**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ**

A logo of a triangle

Description automatically generated**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛИПЕЦКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

|  |  |
| --- | --- |
| Институт | компьютерных наук |
| Кафедра | автоматизированных систем управления |

ЛАБОРАТОРНАЯ РАБОТА №6

По дисциплине "Операционные системы Linux"

На тему "Работа с SSH"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Студент | ПИ-22-1 | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | Первеева Е. Ю. |
| Руководитель | |  |  |  |
| канд.техн.наук, доцент  ученая степень, ученое звание | |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | Кургасов В.В. |

Липецк, 2024 г.

**Оглавление**

[**Цель работы 3**](#_Toc187448487)

[**Ход работы 4**](#_Toc187448488)

[**1. SSH 4**](#_Toc187448489)

[**2. Telnet 9**](#_Toc187448490)

[**Вывод 11**](#_Toc187448491)

[**Контрольные вопросы 12**](#_Toc187448492)

# **Цель работы**

Практическое ознакомление с программным обеспечением удаленного доступа к распределенным системам обработки данных.

# **Ход работы**

## **1. SSH**

Сначала добавим через настройки сетевое соединение между основной системой и виртуальной машинами в VirtualBox посредством сетевого моста. Далее определим IP-адрес виртуальной машины с помощью команды ip addr, IP-адрес = 192.168.43.19. Для проверки доступности виртуальной машины из хостовой выполнена команда ping. Успешный результат выполнения команды, представленный на рисунке 1, подтверждает корректность сетевых настроек.

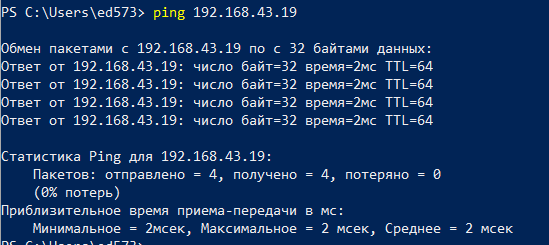


Рисунок 1 - Проверка соединения

Установим SSH при помощи команд:

sudo apt update

sudo apt install -y openssh-server

Проверим статус SSH-сервиса, результат представлен на рисунке 2:

sudo systemctl status ssh

Если сервис не запущен, активируем его:

sudo systemctl start ssh

sudo systemctl enable ssh

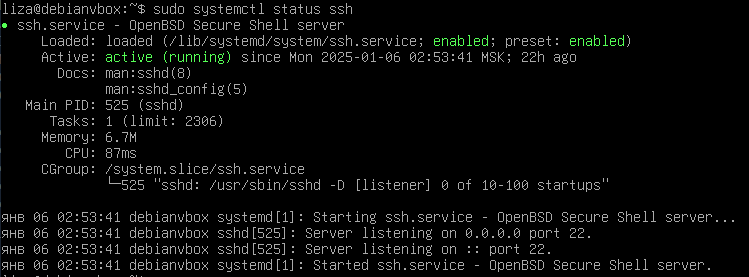


Рисунок 2– SSH-сервер

Создадим пару ключей SSH: открытый и закрытый, при помощи команды: ssh-keygen -t rsa -b 4096, результат представлен на рисунке 3. Укажем тип ключа (-t rsa) Rivest-Shamir-Adleman, так как он является одним из самых распространённых и поддерживаемых алгоритмов шифрования. Так же определим длину ключа в битах (ключ будет длиной 4096 бит).

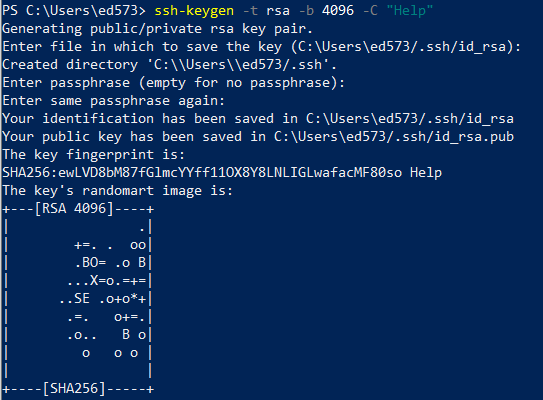


Рисунок 3 - Создание ключей SSH

Далее необходимо передать публичный ключ на гостевую систему при помощи команды: cat ~/.ssh/id\_rsa.pub | ssh user@<ip\_address\_of\_debian> "mkdir -p ~/.ssh && chmod 700 ~/.ssh && cat >> ~/.ssh/authorized\_keys && chmod 600 ~/.ssh/authorized\_keys". Результат представлен на рисунке 4.



