МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛИПЕЦКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Институт компьютерных наук

Кафедра автоматизированных систем управления

ЛАБОРАТОРНАЯ РАБОТА №6

по операционным системам Linux

«Работа с SSH»

Студент ПИ-22-1 _____ Пахомов А.А.

подпись, дата

Руководитель

_____ Кургасов В.В.

подпись, дата

Липецк, 2024 г.

Цель работы

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

Ход работы

1. Часть I

Настроим для нашей виртуальной машины сетевой мост (рис. 1).

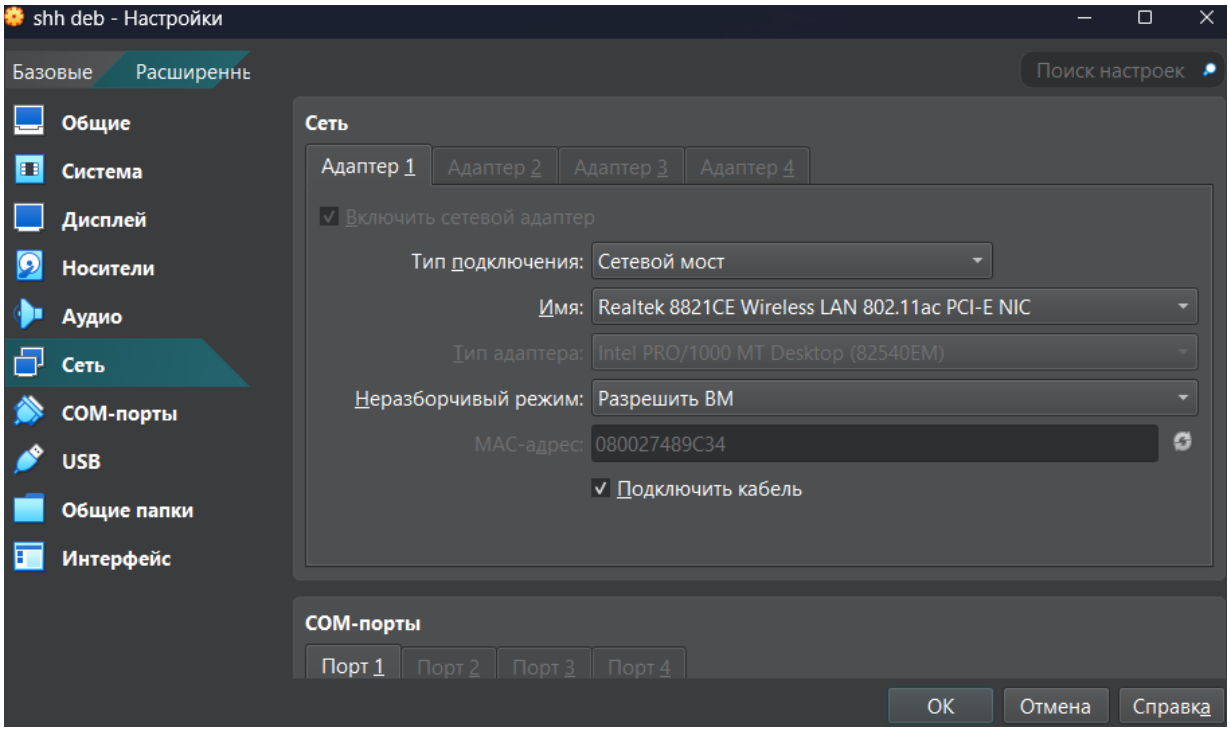

Рисунок 1 – Настройка сетевого подключения

Узнаем ip-адрес виртуальной машины и проверим с помощью команды ping на хостовой системе проверим подключение (рис. 2).

```
PS C:\Users\alexa> ping 192.168.1.10

Обмен пакетами с 192.168.1.10 по с 32 байтами данных:
Ответ от 192.168.1.10: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.10: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.10: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.10: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.1.10:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
PS C:\Users\alexa>
```

Рисунок 2 – Проверка подключения

Установим необходимы пакеты для ssh-сервера. Запустим ssh-сервер с помощью команды systemctl start ssh и проверим статус подключения (рис. 3).

