

# **Отчёт по лабораторной работе 11**

**Настройка безопасного удалённого доступа по протоколу SSH**

Метвалли Ахмед Фарг Набеев

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение</b>	<b>6</b>
2.1	Запрет удалённого доступа по SSH для пользователя root . . . . .	6
2.2	Ограничение списка пользователей для удалённого доступа по SSH	7
2.3	Настройка дополнительных портов для удалённого доступа по SSH	9
2.4	Настройка удалённого доступа по SSH по ключу . . . . .	12
2.5	Организация туннелей SSH и перенаправление TCP-портов . . . .	14
2.6	Запуск консольных приложений через SSH . . . . .	15
2.7	Запуск графических приложений через SSH (X11 Forwarding) . . .	17
2.8	Внесение изменений в настройки внутреннего окружения виртуальной машины . . . . .	18
<b>3</b>	<b>Заключение</b>	<b>20</b>
<b>4</b>	<b>Контрольные вопросы</b>	<b>21</b>

# Список иллюстраций

2.1	Ошибка подключения по SSH под root . . . . .	6
2.2	Файл sshd_config с запретом root-входа . . . . .	7
2.3	Добавление второго порта в sshd_config . . . . .	10
2.4	Ошибка доступа к порту 2022 . . . . .	10
2.5	Открытие порта 2022 и успешный запуск sshd . . . . .	11
2.6	Подключение по стандартному и дополнительному портам . . . .	12
2.7	Разрешение аутентификации по ключу в sshd_config . . . . .	13
2.8	Передача ключа и успешное подключение без пароля . . . . .	14
2.9	Проверка TCP-соединений и организация туннеля SSH . . . . .	15
2.10	Отображение веб-страницы через туннель SSH . . . . .	15
2.11	Проверка имени хоста и содержимого домашнего каталога . . . .	16
2.12	Просмотр почты пользователя через SSH . . . . .	16
2.13	Разрешение X11Forwarding в sshd_config . . . . .	17
2.14	Ошибка при попытке запуска графического приложения через SSH	18
2.15	Создание каталогов и копирование файла sshd_config . . . . .	18
2.16	Содержимое скрипта ssh.sh для автоматизации настройки SSH . .	19

## **Список таблиц**

# 1 Цель работы

Освоение приёмов настройки SSH-сервера для ограничения удалённого доступа: запрета входа под пользователем root и разрешения подключения только определённым пользователям.

## 2 Выполнение

### 2.1 Запрет удалённого доступа по SSH для пользователя root

1. С клиента выполнена попытка подключения к серверу от имени пользователя root.

Сервер трижды запрашивал пароль, после чего выдал сообщение об ошибке.

Это означает, что вход под root запрещён на уровне конфигурации SSH.

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

Рис. 2.1: Ошибка подключения по SSH под root

2. В конфигурационном файле /etc/ssh/sshd\_config установлено значение параметра PermitRootLogin no.

После перезапуска службы sshd подключение под root остаётся невозможным, что подтверждает корректную работу настройки.

```

28 #HostKey /etc/ssh/ssh_host_ed25519_key
29
30 # Ciphers and keying
31 #RekeyLimit default none
32
33 # Logging
34 #SyslogFacility AUTH
35 #LogLevel INFO
36
37 # Authentication:
38
39 #LoginGraceTime 2m
40
41 PermitRootLogin no
42
43 #StrictModes yes
44 #MaxAuthTries 6
45 #MaxSessions 10
46
47 #PubkeyAuthentication yes
48

```

Рис. 2.2: Файл sshd\_config с запретом root-входа

## 2.2 Ограничение списка пользователей для удалённого доступа по SSH

1. При попытке входа на сервер под пользователем ahmedfarg с клиента доступ был успешно получен, так как данный пользователь разрешён в текущей конфигурации SSH.

```

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

```

```

[ahmedfarg@client.ahmedfarg.net ~]$ ssh root@server.ahmedfarg.net
[ahmedfarg@client.ahmedfarg.net ~]$ ssh root@server.ahmedfarg.net
ahmedfarg@server.ahmedfarg.net:~$
Web console: https://server.ahmedfarg.net/

Last login: Mon Oct 20 08:39:00 2020
[ahmedfarg@server.ahmedfarg.net ~]$
logout
Connection to server.ahmedfarg.net closed.
[ahmedfarg@client.ahmedfarg.net ~]$

```

2. Для ограничения доступа только определённым пользователям в файл

/etc/ssh/sshd\_config добавлена строка AllowUsers vagrant.

