Практическая работа №6. Безопасный удаленный доступ. Использование и настройка SSH

Вариант	Способ	Порт	Шифрование
1	init.d	2222	RSA

1. Проверьте, установлен ли в вашей OpenSSH. Если он не установлен, установите.

```
sudo apt install openssh-server
```

```
mrs4g0@MRS4G0-PC:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:8.2p1-4ubuntu0.7).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

2. Используйте один из способов запуска ssh-сервера в соответствии с вашим вариантом.

```
sudo service ssh start
```

```
mrs4g0@MRS4G0-PC:~$ sudo service ssh start
 * Starting OpenBSD Secure Shell server sshd
```

3. Проверьте статус вашего ssh-сервера.

```
sudo service ssh status
```

```
mrs4g0@MRS4G0-PC:~$ sudo service ssh status
 * sshd is running
```

4. Определите IP-адрес вашего ssh-сервера и подключитесь к нему по ssh.

```
ssh mrs4g0@localhost
```

5. Создайте резервную копию конфигурационного файла с настройками sh.

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
```

6. Измените порт подключения по ssh в соответствующем конфигурационном файле согласно вашему варианту.

```
sudo nano /etc/ssh/sshd_config
```

```
Port 2222
```

Запретите вход по ssh от имени root.

```
PermitRootLogin no
```

Установите время, за которое пользователь должен успеть подключиться по ssh. Время выберите из диапазона [20;40]. Например, 30 секунд.

```
LoginGraceTime 30
```

Ограничьте максимальное количество попыток входа по ssh значением из диапазона [2-5].

```
MaxAuthTries 3
```

```
Port 2222
#AddressFamily any
#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 30s
PermitRootLogin no
#StrictModes yes
MaxAuthTries 3
#MaxSessions 10
```

Перезапустите ssh-сервер.

```
sudo service ssh restart
```

```
mrs4g0@MRS4G0-PC:~$ sudo service ssh restart
 * Restarting OpenBSD Secure Shell server sshd
```

7. Подключитесь к серверу с учетом новых настроек.

```
ssh user@ip -p 2222
```

8. Запретите вход по паролю и настройте способ входа на ваш ssh-сервер по ключу. Сгенерируйте публичный и приватный ключи. Алгоритм шифрования выбирается в соответствии с вашим вариантом.

```
ssh-keygen -t rsa
```

Передача публичного ключа на сервер.

```
ssh-copy-id user@ip -p 2222
```

Подключение к серверу по ключу.

```
ssh user@ip -p 2222
```

9. Перезапустите ssh-сервер и подключитесь к нему, используя ключи для входа.

```
sudo service ssh restart
```

```
ssh user@ip -p 2222
```

10. Настройте подключение к серверу по одноразовому паролю (Google-authentication).

```
sudo apt install libpam-google-authenticator
```

```
google-authenticator
```

```
sudo nano /etc/pam.d/sshd
```

```
auth required pam_google_authenticator.so
```

```
sudo nano /etc/ssh/sshd_config
```

```
ChallengeResponseAuthentication yes
```

```
sudo service ssh restart
```

```
ssh user@ip -p 2222
```

11. Измените приветственное сообщение: должна выводиться строка «Gordeev A. S. KE-301».

```
sudo nano /etc/motd
```

```
Gordeev A. S. KE-301
```

Ответы на контрольные вопросы

1. Как определить, установлен ли в вашей системе OpenSSH?

```
dpkg -l | grep openssh-server
```

2. При помощи какой команды вы установили в своей системе OpenSSH?

```
sudo apt install openssh-server
```

3. При помощи какой команды вы запускали свой ssh-сервер? Какая альтернативная команда может быть применена?

```
sudo service ssh start
```

```
sudo systemctl start ssh
```

4. Как определить состояние ssh-сервера?

```
sudo service ssh status
```

5. Для чего используется настройка PermitRootLogin?

```
PermitRootLogin no
```

   Запрещает вход по ssh от имени root.

6. Для чего используется настройка PasswordAuthentication?

```
PasswordAuthentication no
```

Запрещает вход по паролю.

7. Для чего используется настройка PermitEmptyPasswords?

```
PermitEmptyPasswords no
```

Запрещает вход по пустому паролю.

8. Для чего используется настройка PubkeyAuthentication?

```
PubkeyAuthentication yes
```

Разрешает вход по ключу.

9. Для чего используется настройка MaxAuthTries?

```
MaxAuthTries 3
```

Ограничивает количество попыток входа по ssh.

10. Для чего используется настройка MaxStartups?

```
MaxStartups 10:30:60
```

Ограничивает количество одновременных подключений.

11. Для чего используется настройка LoginGraceTime?

```
LoginGraceTime 30
```

Устанавливает время, за которое пользователь должен успеть подключиться по ssh.

12. Что такое SSH-ключи? Какие выделяют виды этих ключей?

SSH-ключи — это способ аутентификации, при котором вместо пароля используется пара ключей: публичный и приватный. Публичный ключ распространяется на все серверы, к которым вы хотите иметь доступ, а приватный ключ хранится только у вас. При подключении к серверу по ssh, сервер проверяет, что вы владеете приватным ключом, соответствующим публичному ключу, который вы предоставили. Если ключи совпадают, то сервер разрешает вам вход.

Виды ключей:

- RSA
- DSA
- ECDSA
- ED25519

13. Как сгенерировать ключи для входа по ssh?

```
ssh-keygen -t rsa
```

```
ssh-keygen -t rsa -b 4096
```

```
ssh-keygen -t dsa
```

```
ssh-keygen -t ecdsa -b 521
```

```
ssh-keygen -t ed25519
```