφέραμε.

Όπως παρατηρούμε όλα λειτουργούν άψογα.

### A3.

```
loannis@ioannisserver:~$ adduser icsd18107
adduser: Only root may add a user or group to the system.
loannis@ioannisserver:~$ sudo adduser icsd18107
Adding user 'icsd18107' (1001) ...
Adding new group 'icsd18107' (1001)
Creating home directory '/home/icsd18107' ...
Copying files from '/etc/skel' ...
New password:
Re-enter new password:
passwd: password updated successfully
Changing the user information for icsd18107
Enter the new value, or press ENTER for the default
  Full Name []: icsd18107
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [y/n] y
loannis@ioannisserver:~$ apt-get install sudo
E: Could not open lock file /var/lib/dpkg/lock-frontend - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), are you root?
loannis@ioannisserver:~$ sudo apt-get install sudo
Reading package lists... Done
Building dependency tree
Reading state information... Done
sudo is already the newest version (1.8.31-1ubuntu1.2).

```

- Με την πρώτη εντολή προσθέτουμε έναν user με όνομα icsd18107 τον οποίο θα τον χρησιμοποιήσουμε για να συνδεόμαστε μέσω ssh στον σέρβερ.

- Κάνουμε εγκατάσταση τις λειτουργίες root "sudo" (υπάρχουν ήδη στο σύστημα).

- Με την εντολή "sudo nano /etc/ssh/sshd\_config" τροποποιούμε το αρχείο που περιέχει τις πληροφορίες ssh έτσι ώστε να απαγορεύσουμε root login μέσω ssh.

- Τροποποιούμε και βάζουμε μία εξαίρεση για την δική μας ευκολία. Επιτρέπουμε μόνο σε έναν με root δικαιώματα να χρησιμοποιεί το ssh.

- Κάνουμε restart το ssh.

```
loannis@ioannisserver:~$ passwd
passwd: password updated successfully
Changing the user information for icsd18107
Enter the new value, or press ENTER for the default
  Full Name []: icsd18107
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [y/n] y
loannis@ioannisserver:~$ apt-get install sudo
E: Could not open lock file /var/lib/dpkg/lock-frontend - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), are you root?
loannis@ioannisserver:~$ sudo apt-get install sudo
Reading package lists... Done
Building dependency tree
Reading state information... Done
sudo is already the newest version (1.8.31-1ubuntu1.2).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
loannis@ioannisserver:~$ sudo usermod -a -G sudo icsd18107
loannis@ioannisserver:~$ sudo grep Port /etc/ssh/sshd_config
#Port 22
#GatewayPorts no
loannis@ioannisserver:~$ sudo nano /etc/ssh/sshd_config
loannis@ioannisserver:~$ sudo nano /etc/ssh/sshd_config
loannis@ioannisserver:~$ service ssh restart

```

```
GNU nano 4.8 /etc/ssh/sshd_config Modified
#Port 40
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#LogLevel AUTH
#LogLevel INFO

# Authentication:
#LoginGraceTime 2m
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
#AllowUsers icsd18107

# Get Help   Write Out  Where Is  Cut Text  Justify  Cur Pos
# Exit     Read File  Replace  Paste Text To Spell  Go To Line
```



## A4.

```

Activities Terminal Map 2 11:08
ioannis@ioannissserver:~$ Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y
ioannis@ioannissserver:~$ sudo apt-get install sudo
E: Could not open lock file /var/lib/dpkg/lock-frontend - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), are you root?
A: ioannis@ioannisserver:~$ sudo apt-get install sudo
Reading package lists... Done
Building dependency tree
Reading state information... Done
sudo is already the newest version (1.8.31-1ubuntu1.2).
sudo set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
ioannis@ioannisserver:~$ sudo usermod -a -G sudo icsd18107
ioannis@ioannisserver:~$ sudo grep Port /etc/ssh/sshd_config
#Port 22
#GatewayPorts no
ioannis@ioannisserver:~$ sudo nano /etc/ssh/sshd_config
ioannis@ioannisserver:~$ sudo nano /etc/ssh/sshd_config
ioannis@ioannisserver:~$ service ssh restart
ioannis@ioannisserver:~$ sudo passwd -l root
passwd: password expiry information changed.
ioannis@ioannisserver:~$ 

```

- Με την εντολή "sudo passwd -l root" απαγορεύουμε το root login μέσω δήλωσης του root password ως ληγμένο.

## A5.

```

Activities Terminal Map 2 11:12
ioannis@ioannisserver:~$ sudo apt install unattended-upgrades
Reading package lists... Done
Building dependency tree
Reading state information... Done
unattended-upgrades is already the newest version (2.3ubuntu0.1).
unattended-upgrades set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
A: unattended-upgrades.service - Unattended Upgrades Shutdown
   Loaded: loaded (/lib/systemd/system/unattended-upgrades.service; enabled; v
     Active: active (running) since Tue 2021-03-02 10:25:28 EET; 46min ago
       Docs: man:unattended-upgrade(8)
      Main PID: 619 (unattended-upgr)
         Tasks: 2 (limit: 4654)
        Memory: 11.0M
       CGroup: /system.slice/unattended-upgrades.service
              └─ 619 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upg
Map 02 10:25:28 ioannisserver systemd[1]: Started Unattended Upgrades Shutdown.
[lines 1-11/11 (END)]
[2]+ Stopped                  systemctl status unattended-upgrades
ioannis@ioannisserver:~$ 

```

- Με την πρώτη εντολή εγκαθιστούμε το πακέτο unattended-updates που θα μας βοηθήσει να ενεργοποιήσουμε τις αυτόματες ενημερώσεις ασφαλείας.

- Με την δεύτερη εντολή ελέγχουμε την τρέχουσα κατάσταση (ενεργοποιημένες).

- Με την τρίτη εντολή θα τροποποιήσουμε το αρχείο που περιέχει τις λειτουργίες των αυτόματων ενημερώσεων.

- Σβήνουμε μπροστά από την σημειωμένη με κόκκινο γραμμή τους χαρακτήρες «//» για να λειτουργήσει η γραμμή.

```

Activities Terminal Map 2 11:15
ioannis@ioannisserver:~$ GNU nano 4.8 /etc/apt/apt.conf.d/50unattended-upgrades
// Automatically upgrade packages from these (origin:archive) pairs
//
// Note that in Ubuntu security updates may pull in new dependencies
// from non-security sources (e.g. chromium). By allowing the release
// pocket these get automatically pulled in.
Unattended-Upgrade::Allowed-Origins {
    //${distro_id}:${distro_codename}-security";
    //${distro_id}:${distro_codename}-updates";
    //${distro_id}:${distro_codename}-proposed";
    //${distro_id}:${distro_codename}-backports";
};

// Python regular expressions, matching packages to exclude from upgrading
Unattended-Upgrade::Package-Blacklist {
    // The following matches all packages starting with linux-
    // "linux-";
};

// Use $ to explicitly define the end of a package name. Without
// Read 131 lines
ioannis@ioannisserver:~$ 

```



**321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων**

## **Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση**

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

```
Activities Terminal Map 2 11:19 ioannis@ioannissserver:~ Reading package lists... Done  
Building dependency tree  
Building state information... Done  
unattended-upgrades is already the newest version (2.ubuntu0.1).  
0 upgrades were installed, 0 to remove and 3 not upgraded.  
ioannis@ioannisserver:~$ systemctl status unattended-upgrades  
● unattended-upgrades.service - Unattended Upgrades Shutdown  
   Loaded: loaded (/lib/systemd/system/unattended-upgrades.service; enabled; v...  
   Active: active (running) since Tue 2021-03-02 10:25:28 EET; 46min ago  
     Docs: man:unattended-upgrade(8)  
   Main PID: 616 (unattended-upgr)  
     Tasks: 2 (limit: 4654)  
    Memory: 11.0M  
   CGroup: /system.slice/unattended-upgrades.service  
          └─ 619 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upg...  
  
Map 02 10:25:28 ioannissserver systemd[1]: Started Unattended Upgrades Shutdown.  
[lines 1-11/11 (END)]  
[2]+  Stopped                  systemctl status unattended-upgrades  
  
ioannis@ioannissserver:~$ sudo nano /etc/apt/apt.conf.d/50unattended-upgrades  
ioannis@ioannissserver:~$ sudo nano /etc/apt/apt.conf.d/20auto-upgrades  
ioannis@ioannissserver:~$
```

- Με την εντολή “sudo nano /etc/apt/apt.conf.d/20auto-upgrades” θα τροποποιήσουμε το αρχείο που περιέχει την συχνότητα, την ενεργοποίηση και την απενεργοποίηση αυτόματων ενημερώσεων.
  - Με το νούμερο 1 δηλώνουμε την ενεργοποίηση και με το 0 την απενεργοποίηση. Με το 7 δηλώνουμε ότι το σύστημα θα εκκαθαρίζει τα στοιχεία λήψεις κάθε 7 ημέρες.
  - Συμπερασματικά έχουμε ενεργοποιήσει ενημερώσεις πακέτων, αυτόματη αναβάθμιση και αυτόματο σβήσιμο των στοιχείων λήψης κάθε 7 ημέρες.

Με αυτή την εντολή επιβεβαιώνουμε αν  
η λειτουργία των αυτόματων  
ενημερώσεων έχουν τροποποιηθεί  
σωστά

Όπως παρατηρούμε κανένα από τα πακέτα δεν χρειάζεται ενημέρωση και δεν αναμένεται αυτόματη διαγραφή των στοιχείων λήψης την τρέχουσα στιγμή. Επομένως έχουν όλα εφαρμοστεί σωστά.



## ΝΜΑΡ ΚΑΙ NESSUS ΕΛΕΓΧΟΣ ΠΡΙΝ ΠΡΟΧΩΡΗΣΟΥΜΕ ΣΕ ΕΝΔΥΝΑΜΩΣΗ ΤΟΥ ΛΣ.

```
zenmap - Scan [Profile: Intense scan, all TCP ports] [Scan] [Cancel]
Target: 94.65.57.13 | Command: nmap -p 1-65535 -T4 -A -v 94.65.57.13
Hosts: 1 host up
OS: 94.65.57.13 (Ubuntu 8.2)
Services: 1 service on 94.65.57.13.home.otenet.gr (94.65.57.13)
Ports: 65532 filtered ports
PORT      STATE SERVICE VERSION
1990/tcp  closed  stun-p1
5916/tcp  closed  unknown
22000/tcp open   ssh    OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 3072 b0:6d:5f:ad:2f:b4:2e:3d:51:c4:c5:2e:bb:55:7b:03 (RSA)
|_ 256 cf:aec2:a4:7f:32:b4:8c:0f:3b:b3:a5:53:39:5b:9b (ECDSA)
|_ 256 69:d4:b0:39:fe:61:4d:31:06:bb:22:2f:85:e7:70:77 (ED25519)
Aggressive OS guesses: Linux 4.15 - 5.6 (99%), Linux 5.0 - 5.3 (97%), Linux 5.0 - 5.4 (95%), Linux 2.6.32 (95%), Linux 3.2 - 4.9 (95%), Linux 2.6.32 - 3.10 (94%), Linux 5.3 - 5.4 (94%), Linux 5.4 (94%), Linux 3.4 - 3.10 (93%), Linux 3.1 (93%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 6.079 days (since Thu Mar 04 11:49:25 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1990/tcp)
HOP RTT      ADDRESS
1  0.00 ms  94.65.57.13.home.otenet.gr (94.65.57.13)

NSE: Script Post-scanning.
Initiating NSE at 13:43
Completed NSE at 13:43, 0.00s elapsed
Initiating NSE at 13:43
Completed NSE at 13:43, 0.00s elapsed
Initiating NSE at 13:43
Completed NSE at 13:43, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Map done: 1 IP address (1 host up) scanned in 323.49 seconds
Raw packets sent: 131185 (5.775MB) | Rcvd: 202 (10.704KB)
```

Αρχικά, πραγματοποιήσαμε port scanning με την βοήθεια του λογισμικού ημάρ. Παρατηρούμε ότι μετά το άνοιγμα της θύρας 22000 για την λειτουργία ssh, το ημάρ την ανίχνευσε. Επίσης ανίχνευσε την υπηρεσία που εκτελείται σε αυτή την πόρτα καθώς και την έκδοση της εφαρμογής που επιτυγχάνει την υπηρεσία. Επιπρόσθετα μπόρεσε και βρήκε το λειτουργικό σύστημα που τρέχει ο σέρβερ.



## 321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

The screenshot shows the Nessus Essentials interface with a completed scan report. The left sidebar includes sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules), and TENABLE (Community, Research). A Tenable News sidebar is also present. The main content area displays a table of vulnerabilities under the 'Vulnerabilities' tab, with a total of 32 entries. The table columns include Severity (Sev), Name, Family, and Count. A pie chart in the bottom right corner indicates the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Sev	Name	Family	Count
MIXED	SSL (Multiple Issues)	General	5
LOW	Network daemons not managed by the pa...	Misc.	1
INFO	SSH (Multiple Issues)	General	6
INFO	Netstat Portscanner (SSH)	Port scanners	6
INFO	Remote listeners enumeration (Linux / AIX)	Service detection	6
INFO	Service Detection	Service detection	3
INFO	HTTP (Multiple Issues)	Web Servers	2
INFO	SSH (Multiple Issues)	Misc.	2
INFO	TLS (Multiple Issues)	Service detection	2
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Hostname	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Ethernet MAC Addresses	General	1
INFO	Host Fully Qualified Domain Name (FQD...	General	1
INFO	Inconsistent Hostname and IP Address	Settings	1
INFO	Linux User List Enumeration	General	1

This screenshot shows another completed scan report in the Nessus Essentials interface. The left sidebar and Tenable News section are identical to the first screenshot. The main content area displays a table of vulnerabilities under the 'Vulnerabilities' tab, with a total of 17 entries. The table columns include Severity (Sev), Name, Family, and Count. The distribution of vulnerabilities by severity is shown in a pie chart in the bottom right corner.

Sev	Name	Family	Count
INFO	Ethernet MAC Addresses	General	1
INFO	Host Fully Qualified Domain Name (FQD...	General	1
INFO	Inconsistent Hostname and IP Address	Settings	1
INFO	Linux User List Enumeration	General	1
INFO	Local Checks Enabled	Settings	1
INFO	mDNS Detection (Local Network)	Service detection	1
INFO	Nessus Scan Information	Settings	1
INFO	Nessus Server Detection	Service detection	1
INFO	Netstat Connection Information	General	1
INFO	OS Identification	General	1
INFO	SSH Server Type and Version Information	Service detection	1
INFO	SSL / TLS Versions Supported	General	1
INFO	Strict Transport Security (STS) Detection	Service detection	1
INFO	System Information Enumeration (via DMI)	General	1
INFO	Target Credential Issues by Authenticatio...	Settings	1
INFO	Target Credential Status by Authenticatio...	Settings	1
INFO	Time of Last System Startup	General	1
INFO	Unix / Linux - Local Users Information : P...	Misc.	1
INFO	Unix / Linux Running Processes Information	General	1

Τέλος, πραγματοποιήσαμε port scanning με την βοήθεια του λογισμικού Nessus. Παρατηρούμε ότι στον σέρβερ μας υπάρχουν 32 ευαισθησίες οι οποίες είναι πληροφοριακές και όχι κρίσιμες ή υψηλού ρίσκου. Με την βοήθεια αυτού του ελέγχου, μπορούμε να χτίσουμε έναν ασφαλή σέρβερ ο οποίος θα εκτελεί τις λειτουργίες που του έχουμε ρυθμίσει.



321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

## **ΚΕΦΑΛΑΙΟ 2**

Εγκατάσταση Υπηρεσιών και Ενδυνάμωση



## B1.

The terminal window displays three separate command executions:

- Screenshot 1:** The command `sudo apt purge --auto-remove snapd squashfs-tools friendly-recovery apport at` is run. The output shows the removal of several packages, including `friendly-recovery`, `gdb`, `gdbserver`, `libbbeltrace`, `llbc6-dbg`, `libcct1-dbg`, `libdw1* python3-systemd`, `snapd`, and `squashfs-tools`. It also removes `apport`, `apport-pk`, `friendly-recovery`, `gdb`, `gdbserver`, `libbbeltrace`, `llbc6-dbg`, `libcct1-dbg`, `libdw1* python3-systemd`, `snapd`, and `squashfs-tools`. The command concludes with a note about freeing 217 MB of disk space.
- Screenshot 2:** The command `service --status-all | grep '+'` is run. The output lists numerous services in status '+', including `acpid`, `aparmor`, `avahi-daemon`, `cron`, `cups`, `cups-browsed`, `dbus`, `gdm3`, `grub-common`, `kerneloops`, `kmod`, `network-manager`, `openvpn`, `procs`, `rsyslog`, `ssh`, `udev`, `ufw`, `unattended-upgrades`, and `whoopsie`.
- Screenshot 3:** The command `sudo apt-get --purge remove xinetd nis yp-tools tftpd atftpd tftpd-hpa telnetd rs-h-server rsh-redone-server` is run. The output shows that none of the specified packages are installed, so nothing is removed.

Με αυτή την εντολή διαγράφουμε τα άχρηστα πακέτα που υπάρχουν στο λειτουργικό μας. Αυτά έχουν εγκατασταθεί από την αρχή με αποτέλεσμα ορισμένα από αυτά να μην χρειάζονται.

Με αυτή την εντολή βλέπουμε όλες τις υπηρεσίες που τρέχουν την τρέχουσα στιγμή στο παρασκήνιο.

Με αυτή την εντολή επιχειρούμε να διαγράψουμε ορισμένες υπηρεσίες οι οποίες δεν προτείνονται για έναν σέρβερ. Όπως παρατηρούμε καμία από αυτές δεν υπάρχει στον υπολογιστή μας.



```
Activities Terminal Map 2 12:49
ioannis@ioannisserver:~$ sudo systemctl stop smbd
[sudo] password for ioannis:
Failed to stop smbd.service: Unit smbd.service not loaded.
ioannis@ioannisserver:~$ sudo systemctl disable smbd
Failed to disable unit: Unit file smbd.service does not exist.
ioannis@ioannisserver:~$ sudo systemctl mask smbd
Unit smbd.service does not exist, proceeding anyway.
Created symlink /etc/systemd/system/smbd.service → /dev/null.
ioannis@ioannisserver:~$ sudo systemctl stop nmbd
Failed to stop nmbd.service: Unit nmbd.service not loaded.
ioannis@ioannisserver:~$ sudo systemctl disable nmbd
Unit /etc/systemd/system/smbd.service is masked, ignoring.
ioannis@ioannisserver:~$ sudo systemctl disable nmbd
Failed to disable unit: Unit file nmbd.service does not exist.
ioannis@ioannisserver:~$ sudo systemctl mask nmbd
Unit nmbd.service does not exist, proceeding anyway.
Created symlink /etc/systemd/system/nmbd.service → /dev/null.
ioannis@ioannisserver:~$ /etc/xinetd.d/rsh
bash: /etc/xinetd.d/rsh: No such file or directory
ioannis@ioannisserver:~$ sudo systemctl stop rexecd
Failed to stop rexecd.service: Unit rexecd.service not loaded.
ioannis@ioannisserver:~$ sudo systemctl disable rexecd
Failed to disable unit: Unit file rexecd.service does not exist.
ioannis@ioannisserver:~$ sudo systemctl mask rexecd
Unit rexecd.service does not exist, proceeding anyway.
Created symlink /etc/systemd/system/rexecd.service → /dev/null.
ioannis@ioannisserver:~$ systemctl mask udisks2
Created symlink /etc/systemd/system/udisks2.service → /dev/null.
ioannis@ioannisserver:~$ systemctl mask rpcbind
Unit rpcbind.service does not exist, proceeding anyway.
Created symlink /etc/systemd/system/rpcbind.service → /dev/null.
ioannis@ioannisserver:~$ systemctl mask inetd
Unit inetd.service does not exist, proceeding anyway.
Created symlink /etc/systemd/system/inetd.service → /dev/null.
ioannis@ioannisserver:~$
```

Στο παραπάνω στιγμιότυπο φαίνονται με την σειρά οι παρακάτω ενέργειες:

- Απενεργοποίηση του smbd: παρέχει filesharing and printing υπηρεσίες σε πελάτες Windows.
- Απενεργοποίηση του nmbd: καταλαβαίνει και απαντά σε NetBIOS μέσω IP name service αιτήματα.
- Απενεργοποίηση του rexec: επιτρέπει να εκτελούνται εντολές κελύφους σε έναν απομακρυσμένο υπολογιστή.
- Απενεργοποίηση του automount: προσαρμόζει αυτόματα διαφορετικά συστήματα αρχείων για να εμφανίσει το σύστημα αρχείων δικτύου.
- Απενεργοποίηση του portmap: εάν αυτή η υπηρεσία εκτελείται, σημαίνει ότι εκτελείται διακομιστής NFS.
- Απενεργοποίηση του inetd: εάν εκτελείται αυτόνομη εφαρμογή όπως το ssh που χρησιμοποιεί άλλη αυτόνομη εφαρμογή τότε δεν χρειάζεται το inetd.

#### ΠΡΟΣΟΧΗ!

Σε ορισμένα στιγμιότυπα, η ημερομηνία είναι προγενέστερη λόγω λαθών που είχαμε και τα διορθώσαμε μελλοντικά. Για παράδειγμα, ο web server μας πήρε αρκετή ώρα για να λειτουργήσει λόγω ασάφειας πολλών sites από τις οποίες συμβουλευτήκαμε την δημιουργία του.



