Laborator 07

Cuprins:

```
student@host:~# update_lab --force
student@host:~# start_lab lab-iptables
```

Task 01 | Conectare SSH folosind cheie publica

> Tot ce a trebuit sa fac a fost sa rulez comenzile (copy paste direct).

```
student@red:~$ ssh student@host
student@red:~$ ssh -l student host   # La fel ca mai sus
student@red:~$ cat ~/.ssh/id_rsa.pub
student@red:~$ ssh -l student host "cat ~/.ssh/authorized_keys"
```

Task 02 | Generare cheie publica si autentificare

```
corina@blue:~$ # Va genera automat, fara sa mai puna intrebari (in stdin)
corina@blue:~$ ssh-keygen -t rsa -f ~/.ssh/id_rsa -N ""
```

```
Generating public/private rsa key pair.
Created directory '/home/corina/.ssh'.
Your identification has been saved in /home/corina/.ssh/id_rsa
Your public key has been saved in /home/corina/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Q5NgDifhHuRowGD9+Lgm8l/ZqeLfne3BLB+5BeZd84A corina@blue
The key's randomart image is:
+---[RSA 3072]----+
|=.. =.+          |
|.o * * . .       |
|  o * . +        |
| . o o . .   .   |
|    +   S   E ...|
|   . . o o = + oo|
|    . o o . B o .|
|.. o.. o . = =   |
|..+oooo . o.=    |
+----[SHA256]-----+
```

```
corina@blue:~$ cat ~/.ssh/id_rsa.pub   # O copiez in student@host:~/.ssh/authorized_keys
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC/WCRqCRamkGgX+cYds/LtxkapEFHGUYKYiafed9C6wMoAIeIvACwD9+JEkPaU96inoVxWPLAgkUjtXG6QHQ8KafXCp/YnvedqBDAwZd1jfCuU4fIEOA7NXB2+xL2x2YAyA1JBm25ELEOrs+cra40R2JgSwd6/xOOLdbpIV5CsRdVJEIvum3H9FbzdXoX6oeza1GbCUxemRtvmEDTHCovfNZAuhQiff+lGaYlveMPrWvIy9qZexjsee/lIYbDKsCA9ZfgE6RInOVuOJu0w/F+TMAivzmUOyTc+2ACBtaHU2LgducM6AB+kUHbSerzf5Oz0yGSWMgfVSiJmZT0q9n/jGS9w0IvVUcgWM5oxwusmYkCY6t1HYHU0zDM/ZHTsD1fAWvnI6wkbcQVpWtGBhQTEyQ80hJedW66gJN1uPjx9b5whOjorTrXQZZqCGXPRh3sMCabQy8AA2HGCxDxfLxPVeku5HX+/YQoTRT16vPYYRJtmhVfRZIydrHrDk/Cxyp0= corina@blue
```

```
student@host:~$ nano -l ~/.ssh/authorized_keys
student@host:~$ grep --color=ALWAYS 'corina@blue' ~/.ssh/authorized_keys
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC/WCRqCRamkGgX+cYds/LtxkapEFHGUYKYiafed9C6wMoAIeIvACwD9+JEkPaU96inoVxWPLAgkUjtXG6QHQ8KafXCp/YnvedqBDAwZd1jfCuU4fIEOA7NXB2+xL2x2YAyA1JBm25ELEOrs+cra40R2JgSwd6/xOOLdbpIV5CsRdVJEIvum3H9FbzdXoX6oeza1GbCUxemRtvmEDTHCovfNZAuhQiff+lGaYlveMPrWvIy9qZexjsee/lIYbDKsCA9ZfgE6RInOVuOJu0w/F+TMAivzmUOyTc+2ACBtaHU2LgducM6AB+kUHbSerzf5Oz0yGSWMgfVSiJmZT0q9n/jGS9w0IvVUcgWM5oxwusmYkCY6t1HYHU0zDM/ZHTsD1fAWvnI6wkbcQVpWtGBhQTEyQ80hJedW66gJN1uPjx9b5whOjorTrXQZZqCGXPRh3sMCabQy8AA2HGCxDxfLxPVeku5HX+/YQoTRT16vPYYRJtmhVfRZIydrHrDk/Cxyp0= corina@blue
```

Verificare

```
corina@blue:~$ ssh student@host
```

> La prima autentificare cu `ssh`, ma va intreba "Are you sure you want to continue connecting". Raspund cu "yes", iar altadata nu va mai intreba nimic (se va conecta automat).

