Laborator 08

Cuprins:

```
root@host:~# update_lab --force
root@host:~# start_lab lab-nat
```

Task 01 | Configurare translatare de adrese (**MASQUERADE**)

Doar ruleaza comenzile 😃.

```
# Cel mai important
root@host:~# iptables -t nat -A POSTROUTING -j MASQUERADE

# Verificare
root@host:~# iptables -t nat -L POSTROUTING -n -v
```

Task 02 | Format de pachete la translatare (`tcpdump`)

```
root@host:~# tcpdump -n -i eth0 ip dst host 8.8.8.8
root@host:~# tcpdump -n -i veth-red ip dst host 8.8.8.8
root@host:~# tcpdump -n -i any ip dst host 8.8.8.8

root@host:~# # Cu pachete de reply
root@host:~# tcpdump -n -i any ip src host 8.8.8.8

root@host:~# # fara Domain Name Server
root@host:~# tcpdump -i any ip dst host 8.8.8.8
```

Task 03 | Format de pachete TCP la translatare (`tcpdump`)

```
# Daca pun cs.pub.ro in loc de IP cu nr., imi zice unkown host
root@host:~# tcpdump -i any dst 141.85.241.57 and dst port 80
root@host:~# tcpdump -i any dst 141.85.241.57 and tcp dst port 80
root@host:~# tcpdump -n -i any dst 141.85.241.57 and tcp dst port 80
```

> tcdump sheet: https://cdn.comparitech.com/wp-content/uploads/2019/06/tcpdump-cheat-sheet-1.pdf.

```
root@red:student$ wget cs.pub.ro
```

```
root@host:~# tcpdump -n -i any 141.85.241.57 and tcp port 80
```

```
root@red:student$ wget cs.pub.ro
```

Task 04 | Configurare incorecta a translatarii

A nu se rula pe host:

```
root@host:~# # NUUU
root@host:~# tcpdump -n -i any
```

Ori rulam cate `tcpdump` pt cate o interfata pe rand, ori asa:

```
root@host:~# tcpdump -n -i veth-blue & tcpdump -n -i veth-green & tcpdump -n -i veth-red & wait
```

La final

```
root@host:~# pkill tcpdump
```

Task 05 | Port Forwarding

```
ssh -l student 10.9.4.221 -p 10022
```

```
root@host:~# # Sterge regula veche
root@host:~# iptables -t nat -D PREROUTING -p tcp --dport 10022 -j DNAT --to-destination 192.168.1.2:22

root@host:~# # Regula noua, pt limitare port-forwarding
root@host:~# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 10022 -j DNAT --to-destination 192.168.1.2:22

root@host:~# iptables -t nat -L PREROUTING -n -v
```

```
ssh -l student 10.9.4.221 -p 10022
```

