

## **Тема и цель работы**

Тема: Настройка Telnet и SSH. Перехват трафика средствами Wireshark.

Цель: научиться устанавливать, проводить удаленное подключение по SSH и Telnet, следить за трафиком через Wireshark.

## Оборудование, ПО

Таблица 1 – Информация об оборудовании

Устройство	Операционная система	IP адрес/Маска	Шлюз	DNS
CLI_A1	Astra Linux SE 1.8.1	10.0.0.1/24	-	-
CLI_A2	Astra Linux SE 1.8.1	10.0.2.15/24	-	-

## Выполнение лабораторной работы

1. Все действия выполняются на двух виртуальных машинах. Для того, чтобы настроить на машинах дополнительно выход в интернет, необходимо включить второй адаптер с NAT. Зайдём в «Настройки» виртуальной машины.

В настройках «Сети» необходимо включить второй адаптер с типом подключения NAT.

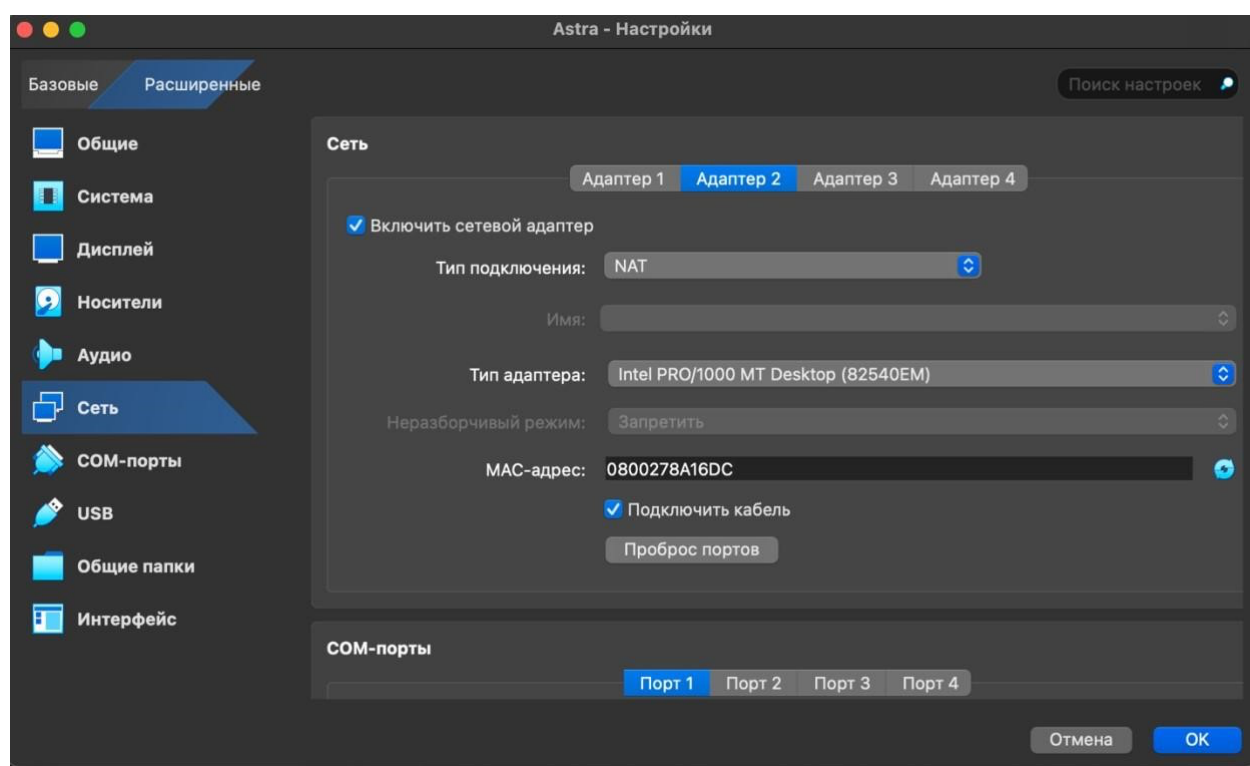


Рисунок 1 – Подключение второго адаптера NAT

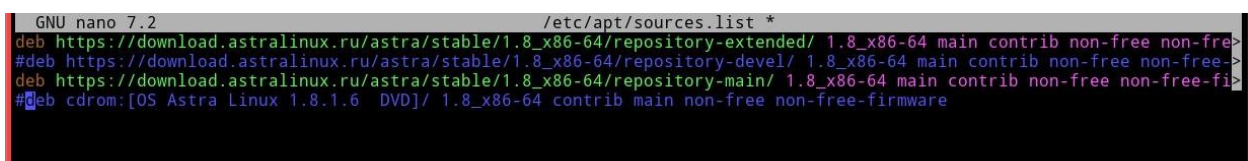
2. В `/etc/network/interfaces` необходимо добавить следующие строки:

```
auto enp0s8
iface enp0s8 inet dhcp
```