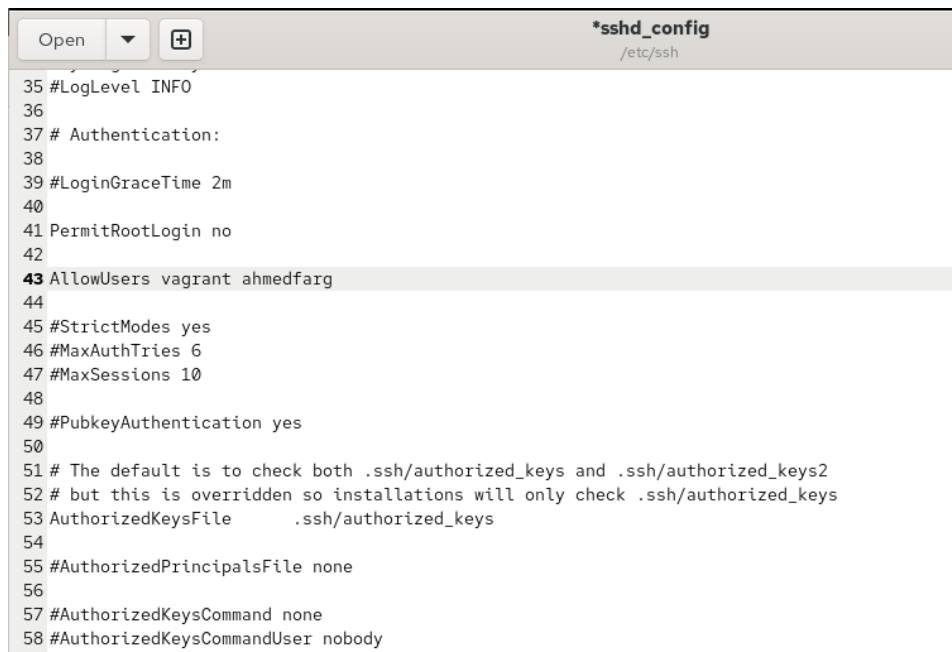
После перезапуска службы sshd подключение под пользователем ahmedfarg стало невозможным.

```
26 #HostKey /etc/ssh/ssh_host_rsa_key
27 #HostKey /etc/ssh/ssh_host_ecdsa_key
28 #HostKey /etc/ssh/ssh_host_ed25519_key
29
30 # Ciphers and keying
31 #RekeyLimit default none
32
33 # Logging
34 #SyslogFacility AUTH
35 #LogLevel INFO
36
37 # Authentication:
38
39 #LoginGraceTime 2m
40
41 PermitRootLogin no
42
43 AllowUsers vagrant|
44
45 #StrictModes yes
46 #MaxAuthTries 6
47 #MaxSessions 10
48
```

```
[ahmedfarg@client.ahmedfarg.net]
[ahmedfarg@client.ahmedfarg.net]
ahmedfarg@server.ahmedfarg.net:
Permission denied, please try
ahmedfarg@server.ahmedfarg.net:
Permission denied, please try
ahmedfarg@server.ahmedfarg.net:
ahmedfarg@server.ahmedfarg.net:
-with-mic,password).
[ahmedfarg@client.ahmedfarg.net]
```

3. После добавления обоих пользователей в список разрешённых AllowUsers vagrant ahmedfarg вход под ahmedfarg снова стал возможен.





```
35 #LogLevel INFO
36
37 # Authentication:
38
39 #LoginGraceTime 2m
40
41 PermitRootLogin no
42
43 AllowUsers vagrant ahmedfarg
44
45 #StrictModes yes
46 #MaxAuthTries 6
47 #MaxSessions 10
48
49 #PubkeyAuthentication yes
50
51 # The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
52 # but this is overridden so installations will only check .ssh/authorized_keys
53 AuthorizedKeysFile .ssh/authorized_keys
54
55 #AuthorizedPrincipalsFile none
56
57 #AuthorizedKeysCommand none
58 #AuthorizedKeysCommandUser nobody
```



