

Отчёт по лабораторной работе 11

Настройка безопасного удалённого доступа по протоколу SSH

Заур Мустафаев

Содержание

1 Цель работы	5
2 Выполнение работы	6
2.1 Запрет удалённого доступа по SSH для пользователя root	6
2.2 Ограничение списка пользователей для удалённого доступа по SSH	8
2.3 Настройка дополнительных портов для удалённого доступа по SSH	11
2.4 Настройка удалённого доступа по SSH по ключу	14
2.5 Организация SSH-туннеля (перенаправление TCP-портов)	15
2.6 Запуск консольных приложений на сервере через SSH	17
2.7 Запуск графических приложений через SSH (X11Forwarding) . . .	18
2.8 Внесение изменений в настройки внутреннего окружения виртуальной машины	20
3 Вывод	22
4 Контрольные вопросы	23

Список иллюстраций

2.1 Попытка подключиться по SSH под root	6
2.2 Редактирование параметра PermitRootLogin no	7
2.3 Повторная попытка входа под root после изменения	7
2.4 Успешная авторизация пользователем zmustafaev	8
2.5 Добавление AllowUsers vagrant	9
2.6 Отказ при подключении после AllowUsers vagrant	9
2.7 Добавление второго пользователя в AllowUsers	10
2.8 Успешный вход после добавления пользователя	10
2.9 Добавление порта 2022 в sshd_config	12
2.10 Перезапуск и проверка статуса службы SSH	12
2.11 Проверка статуса после исправления SELinux и firewall	13
2.12 Подключение к серверу по стандартному порту 22	14
2.13 Успешное подключение по ключу	15
2.14 Создание SSH-туннеля	16
2.15 Проверка работы туннеля	16
2.16 Страница, доступная через SSH-туннель	17
2.17 Пример выполнения удалённых команд через SSH	18
2.18 Включение X11Forwarding в sshd_config	19
2.19 Попытка запуска графического приложения через SSH	20
2.20 Создание каталога для конфигурации SSH	20
2.21 Содержимое скрипта ssh.sh	21

Список таблиц

1 Цель работы

Приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

2 Выполнение работы

2.1 Запрет удалённого доступа по SSH для пользователя root

1. На сервере был установлен пароль для пользователя root.
2. Запущен мониторинг системных событий с помощью journalctl.
3. С клиента выполнена попытка подключения по SSH под пользователем root.

```
[zmustafaev@client.zmustafaev.net ~]$ ssh root@server.zmustafaev.net
The authenticity of host 'server.zmustafaev.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxnw0XTU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.zmustafaev.net' (ED25519) to the list of known hosts.
root@server.zmustafaev.net's password:
Permission denied, please try again.
root@server.zmustafaev.net's password:
Permission denied, please try again.
root@server.zmustafaev.net's password:
root@server.zmustafaev.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,
password).
[zmustafaev@client.zmustafaev.net ~]$
```

Рис. 2.1: Попытка подключиться по SSH под root

сервер запрашивает пароль, но вход не выполняется — попытки аутентификации завершаются ошибкой.

- На сервере в файле конфигурации `/etc/ssh/sshd_config` изменён параметр `PermitRootLogin` на значение `no`.

```
sshd_config      [-M--] 18 L:[ 23+17  40/131] *(1154/3658b) 0010 0x00A
#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 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile<---->.ssh/authorized_keys

#AuthorizedPrincipalsFile none
```

Рис. 2.2: Редактирование параметра `PermitRootLogin no`

- Произведён перезапуск службы SSH.
- Повторная попытка подключения к серверу под пользователем root.

```
[zmustafaev@client.zmustafaev.net ~]$ [zmustafaev@client.zmustafaev.net ~]$ ssh root@server.zmustafaev.net
root@server.zmustafaev.net's password:
Permission denied, please try again.
root@server.zmustafaev.net's password:
Permission denied, please try again.
root@server.zmustafaev.net's password:
root@server.zmustafaev.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,
password).
[zmustafaev@client.zmustafaev.net ~]$
```

Рис. 2.3: Повторная попытка входа под root после изменения

удалённый вход под root стал невозможен — сервер блокирует попытку

подключения, выводя ошибку `Permission denied.`

Это подтверждает, что вход `root` по SSH запрещён.