Task 03 | Download si upload de director folosind `scp`

Task 03 | Download prin `scp` (from remote to local)

Descarc directorul `assignment/` din directorul `home` al utilizatorului `student` de pe statia `host`.

```
corina@blue:~$ scp -r student@host:~/assignment student-assignment
```

```
corina@blue:~$ scp -r student@host:~/assignment student-assignment
linear.txt                                                                    100%
10    15.7KB/s   00:00
cubic.txt                                                                     100%
24    50.2KB/s   00:00
quadratic.txt                                                                 100%
17    39.9KB/s   00:00
corina@blue:~$ ls
blue-file-10M.dat  solution  student-ass*ignment
corina@blue:~$ cd student-assignment/
corina@blue:~/student-assignment$ ls
cubic.txt  linear.txt  quadratic.txt
corina@blue:~/student-assignment$ cat cubic.txt
x^3 - 6x^2 + 11x -6 = 0
corina@blue:~/student-assignment$ cat linear.txt
x - 1 = 0
corina@blue:~/student-assignment$ cat quadratic.txt
x^2 - 3x + 2 = 0
```

Task 03 | Upload prin `scp` (from local to remote)

Uploadez direcorul `solution/` in directorul `home` al utilizatorului `student` de pe `host`.

```
corina@blue:~$ scp -r student@host:~/assignment student-assignment
```

```
corina@blue:~$ scp -r student@host:~/assignment student-assignment
linear.txt                                                                  100%
10    15.7KB/s   00:00
cubic.txt                                                                   100%
24    50.2KB/s   00:00
quadratic.txt                                                               100%
17    39.9KB/s   00:00

student@host:~$ ls
assignment  host-file-10M.dat  pwndbg  solution
student@host:~$ cd solution/
student@host:~/solution$ ls
cubic.txt  linear.txt  quadratic.txt
student@host:~/solution$ cat cubic.txt
x1 = 1, x2 = 2, x3 = 3
student@host:~/solution$ cat linear.txt
x = 1
student@host:~/solution$ cat quadratic.txt
x1 = 1, x2 = 2
```

Task 04 | Copiere fisiere cu diverse protocoale: durata si consum de resurse

Task 04 | Transfer prin `netcat` (a.k.a `nc`)

```
# Terminal 1
student@host:~$ nc -l 12345 > file-100M-nc.dat
```

```
# Terminal 2
student@green:~$ time cat file-100M.dat | nc -q0 host 12345

real    0m0.225s
user    0m0.011s
sys 0m0.081s
```

Verific **hash**-urile:

```
# Terminal 1
student@host:~$ sha512sum file-100M-nc.dat
0fd2d103367c010b4f21ab2c6d1be7adf888e186f0e19363d8e19dbbfef1b491540566894a8
2f2d701f108a6aff589e70286537da9641f076639626058c38614  file-100M-nc.dat
```

```
# Terminal 2
student@green:~$ sha512sum file-100M.dat
0fd2d103367c010b4f21ab2c6d1be7adf888e186f0e19363d8e19dbbfef1b491540566894a8
2f2d701f108a6aff589e70286537da9641f076639626058c38614  file-100M.dat
```

Task 04 | Transfer prin FTP

```
student@green:~$ time curl -T file-100M.dat -u student:student
ftp://host/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   278M --:--:-- --:--:-- --:--:--
279M

real    0m0.505s
user    0m0.004s
sys 0m0.048s
```

Task 04 | Transfer prin SSH

```
student@green:~$ time scp file-100M.dat student@host:file-100M-scp.dat

file-100M.dat                                                         100%
100MB 181.5MB/s   00:00

real    0m0.714s
user    0m0.164s
sys 0m0.083s
```