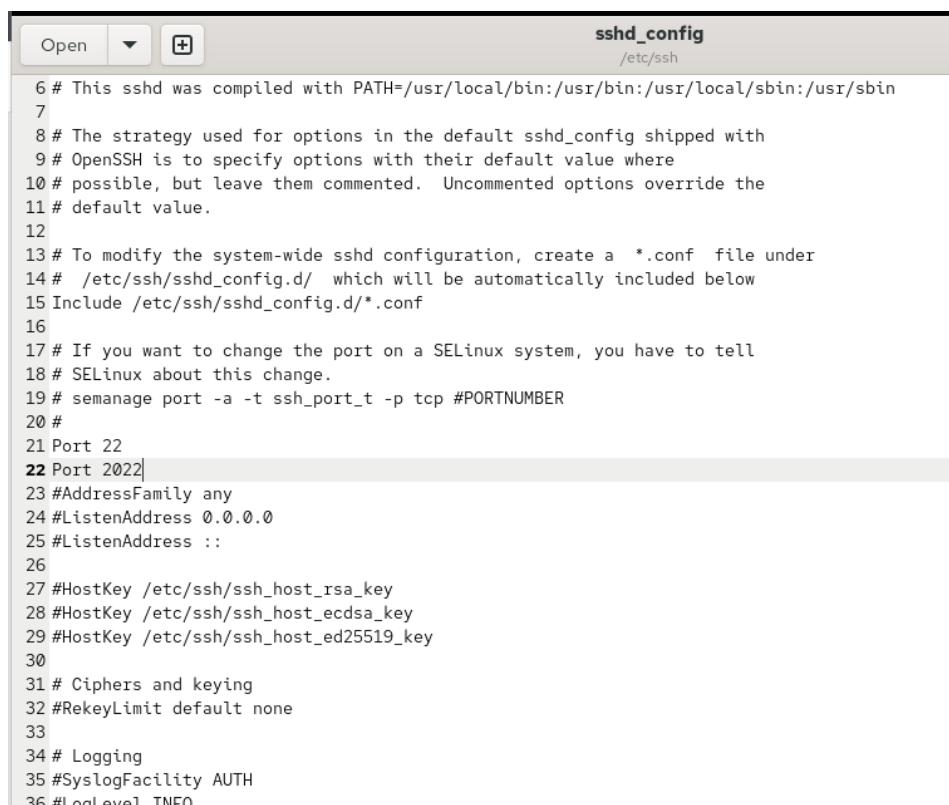
```
[ahmedfarg@client.ahmedfarg.net ~]$ ssh ahmedfarg@server.ahmedfarg.net
ahmedfarg@server.ahmedfarg.net:~$
Web console: https://server.ahmedfarg.net/

Last failed login: Mon Oct 20 08:49:10 UTC 2025
There were 3 failed login attempts
Last login: Mon Oct 20 08:49:10 UTC 2025 on pts/0
[ahmedfarg@server.ahmedfarg.net ~]$
logout
Connection to server.ahmedfarg.net closed.
[ahmedfarg@client.ahmedfarg.net ~]$
```

## 2.3 Настройка дополнительных портов для удалённого доступа по SSH

1. В конфигурационном файле `/etc/ssh/sshd_config` добавлены строки Port 22 и Port 2022.

Это позволяет использовать два порта для подключения по SSH, обеспечивая резервное соединение в случае ошибки конфигурации.

