

Olaru Gabriel Iulian  
334CC  
Lab 08 ReLe

EX 1-3: aratat la lab

Ex4: Diferente de timpi de transfer intre diverse protocoale

```
gabriel.olaru@fep7-1:~  
File Edit View Search Terminal Help  
student@host:~$ nc -l 12345 > file-100M-nc.dat  
student@host:~$  
  
gabriel.olaru@fep7-1:~  
File Edit View Search Terminal Help  
student@green:~$ time cat file-100M.dat | nc -q0 host 12345  
real    0m0.567s  
user    0m0.009s  
sys     0m0.241s  
student@green:~$ ls  
file-100M.dat  
student@green:~$ time curl -T file-100M.dat -u student:student ftp://red/file-100M-ftp.dat  
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current  
             Dload  Upload  Total   Spent    Left   Speed  
100 100M    0     0 100 100M      0   245M --:--:-- --:--:-- --:--:-- 245M  
real    0m2.118s  
user    0m0.017s  
sys     0m0.105s  
student@green:~$ time scp file-100M.dat student@host:file-100M-scp.dat  
student@host's password:  
file-100M.dat                                     100% 100MB 58.2MB/s  00:01  
real    0m5.664s  
user    0m0.630s  
sys     0m0.187s  
student@green:~$
```

### Ex5: Pacote plain sight (ftp) vs criptate (ssh)

```

07:20:57.338805 IP (tos 0x10, ttl 63, id 64140, offset 0, flags [DF], proto TCP (6), length 66)
    red.33592> green.ftp: Flags [P], cksum 0x8489 (incorrect -> 0x17b0), seq 115, ack 21, win 83, options [nop,nop,TS val 2933637857 ecr 1873511963], length 14: FTP, length: 14
    USER student
07:20:57.338919 IP (tos 0x0, ttl 63, id 13417, offset 0, flags [DF], proto TCP (6), length 52)
    green.ftp> red.33592: Flags [.], cksum 0x847b (incorrect -> 0x1241), seq 21, ack 15, win 85, options [nop,nop,TS val 1873512727 ecr 2933637857], length 0
07:20:57.339436 IP (tos 0x0, ttl 63, id 13418, offset 0, flags [DF], proto TCP (6), length 80)
    red.33592> green.ftp: Flags [P], cksum 0x849d (incorrect -> 0xcacfa), seq 21:55, ack 15, win 85, options [nop,nop,TS val 1873512728 ecr 2933637857], length 34: FTP, length: 34
    331 Please specify the password
07:20:57.339453 IP (tos 0x10, ttl 63, id 64141, offset 0, flags [DF], proto TCP (6), length 52)
    red.33592> green.ftp: Flags [I], cksum 0x8476 (incorrect -> 0x121f), seq 15, ack 55, win 83, options [nop,nop,TS val 2933637858 ecr 1873512728], length 0
07:21:00.000018 IP (tos 0x10, ttl 63, id 64142, offset 0, flags [DF], proto TCP (6), length 66)
    red.33592> green.ftp: Flags [P], cksum 0x8489 (incorrect -> 0xd6d55), seq 15:29, ack 55, win 83, options [nop,nop,TS val 2933646100 ecr 1873512728], length 14: FTP, length: 14
    PASS student

```

```
07:23:12.801432 IP (tos 0x10, ttl 63, id 14666, offset 0, flags [DF], proto TCP (6), length 52)
    red.53884 > green.ssh: Flags [.], cksum 0x847b (incorrect -> 0x3eb1), seq 3406, ack 4310, win 83, options [nop,nop,TS val 2933772521 ecr 1873652741], length 0
07:23:12.802297 IP (tos 0x10, ttl 64, id 51422, offset 0, flags [DF], proto TCP (6), length 96)
    green.ssh > red.53884: Flags [P.], cksum 0x84a7 (incorrect -> 0xa7b2), seq 4310:4354, ack 3406, win 83, options [nop,nop,TS val 1873652742 ecr 2933772521], length 44
07:23:12.802316 IP (tos 0x10, ttl 63, id 15467, offset 0, flags [DF], proto TCP (6), length 52)
    red.53884 > green.ssh: Flags [.], cksum 0x847b (incorrect -> 0x3eb3), seq 3406, ack 4354, win 83, options [nop,nop,TS val 2933772522 ecr 1873652742], length 0
```

