Lab Assignment 5: Preparation

- For this lab assigment we will need two virtual machines, which we will refer to **fso2024** and **klone**. Please download the machine KLONE and import it in virtualbox
- Make sure that NICS 2 and 3 of both machines are connected to the same internal network of VirtualBox.
- Alternatively FSO2024 and KLONE can be in different PC's. In this case NICs 2 and 3 showld in virtualbox should be configured as bridged adapters connected to the host ethernet, and both PC's linked with an ethernet cable
- We will try connections which will be originated in **klone** and have their destinations to **fso2024**

Lab Assignment 5: Preparation

- If you don't want/cannot download the KLONE machine, you can create your own by
  - CLONE the virtual machine and rename it **klone** . (Or you can reimport the ova file and name it **klone**
  - change `/etc/hostname` file in the clone machine to reflect the new name.
  - change the `/etc/network/interface` file in the clone machine to reflect the new ip addresses (in next slide)
  - Install the ftp client in **klone** (*apt-get install ftp*)
  - when importing it in Virtualbox. Make sure network adapters 2 and 3 are connected to the same internal networks as the machine we used in previous lab assignments

Lab Assigment 5: Summary of configuration

- **fso2024** machine should have this configuration
  - **NIC 1 (enp0s3):** using DHCP (VirtualBox's NAT)
  - **NIC 2 (enp0s8):** ips 192.168.10.101, 192.168.11.101 and 192.168.12.101
  - **NIC 3 (enp0s9):** ips 192.168.20.101, 192.168.21.101 and 192.168.22.101
- **klone** machine should have this configuration
  - **NIC 1 (enp0s3):** using DHCP (VirtualBox's NAT)
  - **NIC 2 (enp0s8):** ips 192.168.10.102, 192.168.11.102 and 192.168.12.102
  - **NIC 3 (enp0s9):** ips 192.168.20.102, 192.168.21.102 and 192.168.22.102

Lab Assigment 5: Summary of configuration

- To perform the lab assigment **fso24** and **klone** 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 **fso24** and **klone** 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 **fso24** and **klone** running on different host machines, in that case both host machines should be linked by an ethernet cable and **fso24** and **klone** machine's NIC 2 and 3 should be connected in bridge mode to the ethernet interface of the host machine

Lab Assigment 5: Access Control at application level

1. check ftp and ssh connections from **klone** to **fso24**, using all the six addresses of local networks
2. enable ftp services running from inetd in **fso24** by adding the following line to `/etc/inetd.conf` and restarting inetd

   ```
   ftp     stream  tcp nowait root /usr/sbin/ftpd    ftpd
   ```

3. check ftp ssh connections from **klone** to **fso24**, using all the six addresses of local networks
4. configure *tcpwrappers* (files `/etc/hosts.allow` `/etc/hosts.deny`) on **fso24** to
   - accept all ftp conections except networks 192.168.20. 192.168.21.* and 192.168.22.*
   - reject all ssh connections for network 192.168.10. and 192.168.11. and 192.168.12.
5. check ftp and ssh connections from **klone** to **fso24**, using all the six local networks

Lab Assigment 5: Access Control at application level

6. In **fso24** substitute the line previously added to `/etc/inetd.conf` (without modifying nor `/etc/hosts.allow` neither `/etc/hosts.deny`) with

   ```
   ftp     stream  tcp nowait root /usr/sbin/tcpd     ftpd
   ```

7. restart inetd (`/etc/init.d/openbsd-inetd restart`, `systemctl restart openbsd-inetd.service`, `kill -HUP pid_de_inetd`)
8. check ftp and ssh connections from **klone** to **fso24**, using all the six local networks

Lab Assignment 5: Access Control at packet level

9. (on **fso24**) for the ftp protocol (port 21): use nftables to establish the action DROP for connections in networks 192.168.10.* and 192.168.20.* and REJECT for networks 192.168.11.* y 192.168.21.*
10. (on **fso24**) for the ssh protocol (port 22): use nftables to establish the action DROP for connections in networks 192.168.10.* and 192.168.20.* and REJECT for networks 192.168.11.* y 192.168.21.*
11. check ftp and ssh connections from **klone** to **fso24**, using all the six local networks.
12. 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

13. Configure the container in **fso24** done on the previous lab assignment to have a static ip
14. Arrange for connections on the 222 and web ports reaching the host machine to be redirected to the container (remember the container ssh port is 222)
15. Check that accesing the machine **fso24** from **klone**, in fact, the container (for both 222 and web)
16. Configure ths ssh server at **fso** to use double authentification (using google authenticator) for user000, user001 and user002

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 t`
- 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