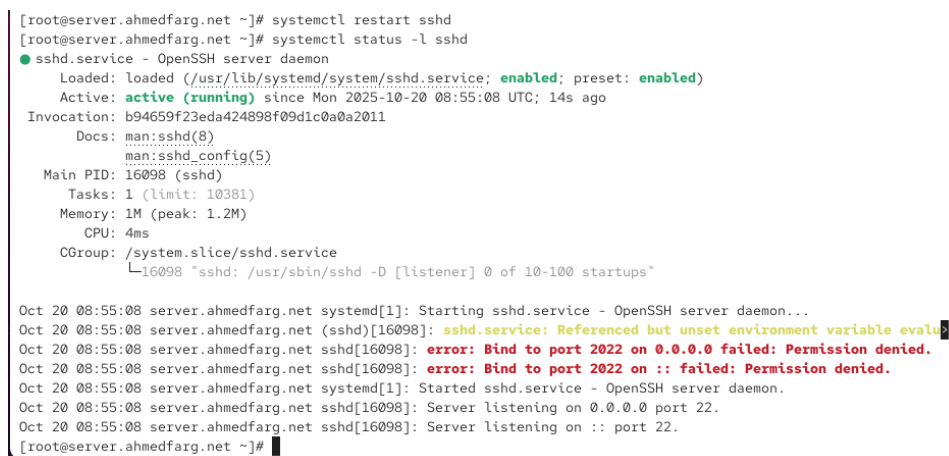


```
6 # This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin
7
8 # The strategy used for options in the default sshd_config shipped with
9 # OpenSSH is to specify options with their default value where
10 # possible, but leave them commented. Uncommented options override the
11 # default value.
12
13 # To modify the system-wide sshd configuration, create a *.conf file under
14 # /etc/ssh/sshd_config.d/ which will be automatically included below
15 Include /etc/ssh/sshd_config.d/*.conf
16
17 # If you want to change the port on a SELinux system, you have to tell
18 # SELinux about this change.
19 # semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
20 #
21 Port 22
22 Port 2022
23 #AddressFamily any
24 #ListenAddress 0.0.0.0
25 #ListenAddress ::
26
27 #HostKey /etc/ssh/ssh_host_rsa_key
28 #HostKey /etc/ssh/ssh_host_ecdsa_key
29 #HostKey /etc/ssh/ssh_host_ed25519_key
30
31 # Ciphers and keying
32 #RekeyLimit default none
33
34 # Logging
35 #SyslogFacility AUTH
36 #LogLevel INFO
```

Рис. 2.3: Добавление второго порта в sshd\_config

2. После сохранения изменений и перезапуска службы sshd команда `systemctl status -l sshd` показала сообщение об ошибке.

Система выдала предупреждение об отказе в доступе к порту 2022 из-за ограничений SELinux.



```
[root@server.ahmedfarg.net ~]# systemctl restart sshd
[root@server.ahmedfarg.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 2025-10-20 08:55:08 UTC; 14s ago
   Invocation: b94659f23eda424898f09d1c0a0a2011
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 16098 (sshd)
     Tasks: 1 (limit: 10381)
    Memory: 1M (peak: 1.2M)
       CPU: 4ms
   CGroup: /system.slice/sshd.service
           └─16098 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 20 08:55:08 server.ahmedfarg.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
Oct 20 08:55:08 server.ahmedfarg.net (sshd)[16098]: sshd.service: Referenced but unset environment variable evalu
Oct 20 08:55:08 server.ahmedfarg.net sshd[16098]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
Oct 20 08:55:08 server.ahmedfarg.net sshd[16098]: error: Bind to port 2022 on :: failed: Permission denied.
Oct 20 08:55:08 server.ahmedfarg.net systemd[1]: Started sshd.service - OpenSSH server daemon.
Oct 20 08:55:08 server.ahmedfarg.net sshd[16098]: Server listening on 0.0.0.0 port 22.
Oct 20 08:55:08 server.ahmedfarg.net sshd[16098]: Server listening on :: port 22.
[root@server.ahmedfarg.net ~]#
```

Рис. 2.4: Ошибка доступа к порту 2022

Это означает, что SELinux блокировал использование нового порта для SSH-подключений.

3. Для устранения проблемы к порту 2022 была добавлена метка SELinux, разрешающая его использование для SSH: команда `semanage port -a -t ssh_port_t -p tcp 2022`.
4. В настройках межсетевого экрана открыт порт 2022 для протокола TCP с помощью команд `firewall-cmd`.