2.2 Ограничение списка пользователей для удалённого доступа по SSH

- С клиента выполнена попытка подключения по SSH под обычным пользователем.

```
[zmustataev@client.zmustataev.net ~]$  
[zmustataev@client.zmustataev.net ~]$ ssh zmustataev@server.zmustataev.net  
zmustataev@server.zmustataev.net's password:  
Web console: https://server.zmustataev.net:9090/ or https://192.168.1.1:9090/  
  
Last login: Mon Nov 10 11:55:29 2025  
[zmustataev@server.zmustataev.net ~]$  
logout  
Connection to server.zmustataev.net closed.  
[zmustataev@client.zmustataev.net ~]$  
[zmustataev@client.zmustataev.net ~]$ █
```

Рис. 2.4: Успешная авторизация пользователем `zmustataev`

вход выполнен успешно, пользователь получает доступ к серверу.

- В файле `/etc/ssh/sshd_config` добавлена строка `AllowUsers vagrant`.

```
sshd_config      [----] 18 L:[ 31+16 47/133] *(1250/3678b) 0010 0x00A
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

AllowUsers vagrant

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile<---->.ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
 1Help   2Save  3Mark  4Replace  5Copy  6Move  7Search
```

Рис. 2.5: Добавление AllowUsers vagrant

3. Служба SSH была перезапущена.
4. Выполнена повторная попытка подключения под пользователем zmustafaev.

```
[zmustafaev@client.zmustafaev.net ~]$ 
[zmustafaev@client.zmustafaev.net ~]$ ssh zmustafaev@server.zmustafaev.net
zmustafaev@server.zmustafaev.net's password:
Permission denied, please try again.
zmustafaev@server.zmustafaev.net's password:
Permission denied, please try again.
zmustafaev@server.zmustafaev.net's password:
zmustafaev@server.zmustafaev.net: Permission denied (publickey,gssapi-keyex,gssapi-wit
h-mic,password).
[zmustafaev@client.zmustafaev.net ~]$
```

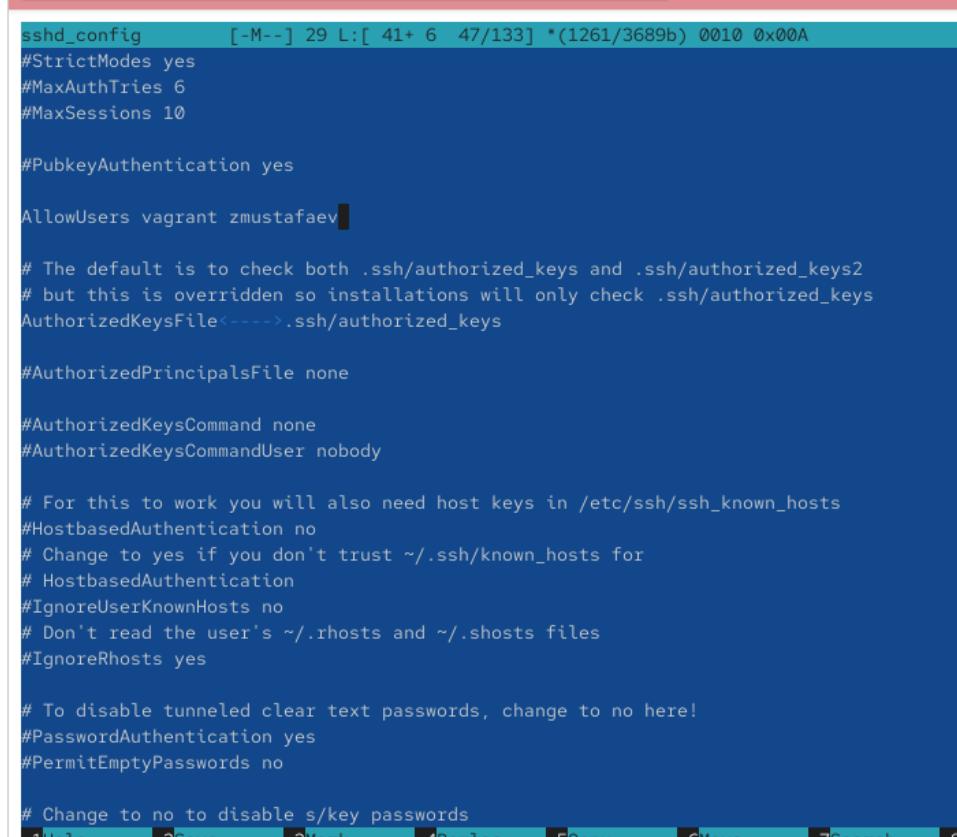
Рис. 2.6: Отказ при подключении после AllowUsers vagrant

доступ отклонён, так как в конфигурации разрешён только пользователь

vagrant.