Task 06 | Extindere port forwarding

```
student@host:~$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc fq_codel state UP group default qlen 1000
    link/ether fa:16:3e:da:0d:4a brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    altname ens3
    inet 10.9.4.221/16 brd 10.9.255.255 scope global dynamic eth0
       valid_lft 80832sec preferred_lft 80832sec
    inet6 fe80::f816:3eff:feda:d4a/64 scope link
       valid_lft forever preferred_lft forever

student@host:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc fq_codel state UP group default qlen 1000
    link/ether fa:16:3e:da:0d:4a brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    altname ens3
    inet 10.9.4.221/16 brd 10.9.255.255 scope global dynamic eth0
       valid_lft 80741sec preferred_lft 80741sec
    inet6 fe80::f816:3eff:feda:d4a/64 scope link
       valid_lft forever preferred_lft forever
17: veth-red@if16: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc noqueue state UP group default qlen 1000
    link/ether 56:74:a3:ff:aa:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.1.1/24 scope global veth-red
       valid_lft forever preferred_lft forever
19: veth-green@if18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc
```

```
noqueue state UP group default qlen 1000
    link/ether d6:db:ad:3d:92:b5 brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet 192.168.2.1/24 scope global veth-green
       valid_lft forever preferred_lft forever
21: veth-blue@if20: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc noqueue state UP group default qlen 1000
    link/ether 26:ab:66:e7:78:4f brd ff:ff:ff:ff:ff:ff link-netnsid 2
    inet 192.168.3.1/24 scope global veth-blue
       valid_lft forever preferred_lft forever
```

```
student@green:~$ ip addr show green-eth0
18: green-eth0@if19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc noqueue state UP group default qlen 1000
    link/ether d6:5e:96:07:5f:8a brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.2.2/24 scope global green-eth0
       valid_lft forever preferred_lft forever
```

```
student@red:~$ ip addr show red-eth0
16: red-eth0@if17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc noqueue state UP group default qlen 1000
    link/ether ca:dc:78:7e:1d:6e brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.1.2/24 scope global red-eth0
       valid_lft forever preferred_lft forever
```

```
student@blue:~$ ip addr show blue-eth0
20: blue-eth0@if21: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc noqueue state UP group default qlen 1000
    link/ether 9a:7b:cf:3a:63:0a brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.3.2/24 scope global blue-eth0
       valid_lft forever preferred_lft forever
```

```
root@host:~# # Regula noua, pt limitare port-forwarding
root@host:~# # iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 10022 -j DNAT --to-destination 192.168.1.2:22


# Port forwarding: portul 22 al lui green (192.168.2.2) este mapat la portul 20022 al host-ului
root@host:~# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 20022 -j DNAT --to-destination 192.168.2.2:22
```

```
# Port forwarding: portul 22 al lui blue (192.168.3.2) este mapat la portul
30022 al host-ului
root@host:~#  iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 30022 -j
DNAT --to-destination 192.168.3.2:22


# Packetele de raspuns sunt si rutate
root@host:~# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# Verificare
root@host:~# iptables -t nat -L -v -n
```

```
root@host:/home/student# iptables -t nat -L -v -n
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    3   180 DNAT       tcp  --  eth0   *       0.0.0.0/0
0.0.0.0/0            tcp dpt:10022 to:192.168.1.2:22
    0     0 DNAT       tcp  --  eth0   *       0.0.0.0/0
0.0.0.0/0            tcp dpt:20022 to:192.168.2.2:22
    0     0 DNAT       tcp  --  eth0   *       0.0.0.0/0
0.0.0.0/0            tcp dpt:30022 to:192.168.3.2:22

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
   17  1275 MASQUERADE  all  --  *      eth0    0.0.0.0/0
0.0.0.0/0
    0     0 MASQUERADE  all  --  *      eth0    0.0.0.0/0
0.0.0.0/0

Chain DOCKER (0 references)
 pkts bytes target     prot opt in     out     source
destination
```

```
moodle_username@fep8.grid.pub.ro$  # Conectare red
moodle-username@fep8.grid.pub.ro$ ssh -l student 10.9.4.221 -p 10022
```

```
moodle-username@fep8.grid.pub.ro$  # Conectare green
moodle-username@fep8.grid.pub.ro$ ssh -l student 10.9.4.221 -p 20022


moodle-username@fep8.grid.pub.ro$  # Conectare blue
moodle-username@fep8.grid.pub.ro$ ssh -l student 10.9.4.221 -p 30022
```

> Difera doar numarul portului.

Task 07 | Format de pachete la port forwarding (`tcpdump`)

```
eu@localhost$  # Asa ma contectez
eu@localhost$  ssh -J moodle-username@fep.grid.pub.ro student@10.9.4.221
```

```
eu@localhost$  # Asa copiez un fisier
eu@localhost$ scp -J moodle-username@fep.grid.pub.ro
student@10.9.4.221:/home/student/portfwd_eth0_output.pcap ~/Downloads/lab8-
ex7-1.pcap
eu@localhost$ wireshark ~/Downloads/lab8-ex7-1.pcap &
```

```
eu@localhost$ scp -J moodle-username@fep.grid.pub.ro
student@10.9.4.221:/home/student/portfwd_veth-red_output.pcap
~/Downloads/lab8-ex7-2.pcap
eu@localhost$ wireshark ~/Downloads/lab8-ex7-2.pcap &
```

> Observ ca dupa portforwarding, wireshark-ul nu imi spune packetele TCP in plan. Vad cv cu Diffie-Hellman, SSH.
>
> La prima captura, destinatia este cea din adresa privata 10.9.x.x (netranslatata)

Task 08 | Port forwarding pentru `telnet`

```
# Port forward: port-ul 23 al lui green (192.168.1.2) este mapat la portul
10023 de pe host
root@host:~# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 10023 -j
DNAT --to-destination 192.168.1.2:23

# Port forward: port-ul 23 al lui green (192.168.2.2) este mapat la portul
20023 de pe host
root@host:~# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 20023 -j
DNAT --to-destination 192.168.2.2:23

# Port forward: port-ul 23 al lui green (192.168.3.2) este mapat la portul
30023 de pe host
```

```
root@host:~# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 30023 -j
DNAT --to-destination 192.168.3.2:23

# Verificare
root@host:~# iptables -t nat -L -v -n
```

```
root@host:~# sysctl -w net.ipv4.ip_forward=1
```

```
moodle-username@fep8.grid.pub.ro$ # Conectare la red
moodle-username@fep8.grid.pub.ro$ telnet 10.9.4.221 10023

moodle-username@fep8.grid.pub.ro$ # Conectare la green
moodle-username@fep8.grid.pub.ro$ telnet 10.9.4.221 20023

moodle-username@fep8.grid.pub.ro$ # Conectare la blue
moodle-username@fep8.grid.pub.ro$ telnet 10.9.4.221 30023
```