После этого служба `sshd` была перезапущена, и статус показал, что теперь сервер прослушивает оба порта.

```
[root@server.ahmedfarg.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.ahmedfarg.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.ahmedfarg.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.ahmedfarg.net ~]# systemctl restart sshd
[root@server.ahmedfarg.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 2025-10-20 08:56:36 UTC; 3s ago
  Invocation: d9ec207bf99548e592468acaa354ba97
     Docs: man:sshd(8)
           man:sshd_config(5)
    Main PID: 16527 (sshd)
      Tasks: 1 (limit: 10381)
     Memory: 1M (peak: 1.1M)
        CPU: 5ms
    CGroup: /system.slice/sshd.service
            └─16527 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 20 08:56:36 server.ahmedfarg.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
Oct 20 08:56:36 server.ahmedfarg.net (sshd)[16527]: sshd.service: Referenced but unset environment variable evalu
Oct 20 08:56:36 server.ahmedfarg.net sshd[16527]: Server listening on 0.0.0.0 port 2022.
Oct 20 08:56:36 server.ahmedfarg.net sshd[16527]: Server listening on :: port 2022.
Oct 20 08:56:36 server.ahmedfarg.net systemd[1]: Started sshd.service - OpenSSH server daemon.
Oct 20 08:56:36 server.ahmedfarg.net sshd[16527]: Server listening on 0.0.0.0 port 22.
Oct 20 08:56:36 server.ahmedfarg.net sshd[16527]: Server listening on :: port 22.
[root@server.ahmedfarg.net ~]#
```

Рис. 2.5: Открытие порта 2022 и успешный запуск `sshd`

5. С клиента выполнено подключение к серверу по стандартному порту 22, а затем по дополнительному порту 2022.

В обоих случаях соединение установлено успешно, вход выполнен под пользователем `ahmedfarg`, после чего получен доступ `root` с помощью `sudo -i`.

```

[ahmedfarg@client.ahmedfarg.net ~]$ ssh ahmedfarg@server.ahmedfarg.net
ahmedfarg@server.ahmedfarg.net's password:
Web console: https://server.ahmedfarg.net:9090/ or https://192.168.1.1:9090/

Last login: Mon Oct 20 08:51:16 2025 from 192.168.1.30
[ahmedfarg@server.ahmedfarg.net ~]$ sudo -i
[sudo] password for ahmedfarg:
[root@server.ahmedfarg.net ~]#
logout
[ahmedfarg@server.ahmedfarg.net ~]$
logout
Connection to server.ahmedfarg.net closed.
[ahmedfarg@client.ahmedfarg.net ~]$ ssh -p2022 ahmedfarg@server.ahmedfarg.net
ahmedfarg@server.ahmedfarg.net's password:
Web console: https://server.ahmedfarg.net:9090/ or https://192.168.1.1:9090/

Last login: Mon Oct 20 08:59:16 2025 from 192.168.1.30
[ahmedfarg@server.ahmedfarg.net ~]$ sudo -i
[sudo] password for ahmedfarg:
[root@server.ahmedfarg.net ~]#
logout
[ahmedfarg@server.ahmedfarg.net ~]$
logout
Connection to server.ahmedfarg.net closed.
[ahmedfarg@client.ahmedfarg.net ~]$
[ahmedfarg@client.ahmedfarg.net ~]$

```

Рис. 2.6: Подключение по стандартному и дополнительному портам

## 2.4 Настройка удалённого доступа по SSH по ключу

1. В конфигурационном файле `/etc/ssh/sshd_config` на сервере установлен параметр `PubkeyAuthentication yes`, разрешающий аутентификацию по ключам.

```
27 #HostKey /etc/ssh/ssh_host_rsa_key
28 #HostKey /etc/ssh/ssh_host_ecdsa_key
29 #HostKey /etc/ssh/ssh_host_ed25519_key
30
31 # Ciphers and keying
32 #RekeyLimit default none
33
34 # Logging
35 #SyslogFacility AUTH
36 #LogLevel INFO
37
38 # Authentication:
39
40 #LoginGraceTime 2m
41
42 PermitRootLogin no
43
44 AllowUsers vagrant ahmedfarg
45
46 #StrictModes yes
47 #MaxAuthTries 6
48 #MaxSessions 10
49 |
50 PubkeyAuthentication yes
51
```