Рисунок 2 - Сетевая настройка `enp0s8` при помощи `dhcp`

3. Telnet - это сетевая утилита, которая позволяет соединиться с удаленным портом любого компьютера и установить интерактивный канал связи,

например, для передачи команд или получения информации. Протокол работает на основе TCP, и позволяет передавать обычные строковые команды на другое устройство. Он может использоваться не только для ручного управления, но и для взаимодействия между процессами. Перед установкой необходимо отредактировать файл `/etc/apt/sources.list`, чтобы разрешить производить установку с сайтов.



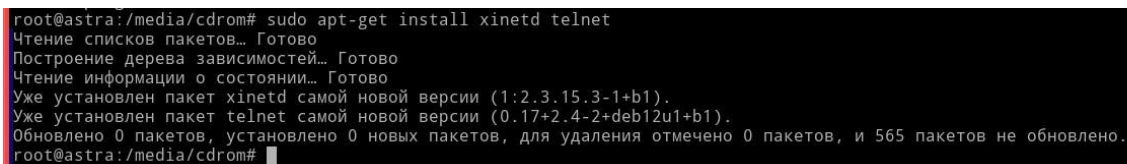
```
GNU nano 7.2 /etc/apt/sources.list *
deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-extended/ 1.8_x86-64 main contrib non-free non-free-firmware
#deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-devel/ 1.8_x86-64 main contrib non-free non-free-firmware
deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-main/ 1.8_x86-64 main contrib non-free non-free-firmware
#deb cdrom:[OS Astra Linux 1.8.1.6 DVD]/ 1.8_x86-64 contrib main non-free non-free-firmware
```

Рисунок 3 – Редактирование файла `/etc/apt/sources.list` для установки с сайтов

4. Для установки Telnet в терминале надо написать следующие строки:

**apt-get update sudo apt-get install**

**xinetd telnet telnetd**



```
root@astra:/media/cdrom# sudo apt-get install xinetd telnet
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Уже установлен пакет xinetd самой новой версии (1:2.3.15.3-1+b1).
Уже установлен пакет telnet самой новой версии (0.17+2.4-2+deb12u1+b1).
Обновлено 0 пакетов, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 565 пакетов не обновлено.
root@astra:/media/cdrom#
```

Рисунок 4 – Установка Telnet

5. Необходимо создать файл `/etc/xinetd.d/telnet` и ввести следующие команды:

**service telnet**

**{**

**disable = no flags =**

**REUSE socket\_type =**

**stream wait = no user = root**

**server =**

**/usr/sbin/telnetd**

**log\_on\_failure += USERID**

**}**

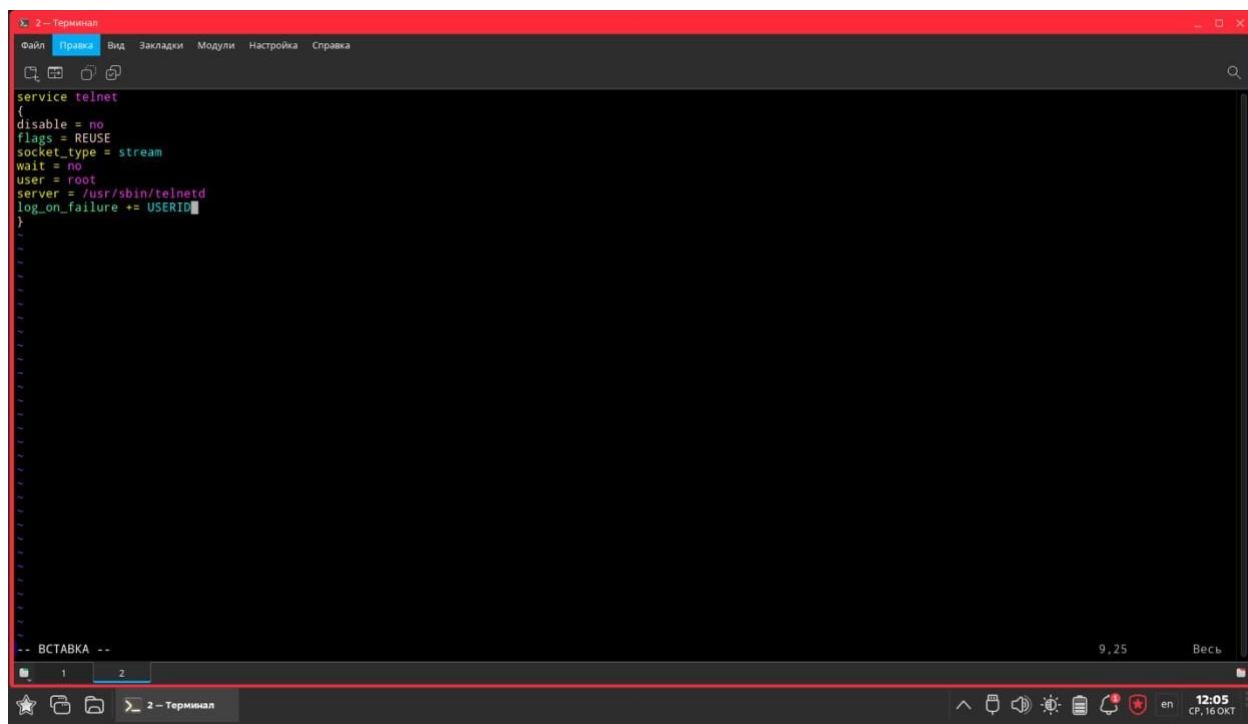


Рисунок 5 – Создание файла /etc/xinetd.d/telnet

6. Далее нужно перезагрузить сервис xinetd и проверить работу telnet при помощи следующих команд: **systemctl restart xinetd telnetd localhost**

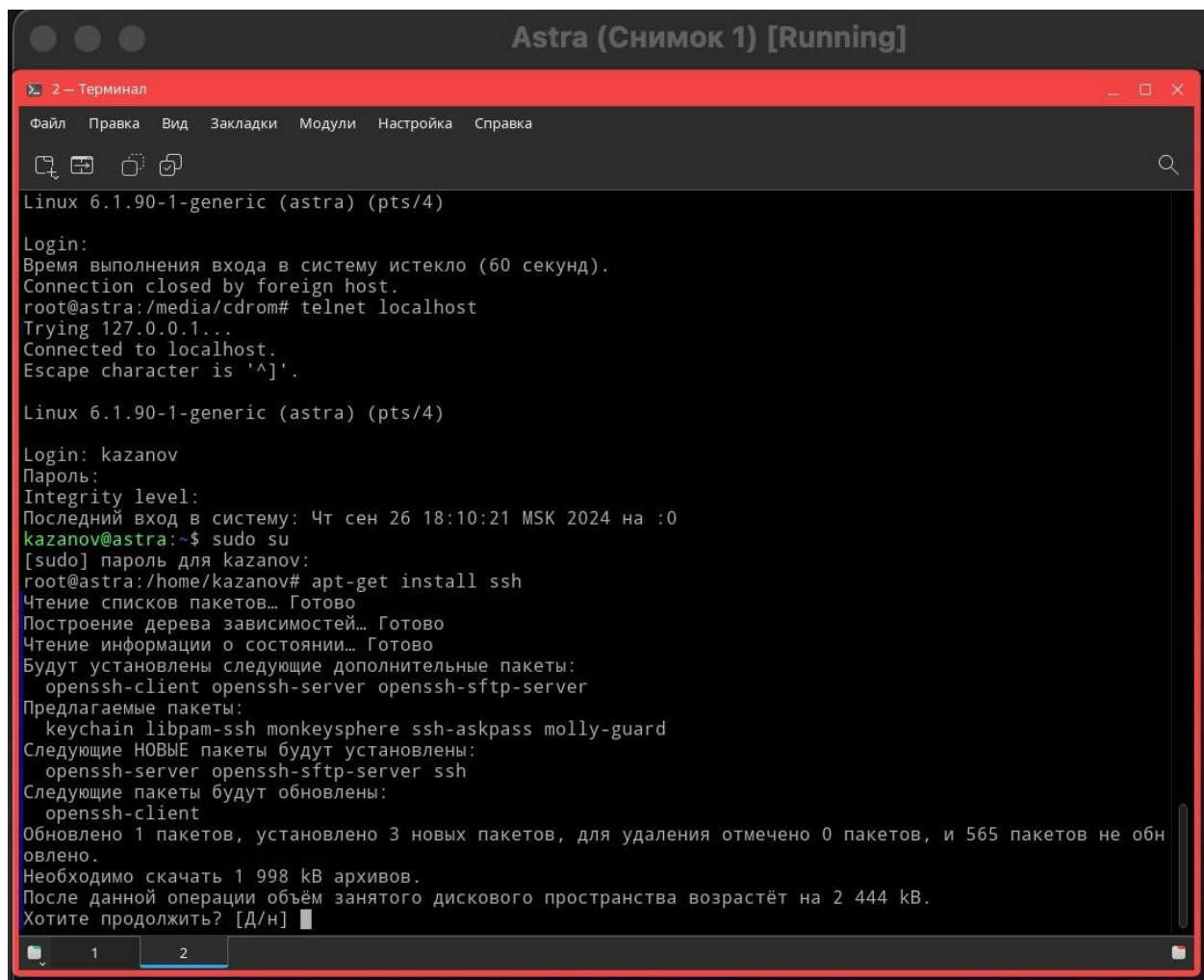
```
root@astra:/media/cdrom# telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Linux 6.1.90-1-generic (astra) (pts/4)
Login: █
```