5. В файл /etc/ssh/sshd_config добавлены два пользователя:

AllowUsers vagrant zmustafaev



```
sshd_config      [-M--] 29 L:[ 41+ 6  47/133] *(1261/3689b) 0010 0x00A
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

AllowUsers vagrant zmustafaev

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile<----->.ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

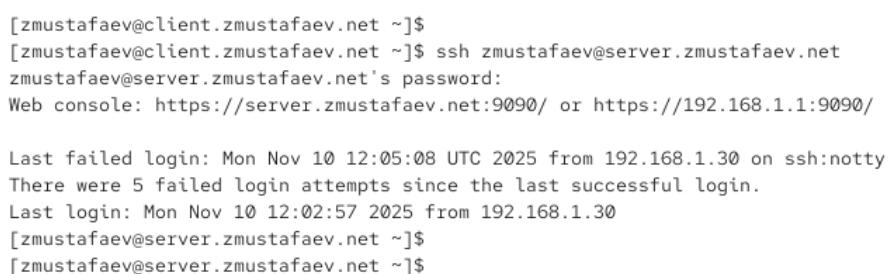
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
[1Help 2Save 3Mark 4Paste 5Copy 6Delete 7Search 8]
```

Рис. 2.7: Добавление второго пользователя в AllowUsers

6. После перезапуска службы SSH выполнена попытка входа под пользователем zmustafaev.



```
[zmustafaev@client.zmustafaev.net ~]$ [zmustafaev@client.zmustafaev.net ~]$ ssh zmustafaev@server.zmustafaev.net
zmustafaev@server.zmustafaev.net's password:
Web console: https://server.zmustafaev.net:9090/ or https://192.168.1.1:9090/
Last failed login: Mon Nov 10 12:05:08 UTC 2025 from 192.168.1.30 on ssh:notty
There were 5 failed login attempts since the last successful login.
Last login: Mon Nov 10 12:02:57 2025 from 192.168.1.30
[zmustafaev@server.zmustafaev.net ~]$ [zmustafaev@server.zmustafaev.net ~]$
```

Рис. 2.8: Успешный вход после добавления пользователя

теперь пользователь входит успешно, так как он добавлен в список разрешённых пользователей.

2.3 Настройка дополнительных портов для удалённого доступа по SSH

1. На сервере в файле конфигурации `/etc/ssh/sshd_config` добавлены строки:

- Port 22
- Port 2022

Это позволяет службе SSH работать на двух портах одновременно, обеспечивая возможность подключения даже при ошибке в конфигурации одного из них.

```

sshd_config      [-M--]  0 L:[ 5+21 26/134] *(900 /3698b) 0010 0x00A

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

# To modify the system-wide sshd configuration, create a *.conf file under
# /etc/ssh/sshd_config.d/ which will be automatically included below
Include /etc/ssh/sshd_config.d/*.conf

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22
Port 2022
#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

```

1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Del

Рис. 2.9: Добавление порта 2022 в sshd_config

2. После сохранения изменений служба SSH была перезапущена, затем проверен её статус.

```

[root@server.zmustafaev.net ~]# systemctl restart sshd
[root@server.zmustafaev.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
    Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
    Active: active (running) since Mon 2025-11-10 12:07:41 UTC; 9s ago
      Invocation: a990654567d840218139a5aeeee5a597
        Docs: man:sshd(8)
               man:sshd_config(5)
     Main PID: 11579 (sshd)
        Tasks: 1 (limit: 10381)
       Memory: 1M (peak: 1.1M)
          CPU: 4ms
         CGroup: /system.slice/sshd.service
                   └─11579 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Nov 10 12:07:41 server.zmustafaev.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
Nov 10 12:07:41 server.zmustafaev.net (sshd)[11579]: sshd.service: Referenced but unset environment variable evaluates >
Nov 10 12:07:41 server.zmustafaev.net sshd[11579]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
Nov 10 12:07:41 server.zmustafaev.net sshd[11579]: error: Bind to port 2022 on :: failed: Permission denied.
Nov 10 12:07:41 server.zmustafaev.net systemd[1]: Started sshd.service - OpenSSH server daemon.
Nov 10 12:07:41 server.zmustafaev.net sshd[11579]: Server listening on 0.0.0.0 port 22.
Nov 10 12:07:41 server.zmustafaev.net sshd[11579]: Server listening on :: port 22.