**321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων**

## **Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση**

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

**B2.**

```
Activities Terminal Map 2 13:04
loannis@loannisserv: ~
E: Unable to locate package alsautils-libs:i386
loannis@loannisserv: ~$ sudo apt-get remove alsierlot
Reading packages...
Building dependency tree...
Reading state information...
The following packages were automatically installed and are no longer required:
  gule-2.2-libs libgcrc2
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  alsierlot
0 upgraded, 0 newly installed, 1 to remove and 3 not upgraded.
After this operation, 9011 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database... 185882 files and directories currently installed.)
Removing alsierlot (1.0.0-1ubuntu1) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for libgbib2.0-0:amd64 (2.64.6-1~ubuntu20.04.1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu1) .
loannis@loannisserv: ~$ sudo apt-get remove gnome-mahjongg
Reading package lists... done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gule-2.2-libs libgcrc2
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  gnome-mahjongg
0 upgraded, 0 newly installed, 1 to remove and 3 not upgraded.
After this operation, 3441 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database... 183925 files and directories currently installed.)
Removing gnome-mahjongg (1.13.36.1-1) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for libgbib2.0-0:amd64 (2.64.6-1~ubuntu20.04.1) ...
```

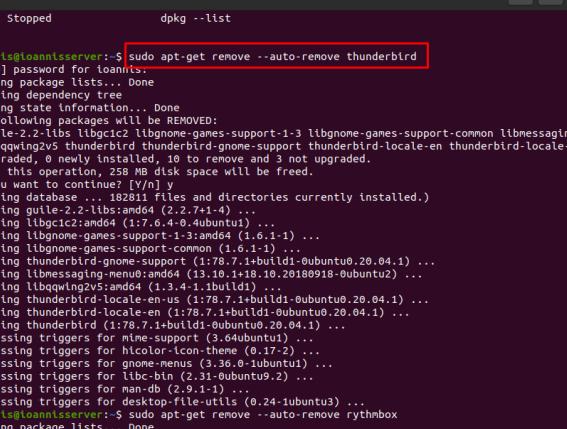
- Με την πρώτη εντολή διαγράφουμε το παιχνίδι που λέγεται *aisleriot*

- Με την δεύτερη εντολή διαγράφουμε το παιχνίδι mahjongg

```
Activities Terminal Map 2 13:04
loannis@loannisserver: ~
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for libglib2.0-0:amd64 (2.64.6-1ubuntu20.04.1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
loannis@loannisserver: $ sudo apt-get remove gnome-mines
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  guile-2.2.1-libs libgpgc2 libphoneme-games-support-1-i3 libgnome-games-support-common
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  gnome-mines
  0 upgraded, 0 newly installed, 1 to remove and 3 not upgraded.
After this operation, 782 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 183454 files and directories currently installed.)
Removing gnome-mines (1:3.36.0-1ubuntu1) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for libglib2.0-0:amd64 (2.64.6-1ubuntu20.04.1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
loannis@loannisserver: $ sudo apt-get remove gnome-sudoku
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  guile-2.2.1-libs libgpgc2 libphoneme-games-support-1-i3 libgnome-games-support-common liblqqwing2v5
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  gnome-sudoku
  0 upgraded, 0 newly installed, 1 to remove and 3 not upgraded.
After this operation, 963 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 183264 files and directories currently installed.)
```

- Με την πρώτη εντολή διαγράφουμε το παιχνίδι που λέγεται mines

- Με την δεύτερη εντολή διαγράφουμε το παιχνίδι sudoku



```
Activities Terminal Map 2 14:08
loannis@loannisserver:~ [8]+ Stopped dpkg --list
loannis@loannisserver:~ $ sudo apt-get remove --auto-remove thunderbird
[sudo] password for loannis:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  guile-2.2-libs libglibc2 libgnome-games-support-1-3 libgnome-games-support-common libmessaging-menubar0
  libgwingv2s thunderbird thunderbird-gnome-support thunderbird-locale-en thunderbird-locale-en-us
0 upgraded, 0 newly installed, 10 to remove and 3 not upgraded.
After this operation, 258 MB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 182811 files and directories currently installed.)
Removing guile-2.2-libs:amd64 (2.2.7.1-4) ...
Removing libglibc2:amd64 (1:7.6.4-0.4ubuntu1) ...
Removing libgnome-games-support-1-3:amd64 (1:3.0.1-1) ...
Removing libgnome-games-support-common (1:3.0.1-1) ...
Removing libmessaging-menubar0:amd64 (17.0.1+build1:0ubuntu0.20.04.1) ...
Removing libgwingv2s:amd64 (1:3.4.1-1ubuntu1) ...
Removing thunderbird-locale-en (1:78.7.1+build1:0ubuntu0.20.04.1) ...
Removing thunderbird-locale-en (1:78.7.1+build1:0ubuntu0.20.04.1) ...
Removing thunderbird (1:78.7.1+build1:0ubuntu0.20.04.1) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
loannis@loannisserver:~ $ sudo apt-get remove --auto-remove rythmbox
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package rythmbox
loannis@loannisserver:~ $ sudo apt-get remove --auto-remove rythmbox
Reading package lists... Done
```

- Με την πρώτη εντολή διαγράφουμε την εφαρμογή που λένεται *thunderbird*

- Με την δεύτερη εντολή διαγράφουμε την εφαρμογή που λένεται rhythmbox



## 321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

## **Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση**

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

Με αυτή την εντολή  
διαγράφουμε τις εφαρμογές  
libreoffice.

Με αυτή την εντολή  
διαγράφουμε την εφαρμογή  
transmission-gtk.

```
Activities Terminal Map 2 14:13
loannis@loannisserver:~
```

Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...

```
loannis@loannisserver:~$ sudo apt-get remove --auto-remove remmina
```

Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages will be REMOVED:  
libavahi-ui-gtk3-0 libfreerdp-client2-2 libfreerdp2-2 libvncclient1 libwinpr2-2 remmina remmina-common  
0 upgraded, 0 newly installed, 10 to remove and 3 not upgraded.  
After this operation, 19.5 MB disk space will be freed.  
Do you want to continue? [y/n] y  
(Reading database ... 168341 files and directories currently installed.)  
Removing remmina-plugin-vnc:amd64 (1:4.2+dfsg-1ubuntu1) ...  
Removing remmina-plugin-vnc:amd64 (1:4.2+dfsg-1ubuntu1) ...  
Removing remmina-plugin-rdp:amd64 (1:4.2+dfsg-1ubuntu1) ...  
Removing libfreerdp-client2-2:amd64 (2.2.0+dfsg1-0ubuntu20.04.1) ...  
Removing libfreerdp2-2:amd64 (2.2.0+dfsg1-0ubuntu20.04.1) ...  
Removing libvncclient1:amd64 (0.9.12+dfsg-9ubuntu0.3) ...  
Removing libwinpr2-2:amd64 (2.2.0+dfsg1-0ubuntu20.04.1) ...  
Removing remmina (1:4.2+dfsg-1ubuntu1) ...  
Removing libavahi-ui-gtk3-0:amd64 (0.7-1ubuntu7) ...  
Removing remmina-common (1:4.2+dfsg-1ubuntu1) ...  
Processing triggers for gnome-icon-theme (0.17-2) ...  
Processing triggers for gnome-menu (3.36.0-1ubuntu1) ...  
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...  
Processing triggers for man-db (2.9.1-1) ...  
Processing triggers for shared-mime-info (1:15.1-1) ...  
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...  
loannis@loannisserver:~\$ sudo apt-get remove --auto-remove livepatch

Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
E: Unable to locate package livepatch

```
loannis@loannisserver:~$ sudo apt-get clean
```

```
loannis@loannisserver:~$ sudo apt-get autoremove
```

Reading package lists... Done  
Building dependency tree  
Reading state information... Done

- Με την πρώτη εντολή διαγράφουμε την εφαρμογή που λέγεται remmina.

- Με την δεύτερη εντολή κάνουμε ένα καθάρισμα στο λειτουργικό μας.

- Με την τρίτη εντολή αφαιρούμε όλα τα πακέτα που εγκαταστάθηκαν αυτόματα επειδή απαιτούσαν κάποια άλλα πακέτα



## B3. [WEB SERVICE]

```
loannis@ioannissserver:~$ sudo apt update
Hit:1 http://gr.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [109 kB]
Get:3 http://security.ubuntu.com/ubuntu focal-updates InRelease [110 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-backports InRelease [24,3 kB]
Get:5 http://gr.archive.ubuntu.com/ubuntu focal Metadata [59,2 kB]
Get:6 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Metadata [59,2 kB]
Get:7 http://gr.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [264 kB]
Get:8 http://gr.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Metadata [302 kB]
Get:9 http://gr.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11 48x48 Icons [196 kB]
Get:10 http://gr.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Metadata [2468 kB]
Get:11 http://gr.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11 Metadata [1768 kB]
Fetched 1173 kB in 2s (540 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
3 packages can be upgraded. Run 'apt list --upgradable' to see them.
loannis@ioannissserver:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
  libcurl4 liblbu5.2-0
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2-bin apache2-data apache2-utils libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libcurl4 liblbu5.2-0
0 upgraded, 3 newly installed, 0 to remove and 3 not upgraded.
Need to get 0 B of archives.
After this operation, 8639 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://gr.archive.ubuntu.com/ubuntu focal/main amd64 libapr1 amd64 1.6.5-1ubuntu1 [91,4 kB]
Get:2 http://gr.archive.ubuntu.com/ubuntu focal/main amd64 libaprutil1 amd64 1.6.1-4ubuntu2 [84,7 kB]
Get:3 http://gr.archive.ubuntu.com/ubuntu focal/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-4ubuntu2 [0,5 kB]
Get:4 http://gr.archive.ubuntu.com/ubuntu focal/main amd64 libaprutil1-ldap amd64 1.6.1-4ubuntu2 [8736 B]
Gpg: https://archive.ubuntu.com/ubuntu Fingerprint: 40 14 3b 8d 8e 20 41 7f 9b 1c 2c 3d 93 4d 1d 11
```

- Με την πρώτη εντολή κάνουμε μία γενική ενημέρωση στο ΛΣ.

- Με την δεύτερη εντολή εγκαθιστούμε το apache2 που είναι απαραίτητο για τη δημιουργία του web service του σέρβερ μας.

```
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
loannis@ioannissserver:~$ sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  CUPS
  OpenSSH
loannis@ioannissserver:~$ sudo ufw allow 'Apache'
Rule added
Rule added (v6)
loannis@ioannissserver:~$ sudo ufw status
Status: active

To                         Action      From
--                         --          --
OpenSSH                   ALLOW      Anywhere
Apache                    ALLOW      Anywhere
OpenSSH (v6)               ALLOW      Anywhere (v6)
Apache (v6)                ALLOW      Anywhere (v6)

loannis@ioannissserver:~$ sudo systemctl status apache2
● apache2.service - The Apache2 HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-03-02 14:19:00 EET; 2min 15s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 13181 (apache2)
      Tasks: 55 (limit: 4654)
     Memory: 5.0M
        CPU: 0.000 CPU(s)
       CGroup: /system.slice/apache2.service
               ├─13181 /usr/sbin/apache2 -k start
               ├─13184 /usr/sbin/apache2 -k start
               └─13185 /usr/sbin/apache2 -k start

Mar 02 14:19:00 ioannissserver systemd[1]: Starting The Apache HTTP Server...
Mar 02 14:19:00 ioannisserver apache2[13180]: AH00550: apache2: Could not reliably determine the server's fully qualified name, using 192.168.1.155 for Port 80
Mar 02 14:19:00 ioannisserver systemd[1]: Started The Apache HTTP Server.
lines: 1-15 (END)
```

- Με την πρώτη εντολή βλέπουμε ποιες εφαρμογές μπορούν να τρέξουν στο firewall.

- Με την δεύτερη εντολή επιτρέπουμε στο Apache να περνάει μέσα από το firewall.

- Με την τρίτη εντολή βλέπουμε ποιες εφαρμογές τρέχουν στο firewall καθώς και την κατάστασή του την τρέχουσα χρονική στιγμή.

- Με την τέταρτη εντολή βλέπουμε την τρέχουσα κατάσταση του apache2 (ενεργοποιημένο).

The screenshot shows a Firefox browser window displaying the "Apache2 Ubuntu Default Page". The page title is "Apache2 Ubuntu Default Page" and the header features the Ubuntu logo. The main content says "It works!" and provides a brief overview of the Apache server's default configuration. A "Configuration Overview" section details the layout of the configuration files, mentioning "/etc/apache2/", "/etc/apache2/conf-available/", and "/etc/apache2/sites-available/". The browser's address bar shows the URL "192.168.1.155". On the right side of the screen, there is a terminal window showing the command line interface with several tabs open, including "HTTP S" and "TTP Se".

Αφού ολοκληρώσουμε όλα τα παραπάνω βήματα, εάν πάμε στον browser και πληκτρολογήσουμε την IP του σέρβερ μας, θα δούμε ότι το apache δούλεψε κανονικά και ότι το web service δουλεύει άψογα (βλέπουμε την αρχική σελίδα του apache).



- Με την πρώτη εντολή κάνουμε εγκατάσταση το πακέτο curl για να μάθουμε την public ip μας.

- Με την δεύτερη εντολή μαθαίνουμε την public ip μας.

- Με την πρώτη εντολή μαθαίνουμε το hostname του σέρβερ μας το οποίο θα φιλοξενήσει web service, dns service καθώς και sftp service.

- Με την δεύτερη εντολή επαναφορτώνουμε το apache.

- Με την τρίτη εντολή ελέγχουμε ποιες εφαρμογές τρέχουν στο firewall.

- Με την τέταρτη εντολή επιτρέπουμε την εφαρμογή Apache Full στο firewall (http & https).

- Με την πέμπτη εντολή διαγράφουμε το απλό Apache από το firewall (http).

```
Activities Terminal Map 4 09:11
loannis@loannisserver:~
```

loannis@loannisserver:~ \$ sudo ufw status  
[sudo] password for loannis:  
Status: active

To	Action	From
...	---	---
OpenSSH	ALLOW	Anywhere
Apache Full	ALLOW	Anywhere
53	ALLOW	192.168.0.0/24
5 Filesystem root	ALLOW	192.168.0.0/24
OpenSSH (v6)	ALLOW	Anywhere (v6)
Apache Full (v6)	ALLOW	Anywhere (v6)

loannis@loannisserver:~ \$ sudo ufw allow http  
Rule added  
Rule added (v6)  
loannis@loannisserver:~ \$ sudo ufw allow 80  
Rule added  
Rule added (v6)  
loannis@loannisserver:~ \$ sudo ufw status  
Status: active

To	Action	From
...	---	---
OpenSSH	ALLOW	Anywhere
Apache Full	ALLOW	Anywhere
53	ALLOW	192.168.0.0/24
5 Filesystem root	ALLOW	192.168.0.0/24
80/tcp	ALLOW	Anywhere
80	ALLOW	Anywhere
OpenSSH (v6)	ALLOW	Anywhere (v6)
Apache Full (v6)	ALLOW	Anywhere (v6)
80/tcp (v6)	ALLOW	Anywhere (v6)
80 (v6)	ALLOW	Anywhere (v6)

loannis@loannisserver:~ \$ sudo ufw allow https

- Με την πρώτη εντολή ελέγχουμε ποιες εσφαρμογές τρέχουν στο firewall.

- Με την δεύτερη εντολή επιτρέπουμε το http στο firewall.

- Με την τρίτη εντολή ανοίγουμε την πόρτα 80 firewall (http).

- Με την τέταρτη εντολή ελέγχουμε ποιες εφαρμογές τούχουν στο firewall.

- Με την πέμπτη εντολή επιτρέπουμε το https στο firewall



## 321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

```

Activities Terminal Map 4 09:11
loannis@ioannisserver: ~
loannis@ioannisserver:~$ sudo ufw allow http
Rule added
Rule added (v6)
loannis@ioannisserver:~$ sudo ufw allow 80
Rule added
Rule added (v6)
loannis@ioannisserver:~$ sudo ufw status
Status: active
To Action From
-- -
OpenSSH ALLOW Anywhere
Apache Full ALLOW Anywhere
53 ALLOW 192.168.0.0/24
53 ALLOW 192.168.1.0/24
5 ALLOW 192.168.0.0/24
OpenSSH (v6) ALLOW Anywhere (v6)
Apache Full (v6) ALLOW Anywhere (v6)
80/tcp ALLOW Anywhere
80 ALLOW Anywhere
OpenSSH (v6) ALLOW Anywhere (v6)
Apache Full (v6) ALLOW Anywhere (v6)
80/tcp (v6) ALLOW Anywhere (v6)
80 (v6) ALLOW Anywhere (v6)

loannis@ioannisserver:~$ sudo ufw allow https
Rule added
Rule added (v6)
loannis@ioannisserver:~$ sudo ufw allow 443
Rule added
Rule added (v6)
loannis@ioannisserver:~$ 

```

```

Activities Terminal Map 5 13:08
loannis@ioannisserver: ~
loannis@ioannisserver:~$ sudo cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/e/ioannisserver.com.conf
1
loannis@ioannisserver:~$ sudo nano /etc/apache2/sites-available/000-default.conf
2
loannis@ioannisserver:~$ sudo a2ensite ioannisserver.com.conf
3
loannis@ioannisserver:~$ sudo service apache2 restart
4
Enabling site ioannisserver.com.
To activate the new configuration, you need to run:
  systemctl reload apache2
5
loannis@ioannisserver:~$ systemctl reload apache2
6
loannis@ioannisserver:~$ cd /var/www
7
loannis@ioannisserver:/var/www$ mkdir ioannisserver
mkdr: cannot create directory 'ioannisserver': Permission denied
loannis@ioannisserver:/var/www$ sudo mkdir ioannisserver

```

Με αυτή εντολή ανοίγουμε την πόρτα 443 firewall (https).

1. Αντιγράφουμε τα περιεχόμενα του αρχείου 000-default.conf στο αρχείο ioannisserver.com.conf που αποτελεί το virtual host της ιστοσελίδας www.ioannisserver.com.
2. Προσθέτουμε στο αρχείο 000-default.conf αυτό που είναι σημεωμένο σε κόκκινο περίγραμμα. Αυτό βοηθά στο redirection από http σε https.
3. Στο αρχείο ioannisserver.com.conf ρυθμίζουμε το όνομα του σέρβερ, το email, την τοποθεσία που βρίσκεται η ιστοσελίδα που θα φτιάξουμε και ενεργοποιούμε το https προσθέτοντας τις διαδρομές που βρίσκονται τα απαραίτητα πιστοποιητικά για να ενεργοποιηθεί το https.
4. Ενεργοποιούμε την ιστοσελίδα www.ioannisserver.com.
5. Επαναφορτώνουμε το apache2 για να δουλέψει η ιστοσελίδα.
6. Αλλάζουμε directory και προσθίνουμε εκεί που υπάρχουν οι ιστοσελίδες μας.
7. Δημιουργούμε έναν φάκελο που θα περιέχει τα αρχεία της ιστοσελίδας μας.

