Lab Assignment 5: Preparation

- For this lab assigment we will need two virtual machines, which we will refer to **MAQUINA1** and **MAQUINA**.
- MAQUINA1 is the machine used in previos lab assigments and MAQUINA2 is a clone of it
- We add to ecah of this machines TWO more NICS. We have tw options
  a. MAQUINA1 and MAQUINA2 are on the same host: we connect the two new NICS to VB internal network
  b. MAQUINA1 and MAQUINA2 are on different host: we coonect the two new NICS in bridge mode to the ethernet adapter of the host, and we link both hosts with an ethernet cable

Lab Assignment 5: Preparation

- the `/etc/network/interfaces` for MAQUINA1 (after the loopback interface)

```
auto enp0s3
iface enp0s3 inet dhcp

auto enp0s8
iface enp0s8 inet static
    address 192.168.2.10/24
iface enp0s8 inet static
    address 192.168.3.10/24
iface enp0s8 inet static
    address 192.168.4.10/24

auto enp0s9
iface enp0s9 inet static
    address 192.168.12.10/24
iface enp0s9 inet static
    address 192.168.13.10/24
iface enp0s9 inet static
    address 192.168.14.10/24
```

Lab Assignment 5: Preparation

- the `/etc/network/interfaces` for MAQUINA2 (after the loopback interface)

```
auto enp0s3
iface enp0s3 inet dhcp

auto enp0s8
iface enp0s8 inet static
    address 192.168.2.15/24
iface enp0s8 inet static
    address 192.168.3.15/24
iface enp0s8 inet static
    address 192.168.4.15/24

auto enp0s9
iface enp0s9 inet static
    address 192.168.12.15/24
iface enp0s9 inet static
    address 192.168.13.15/24
iface enp0s9 inet static
    address 192.168.14.15/24
```

Lab Assigment 5: Summary of configuration

- **MAQUINA1** machine should have this configuration
  - **NIC 1 (enp0s3):** using DHCP (VirtualBox's NAT)
  - **NIC 2 (enp0s8):** ips 192.168.2.10, 192.168.3.10 and 192.168.4.10
  - **NIC 3 (enp0s9):** ips 192.168.12.10, 192.168.13.10 and 192.168.14.10
- **MAQUINA2** machine should have this configuration
  - **NIC 1 (enp0s3):** using DHCP (VirtualBox's NAT)
  - **NIC 2 (enp0s8):** ips 192.168.2.15, 192.168.3.15 and 192.168.4.15
  - **NIC 3 (enp0s9):** ips 192.168.12.15, 192.168.13.15 and 192.168.14.15

Lab Assigment 5: Summary of configuration

- To perform the lab assigment **MAQUINA1** and **MAQUINA2** should be both running at the same time
- NIC2 and NIC3 of both machines must be connected to the same VirtuaBox internal network.
- `Machine->Settings->Network->Adapter2->Advanced` and `Machine->Settings->Network->Adapter3->Advanced` must have both **'Cable Connected'** checked
- As **MAQUINA1** and **MAQUINA2** are preconfigured to use 1.5Gb RAM memory each, it's possible that, depending on the available RAM, your host machine cannot cope with both of them running simultaneously. Should that be the case, reconfigure them to use 1Gb or less.
- it's also possible to have **MAQUINA1** and **MAQUINA2** running on different host machines, in that case both host machines should be linked by an ethernet cable and **MAQUINA1** and **MAQUINA2**

Lab Assigment 5: Access Control at application level

1. enable ftp services running **MAQUINA1** by executing `/usr/sbin/ftp -D`
2. check ftp and ssh connections from **MAQUINA2** to **MAQUINA1**, using all the six addresses of local networks
3. configure *tcpwrappers* (files `/etc/hosts.allow` `/etc/hosts.deny`) on **MAQUINA1** to
   - accept all ftp conections except networks 192.168.2. 192.168.3. and 192.168.4.
   - reject all ssh connections for network 192.168.12. and 192.168.13. and 192.168.14.
4. check ftp and ssh connections from **MAQUINA2** to **MAQUINA1**, using all the six local networks

Lab Assigment 5: Access Control at application level

5. In **MAQUINA1** enable telnet services with the following line added to `/etc/inetd.conf`

   ```
   telnet     stream  tcp nowait root /usr/sbin/tcpd     telnetd
   ```

6. restart inetd (`/etc/init.d/inetutils-inetd restart`, `systemctl restart inetutils-inetd.service`, `kill -HUP pid_de_inetd`)
7. check telnet connections from **MAQUINA2** to **MAQUINA1**, using all the six local networks
8. configure *tcpwrappers* to reject all telnet connections for network 192.168.12. and 192.168.13. and 192.168.14.

Lab Assigment 5: Access Control at application level

9. check telnet connections from **MAQUINA2** to **MAQUINA1**, using all the six local networks
10. substitute the previous line in `/etc/inetd.conf` with the next line and restart inetd

```
telnet     stream  tcp nowait root /usr/sbin/telnetd     telnetd
```

11. check telnet connections from **MAQUINA2** to **MAQUINA1**, using all the six local networks
12. look at the libraries used by sshd, ftpd, inetd, tcpd and telnetd.

Lab Assignment 5: Access Control at packet level

13. (on **MAQUINA1**) for the ftp protocol (port 21): use nftables to establish the action DROP for connections in networks 192.168.2.* and 192.168.3.* and REJECT for networks 192.168.12.* y 192.168.13.*
14. (on **MAQUINA1**) for the ssh protocol (port 22): use nftables to establish the action DROP for connections in networks 192.168.12.* and 192.168.13.* and REJECT for networks 192.168.2.* y 192.168.3.*
15. check ftp and ssh connections from **MAQUINA2** to **MAQUINA1**, using all the six local networks.
16. log the rejected connections and see if they appear on `/var/log/messages` and in `/var/log/kern.log`

Lab Assignment 5: NAT ad double step authentication

17. Configure the container in **MAQUINA1** done on the previous lab assignment to have a static ip
18. Arrange for connections on the web port reaching the host machine to be redirected to the container
19. Arrange for connections on the ssh port in the NIC2 of the machine to be redirected to the container
20. Check that accesing the machine **MAQUINA1** from **MAQUINA2**, acesses, in fact, the container

Lab Assignment 5: Work submission

- After performing the corresponding tasks of the lab assigment, a pdf document, describing what has been done (including screenshots showing the behaviour of the virtual machine, changes made to configuraton files, output from commands...) should be sent to
  - `antonio.yanez@udc.es`. (students at udc)
  - `yolanda@det.uvigo.es`. (students at uvigo)
- The subject of the mail should be *FSO: practica-5*
- The attachement should be named with the lab assignment number and the surname and name of the student, in the form P5-Surname-Name.pdf, avoiding non-ascii characteres (á, é, ñ ...)
  - Example: work submitted by student *Donald Trump Núñez* should come as an attached file named `P5-TrumpNunez-Donald.pdf`
- In the case the lab assigment is made by two students, submit only one copy (named after ONE of the students) and state BOTH names in the pdf document