```

lines 1-20/20 (END)

Рис. 2.10: Перезапуск и проверка статуса службы SSH

служба SSH запущена, но система сообщает об ошибке Bind to port 2022

failed: Permission denied.

Это означает, что SELinux не разрешает процессу sshd прослушивать новый порт 2022.

3. Для устранения ошибки были назначены корректные метки SELinux для порта 2022 с типом `ssh_port_t`.
4. После этого межсетевой экран был настроен на разрешение входящих соединений через порт 2022 протокола TCP.
5. Служба SSH была перезапущена повторно, и её состояние проверено повторно.

```
root@server.zmustafaev.net ~# systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-11-10 12:08:52 UTC; 2s ago
     Invocation: 1412a5888a3d4c82b8d8fd63489cd441
       Docs: man:sshd(8)
              man:sshd_config(5)
    Main PID: 11755 (sshd)
      Tasks: 1 (limit: 10381)
        Memory: 1M (peak: 1.2M)
          CPU: 5ms
        CGroup: /system.slice/sshd.service
                  └─11755 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Nov 10 12:08:52 server.zmustafaev.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
Nov 10 12:08:52 server.zmustafaev.net (sshd)[11755]: sshd.service: Referenced but unset environment variable evaluates >
Nov 10 12:08:52 server.zmustafaev.net sshd[11755]: Server listening on 0.0.0.0 port 2022.
Nov 10 12:08:52 server.zmustafaev.net sshd[11755]: Server listening on :: port 2022.
Nov 10 12:08:52 server.zmustafaev.net sshd[11755]: Server listening on 0.0.0.0 port 22.
Nov 10 12:08:52 server.zmustafaev.net sshd[11755]: Server listening on :: port 22.
Nov 10 12:08:52 server.zmustafaev.net systemd[1]: Started sshd.service - OpenSSH server daemon.
lines 1-20/20 (END)
```

Рис. 2.11: Проверка статуса после исправления SELinux и firewall

теперь процесс SSH успешно слушает оба порта — 22 и 2022, что подтверждается сообщениями журнала.

6. С клиента выполнено подключение к серверу по SSH без указания порта.

```
[zmustafaev@client.zmustafaev.net ~]$  
[zmustafaev@client.zmustafaev.net ~]$ ssh zmustafaev@server.zmustafaev.net  
zmustafaev@server.zmustafaev.net's password:  
Web console: https://server.zmustafaev.net:9090/ or https://192.168.1.1:9090/  
  
Last login: Mon Nov 10 12:05:16 2025 from 192.168.1.30  
[zmustafaev@server.zmustafaev.net ~]$ sudo -i  
[sudo] password for zmustafaev:  
[root@server.zmustafaev.net ~]#  
logout  
[zmustafaev@server.zmustafaev.net ~]$  
logout  
Connection to server.zmustafaev.net closed.  
[zmustafaev@client.zmustafaev.net ~]$ ssh zmustafaev@server.zmustafaev.net -p2022  
zmustafaev@server.zmustafaev.net's password:  
Web console: https://server.zmustafaev.net:9090/ or https://192.168.1.1:9090/  
  
Last login: Mon Nov 10 12:09:22 2025 from 192.168.1.30  
[zmustafaev@server.zmustafaev.net ~]$ sudo -i  
[sudo] password for zmustafaev:  
[root@server.zmustafaev.net ~]#  
logout  
[zmustafaev@server.zmustafaev.net ~]$  
logout  
Connection to server.zmustafaev.net closed.  
[zmustafaev@client.zmustafaev.net ~]$
```

Рис. 2.12: Подключение к серверу по стандартному порту 22

соединение установлено успешно, доступ к серверу получен, пользователь смог получить права root через sudo.

7. После выхода из системы выполнена повторная попытка подключения, но с указанием нового порта 2022.

Подключение прошло успешно, подтверждая корректную настройку дополнительного порта SSH.

2.4 Настройка удалённого доступа по SSH по ключу

1. На сервере в файле `/etc/ssh/sshd_config` включена аутентификация по ключу с помощью параметра `PubkeyAuthentication yes`.