### Νούμερο 2 (από τα παραπάνω βήματα)

ΑΡΧΕΙΟ: 000-default.conf

```

Activities Terminal Map 5 13:31
loannis@ioannisserver: ~
loannis@ioannisserver:~$ nano 000-default.conf
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # directive sets the host name and port used by the virtual host to
    # match this virtual host. For the default virtual host (this file), this
    # value is not decisive as it is used as a last resort host regardless.
    # However, if you ever set it for any further virtual host explicitly,
    # it overrides the value set here.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    Redirect "/" "https://www.ioannisserver.com/"

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include them by reference and combine them. It is also possible to
    # follow a link to an external file and include that file here. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 noet

```

### Νούμερο 3 (από τα παραπάνω βήματα)

ΑΡΧΕΙΟ: ioannisserver.com.conf

```

Activities Terminal Map 5 13:16
loannis@ioannisserver: ~
loannis@ioannisserver:~$ nano ioannisserver.com.conf
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # directive sets the host name and port used by the virtual host to
    # match this virtual host. For the default virtual host (this file), this
    # value is not decisive as it is used as a last resort host regardless.
    # However, if you ever set it for any further virtual host explicitly,
    # it overrides the value set here.
    ServerName www.ioannisserver.com
    ServerAdmin ioannis@ioannisserver.com
    DocumentRoot /var/www/ioannisserver/public_html

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
    BrowserMatch "MSIE [2-6]" \
        nonkeepalive ssl-unclean-shutdown \
        downgrade-1.0 force-response-1.0
    # For most configuration files from conf-available/, which are

```



321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

## **Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση**

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

```
Activities Terminal Map 5 13:17 en ⓘ
loannis@loannisserver:~
```

```
[loannis@loannisserver:~/var/www]$ cd loannisserver
[loannis@loannisserver:~/var/www/loannisserver]$ mkdir public_html
mkdir: cannot create directory 'public_html': Permission denied
[loannis@loannisserver:~/var/www/loannisserver]$ sudo mkdir public_html
[loannis@loannisserver:~/var/www/loannisserver]$ cd public_html
[loannis@loannisserver:~/var/www/loannisserver/public_html]$ ls
[loannis@loannisserver:~/var/www/loannisserver/public_html]$ nano index.html
[loannis@loannisserver:~/var/www/loannisserver/public_html]$ sudo nano index.html
[loannis@loannisserver:~/var/www/loannisserver/public_html]$ sudo service apache2 restart
[loannis@loannisserver:~/var/www/loannisserver/public_html]$ sudo nano /etc/apache2/sites-available/loannisserver.com.conf
[loannis@loannisserver:~/var/www/loannisserver/public_html]$ sudo service apache2 restart
[loannis@loannisserver:~/var/www/loannisserver]$ cd ..
[loannis@loannisserver:~/var/www]$ sudo nano /etc/resolv.conf
[loannis@loannisserver:~/var/www]$ sudo nano /etc/apache2/sites-available/loannisserver.com.conf
[loannis@loannisserver:~/var/www]$ sudo nano /etc/network/01-network-manager-all.yaml
[loannis@loannisserver:~/var/www]$ sudo nano /etc/network/interfaces
[loannis@loannisserver:~/var/www]$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt
Generating a RSA private key
.....+=====
writing new private key to '/etc/ssl/private/apache-selfsigned.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields, but you can leave some blank
For some fields there will be a default value
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:GR
State or Province Name (full name) [Some-State]:Samos
Locality Name (eg, city) []:Karlovasi
Organization Name (eg, company) [Internet Widgets Pty Ltd]:PanosIoannis
Organizational Unit Name (eg, section) []:server
Common Name (e.g. server FQDN or YOUR name) []:loannisserver.com
Email Address []:loannis@loannisserver.com
```

1. Αλλάζουμε directory και μπαίνουμε μέσα στον φάκελο των οποίο δημιουργήσαμε πριν και περιέχει όλα τα αρχεία της ιστοσελίδας μας.
  2. Φτιάχνουμε έναν φάκελο που θα περιέχει την δημόσια ιστοσελίδα.
  3. Πηγαίνουμε στον φάκελο που φτιάχαμε στο βήμα 2.
  4. Βλέπουμε αν έχει κάποιο άλλο αρχείο μέσα.
  5. Δημιουργούμε ένα δοκιμαστικό html αρχείο για να δούμε αν δουλεύει η ιστοσελίδα μας στην συνέχεια.
  6. Τροποποιούμε το δοκιμαστικό html αρχείο.
  7. Επανεκκινούμε το apache2 για να ενεργοποιηθούν οι αλλαγές.
  8. Αλλάζουμε directory και πηγαίνουμε στο αρχικό μας.
  9. Ρυθμίζουμε εκείνα που είναι μέσα σε κόκκινο περίγραμμα στο παρακάτω screenshot. Οταν βλέπει την δ/ση 127.0.0.1 θα καταλαβαίνει ότι είναι ο σέρβερ με hostname ioannissserver.com.
  10. Ρυθμίζουμε εκείνα που είναι μέσα σε κόκκινο περίγραμμα σε παρακάτω screenshot. Η ιστοσελίδα μας θα έχει τον σέρβερ μας για DNS server τον οποίο θα τον τροποποιήσουμε στην συνέχεια.
  11. Ρυθμίζουμε εκείνα που είναι μέσα σε κόκκινο περίγραμμα σε παρακάτω screenshot. Βάζουμε τα στοιχεία του σέρβερ μας έτσι ώστε η ιστοσελίδα να έχει για DNS server τον δικό μας σέρβερ.
  12. Ενεργοποιούμε το SSL Certificate βάζοντας τα στοιχεία μας. Στην ουσία δημιουργεί αρχεία σε ένα συγκεκριμένο χώρο και μετά οδηγούμε την ιστοσελίδα σε αυτά τα αρχεία. Εμείς χρησιμοποιήσαμε το openssl για την ενεργοποίηση του https.

**Νούμερο 9 (από τα παραπάνω βήματα)**

## APXEIO: resolv.conf

```
Activities Terminal Map 5:1307 en
loannis@loannisserver: ~
GNU nano 4.8
/etc/resolv.conf
# /etc/resolv.conf(5) FILE for glibc resolver library. See resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the system-resolved stub resolver.
# run "systemctl resolve --status" to see details about the actual nameservers.

nameserver 127.0.0.1
search loannisserver.com

Get Help Exit Write Out Read File Where Is Replace Cut Text Paste Text Justify Undo Redo
```

#### **Νούμερο 10 (από τα παραπάνω βήματα)**

## **APXEIO: 01-network-manager-all.conf**

### Νούμερο 11 (από τα παραπάνω βήματα)

## APXEIO: interfaces

```
Activities Terminal Map 5 13:14
loannis@loannisserver: ~
GNU nano 4.8
# /etc/network/interfaces
auto lo
iface lo inet loopback
auto ens33
iface ens33 inet static
    address 192.168.1.155
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255
    gateway 192.168.1.1
    dns-nameservers 127.0.0.1
    dns-search loannisserver.com
```



```

Activities Terminal Map 5 13:42
loannis@ioannisserv:~ 
[sudo] password for ioannis: 
loannis@ioannisserv:~ $ sudo nano /etc/apache2/conf-available/ssl-params.conf
loannis@ioannisserv:~ $ sudo nano /etc/apache2/conf-available/ssl-params.conf
loannis@ioannisserv:~ $ sudo cp /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-available/ssl-params.conf.bak
loannis@ioannisserv:~ $ sudo nano /etc/apache2/sites-available/default-ssl.conf
loannis@ioannisserv:~ $ sudo nano /etc/apache2/sites-available/default-ssl.conf
loannis@ioannisserv:~ $ sudo nano /etc/apache2/sites-available/default-ssl.conf
loannis@ioannisserv:~ $ sudo nano /etc/apache2/sites-available/ssl-params.conf
loannis@ioannisserv:~ $ sudo nano /etc/apache2/sites-available/ssl-params.conf
loannis@ioannisserv:~ $ sudo nano /etc/apache2/conf-available/ssl-params.conf

Your choices are: access_compat actions alias allowmethods asts auth_basic auth_digest auth_form authn_anon
authn_core authn_dbd authn_file authn_socache authnz_fcgI authnz_ldap authnz_core authnz_dbd auth
bz_dbm authz_groupfile authz_host authz_owner authz_user autoindex_brotli buffer cache cache_disk cache_so
cache_cern_meta cgi cgi_lsseal_lite data dav dav_fs dav_lock dbd deflate dialup dir dump_lo echo env exp
ires ext_filter file_cache filter headers heartbeat heartbeat_monitor http2 ident imagemap include info libmetho
d_imbusyness libmethod_byrequests libmethod_forensic ldap log_debug log_forensic lua macro
mime_magic mime_event mpn_prefork mpn_worker negotiation proxy proxy_ajp proxy_balancer proxy_co
nnect proxy_express proxy_fcgi proxy_http proxy_scgi proxy_uwsgi proxy_wstunnel reflector rewrite requirement request_rewrite sed session
set_cookie session_crypto session_dbd setenvif slotmem_plain slotmem_shm socache_dbm socache_mencache socac
he_redis socache_shmcb spelling ssl status substitute suexec unique_id userdir usertrack vhost_alias xmlien
c

Which module(s) do you want to enable (wildcards ok)?
^Z
[1]+  Stopped                  sudo a2enmod
loannis@ioannisserv:~ $ sudo a2enmod ssl
Considering dependency ssl for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
loannis@ioannisserv:~ $ sudo a2enmod headers
Enabling module headers.

```

1. Φτιάχνουμε ένα backup για το αρχείο default-ssl.conf το οποίο περιέχει τα ορίσματα για το ssl πιστοποιητικό.

2. Ρυθμίζουμε εκείνα που είναι μέσα σε κόκκινο περίγραμμα σε παρακάτω screenshot. Όπου βλέπουμε localhost, το αντικαθιστούμε με το hostname του σέρβερ μας (ioannisserv.com). Δηλώνουμε το μονοπάτι για την ιστοσελίδα μας, ενεργοποιούμε το SSL και υποδεικνύουμε τις διαδρομές προς τα αρχεία (το πιστοποιητικό και το κλειδί) που αποτελούν το ssl.

3. Ρυθμίζουμε εκείνα που είναι μέσα σε κόκκινο περίγραμμα σε παρακάτω screenshot. Βάζουμε τις παραμέτρους που θέλουμε να λειτουργεί το πιστοποιητικό ssl. Για παράδειγμα, δηλώνουμε την νεότερη έκδοση του πιστοποιητικού, την ηλικία του καθώς και την εμφάνιση του https στην περιοχή του URL του browser.

4. Ενεργοποιούμε το ssl certificate.

5. Ενεργοποιούμε τις κεφαλίδες για την εμφάνιση του https στην περιοχή του URL του browser.

**Νούμερο 2 (από τα παραπάνω βήματα)****ΑΡΧΕΙΟ: default-ssl.conf**

```

Activities Terminal Map 5 13:31
loannis@ioannisserv:~ 
GNU nano 4.8 /etc/apache2/sites-available/default-ssl.conf
[ifModule mod_ssl.c]
<VirtualHost _default_:443>
    ServerAdmin ioannis@ioannisserv.com
    ServerName www.ioannisserv.com
    ServerName ioannisserv.com
    DocumentRoot /var/www/ioannisserv/public_html

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example
    # the "Include conf-available/serve-cgi-bin.conf" line above.
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf

    # SSL Engine Switch:
    #   Enable/Disable SSL for this virtual host.
    SSLEngine on

    # A self-signed (snakeoil) certificate can be created by installing
    # the self-signed package:
    # /usr/share/doc/python2.7/README.Debian.gz for more info.
    # If both key and certificate are stored in the same file, only the
    # SSLCertificateFile directive is needed.
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

```

**ΠΡΟΣΟΧΗ!**

Εντολές που δεν έχουμε περιλάβει σε κόκκινο πλαίσιο, σημαίνει ότι είτε έχουν επαναληφθεί σε προηγούμενα βήματα, είτε χρησιμοποιήθηκαν για να βγουν τα στιγμιότυπα, είτε για να διορθώσουμε ορισμένα πράγματα που είχαμε παραλείψει.

**Νούμερο 3 (από τα παραπάνω βήματα)****ΑΡΧΕΙΟ: ssl-params.conf**

```

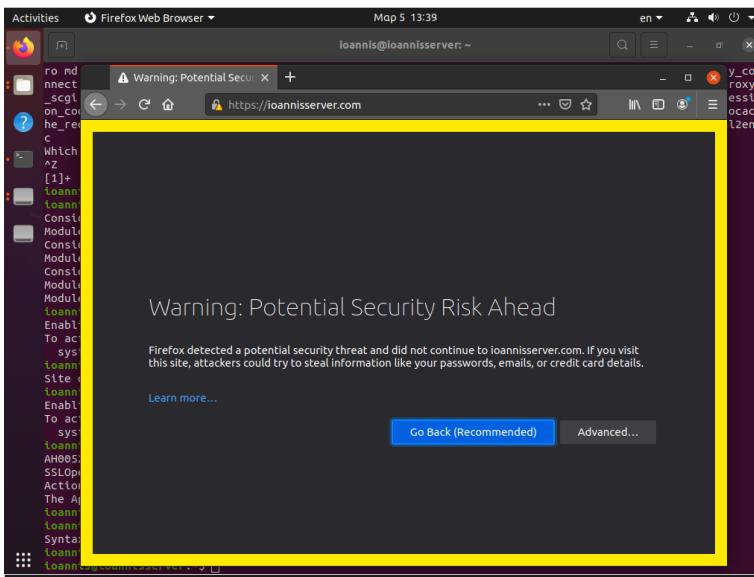
Activities Terminal Map 5 13:37
loannis@ioannisserv:~ 
GNU nano 4.8 /etc/apache2/conf-enabled/ssl-params.conf
SSLCipherSuite ECDH+AESGCM:EDH+AESGCM:AE5256+ECDH:AE5256+EDH
SSLProtocol All -SSLv2 +SSLv3
SSLHonorCipherOrder On
# Disable preloading HSTS for now. You can use the commented out header line that includes
# a "preload" directive if you understand its implications.
#Header always set Strict-Transport-Security "max-age=63072000; includeSubdomains; preload"
Header always set Strict-Transport-Security "max-age=63072000; includeSubdomains"
Header always set X-Frame-Options DENY
Header always set X-Content-Type-Options nosniff
# Requires Apache >= 2.4
SSLOptions +StdEnvVars
SSLSessionTickets Off
SSLUseStapling on
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"
```



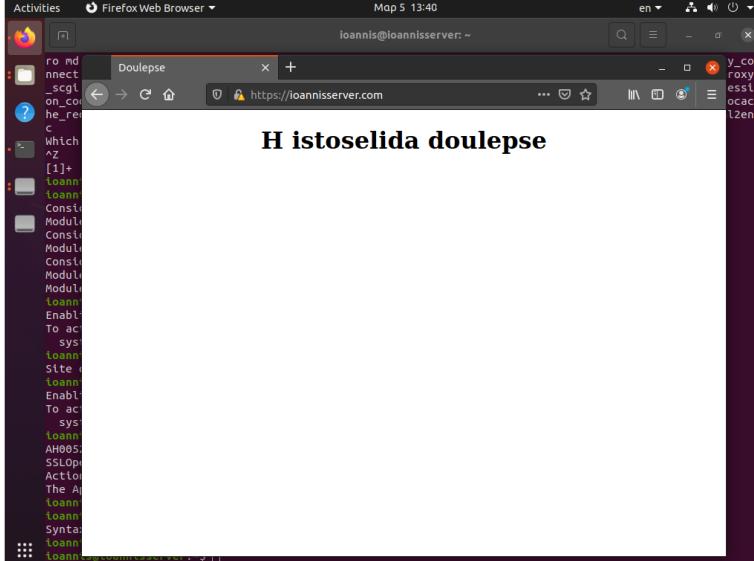
```
ro md mime mime_magic mime_event mpm_prefork mpm_worker negotiation proxy proxy_balancer proxy_connect proxy_express proxy_fcgi proxy_fdpass proxy_ftp proxy_hcheck proxy_html proxy_http proxy_http2 proxy_scgi proxy_uwsgi proxy_wstunnel ratelimit reflector remotelog requiretimeout request rewrite sed session sessi on_cookie session_crypto session_dbd setenvif slotmem_plain slotmem_shm socache_dbm socache_memcache socac he_redis socache_shmcb spelling ssl status substitute suexec unique_id userdir usertrack vhost_alias xml2en c

Which module(s) do you want to enable (wildcards ok)?
[1]+ Stopped sudo azenmod
loannis@ioannisserver:~$ sudo azenmod ssl
Considering dependency ssl for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
loannis@ioannisserver:~$ sudo azenmod headers
Enabling module headers.
To activate the new configuration, you need to run:
systemctl restart apache2
loannis@ioannisserver:~$ sudo a2ensite default-ssl
Site default-ssl already enabled
loannis@ioannisserver:~$ sudo a2enconf ssl-params
Enabling conf ssl-params
To activate the new configuration, you need to run:
systemctl reload apache2
loannis@ioannisserver:~$ sudo apachectl configtest
AH00526: Syntax error on line 19 of /etc/apache2/conf-enabled/ssl-params.conf:
SSLPSLConfCnd: file '/etc/ssl/certs/dhparam.pem' does not exist or is empty
Action 'configtest' failed.
The Apache error log may have more information.
loannis@ioannisserver:~$ sudo nano /etc/apache2/conf-enabled/ssl-params.conf
loannis@ioannisserver:~$ sudo apachectl configtest
Syntax OK
loannis@ioannisserver:~$ sudo systemctl restart apache2
loannis@ioannisserver:~$
```

1. Ενεργοποιούμε το αρχείο default-ssl για να λειτουργήσει το ssl certificate.
2. Ενεργοποιούμε το αρχείο ssl-params που περιέχει τις παραμέτρους του πιστοποιητικού.
3. Ελέγχουμε αν το apachectl που επικοινωνεί με τα αρχεία του πιστοποιητικού έχει κάποιο συντακτικό λάθος.
4. Επανεκκινούμε το apache2 για να λάβουν μέρος οι αλλαγές που επιφέραμε και να ενεργοποιηθεί το πιστοποιητικό ssl.



Εάν πληκτρολογήσουμε στο browser το url <https://ioannisserver.com> θα μας εμφανίσει ότι το πιστοποιητικό δεν αναγνωρίζεται από τον περιηγητή επειδή είναι self signed. Δεν είναι κάτι λάθος απλώς μας προειδοποιεί για πιθανό κίνδυνο στην ιστοσελίδα μας.



Εάν πατήσουμε Advanced και Accept the Risk and Continue θα μας οδηγήσει στην σελίδα που φτάξαμε.

Επομένων τελειώσαμε με το web service του σέρβερ μας.



### **B3. [DNS CACHING NAMESERVER]**

```
Activities Terminal Map 2 16:53
loannis@loannisserver:~ [sudo] password for loannis:
loannis@loannisserver:~ % sudo apt update
Hit:1 http://gr.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://ppa.launchpad.net/certbot/certbot/ubuntu focal InRelease
Hit:3 http://ppa.launchpad.net/certbot/certbot/ubuntu focal-updates InRelease
Hit:4 http://gr.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease
Err:6 http://ppa.launchpad.net/certbot/certbot/ubuntu focal Release
  404 Not Found [IP: 91.189.95.80]
Reading package lists... Done
E: The repository 'http://ppa.launchpad.net/certbot/certbot/ubuntu focal' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
loannis@loannisserver:~ % sudo apt install bind9 bind9utils bind9-doc bind9-host
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  bind9-dnsutils bind9-lbs bind9-utils python3-ply
Suggested packages:
  bind-doc resolvconf python3-ply-doc
The following NEW packages will be installed:
  bind9 bind9-doc bind9-utils bind9utils python3-ply
The following packages will be upgraded:
  bind9-dnsutils bind9-lbs
3 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
Need to get 2001 kB of archives.
After this operation, 3828 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://gr.archive.ubuntu.com/ubuntu focal-updates/main amd64 bind9-host amd64 1:9.16.1-0ubuntu2.7 [4 3.0 kB]
Get:2 http://gr.archive.ubuntu.com/ubuntu focal-updates/main amd64 bind9-dnsutils amd64 1:9.16.1-0ubuntu2.7 [134 kB]
Get:3 http://gr.archive.ubuntu.com/ubuntu focal-updates/main amd64 bind9-lbs amd64 1:9.16.1-0ubuntu2.7 [114 kB]
Get:4 http://gr.archive.ubuntu.com/ubuntu focal/main amd64 python3-ply all 3.11.3-3build1 [46,4 kB]
Get:5 http://gr.archive.ubuntu.com/ubuntu focal-updates/main amd64 bind9-utils amd64 1:9.16.1-0ubuntu2.7 [
```

- Με την πρώτη εντολή κάνουμε μία γενική ενημέρωση το σύστημά μας.

- Με την δεύτερη εντολή εγκαθιστούμε το bind9 πακέτο και όλα εκείνα που θα μας βοηθήσουν για να δημιουργήσουμε έναν DNS server.

```
Activities Terminal Map 2 16:54
loannis@loannisserver: ~
Processing triggers for systemd (245.4-4ubuntu3.4) ...
Processing triggers for Mail-db (2.9.1+1) ...
Processing triggers for libatk-bridge-2.0-0ubuntu9.2 (2.31-0ubuntu9.2) ...
libatk-bridge-2.0-0ubuntu9.2: /usr/lib/x86_64-linux-gnu/libatk-bridge-2.0.so.0
7 BIND 9.16.1-ubuntu (Stable) <id:497c32>
loannis@loannisserver: ~ systemctl status named
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-03-02 16:52:47 EET; 1min 9s ago
     Docs: man:named(8)
 Main PID: 20534 (named)
   Tasks: 5 (limit: 4654)
  Memory: 12.1M
    CGroup: /system.slice/named.service
           └─20534 /usr/sbin/named -f -u bind

Mar 02 16:52:47 loannisserver named[20534]: network unreachable resolving '.DNSKEY/IN': 2001:500:2d::#d53
Mar 02 16:52:47 loannisserver named[20534]: network unreachable resolving '.NS/IN': 2001:500:2d::#d53
Mar 02 16:52:47 loannisserver named[20534]: network unreachable resolving '.DNSKEY/IN': 2001:7fd::#f53
Mar 02 16:52:47 loannisserver named[20534]: network unreachable resolving '.NS/IN': 2001:7fd::#f53
Mar 02 16:52:47 loannisserver named[20534]: network unreachable resolving '.DNSKEY/IN': 2001:503:b3ae::#2309
Mar 02 16:52:47 loannisserver named[20534]: network unreachable resolving '.NS/IN': 2001:503:b3ae::#2309
Mar 02 16:52:47 loannisserver named[20534]: network unreachable resolving '.DNSKEY/IN': 2001:500:9f::#42#53
Mar 02 16:52:47 loannisserver named[20534]: network unreachable resolving '.NS/IN': 2001:500:9f::#42#53
Mar 02 16:52:47 loannisserver named[20534]: managed-keys-zone: Initializing automatic trust anchor management
Mar 02 16:52:47 loannisserver named[20534]: resolver priming query complete
...skipping...
```

- Με την πρώτη εντολή βλέπουμε την έκδοση του bind9 που έχουμε εγκαταστήσει.

