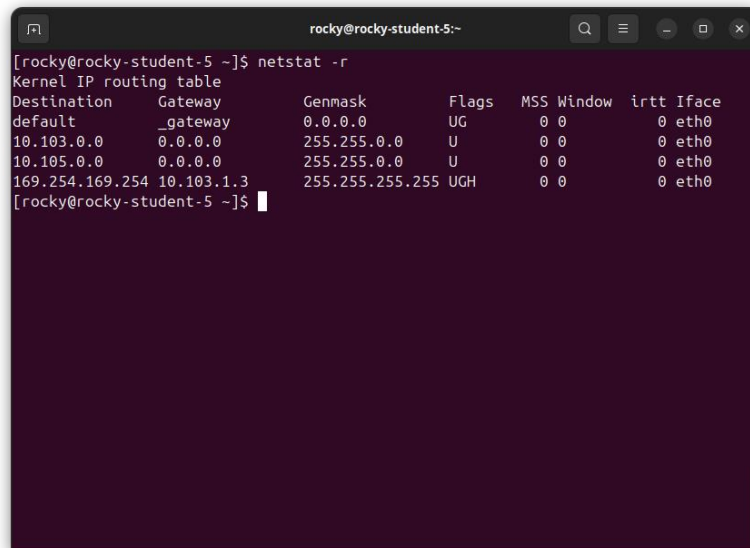


3. Zistiť smerovaciu tabuľku

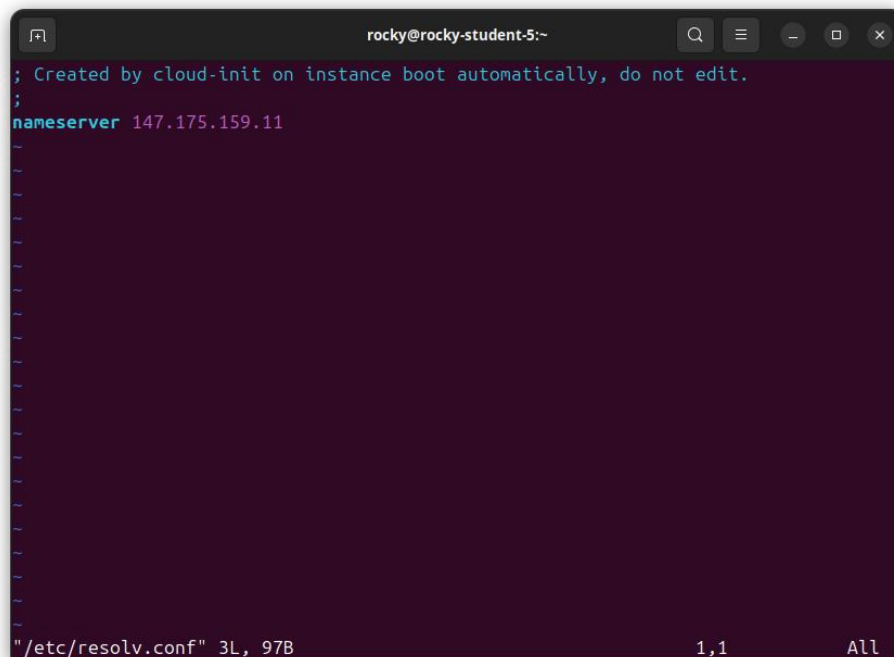
netstat -r – vypísanie smerovacej tabuľky



```
rocky@rocky-student-5:~$ netstat -r
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
default _gateway 0.0.0.0 UG 0 0 0 eth0
10.103.0.0 0.0.0.0 255.255.0.0 U 0 0 0 eth0
10.105.0.0 0.0.0.0 255.255.0.0 U 0 0 0 eth0
169.254.169.254 10.103.1.3 255.255.255.255 UGH 0 0 0 eth0
[rocky@rocky-student-5 ~]$
```

4. Zistiť nastavenia DNS

sudo vim /etc/resolv.conf – nastavenia DNS sa dajú nájsť v súbore */etc/resolv.conf*



