# Lab Assignment 6: Preparation



1. Keep the network configuration of the machines of **MAQUINA1** and **MAQUINA2** from the previous lab assignment.
2. **MAQUINA1** has a container which is running ssh in port 222. Port 222 at local ips of **MAQUINA1** is redirected to the container

```
#!/usr/sbin/nft -f
#en esta maquina la direccion del container es 10.0.3.200
table ip nat {
  chain PREROUTING {
     type nat hook prerouting priority dstnat; policy accept;
     ip daddr {192.168.2.10, 192.168.3.10, 192.168.4.10} tcp dport {222} log
     ip daddr {192.168.12.10, 192.168.13.10, 192.168.14.10} tcp dport {222} log
     ip daddr {192.168.2.10, 192.168.3.10, 192.168.4.10} tcp dport {222} dnat to 10.0.3.200
     ip daddr {192.168.12.10, 192.168.13.10, 192.168.14.10} tcp dport {222} dnat to 10.0.3.200
  }
}
```

3. Install syslogd in the container (`apt-get install inetutils-syslogd`)
4. Create user *hideous* in the container (`useradd -m hideous`)

# Lab Assignment 6: Preparation



1. Create rsa keys for user001 user002 and user003 in **MAQUINA2**. user003 should protect his/her with a passphrase.
2. Enable user001, user002 and user003 to login into **MAQUINA1** (port 22) from **MAQUINA2** without being asked for a password, although user003 might have to supply the key's passphrase.

# Lab Assignment 6



3. Arrange for user001, user002 and user003 in **MAQUINA2** to log directly into the container of **MAQUINA1** (port 222, using **MAQUINA1** ips) as user *hideous* without being asked for a password.
4. Arrange for the authentication logs of machine **MAQUINA2** to be sent to machine **MAQUINA1** and to file `/dev/tty3` in **MAQUINA2**. Check that it works.

NOTE: machine receiving logs has to invoke syslog with the `-r` or `--inet` option, machine sending the logs cannot have syslogd invoked with `--no-forward`. Check `/etc/default/` and syslogd man page.

# Lab Assignment 6



5 Arrange for the authentication logs on machine **MAQUINA2** to be sent ALSO to the container in **MAQUINA1**. Use these three different solutions:
   a) **MAQUINA1** sends its authentication logs to the container (with @ip_of_container)
   b) machine **MAQUINA1** writes its authentication logs to a file in the container
   c) all traffic from one of **MAQUINA1** IPs is redirected to the container (using nftables)

6 Execute *lynis* program audit **MAQUINA1** and use its output to harden the ssh server. Allow only user001, user002, user003, user004, user005 and user006 to login.