- Με την δεύτερη εντολή βλέπουμε την τρέχουσα κατάσταση της υπηρεσίας named.

```
Activities Terminal Map 2 16:57
loannis@loannisserver:~
```

loannis@loannisserver:~\$ sudo systemctl start named  
loannis@loannisserver:~\$ sudo systemctl enable named  
Synchronizing state of named.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable named  
loannis@loannisserver:~\$ sudo netstat -lnpnt | grep named  
tcp 0 0 127.0.0.1:1953 0.0.0.0:\* LISTEN 20534/named  
tcp 0 0 192.168.1.1:553 0.0.0.0:\* LISTEN 20534/named  
tcp 0 0 127.0.1:1:53 0.0.0.0:\* LISTEN 20534/named  
tcp6 0 0 ::1:953 ::\* LISTEN 20534/named  
tcp6 0 0 fe80::a00:27ff:fe73::53 ::\* LISTEN 20534/named  
tcp6 0 0 ::1:53 ::\* LISTEN 20534/named  
udp 0 0 192.168.1.155:53 0.0.0.0.\* 20534/named  
udp 0 0 127.0.1:53 0.0.0.0.\* 20534/named  
udp6 0 0 ::1:53 ::\* LISTEN 20534/named  
udp6 0 0 fe80::a00:27ff:fe73::53 ::\* LISTEN 20534/named  
loannis@loannisserver:~\$ sudo rndc status  
version: BIND 9.16.1-0ubuntu1 (stable release) <ld:d497c32>  
running on loannisserver: Linux x86\_64 5.8.0-44-generic #50~20.04.1-Ubuntu SMP Wed Feb 10 21:07:30 UTC 2021  
i  
boot time: Tue, 02 Mar 2021 14:52:47 GMT  
last configured: Tue, 02 Mar 2021 14:52:47 GMT  
configuration file: /etc/bind/named.conf  
CPUs found: 1  
worker threads: 1  
UDP listeners per interface: 1  
number of zones: 102 (97 automatic)  
debug level: 0  
xfers running: 0  
xfers deferred: 0  
soa queries in progress: 0  
query logging is OFF  
recursive clients: 0/900/1000  
tcp clients: 0/0  
TCP port: 53  
server is listening and running  
loannis@loannisserver:~\$ sudo nano /etc/bind/named.conf.options

- Με την πρώτη εντολή  
βλέπουμε την κατάσταση του  
σέρβερ μας.

- Με την δεύτερη εντολή θα τροποποιήσουμε το αρχείο που περιέχει όλες τις βασικές πληροφορίες για να επιτευχθεί ένας DNS server.



The screenshot shows two terminal windows. The top window displays the contents of the `/etc/bind/named.conf.options` file, specifically the `forwarders { 8.8.8.8; };` section, which is highlighted with a red box. The bottom window shows a series of terminal commands run by the user `ioannis` to install `dnsutils`, update the system, restart the `bind9` service, and configure the firewall (`ufw`) to allow port 53.

```

# /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/880113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        8.8.8.8;
    };

    //========================================================================
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.tsc.org/bind-keys
    //================================================================
    dnssec-validation auto;

};

listen-on-v6 { any; };

```

```

Reading database ... 170389 files and directories currently installed.
Preparing to unpack .../dnsutils_1x3a9.16.1~ubuntu2.7_all.deb ...
Unpacking dnsutils (1:9.16.1~ubuntu2.7) ...
Setting up dnsutils (1:9.16.1~ubuntu2.7) ...
[ioannis@ioannisserver: ~]$ sudo nano /etc/bind/named.conf.options
[ioannis@ioannisserver: ~]$ sudo systemctl restart bind9.service
[ioannis@ioannisserver: ~]$ hostname -i
ioannisserver.com
[ioannis@ioannisserver: ~]$ sudo nano /etc/bind/db.local
[ioannis@ioannisserver: ~]$ sudo cp /etc/bind/db.local /etc/bind/db.ioannisserver.com
[ioannis@ioannisserver: ~]$ sudo nano /etc/bind/db.ioannisserver.com
[ioannis@ioannisserver: ~]$ sudo systemctl restart bind9.service
[ioannis@ioannisserver: ~]$ sudo cp /etc/bind/db.127 /etc/bind/db.192
[ioannis@ioannisserver: ~]$ sudo systemctl restart bind9.service
[ioannis@ioannisserver: ~]$ sudo nano /etc/bind/db.192
[ioannis@ioannisserver: ~]$ sudo ufw allow 53/tcp
[ioannis@ioannisserver: ~]$ [sudo] password for ioannis:
[ioannis@ioannisserver: ~]$ Skipping adding existing rule (v6)
[ioannis@ioannisserver: ~]$ Skipping adding existing rule (v6)

```

- Διορθώνουμε τους forwarders που φαίνονται δίπλα και βάζουμε την δ/ση ενός σέρβερ της Google.

- Ρυθμίζουμε εκείνα που είναι μέσα σε κόκκινο περίγραμμα σε παρακάτω screenshot. Τροποποιούμε αρχικά την forward zone η οποία επιτρέπει στον διακομιστή DNS να επιτύχει ερωτήματα όπου ο πελάτης στέλνει ένα όνομα στον διακομιστή DNS για να ζητήσει τη διεύθυνση IP του ητούμενου κεντρικού υπολογιστή. Στην συνέχεια τροποποιούμε την reverse zone η οποία είναι μια έγκυρη ζώνη DNS που χρησιμοποιείται κυρίως για την επίλυση διευθύνσεων IP σε ονόματα πόρων δικτύου. Αυτός ο τύπος ζώνης μπορεί να είναι πρωτεύων, δευτερεύων ή Active Directory - integrated. Όπου βλέπουμε localhost, βάζουμε το hostname του συστήματός μας.
- Αντιγράφουμε τα περιεχόμενα του αρχείου db.local στο αρχείο που θα τα τροποποιήσουμε db.ioannisserver.com.
- Ρυθμίζουμε εκείνα που είναι μέσα σε κόκκινο περίγραμμα σε παρακάτω screenshot. Τροποποιούμε αρχικά το αρχείο forward zone.
- Αντιγράφουμε τα περιεχόμενα του αρχείου db.127 στο αρχείο που θα τα τροποποιήσουμε db.192.
- Ρυθμίζουμε εκείνα που είναι μέσα σε κόκκινο περίγραμμα σε παρακάτω screenshot. Τροποποιούμε το αρχείο reverse zone.
- Επανεκκινούμε την υπηρεσία bind9 για να ενεργοποιηθούν οι αλλαγές.
- Ενεργοποιούμε την πόρτα 53 στο firewall (dns service).

The screenshot shows a terminal window with the command `sudo nano /etc/bind/named.conf.local`. The configuration file contains sections for a primary server and a secondary server, both named `ioannisserver.com`. The primary server section includes a `zone "ioannisserver.com" { type master; file "/etc/bind/db.ioannisserver.com"; allow-transfer { 192.168.1.1; }; also-notify { 192.168.1.1; };};` block, which is highlighted with a red box. The secondary server section includes a `zone "1.168.192.in-addr.arpa" { type master; file "/etc/bind/db.192"; allow-transfer { 192.168.1.1; }; also-notify { 192.168.1.1; };};` block, also highlighted with a red box.

```

// 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 "ioannisserver.com" {
    type master;
    file "/etc/bind/db.ioannisserver.com";
    allow-transfer { 192.168.1.1; };
    also-notify { 192.168.1.1; };
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
    allow-transfer { 192.168.1.1; };
    also-notify { 192.168.1.1; };
};

```



## 321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

### Νούμερο 3 (από τα παραπάνω βήματα)

**APXEIO:** db.ioannissserver.com

```
Activities Terminal Map 5 10:20
ioannis@ioannissserver:~
```

```
GNU nano 4.8 /etc/bind/db.ioannissserver.com
; BIND data file for local loopback interface
$TTL 604800
@ IN SOA loannissserver.com. root.loannissserver.com. (
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
; IN NS ns.loannissserver.com. Δ/ση του DNS Server μας
@ IN A 192.168.1.155
@ IN AAAA ::1
ns IN A 192.168.1.155
```

### Νούμερο 5 (από τα παραπάνω βήματα)

**APXEIO:** db.192

```
Activities Terminal Map 5 10:20
ioannis@ioannissserver:~
```

```
GNU nano 4.8 /etc/bind/db.192
; BIND reverse data file for local loopback interface
$TTL 604800
@ IN SOA ns.loannissserver.com. root.loannissserver.com. (
        604800 ; Serial
        86400 ; Refresh
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
; IN NS ns.
@ IN PTR ns.loannissserver.com.
```

```
Activities Terminal Map 5 11:00
ioannis@ioannisserver:~
```

```
loannis@ioannisserver:~$ sudo systemctl restart NetworkManager
Global
LLMNR setting: no
MulticastDNS setting: no
DNSOverTLS setting: no
DNSSEC setting: no
DNSSEC supported: no
DNS Domain: loannissserver.com
DNSSEC NTA: 192.168.1.155
16.172.1n-addr.arpa
16.172.1n-addr.arpa
16.192.1n-addr.arpa
17.172.1n-addr.arpa
18.172.1n-addr.arpa
19.172.1n-addr.arpa
20.172.1n-addr.arpa
21.172.1n-addr.arpa
22.172.1n-addr.arpa
23.172.1n-addr.arpa
24.172.1n-addr.arpa
25.172.1n-addr.arpa
26.172.1n-addr.arpa
27.172.1n-addr.arpa
28.172.1n-addr.arpa
29.172.1n-addr.arpa
30.172.1n-addr.arpa
31.172.1n-addr.arpa
corp
d.f.tpd.arpa
home
internal
internet
lan
local
private
test

Link 2 (enp0s3)
Current Scopes: DNS
DefaultRoute setting: yes
LLMNR setting: yes
MulticastDNS setting: no
DNSOverTLS setting: no
DNSSEC setting: no
DNSSEC supported: no
Current DNS Server: 127.0.0.1
DNS Servers: 127.0.0.1
DNS Domain: ~
loannissserver.com

inet 1:1-47/47 (ENO)
[6]+ Stopped                  systemd-resolve --status
```

```
Activities Terminal Map 5 11:00
ioannis@ioannisserver:~
```

```
21.172.1n-addr.arpa
22.172.1n-addr.arpa
23.172.1n-addr.arpa
24.172.1n-addr.arpa
25.172.1n-addr.arpa
26.172.1n-addr.arpa
27.172.1n-addr.arpa
28.172.1n-addr.arpa
29.172.1n-addr.arpa
30.172.1n-addr.arpa
31.172.1n-addr.arpa
corp
d.f.tpd.arpa
home
internal
internet
lan
local
private
test

Link 2 (enp0s3)
Current Scopes: DNS
DefaultRoute setting: yes
LLMNR setting: yes
MulticastDNS setting: no
DNSOverTLS setting: no
DNSSEC setting: no
DNSSEC supported: no
Current DNS Server: 127.0.0.1
DNS Servers: 127.0.0.1
DNS Domain: ~
loannissserver.com

inet 1:1-47/47 (ENO)
[6]+ Stopped                  systemd-resolve --status
```

- Με την εντολή "systemctl status" βλέπουμε την κατάσταση της DNS υπηρεσίας που τρέχει στο σύστημά μας. Σύμφωνα με τα αποτελέσματα έχουμε ότι το DNS domain έχει οριστεί σωστά δείχνοντας το hostname του υπολογιστή μας και ο dns server είναι ο υπολογιστής μας.

- Με την εντολή "dig ubuntu.com" βλέπουμε αν λειτουργεί σωστά ο σέρβερ μας και επικοινωνεί με την διεύθυνση που του έχουμε πει να «μιλήσει». Όπως βλέπουμε, αναγράφεται NOERROR.

```
loannis@ioannisserver:~$ dtg ubuntu.com
; <>> DiG 9.16.1-Ubuntu <>> ubuntu.com
; global options: +cmd
; Got answer:
; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 37338
; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; COOKIE: 6624fa631a5f37d501000000604a4cdb8d9f4317d3f5e395 (good)
; QUESTION SECTION:
;ubuntu.com.           IN      A
;
; ANSWER SECTION:
ubuntu.com.       600    IN      A      91.189.91.44
ubuntu.com.       600    IN      A      91.189.88.181
ubuntu.com.       600    IN      A      91.189.88.180
ubuntu.com.       600    IN      A      91.189.91.45
;
; Query time: 252 msec
; SERVER: 127.0.0.1#53(127.0.0.1)
; WHEN: Μερ Μαρ 11 19:01:15 EET 2021
; MSG SIZE  rcvd: 171
```



## B3. [SECURE FTP SERVICE]

The image shows three terminal windows from a Linux desktop environment. The first window (Map 4) shows the configuration of the SSHD service with commands like `sudo nano /etc/ssh/sshd\_config` and `sudo systemctl restart ssh`. The second window (Map 4) shows the creation of an SFTP user with `sudo useradd -n sftpuser -g sftp` and `sudo passwd sftpuser`. The third window (Map 5) shows the configuration of the SFTP subsystem in the SSHD config file and the testing of the service via SFTP.

```
Map 4 19:59
ioannis@ioannissERVER:~$ sudo nano /etc/ssh/sshd_config
ioannis@ioannissERVER:~$ sudo systemctl restart ssh
ioannis@ioannissERVER:~$ sudo addgroup sftp
Adding group 'sftp' (GID 1002) ...
Done.
ioannis@ioannissERVER:~$ sudo useradd -n sftpuser -g sftp
New password:
Retype new password:
passwd: password updated successfully

Map 4 19:21
ioannis@ioannissERVER:~$ /etc/ssh/sshd_config
Modified

#PrintLastLog yes
#TCPKeepAlive yes
#ServerAliveInterval no
#Compression delayed
#ClientAliveInterval 8
#ClientAliveCountMax 3
#useDNS no
#pidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anonyms
#   X11Forwarding no
#   AllowTcpForwarding no
#   PermitTTY no
#   ForceCommand cvs server

Match group sftp
    ChrootDirectory /home
    X11Forwarding no
    AllowTcpForwarding no
    ForceCommand internal-sftp

Map 5 10:48
ioannis@ioannissERVER:~$ sudo chmod 700 /home/sftpuser/
[sudo] password for ioannis:
ioannis@ioannissERVER:~$ sftp sftp@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:qs1dnVYSPzoUuUjeku4rd0knHADHsi1vg6a5RJU0pxXKY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
sftp@127.0.0.1's password:
Permission denied, please try again.
sftp@127.0.0.1's password:
Permission denied, please try again.
sftp@127.0.0.1's password:
sftp@127.0.0.1: Permission denied (publickey,password).
Connection closed.
ioannis@ioannissERVER:~$ sudo sftp sftp@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:qs1dnVYSPzoUuUjeku4rd0knHADHsi1vg6a5RJU0pxXKY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
sftp@127.0.0.1's password:
Permission denied, please try again.
sftp@127.0.0.1's password:
[3]+  Stopped                  sudo sftp sftp@127.0.0.1
ioannis@ioannissERVER:~$ sudo sftp sftpuser@127.0.0.1
sftpuser@127.0.0.1's password:
Connected to 127.0.0.1.
sftp> cd sftpuser
sftp> mkdir sftpuser/admin/
sftp> ls
icsd18107 ioannis      sftpuser
sftp> ls admin
Can't ls: './admin' not found
sftp> exit
ioannis@ioannissERVER:~$ sudo sftp sftpuser@127.0.0.1
sftpuser@127.0.0.1's password:
Connected to 127.0.0.1.
sftp> cd sftpuser
sftp> mkdir sftp-test
sftp> ls sftp-test
sftp> 
```

- Με την πρώτη εντολή θα τροποποιήσουμε το αρχείο που περιέχει όλες τις πληροφορίες για την δημιουργία του sftp service. Στο επόμενο στιγμιότυπο φαίνονται αναλυτικά οι τροποποιήσεις μας.

- Με την δεύτερη εντολή επανεκκινούμε το ssh πάνω στο οποίο τρέχει το sftp service.

- Με την τρίτη εντολή προσθέτουμε μία sftp ομάδα.

- Με την τέταρτη εντολή προσθέτουμε έναν sftp χρήστη στην παραπάνω ομάδα που δημιουργήσαμε.

- Με την πέμπτη εντολή βάζουμε κωδικό πρόσβασης για τον χρήστη που δημιουργήσαμε παραπάνω.

Στο διπλανό στιγμιότυπο αυτά που συμπληρώσαμε επιτρέπουν στους χρήστες της ομάδας sftp να έχουν πρόσβαση στους οικιακούς τους καταλόγους μέσω SFTP, αλλά τους αρνείται την κανονική πρόσβαση SSH, οπότε δεν μπορούν ποτέ να έχουν πρόσβαση σε ένα κέλυφος.

- Με την πρώτη εντολή, δίνουμε στον χρήστη που δημιουργήσαμε παραπάνω, όλα τα δικαιώματα για τον δικό του φάκελο.

- Με την δεύτερη εντολή βλέπουμε αν λειτουργεί σωστά το sftp.



## B4.

```
Activities Terminal Map 5 11:00 ioannis@ioannisserver:~  
loannis@ioannisserver:~$ sudo apt install stubby  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
libev4 libevent-2.1-7 libevent-core-2.1-7 libgetdns10 libunbound8  
The following NEW packages will be installed:  
libev4 libevent-2.1-7 libevent-core-2.1-7 libgetdns10 libunbound8 stubby  
0 new packages to install, 0 to remove and 3 not upgraded.  
Need to get 827 kB of archives.  
After this operation, 2479 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://gr.archive.ubuntu.com/ubuntu focal/main amd64 libevent-2.1-7 amd64 2.1.11-stable-1 [138 kB]  
Get:2 http://gr.archive.ubuntu.com/ubuntu focal/main amd64 libgetdns10 amd64 1.9.4-2ubuntui.1 [349 kB]  
Get:3 http://gr.archive.ubuntu.com/ubuntu focal/universe amd64 libev4 amd64 1:4.31.1 [31,2 kB]  
Get:4 http://gr.archive.ubuntu.com/ubuntu focal-updates/main amd64 libunbound8 amd64 1.9.4-2ubuntui.1 [349 kB]  
Get:5 http://gr.archive.ubuntu.com/ubuntu focal/universe amd64 libgetdns10 amd64 1.9.4-1ubuntui.1 [349 kB]  
Get:6 http://gr.archive.ubuntu.com/ubuntu focal/universe amd64 stubby amd64 1.5.1-1build1 [31,1 kB]  
Fetched 827 kB in 1s (2479 kB/s)  
Selecting previously unselected package libevent-2.1-7:amd64.  
(Reading database ... 17099 files and directories currently installed.)  
Preparing to unpack .../0-libevent-2.1-7_2.1.11-stable-1_amd64.deb ...  
Unpacking libevent-2.1-7:amd64 (2.1.11-stable-1)  
Selecting previously unselected package libevent-core-2.1-7:amd64.  
Preparing to unpack .../1-libevent-core-2.1-7_2.1.11-stable-1_amd64.deb ...  
Unpacking libevent-core-2.1-7:amd64 (2.1.11-stable-1)  
Selecting previously unselected package libev4:amd64.  
Preparing to unpack .../2-libev4_1x34.31.1_amd64.deb ...  
Unpacking libev4:amd64 (1:4.31.1)  
Selecting previously unselected package libunbound8:amd64.  
Preparing to unpack .../3-libunbound8_1.9.4-2ubuntui.1_amd64.deb ...  
Unpacking libunbound8:amd64 (1.9.4-2ubuntui.1)  
Selecting previously unselected package libgetdns10:amd64.  
Preparing to unpack .../4-libgetdns10_1.9.4-1ubuntui.1_amd64.deb ...  
Unpacking libgetdns10:amd64 (1.9.4-1ubuntui.1)  
Selecting previously unselected package stubby.  
[...]  
Activities Terminal Map 5 11:00 ioannis@ioannisserver:~  
loannis@ioannisserver:~$ systemctl status stubby  
Unknown operation status.  
loannis@ioannisserver:~$ systemctl status stubby  
Unknown operation status.  
loannis@ioannisserver:~$ systemctl status stubby  
● stubby.service - DNS Privacy Stub Resolver  
   Loaded: loaded (/lib/systemd/system/stubby.service; enabled; vendor preset: enabled)  
   Active: active (running) since Fri 2021-03-05 10:49:51 EET; 46s ago  
     Docs: https://dnspriVacy.org/wikt/DNS+Privacy+Daemon++Stubby  
   Main PID: 3177 (stubby)  
     Tasks: 1 (limit: 464)  
    Memory: 1.5M  
      CGroup: /system.slice/stubby.service  
             └─3177 /usr/bin/stubby  
  
Map 05 10:49:51 ioannisserver systemd[1]: Started DNS Privacy Stub Resolver.  
Map 05 10:49:51 ioannisserver stubby[3177]: [08:10:49:51.797211] STUBBY: Read config from file /etc/stubby/stubby.conf  
Map 05 10:49:51 ioannisserver stubby[3177]: [08:10:49:51.802278] STUBBY: DNSSEC Validation is OFF  
Map 05 10:49:51 ioannisserver stubby[3177]: [08:10:49:51.802425] STUBBY: Transport list is:  
Map 05 10:49:51 ioannisserver stubby[3177]: [08:10:49:51.802480] STUBBY: TLS  
Map 05 10:49:51 ioannisserver stubby[3177]: [08:10:49:51.802525] STUBBY: Privacy Usage Profile is Strict (Autodetected)  
Map 05 10:49:51 ioannisserver stubby[3177]: [08:10:49:51.802571] STUBBY: (NOTE a Strict Profile only applies to recursive queries)  
Map 05 10:49:51 ioannisserver stubby[3177]: [08:10:49:51.802631] STUBBY: Starting DAEMON...  
[4]+ Stopped systemctl status stubby  
loannis@ioannisserver:~$  
loannis@ioannisserver:~$ sudo netstat -lnpnt | grep stubby  
udp        0      0 127.0.0.1:53          0.0.0.0:*                           3177/stubby  
loannis@ioannisserver:~$ sudo netstat -lnpnt | grep systemd-resolv  
tcp        0      0 127.0.0.53:53       0.0.0.0.*                           LISTEN    424/systemd-resolve  
tcp        0      0 127.0.0.53:53       0.0.0.0.*                           LISTEN    424/systemd-resolve  
loannis@ioannisserver:~$ sudo nano /etc/stubby/stubby.yml  
loannis@ioannisserver:~$ cd /etc/NetworkManager/system-connections/  
bash: cd: /etc/NetworkManager/system-connections/: No such file or directory  
loannis@ioannisserver:~$ ls  
01-network-manager-all.yaml.bak  Documents  listening-services  Pictures  Templates  
Activities Terminal Map 5 11:20 ioannis@ioannisserver:~  
GNU nano 4.8 /etc/bind/named.conf.options  
options {  
    directory "/var/cache/bind";  
  
    // If there is a firewall between you and nameservers you want  
    // to talk to, you may need to fix the firewall to allow multiple  
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113  
  
    // If your ISP provided one or more IP addresses for stable  
    // nameservers, you probably want to use them as forwarders.  
    // Uncomment the following block, and insert the addresses replacing  
    // the all-0's placeholder.  
  
    forwarders {  
        8.8.8.8;  
        8.8.4.4;  
    };  
  
    //=====================================================================  
    // If BIND logs error messages about the root key being expired,  
    // you will need to update your keys. See https://www.isc.org/bnd-keys  
    //=====================================================================  
    dnssec-enable yes;  
    dnssec-validation auto;  
};  
listen-on-v6 { any; };  
};  
[...]  
Activities Terminal Map 5 11:20 ioannis@ioannisserver:~  
loannis@ioannisserver:~$  
[Read 28 lines]
```

Εγκαθιστούμε το πακέτο stubby το οποίο ενεργεί ως τοπικό πρόγραμμα επίλυσης απορρήτου DNS, χρησιμοποιώντας DNS-over-TLS. Το Stubby κρυπτογραφεί ερωτήματα DNS που αποστέλλονται από τον τοπικό υπολογιστή σε πρόγραμμα DNS privacy resolver, αυξάνοντας το privacy των τελικών χρηστών.