2. Служба SSH была перезапущена, чтобы изменения вступили в силу.

3. На клиенте под пользователем был сгенерирован SSH-ключ (`ssh-keygen`).

Созданы два файла: закрытый ключ `id_rsa` и открытый ключ `id_rsa.pub`.

4. Открытый ключ был скопирован на сервер с клиента.
5. Выполнено SSH-подключение к серверу без ввода пароля.

```
| . . . o |
| oo.+.* = .|
| SB *.=oB |
| o *.=oo+.|
| *.Bo.o o|
| @=. o*|
| .o+o .E*|
+---[SHA256]---+
[zmustafaev@client.zmustafaev.net ~]$ ssh-copy-id zmustafaev@server.zmustafaev.net
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ssh-add -L
/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
zmustafaev@server.zmustafaev.net's password:

Number of key(s) added: 1

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

[zmustafaev@client.zmustafaev.net ~]$ ssh zmustafaev@server.zmustafaev.net -p2022
Web console: https://server.zmustafaev.net:9090/ or https://192.168.1.1:9090/

Last login: Mon Nov 10 12:09:41 2025 from 192.168.1.30
[zmustafaev@server.zmustafaev.net ~]$ █
```

Рис. 2.13: Успешное подключение по ключу

вход на сервер по SSH теперь выполняется без запроса пароля, что подтверждает успешную настройку SSH-аутентификации по ключу.

2.5 Организация SSH-туннеля (перенаправление TCP-портов)

1. На клиенте был запущен просмотр активных TCP-подключений.
2. Выполнено создание SSH-туннеля: локальный порт 8080 был связан с портом 80 на сервере.

```
[zmustafaev@client.zmustafaev.net ~]$  
[zmustafaev@client.zmustafaev.net ~]$ lsof | grep TCP  
[zmustafaev@client.zmustafaev.net ~]$ ssh -fNL 8080:localhost:80 zmustafaev@server.zmu  
stafaev.net  
[zmustafaev@client.zmustafaev.net ~]$ lsof | grep TCP  
ssh      15084          zmustafaev    3u      IPv4          90271  
 0t0      TCP client.zmustafaev.net:57304->mail.zmustafaev.net:ssh (ESTABLISHED)  
ssh      15084          zmustafaev    4u      IPv6          90281  
 0t0      TCP localhost:webcache (LISTEN)  
ssh      15084          zmustafaev    5u      IPv4          90282  
 0t0      TCP localhost:webcache (LISTEN)  
[zmustafaev@client.zmustafaev.net ~]$
```

Рис. 2.14: Создание SSH-туннеля

3. Повторный вывод списка TCP-соединений показал, что теперь локальный порт 8080 находится в состоянии LISTEN.

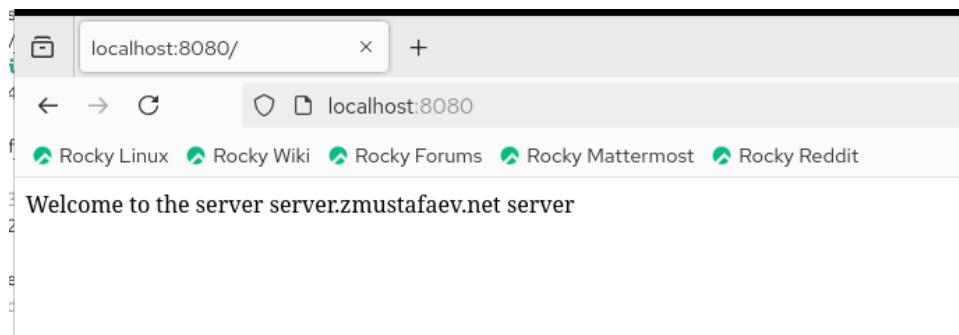


Рис. 2.15: Проверка работы туннеля

в выводе видно, что процесс `ssh` слушает локальный порт 8080, перенаправляя весь трафик на порт 80 сервера.