Task 05 | Trafic criptat si necriptat

Se ruleaza comenzile cu copy-paste

```
# Terminal 1
root@host:~# tcpdump -vvv -A -i veth-green
```

```
# Terminal 2
root@red:~# telnet green    # (usernmae: student; parola: student)
root@red:~# ftp green       # Same
root@red:~# ssh -l student green
```

Task 06 | Blocare servicii necriptate

```
root@host:~# # Blocheaza 'telent green'
root@host:~# iptables -A FORWARD -d green -p tcp --dport telnet -j REJECT
root@host:~# # Blocheaza 'ftp green'
root@host:~# iptables -A FORWARD -d green -p tcp --dport ftp -j REJECT
```

> In loc de argumentul `telnet`/`ftp` pentru `--dport`, se poate folosi portul numeric `23`/`21`.

> Asocierile dintre protocol si port se gasesc in `/etc/services`.

```
student@red:~$ ftp green
ftp: Can't connect to `192.168.2.2:21': Bad file descriptor
ftp: Can't connect to `green:ftp'
ftp>
ftp> ls
Not connected.
ftp> ls
Not connected.
ftp> ls
Not connected.
ftp> ^D
student@red:~$
exit
root@host:~# iptables -L FORWARD -v -n
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain FORWARD (policy ACCEPT 403 packets, 34224 bytes)
 pkts bytes target     prot opt in     out     source
destination
    2   120 REJECT     tcp  --  *      *       0.0.0.0/0
192.168.2.2          tcp dpt:23 reject-with icmp-port-unreachable
    1    60 REJECT     tcp  --  *      *       0.0.0.0/0
192.168.2.2          tcp dpt:21 reject-with icmp-port-unreachable
```

Task 07 | Blocare SSH

```
root@host:~# iptables -A FORWARD -d green -p tcp --dport ssh -j REJECT
root@host:~# go red
student@red:~$ ssh student@green
ssh: connect to host green port 22: Connection refused
```

```
# Comenzi de verificare iptables
root@host:~# iptables -L FORWARD
```

```
root@host:~# iptables -L FORWARD -vv -n
```

```
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain FORWARD (policy ACCEPT 403 packets, 34224 bytes)
 pkts bytes target     prot opt in     out     source
destination
    2   120 REJECT     tcp  --  *      *       0.0.0.0/0
192.168.2.2          tcp dpt:23 reject-with icmp-port-unreachable
    1    60 REJECT     tcp  --  *      *       0.0.0.0/0
192.168.2.2          tcp dpt:21 reject-with icmp-port-unreachable
    2   120 REJECT     tcp  --  *      *       0.0.0.0/0
192.168.2.2          tcp dpt:22 rejec
```

Task 08 | Permitere trafic SSH

```
root@host:~# iptables -I FORWARD 3 -s red -d green -p tcp --dport ssh -j
ACCEPT
```

```
# Comanda de verificare
root@host:~# iptables -L FORWARD -vv -n
```

```
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain FORWARD (policy ACCEPT 403 packets, 34224 bytes)
 pkts bytes target     prot opt in     out     source
destination
    2   120 REJECT     tcp  --  *      *       0.0.0.0/0
192.168.2.2          tcp dpt:23 reject-with icmp-port-unreachable
    1    60 REJECT     tcp  --  *      *       0.0.0.0/0
192.168.2.2          tcp dpt:21 reject-with icmp-port-unreachable
    0     0 ACCEPT     tcp  --  *      *       192.168.1.2
192.168.2.2          tcp dpt:22
    2   120 REJECT     tcp  --  *      *       0.0.0.0/0
192.168.2.2          tcp dpt:22 reject-with icmp-port-unreachable
```

```
# Verificare
student@red:~$ ssh student@green    # Merge
student@blue:~$ ssh student@green   # Connection refused (e bine) :)
```

Task 09 | Stergere regului adaugate

```
root@host:~# iptables -F FORWARD
```

```
# Comanda de verificare
root@host:~# iptables -L FORWARD -n -v
```

```
student@red:~$ telnet green       # Merge
student@red:~$ ftp student@green  # Merge
student@red:~$ ssh student@green  # Merge

student@blue:~$ telnet green       # Merge
student@blue:~$ ftp student@green  # Merge
student@blue:~$ ssh student@green  # Merge
```

