eh1act05 – Firewalls

GENERAL CONDITIONS

1- Deadline: **28-04-2025**
2- Teacher will check that your operating system is working properly

DOCUMENTATION

1- Basic ideas

A **firewall** is a security system that monitors and controls **incoming and outgoing network traffic** based on **predetermined security rules**. It acts like a **barrier** between a trusted network (like your home or office network) and an untrusted one (like the internet).

A **firewall** performs tasks such as:

- **Blocking unauthorized access** to or from a private network.
- **Monitoring traffic** for suspicious activity.
- **Allowing safe communication** between trusted systems.
- **Preventing malware** and hackers from accessing your system.

A **firewall** should be used in order to:

- To **protect personal or organizational data**.
- To **control employee access** to certain websites.
- To **create secure connections** (especially important for remote work).
- To **comply with regulations** like **GDPR** (General Data Protection Regulation) that is **European Union law** that came into effect on **May 25, 2018**, and it governs how organizations collect, use, store, and protect **personal data** of individuals in the EU.

There are diferent types of **firewall** but, on most personal computers, users install a **Packet-Filtering firewall** that is a software that filters data based on IP addresses, ports, protocols or direction of traffic (inbound or outbound).

A Packet-Filtering firewall works with **rules**. These rules are a set of instructions that tell a packet-filtering firewall what traffic to allow or block based on IP addresses, ports, protocols or direction of traffic.

UFW (Uncomplicated Firewall) It's a **user-friendly** software for **managing** firewall **rules** on **Linux** systems. It makes setting up a firewall **simple** and **quick**, even for beginners.

2- Installing, managing and monitoring UFW

a) Installation: **sudo aptitude install ufw**
b) Enabling UFW: **sudo ufw enable**
c) Disabling UFW: **sudo ufw disable**
d) Monitorig status and default setting of UFW: **sudo ufw status verbose**
e) Disabling and resetting firewall to installation defaults: **sudo ufw reset**

NOTE 1: If you enable UFW, it is started immediately and also, it will be started during the boot process.
NOTE 2: If you disable UFW, it is stopped immediately and also, it will not be started during the boot process.
NOTE 3: By default, all incoming traffic is blocked
NOTE 4: By default, all outgoing traffic is allowed.

3- Basic rules to filter connections to specific ports of your computer

a) Adding a rule to **DENY** traffic to an specific port number of your computer:

sudo ufw deny <Port number>

where **<Port number>** of your computer that is blocked to all incoming connections. For instance:

sudo ufw deny 3306

blocks incoming connections to port number 3306 (typically used by MySQL).

b) Adding rules to **DENY** traffic to an specific port number of your computer to any computer with the exception of one trusted computer with an specific IP address:

sudo ufw allow from <IP address> to any port <Port number>
sudo ufw deny to any port <Port number>

where:

- **<IP address>** is the IP address of a trusted computer
- **<Port number>** is a port number of your computer

For instance:

sudo ufw allow from 192.168.1.100 to any port 3306
sudo ufw deny to any port 3306

allows access computer **192.168.1.100** to port **3306** of your computer.

c) Removing a rule:

- Firt of all, check active rules running: **sudo ufw status numbered**
- Secondly, find the rule number
- Finally, remove the rule: **sudo ufw delete [rule number]** where [rule number] is the number found in the previous step.

4- Basic rules to deny ping to your computer

a) First of all, edit the UFW "before rules" file: **sudo nano /etc/ufw/before.rules**
b) Secondly, find the section **#ok icmp codes** (lines 33 to 43).
c) Thirdly, comment any line related to **icmp**.
d) Fourthly, save **/etc/ufw/before.rules** and exit.
e) Finally, reload UFW:

sudo ufw disable
sudo ufw enable

NOTE 1: If you want to allow pings again you have to undo the previous steps.

6- Documentation about UFW

a) https://www.digitalocean.com/community/tutorials/ufw-essentials-common-firewall-rules-and-commands
b) https://help.ubuntu.com/community/UFW
c) https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu
d) https://snubmonkey.com/how-to-configure-a-firewall-with-ufw/#gsc.tab=0

PRACTICAL EXERCISE

PART 1
1- Install and enable UFW on your virtual machine. Check the UFW status
2- Start service **apache** on your computer. Check the **port** opened by **apache**.
3- Creates a new **index.html** on your virtual computer that displays information about your name and group (asix1 or daw1).
4- Check the IP address of your physical computer.
5- Allow only your physical computer to access **apache service** on your virtual machine. Check:
- Rules of UFW
- That your physical computer can access to apache service and that index.html is displayed.
- Another physical computer can not access apache service and that index.html is not displayed.

PART 2
1- Install and enable UFW on your virtual machine. Check the UFW status
2- Deny pings to your virtual machine. Check from your physical computer that pings requests are not answered by your virtual machine.

PART 3
1- Reset UFW
2- Check that UFW is disabled and it has been reseted to installation defaults.