- Με την πρώτη εντολή ελέγχουμε την τρέχουσα κατάσταση του stubby (ενεργοποιημένο).

- Με την δεύτερη εντολή βλέπουμε ότι το stubby ακούει στην πόρτα 53.

- Με την δεύτερη εντολή βλέπουμε ότι το default stub resolver παρέχεται από το system-resolved και ακούει στην πόρτα 53 του 127.0.0.53.

Τροποποιούμε το αρχείο named.conf.options με την εντολή "sudo nano /etc/bind/named.conf.options" για να ενεργοποιήσουμε το DNSSEC. Οι επεκτάσεις ασφάλειας συστήματος ονόματος τομέα (DNSSEC) επιτρέπουν την επικύρωση των αποκρίσεων DNS με έλεγχο ταυτότητας της επικοινωνίας μεταξύ διακομιστών DNS. Αυτό σημαίνει ότι οι χρήστες μπορούν να εμπιστεύονται ότι οι αποκρίσεις DNS που λαμβάνουν ταιριάζουν με το περιεχόμενο του αρχείου έγκυρης ζώνης.



## B5.

```
loannis@loannissserver:~$ sysctl -a
abi.vsyscall32 = 1
debug.exception-trace = 1
debug.kprobes-optimize = 1
dev.cdrom.autoclose = 1
dev.cdrom.autoeject = 0
dev.cdrom.check_media = 0
dev.cdrom.debug = 0
dev.cdrom.info = CD-ROM Information, Id: cdrom.c 3.20 2003/12/17
dev.cdrom.info = drive name: sr0
dev.cdrom.info = drive speed: 32
dev.cdrom.info = drive # of slots: 1
dev.cdrom.info = Can close tray: 1
dev.cdrom.info = Can open tray: 1
dev.cdrom.info = Can lock tray: 1
dev.cdrom.info = Can change speed: 1
dev.cdrom.info = Can select disk: 0
dev.cdrom.info = Can read multisession: 1
dev.cdrom.info = Can read MCN: 1
dev.cdrom.info = Reports media changed: 1
dev.cdrom.info = Can play audio: 1
dev.cdrom.info = Can write CD-R: 0
dev.cdrom.info = Can write CD-RW: 0
dev.cdrom.info = Can read DVD: 1
dev.cdrom.info = Can write DVD-R: 0
dev.cdrom.info = Can write DVD-RAM: 0
dev.cdrom.info = Can read MRW: 1
dev.cdrom.info = Can write MRW: 1
dev.cdrom.info = Can write RAM: 1
dev.cdrom.info =
dev.cdrom.info =
dev.cdrom.info =
dev.cdrom.info =
dev.cdrom.lock = 0
dev.hpet.max-user-freq = 64
dev.mac_hid.mouse_button2.keyCode = 97
dev.mac_hid.mouse_button3.keyCode = 100
dev.mac_hid.mouse_button_emulation = 0
dev.parport.default.spintime = 500
Activities Terminal Map 17 11:19 loannis@loannissserver:~
```

```
loannis@loannissserver:~$ sysctl -A
abi.vsyscall32 = 1
debug.exception-trace = 1
debug.kprobes-optimize = 1
dev.cdrom.autoclose = 1
dev.cdrom.autoeject = 0
dev.cdrom.check_media = 0
dev.cdrom.debug = 0
dev.cdrom.info = CD-ROM Information, Id: cdrom.c 3.20 2003/12/17
dev.cdrom.info = drive name: sr0
dev.cdrom.info = drive speed: 32
dev.cdrom.info = drive # of slots: 1
dev.cdrom.info = Can close tray: 1
dev.cdrom.info = Can open tray: 1
dev.cdrom.info = Can lock tray: 1
dev.cdrom.info = Can change speed: 1
dev.cdrom.info = Can select disk: 0
dev.cdrom.info = Can read multisession: 1
dev.cdrom.info = Can read MCN: 1
dev.cdrom.info = Reports media changed: 1
dev.cdrom.info = Can play audio: 1
dev.cdrom.info = Can write CD-R: 0
dev.cdrom.info = Can write CD-RW: 0
dev.cdrom.info = Can read DVD: 1
dev.cdrom.info = Can write DVD-R: 0
dev.cdrom.info = Can write DVD-RAM: 0
dev.cdrom.info = Can read MRW: 1
dev.cdrom.info = Can write MRW: 1
dev.cdrom.info = Can write RAM: 1
dev.cdrom.info =
dev.cdrom.info =
dev.cdrom.info =
dev.cdrom.info =
dev.cdrom.lock = 0
dev.hpet.max-user-freq = 64
dev.mac_hid.mouse_button2.keyCode = 97
dev.mac_hid.mouse_button3.keyCode = 100
dev.mac_hid.mouse_button_emulation = 0
dev.parport.default.spintime = 500
Activities Terminal Map 17 11:20 loannis@loannissserver:~
```

```
vn.max_map_count = 65530
vn.memory_failure_early_kill = 0
vn.memory_failure_recovery = 1
vn.mln_free_kbbytes = 67584
vn.mln_free_kbtray = 0
vn.mln_mapped_ratio = 1
vn.mmap.mln_addr = 65536
sysctl: permission denied on key 'vm.mmap_rnd_bits'
sysctl: permission denied on key 'vm.mmap_rnd_compat_bits'
vn.nr_hugepages = 0
vn.nr_hugepages_nepolicy = 0
vn.nr_overcommit_hugepages = 0
vn.nr_overcommit_ratio = 1
vn.numa_zonelist_order = Node
vn.oom_dump_tasks = 1
vn.oom_kill Allocating_task = 0
vn.overcommit_kbbytes = 0
vn.overcommit_memory = 0
vn.overcommit_ratio = 50
vn.page_cluster = 3
vn.page_size_kb = 0
vn.percpu_pagelist_fraction = 0
vn.stat_interval = 1
sysctl: permission denied on key 'vm.stat_refresh'
vn.swappiness = 60
vn.unprivileged_userfaultfd = 1
vn.user_reserve_kbbytes = 122979
vn.vfs_max_zone_ratio = 100
vn.watermark_boost_factor = 0
vn.watermark_scale_factor = 10
vn.zone_reclaim_mode = 0
loannis@loannissserver:~$ sysctl m1b
sysctl: cannot stat /proc/sys/m1b: No such file or directory
loannis@loannissserver:~$ sysctl net.ipv4.conf.all.rp_filter
net.ipv4.conf.all.rp_filter = 2
loannis@loannissserver:~$ sysctl -a --pattern 'net.ipv4.conf.(eth|wlan)0.arp'
loannis@loannissserver:~$ sysctl -p
loannis@loannissserver:~$
```

Με αυτή την εντολή βλέπουμε τις τρέχουσες τιμές στις παραμέτρους.

Με αυτή την εντολή βλέπουμε τις τρέχουσες τιμές στις παραμέτρους.

Με την τελευταία εντολή φορτώνουμε τις ρυθμίσεις. Με όλες τις από πάνω εντολές βλέπουμε τις τρέχουσες τιμές στις παραμέτρους.



## 321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

```

Activities Terminal Map 17 11:25
loannis@ioannisserv:~$ sudo nano /etc/sysctl.conf
[sudo] password for loannis:
loannis@ioannisserv:~$ sudo nano /etc/sysctl.d/99-custom.conf
loannis@ioannisserv:~$ sudo nano /etc/sysctl.d/99-custom.conf
loannis@ioannisserv:~$
```

- Με την πρώτη εντολή θα δούμε τα περιεχόμενα αυτού του αρχείου. Δεν θα τροποποιήσουμε τίποτα στο αρχείο αυτό.

- Με την δεύτερη εντολή θα τροποποιήσουμε το εξής αρχείο κάνοντας:

- Διαμόρφωση του περιορισμού για το IPv4

- Διαμόρφωση του περιορισμού για το IPv6

- Ενεργοποίηση της προστασίας execshield

- Αποτροπή κατά της κοινής «syn flood attack»

- Ενεργοποίηση της επαλήθευσης διεύθυνσης IP πηγής

- Αποτροπή του cracker να χρησιμοποιήσει μια πλαστογράφηση επίθεσης στη διεύθυνση IP του διακομιστή.

- Καταγραφή διάφορων τύπων ύποπτων πακέτων, όπως πακέτα πλαστογράφησης, πακέτα δρομολόγησης πηγής και ανακατευθύνσεις.

Περεταίρω ανάλυση για το τι κάνει η συγκεκριμένη εντολή, ωπόρχει ως σχόλιο για κάθε εντολή στα παρακάτω στιγμότυπα.

```

Activities Terminal Map 17 11:24
loannis@ioannisserv:~$ GNU nano 4.8
# The following is suitable for dedicated web server, Mail, TCP server etc.
# # Boolean Values:
# $1 == 1 (true) ==> enabled / yes / true
# $1 == 0 (zero) ==> disabled / no / false
# $1 == -1 (minus one) ==> disabled / yes / true
# Controls IP packet forwarding
net.ipv4.ip_forward = 0

# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0

# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 0

# Controls whether core dumps will append the PID to the core filename
# Useful for debugging multi-threaded applications
kernel.core_uses_pid = 1

# Controls the use of TCP syncokes
# Syncokes help prevent TCP connections
net.ipv4.tcp_syncokes = 1
net.ipv4.tcp_synack_retries = 5

#####
# IPv4 networking start #####
# Send redirects, if router, but this is just server
# So no routing allowed
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0

# Accept packets with SWI options NO
net.ipv4.conf.all.accept_source_route = 0

# Accept Redirects? No, this is not router
net.ipv4.conf.all.arp_accept_redirects = 0

#####
# Get Help   Write Out  Where Is  Cut Text  Justify  Cur Pos  Undo
# Read File  Replace   Paste Text To Spell  Go To Line  Redo
# Exit      Read File Replace  Paste Text To Spell  Go To Line  Undo
# Write Out  Where Is  Cut Text  Justify  Cur Pos  Undo
# Replace   Paste Text To Spell  Go To Line  Redo
# Cut Text  Justify  Cur Pos  Undo
# To Spell  Go To Line  Redo
# Cur Pos  Undo
# Go To Line  Redo
# Undo
```

```

Activities Terminal Map 17 11:25
loannis@ioannisserv:~$ GNU nano 4.8
# Accept Redirects? No, this is not router
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0

# Log packets with impossible addresses to kernel log? yes
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0

# Ignore all ICMP ECHO and TIMESTAMP requests sent to it via broadcast/multicast
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Prevent against the common 'syn flood attack'
net.ipv4.tcp_syncookies = 1

# Enable source validation by reversed path, as specified in RFC1812
net.ipv4.conf.all.rp_filter = 1

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1

#####
# IPv6 networking start #####
# Number of Router Solicitations to send until assuming no routers are present.
# This is host and not router
net.ipv6.conf.default.router_solicitations = 0

# Accept Router Preference In RAR
net.ipv6.conf.default.accept_ra_rtr_pref = 0

# Learn Prefix Information In Router Advertisement
net.ipv6.conf.default.accept_ra_pinfo = 0

#####
# Get Help   Write Out  Where Is  Cut Text  Justify  Cur Pos  Undo
# Read File  Replace   Paste Text To Spell  Go To Line  Redo
# Exit      Read File Replace  Paste Text To Spell  Go To Line  Undo
# Write Out  Where Is  Cut Text  Justify  Cur Pos  Undo
# Replace   Paste Text To Spell  Go To Line  Redo
# Cut Text  Justify  Cur Pos  Undo
# To Spell  Go To Line  Redo
# Cur Pos  Undo
# Go To Line  Redo
# Undo
```

```

Activities Terminal Map 17 11:25
loannis@ioannisserv:~$ GNU nano 4.8
# Setting controls whether the system will accept Hop Limit settings from a router advertisement
net.ipv6.conf.default.accept_ra_defrtr = 0

# Router advertisements can cause the system to assign a global unicast address to an interface
net.ipv6.conf.default.autoconf = 0

# How many neighbor solicitations to send out per address?
net.ipv6.conf.default.dad_transmits = 0

# How many global unicast IPv6 addresses can be assigned to each interface?
net.ipv6.conf.default.max_addresses = 1

#####
# IPv6 networking ends #####
# Enable ExecShield protection
# Set value to 1 or 2 (recommended)
# kernel.exec-shield = 2
# kernel.randomize_va_space=2

# TCP and memory optimization
# Increase TCP max buffer size setable using setsockopt()
net.ipv4.tcp_rmem = 4096 67380 8388608
net.ipv4/tcp_wmem = 4096 67380 8388608

# Increase Linux auto tuning TCP buffer limits
# net.ipv4.tcp_rmem = 4096 67380 8388608
# net.ipv4/tcp_wmem = 4096 67380 8388608
# net.core.wmem_max = 8388608
# net.core.netdev_max_backlog = 5000
# net.ipv4.tcp_window_scaling = 1

# Increase system file descriptor limit
fs.file-max = 65535

# Allow for more PIDs
allow_other = 1

#####
# Get Help   Write Out  Where Is  Cut Text  Justify  Cur Pos  Undo
# Read File  Replace   Paste Text To Spell  Go To Line  Redo
# Exit      Read File Replace  Paste Text To Spell  Go To Line  Undo
# Write Out  Where Is  Cut Text  Justify  Cur Pos  Undo
# Replace   Paste Text To Spell  Go To Line  Redo
# Cut Text  Justify  Cur Pos  Undo
# To Spell  Go To Line  Redo
# Cur Pos  Undo
# Go To Line  Redo
# Undo
```

```

Activities Terminal Map 17 11:25
loannis@ioannisserv:~$ GNU nano 4.8
# How many global unicast IPv6 addresses can be assigned to each interface?
net.ipv6.conf.default.max_addresses = 1

#####
# IPv6 networking ends #####
# Enable ExecShield protection
# Set value to 1 or 2 (recommended)
# kernel.exec-shield = 2
# kernel.randomize_va_space=2

# TCP and memory optimization
# Increase TCP max buffer size setable using setsockopt()
net.ipv4.tcp_rmem = 4096 67380 8388608
net.ipv4/tcp_wmem = 4096 67380 8388608

# Increase Linux auto tuning TCP buffer limits
# net.ipv4.tcp_rmem = 4096 67380 8388608
# net.ipv4/tcp_wmem = 4096 67380 8388608
# net.core.wmem_max = 8388608
# net.core.netdev_max_backlog = 5000
# net.ipv4.tcp_window_scaling = 1

# Increase system file descriptor limit
fs.file-max = 65535

# Allow for more PIDs
allow_other = 1

#####
# Get Help   Write Out  Where Is  Cut Text  Justify  Cur Pos  Undo
# Read File  Replace   Paste Text To Spell  Go To Line  Redo
# Exit      Read File Replace  Paste Text To Spell  Go To Line  Undo
# Write Out  Where Is  Cut Text  Justify  Cur Pos  Undo
# Replace   Paste Text To Spell  Go To Line  Redo
# Cut Text  Justify  Cur Pos  Undo
# To Spell  Go To Line  Redo
# Cur Pos  Undo
# Go To Line  Redo
# Undo
```



## B6.

The terminal window displays three distinct sessions:

- Session 1:** Shows the user updating the system and creating a new repository. The user runs `sudo apt-get update && sudo apt-get upgrade`. The output shows numerous package downloads from `http://archive.ubuntu.com/ubuntu` and `http://archive.ubuntu.com/ubuntu focal`, including `focal-updates` and `focal-security` packages. It also shows the creation of a new repository at `http://ppa.launchpad.net/certbot/certbot/ubuntu focal`.
- Session 2:** Shows the user running `manpage` on the `usermod` command. The output provides detailed information about various options for modifying user accounts, such as `-b` for base directory, `-c` for comment, `-d` for home directory, and `-e` for expiration date.
- Session 3:** Shows the user creating a directory `/home/aploixrhstes` and adding a user `aploixrhstes` with a specific SELinux context. The user runs `sudo useradd -m -d /home/aploixrhstes foititis1` and `sudo usermod -n foititis2`. The user then lists the contents of `/home/aploixrhstes` and changes to the `foititis2` directory.

Τροποποιούμε το αρχείο `named.conf.options` με την εντολή `sudo nano /etc/bind/named.conf.options` για να ενεργοποιήσουμε το DNSSEC. Οι επεκτάσεις ασφάλειας συστήματος ονόματος τομέα (DNSSEC) επιτρέπουν την επικύρωση των αποκρίσεων DNS με έλεγχο ταυτότητας της επικοινωνίας μεταξύ διακομιστών DNS. Αυτό σημαίνει ότι οι χρήστες μπορούν να εμπιστεύονται ότι οι αποκρίσεις DNS που λαμβάνουν ταιριάζουν με το περιεχόμενο του αρχείου έγκυρης ζώνης.

Κάνουμε τον `sftpuser` που είχαμε δημιουργήσει παραπάνω ως διαχειριστή του web service (τον έχουμε κάνει ήδη διαχειριστή του `sftp` service).

- Με την πρώτη εντολή φτιάχνουμε έναν φάκελο ο οποίος θα περιέχει όλους τους απλούς χρήστες.

- Με την δεύτερη εντολή βλέπουμε τους φάκελους που υπάρχουν στο μονοπάτι `/home`.

- Με την τρίτη εντολή δημιουργούμε έναν χρήστη με όνομα `foititis1` και την τέταρτη εντολή δημιουργούμε έναν χρήστη με όνομα `foititis2`.

- Με την πέμπτη εντολή βλέπουμε τους φάκελους που υπάρχουν στο μονοπάτι `/home/aploixrhstes`.

- Με την έκτη εντολή δημιουργούμε έναν χρήστη με όνομα `kathigitis`.