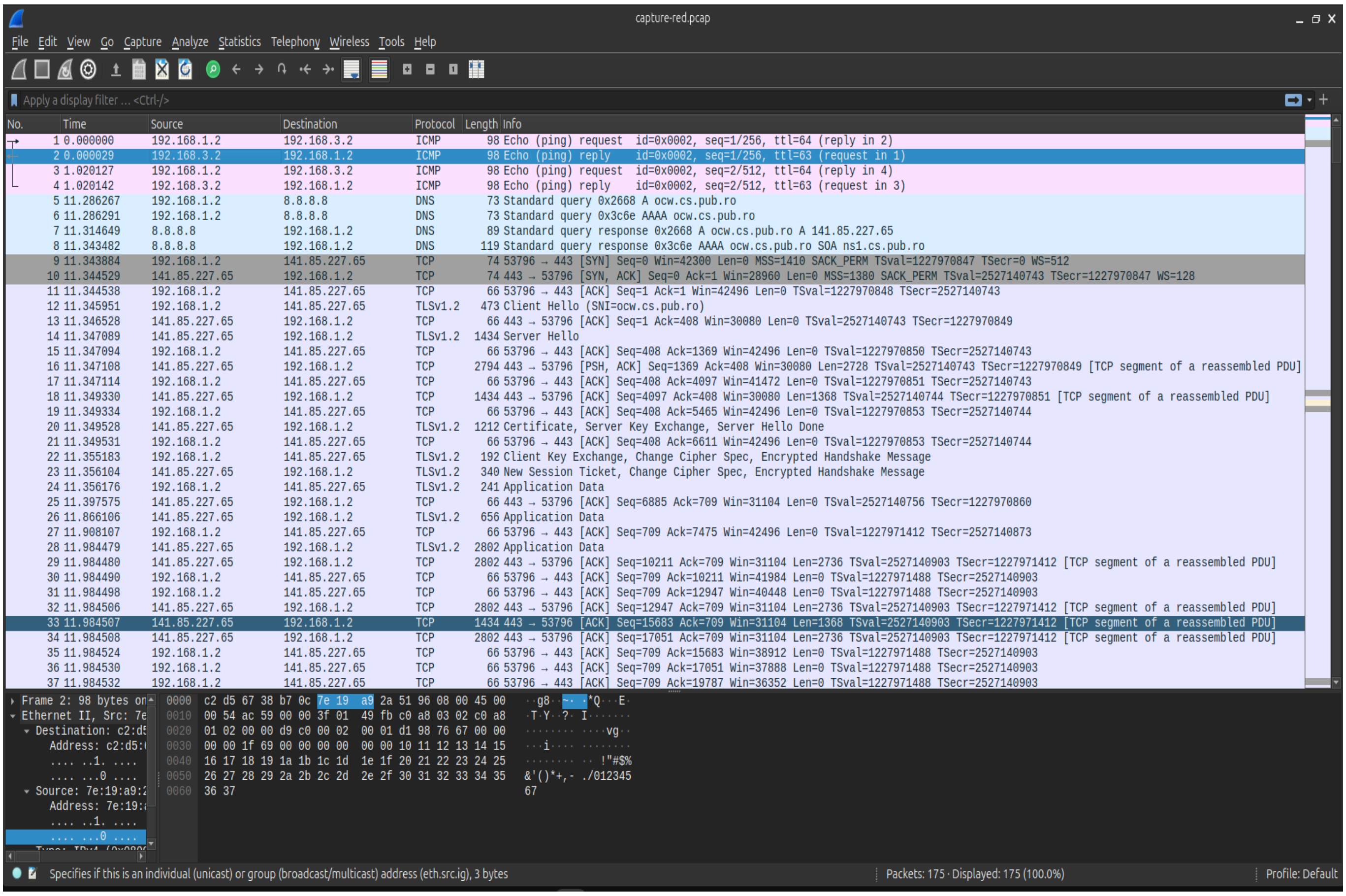
Task 10 | Captura de trafic

```
# Terminalul 1
root@host:~# tcpdump -i veth-red -v -w capture-red.pcap
```

```
# Terminalul 2
student@red:~$ ping blue
student@red:~$ wget https://ocw.cs.pub.ro/courses/rl/labs/07
student@red:~$ ssh student@green
```

```
root@host:~# mv capture-red.pcap /home/student/
```

```
je@localhost:~$ scp -J moodle-username@fep.grid.pub.ro student@<IP-VM>:~/capture-red.pcap ~/Downloads/capture-red.pcap
je@localhost:~$ wireshark ~/Downloads/capture-red.pcap &
```