Рисунок 4 - Передача публичного ключа на гостевую систему

Теперь для доступа к гостевой системе необходимо будет указать файл ключа, и вход будет осуществлен без пароля. Результат представлен на рисунке 5.

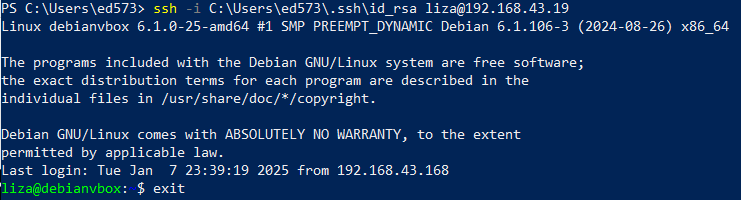


Рисунок 5 - Доступ к гостевой системе без пароля

Настроим зашифрованный туннель через SSH: ssh -L 12345:localhost:22 user@remote\_host. -L — Указывает на настройку локального перенаправления порта (Local port forwarding). 12345:localhost:22 — Параметры перенаправления: 12345 (порт на локальной машине, на который будет перенаправлен трафик). 22 (порт на удалённой системе, к которому подключается туннель (порт SSH)).

Пример передачи файла через зашифрованный туннель представлен на рисунках 6-7.



Рисунок 6 - Передача файла через зашифрованный туннель



Рисунок 7 - Результат передачи файла через зашифрованный туннель

Запустим сессию screen, информация о запущенной сессии представлена на рисунке 8.

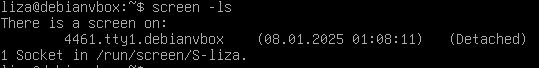


Рисунок 8 - сессии screen

В screen подключимся к основной системе через SSH, пример приведен на рисунке 9.



Рисунок 9 - подключение через SSH в screen

Для анализа сетевого трафика с прослушиванием порта 22 (используемого SSH) запустим tcpdump:

- sudo tcpdump -l -v -nn tcp and src port 22 or dst port 22 | tee ssh.log

На хостовой машине выполним подключение к виртуальной машине через ssh.

Выполним команду uname -a. Все действия представлены на рисунке 10.

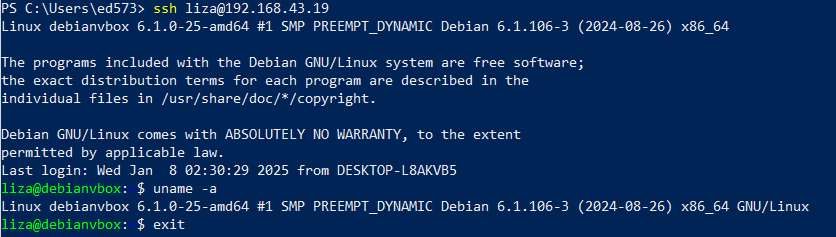


Рисунок 10 - Сессия ssh

Создаем текстовый файл на хостовой машине с названием LR\_6\_test\_file.txt, содержащий ФИО и номер лабораторной работы. Далее передаем его на виртуальную машину с использованием scp: scp -i <ключ> <путь к файлу на хостовой машине> <пользователь>@<IP-адрес виртуальной машины>:<будущее расположение файла> Процесс передачи показан на рисунке 11.



Рисунок 11 - Передача файла по ключу

На рисунке 12 демонстрируется содержимое переданного файла, а также результаты команды ls, подтверждающие его наличие.

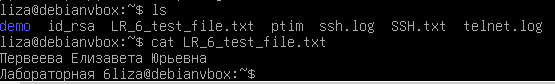


Рисунок 12 - Содержимое переданного файла

После завершения сессии можно остановить анализатор сетевого трафика tcpdump на виртуальной машине и выполнить анализ собранных логов. Для фильтрации пакетов и отображении только пакетов инициализации (S) и завершения соединения (F) применим команду:

- cat ssh.log | grep -P '\[[SF].\*?\]' telnet.log

Результат представлен на рисунке 13.

