Zadanie 1

Ip adresu a MAC som zistil pomocou ip addr

```
[rocky@rocky-student-32 ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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 1500 qdisc fq_codel state UP grou
p default qlen 1000
    link/ether fa:f1:17:13:39:4a brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    altname ens3
    inet 10.103.1.39/16 brd 10.103.255.255 scope global dynamic noprefixroute et
h0
       valid_lft 47495sec preferred_lft 47495sec
    inet6 fe80::f8f1:17ff:fe13:394a/64 scope link
       valid_lft forever preferred_lft forever
```

IP adresa: 10.103.1.39/16

MAC: fa:f1:17:13.39:4a

Pozivame dhcp (BOOTPROTO=dhcp)

```
[rocky@rocky-student-32 /]$ cat etc/sysconfig/network-scripts/ifcfg-eth0
# Created by cloud-init on instance boot automatically, do not edit.
#
AUTOCONNECT_PRIORITY=999
BOOTPROTO=dhcp
DEVICE=eth0
HWADDR=fa:f1:17:13:39:4a
MTU=1500
ONBOOT=yes
TYPE=Ethernet
USERCTL=no
```

Routing table:

```
[rocky@rocky-student-32 /]$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.103.0.1      0.0.0.0         UG    100    0        0 eth0
10.103.0.0      0.0.0.0         255.255.0.0     U     100    0        0 eth0
10.105.0.0      0.0.0.0         255.255.0.0     U     100    0        0 eth0
169.254.169.254 10.103.1.3      255.255.255.255 UGH   100    0        0 eth0
```

DNS server:

```
[rocky@rocky-student-32 /]$ cat etc/resolv.conf
; Created by cloud-init on instance boot automatically, do not edit.
;
nameserver 147.175.159.11
```

Pingnutim google.com zistime ci sme pripojeny na internet

```
[rocky@rocky-student-32 /]$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=6.51 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=7.14 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=7.85 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=6.58 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 6.506/7.019/7.853/0.539 ms
```

Zadanie 2

```
[rocky@rocky-student-32 /]$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLI
ISHED,RELATED -j ACCEPT
```

Appendnem do input, pomocou modulu conntrack matchuje pakety ktore su ESTABLISHED alebo RELATED a jumpne rovno na ACCEPT

sudo iptables -A INPUT -p icmp -j ACCEPT

podobne, len specifikujem protocol icmp

sudo iptables -A INPUT -i lo -j ACCEPT

-i (interface) lo (loopback)

sudo iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW -j ACCEPT

-p tcp –dport 22 (22 je ssh)

Cez conntrack matchujem nove requesty na pripojenie

sudo iptables -A INPUT -p tcp -s 10.103.0.0/16 --dport 0:1023 -m conntrack --ctstate NEW -j ACCEPT

-s – source adresa alebo subnet

--dport 0:1023 – well known porty

sudo iptables -A INPUT -j LOG

Jumpne rovno na logovanie

sudo iptables -A INPUT -j DROP

A nasledne ich drone

save

```
[rocky@rocky-student-32 /]$ sudo service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables: [  OK  ]
```

Zadanie 3

V súbore /etc/ssh/sshd_config zmenime nasledovne:

Zrusenie prihlasenia rootu

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Zrusenie autentifikacie heslom:

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
#KbdInteractiveAuthentication yes
```

X11 forwarding: