

1. Создать сервер t2.micro(Ubuntu), он должен иметь публичный ip и доступ в интернет. Также можно использовать две виртуальные машины (Ubuntu), поднятые на одном компьютере. Либо виртуальную машину и основной компьютер (если ОС твоего основного компьютера Ubuntu). Главное, чтобы два хоста находились в одной сети и имели доступ друг к другу.

Далее в заданиях будет использована терминология основной хост и удаленный хост. Нет особой разницы какой ты сделаешь основным, главное чтобы далее ты не путался в формулировках.

```
vboxuser@Ubuntu1:~$ ip a
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 noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d5:0e:f9 brd ff:ff:ff:ff:ff:ff
    inet 10.241.32.125/23 brd 10.241.33.255 scope global dynamic noprefixroute enp0s3
        valid_lft 454sec preferred_lft 454sec
    inet6 fe80::a00:27ff:fed5:ef9/64 scope link
        valid_lft forever preferred_lft forever
```

```
vboxuser1@Ubuntu2:~$ ip a
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 noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:86:0c:53 brd ff:ff:ff:ff:ff:ff
    inet 10.241.32.124/23 brd 10.241.33.255 scope global dynamic noprefixroute enp0s3
        valid_lft 459sec preferred_lft 459sec
    inet6 fe80::a00:27ff:fe86:c53/64 scope link
        valid_lft forever preferred_lft forever
```

2. Проверь доступность интернета на основном хосте, воспользовавшись командой ping. Для этого нужно пропинговать доверенный адрес в интернете, который точно будет доступен (например, google.com). Запиши вывод в файл.

```
vboxuser@Ubuntu1:~$ ping google.com > inetcheck.txt
^Cvboxuser@Ubuntu1:~$ sudo nano inetcheck.txt
[sudo] password for vboxuser:
```

```
GNU nano 7.2                                inetcheck.txt
PING google.com (142.250.203.142) 56(84) bytes of data.
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=1 ttl=109 time=22.7 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=2 ttl=109 time=34.1 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=3 ttl=109 time=35.6 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=4 ttl=109 time=37.5 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=5 ttl=109 time=34.7 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=6 ttl=109 time=34.2 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=7 ttl=109 time=23.7 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=8 ttl=109 time=34.7 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=9 ttl=109 time=35.6 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=10 ttl=109 time=33.2 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=11 ttl=109 time=36.8 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=12 ttl=109 time=34.1 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=13 ttl=109 time=35.8 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=14 ttl=109 time=36.3 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=15 ttl=109 time=36.3 ms

--- google.com ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14031ms
rtt min/avg/max/mdev = 22.745/33.685/37.531/4.265 ms
```

3. Выполни команду `tracert` до доверенного адреса в интернете, который точно будет доступен (например, `google.com`). Изучи вывод команды. Запиши вывод в файл.

```
vboxuser@Ubuntu1:~$ tracert google.com > inetcheck2.txt
vboxuser@Ubuntu1:~$ sudo nano inetcheck2.txt
```

```
GNU nano 7.2                                inetcheck2.txt
tracert to google.com (172.217.16.46), 30 hops max, 60 byte packets
 1 _gateway (10.241.32.1)  2.901 ms  2.828 ms  2.797 ms
 2 10.131.10.1 (10.131.10.1)  21.003 ms  20.931 ms  20.897 ms
 3 10.63.139.105 (10.63.139.105)  22.456 ms  22.426 ms  21.763 ms
 4 146.59.86.1 (146.59.86.1)  22.302 ms  22.266 ms  22.218 ms
 5 192.168.143.254 (192.168.143.254)  22.180 ms  22.149 ms  22.629 ms
 6 10.13.31.126 (10.13.31.126)  22.574 ms  21.618 ms  22.453 ms
 7 10.13.26.160 (10.13.26.160)  21.533 ms  22.271 ms  10.13.26.158 (10.13.26.158)  21.711 ms
 8 10.13.49.58 (10.13.49.58)  21.677 ms  22.754 ms  10.13.26.186 (10.13.26.186)  22.728 ms
 9 10.73.24.204 (10.73.24.204)  22.088 ms  10.73.24.210 (10.73.24.210)  22.062 ms  10.73.24.208 (10.73.24.208)  22.035 ms
10 10.73.248.196 (10.73.248.196)  23.432 ms  23.398 ms  23.371 ms
11 be101.waw-atm-sbb1-nc5.pl.eu (213.186.32.202)  23.317 ms waw-wa2-sbb1-nc5.pl.eu (91.121.131.150)  23.276 ms be101.waw-atm-sbb1-nc5.pl.eu (213.186.32.202)  23.317 ms
12 10.200.0.93 (10.200.0.93)  25.474 ms 10.200.0.91 (10.200.0.91)  25.446 ms 10.200.0.87 (10.200.0.87)  22.791 ms
13 * * *
14 192.178.97.13 (192.178.97.13)  22.597 ms 192.178.96.241 (192.178.96.241)  25.485 ms 192.178.97.15 (192.178.97.15)  22.771 ms
15 216.239.41.133 (216.239.41.133)  23.257 ms 74.125.251.103 (74.125.251.103)  23.743 ms 216.239.41.133 (216.239.41.133)  23.257 ms
16 muc03s08-in-f46.1e100.net (172.217.16.46)  22.948 ms 23.629 ms 22.771 ms
```

4. Узнай IP-адрес основного и удаленного хостов. Посмотри какие сетевые интерфейсы у тебя используются.

```
vboxuser1@Ubuntu1:~$ ip a
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 noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d5:0e:f9 brd ff:ff:ff:ff:ff:ff
    inet 10.241.32.125/23 brd 10.241.33.255 scope global dynamic noprefixroute enp0s3
        valid_lft 413sec preferred_lft 413sec
    inet6 fe80::a00:27ff:fed5:ef9/64 scope link
        valid_lft forever preferred_lft forever
```

```
vboxuser1@Ubuntu2:~$ ip a
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 noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:86:0c:53 brd ff:ff:ff:ff:ff:ff
    inet 10.241.32.124/23 brd 10.241.33.255 scope global dynamic noprefixroute enp0s3
        valid_lft 412sec preferred_lft 412sec
    inet6 fe80::a00:27ff:fe86:c53/64 scope link
        valid_lft forever preferred_lft forever
```

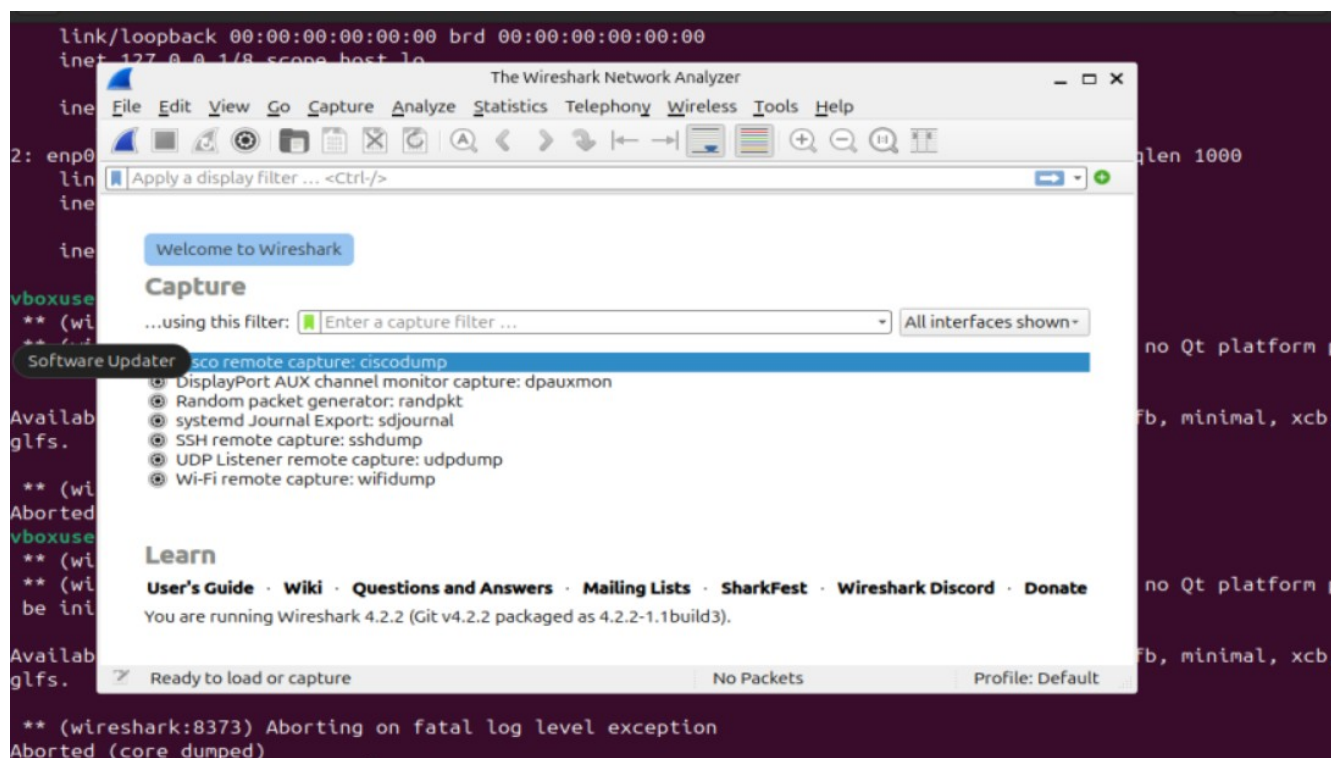
Enp0s3 и lo

5. Проверь статус межсетевого экрана на удаленном хосте. Используй команду "sudo ufw status". В случае если он включен, отключи его.

```
vboxuser1@Ubuntu2:~$ sudo ufw status
Status: inactive
vboxuser1@Ubuntu2:~$
```

6. Установи себе на основной хост wireshark. Запусти его, ознакомься с интерфейсом.





7. Установи на удаленный хост telnet и подключись по telnet с основного к локальному хосту (в случае с AWS тебе необходимо будет создать нового юзера на удаленном хосте под кредами которого ты будешь подключаться).

```
root@Ubuntu1:~# telnet 10.241.32.124
Trying 10.241.32.124...
Connected to 10.241.32.124.
Escape character is '^]'.

Linux 6.14.0-28-generic (Ubuntu2) (pts/3)

Ubuntu2 login: vboxuser
Login timed out after 60 seconds.
Connection closed by foreign host.
root@Ubuntu1:~# telnet 10.241.32.124
Trying 10.241.32.124...
Connected to 10.241.32.124.
Escape character is '^]'.

Linux 6.14.0-28-generic (Ubuntu2) (pts/3)

Ubuntu2 login: vboxuser
Password:

Login incorrect
Ubuntu2 login: vboxuser1
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.
```

8. Запусти Wireshark на основном хосте. При запущенном Wireshark введи команду "uname -a" в терминале с открытой telnet сессией. Отыщи информацию передаваемую по telnet протоколу в wireshark. Проанализируй что ты видишь.

```
telnet: Unable to connect to remote host: Connection refused
vboxuser@Ubuntu1:~$ telnet 10.241.32.124
Trying 10.241.32.124...
Connected to 10.241.32.124.
Escape character is '^]'.

Linux 6.14.0-28-generic (Ubuntu2) (pts/1)

Ubuntu2 login: vboxuser1
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

8 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

vboxuser1@Ubuntu2:~$ hi
Command 'hi' not found, but can be installed with:
sudo snap install hi
vboxuser1@Ubuntu2:~$
```

Ubuntu2 [Running] - Oracle VirtualBox

Aug 21 09:05

Capturing from enp0s3

vboxuser1@Ubuntu2:~\$ wireshark  
vboxuser1@Ubuntu2:~\$ wireshark  
umane -a  
^C  
vboxuser1@Ubuntu2:~\$ wireshark  
\*\* (wireshark:3022) 09:03:40.000000 10.241.32.125 → 10.241.32.124 TCP 66 43050 → 23 [ACK] Seq=312123123 Win=0 Len=0  
ss: Permission denied", "(  
Help \*\* (wireshark:3022) 09:03:40.000000 10.241.32.125 → 10.241.32.124 TELNET 67 Telnet Data .  
\*\* (wireshark:3022) 09:03:40.000000 10.241.32.125 → 10.241.32.124 TELNET 67 Telnet Data .  
\*\* (wireshark:3022) 09:03:40.000000 10.241.32.125 → 10.241.32.124 TCP 66 43050 → 23 [ACK] Seq=312123123 Win=0 Len=0  
ss: Permission denied", "(  
\*\* (wireshark:3022) 09:03:40.000000 10.241.32.125 → 10.241.32.124 MDNS 87 Standard query response  
\*\* (wireshark:3022) 09:03:40.000000 10.241.32.125 → 10.241.32.124 MDNS 107 Standard query response  
ipe: \*\* (udpdump:3072) 09:03:40.000000 Routerboardc\_c1:c1::1 → PCSSystemtec\_d5:0e:... ARP 60 10.241.32.1 i  
put file: Interrupted syst  
vboxuser1@Ubuntu2:~\$ sudo  
[sudo] password for vboxuser1:  
\*\* (wireshark:3090) 09:03:40.000000 Ubiquiti\_e8:b8:43 (70:a7:4) LLDP Multicast 159 MA/70:a7:41:e  
me-root'  
\*\* (wireshark:3090) 09:03:40.000000 10.241.32.125 → 10.241.32.124 TELNET 67 Telnet Data .  
\*\* (wireshark:3090) 09:03:40.000000 10.241.32.125 → 10.241.32.124 TELNET 78 Telnet Data .  
\*\* (wireshark:3090) 09:03:40.000000 10.241.32.125 → 10.241.32.124 TCP 66 43050 → 23 [ACK] Seq=312123123 Win=0 Len=0  
\*\* (wireshark:3090) 09:03:40.000000 10.241.32.125 → 10.241.32.124 TELNET 140 Telnet Data .  
\*\* (wireshark:3090) 09:03:40.000000 10.241.32.125 → 10.241.32.124 TCP 66 43050 → 23 [ACK] Seq=312123123 Win=0 Len=0  
\*\* (wireshark:3090) 09:03:40.000000 10.241.32.125 → 10.241.32.124 TELNET 146 Telnet Data .  
\*\* (wireshark:3090) 09:03:40.000000 10.241.32.125 → 10.241.32.124 TCP 66 43050 → 23 [ACK] Seq=312123123 Win=0 Len=0

9. Выключи или удали telnet на удаленном хосте.

```
vboxuser1@Ubuntu2:~$ sudo systemctl stop xinetd
vboxuser1@Ubuntu2:~$ sudo systemctl status xinetd
○ xinetd.service - Xinetd A Powerful Replacement For Inetd
   Loaded: loaded (/usr/lib/systemd/system/xinetd.service; enabled; preset: enabled)
   Active: inactive (dead) since Thu 2025-08-21 09:11:00 UTC; 5s ago
     Duration: 27min 55.772s
    Docs: man:xinetd
          man:xinetd.conf
          man:xinetd.log
   Process: 1039 ExecStart=/usr/sbin/xinetd -stayalive -dontfork (code=exited, status=0/SUCCESS)
   Main PID: 1039 (code=exited, status=0/SUCCESS)
      CPU: 224ms

Aug 21 08:43:05 Ubuntu2 xinetd[1039]: Reading included configuration file: /etc/xinetd.d/time-udp [file=/etc/xinetd.d/t
Aug 21 08:43:05 Ubuntu2 xinetd[1039]: 2.3.15.4 started with libwrap loadavg labeled-networking options compiled in.
Aug 21 08:43:05 Ubuntu2 xinetd[1039]: Started working: 1 available service
Aug 21 09:02:36 Ubuntu2 login[2936]: PAM unable to dlopen(pam_lastlog.so): /usr/lib/security/pam_lastlog.so: cannot ope
Aug 21 09:02:36 Ubuntu2 login[2936]: PAM adding faulty module: pam_lastlog.so
Aug 21 09:02:43 Ubuntu2 login[2936]: pam_unix(login:session): session opened for user vboxuser1(uid=1000) by vboxuser1(
Aug 21 09:11:00 Ubuntu2 xinetd[1039]: Exiting...
Aug 21 09:11:00 Ubuntu2 systemd[1]: Stopping xinetd.service - Xinetd A Powerful Replacement For Inetd...
Aug 21 09:11:00 Ubuntu2 systemd[1]: xinetd.service: Deactivated successfully.
Aug 21 09:11:00 Ubuntu2 systemd[1]: Stopped xinetd.service - Xinetd A Powerful Replacement For Inetd.
lines 1-21/21 (END)
```