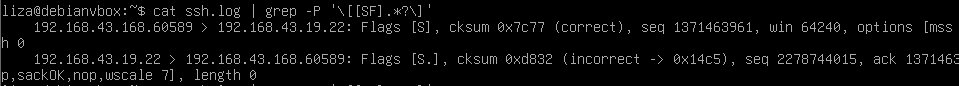


Рисунок 13 - Пакеты инициализации и завершения сессии

Чтобы избежать постоянного указания пути к ключу, создаем файл конфигурации ~/.ssh/config на хостовой машине со следующим содержимым:

Host sicret

HostName 192.168.43.19

User liza

Port 22

IdentityFile C:\Users\ed573\.ssh\id\_rsa

На рисунке 14 показан успешный вход на сервер по ключу, без лишних параметров.

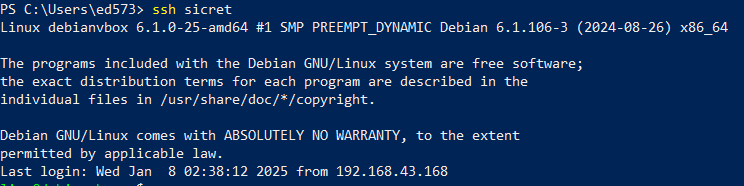


Рисунок 14 – Сессия ssh

## **2. Telnet**

Для работы Telnet необходимо установить inetd, который отвечает за управление сетевыми службами: sudo apt install openbsd-inetd -y

После установки отредактируем конфигурационный файл inetd, изменив строку: telnet stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.telnetd. Это действие позволяет активировать Telnet-сервис.

Убедимся, что порт 23 активен для Telnet, данный результат представлен на рисунке 15. Из вывода команды ss -lt видно, что порт 23 (Telnet) прослушивается и готов к подключениям (0.0.0.0:telnet и [::]:telnet).

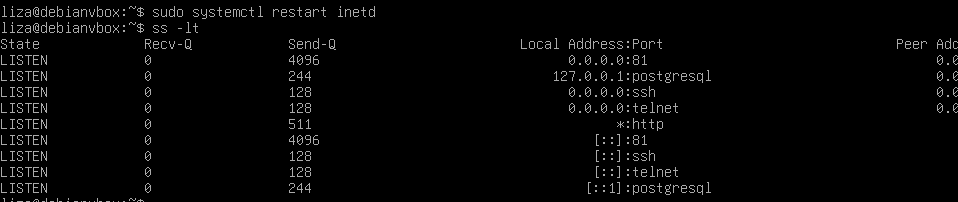


Рисунок 15 - Прослушиваемые порты

На виртуальной машине включаем анализ сетевого трафика с фильтрацией, связанного с портом 23**: sudo tcpdump -l -v -nn tcp and src port 23 or dst port 23 | tee telnet.log**. "-l": вывод в реальном времени. "-v": подробный вывод. "-nn": отключение разрешения имен хостов и служб. - tcp: фильтрация только трафика TCP. - src port 23 or dst port 23: анализ трафика с исходным или целевым портом 23. - tee telnet.log: запись вывода команды в файл telnet.log.

На хостовой машине выполним команду подключения через Telnet: telnet <IP-адрес виртуальной машины>

После успешного подключения была выполнена команда uname -a, результат представлен на рисунке 16.

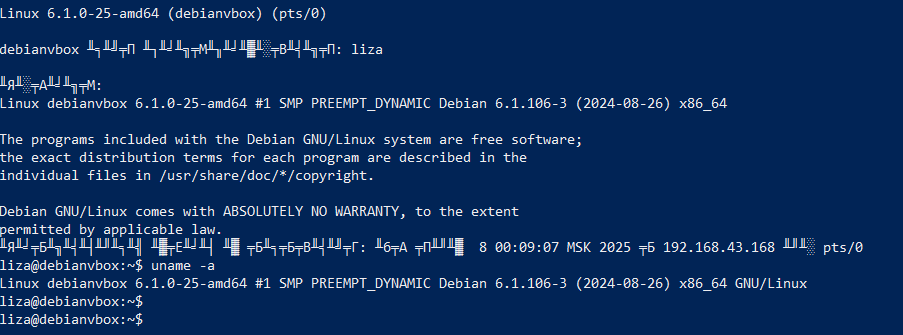


Рисунок 16 - Сессия telnet

После завершения сессии Telnet можно остановить анализатор сетевого трафика tcpdump на виртуальной машине и выполнить анализ собранных логов: cat teltnet.log | grep -P '\[[SF].\*?\]' telnet.log

Результат предоставлен на рисунке 17.