## Ex6: Blocare porturi pentru diverse protocoale

```
gabriel.olaru@tep71-1
File Edit View Search Terminal Help

target  prot opt source      destination
REJECT  tcp  -- anywhere          tcp dpt:telnet reject-with icmp-port-unreachable
green
root@host:/home/student# iptables -L FORWARD -v
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 REJECT tcp -- * * 0.0.0/0 192.168.2.2
rt-unreachable
root@host:/home/student# iptables -L FORWARD -v -n
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 REJECT tcp -- * * 0.0.0/0 192.168.2.2
rt-unreachable
root@host:/home/student# iptables -L FORWARD -v -n
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
2 120 REJECT tcp -- * * 0.0.0/0 192.168.2.2
rt-unreachable
root@host:/home/student# iptables -L FORWARD -v -n
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
4 240 REJECT tcp -- * * 0.0.0/0 192.168.2.2
rt-unreachable
root@host:/home/student# iptables -L FORWARD -v -n
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
6 360 REJECT tcp -- * * 0.0.0/0 192.168.2.2
rt-unreachable
root@host:/home/student#
```

```
gabriel.olaru@tep71-1
File Edit View Search Terminal Help

root@host:/home/student# telnet green
Trying 192.168.2.2...
telnet: Unable to connect to remote host: Connection refused
root@host:/home/student# telnet green
Connected to green.
220 (vsFTPd 3.0.3)
Name (green:student): student
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> quit
221 Goodbye.
root@host:/home/student# ssh -l student green
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Dec 11 07:23:06 2020 from 192.168.1.2
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

The image displays two terminal windows side-by-side. The left window, titled 'gabriel.lolaru@fep7-1:~', shows the configuration of iptables rules. The user sets a default policy of 'REJECT' for the 'FORWARD' chain and creates a rule to allow traffic from 192.168.2.2 to port 21. The right window, also titled 'gabriel.lolaru@fep7-1:~', shows the output of the 'netstat -tlnp' command, which lists the listening ports and the processes associated with them. The output shows 'tcp 0 0 0.0.0.0:21 0.0.0.0:\* LISTEN' for 'sshd' and 'tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN' for 'sshd'. The 'sshd' process is also shown as the owner of the 'sshd' process.

```
gabriel.lolaru@fep7-1:~  
root@host:/home/student# iptables -A FORWARD -d green -p tcp --dport telnet -j REJECT  
root@host:/home/student# iptables -A FORWARD -d green -p tcp --dport 21 -j REJECT  
root@host:/home/student# iptables -L FORWARD -v -n  
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination  
6 360 REJECT tcp -- * * 0.0.0.0/0 192.168.2.2 tcp dpt:23 reject-with icmp-po  
rt-unreachable  
0 0 REJECT tcp -- * * 0.0.0.0/0 192.168.2.2 tcp dpt:23 reject-with icmp-po  
rt-unreachable  
0 0 REJECT tcp -- * * 0.0.0.0/0 192.168.2.2 tcp dpt:21 reject-with icmp-po  
rt-unreachable  
root@host:/home/student#
```

```
gabriel.lolaru@fep7-1:~  
File Edit View Search Terminal Help  
tcp green  
ftp: connect: Connection refused  
ftp>
```

## Ex7: bloccare port ssh

```
gabriel.lolaru@fep7-1:~$ sudo iptables -L FORWARD -v -n
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
6 360 REJECT tcp -- * * 0.0.0.0/0 192.168.2.2 tcp dpt:23 reject-with icmp-po
rt-unreachable
0 0 REJECT tcp -- * * 0.0.0.0/0 192.168.2.2 tcp dpt:23 reject-with icmp-po
rt-unreachable
3 180 REJECT tcp -- * * 0.0.0.0/0 192.168.2.2 tcp dpt:21 reject-with icmp-po
rt-unreachable
0 0 REJECT tcp -- * * 0.0.0.0/0 192.168.2.2 tcp dpt:22 reject-with icmp-po
rt-unreachable
root@host:/home/student#
```

```
gabriel.lolaru@fep7-1:~$ ssh -l student green
ssh: connect to host green port 22: Connection refused
student@green:~$
```

## Ex8: permettere traffic ssh

```
gabriel.lolaru@fep7-1:~$ sudo iptables -A FORWARD -d green -p tcp --dport 22 -j ACCEPT
root@host:/home/student# iptables -D FORWARD -d green -p tcp --dport 22 -j ACCEPT
root@host:/home/student# iptables -I FORWARD -d green -p tcp --dport 22 -j ACCEPT
root@host:/home/student#
```

```
gabriel.lolaru@fep7-1:~$ ssh -l student green
ssh: connect to host green port 22: Connection refused
student@green:~$ ssh -l student green
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Dec 11 07:37:47 2020 from 192.168.1.2
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

student@green:~$ exit
logout
Connection to green closed.
student@fep7:~$
```

## Ex9: flush

```
gabriel.lolaru@fep7-1:~$ sudo su
student@host:~$ sudo su
root@host:/home/student# iptables -F
root@host:/home/student# iptables -L FORWARD -v -n
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
root@host:/home/student#
```

```
gabriel.lolaru@fep7-1:~$ ssh -l student green
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Dec 11 07:46:02 2020 from 192.168.1.2
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

student@green:~$ exit
logout
Connection to green closed.
Connected to green.
220 (vsFTPd 3.0.3)
Name (green:student): student
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> quit
221 Goodbye.
```

## Ex 10: trimitere rezultat telnet catre masina locala si deschidere cu wiresark