## 321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

```
ioannis@ioannisserver:~$ tree /home
/home
├── aploixrhstes
│   ├── foititis1
│   ├── foititis2
│   └── kathigitis
└── icsd18107
    ├── 01-network-manager-all.yaml.bak
    ├── Desktop
    ├── Documents
    ├── Downloads
    └── Nessus-8.13.1-ubuntu110_amd64.deb
        └── listening.services
            └── Music
                └── Pictures
                    ├── Screenshot from 2021-02-26 20-04-56.png
                    ├── Screenshot from 2021-03-02 11-08-39.png
                    ├── Screenshot from 2021-03-03 13-28-21.png
                    ├── Screenshot from 2021-03-03 14-15-28.png
                    ├── Screenshot from 2021-03-03 14-17-23.png
                    ├── Screenshot from 2021-03-04 10-29-02.png
                    ├── Screenshot from 2021-03-04 12-44-51.png
                    ├── Screenshot from 2021-03-04 15-06-28.png
                    ├── Screenshot from 2021-03-04 19-14-37.png
                    └── Screenshot from 2021-03-05 13-07-13.png
            └── Public
            └── Templates
            └── Videos
        └── sftpuser [error opening dir]
    15 directories, 13 files
ioannis@ioannisserver:~$
```

Με αυτή την εντολή βλέπουμε την δομή του μονοπατιού /home

```
ioannis@ioannisserver:~$ ls -al
total 128
drwxr-xr-x 16 ioannis ioannis 4096 Map 3 14:58 .
drwxr-xr-x  6 icsd18107 icsd18107 4096 Map 8 09:27 ..
drwxr--r--  1 root   root   104 Map 2 16:28 01-network-manager-all.yaml.bak
drwxr--r--  1 ioannis ioannis 32739 Map 7 12:49 .bash_history
drwxr--r--  1 ioannis ioannis 220 Φεβ 26 20:00 .bash_logout
drwxr--r--  1 ioannis ioannis 3771 Φεβ 26 20:00 .bashrc
drwxr-xr-x  15 ioannis ioannis 4096 Map 5 20:45 .cache
drwxr-xr-x  15 ioannis ioannis 4096 Map 5 11:04 .config
drwxr-xr-x  2 ioannis ioannis 4096 Φεβ 26 20:04 Desktop
drwxr-xr-x  2 ioannis ioannis 4096 Φεβ 26 20:04 Documents
drwxr-xr-x  2 ioannis ioannis 4096 Map 5 14:02 Downloads
drwxr--r--  3 ioannis ioannis 4096 Map 2 13:17 .gnupg
drwxr--r--  1 ioannis ioannis 660 Map 2 12:00 listening.services
drwxr-xr-x  3 ioannis ioannis 4096 Φεβ 26 20:04 .local
drwxr-xr-x  5 ioannis ioannis 4096 Map 2 14:23 .mozilla
drwxr-xr-x  2 ioannis ioannis 4096 Φεβ 26 20:04 Music
drwxr-xr-x  2 ioannis ioannis 4096 Map 8 09:35 Pictures
drwxr--r--  1 ioannis ioannis 807 Φεβ 26 20:00 .profile
drwxr-xr-x  2 ioannis ioannis 4096 Φεβ 26 20:04 Public
drwxr--r--  2 ioannis ioannis 4096 Map 5 10:42 .ssh
drwxr--r--  1 ioannis ioannis 0 Map 1 12:06 .sudo_as_admin_successful
drwxr-xr-x  2 ioannis ioannis 4096 Φεβ 26 20:04 Templates
drwxr-xr-x  2 ioannis ioannis 4096 Φεβ 26 20:04 Videos
ioannis@ioannisserver:~$ sudo chown foititis1:foititis1 /home/aploixrhstes/foititis1
ioannis@ioannisserver:~$ sudo chown foititis2:foititis2 /home/aploixrhstes/foititis2
ioannis@ioannisserver:~$ sudo chown kathigitis:kathigitis /home/aploixrhstes/kathigitis
```

- Με την πρώτη εντολή κάνουμε τον χρήστη icsd18107 owner όλων των φακέλων που βρίσκονται στο /home.

- Με την δεύτερη εντολή βλέπουμε τους διαχειριστές του συστήματος.

- Με την τρίτη εντολή κάνουμε τον χρήστη foititis1 owner του κύριου φακέλου του, με την τέταρτη εντολή κάνουμε τον χρήστη foititis3 owner του κύριου φακέλου του και με την πέμπτη εντολή κάνουμε τον χρήστη kathigitis owner του κύριου φακέλου του.

```
ioannis@ioannisserver:~$ sudo chmod 0750 /home/ioannis
ioannis@ioannisserver:~$ pwd
/home/ioannis
ioannis@ioannisserver:~$ sudo addgroup diaxeiristes
Adding group `diaxeiristes` (GID 1003) ...
Done.
ioannis@ioannisserver:~$ sudo addgroup aploixrhstes
Adding group `aploixrhstes` (GID 1004) ...
Done.
ioannis@ioannisserver:~$ sudo usermod -a -G diaxeiristes ioannis
ioannis@ioannisserver:~$ sudo usermod -a -G diaxeiristes icsd18107
ioannis@ioannisserver:~$ sudo usermod -a -G diaxeiristes sftpuser
ioannis@ioannisserver:~$ sudo usermod -a -G aploixrhstes foititis1
ioannis@ioannisserver:~$ sudo usermod -a -G aploixrhstes foititis2
ioannis@ioannisserver:~$ sudo usermod -a -G aploixrhstes kathigitis
ioannis@ioannisserver:~$ sudo chown ioannis:diaxeiristes /home
ioannis@ioannisserver:~$ sudo chown icsd18107:diaxeiristes /home
ioannis@ioannisserver:~$ sudo ls -l /home
total 16
drwxr-xr-x  5 root   root   4096 Map  8 09:31 aploixrhstes
drwxr-xr-x  5 icsd18107 icsd18107 4096 Map  4 11:22 icsd18107
drwxr-xr-x  16 ioannis ioannis 4096 Map  3 14:58 ioannis
drwxr-----  7 sftpuser sftpuser 4096 Map  5 10:47 sftpuser
```

- Με την πρώτη εντολή δημιουργούμε μία ομάδα με όνομα diaxeiristes.

- Με την δεύτερη εντολή δημιουργούμε μία ομάδα με όνομα aploixrhstes.

- Με τις εντολές "sudo usermod ..." βάζουμε τον κάθε χρήστη στην ομάδα που αντιστοιχεί. Διαχειριστές με διαχειριστές και απλοί χρήστες με απλούς χρήστες.

- Με τις εντολές "sudo chown" κάνουμε τους δύο διαχειριστές του συστήματος owners του /home.



## B7.

```

loannis@ioannissserver:~$ sudo apt update
Get:1 http://security.ubuntu.com/ubuntu focal-security InRelease [109 kB]
Get:2 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metadata [24,3 kB]
Get:3 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Metadata [58,2 kB]
Hit:4 http://ppa.launchpad.net/certbot/certbot/ubuntu focal InRelease
Ign:5 http://ppa.launchpad.net/certbot/certbot/ubuntu focal-updates InRelease [114 kB]
Err:6 http://ppa.launchpad.net/certbot/certbot/ubuntu focal Release
  404 Not Found [IP: 2001:67c:1:568:8000::19 80]
...
Get:8 http://gr.archive.ubuntu.com/ubuntu focal-backports InRelease [101 kB]
Get:9 http://gr.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [434 kB]
Get:10 http://gr.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [841 kB]
Get:11 http://gr.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [264 kB]
Get:12 http://gr.archive.ubuntu.com/ubuntu focal-updates/universe [746 kB]
Get:13 http://gr.archive.ubuntu.com/ubuntu focal-updates/universe i386 Packages [555 kB]
Get:14 http://gr.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Metadata [302 kB]
Get:15 http://gr.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11 Metadata [2468 kB]
Get:16 http://gr.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Metadata [1768 kB]
Reading package lists... Done
E: The repository 'http://ppa.launchpad.net/certbot/certbot/ubuntu focal Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8)'s manpage for repository creation and user configuration details.
loannis@ioannissserver:~$ sudo apt install quota
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  liblirc2 liblircipc-conversion3 liblircrc2_16-0 liblircscore3 liblircdbus5 liblircsgui5 liblircmultimedia5
  liblircmultimedias-plugins liblircmultimediatools5 liblircmultimedawidgets5 liblircnetwork5
  liblircopenpgl5 liblircprintsupport5 liblircssvg5 liblircswidgets5 liblsmzldbl libsnappy5 libspandsp2
  libssh-gcrypt-4 libwireshark-data libwireshark13 libwireshark10 libwsutil11 libxcb-xinerama0
  libxcb-xinput0 qt5-qtk-platformtheme qtranslations5-l10n wireshark-common wireshark-qt
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  liblircp-common liblircpc3
Suggested packages:
  libnet-ldap-perl rpcbind default-mta | mail-transport-agent
...
Activities Terminal Map 8 10:59 en
loannis@ioannissserver:~$
```

```

Selecting previously unselected package quota.
Preparing to unpack .../quota_4.05-1_amd64.deb ...
Unpacking quota (4.05-1) ...
Setting up liblircp-common (1.2.5-1) ...
Setting up liblircrc3:amd64 (1.2.5-1) ...
Setting up quota (4.05-1) ...
Processing triggers for sysvinit (245.4-ubuntu3.4) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for liblc_bln (2.31-ubuntuv9.2) ...
loannis@ioannissserver:~$ sudo nano /etc/fstab
loannis@ioannisserver:~$ sudo requota -s /
requota: Mountpoint (or device) / not found or has no quota enabled.
requota: Not all specified mountpoints are using quota.
loannis@ioannisserver:~$ sudo mount -o remount /
requota: Mountpoint (or device) / not found or has no quota enabled.
requota: Not all specified mountpoints are using quota.
loannis@ioannisserver:~$ sudo edquota -g apolloxrhstes
No filesystem with quota detected.
loannis@ioannisserver:~$ sudo quotacheck -ugm /
quotacheck: Mountpoint (or device) / not found or has no quota enabled.
quotacheck: Cannot find filesystem to check or filesystem not mounted with quota option.
loannis@ioannisserver:~$ sudo nano /etc/fstab
loannis@ioannisserver:~$ sudo mount -o remount /
loannis@ioannisserver:~$ sudo quotacheck -ucm /
...
Activities Terminal Map 8 11:00 en
loannis@ioannisserver:~$
```

Με αυτή την εντολή εγκαθιστούμε το πακέτο quota. Αυτή η δυνατότητα του Linux επιτρέπει στο διαχειριστή του συστήματος να εκχωρήσει ένα μέγιστο χώρο στο δίσκο που μπορεί να χρησιμοποιήσει ένας χρήστης ή ομάδα. Μπορεί να είναι ευέλικτο στην τήρηση των κανόνων που έχουν εκχωρηθεί και εφαρμόζεται ανά σύστημα αρχείων.

- Με την πρώτη εντολή θα τροποποιήσουμε το αρχείο fstab το οποίο καθορίζει τη διαμόρφωση των διαφόρων συστημάτων αρχείων και πώς να τα προσαρτήσουμε ανάλογα με τις ρυθμίσεις που καθορίζονται στο αρχείο..

- Με την δεύτερη εντολή ενεργοποιούμε τις αλλαγές που επιφέρουμε.

- Με την τρίτη εντολή θα εξετάσουμε το σύστημα αρχείων και θα δημιουργήσουμε τα απαιτούμενα αρχεία για το βοηθητικό πρόγραμμα ποσοστώσεων. Η εντολή θα δημιουργήσει ένα αρχείο με το όνομα aquota.user έναν δεν υπάρχει ήδη στο σύστημα.

Νούμερο 1 (από τα παραπάνω βήματα)

## APXEIO: fstab

```

# /etc/fstab: static file system information.
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID in a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
#                
# / was on /dev/sda5 during installation
UUID=beaa37a2-d1f6-40ba-13d39a87c7c5 /           ext4      errors=remount-ro,usrquota 0      1
# /boot/efi was on /dev/sda1 during installation
UUID=664E-C642 /boot/efi   vfat     umask=0077    0      1
/swappfile          none      swap      sw            0      0
...
Activities Terminal Map 8 10:41 en
loannis@ioannisserver:~$
```



```
Activities Terminal Map 8 11:00
Ioannis@Ioannisserver: ~

[u] -u, --user          set limits for user
[g, --group           set limits for group
[P, --project          set limits for project
[a, --all              set limits for all filesystems
[... --always-resolve always try to resolve name, even if is composed only of digits
[F, --format=formatname operate on specific quota format
[p, --prototype=prototype copy limits from user/group/project
[b, --batch             read limits from standard input
[c, --continue=batch   continue in input processing in case of an error
[r, --remote            trim leading slashes from NFSv4 mountpoints
[m, --no-mixed-pathnames edit grace period
[t, --edit-period      edit grace times for user/group/project
[T, --edit-times       edit grace times for user/group/project
[h, --help              display this help text and exit
[v, --version           display version information and exit

Bugs to: jack@suse.cz
Ioannis@Ioannisserver: $ sudo edquota -u foititis1
edquota: WARNING - /dev/sda5: cannot change current block allocation
Ioannis@Ioannisserver: $ sudo quota -v foititis1
Disk quotas for user foititis1 (uid 1006):
  Filesystem space quota limit grace files quota limit grace
  /dev/sda5 16K     8K      0K    4     0     0
Ioannis@Ioannisserver: $ sudo edquota -u foititis1
edquota: WARNING - /dev/sda5: cannot change current block allocation
Ioannis@Ioannisserver: $ sudo quota -v foititis1
Disk quotas for user foititis1 (uid 1006):
  Filesystem space quota limit grace files quota limit grace
  /dev/sda5 16K    700M    700M    4     0     0
Ioannis@Ioannisserver: $ sudo setquota -u foititis2 700M 700M 0 0 /
Ioannis@Ioannisserver: $ sudo setquota -u kathigitis 700M 700M 0 0 /
```

- Με την πρώτη εντολή θα τροποποιήσουμε το αρχείο που περιέχει τα quotas του χρήστη foititis1. Στο παρακάτω στιγμιότυπο θα δούμε τις ακριβώς διορθώσαμε.

- Με την δεύτερη εντολή ενεργοποιούμε τις αλλαγές που επιφέραμε.

- Με την τρίτη και τέταρτη εντολή δίνουμε τον χώρο που θέλουμε να δώσουμε στον χρήστη. 700MB για απλούς χρήστες και 2GB για διαχειριστές συγκεκριμένων υπηρεσιών.

```
Activities Terminal Map 8 11:04
Ioannis@Ioannisserver: ~

[u] -u icisd18107 0 0 0 0 /
Ioannis@Ioannisserver: $ sudo setquota -u loannis 0 0 0 0 /
Ioannis@Ioannisserver: $ sudo repquota -s
** Report for user quota on disk /dev/sda5
Block grace time: 7days Inode grace time: 7days
Filesystem space limits file limits
User used soft hard grace used soft hard grace
root .. 15031M 8K 0K 320K 0 0
nan .. 1612K 8K 0K 169 0 0
lp .. 0K 0K 0K 1 0 0
www-data .. 288K 8K 0K 10 0 0
system-network .. 16K 0K 0K 4 0 0
syslog .. 4176K 8K 0K 15 0 0
_apt .. 32K 0K 0K 4 0 0
tss .. 4K 0K 0K 1 0 0
avahi-autoipd .. 4K 0K 0K 1 0 0
dnsmasq .. 4K 0K 0K 1 0 0
speech-dispatcher .. 8K 0K 0K 2 0 0
nm-openvpn .. 8K 0K 0K 1 0 0
httpd .. 4K 0K 0K 2 0 0
colord .. 58K 0K 0K 5 0 0
geoclue .. 4K 0K 0K 1 0 0
gdm .. 5540K 0K 0K 145 0 0
loannis .. 266M 0K 0K 6217 0 0
icisd18107 .. 8024K 0K 0K 41 0 0
bind .. 72K 0K 0K 18 0 0
sftpuser .. 8024K 2948M 2048M 40 0 0
foititis1 .. 16K 700M 700M 4 0 0
foititis2 .. 16K 700M 700M 4 0 0
kathigitis .. 16K 700M 700M 4 0 0
#62083 .. 576K 0K 0K 4 0 0

Ioannis@Ioannisserver: $
```

- Με την πρώτη εντολή δίνουμε τον απεριόριστο χώρο στους δύο διαχειριστές του συστήματος.

- Με την δεύτερη εντολή επιβεβαιώνουμε τους χώρους που έχουμε αναθέσει σε κάθε χρήστη. Όπως παρατηρούμε, όλα είναι σωστά.

### Νούμερο 1 (από τα παραπάνω βήματα)

ΑΡΧΕΙΟ: disk quota του χρήστη foititis1

```
GNU nano 4.8                               /tmp//EdP.aRddp8t
Disk quotas for user foititis1 (uid 1006):
Filesystem blocks soft hard inodes soft hard
/dev/sda5      16    716800  716800      4     0     0

Ta 716800 είναι 700MB
```



## B8.

```
Activities Terminal Map 9 10:20
loannis@ioannissserver:~$ sudo passwd foititis1
New password:
Retype new password:
password: password updated successfully
loannis@ioannissserver:~$ sudo passwd foititis2
New password:
Retype new password:
password: password updated successfully
loannis@ioannissserver:~$ sudo passwd kathigitis
New password:
Retype new password:
password: password updated successfully
loannis@ioannissserver:~$ vi /etc/rsyslog.conf
[1]+ Stopped                  vi /etc/rsyslog.conf
loannis@ioannissserver:~$ sudo nano /etc/rsyslog.d/50-default.conf
loannis@ioannisserver:~$ /etc/init.d/rsyslog restart
Restarting rsyslog (via systemctl): rsyslog.service.
loannis@ioannisserver:~$ cat /var/log/nea.log
cat: /var/log/nea.log: No such file or directory
loannis@ioannisserver:~$ cat /var/log/users.log
cat: /var/log/users.log: No such file or directory
loannis@ioannisserver:~$ logger -p user.info "Auto einai to log arxeio gia tous xrhstes"
loannis@ioannisserver:~$ cat /var/log/users.log
Mar 9 10:20:22 ioannisserver loannis: Auto einai to log arxeio gia tous xrhstes
loannis@ioannissserver:~$ Mar 9 10:20:22 ioannisserver loannis: Auto einai to log arxeio gia tous xrhstes
loannis@ioannisserver:~$
```

Νούμερο 2 (από τα παραπάνω βήματα)

### ΑΡΧΕΙΟ: rsyslog.conf

```
Activities Terminal Map 9 10:16
loannis@ioannisserver:~$ nano /etc/rsyslog.d/*.*conf
SIncludeConfig /etc/rsyslog.d/*.*conf
Modified

#EOF RULES #####
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
# kern.*          /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none          /var/log/messages
# The authpriv file has restricted access.
authpriv.*                                         /var/log/auth

# Log all the mail messages in one place.
mail.*                                            -/var/log/maillog

# Log cron stuff
cron.*                                             /var/log/cron

# Everybody gets emergency messages
*.emerg                                             *

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                      /var/log/spooler

# Save boot messages also to boot.log
local7.*                                           /var/log/boot.log

user.*                                              /var/log/users.log
news.*                                              /var/log/nea.log

Activities Terminal Map 9 10:28
loannis@ioannisserver:~$ sudo nano /etc/rsyslog.conf
loannis@ioannisserver:~$ /etc/init.d/rsyslog restart
Restarting rsyslog (via systemctl): rsyslog.service.
loannis@ioannisserver:~$ cat /var/log/nea.log
cat: /var/log/nea.log: No such file or directory
loannis@ioannisserver:~$ cat /var/log/users.log
cat: /var/log/users.log: No such file or directory
loannis@ioannisserver:~$ logger -p user.info "Auto einai to log arxeio gia tous xrhstes"
loannis@ioannisserver:~$ cat /var/log/users.log
Mar 9 10:20:22 ioannisserver loannis: Auto einai to log arxeio gia tous xrhstes
loannis@ioannisserver:~$ # see "man logrotate" for details
# rotate log files weekly
weekly

# use the adm group by default, since this is the owning group
# of /var/log/syslog.
su root adm

# keep 4 weeks worth of backlogs
rotate 4

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

# use date as a suffix of the rotated file
#dateext

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

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

# system-specific logs may be also be configured here.
loannis@ioannisserver:~$ sudo nano /etc/logrotate.conf
loannis@ioannisserver:~$ sudo nano /etc/logrotate.d/rsyslog
loannis@ioannisserver:~$
```

```
Activities Terminal Map 9 10:28
loannis@ioannisserver:~$ sudo nano /etc/rsyslog.conf
loannis@ioannisserver:~$ /etc/init.d/rsyslog restart
Restarting rsyslog (via systemctl): rsyslog.service.
loannis@ioannisserver:~$ cat /var/log/nea.log
cat: /var/log/nea.log: No such file or directory
loannis@ioannisserver:~$ cat /var/log/users.log
cat: /var/log/users.log: No such file or directory
loannis@ioannisserver:~$ logger -p user.info "Auto einai to log arxeio gia tous xrhstes"
loannis@ioannisserver:~$ cat /var/log/users.log
Mar 9 10:20:22 ioannisserver loannis: Auto einai to log arxeio gia tous xrhstes
loannis@ioannisserver:~$ # see "man logrotate" for details
# rotate log files weekly
weekly

# use the adm group by default, since this is the owning group
# of /var/log/syslog.
su root adm

# keep 4 weeks worth of backlogs
rotate 4

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

# use date as a suffix of the rotated file
#dateext

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

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

# system-specific logs may be also be configured here.
loannis@ioannisserver:~$ sudo nano /etc/logrotate.conf
loannis@ioannisserver:~$ sudo nano /etc/logrotate.d/rsyslog
loannis@ioannisserver:~$
```

1. Δίνουμε κωδικούς στους χρήστες foititis1, foititis2 και kathigitis αντίστοιχα. Βάζουμε εύκολους κωδικούς για εύκολη διαχείριση. Αυτό όμως δεν θα το κάνουμε σε πραγματικό δημόσιο σέρβερ για λόγους ασφαλείας.
2. Ρυθμίζουμε στο αρχείο αυτά που είναι σημειωμένα με κόκκινο περίγραμμα. Προσθέτουμε, δηλαδή, επιπλέον logs που θέλουμε να καταγράφονται για την ευκολότερη επίβλεψη του συστήματος. Εμείς θα προσθέσουμε logs για τους users (καταγράφει τα μηνύματα που προέρχονται από προγράμματα χρηστών) και news (μηνύματα που προέρχονται από το υποσύστημα νέων του δικτύου).
3. Επανεκκινούμε την rsyslog υπηρεσία που καταγράφει τα logs.
4. Βλέπουμε αν περιέχει κάποιο κείμενο μέσα το αρχείο nea.log όπου εκεί καταγράφονται τα μηνύματα που προέρχονται από το υποσύστημα νέων του δικτύου.
5. Βλέπουμε αν περιέχει κάποιο κείμενο μέσα το αρχείο users.log όπου καταγράφει τα μηνύματα που προέρχονται από προγράμματα χρηστών.
6. Εισάγουμε ένα κείμενο στο αρχείο users.log για να δούμε αν καταγράφει ορθώς όλες τις απαραίτητες πληροφορίες.
7. Εμφανίζουμε τα περιεχόμενα που αρχείου users.log και βλέπουμε ότι κατέγραψε την κίνησή μας την συγκεκριμένη ημερομηνία και ώρα από τον συγκεκριμένο χρήστη.