capture-red.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No. Time      Source         Destination    Protocol Length Info
  1 0.000000  192.168.1.2    192.168.3.2    ICMP      98 Echo (ping) request  id=0x0002, seq=1/256, ttl=64 (reply in 2)
  2 0.000029  192.168.3.2    192.168.1.2    ICMP      98 Echo (ping) reply    id=0x0002, seq=1/256, ttl=63 (request in 1)
  3 1.020127  192.168.1.2    192.168.3.2    ICMP      98 Echo (ping) request  id=0x0002, seq=2/512, ttl=64 (reply in 4)
  4 1.020142  192.168.3.2    192.168.1.2    ICMP      98 Echo (ping) reply    id=0x0002, seq=2/512, ttl=63 (request in 3)
  5 11.286267 192.168.1.2    8.8.8.8        DNS       73 Standard query 0x2668 A ocw.cs.pub.ro
  6 11.286291 192.168.1.2    8.8.8.8        DNS       73 Standard query 0x3c6e AAAA ocw.cs.pub.ro
  7 11.314649 8.8.8.8        192.168.1.2    DNS       89 Standard query response 0x2668 A ocw.cs.pub.ro A 141.85.227.65
  8 11.343482 8.8.8.8        192.168.1.2    DNS      119 Standard query response 0x3c6e AAAA ocw.cs.pub.ro SOA ns1.cs.pub.ro
  9 11.343884 192.168.1.2    141.85.227.65  TCP       74 53796 → 443 [SYN] Seq=0 Win=42300 Len=0 MSS=1410 SACK_PERM TSval=1227970847 TSecr=0 WS=512
 10 11.344529 141.85.227.65  192.168.1.2    TCP       74 443 → 53796 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM TSval=2527140743 TSecr=1227970847 WS=128
 11 11.344538 192.168.1.2    141.85.227.65  TCP       66 53796 → 443 [ACK] Seq=1 Ack=1 Win=42496 Len=0 TSval=1227970848 TSecr=2527140743
 12 11.345951 192.168.1.2    141.85.227.65  TLSv1.2  473 Client Hello (SNI=ocw.cs.pub.ro)
 13 11.346528 141.85.227.65  192.168.1.2    TCP       66 443 → 53796 [ACK] Seq=1 Ack=408 Win=30080 Len=0 TSval=2527140743 TSecr=1227970849
 14 11.347089 141.85.227.65  192.168.1.2    TLSv1.2 1434 Server Hello
 15 11.347094 192.168.1.2    141.85.227.65  TCP       66 53796 → 443 [ACK] Seq=408 Ack=1369 Win=42496 Len=0 TSval=1227970850 TSecr=2527140743
 16 11.347108 141.85.227.65  192.168.1.2    TCP     2794 443 → 53796 [PSH, ACK] Seq=1369 Ack=408 Win=30080 Len=2728 TSval=2527140743 TSecr=1227970849 [TCP segment of a reassembled PDU]
 17 11.347114 192.168.1.2    141.85.227.65  TCP       66 53796 → 443 [ACK] Seq=408 Ack=4097 Win=41472 Len=0 TSval=1227970851 TSecr=2527140743
 18 11.349330 141.85.227.65  192.168.1.2    TCP     1434 443 → 53796 [ACK] Seq=4097 Ack=408 Win=30080 Len=1368 TSval=2527140744 TSecr=1227970851 [TCP segment of a reassembled PDU]