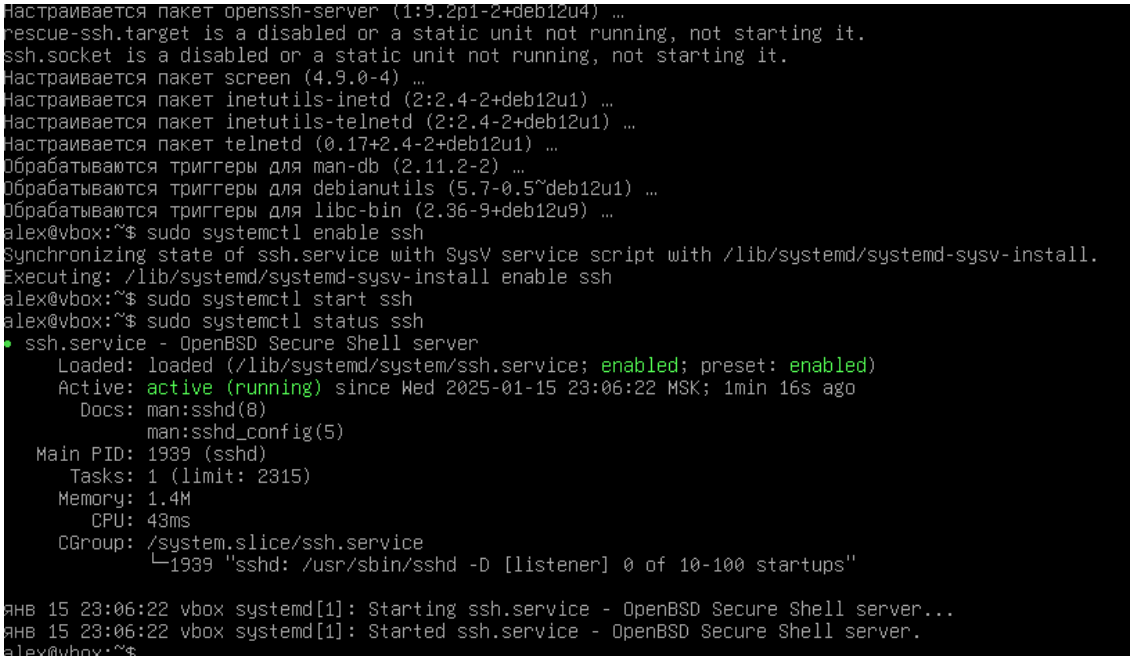

Рисунок 3 – Запуск ssh-сервера

Для работы telnetd настроим демон inetd, запускающий по необходимости другие сетевые серверные процессы. Раскомментируем строку с telnet в файле inetd.conf и сохраним изменения (рис. 4).