- Με την πρώτη εντολή βλέπουμε τα περιεχόμενα του αρχείου. Δεν τροποποιήσαμε τίποτα σε αυτό το αρχείο διότι το συγκεκριμένο είναι το εξ' ορισμού αρχείο του συστήματος.

- Με την δεύτερη εντολή τροποποιούμε το αρχείο όπως φαίνεται σε παρακάτω στιγμιότυπο εντός κόκκινου περιγράμματος. Το αρχείο syslog θα αρχικοποιείται κάθε μέρα με αρχεία καταγραφής επτά ημερών και διατηρούνται online. Αξίζει επίσης να σημειωθεί το postrotate. Αυτό καθορίζει την ενέργεια που συμβαίνει μετά την ολοκλήρωση ολόκληρης της περιστροφής καταγραφής.

**Νούμερο -1 (από τα παραπάνω βήματα με -)****ΑΡΧΕΙΟ:** logrotate.conf

```
GNU nano 4.8
# /etc/logrotate.conf
#(root) rotate 4 weeks worth of backlogs
rotate 4
# create new (empty) log files after rotating old ones
create
# use date as a suffix of the rotated file
dateext
# uncomment this if you want your log files compressed
compress
# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may be also be configured here.
# e.g. /var/log/wtmp, or /tmp/btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
    create 6864 root utmp
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 8660 root utmp
    rotate 1
}

```

**Νούμερο -2 (από τα παραπάνω βήματα με -)****ΑΡΧΕΙΟ:** logrotate.d/rsyslog

```
GNU nano 4.8
/var/log/syslog {
    rotate 7
    daily
    missingok
    notifempty
    delaycompress
    compress
    postrotate
        /usr/lib/rsyslog/rsyslog-rotate
    endscript
}

/var/log/mail.info
/var/log/mail.warn
/var/log/mail.err
/var/log/mail.log
/var/log/kern.log
/var/log/kern.log
/var/log/auth.log
/var/log/fcron.log
/var/log/lpr.log
/var/log/cron.log
/var/log/debug
/var/log/messages
{
    rotate 7
    daily
    missingok
    notifempty
    compress
    delaycompress
    sharedscripts
    postrotate
    endscript
}

GNU nano 4.8
missingok
notifempty
delaycompress
compress
postrotate
    /usr/lib/rsyslog/rsyslog-rotate
endscript

}

/var/log/mail.info
/var/log/mail.warn
/var/log/mail.err
/var/log/mail.log
/var/log/dmeson.log
/var/log/kern.log
/var/log/auth.log
/var/log/user.log
/var/log/lpr.log
/var/log/cron.log
/var/log/debug
/var/log/messages
{
    rotate 7
    daily
    missingok
    notifempty
    compress
    delaycompress
    sharedscripts
    postrotate
    /usr/lib/rsyslog/rsyslog-rotate
    endscript
}
```



**B9.**

```
Activities Terminal Map 9 10:40 en
loannis@loannisserver:~
loannis@loannisserver:~$ systemctl.mask ctrl-alt-del.target
Created symlink /etc/systemd/system/ctrl-alt-del.target → /dev/null.
loannis@loannisserver:~$ systemctl daemon-reload
Unknown operation daemon-reload.
loannis@loannisserver:~$ systemctl daemon-reload
loannis@loannisserver:~$ ufw logging on
ERROR: You need to be root to run this script
loannis@loannisserver:~$ sudo ufw logging on
Logging enabled
loannis@loannisserver:~$
```

- Με την πρώτη εντολή ενεργοποιούμε το console security. Το console security σημαίνει απλώς ότι ο περιορισμός της πρόσβασης στον ίδιο τον φυσικό διακομιστή είναι το λειδίνι για να διασφαλίσει ότι μόνο εκείνοι με την κατάλληλη πρόσβαση μπορούν να φτάσουν στον διακομιστή. Όποιος έχει πρόσβαση στον διακομιστή μπορεί να αποκτήσει είσοδο στον διακομιστή, να τον επανεκκινήσει, να αφαρέσει σκληρούς δίσκους, να αποσυνδέσει καλώδια ή ακόμα και να απενεργοποιήσει τον διακομιστή! Για τον περιορισμό κακόβουλων actors με επιβλαβείς προθέσεις, μπορούμε να διασφαλίσουμε ότι οι διακομιστές διατηρούνται σε ασφαλή τοποθεσία.

- Με την δεύτερη εντολή επανεκκινούμε το daemon για να λάβουν μέρος οι αλλαγές που επιφέραμε.

- Με την τρίτη εντολή ενεργοποιούμε τα firewall logs. Το firewall log είναι ένα αρχείο καταγραφής που δημιουργεί και αποθηκεύει πληροφορίες σχετικά με απότελεσματαρικές και άλλες συνδέσεις με το διακομιστή. Η παρακολούθηση αυτών των αρχείων καταγραφής για ασυνήθιστη δραστηριότητα ή / και κακόβουλες απότελεσματαρικές πρόσβασης στο διακομιστή θα βοηθήσει στην ασφάλεια του διακομιστή.

```
Activities Terminal Map 9 10:42 en
loannis@loannisserver:~
```

loannis@loannisserver:~\$ apt install apparmor-profiles  
[1] Could not open lock file /var/lib/dpkg/lock-frontend - open (13: Permission denied)  
[2] Unable to acquire the dpkg frontend lock [/var/lib/dpkg/lock-frontend], are you root?  
loannis@loannisserver:~\$ sudo apt install apparmor-profiles  
[2] E: libapparmorext-0.1:1.0.0-1\_amd64.deb: cannot be installed at this time.  
R: libapparmorext-0.1:1.0.0-1\_amd64.deb  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
libbc-ares2 libdouble-conversion3 libpcre2-16-0 libqt5core5a libqt5dbus libqt5multimedia5  
libqt5multimediawidgets5 libqt5network5 libqt5serialport5 libqt5textformat5 libqt5xml5  
libqrencode5 libtiff5 libtiff5-dev libtiff5-tools libtiff5xx5 libusb-1.0-0 libusb1-0.1 libusb-1.0-0  
liblshh-prcrypt4 libwireshark1 libwireshark1 libwireshartap10 libwutil11 libxcb-xinerama0  
libxcb-xinput0 qt5-gtk-platformtheme qtreversetranslations5 libQt5WebChannel5  
Use 'sudo apt autoremove' to remove them.  
The following new packages will be installed:  
apparmor-profiles  
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.  
Need to get 32,7 kB of archives.  
After this operation, 358 kB of additional disk space will be used.  
Get:1 http://ppa.launchpad.net/apparmor/apparmor/ubuntu focal-updates/main amd64 apparmor-profiles all 2.13.3-7ubuntu5.1 [32,7 kB]  
Fetched 32,7 kB in 0s (16,3 kB/s)  
Selecting previously unselected package apparmor-profiles.  
(Reading database ... 171650 files and directories currently installed.)  
Preparing to unpack .../apparmor-profiles\_2.13.3-7ubuntu5.1\_all.deb ...  
Unpacking apparmor-profiles (2.13.3-7ubuntu5.1) ...  
Setting up apparmor-profiles (2.13.3-7ubuntu5.1) ...  
loannis@loannisserver:~\$ sudo apt-get -y install cryptfs-utils  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
libbc-ares2 libdouble-conversion3 libpcre2-16-0 libqt5core5a libqt5dbus libqt5multimedia5  
libqt5multimediawidgets5 libqt5network5 libqt5serialport5 libqt5textformat5 libqt5xml5  
libqrencode5 libtiff5 libtiff5-dev libtiff5-tools libtiff5xx5 libusb-1.0-0 libusb1-0.1 libusb-1.0-0  
liblshh-prcrypt4 libwireshark1 libwireshark1 libwireshartap10 libwutil11 libxcb-xinerama0  
libxcb-xinput0 qt5-gtk-platformtheme qtreversetranslations5 libQt5WebChannel5  
Use 'sudo apt autoremove' to remove them.

- Με την πρώτη εντολή εγκαθιστούμε και ενεργοποιούμε το apparmor. Το AppArmor είναι μια λειτουργική μονάδα ασφαλείας πυρήνα Linux που επιτρέπει σε έναν διαχειριστή να εφαρμόζει περιορισμούς βάσει προγράμματος (σε αντίθεση με περιορισμούς που βασίζονται σε χρήστες) για τον περιορισμό πόρων και τον έλεγχο της πρόσβασης. Εγκαθίσταται και φορτώνεται από προεπιλογή και χρησιμοποιεί ένα προφίλ προγράμματος για να προσδιορίσει ποια πρόσβαση και / ή δικαιώματα απαιτεί.

- Με την δεύτερη εντολή εγκαθιστούμε και ενεργοποιούμε το eCryptfs. Το eCryptfs είναι λογισμικό που κρυπτογραφεί ένα αρχείο, φάκελο ή διαμέρισμα για να ασφαλίζει τα περιεχόμενά του. Ακούγεται πολύ πιο περίπλοκο από ό, τι είναι, αν και η λειτουργικότητα μπορεί να γίνει βαθιά, η συνήθης εστίαση είναι στη δημιουργία ενός χώρου που προστατεύεται και δεν μπορεί να διαβαστεί εκτός εάν επιτούέπειτα ειδικά από έναν διαγειούστη.



321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

## **Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση**

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

```
Activities Terminal Map 9:11:02 en
loannis@loanisserver:~
```

loanis@loanisserver:~ \$ sudo mkfs /home/loanis/kryptografist  
loanis@loanisserver:~ \$ sudo mount -t encryptfs /home/loanis/kryptografist /home/loanis/kryptografist  
Passphrase:  
Wrong input, non-empty value required!  
Passphrase:  
Selection [yes/no]:  
Selected cipher:  
1) aes: blocksize = 16; min keysize = 16; max keysize = 32  
2) blowfish: blocksize = 8; min keysize = 16; max keysize = 56  
3) des3\_ede: blocksize = 8; min keysize = 24; max keysize = 24  
4) twofish: blocksize = 16; min keysize = 16; max keysize = 32  
5) cast5: blocksize = 16; min keysize = 16; max keysize = 32  
6) blowfish: blocksize = 8; min keysize = 5; max keysize = 16  
Selection [aes]:^Z  
[3]+ Stopped sudo mount -t encryptfs /home/loanis/kryptografist /home/loanis/kryptografist  
st  
loanis@loanisserver:~ \$ sudo mount -t encryptfs /home/loanis/kryptografist /home/loanis/kryptografist  
Passphrase:  
Selection cipher:  
1) aes: blocksize = 16; min keysize = 16; max keysize = 32  
2) blowfish: blocksize = 8; min keysize = 16; max keysize = 56  
3) des3\_ede: blocksize = 8; min keysize = 24; max keysize = 24  
4) twofish: blocksize = 16; min keysize = 16; max keysize = 32  
5) cast5: blocksize = 16; min keysize = 16; max keysize = 32  
6) blowfish: blocksize = 8; min keysize = 5; max keysize = 16  
Selection [aes]: 3  
Select key bytes:  
1) 24  
Selection [24]: 1  
Enable plaintext passthrough (y/n) [n]:  
Enable transparent encryption (y/n) [n]:  
Attempting to mount with the following options:  
encryptfs unlkng\_sigs  
encryptfs key bytes=24  
encryptfs\_cipher=des3\_ede  
encryptfs\_slg=2237dia9f4e1328f  
WARNING! Overwriting the contents of [/root/.encryptfs/sig-cache.txt],  
it seems like another session was mounted with this key  
before. This could mean that you have typed your

- Με την πρώτη εντολή φτιάχνουμε έναν φάκελο στον οποίο όταν αποθηκεύονται αρχεία, θα κρυπτογραφούνται για λόγους ασφαλείας.

- Με την δεύτερη εντολή κρυπτογραφούμε τον φάκελο που δημιουργήσαμε πριν τοποθετώντας το με το σύστημα αρχείων τύπου eCryptfs.

- Με την πρώτη εντολή φτιάχνουμε ένα αρχείο κειμένου στο οποίο θα γράψουμε ένα απλό κείμενο ώστε να δούμε την λειτουργία της κρυπτονόφθασης.

- Με την δεύτερη εντολή βλέπουμε το κείμενο που έχουμε βάλει μέσα στο αρχείο.

- Με την τρίτη εντολή αποσυνδέουμε τον φάκελο ώστε να κρυπτογραφηθεί το κείμενο.

- Με την τέταρτη εντολή βλέπουμε τα περιεχόμενα του αρχείου κειμένου που φτιάξαμε παραπάνω. Παρατηρούμε ότι το κείμενο έχει κρυπτογραφηθεί επιτυχώς.

```
Activities Terminal Map 9:112 en
loannis@loannisserver:~ Reading package lists... done
Building dependency tree
Reading state information... done
The following packages were automatically installed and are no longer required:
liblbc-area52 libdouble-conversion liblpcr2-16.0 liblqtscore5a liblqt5dbus liblqt5gu5 liblqt5multimedia
liblqt5multimediacore liblqt5multimediacore5 liblqt5multimediacore5a liblqt5multimediacore5t liblqt5networks
liblqt5networks5 liblqt5printsupport liblqt5wp5 liblqt5wp5t liblqt5wp5t5 liblqt5wp5t5a liblqt5wp5t5t libspansp2
liblssh2-crypt4 liblwxreshark-data liblwxreshark13 liblwxretp10 libwsutil11 libxcb-xinerama8
libxcb-xinput8 qt-gtk-platformtheme qtranslations5-l10n wireshark-common wireshark-qt
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
liblbpam-pwquality
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 11,2 kB of archives.
After this operation, 39,9 kB of additional disk space will be used.
Get: http://ppa.launchpad.net/ubuntuteam/libpam-pwquality/ubuntu focal/main amd64 liblbpam-pwquality amd64 1.4.2-1build1 [11,2 kB]
Fetched 11,2 kB in 2s (5807 B/s)
Selecting previously unselected package liblbpam-pwquality:amd64.
(Reading database changes... 1728 files and directories currently installed.)
Preparing to unpack .../liblbpam-pwquality_1.4.2-1build1_amd64.deb ...
Unpacking liblbpam-pwquality:amd64 (1.4.2-1build1) ...
Setting up liblbpam-pwquality:amd64 (1.4.2-1build1) ...
Processing triggers for man-db (2.9.1-1) ...
loannis@loannisserver:~$ sudo cp /etc/pam.d/common-password /etc/pam.d/common-password.backup
loannis@loannisserver:~$ sudo nano /etc/pam.d/common-password
loannis@loannisserver:~$ reboot
```

- Με την πρώτη εντολή εγκαθιστούμε ένα πακέτο που θα μας βοηθήσει να ασφαλίσουμε το σύστημά μας με το να επιβάλλουμε στους χρήστες να βάλουν δυνατούς κωδικούς πρόσβασης.

- Με τη δεύτερη εντολή φτιάχνουμε ένα backup για το εξ' ορισμού αρχείο του συστήματος που περιέχει τις προϋποθέσεις για τους κωδικούς πρόσβασης των χρηστών.

- Με την τρίτη εντολή θα τροποποιήσουμε κατά τις δικές μας απαιτήσεις το αρχείο που περιέχει τις προύστωθεσί για τους κωδικούς πρόσβασης των χρηστών. Έχουμε τις εξής απαιτήσεις: α) ο χρήστης μπορεί μέχρι 3 φορές να βάλει λάθος κωδικό, β) ελάχιστο μήκος κωδικού είναι οι 8 χαρακτήρες, γ) πόσοι χαρακτήρες είναι ίδιοι με αυτούς παλαιότερου κωδικού (3), δ) ελάχιστος αριθμός μη κεφαλαίων γραμμάτων (1), ε) ελάχιστος αριθμός κεφαλαίων γραμμάτων (1), στ) ελάχιστος αριθμός ψηφίων (1), ζ) ελάχιστος αριθμός συμβόλων (1), η) απορρίπτει κωδικού που περιέχει το username του χρήστη, θ) τα ίδια ισχύουν και για τον root user.

- Με την τέταρτη εντολή επανεκκινούμε το σύστημά μας για να λάβουν μέρος οι αλλαγές που επιφέρουμε.



## 321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

### Νούμερο -3 (από τα παραπάνω βήματα με -)

ΑΡΧΕΙΟ: pam.d/common-password

```
GNU nano 4.8 /etc/pam.d/common-password Modified
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.

# Explanation of pam_unix options:
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
# The "obscure" option replaces the old 'OBSCURE_CHECKS_ENAB' option in
# login.defs.
# See the pam_unix manpage for other options.

# As of pam 1.8.1-6, 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)
password    requisite      pam_pwhistory.so retry=3 maxlen=8 difok=3 lcredit=1 uret=1
password    [success=1 default=ignore]  pam_unix.so obscure use_authtok try_first_pass sha512
# here's the fallback if no module succeeds
password    requisite      pam_deny.so
password    requisite      pam_permit.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
password    required       pam_permit.so
# and here are more per-package modules (the "Additional" block)

# Here are the per-package modules (the "Primary" block)
password    requisite      pam_unix.so obscure use_authtok try_first_pass sha512
password    [success=1 default=ignore]  pam_unix.so obscure use_authtok try_first_pass sha512
# here's the fallback if no module succeeds
password    requisite      pam_deny.so
password    requisite      pam_permit.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
password    required       pam_permit.so
# and here are more per-package modules (the "Additional" block)
```

- Με την πρώτη εντολή τροποποιούμε το αρχείο για να καθορίσουμε την συχνότητα αλλαγής κωνικών καθώς και το πότε λήγει ο κωδικός ενός χρήστη. Φαίνονται παρακάτω στο στιγμιότυπο με κόκκινο περίγραμμα. Θα καθορίσουμε α) μένιστο αριθμό ημερών όπου ο κωδικός μπορεί να χρησιμοποιηθεί, τις 120, β) ελάχιστο αριθμό ημερών όπου ανάμεσα στους μπορεί ο χρήστης να πραγματοποιήσει αλλαγές στον κωδικό, τις 0, γ) αριθμό ημερών που ενημερώνουν τον χρήστη ότι ο κωδικός του λήγει, τις 8.

- Με την δεύτερη εντολή βλέπουμε όλα τα στοιχεία του κωδικού του χρήστη μας. Ο κωδικός του χρήστη αυτού καθορίστηκε στις 26 Φεβρουαρίου, πριν, δηλαδή, από την τροποποίηση των προϋποθέσεων για έναν κωδικό πρόσβασης. Γι' αυτό τον λόγο οι πληροφορίες που βγάζει είναι λάθος. Εάν αναθέταμε έναν κωδικό με τις τρέχουσες προϋποθέσεις αυτή την στιγμή, θα μας έδειχνε τις σωστές πληροφορίες.

### Νούμερο -1 (από τα παραπάνω βήματα με -)

ΑΡΧΕΙΟ: login.defs

```
GNU nano 4.8 /etc/login.defs Modified
# useradd and newusers to set the mode of the new home directories.
# 022 is the "historical" value in Debian for UMASK
# 027, or even 077, could be considered better for privacy
# There is no One True Answer here : each sysadmin must make up his/her
# mind.

# If USERGROUPS_ENAB is set to "yes", that will modify this UMASK default value
# for private user groups, i. e. the uid is the same as gid, and username is
# the same as the primary group name: for these, the user permissions will be
# used as group permissions, e. g. 022 will become 002.
#
# Prefix these values with "0" to get octal, "0x" to get hexadecimal.

# ERASECHAR      0177
# KILLCHAR       025
# UMASK          022

#
# Password aging controls:
#
#   PASS_MAX_DAYS   Maximum number of days a password may be used.
#   PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#   PASS_WARN_AGE   Number of days warning given before a password expires.

#   PASS_MAX_DAYS  120
#   PASS_MIN_DAYS  0
#   PASS_WARN_AGE  8

#
# Min/max values for automatic uid selection in useradd
#
#   UID_MIN        1000
#   UID_MAX        60000
#   # System accounts
```



## B10.

```
Activities Terminal Map 9 11:41
loannis@ioannisserv:~$ sudo nano /etc/pam.d/common-password
[sudo] password for ioannis:
loannis@ioannisserv:~$ sudo nano /etc/pam.d/system-auth
loannis@ioannisserv:~$ sudo nano /etc/pam.d/common-auth
loannis@ioannisserv:~$ sudo systemctl restart sshd
loannis@ioannisserv:~$
```

- Με την πρώτη εντολή τροποποιούμε το αρχείο για να απαγορεύσουμε σε έναν χρήστη να χρησιμοποιήσει κάπιον από τους παλαιότερους κωδικούς που έχει χρησιμοποιήσει. Αυτό φαίνεται σε παρακάτω στιγμιότυπο σε κόκκινο περίγραμμα.