Рис. 2.7: Разрешение аутентификации по ключу в sshd\_config

2. На клиенте сгенерирована пара SSH-ключей. Закрытый ключ сохранён в `~/.ssh/id_rsa`, открытый — в `~/.ssh/id_rsa.pub`.  
Открытый ключ скопирован на сервер с помощью команды `ssh-copy-id`.
3. После копирования ключа выполнено подключение к серверу. Аутентификация прошла без запроса пароля, что подтверждает корректную настройку SSH-доступа по ключу.

```

      | . . . + = . . = + 0 E |
      | o o . oo + . o . B * |
      | . o . = . . o . . o . + |
      | . = o . . o * o . . |
      | . . . S + + . . |
      | . B . . o |
      | . + . |
      | . |
      +-----[SHA256]-----+
[ahmedfarg@client.ahmedfarg.net ~]$ ssh-copy-id ahmedfarg@server.ahmedfarg.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 t
he new keys
ahmedfarg@server.ahmedfarg.net's password:

Number of key(s) added: 1

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

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

Last login: Mon Oct 20 08:59:39 2025 from 192.168.1.30
[ahmedfarg@server.ahmedfarg.net ~]$
logout
Connection to server.ahmedfarg.net closed.
[ahmedfarg@client.ahmedfarg.net ~]$ █

```

Рис. 2.8: Передача ключа и успешное подключение без пароля

## 2.5 Организация туннелей SSH и перенаправление

### TCP-портов

1. На клиенте выполнена проверка активных TCP-соединений — активных процессов, использующих TCP, не обнаружено.
2. Затем выполнено перенаправление порта 80 сервера на порт 8080 локальной машины с помощью SSH-туннеля.

После выполнения команды `lsof | grep TCP` отображается установленное SSH-соединение и локальное прослушивание порта 8080.

```
ahmedfarg@client.ahmedfarg.net ~$  
[ahmedfarg@client.ahmedfarg.net ~]$ lsof | grep TCP  
[ahmedfarg@client.ahmedfarg.net ~]$ ssh -fNL 8080:localhost:80 ahmedfarg@server.ahmedfarg.net  
[ahmedfarg@client.ahmedfarg.net ~]$ lsof | grep TCP  
ssh      16058          ahmedfarg    3u      IPv4          106560      0t0      TCP clie  
nt.ahmedfarg.net:33522->server.ahmedfarg.net:ssh (ESTABLISHED)  
ssh      16058          ahmedfarg    4u      IPv6          106567      0t0      TCP loca  
lhost:webcache (LISTEN)  
ssh      16058          ahmedfarg    5u      IPv4          106568      0t0      TCP loca  
lhost:webcache (LISTEN)  
[ahmedfarg@client.ahmedfarg.net ~]$
```

Рис. 2.9: Проверка TCP-соединений и организация туннеля SSH

3. При обращении к адресу localhost:8080 в браузере открылась страница приветствия сервера, что подтверждает успешное создание SSH-туннеля.