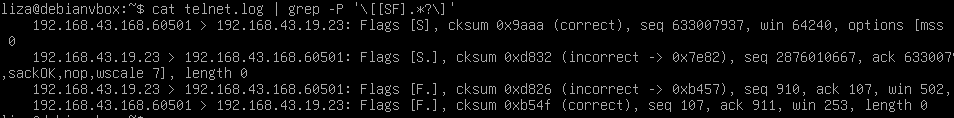


Рисунок 17 - Пакеты инициализации и завершения сессии

# **Вывод**

В ходе выполнения данной лабораторной работы я приобрела навыки работы с программным обеспечением удаленного доступа к распределенным системам обработки данных. Изучила способы авторизации пользователя на удаленном сервере и настройку сервера для приема соединений с пещью программного обеспечения Telnet и SSH.

# **Контрольные вопросы**

**1. Определите основные цели и задачи решаемые с помощью ПО удаленного доступа?**

Основные задачи решаемые с помощью ПО удаленного доступа это возможность удаленного администрирования, управления и технической поддержки серверов и сетевых устройств без физического доступа к ним.

Такие решения позволяют пользователям взаимодействовать с удаленными системами для выполнения рабочих задач, разработки программного обеспечения, управления файлами и данными, а также устранения неисправностей.

**2. Выделите отличительные особенности между режимами работы удаленного доступа по протоколам Telnet и SSH?**

Telnet не использует шифрование, все данные, включая логины и пароли, передаются в открытом виде, что делает протокол уязвимым для перехвата данных. Так же он использует простую аутентификацию с логином и паролем, которые передаются в открытом виде.

В то время как SSH использует шифрование данных. Данные шифруются с использованием криптографических методов, что делает их защищёнными от перехвата. Он поддерживает аутентификацию через логин и пароль, а также аутентификацию по ключам (асимметричные пары ключей), что обеспечивает дополнительный уровень защиты.

**3. Опишите способы установления соединения при использовании протокола SSH? Охарактеризуйте положительные и отрицательные аспекты приведенных методов**

- Установление соединения с использованием логина и пароля: пользователь вводит имя и пароль для подключения, после чего создается защищенный канал связи.

Плюсы: не требует предварительной настройки ключей. работает на всех системах без дополнительных инструментов.

Минусы: если пароль слабый, его легко подобрать, подвержен атакам с перебором паролей (brute-force), неудобство при частом подключении, так как требуется ввод пароля каждый раз.

- Установление соединения с использованием ключевой аутентификации: клиент генерирует пару ключей (приватный и публичный), публичный ключ передается серверу для авторизации. Если клиент предоставляет соответствующий приватный ключ, соединение устанавливается. Закрытый ключ остаётся у клиента и используется для подписи.

Плюсы: исключает риск перехвата пароля, сложность подбора ключей делает метод устойчивым к атакам brute-force, удобство при частых подключениях.

Минусы: сложность первоначальной настройки, требуется генерация и установка ключей, риск потери закрытого ключа.

- Установление соединения через туннелирование (Port Forwarding): например, можно перенаправлять порт локального устройства через SSH для безопасного доступа к удалённому ресурсу.

Плюсы: безопасность передачи данных: весь трафик шифруется, можно передавать данные любых протоколов через SSH.

Минусы: сложность настройки: туннели требуют правильной конфигурации, задержки из-за шифрования и маршрутизации трафика.

**4. Основываясь на заданиях лабораторной работы, приведите практический пример использования систем удаленного доступа?**

Примером может служить подключение к виртуальной машине для выполнения системных команд, передачи файлов или настройки сервисов. В лабораторной работе SSH использовался для подключения к Debian, выполнения команд управления системой и передачи текстовых файлов через зашифрованный канал с помощью утилиты scp. Это демонстрирует, как удаленный доступ упрощает взаимодействие с системами без физического присутствия.

**5. Перечислите распространенные сетевые службы, основанные на использовании шифрованного соединения по протоколу SSH? Приведите пример использования службы передачи файлов по безопасному туннелю?**

OpenSSH реализуюет протокол SSH - основная служба, предоставляющая защищённый доступ к удалённым серверам и устройствам для администрирования, содержит утилиты ssh [user@server.com](mailto:user@server.com).

Передача файлов (SCP и SFTP):

- scp (односторонняя передача данных);

- sftp (двусторонний безопасный канал).

Пример использования: scp file.txt [user@192.168.3.40:/home/user/](mailto:user@192.168.3.40:/home/user/)

Туннелирование (Port Forwarding):

Создание защищённых туннелей для передачи данных приложений или проксирования трафика.

ssh -L 8080:localhost:80 user@server.com