Рисунок 6 – Проверка работы Telnet

настроен.

7. SSH - (Secure Shell) - это протокол для удалённого доступа к любым устройствам с операционной системой Linux: компьютерам, серверам, телефонам и так далее. Иными словами, это некий набор правил, позволяющий устанавливать соединение с устройством, которое физически расположено в любой точке мира. Для установки нужно использовать команду:



```
Linux 6.1.90-1-generic (astra) (pts/4)
Login:
Время выполнения входа в систему истекло (60 секунд).
Connection closed by foreign host.
root@astra:/media/cdrom# telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Linux 6.1.90-1-generic (astra) (pts/4)
Login: kazanov
Пароль:
Integrity level:
Последний вход в систему: Чт сен 26 18:10:21 MSK 2024 на :0
kazanov@astra:~$ sudo su
[sudo] пароль для kazanov:
root@astra:/home/kazanov# apt-get install ssh
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  openssh-client openssh-server openssh-sftp-server
Предлагаемые пакеты:
  keychain libram-ssh monkeysphere ssh-askpass molly-guard
Следующие НОВЫЕ пакеты будут установлены:
  openssh-server openssh-sftp-server ssh
Следующие пакеты будут обновлены:
  openssh-client
Обновлено 1 пакетов, установлено 3 новых пакетов, для удаления отмечено 0 пакетов, и 565 пакетов не обн
овлено.
Необходимо скачать 1 998 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 2 444 kB.
Хотите продолжить? [Д/н] n
```

**apt-get install ssh**

Рисунок 7 – Установка SSH

8. Необходимо запустить службу SSH и добавить её в автозагрузку при помощи следующих команд: **sudo systemctl start ssh sudo systemctl enable**

**ssh**

А чтобы проверить службу, следует ввести команду:

**systemctl status ssh**

Рисунок 8 – Проверка службы

```
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:2WAs3SQIhUYaHdr3Fu9/DcUKiQKm6dcAvD3cydato8Y root@astra (ED25519)
Created symlink /etc/systemd/system/ssh.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
ssh.socket is a disabled or a static unit, not starting it.
Обрабатываются триггеры для xserver-xorg-core (2:21.1.7-1ubuntu4astra.se28) ...
update exec ids due to /usr/bin changed
Обрабатываются триггеры для ufw (0.36.2-1.astra.se9) ...
Обрабатываются триггеры для man-db (2.11.2-2+b1) ...
Обрабатываются триггеры для parsec-base (3.9+ci118) ...
Настраивается пакет ssh (1:9.6p1-2~deb10u1astra8se5) ...
root@astra:/media/cdrom# sudo systemctl start ssh
root@astra:/media/cdrom# sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
root@astra:/media/cdrom# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Wed 2024-10-16 17:16:09 MSK; 55s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 4054 (sshd)
     Tasks: 1 (limit: 5430)
    Memory: 1.6M
         CPU: 27ms
    CGroup: /system.slice/ssh.service
            └─4054 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

окт 16 17:16:09 astra systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
окт 16 17:16:09 astra sshd[4054]: Server listening on 0.0.0.0 port 22.
окт 16 17:16:09 astra sshd[4054]: Server listening on :: port 22.
окт 16 17:16:09 astra systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
root@astra:/media/cdrom#
```