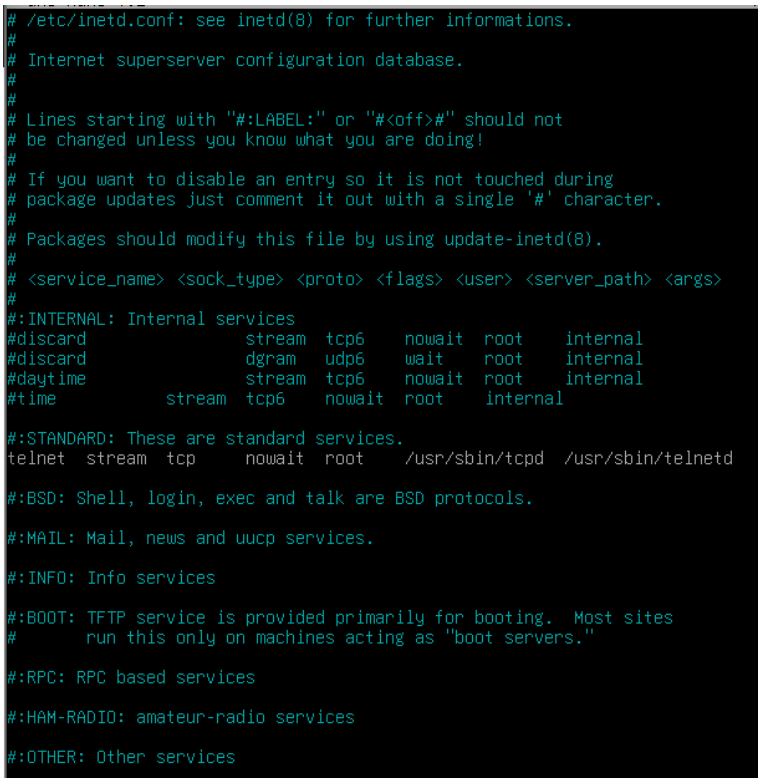

Рисунок 4 – Файл inetd.conf

Перезапустим демон inetd (рис. 5).

```
alex@vbox:~$ sudo systemctl restart inetd
alex@vbox:~$ ss -lt
State          Recv-Q          Send-Q                   Local Address:Port                     Peer A
LISTEN         0               244                          127.0.0.1:postgresql                  0
LISTEN         0               4096                           0.0.0.0:81                          0
LISTEN         0               128                            0.0.0.0:telnet                      0
LISTEN         0               128                            0.0.0.0:ssh                         0
LISTEN         0               244                              [::1]:postgresql                  0
LISTEN         0               4096                             [::]:81                           0
LISTEN         0               511                                 *:http                         0
LISTEN         0               128                              [::]:telnet                       0
LISTEN         0               128                              [::]:ssh                          0
alex@vbox:~$
```

Рисунок 5 – Перезапуск inetd

Для того чтобы подключиться к виртуальной машине через Telnet, необходимо включить клиент Telnet на хостовой системе. Это можно сделать в компонентах Windows (рис.6).

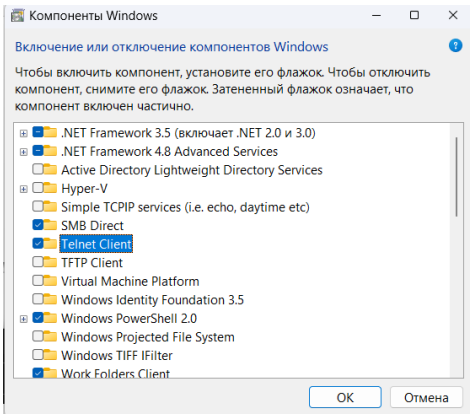

Рисунок 6 – Компоненты Windows

Включим анализ сетевого трафика на виртуальной машине с помощью команды sudo tcpdump -l -v -nn tcp and src port 23 or dst port 23 | tee telnet.log, которая переводит вывод команды в файл telnet.log. На хостовой системе прописываем команду telnet 192.168.1.10, тем самым подключимся через Telnet (рис. 7).

```
Linux 6.1.0-28-amd64 (vbox) (pts/1)

vbox ┗┐┛┗┬П ┗┐┛┗┛┬M┗┐┛┗┛▒┛┬B┗┤┗┬П: alex

┗д┛▒┬A┛┗┛┬M:
Linux vbox 6.1.0-28-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
┗д┛┗┬Б┗┐┛┗┛┗┛┗┛┗┛ ┗▒┬E┛┗┛ ┛▒ ┬Б┗┐┬Б┬В┗┤┛┗┛┬Г: ┗б┬A ┬П┗┛▒ 15 23:22:37 MSK 2025 ┛┗┛▒ tty1
alex@vbox:~$ uname -a
Linux vbox 6.1.0-28-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22) x86_64 GNU/Linux
alex@vbox:~$
alex@vbox:~$ logout


Подключение к узлу утеряно.
PS C:\Users\alexa>
```

Рисунок 7 – Подключение через Telnet

Выведем в терминал строки установки и завершения соединения из файла telnet.log (рис. 8).