Task 09 | Configurare persistenta rutare si NAT

```
eu@localhost$ ssh -J moodle-username@fep.grid.pub.ro student@10.9.4.221
```

```
root@host:/home# update_lab --force
root@host:/home# start_lab lab-nat


# Recapitulare reguli iptables

# Port forwarding (SSH): portul 22 al lui red (192.168.1.2) este mapat la
portul 10022 al host-ului
root@host:~# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 10022 -j
DNAT --to-destination 192.168.1.2:22


# Port forwarding (SSH): portul 22 al lui green (192.168.2.2) este mapat la
portul 20022 al host-ului
root@host:~# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 20022 -j
DNAT --to-destination 192.168.2.2:22

# Port forwarding (SSH): portul 22 al lui blue (192.168.3.2) este mapat la
portul 30022 al host-ului
root@host:~#  iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 30022 -j
DNAT --to-destination 192.168.3.2:22
```

```
# Packetele de raspuns sunt si rutate
root@host:~# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE


# Port forward (telnet): port-ul 23 al lui green (192.168.1.2) este mapat
la portul 10023 de pe host
root@host:~# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 10023 -j
DNAT --to-destination 192.168.1.2:23

# Port forward (telnet): port-ul 23 al lui green (192.168.2.2) este mapat
la portul 20023 de pe host
root@host:~# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 20023 -j
DNAT --to-destination 192.168.2.2:23

# Port forward (telnet): port-ul 23 al lui green (192.168.3.2) este mapat
la portul 30023 de pe host
root@host:~# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 30023 -j
DNAT --to-destination 192.168.3.2:23

# Verificare
root@host:~# iptables -t nat -L -v -n
```

```
root@host:~# sysctl -w net.ipv4.ip_forward=1
```

```
root@host:/home/student# iptables-save > /etc/iptables-rules
# Warning: iptables-legacy tables present, use iptables-legacy-save to see
them
root@host:/home/student# iptables-legacy-save > /etc/iptables-rules
```

```
root@host:~# cat /etc/network/interfaces
[...]
# The primary network interface
auto eth0
iface eth0 inet dhcp
        up iptables-restore < /etc/iptables-rules
```

Task 10 | Tunel SSH invers

Am incercat sa deschid inca un VM sa ma conectez la el, dar nu a mers 😦

Task 11 (Bonus) | Translatare selectiva de adrese

```
root@host:/home/student# ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc fq_codel state UP
```

```
group default qlen 1000
    link/ether fa:16:3e:2d:19:c2 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    altname ens3
    inet 10.9.0.205/16 brd 10.9.255.255 scope global dynamic eth0
       valid_lft 84495sec preferred_lft 84495sec
    inet6 fe80::f816:3eff:fe2d:19c2/64 scope link
       valid_lft forever preferred_lft forever
```

> REMINDER: `10.9.0.205/16` este IP-ul catre exteriorul retelei

```
# Stergerea regulii MASQUERADE
root@host:~# iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE

# Adaug regula SNAT pentru red (192.168.1.2) cu porturi intre 45000 si 50000
root@host:~# iptables -t nat -A POSTROUTING -o eth0 -s 192.168.1.2 -p tcp --sport 45000:50000 -j SNAT --to-source 10.9.0.205:45000-50000

# Adaug regula SNAT pentru green (192.168.2.2) cu porturi intre 50000 si 55000
root@host:~# iptables -t nat -A POSTROUTING -o eth0 -s 192.168.2.2 -p tcp --sport 50000:55000 -j SNAT --to-source 10.9.0.205:50000-55000

# Adaug regula SNAT pentru blue (192.168.3.2) cu porturi intre 55000 si 60000
root@host:~# iptables -t nat -A POSTROUTING -o eth0 -s 192.168.3.2 -p tcp --sport 55000:60000 -j SNAT --to-source 10.9.0.205:55000-60000

# Adaug regula SNAT pentru toate celelalte conexiuni care vor folosi IP-ul extern al host-ului
root@host:~# iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 10.9.0.205

# Verificare
root@host:~# iptables -t nat -L -v -n
```

Testarea conexiunilor HTTP

```
# first thing first
root@host:~# tcpdump -i eth0 'tcp port 80'

# Verificare red
root@red:~# wget http://cs.pub.ro

# Verificare green
root@green:~# wget http://cs.pub.ro
```

```
# Verificare blue
root@blue:~# wget http://cs.pub.ro
```