 19 11.349334 192.168.1.2    141.85.227.65  TCP       66 53796 → 443 [ACK] Seq=408 Ack=5465 Win=42496 Len=0 TSval=1227970853 TSecr=2527140744
 20 11.349528 141.85.227.65  192.168.1.2    TLSv1.2 1212 Certificate, Server Key Exchange, Server Hello Done
 21 11.349531 192.168.1.2    141.85.227.65  TCP       66 53796 → 443 [ACK] Seq=408 Ack=6611 Win=42496 Len=0 TSval=1227970853 TSecr=2527140744
 22 11.355183 192.168.1.2    141.85.227.65  TLSv1.2  192 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 23 11.356104 141.85.227.65  192.168.1.2    TLSv1.2  340 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
 24 11.356176 192.168.1.2    141.85.227.65  TLSv1.2  241 Application Data
 25 11.397575 141.85.227.65  192.168.1.2    TCP       66 443 → 53796 [ACK] Seq=6885 Ack=709 Win=31104 Len=0 TSval=2527140756 TSecr=1227970860
 26 11.866106 141.85.227.65  192.168.1.2    TLSv1.2  656 Application Data
 27 11.908107 192.168.1.2    141.85.227.65  TCP       66 53796 → 443 [ACK] Seq=709 Ack=7475 Win=42496 Len=0 TSval=1227971412 TSecr=2527140873
 28 11.984479 141.85.227.65  192.168.1.2    TLSv1.2 2802 Application Data
 29 11.984480 141.85.227.65  192.168.1.2    TCP     2802 443 → 53796 [ACK] Seq=10211 Ack=709 Win=31104 Len=2736 TSval=2527140903 TSecr=1227971412 [TCP segment of a reassembled PDU]
 30 11.984490 192.168.1.2    141.85.227.65  TCP       66 53796 → 443 [ACK] Seq=709 Ack=10211 Win=41984 Len=0 TSval=1227971488 TSecr=2527140903
 31 11.984498 192.168.1.2    141.85.227.65  TCP       66 53796 → 443 [ACK] Seq=709 Ack=12947 Win=40448 Len=0 TSval=1227971488 TSecr=2527140903
 32 11.984506 141.85.227.65  192.168.1.2    TCP     2802 443 → 53796 [ACK] Seq=12947 Ack=709 Win=31104 Len=2736 TSval=2527140903 TSecr=1227971412 [TCP segment of a reassembled PDU]
 33 11.984507 141.85.227.65  192.168.1.2    TCP     1434 443 → 53796 [ACK] Seq=15683 Ack=709 Win=31104 Len=1368 TSval=2527140903 TSecr=1227971412 [TCP segment of a reassembled PDU]
 34 11.984508 141.85.227.65  192.168.1.2    TCP     2802 443 → 53796 [ACK] Seq=17051 Ack=709 Win=31104 Len=2736 TSval=2527140903 TSecr=1227971412 [TCP segment of a reassembled PDU]
 35 11.984524 192.168.1.2    141.85.227.65  TCP       66 53796 → 443 [ACK] Seq=709 Ack=15683 Win=38912 Len=0 TSval=1227971488 TSecr=2527140903
 36 11.984530 192.168.1.2    141.85.227.65  TCP       66 53796 → 443 [ACK] Seq=709 Ack=17051 Win=37888 Len=0 TSval=1227971488 TSecr=2527140903
 37 11.984532 192.168.1.2    141.85.227.65  TCP       66 53796 → 443 [ACK] Seq=709 Ack=19787 Win=36352 Len=0 TSval=1227971488 TSecr=2527140903
```