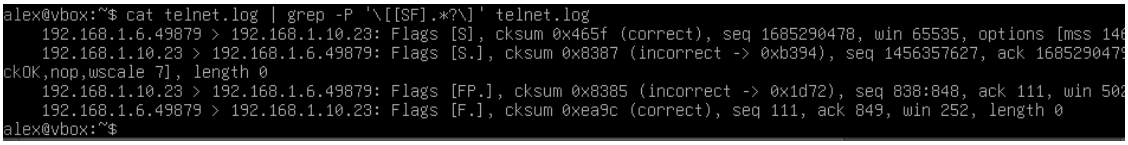

Рисунок 8 – Содержимое файла telnet.log

2. Часть II

Для настройки сетевого соединения через ssh воспользуемся утилитой tcpdump (рис. 9), позволяющую перехватывать и анализировать сетевой трафик, проходящий через компьютер, на котором запущена данная программа.

Рисунок 9 – Анализ сетевого трафика

На хостовой системе подключимся к гостевой с помощью команды ssh <имя пользователя в гостевой системе>@<ip-адрес гостевой системы> (рис. 10).

Рисунок 10 – Подключение по ssh

Создадим файл LR_6_test_file.txt в хостовой системе в папке C:/Users/alexa/. С помощью утилиты для безопасного копирования данных между системами по протоколу SSH scp передадим файл в домашнюю директорию гостевой системы (рис. 11).

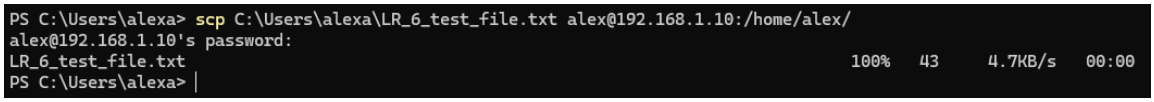

Рисунок 11 – Передача файла по протоколу SSH

На рисунке 12 показана успешная передача файла.

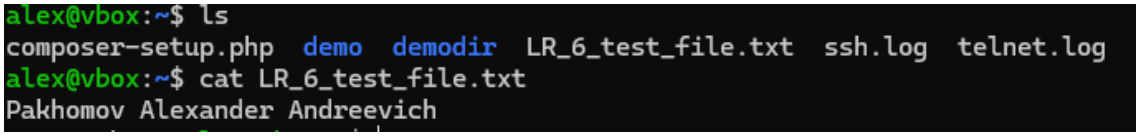

Рисунок 12 – Успешная пересылка файла

Теперь настроим ssh-ключи для подключения без пароля. Для этого изменим права доступа и создадим authorized_keys, в котором будем хранить ключи (рис. 13).

```
alex@vbox:~$ chmod 700 /home/alex/.ssh
alex@vbox:~$ touch /home/alex/.ssh/authorized_keys
alex@vbox:~$ chmod 600 /home/alex/.ssh/authorized_keys
```

Рисунок 13 – Настройка прав доступа

Для создания ключа на гостевой машине воспользуемся командой ssh-keygen (рис. 14). Публичный ключ назовем под именем keyForLab.

```
PS C:\Users\alexa> ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:\Users\alexa/.ssh/id_ed25519): keyForLab
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in keyForLab
Your public key has been saved in keyForLab.pub
The key fingerprint is:
SHA256:vM5Om9xxCSeHdQeg/ZQ4DUp5GeK3/b2xcNgAsd5cFCs alexa@Alexander
The key's randomart image is:
+--[ED25519 256]--+
|          oo++.o.|
|         o.==+.o.|
|          ++*E=o.|
|       .  .++Bo. |
|        S +.++o  |
|         . = .+..|
|        o . oo +o|
|       = + o  o +|
|       .B .    o |
+----[SHA256]-----+
PS C:\Users\alexa> cat .\keyForLab
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACCB9lJBhjgqwGpz/DrI1cJ89hLqz46QiIA9EgXLlxflcAAAAJgIebMfCHmz
HwAAAAtzc2gtZWQyNTUxOQAAACCB9lJBhjgqwGpz/DrI1cJ89hLqz46QiIA9EgXLlxflcA
AAAEBQMfz00FfwKC7hzkB9sVCqE9ELxLN3BPcNP9pw8TIVZIH2UkGGOCrAanP8OsjVwnz2
EurPjpCIgD0SBcuXF+VwAAAAD2FsZXhhQEFsZXhhbmRlcgECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
PS C:\Users\alexa> cat .\keyForLab.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIH2UkGGOCrAanP8OsjVwnz2EurPjpCIgD0SBcuXF+Vw alexa@Alexander
```