На первой машине нужно настроить аутентификацию по ключам под учетными записями `alaitsev` на второй машине. Сначала надо сгенерировать ключ: **ssh – keygen**

После необходимо скопировать полученный ключ на вторую машину.

Рисунок 9 – Копирование ключа

```

root@astra:/media/cdrom# ssh-copy-id kazanov@10.0.2.15
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_ed25519.pub"
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:2WAs3SQIhUYaHdR3Fu9/DcUKiQKm6dcAvD3cydato8Y.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
kazanov@10.0.2.15's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'kazanov@10.0.2.15'"
and check to make sure that only the key(s) you wanted were added.

root@astra:/media/cdrom#

```

9. Необходимо провести попытку подключения к astra-2 по SSH и создать там файл при помощи следующих команд: **ssh user@10.0.2.15 touch file.txt**

```

root@astra:/media/cdrom# ssh kazanov@10.0.2.15
Last login: Wed Oct 16 22:18:19 2024
kazanov@astra:~$ touch file.txt
kazanov@astra:~$ exit
ВЫХОД
Connection to 10.0.2.15 closed.
root@astra:/media/cdrom#

```

Рисунок 10 – Подключение к astra-2 по SSH и создание файла

10. Для проверки нужно зайти на вторую виртуальную машину и проверить список файлов.
11. Wireshark - это мощный сетевой анализатор, который может использоваться для анализа трафика, проходящего через сетевой интерфейс вашего компьютера. Он может понадобиться для обнаружения и решения проблем



с сетью, отладки ваших веб-приложений, сетевых программ или сайтов.

Wireshark позволяет полностью просматривать содержимое пакета на всех

```
root@astra:/media/cdrom# apt-get install wireshark
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  libbcb729-0 libc-ares2 liblua5.2-0 libsmi2ldbl libwireshark-data libwireshark16 libwiretap13 libwsutil14
  wireshark-common wireshark-qt
Предлагаемые пакеты:
  snmp-mibs-downloader geoipupdate geoip-database geoip-database-extra libjs-leaflet libjs-leaflet.markercluster
  wireshark-doc
Следующие НОВЫЕ пакеты будут установлены:
  libbcb729-0 libc-ares2 liblua5.2-0 libsmi2ldbl libwireshark-data libwireshark16 libwiretap13 libwsutil14 wireshark
  wireshark-common wireshark-qt
Обновлено 0 пакетов, установлено 11 новых пакетов, для удаления отмечено 0 пакетов, и 565 пакетов не обновлено.
Необходимо скачать 24,9 МВ архивов.
После данной операции объем занятого дискового пространства возрастёт на 134 МВ.
Хотите продолжить? [Д/н]
```

уровнях: так вы сможете лучше понять как работает сеть на низком уровне.

Для его установки используем команду: **apt-get install wireshark**

```
root@astra:/media/cdrom# chmod +x /usr/bin/dumpcap
root@astra:/media/cdrom# wireshark
** (wireshark:10139) 14:04:56.578242 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runti
me-root'
```

Рисунок 11 – Установка Wireshark

Во время установки нужно выбрать «Да» при настройке Wireshark.

12. Для работы необходимо выдать права на выполнение: **chmod +x /usr/bin/dumpcap**

Рисунок 12 – Выдача прав на выполнение

Следом уже необходимо запустить **wireshark** для проверки работы при помощи терминала командой: **Wireshark**