```
› Frame 2: 98 bytes on
⌄ Ethernet II, Src: 7e
  ⌄ Destination: c2:d5
      Address: c2:d5:(
      .... ..1. ....
      .... ...0 ....
  ⌄ Source: 7e:19:a9:2
      Address: 7e:19:a
      .... ..1. ....
      .... ...0 ....
```

```
0000  c2 d5 67 38 b7 0c 7e 19  a9 2a 51 96 08 00 45 00   ··g8··~· ·*Q···E·
0010  00 54 ac 59 00 00 3f 01  49 fb c0 a8 03 02 c0 a8   ·T·Y··?· I·······
0020  01 02 00 00 d9 c0 00 02  00 01 d1 98 76 67 00 00   ········ ····vg··
0030  00 00 1f 69 00 00 00 00  00 00 10 11 12 13 14 15   ···i···· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.src.ig), 3 bytes | Packets: 175 · Displayed: 175 (100.0%) | Profile: Default

Pachete analizate contin:

- Protocolul ICMP pentru ping-uri
- Este si un ARP undeva pe acolo ("Who has IP....?")
- Protocolul DNS pentru wget (se face domain resolution)
- TLSv1.2 pentru descarcaea paginii web
- SSHv2

Task 11 (Bonus) | Blocare acces `green` -> `red`

```
# Blocheaza traficul TCP initiat de la green la red (green -> red)
root@host:~# iptables -A FORWARD -s green -d red -p tcp -m state --state NEW -j REJECT
```

```
# Comanda de verificare
root@host:~# iptables -L FORWARD -vv -n
```

```
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain FORWARD (policy ACCEPT 1063 packets, 105K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

```
    2   120 REJECT     tcp  --  *      *       192.168.2.2
192.168.1.2          state NEW reject-with icmp-port-unreachable
```

Task 12 (Bonus) | Transfer sincronizat de fisiere folosind `rsync` peste `SSH`

> **TL;DR**: `rsync -avz -r --delete -e "ssh -i /home/ana/.ssh/blue-bogdan" ~/proiecte/ bogdan@blue:~/proiecte-backup`.

```
student@host:~$ sudo su - ana

ana@host:~$ # Generare pereche chei SSH
ana@host:~$ ssh-keygen -t ed25519 -f ~/.ssh/blue-bogdan -N ""
```

```
ana@host:~$ # Nu merge... cere parola :(
ana@host:~$ ssh-copy-id -i ~/.ssh/blue-bogdan.pub bogdan@blue
bogdan@blue's password:
```

De vreme ce `ssh-copy-id -i ~/.ssh/blue-bogdan bogdan@blue` nu functioneaza, va trebui sa copiez manual **cheia publica** in fisierul `~/.ssh/authorized_keys` de pe `bogdan@blue`.

```
ana@host:~$ cat ~/.ssh/blue-bogdan.pub
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAINp7juYp8oqg4v3W5RvvPk5gFUvFHTgkq3X3GlUBD8ot
ana@host
```

Deschid un nou terminal (`Ctrl+Shift+T`) si ma autentific ca `bogdan@blue`.

```
student@host:~$ go blue
student@blue:~$ sudo su - bogdan
bogdan@blue:~$
```

```
bogdan@blue:~$ # Copiez cheia publica aici
bogdan@blue:~$ nano -l ~/.ssh/authorized_keys

bogdan@blue:~$ cat ~/.ssh/authorized_keys
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAINp7juYp8oqg4v3W5RvvPk5gFUvFHTgkq3X3GlUBD8ot
ana@host
```

Apoi, pe `host`:

```
ana@host:~$ # Verificare conectare fara parola
ana@host:~$ ssh -i ~/.ssh/blue-bogdan bogdan@blue
```

```
ana@host:~$ # Sincronizare
ana@host:~$ rsync -avz -r --delete -e "ssh -i /home/ana/.ssh/blue-bogdan" ~/proiecte/ bogdan@blue:~/proiecte-backup
```

Verificare, dupa rularea `rsync`-ului

```
bogdan@blue:~$ ls --recursive
bogdan@blue:~$ # Sau
bogdan@blue:~$ tree
```

Alternativ, se poate crea o intrare in fisierul de configuratie SSH pentru autentificarea fara parola pe `bogdan@blue`.

```
ana@host:~$ nano -l ~/.ssh/config
```

```
Host blue
    HostName blue
    IdentityFile ~/.ssh/blue-bogdan
```

```
ana@host:~$ # Verificare conectare fara parola
ana@host:~$ ssh bogdan@blue
```

```
ana@host:~$ # Sincronizare
ana@host:~$ rsync -avz -r --delete -e ssh ~/proiecte/ bogdan@blue:~/proiecte-backup
ana@host:~$ # Alternativ
ana@host:~$ rsync -avz -r --delete ~/proiecte/ bogdan@blue:~/proiecte-backup
```

> NOTA: Daca exista o configuratie de SSH definita in `~/.ssh/config`, `rsync`-ul va folosi automat intrarea respectiva. In acest caz, optiunea `-e ssh` nu mai este necesara.