Рисунок 14 – Создание ssh-ключа

На рисунке 15 предыдущем способом с помощью команды scp передаем созданный ключ на гостевою систему.

```
PS C:\Users\alexa> scp C:\Users\alexa\keyForLab.pub alex@192.168.1.10:/home/alex/.ssh/temp_key.pub
alex@192.168.1.10's password:
keyForLab.pub                                 100%   98    31.9KB/s
PS C:\Users\alexa>
```

Рисунок 15 – Передача ключа на гостевую систему

Скопируем ключ в ранее созданный файл (рис. 16).

```
alex@vbox:~/.ssh$ cat /home/alex/.ssh/temp_key.pub >> /home/alex/.ssh/authorized_keys
alex@vbox:~/.ssh$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIH2UkGGOCrAanP8OsjVwnz2EurPjpCIgD0SBcuXF+Vw alexa@Alexander
```

Рисунок 16 – Копирование ключа

Теперь можно создать подключение через ssh с помощью указания явного расположения ключа (рис. 17).

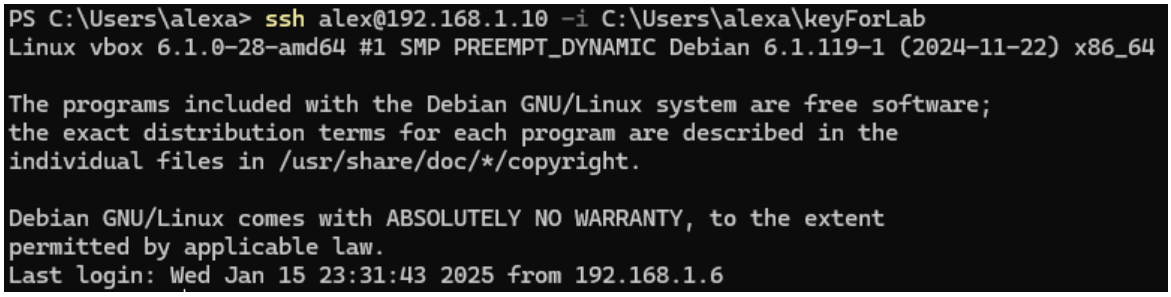

Рисунок 17 – Подключение по ключу

Теперь можно передать новый файл с помощью scp (рис. 18).

Рисунок 18 – Передача файла

Проверим успешность передачи файла на гостевой системе (рис. 19).

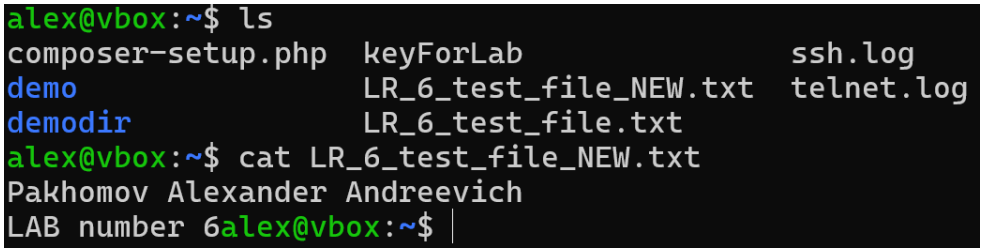

Рисунок 19 – Успешная передача файла

Как и в предыдущей части, выведем содержимое файла ssh.log (рис. 20).