- Με την δεύτερη εντολή τροποποιούμε το αρχείο για να κλειδώσουμε τον λογαριασμό του χρήστη που δίνει πάνω από 3 φορές λάθος κωδικό. Συγκεκριμένα θα τον κλειδώσουμε για μία ώρα δηλαδή 3600 δευτερόλεπτα. Φαίνονται στο παρακάτω στιγμιότυπο σε κόκκινο περίγραμμα.

- Με την τρίτη εντολή επανεκκινούμε το ssh service για να ενεργοποιηθούν οι αλλαγές που επιφέρουμε.

### Νούμερο -1 (από τα παραπάνω βήματα με -)

**APXEIO: common-password**

```
Activities Terminal Map 9 11:22
loannis@ioannisserv:~$ GNU nano 4.8 /etc/pam.d/common-password
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.
#
# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old 'OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.
#
# 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)
password requisite pan_pwquality.so retry=3 minlen=8 difok=3 lcredit=1 ucredit=1
password required pam_pwhistory.so remember=5
password [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass sha512
# here's the fallback if no module succeeds
password 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
password required pam_permit.so
# and here are more per-package modules (the "Additional" block)

::: Get Help Write Out Where Is Cut Text Justify Cur Pos Undo
::: Exit Read File Replace Paste Text To Spell Go To Line Redo
```

### Νούμερο -2 (από τα παραπάνω βήματα με -)

**APXEIO: common-auth**

```
Activities Terminal Map 9 11:40
loannis@ioannisserv:~$ GNU nano 4.8 /etc/pam.d/common-auth
# /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
auth required pam_tally2.so onerr=fail deny=3 unlock_time=3600 audit
# 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_encryptfs.so unrap
auth optional pam_cap.so
# end of pam-auth-update config

::: Get Help Write Out Where Is Cut Text Justify Cur Pos Undo
::: Exit Read File Replace Paste Text To Spell Go To Line Redo
```



## B11.

```
Activities Terminal Map 9 11:46
ioannis@ioannissserver:~$ find . -perm /4000
ioannis@ioannissserver:~$ find . -perm /2000
ioannis@ioannissserver:~$ find . -perm /6000
ioannis@ioannissserver:~$
```

- Με την πρώτη εντολή βρίσκουμε όλα τα αρχεία που έχουν δικαιώμα SUID. Όπως παρατηρούμε, δεν υπάρχει κανένα αρχείο στο σύστημά μας με τέτοια δικαιώματα.

- Με την δεύτερη εντολή βρίσκουμε όλα τα αρχεία που έχουν δικαιώμα SGID. Όπως παρατηρούμε, δεν υπάρχει κανένα αρχείο στο σύστημά μας με τέτοια δικαιώματα.

- Με την τρίτη εντολή βρίσκουμε όλα τα αρχεία που έχουν δικαιώματα SUID και SGID. Όπως παρατηρούμε, δεν υπάρχει κανένα αρχείο στο σύστημά μας με τέτοια δικαιώματα.

## B11.

```
Activities Terminal Map 9 13:00
ioannis@ioannissserver:~$ sudo chmod 1777 /tmp
ioannis@ioannissserver:~$
```

Με αυτή την εντολή ρυθμίζουμε το sticky bit στο /tmp και σε άλλα αρχεία με δυνατότητα εγγραφής σε όλους τους χρήστες.

```
Activities Terminal Map 9 13:02
ioannis@ioannissserver:~$ sudo find / -xdev -type d \(\ -perm -0002 -a ! -perm -1000 \) -print
ioannis@ioannissserver:~$
```

Με αυτή την εντολή εντοπίζουμε τυχόν καταλόγους σε τοπικά διαμερίσματα που είναι παγκόσμια εγγράψιμα και δεν έχουν sticky bit.



## ΝΜΑΡ ΚΑΙ NESSUS ΕΛΕΓΧΟΣ ΠΡΙΝ ΠΡΟΧΩΡΗΣΟΥΜΕ ΣΕ ΕΝΔΥΝΑΜΩΣΗ ΤΟΥ ΛΣ.

The screenshot shows the Zenmap interface with the following details:

- Scan Options:** Target: 94.65.57.13, Profile: Intense scan, Command: nmap -T4 -A -v 94.65.57.13
- Host Details:** Host: ppp-94-65-57-13.hn, OS: Ubuntu Linux 9.16.1 (Ubuntu), Nmap version: 9.16.1-Ubuntu
- Services:** Ports open: 80/tcp (http), 443/tcp (https)
- Service Details:** http: Apache/2.4.41 ((Ubuntu)), https: Apache/2.4.41 ((Ubuntu))
- OS Details:** OS fingerprint: commonName=ioannissserver.com/organizationName=PanosIoannis/stateOrProvinceName=Samos/countryName=GR
- Network Distance:** 1 hop
- Service Info:** OS: Linux; CPE: cpe:/o:linux:linux\_kernel
- Script Output:** Shows various NSE scripts running, including OS detection, service detection, and traceroute.

Χρησιμοποιώντας το λογισμικό πιπαρ για την ανίχνευση ανοιχτών θυρών, παρατηρούμε ότι έχουν ανοίξει άλλες 3 θύρες σε σχέση με τον προηγούμενο έλεγχο. Ενδεικτικά, έχουν ενεργοποιηθεί οι εξής θύρες:

- 53 DNS
- 80 HTTP
- 443 HTTPS

Όλες οι υπόλοιπες είναι κλειστές. Επίσης, δημιουργήθηκε ένα νέο πρόστιμο στην πρώτη θύρα, με πάρομη πληροφορία σχετικά με τις υπηρεσίες που τρέχουν σε συγκεκριμένη πόρτα, το λογισμικό της υπηρεσίας καθώς και άλλες παραμέτρους που έχουν δοθεί σε μία συγκεκριμένη υπηρεσία

Ως απορία έχουμε το εξής: με ποιον τρόπο μπορούμε να εμποδίσουμε το πιπαρ να αναγνωρίζει το λογισμικό μιας συγκεκριμένης υπηρεσίας και τις παραμέτρους που έχουμε θέσει σε αυτή;



## 321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

The screenshot shows the Nessus Essentials web interface. On the left, there's a sidebar with icons for Activities, Firefox Web Browser, Nessus Essentials / Folder, and other system status indicators. The main area displays a scan report for a host named 'o server mou'. The report lists 37 vulnerabilities categorized by service family: General (11), Web Servers (5), DNS (4), Port scanners (11), Service detection (10), and others. A pie chart on the right shows the severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). Scan details indicate it was an Advanced Scan completed today at 1:13 PM, taking 2 minutes.

Από το παραπάνω στιγμιότυπο παρατηρούμε ότι έχουμε 34 ενημερωτικές και 3 μετρίου κινδύνου ευπάθειες. Σε σχέση με τον προηγούμενο έλεγχο που κάναμε, παρατηρούμε ότι αυξήθηκαν οι ευπάθειες διότι ανοίξαμε επιπλέον υπηρεσίες/θύρες με αποτέλεσμα ο σέρβερ μας να είναι αρκετά πιο εκτεθειμένος στο δημόσιο δίκτυο. Επομένως με την ενεργοποίηση 3 υπηρεσιών (web service, dns service και secure ftp service) οι ευπάθειες αυξήθηκαν από 32 σε 37. Ψάχνοντας στην βιβλιογραφία παρατηρήσαμε ότι εφόσον μία πόρτα είναι ανοιχτή και τρέχει πάνω σε αυτή μία υπηρεσία, τότε δεν υπάρχει τρόπος για απαγόρευση του service detection από λογισμικά για vulnerability detection.



321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

## **ΚΕΦΑΛΑΙΟ 3**

Αυτοματοποίηση Διαδικασιών



## SCRIPT 1.

```
Activities Terminal Mar 19 13:23
ioannis@ioannissserver:~/Downloads$ python3 script1.py
Παρακαλώ εισάγετε την επιλογή σας:
clear
ioannis Mar 19 12:30:36 clear
ioannis Mar 19 12:49:49 clear
ioannis Mar 19 12:54:42 clear
ioannis Mar 19 12:57:15 clear
ioannis Mar 19 12:58:13 clear
ioannis Mar 19 12:59:47 clear
ioannis Mar 19 13:13:45 clear
ioannis Mar 19 13:17:54 clear
ioannis Mar 19 13:19:17 clear
ioannis Mar 19 13:22:45 clear
ioannis@ioannissserver:~/Downloads$
```

Το συγκεκριμένο script παίρνει είσοδο από ένα αρχείο που περιέχει μέσα το όνομα του χρήστη, τον μήνα, την ημέρα, την ώρα και την εντολή που εκτέλεσε. Εμείς βάλαμε να ψάχνει ποιοι χρήστες και πότε πληκτρολόγησαν την εντολή clear. Όπως παρατηρούμε, τα αποτελέσματα είναι ορθά.

## SCRIPT 2.

```
Activities Terminal Mar 19 13:24
ioannis@ioannissserver:~/Downloads$ python3 script2.py
Για την συνδεσή σας στο server πιέστε 1
Για την έξοδό σας από τον server πιέστε οποιοδήποτε άλλο πλήκτρο
Παρακαλώ εισάγετε την επιλογή σας:
1

Username:
foltitisi
Κωδικός:
8888
Τα Στοιχεία εισόδου είναι λάθος!

Για την συνδεσή σας στο server πιέστε 1
Για την έξοδό σας από τον server πιέστε οποιοδήποτε άλλο πλήκτρο
Παρακαλώ εισάγετε την επιλογή σας:
1

Username:
foltitisi
Κωδικός:
8888
Τα Στοιχεία εισόδου είναι λάθος!

Για την συνδεσή σας στο server πιέστε 1
Για την έξοδό σας από τον server πιέστε οποιοδήποτε άλλο πλήκτρο
Παρακαλώ εισάγετε την επιλογή σας:
1

Username:
foltitisi
Κωδικός:
8888
Τα Στοιχεία εισόδου είναι λάθος!

Για την συνδεσή σας στο server πιέστε 1
Για την έξοδό σας από τον server πιέστε οποιοδήποτε άλλο πλήκτρο
Παρακαλώ εισάγετε την επιλογή σας:
1

Username:
foltitisi
Κωδικός:
8888
Τα Στοιχεία εισόδου είναι λάθος!

Ο Λογαριασμός σας απενεργοποιήθηκε!!!
```

```
Activities Terminal Mar 19 13:25
ioannis@ioannissserver:~/Downloads$ python3 script2.py
Για την συνδεσή σας στο server πιέστε 1
Για την έξοδό σας από τον server πιέστε οποιοδήποτε άλλο πλήκτρο
Παρακαλώ εισάγετε την επιλογή σας:
1

Username:
ioannis
Κωδικός:
5705
Επιτυχής σύνδεση!
ioannis@ioannissserver:~/Downloads$
```

Το συγκεκριμένο script παίρνει είσοδο από ένα αρχείο που περιέχει μέσα τα ονόματα όλων των χρηστών του συστήματος καθώς και τον κωδικό πρόσβασης του καθενός. Αρχικά θα τσεκάρει αν ο χρήστης και ο κωδικός πρόσβασής του ταιριάζουν. Αν βάλουμε έναν χρήστη που δεν υπάρχει στο σύστημα, θα βγάλει «Τα στοιχεία είναι λάθος» διότι δεν θέλουμε να δώσουμε στον χρήστη που προσπαθεί να μπεί περισσότερες πληροφορίες. Εάν ο κωδικός είναι λάθος 3 συνεχόμενες φορές για τον ίδιο χρήστη, τον απενεργοποιεί αλλά δεν τον διαγράφει. Αν κωδικός και όνομα χρήστη είναι ορθά τότε επιτυχάνεται η σύνδεση. Εάν βάλουμε έναν χρήστη που δεν υπάρχει καν, τότε μετά από 10 αποτυχημένες προσπάθειες δεν μας επιτρέπει να συνεχίσουμε.



### SCRIPT 3.

```
Activities Terminal Map 19 13:19
loannis@ioannissserver:~/Downloads$ python3 script3.py
Χρήστες με κενό password:
Χρήστης: admin8
Χρήστης: test1
Χρήστης: test2
Οι παραπάνω λογαριασμοί απενεργοποιήθηκαν!!!
loannis@ioannissserver:~/Downloads$
```

Το συγκεκριμένο script παίρνει είσοδο από ένα αρχείο που περιέχει μέσα τα ονόματα όλων των χρηστών του συστήματος καθώς και τον κωδικό πρόσβασης του καθενός. Βλέπει ποιοι χρήστες δεν περιέχουν συνθηματικό και τους απενεργοποιεί αλλά δεν τους διαγράφει.

### SCRIPT 4.

```
Activities Terminal Map 19 15:21
loannis@ioannissserver:~/Downloads$ python3 script4.py
Παρακαλώ εισάγετε την διάρκεια σύνδεσης ενός χρήστη (XX:XX):
00:10
ioannis :0 :0 Wed Mar 17 11:16 - down (00:10)
loannis@ioannissserver:~/Downloads$
```

Το συγκεκριμένο script παίρνει είσοδο από ένα αρχείο που περιέχει μέσα το όνομα του χρήστη, την διεύθυνση IP, την ημέρα, τον μήνα, τον αριθμό της ημέρας, την ώρα εισόδου, την ώρα εξόδου και την διάρκεια σύνδεσης. Ο χρήστης εισάγει την διάρκεια σύνδεσης ενός χρήστη σε μορφή XX:XX και εάν υπάρχει χρήστης που να έχει αυτή την διάρκεια, τότε εκτυπώνει όλες τις πληροφορίες του. Όπως παρατηρούμε τα αποτελέσματα είναι ορθά.



321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

## **ΚΕΦΑΛΑΙΟ 4**

### Συμπεράσματα



## Συμπεράσματα

Με την επίλυση αυτής της εργασίας μάθαμε τα εξής:

- Να χτίσουμε έναν δημόσιο σέρβερ σε Linux based Ubuntu OS.
- Να ανοίγουμε και να κλείνουμε πόρτες.
- Να ενεργοποιούμε, να απενεργοποιούμε και να παραμετροποιούμε υπηρεσίες.
- Να ασφαλίζουμε τον σέρβερ και τις υπηρεσίες.
- Να ενημερωνόμαστε για ευπάθειες και ανοιχτές πόρτες που έχει ο σέρβερ μας.
- Να αποδίδουμε δικαιώματα ανάλογα με τον ρόλο του κάθε χρήστη.

Ένας Linux based σέρβερ είναι μία πολύ καλή ευκαιρία να αρχίσει κάποιος να καταλαβαίνει πως λειτουργούν τα πληροφοριακά συστήματα. Είναι σχετικά εύκολος στην χρήση και την παραμετροποίηση. Ωστόσο για να μπορεί να φέρει εις πέρας κρίσιμες υπηρεσίες θα πρέπει η ασφάλεια να είναι αυξημένη προκειμένου να ελαττωθούν οι πιθανότητες για διαρροή δεδομένων και αναστολή λειτουργίας.

Καταναλώσαμε αρκετή ώρα προκειμένου να βρούμε λύσεις στα ερωτήματα που μας ζητήθηκαν. Η αναζήτηση λύσεων στα ερωτήματα πήρε αρκετό χρόνο και γι' αυτό τον λόγο ορισμένα στιγμότυπα αναγράφουν μελλοντική ημερομηνία σε σχέση με την ημερομηνία που επιλύθηκε το συγκεκριμένο ερώτημα. Είναι γεγονός ότι κάθε πηγή πληροφόρησης αναγράφει τον δικό της τρόπο με τον οποίο επιλύει ένα ερώτημα με αποτέλεσμα να προκληθεί σύγχυση στις λύσεις μας. Από την αρχή που ξεκινήσαμε το χτίσιμο του σέρβερ, είχαμε απενεργοποίησει όλες τις άχρηστες λειτουργίες και είχαμε κρατήσει μόνο εκείνες που μας ζητούνται. Δεν βάλαμε δύσκολους κωδικούς πρόσβασης για λόγους ταχύτητας και ευκολίας. Τηρήσαμε κατά γράμμα όλα τα βήματα που αναγράφονται στην βιβλιογραφία διότι είναι η πρώτη φορά που ασχολούμαστε με παρόμοια εργασία.



321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

## **ΚΕΦΑΛΑΙΟ 5**

**Συμπεράσματα**



## Βιβλιογραφία

[A1]: [https://linuxhint.com/install\\_ubuntu\\_virtualbox\\_2004/](https://linuxhint.com/install_ubuntu_virtualbox_2004/)

[A2]: <https://vitux.com/ubuntu-network-configuration/>

[A2]: [https://linuxhint.com/ubuntu\\_20-04\\_network\\_configuration/](https://linuxhint.com/ubuntu_20-04_network_configuration/)

[A2]: <https://www.techrepublic.com/article/how-to-configure-a-static-ip-address-in-ubuntu-server-18-04/>

[A2]: <https://linuxconfig.org/how-to-deny-all-incoming-ports-except-ssh-port-22-on-ubuntu-18-04-bionic-beaver-linux>

[A2]: <https://www.ubuntu18.com/ubuntu-change-ssh-port/>

[A2]: <https://www.a2hosting.com/kb/getting-started-guide/accessing-your-account/changing-the-ssh-server-port-number>

[A3]: <https://www.a2hosting.com/kb/getting-started-guide/accessing-your-account/disabling-ssh-logins-for-root>

[A4]: <https://www.tecmint.com/enable-and-disable-root-login-in-ubuntu/>

[A5]: <https://phoenixnap.com/kb/automatic-security-updates-ubuntu>

[B1]: <https://motorscript.com/cleanup-ubuntu-server/>

[B1]: <https://www.techrepublic.com/blog/10-things/boost-security-by-stopping-these-10-linux-services-on-your-server/>

[B1]: <https://hostadvice.com/how-to/how-to-harden-your-ubuntu-18-04-server/>

[B1]: <https://www.liquidweb.com/kb/top-15-server-security-practices-for-2020/>

[B1]: <https://www.cyberciti.biz/tips/linux-security.html>

[B2]: <https://www.cyberciti.biz/tips/linux-security.html>

[B3]: <https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-20-04>

[B3]: <https://www.answertopia.com/ubuntu/setting-up-an-ubuntu-web-server/>

[B3]: <https://www.linuxbabe.com/ubuntu/set-up-local-dns-resolver-ubuntu-20-04-bind9>

[B3]: <https://www.linuxbabe.com/ubuntu/ubuntu-stubby-dns-over-tls>

[B3]: <https://ubuntu.com/server/docs/service-domain-name-service-dns>

[B3]: <https://linuxconfig.org/how-to-setup-sftp-server-on-ubuntu-20-04-focal-fossa-linux>



321-3404- Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τίτλος Μελέτης: 1<sup>η</sup> Εργαστηριακή Άσκηση

Παπαδόπουλος Παναγιώτης – Κυριαζής Ιωάννης

[B4]: <https://www.cyberciti.biz/tips/linux-security.html>

[B5]: <https://www.cyberciti.biz/faq/linux-kernel-etcctl-conf-security-hardening/>

[B6]: <https://www.digitalocean.com/community/tutorials/how-to-create-a-new-sudo-enabled-user-on-ubuntu-20-04-quickstart>

[B6]: <https://www.cyberciti.biz/faq/ubuntu-add-user-to-group-www-data/>

[B6]: <https://www.digitalocean.com/community/questions/how-do-i-restrict-a-user-to-a-specific-directory>

[B6]: <https://linode.com/create-home-directory-existing-user-linux/>

[B7]: <https://www.digitalocean.com/community/tutorials/how-to-set-filesystem-quotas-on-ubuntu-18-04>

[B7]: [https://www.alibabacloud.com/blog/how-to-set-up-disk-quota-on-ubuntu-18-04-server\\_595877](https://www.alibabacloud.com/blog/how-to-set-up-disk-quota-on-ubuntu-18-04-server_595877)

[B8]: <https://linode.com/setup-log-rotation-logrotate-ubuntu/>

[B8]: <https://www.digitalocean.com/community/tutorials/how-to-view-and-configure-linux-logs-on-ubuntu-and-centos#creating-and-testing-your-own-log-messages>

[B9]: <https://www.liquidweb.com/kb/best-practices-security-new-ubuntu-server/>

[B9]: <https://www.liquidweb.com/kb/best-practices-security-new-ubuntu-server-apparmor-certs-ecryptfs-encrypted-lvm/#lvm>

[B9]: [https://linuxhint.com/secure\\_password\\_policies\\_ubuntu/](https://linuxhint.com/secure_password_policies_ubuntu/)

[B10]: <https://askubuntu.com/questions/754958/how-to-prevent-users-from-changing-their-password-to-one-of-the-last-x-passwords>

[B10]: <https://www.linuxtechi.com/lock-user-account-incorrect-login-attempts-linux/>

[B11]: <https://www.tecmint.com/how-to-find-files-with-suid-and-sgid-permissions-in-linux/>

[B11]: <http://blog.serverbuddies.com/security-verify-that-all-world-writable-directories-have-sticky-bits-set/>

[B12]: [https://docs.oracle.com/cd/E58626\\_01/html/E58630/gqebd.html](https://docs.oracle.com/cd/E58626_01/html/E58630/gqebd.html)

# **ΠΕΡΑΣ 1<sup>ης</sup> ΕΡΓΑΣΤΗΡΙΑΚΗΣ ΑΣΚΗΣΗΣ**



Kyriazis Ioannis | Papadopoulos Panagiotis

Copyright © 2021 – All Rights Reserved