4. В браузере на клиенте в адресной строке введён `localhost:8080`.

```
[zmustafaev@client.zmustafaev.net ~]$ ssh zmustafaev@server.zmustafaev.net hostname  
server.zmustafaev.net  
[zmustafaev@client.zmustafaev.net ~]$ ssh zmustafaev@server.zmustafaev.net ls -Al  
total 56  
-rw----- 1 zmustafaev zmustafaev 105 Nov 4 09:27 .bash_history  
-rw-r--r-- 1 zmustafaev zmustafaev 18 Oct 29 2024 .bash_logout  
-rw-r--r-- 1 zmustafaev zmustafaev 144 Oct 29 2024 .bash_profile  
-rw-r--r-- 1 zmustafaev zmustafaev 711 Oct 8 11:02 .bashrc  
drwx----- 11 zmustafaev zmustafaev 4096 Oct 8 10:58 .cache  
drwx----- 10 zmustafaev zmustafaev 4096 Oct 29 15:21 .config  
drwxr-xr-x 2 zmustafaev zmustafaev 6 Oct 8 10:53 Desktop  
drwxr-xr-x 2 zmustafaev zmustafaev 6 Oct 8 10:53 Documents  
drwxr-xr-x 2 zmustafaev zmustafaev 6 Oct 8 10:53 Downloads  
drwx----- 4 zmustafaev zmustafaev 32 Oct 8 10:53 .local  
drwx----- 5 zmustafaev zmustafaev 4096 Nov 4 09:22 Maildir  
drwxr-xr-x 5 zmustafaev zmustafaev 54 Oct 8 10:53 .mozilla  
drwxr-xr-x 2 zmustafaev zmustafaev 6 Oct 8 10:53 Music  
drwxr-xr-x 2 zmustafaev zmustafaev 6 Oct 8 10:53 Pictures  
drwxr-xr-x 2 zmustafaev zmustafaev 6 Oct 8 10:53 Public  
drwx----- 2 zmustafaev zmustafaev 29 Nov 10 12:12 .ssh
```

Рис. 2.16: Страница, доступная через SSH-туннель

веб-страница загружается через SSH-туннель, что подтверждает корректную работу перенаправления портов.

2.6 Запуск консольных приложений на сервере через SSH

1. С клиента было выполнено удалённое выполнение команды для определения имени хоста сервера.
2. Далее выполнена команда для вывода списка файлов на сервере.
3. После этого был просмотр почтового ящика пользователя на сервере.

```
[zmustafaev@client.zmustafaev.net ~]$ ssh zmustafaev@server.zmustafaev.net MAIL=~/Mail
dir mail
s-nail version v14.9.24. Type `?' for help
/home/zmustafaev/Maildir: 3 messages 1 unread
  1 zmustafaev      2025-10-29 15:09  18/668  "test1"
  2 zmustafaev@client.zm 2025-11-04 09:00  21/855  "LMTP test"
▶U 3 zmustafaev      2025-11-04 09:22  22/840  "test3"
q
Held 3 messages in /home/zmustafaev/Maildir
[zmustafaev@client.zmustafaev.net ~]$
```

Рис. 2.17: Пример выполнения удалённых команд через SSH

команды выполняются на сервере без открытия полноценной интерактивной оболочки. Это позволяет управлять сервером и запускать консольные приложения напрямую из клиентского терминала.

2.7 Запуск графических приложений через SSH (X11Forwarding)

- На сервере в конфигурационном файле `/etc/ssh/sshd_config` была разрешена возможность удалённого вывода графического интерфейса X11 с помощью параметра `X11Forwarding yes`.

```
sshd_config      [-M--] 17 L:[ 87+17 104/134] *(3091/3697b) 0010 0

# Set this to 'yes' to enable PAM authentication, account processing
# and session processing. If this is enabled, PAM authentication wil
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin prohibit-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthenticatio
# and KbdInteractiveAuthentication to 'no'.
# WARNING: 'UsePAM no' is not supported in this build and may cause
# problems.
#UsePAM no

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
 1Help   2Save   3Mark   4Replac   5Copy   6Move
```

Рис. 2.18: Включение X11Forwarding в sshd_config

2. Служба SSH была перезапущена для применения изменений.
3. На клиенте выполнена попытка удалённого запуска графического приложения (firefox) с использованием опции X11-перенаправления.

```
[zmustafaev@client.zmustafaev.net ~]$ ssh -YC zmustafaev@server.zmustafaev.net firefox
Warning: No xauth data; using fake authentication data for X11 forwarding.
X11 forwarding request failed on channel 0
Error: no DISPLAY environment variable specified
[zmustafaev@client.zmustafaev.net ~]$ ssh -YC zmustafaev@server.zmustafaev.net firefox
Warning: No xauth data; using fake authentication data for X11 forwarding.
X11 forwarding request failed on channel 0
Error: no DISPLAY environment variable specified
[zmustafaev@client.zmustafaev.net ~]$
```

Рис. 2.19: Попытка запуска графического приложения через SSH

X11-перенаправление не выполнено. В сообщении указано, что переменная окружения DISPLAY не определена. Это означает, что на клиентской стороне не настроена X11-среда (например, отсутствует X-server).