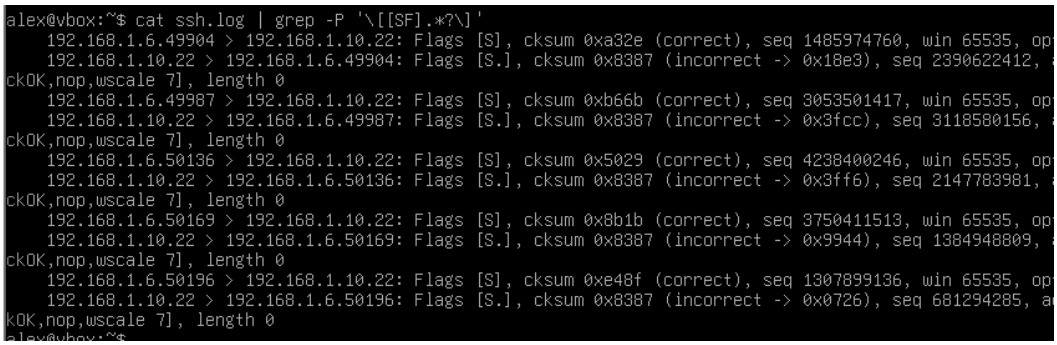

Рисунок 20 – Содержимое файла ssh.log

Контрольные вопросы

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

Программное обеспечение удаленного доступа предназначено для:

1) Управления удаленными системами, обеспечения контроля и настройки серверов, рабочих станций или устройств.

2) Технической поддержки, удаленного решения проблем пользователей.

3) Совместной работы, предоставления доступа к файлам, приложениям и средам разработки.

4) Обеспечения мобильности, доступа к корпоративным системам из любого места.

5) Обучения и демонстрации, проведения презентаций или обучения через удаленный доступ.

2) Выделите отличительные особенности между режимами работы удаленного доступа по протоколам TELNET и SSH?

SSH и Telnet – это два протокола, которые обычно используются для удалённого входа в систему и выполнения задач по настройке и управлению на устройствах, подключённых через сеть. Хотя оба типа беспроводных сетей имеют некоторое сходство в плане общего функционирования, они имеют больше особенностей в аспектах функций безопасности и операций. Благодаря строгим мерам безопасности, реализованным в его протоколах, SSH является наиболее современным в современных сетях.

SSH – это протокол, который обеспечивает безопасные, зашифрованные каналы связи по незащищённой сети. А Telnet – устаревший протокол, обеспечивающий незашифрованную связь по сети.

SSH поддерживает передачу файлов с помощью SCP (безопасное копирование) или SFTP (протокол безопасной передачи файлов). А Telnet изначально не поддерживает передачу файлов.

Telnet проще в использовании и реализации, но он считается небезопасным для большинства приложений и не используется так широко, как заменяющие его протоколы.

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

А) Способ входа по паролю. Ввод логина и пароля для доступа к удаленной системе: ssh user@host.

Плюсы: легкость настройки, не требуется предварительная конфигурация.

Минусы: менее безопасно.

Б) Способ установления соединения по ключам. Использование пары ключей: приватного (хранится на клиенте) и публичного (располагается на сервере).

ssh-keygen -t rsa

ssh-copy-id user@host

ssh user@host

Плюсы: высокая безопасность.

Минусы: требуется предварительная настройка.

В) Способ подключения через SSH-агент. Хранение ключей в памяти для упрощения многократных подключений.

eval $(ssh-agent)

ssh-add ~/.ssh/id_rsa

ssh user@host

Плюсы: удобство при множественных подключениях.

Минусы: потребность в поддержке SSH-агента.

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

Примером является подключение к удаленному серверу для выполнения системных команд, передачи файлов или мониторинга системы. В рамках лабораторной работы SSH использовался для подключения к серверу с ОС

Debian, выполнения команды uname -a для получения системной информации, а также передачи текстового файла через зашифрованный канал с использованием утилиты scp. Это иллюстрирует, как безопасный удаленный доступ позволяет эффективно управлять системой и обмениваться данными без необходимости физического присутствия.

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

Сетевые службы:

- Secure Shell: для удаленного доступа.
- SFTP: для передачи файлов.
- rsync через SSH: синхронизация данных.
- Git через SSH: безопасный доступ к репозиториям.
- Tunnels: защита сетевого трафика.

Передача файлов через безопасный SSH-туннель осуществляется с использованием таких утилит, как scp или rsync поверх SSH.

Передача файла local_file.txt с локального компьютера на сервер: scp local_file.txt user@remote_host:/path/to/remote/directory/.