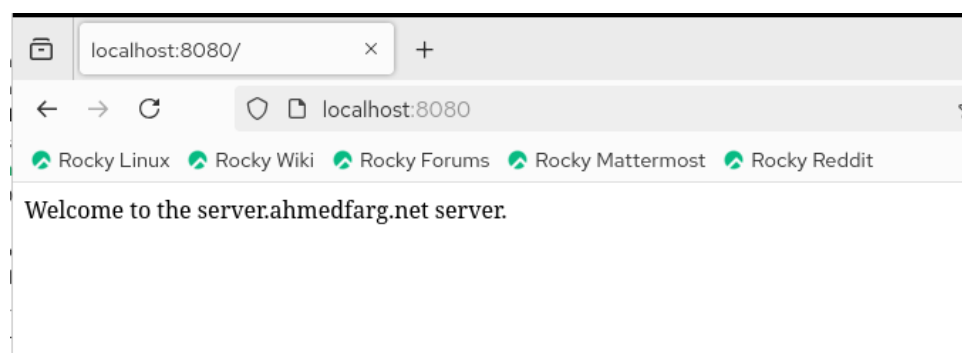


Рис. 2.10: Отображение веб-страницы через туннель SSH

## 2.6 Запуск консольных приложений через SSH

1. С клиента получено имя узла сервера с помощью команды hostname, результат — server.ahmedfarg.net.
2. Выведен список файлов домашнего каталога пользователя на сервере, что подтвердило успешное выполнение удалённой команды через SSH.

```

[ahmedfarg@client.ahmedfarg.net ~]$
[ahmedfarg@client.ahmedfarg.net ~]$ ssh ahmedfarg@server.ahmedfarg.net hostname
server.ahmedfarg.net
[ahmedfarg@client.ahmedfarg.net ~]$ ssh ahmedfarg@server.ahmedfarg.net ls -Al
total 56
-rw-----. 1 ahmedfarg ahmedfarg 368 Oct 15 10:10 .bash_history
-rw-r--r--. 1 ahmedfarg ahmedfarg 18 Oct 29 2024 .bash_logout
-rw-r--r--. 1 ahmedfarg ahmedfarg 144 Oct 29 2024 .bash_profile
-rw-r--r--. 1 ahmedfarg ahmedfarg 549 Sep 17 08:04 .bashrc
drwx-----. 11 ahmedfarg ahmedfarg 4096 Sep 17 08:17 .cache
drwx-----. 10 ahmedfarg ahmedfarg 4096 Sep 17 09:48 .config
drwxr-xr-x. 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Desktop
drwxr-xr-x. 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Documents
drwxr-xr-x. 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Downloads
drwx-----. 4 ahmedfarg ahmedfarg 32 Sep 17 08:17 .local
drwx-----. 5 ahmedfarg ahmedfarg 4096 Oct 15 10:06 Maildir
drwxr-xr-x. 5 ahmedfarg ahmedfarg 54 Sep 17 08:17 .mozilla
drwxr-xr-x. 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Music
drwxr-xr-x. 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Pictures
drwxr-xr-x. 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Public
drwx-----. 2 ahmedfarg ahmedfarg 29 Oct 20 09:02 .ssh
drwxr-xr-x. 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Templates
-rw-r-----. 1 ahmedfarg ahmedfarg 6 Oct 20 08:39 .vboxclient-clipboard-tty2-control.pid
-rw-r-----. 1 ahmedfarg ahmedfarg 6 Oct 20 09:05 .vboxclient-clipboard-tty2-service.pid
-rw-r-----. 1 ahmedfarg ahmedfarg 6 Oct 20 08:39 .vboxclient-draganddrop-tty2-control.pid
-rw-r-----. 1 ahmedfarg ahmedfarg 6 Oct 20 08:39 .vboxclient-hostversion-tty2-control.pid
-rw-r-----. 1 ahmedfarg ahmedfarg 6 Oct 20 08:39 .vboxclient-seamless-tty2-control.pid
-rw-r-----. 1 ahmedfarg ahmedfarg 6 Oct 20 08:39 .vboxclient-vmvga-session-tty2-control.pid
-rw-r-----. 1 ahmedfarg ahmedfarg 6 Oct 20 08:39 .vboxclient-vmvga-session-tty2-service.pid
drwxr-xr-x. 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Videos
[ahmedfarg@client.ahmedfarg.net ~]$
[ahmedfarg@client.ahmedfarg.net ~]$ █

```

Рис. 2.11: Проверка имени хоста и содержимого домашнего каталога

### 3. Проверена работа почтовой программы в каталоге Maildir удалённого пользователя.

На экране отобразился список писем, хранящихся в почтовом каталоге.

```

[ahmedfarg@client.ahmedfarg.net ~]$
[ahmedfarg@client.ahmedfarg.net ~]$ ssh ahmedfarg@server.ahmedfarg.net MAIL=~/.Maildir mail
s-nail version v14.9.24. Type '?' for help
/home/ahmedfarg/Maildir: 3 messages 2 unread
 1 ahmedfarg      2025-10-11 13:27   18/650   "test"           "
►U 2 ahmedfarg@client.ahm 2025-10-15 09:33   21/838   "LMTP test"      "
 U 3 ahmedfarg      2025-10-15 10:06   22/820   "nettest"        "
q
Held 3 messages in /home/ahmedfarg/Maildir
[ahmedfarg@client.ahmedfarg.net ~]$ █