10. Далее повтори то же самое, однако для подключения к удаленному хосту используя ssh. Сравни результаты анализа. Запиши свои выводы (логические выводы) в файл.



```
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

8 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

vboxuser1@Ubuntu2:~$ exit
logout
Connection to 10.241.32.124 closed.
vboxuser1@Ubuntu1:~/.ssh$ ssh vboxuser1@10.241.32.124
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

8 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Thu Aug 21 09:26:20 2025 from 10.241.32.125
vboxuser1@Ubuntu2:~$
```

Ubuntu2 [Running] - Oracle VirtualBox

Aug 21 09:27

vboxuser1@Ubuntu2: ~

Loaded: loaded (/usr/lib/systemd/systemd)
Active: inactive (dead)
TriggeredBy: ● ssh.socket
Docs: man:sshd(8)
man:sshd\_config.5

vboxuser1@Ubuntu2:~\$ sudo

vboxuser1@Ubuntu2:~\$ sudo

● ssh.service - OpenSSH

Loaded: loaded (/usr/lib/systemd/systemd)
Active: active (running)
TriggeredBy: ● ssh.socket
Docs: man:sshd(8)
man:sshd\_config.5

Process: 3938 ExecStart=
Main PID: 3940 (sshd)
Tasks: 1 (limit: 4)
Memory: 1.2M (peak)
CPU: 16ms
CGroup: /system.slice/systemd
└─3940 "sshd"

Aug 21 09:22:17 Ubuntu2:
Aug 21 09:22:17 Ubuntu2:
Aug 21 09:22:17 Ubuntu2:
Aug 21 09:22:17 Ubuntu2:
vboxuser1@Ubuntu2:~\$ sudo
\*\* (wireshark:4106) 09:
me-root'
\*\* (wireshark:4106) 09:
\*\* (wireshark:4106) 09:
\*\* (wireshark:4106) 09:

Capturing from enp0s3

No.	Time	Source	Destination	Protocol	Length	Info
59	10.643648967	10.241.32.125	10.241.32.124	SSHv2	1310	Client:
60	10.653439943	10.241.32.124	10.241.32.125	SSHv2	94	Server:
61	10.653984081	10.241.32.125	10.241.32.124	SSHv2	178	Client:
62	10.694266361	10.241.32.124	10.241.32.125	TCP	66	22 → 38514 [A
63	10.704832689	10.241.32.124	10.241.32.125	SSHv2	842	Server:
64	10.766914641	10.241.32.125	10.241.32.124	TCP	66	38514 → 22 [A
65	10.766965186	10.241.32.124	10.241.32.125	SSHv2	258	Server:
66	10.767316693	10.241.32.125	10.241.32.124	TCP	66	38514 → 22 [A
67	10.767509123	10.241.32.125	10.241.32.124	SSHv2	526	Client:
68	10.767528680	10.241.32.124	10.241.32.125	TCP	66	22 → 38514 [A
69	10.768958094	10.241.32.124	10.241.32.125	SSHv2	174	Server:
70	10.769126419	10.241.32.124	10.241.32.125	SSHv2	614	Server:
71	10.769341051	10.241.32.125	10.241.32.124	TCP	66	38514 → 22 [A
72	10.797622479	10.241.32.124	10.241.32.125	SSHv2	182	Server:
73	10.840953322	10.241.32.125	10.241.32.124	TCP	66	38514 → 22 [A

/tmp/runti

Поменялся протокол передачи данных и роляет то что ssh передает encrypted packet что является более безопасным способом подключения не в локальной сети и убирает возможность перехватить наш трафик как в telnet

11. Включи ufw и настрой запрет на подключение по 22 порту на удаленном хосте. Попробуй подключиться с основного хоста к удаленному по ssh.

The screenshot shows a terminal window with the following commands and output:

```
vboxuser@Ubuntu1:~$ ssh vboxuser1@10.241.32.124
^C
vboxuser@Ubuntu1:~$ ssh vboxuser1@10.241.32.124
^C
vboxuser@Ubuntu1:~$ ssh vboxuser1@10.241.32.124
^C
vboxuser@Ubuntu1:~$ ssh vboxuser1@10.241.32.124 >test.log
```

Below the terminal window, a packet capture window titled "Capturing from enp0s3" is open. It shows a list of captured packets with columns for Source, Destination, Protocol, Length, and Info. The packets include LLDP Multicast, TCP Retransmission, ARP, and MDNS. The packet list is as follows:

No.	Source	Destination	Protocol	Length	Info
10862639	Ubiquiti e8:b8:43	LLDP Multicast	LLDP	159	MA/70:a7:41:e8:b8:41 MA/70:a7:41:e8:b8:41
109260602	10.241.32.125	10.241.32.124	TCP	74	[TCP Retransmission] 57600 → 22 [SYN] Seq=0
59177974	10.241.32.125	10.241.32.124	TCP	74	[TCP Retransmission] 57600 → 22 [SYN] Seq=0
18689718	Routerboardc_c1:c1:...	PCSSystemtec_d5:0e:...	ARP	60	10.241.32.1 is at 2c:c8:1b:c1:a4
137852623	10.241.32.125	10.241.32.124	TCP	74	[TCP Retransmission] 57600 → 22 [SYN] Seq=0
97926293	Routerboardc_c1:c1:...	Broadcast	ARP	60	who has 10.241.32.201? Tell 10.241.32.1
11930049	Ubiquiti e8:b8:43	LLDP Multicast	LLDP	159	MA/70:a7:41:e8:b8:41 MA/70:a7:41:e8:b8:41
108850997	10.241.32.125	10.241.32.124	TCP	74	[TCP Retransmission] 57600 → 22 [SYN] Seq=0
13785364	10.241.32.125	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ipp._tcp.local
13786265	fe80::a00:27ff:fed5::...	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local
20960906	10.241.32.125	10.241.32.124	TCP	74	34154 → 22 [SYN] Seq=0 Win=64240 Len=0
136139315	10.241.32.125	10.241.32.124	TCP	74	[TCP Retransmission] 34154 → 22 [SYN] Seq=0
40708627	PCSSystemtec_d5:0e:...	PCSSystemtec_86:0c:...	ARP	60	who has 10.241.32.124? Tell 10.241.32.1
40729105	PCSSystemtec_86:0c:...	PCSSystemtec_d5:0e:...	ARP	42	10.241.32.124 is at 08:00:27:86:0c:53
100000000	10.241.32.125	10.241.32.124	TCP	74	[TCP Retransmission] 34154 → 22 [SYN] Seq=0

The packet details for the first packet (Frame 1) are shown below:

```
Frame 1: 70 bytes on wire (560 bits), 70 byte captured (560 bits) on interface enp0s3
Ethernet II, Src: PCSSystemtec_d5:0e:f9:08, Dst: PCSSystemtec_86:0c:53:00
Internet Protocol Version 6, Src: fe80::a00:27ff:fed5::..., Dst: ff02::fb
Internet Control Message Protocol v6
```



12. Скачай nmap на основной хост и сделай полное сканирование удаленного хоста. На удаленном хосте введи команду "sudo ss -tuln". Запиши оба вывода в файл. Проанализируй сходство обоих выводов.

```
vboxuser@Ubuntu1:~$ sudo nmap -A -T4 10.241.32.124 full_scan1.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-21 10:29 UTC
Failed to resolve "full_scan1.txt".
Failed to resolve "full_scan1.txt".
Nmap scan report for 10.241.32.124
Host is up (0.00046s latency).
All 1000 scanned ports on 10.241.32.124 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:86:0C:53 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.46 ms 10.241.32.124

Failed to resolve "full_scan1.txt".
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.05 seconds
```

```
vboxuser1@Ubuntu2:~$ sudo ss -tuln
```

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Pr
udp	UNCONN	0	0	0.0.0.0:5353	0.0.0.0:*	
udp	UNCONN	0	0	0.0.0.0:44658	0.0.0.0:*	
udp	UNCONN	0	0	127.0.0.54:53	0.0.0.0:*	
udp	UNCONN	0	0	127.0.0.53%lo:53	0.0.0.0:*	
udp	UNCONN	0	0	:::5353	:::*	
udp	UNCONN	0	0	:::41228	:::*	
tcp	LISTEN	0	4096	127.0.0.54:53	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.1:631	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.53%lo:53	0.0.0.0:*	
tcp	LISTEN	0	4096	0.0.0.0:22	0.0.0.0:*	
tcp	LISTEN	0	4096	:::22	:::*	
tcp	LISTEN	0	4096	:::1:631	:::*	

Ss проверяет изнутри сокет а nmap работает как внешний клиент который подключается к хосту