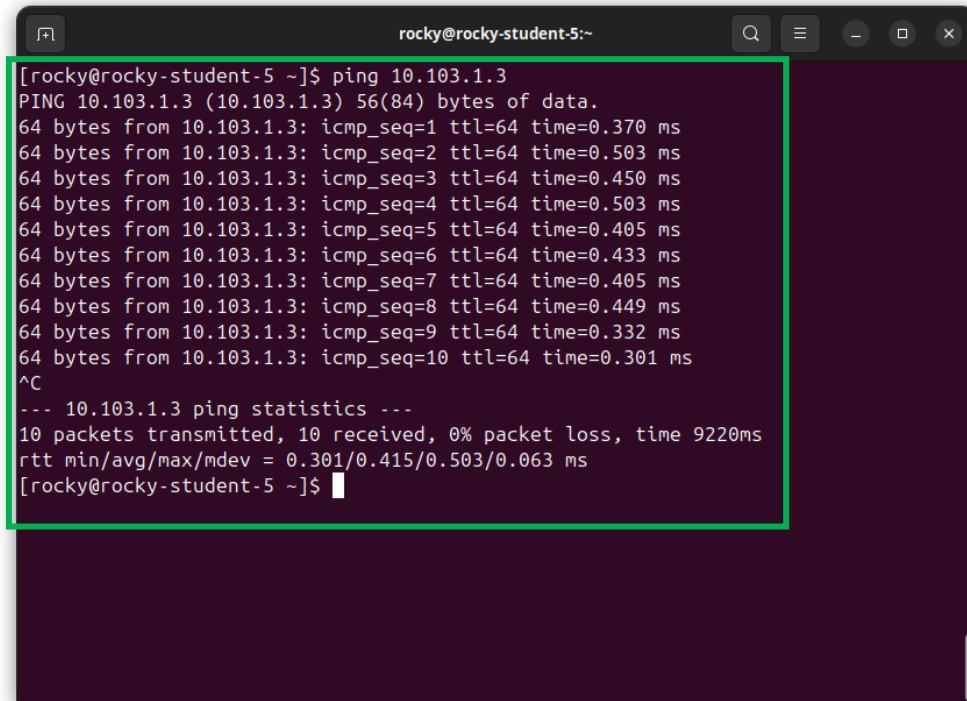
```
rocky@rocky-student-5:~$ sudo vim /etc/resolv.conf
; Created by cloud-init on instance boot automatically, do not edit.
;
nameserver 147.175.159.11

"/etc/resolv.conf" 3L, 97B 1,1 All
```

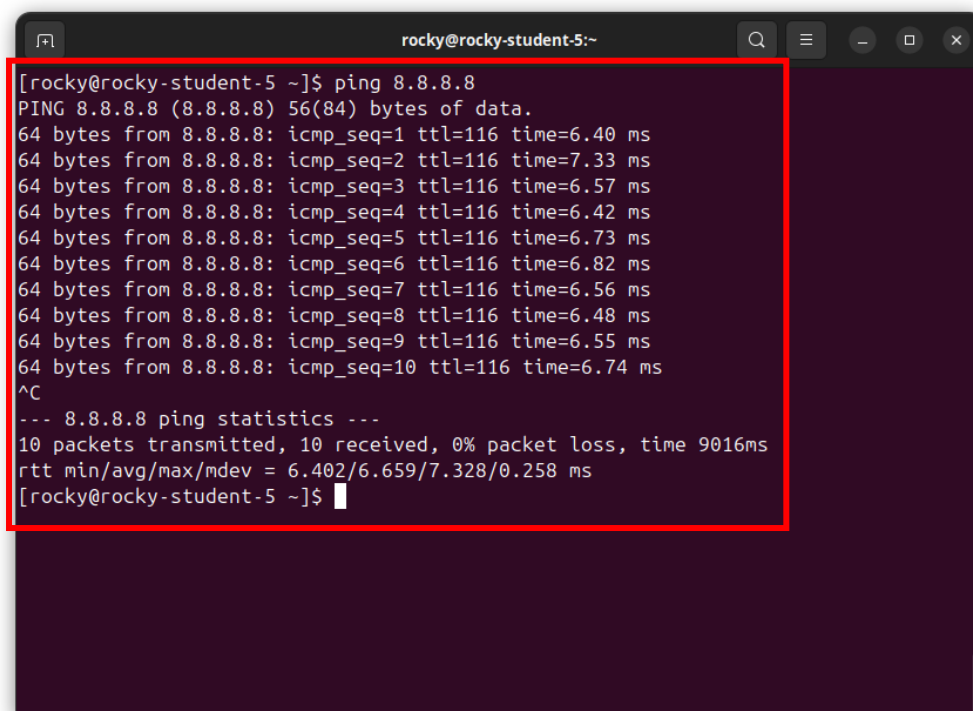
5. Preveriť dostupnosť siete a Internetu pomocou ICMP.

ping 10.103.1.3 – overenie dostupnosti siete (zelená farba)

ping 8.8.8.8 – overenie dostupnosti Internetu (červená farba)



```
rocky@rocky-student-5:~$ ping 10.103.1.3
PING 10.103.1.3 (10.103.1.3) 56(84) bytes of data.
64 bytes from 10.103.1.3: icmp_seq=1 ttl=64 time=0.370 ms
64 bytes from 10.103.1.3: icmp_seq=2 ttl=64 time=0.503 ms
64 bytes from 10.103.1.3: icmp_seq=3 ttl=64 time=0.450 ms
64 bytes from 10.103.1.3: icmp_seq=4 ttl=64 time=0.503 ms
64 bytes from 10.103.1.3: icmp_seq=5 ttl=64 time=0.405 ms
64 bytes from 10.103.1.3: icmp_seq=6 ttl=64 time=0.433 ms
64 bytes from 10.103.1.3: icmp_seq=7 ttl=64 time=0.405 ms
64 bytes from 10.103.1.3: icmp_seq=8 ttl=64 time=0.449 ms
64 bytes from 10.103.1.3: icmp_seq=9 ttl=64 time=0.332 ms
64 bytes from 10.103.1.3: icmp_seq=10 ttl=64 time=0.301 ms
^C
--- 10.103.1.3 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9220ms
rtt min/avg/max/mdev = 0.301/0.415/0.503/0.063 ms
[rocky@rocky-student-5 ~]$
```



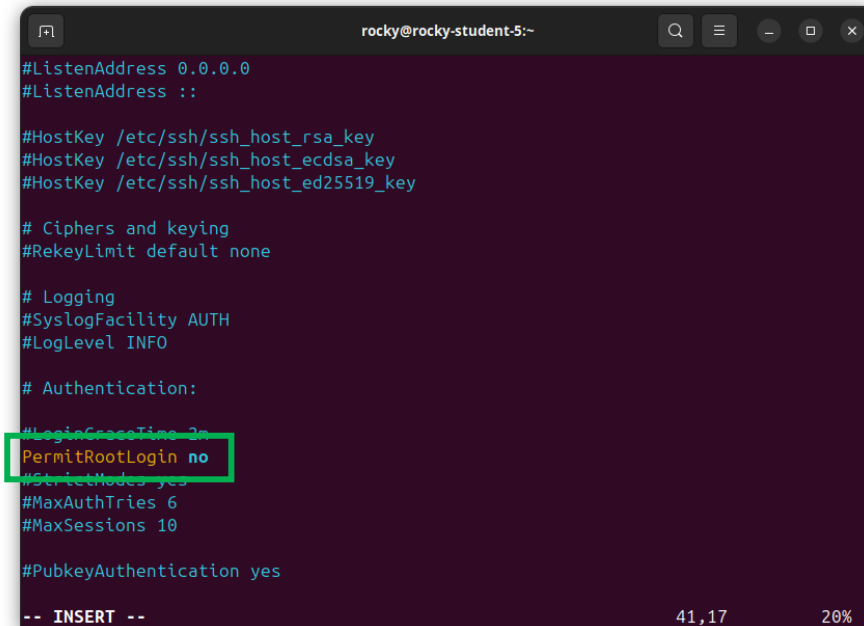
```
rocky@rocky-student-5:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=6.40 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=7.33 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=6.57 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=6.42 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=116 time=6.73 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=116 time=6.82 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=116 time=6.56 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=116 time=6.48 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=116 time=6.55 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=116 time=6.74 ms
^C
--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9016ms
rtt min/avg/max/mdev = 6.402/6.659/7.328/0.258 ms
[rocky@rocky-student-5 ~]$
```


Úloha č. 3

Nastaviť službu SSH na Vašom virtuálnom stroji, aby:

1. **neumožnila prihlásenie používateľa 'root',**

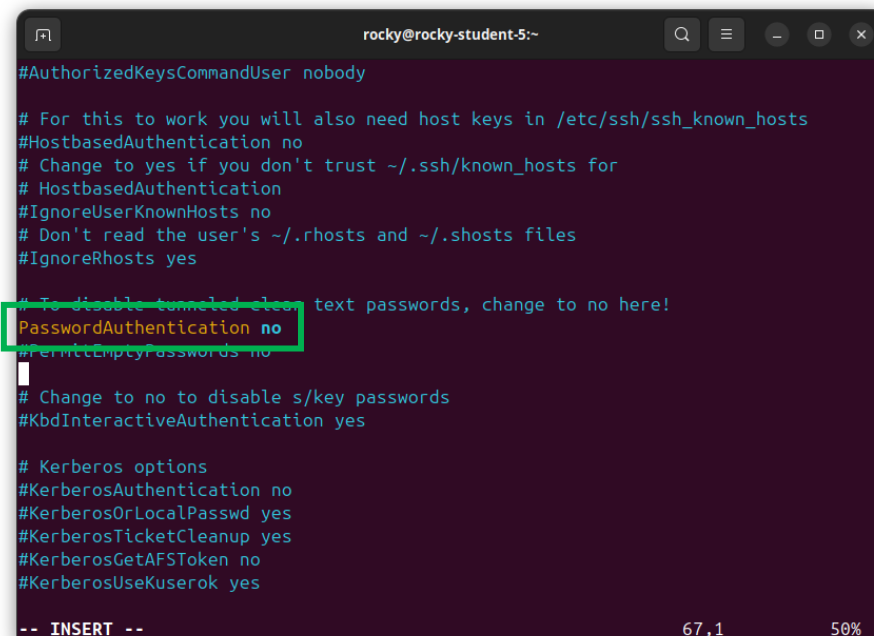
Je potrebné zmeniť vyznačený riadok na „no“ v súbore `/etc/ssh/sshd_config`



```
rocky@rocky-student-5:~  
#ListenAddress 0.0.0.0  
#ListenAddress ::  
  
#HostKey /etc/ssh/ssh_host_rsa_key  
#HostKey /etc/ssh/ssh_host_ecdsa_key  
#HostKey /etc/ssh/ssh_host_ed25519_key  
  
# Ciphers and keying  
#RekeyLimit default none  
  
# Logging  
#SyslogFacility AUTH  
#LogLevel INFO  
  
# Authentication:  
#LoginGraceTime 3m  
PermitRootLogin no  
#StrictModes yes  
#MaxAuthTries 6  
#MaxSessions 10  
  
#PubkeyAuthentication yes  
  
-- INSERT --
```

2. **neumožnila autentifikáciu heslom (iba kľúčom),**

Je potrebné zmeniť vyznačený riadok na „no“ v súbore `/etc/ssh/sshd_config`



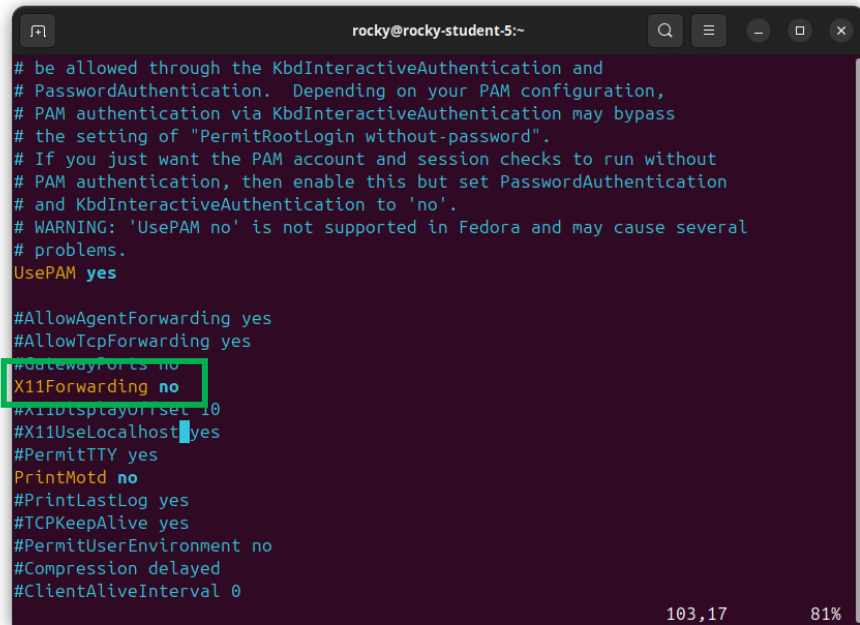
```
rocky@rocky-student-5:~  
#AuthorizedKeysCommandUser nobody  
  
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts  
#HostbasedAuthentication no  
# Change to yes if you don't trust ~/.ssh/known_hosts for  
# HostbasedAuthentication  
#IgnoreUserKnownHosts no  
# Don't read the user's ~/.rhosts and ~/.shosts files  
#IgnoreRhosts yes  
  
# To disable tunneled clear text passwords, change to no here!  
PasswordAuthentication no  
#PermitEmptyPasswords no  
  
# Change to no to disable s/key passwords  
#KbdInteractiveAuthentication yes  
  
# Kerberos options  
#KerberosAuthentication no  
#KerberosOrLocalPasswd yes  
#KerberosTicketCleanup yes  
#KerberosGetAFSToken no  
#KerberosUseKuserok yes  
  
-- INSERT --
```

Tomáš Brček, ID:120761

Cvičenie: Pondelok 17:00

3. neumožnila presmerovanie X11.

Je potrebné zmeniť vyznačený riadok na „no“ v súbore `/etc/ssh/sshd_config`



```
rocky@rocky-student-5:~  
# be allowed through the KbdInteractiveAuthentication and  
# PasswordAuthentication. Depending on your PAM configuration,  
# PAM authentication via KbdInteractiveAuthentication may bypass  
# the setting of "PermitRootLogin without-password".  
# If you just want the PAM account and session checks to run without  
# PAM authentication, then enable this but set PasswordAuthentication  
# and KbdInteractiveAuthentication to 'no'.  
# WARNING: 'UsePAM no' is not supported in Fedora and may cause several  
# problems.  
UsePAM yes  
  
#AllowAgentForwarding yes  
#AllowTcpForwarding yes  
#GatewayPorts no  
X11Forwarding no  
#X11UseLocalhost yes  
#PermitTTY yes  
PrintMotd no  
#PrintLastLog yes  
#TCPKeepAlive yes  
#PermitUserEnvironment no  
#Compression delayed  
#ClientAliveInterval 0
```

103,17 81%

Úloha 4

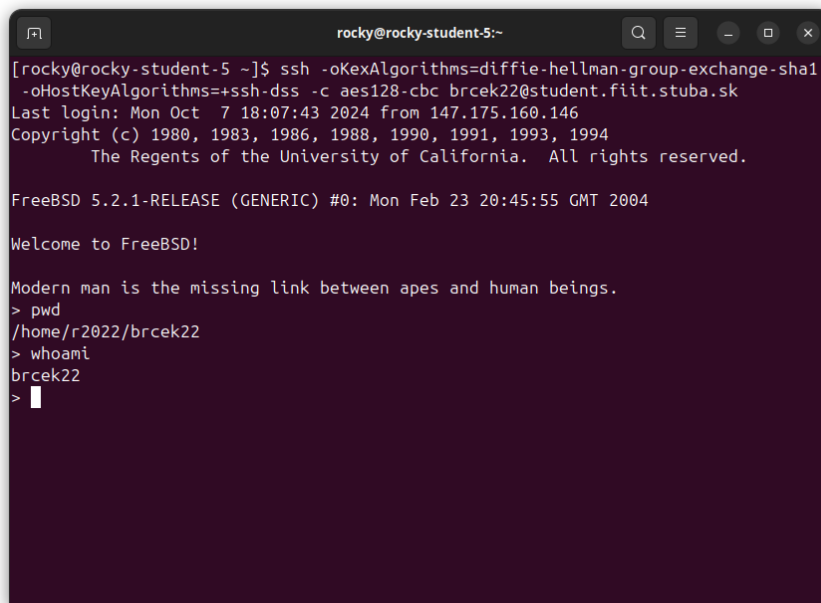
Nastaviť SSH na stroji 'student' tak, aby umožnila autentifikáciu bez zadávania hesla (pomocou kľúča).

ssh-keygen -t rsa – vygenerovanie SSH kľúča v rocky linux

ssh-copy-id -o KexAlgorithms=diffie-hellman-group-exchange-sha1 -o HostKeyAlgorithms=+ssh-dss -o Ciphers=aes128-cbc brcek22@student.fiit.stuba.sk

- vygenerovaný verejný kľúč som skopíroval na cieľový stroj, teda stroj student

ssh -oKexAlgorithms=diffie-hellman-group-exchange-sha1 -oHostKeyAlgorithms=+ssh-dss -c aes128-cbc brcek22@student.fiit.stuba.sk – prihlásenie na stroj student bez hesla



```
rocky@rocky-student-5:~  
[rocky@rocky-student-5 ~]$ ssh -oKexAlgorithms=diffie-hellman-group-exchange-sha1  
-oHostKeyAlgorithms=+ssh-dss -c aes128-cbc brcek22@student.fiit.stuba.sk  
Last login: Mon Oct 7 18:07:43 2024 from 147.175.160.146  
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994  
The Regents of the University of California. All rights reserved.  
  
FreeBSD 5.2.1-RELEASE (GENERIC) #0: Mon Feb 23 20:45:55 GMT 2004  
  
Welcome to FreeBSD!  
  
Modern man is the missing link between apes and human beings.  
> pwd  
/home/r2022/brcek22  
> whoami  
brcek22  
> 
```

Aké je najvhodnejšie poradie nastavení (úloh) z hľadiska bezpečnosti?

Najvhodnejšie poradie nastavení je:

1. najprv firewall a sieťové pravidlá, aby sme obmedzili prístup k službám zvonku
2. potom SSH autentifikácia (kľúč a zakázanie hesiel)
3. nakoniec špecifické pravidlá pre prihlásenie root a X11 presmerovanie