```

Рис. 2.12: Просмотр почты пользователя через SSH



## 2.7 Запуск графических приложений через SSH (X11 Forwarding)

1. В конфигурационном файле `/etc/ssh/sshd_config` на сервере включён параметр `X11Forwarding yes` и перезапущен `sshd`.

```
85 #GSSAPICleanupCredentials yes
86 #GSSAPIStrictAcceptorCheck yes
87 #GSSAPIKeyExchange no
88 #GSSAPIEnablek5users no
89
90 # Set this to 'yes' to enable PAM authentication, account processing,
91 # and session processing. If this is enabled, PAM authentication will
92 # be allowed through the KbdInteractiveAuthentication and
93 # PasswordAuthentication. Depending on your PAM configuration,
94 # PAM authentication via KbdInteractiveAuthentication may bypass
95 # the setting of "PermitRootLogin prohibit-password".
96 # If you just want the PAM account and session checks to run without
97 # PAM authentication, then enable this but set PasswordAuthentication
98 # and KbdInteractiveAuthentication to 'no'.
99 # WARNING: 'UsePAM no' is not supported in this build and may cause several
100 # problems.
101 #UsePAM no
102
103 #AllowAgentForwarding yes
104 #AllowTcpForwarding yes
105 #GatewayPorts no
106 X11Forwarding yes
107 #X11DisplayOffset 10
108 #X11UseLocalhost yes
109 #PermitTTY yes
110 #PrintMotd yes
111 #PrintLastLog yes
112 #TCPKeepAlive yes
113 #PermitUserEnvironment no
114 #Compression delayed
115 #ClientAliveInterval 0
116 #ClientAliveCountMax 3
117 #UseDNS no
```

Рис. 2.13: Разрешение `X11Forwarding` в `sshd_config`

2. При попытке запустить графическое приложение `firefox` через SSH с клиента выводится сообщение об ошибке — отсутствует переменная `DISPLAY`, что свидетельствует о невозможности запуска X11-сеанса в текущих настройках среды.

```
[ahmedfarg@client.ahmedfarg.net ~]$
[ahmedfarg@client.ahmedfarg.net ~]$ ssh -YC ahmedfarg@server.ahmedfarg.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
[ahmedfarg@client.ahmedfarg.net ~]$ ssh -YC ahmedfarg@server.ahmedfarg.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
[ahmedfarg@client.ahmedfarg.net ~]$ █
```

Рис. 2.14: Ошибка при попытке запуска графического приложения через SSH

## 2.8 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На сервере создан каталог `/vagrant/provision/server/ssh` с подкаталогом `etc/ssh`, в который был скопирован текущий файл конфигурации `sshd_config`.

Это позволяет хранить настройки SSH в структуре проекта Vagrant.

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

Рис. 2.15: Создание каталогов и копирование файла `sshd_config`

2. В каталоге `/vagrant/provision/server` создан исполняемый файл `ssh.sh`, содержащий команды для автоматической настройки SSH.

Скрипт выполняет копирование конфигурационных файлов, настройку SELinux и межсетевого экрана, а также перезапускает службу `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
13
```

Рис. 2.16: Содержимое скрипта ssh.sh для автоматизации настройки SSH

## 3 Заключение

В ходе лабораторной работы были освоены методы администрирования SSH-сервера: настройка портов, ограничение доступа пользователей, создание туннелей, запуск консольных и графических приложений, а также автоматизация конфигурации с помощью скрипта.

Результаты подтвердили корректность работы SSH при изменённых параметрах безопасности и сетевого взаимодействия.

## 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 параметр `PermitRootLogin` no для запрета входа root и добавить строку `AllowUsers alice` для разрешения входа пользователю alice.

После внесения изменений необходимо перезапустить службу SSH.

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

В файле `/etc/ssh/sshd_config` указать несколько строк с параметром `Port`, например `Port 22` и `Port 2022`.

Это обеспечивает резервный канал подключения в случае блокировки или ошибки на основном порту.

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

Используются параметры `fNL`, где `f` переводит соединение в фоновый режим, `N` запрещает выполнение удалённых команд, а `L` задаёт локальное перенаправление портов.

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

Необходимо использовать перенаправление с указанием локального и уда-

лённого портов, чтобы обращения к адресу localhost:5555 перенаправлялись на порт 80 сервера server2.example.com.

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

Добавить разрешение для SELinux, установив метку безопасности ssh\_port\_t для порта 2022, чтобы процесс SSH мог использовать этот порт.

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

Добавить разрешающее правило в межсетевой экран firewalld для порта 2022 протокола TCP и сохранить изменения для постоянного применения.