2.8 Внесение изменений в настройки внутреннего окружения виртуальной машины

- На сервере был выполнен переход в каталог `/vagrant/provision/server/` и создана структура каталогов для хранения конфигурационных файлов SSH.

Затем файл `sshd_config` был скопирован в новую структуру каталогов.

```
[root@server.zmustafaev.net ~]# cd /vagrant/provision/server/
[root@server.zmustafaev.net ~]# mkdir /vagrant/provision/server/ssh/etc/ssh
[root@server.zmustafaev.net server]# cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/
[root@server.zmustafaev.net server]# touch ssh.sh
[root@server.zmustafaev.net server]#
```

Рис. 2.20: Создание каталога для конфигурации SSH

- В каталоге `/vagrant/provision/server/` был создан исполняемый файл `ssh.sh`, в который внесён скрипт для:

- копирования конфигурационных файлов SSH в `/etc`,
- настройки SELinux для работы порта 2022,
- открытия порта 2022 в firewall,
- перезапуска службы `sshd`.

```
1 #!/bin/bash
2 echo "Provisioning script $0"
3 echo "Copy configuration files"
4 cp -R /vagrant/provision/server/ssh/etc/* /etc
5 restorecon -vR /etc
6 echo "Configure firewall"
7 firewall-cmd --add-port=2022/tcp
8 firewall-cmd --add-port=2022/tcp --permanent
9 echo "Tuning SELinux"
10 semanage port -a -t ssh_port_t -p tcp 2022
11 echo "Restart sshd service"
12 systemctl restart sshd
```

Рис. 2.21: Содержимое скрипта ssh.sh

теперь при автоматическом запуске виртуальной машины происходит применение настроек SSH, включая открытие порта 2022, корректную настройку SELinux и перезапуск службы sshd. Это позволяет быстро развернуть виртуальную машину с заранее подготовленной конфигурацией.

3 Вывод

В ходе работы была выполнена настройка удалённого доступа по SSH: запрещён вход под пользователем root, ограничен доступ списком разрешённых пользователей, добавлен дополнительный порт для подключения и настроены правила SELinux и межсетевого экрана. Реализована аутентификация по ключу и создан SSH-туннель с локальным перенаправлением порта. Развёрнут автоматизационный скрипт, позволяющий повторно применять конфигурацию.

4 Контрольные вопросы

1. Вы хотите запретить удалённый доступ по SSH на сервер пользователю root и разрешить доступ пользователю alice. Как это сделать?

В файле /etc/ssh/sshd_config установить:

- PermitRootLogin no — запрет входа root по SSH,
- AllowUsers alice — разрешение доступа только пользователю alice, затем перезапустить sshd.

2. Как настроить удалённый доступ по SSH через несколько портов? Для чего это может потребоваться?

В файле sshd_config указать несколько строк Port, например:

- Port 22
- Port 2022

Это позволяет подключаться по альтернативному порту при ошибках настройки или для повышения безопасности.

3. Какие параметры используются для создания туннеля SSH, когда команда ssh устанавливает фоновое соединение и не ожидает конкретной команды?

Используются параметры:

- -f — перевод ssh в фоновый режим,
- -N — не запускать удалённую команду,
- -L — локальное перенаправление порта.

4. Как настроить локальную переадресацию с локального порта 5555 на порт 80 сервера server2.example.com?

Использовать команду: `ssh -fNL 5555:localhost:80 user@server2.example.com`

Теперь обращение к `localhost:5555` перенаправляется на порт 80 сервера.

5. Как настроить SELinux, чтобы позволить SSH связываться с портом 2022?

Добавить порт в список разрешённых для ssh: `semanage port -a -t ssh_port_t -p tcp 2022`

6. Как настроить межсетевой экран на сервере, чтобы разрешить входящие подключения по SSH через порт 2022?

Внести порт в правила firewalld:

```
firewall-cmd --add-port=2022/tcp      firewall-cmd --add-port=2022/tcp --  
permanent
```

Затем перезапустить правила либо службу firewalld.