Нужно выбрать **enr0s3**, чтобы следить за его трафиком

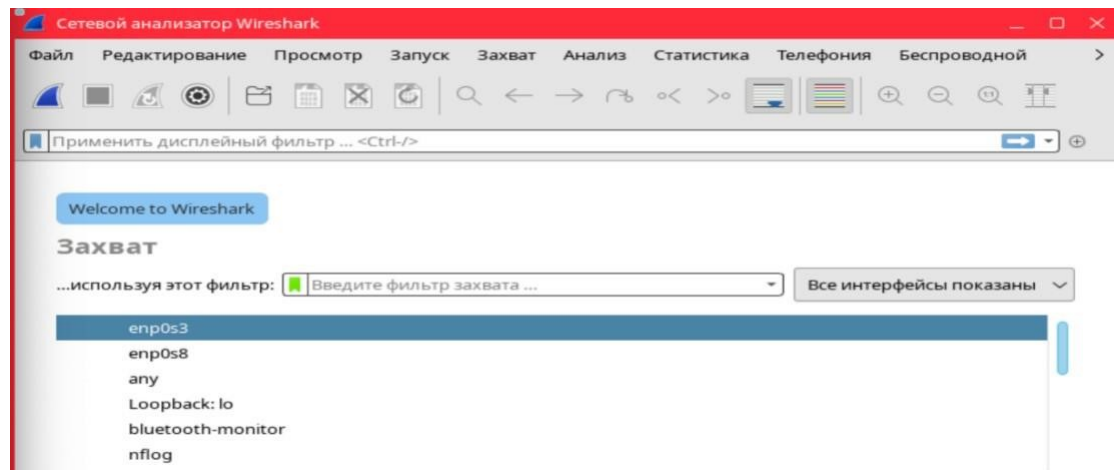


Рисунок 13 – Выбор enp0s3 в Wireshark

13. Чтобы проверить работу Wireshark, нужно произвести пинг второй машины.

При просмотре wireshark обнаружены передачи пакетов между машинами,

значит,

wireshark

работает.

61	18.503375913	10.0.0.7	10.0.0.11	ICMP	98 Echo (ping) reque
62	18.504748227	10.0.0.11	10.0.0.7	ICMP	98 Echo (ping) reply
63	19.506222227	10.0.0.7	10.0.0.11	ICMP	98 Echo (ping) reque
64	19.507569588	10.0.0.11	10.0.0.7	ICMP	98 Echo (ping) reply
65	20.507686607	10.0.0.7	10.0.0.11	ICMP	98 Echo (ping) reque
66	20.509163873	10.0.0.11	10.0.0.7	ICMP	98 Echo (ping) reply
67	21.510324777	10.0.0.7	10.0.0.11	ICMP	98 Echo (ping) reque
68	21.511472003	10.0.0.11	10.0.0.7	ICMP	98 Echo (ping) reply
69	22.512240783	10.0.0.7	10.0.0.11	ICMP	98 Echo (ping) reque
70	22.513978160	10.0.0.11	10.0.0.7	ICMP	98 Echo (ping) reply
71	23.513737070	10.0.0.7	10.0.0.11	ICMP	98 Echo (ping) reque
72	23.514370241	10.0.0.11	10.0.0.7	ICMP	98 Echo (ping) reply

Рисунок 14 – Проверка передачи пакетов в Wireshark

## **Вывод**

В ходе лабораторной работы были установлены Telnet, SSH и Wireshark, проведены удаленные подключения от одной виртуальной машины к другой при помощи SSH и Telnet и создан удаленно файл. Также произведен пинг второй машины, и при помощи wireshark отследили передачи пакетов между машинами.

## **Контрольные вопросы**

### **1. Для чего используется Telnet?**

Telnet - это сетевая утилита, которая позволяет соединиться с удаленным портом любого компьютера и установить интерактивный канал связи, например, для передачи команд или получения информации. Протокол работает на основе TCP, и позволяет передавать обычные строковые команды на другое устройство. Он может использоваться не только для ручного управления, но и для взаимодействия между процессами.

### **2. Для чего используется SSH?**

SSH - (Secure Shell) - это протокол для удалённого доступа к любым устройствам с операционной системой Linux: компьютерам, серверам, телефонам и так далее. Иными словами, это некий набор правил, позволяющий устанавливать соединение с устройством, которое физически расположено в любой точке мира.

### **3. Для чего используется Wireshark?**

Wireshark - это мощный сетевой анализатор, который может использоваться для анализа трафика, проходящего через сетевой интерфейс вашего компьютера. Он может понадобиться для обнаружения и решения проблем с сетью, отладки ваших веб-приложений, сетевых программ или сайтов. Wireshark позволяет полностью просматривать содержимое пакета на всех уровнях: так вы сможете лучше понять как работает сеть на низком уровне.