

# **Отчёт по лабораторной работе №11**

**Дисциплина: Администрирование сетевых подсистем**

Ибрахим Мухсейн Алькамаль

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Выполнение лабораторной работы</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, перенаправление TCP-портов . . . . .	13
2.6 Запуск консольных приложений через SSH . . . . .	14
2.7 Запуск графических приложений через SSH (X11Forwarding) . . . . .	15
2.8 Внесение изменений в настройки внутреннего . . . . .	17
<b>3 Выводы</b>	<b>19</b>
<b>4 Контрольные вопросы</b>	<b>20</b>

# Список иллюстраций

2.1	Изменение пароля пользователя root с помощью passwd . . . . .	6
2.2	Отказ в аутентификации при SSH-подключении пользователя root . . . . .	7
2.3	Параметр PermitRootLogin no в файле sshd_config . . . . .	7
2.4	Повторная ошибка SSH-аутентификации после запрета входа root . . . . .	7
2.5	Успешное SSH-подключение пользователя alkamal к серверу . . . . .	8
2.6	Добавление директивы AllowUsers vagrant в sshd_config . . . . .	8
2.7	Перезапуск службы sshd после изменения конфигурации . . . . .	8
2.8	Отказ в SSH-доступе пользователю alkamal после ограничения AllowUsers . . . . .	9
2.9	Расширение списка AllowUsers: vagrant alkamal . . . . .	9
2.10	Успешное SSH-подключение после добавления пользователя в AllowUsers . . . . .	9
2.11	Добавление порта 2022 в конфигурацию sshd . . . . .	10
2.12	Ошибка привязки к порту 2022 в статусе sshd . . . . .	10
2.13	Настройка SELinux и firewall для порта 2022 . . . . .	11
2.14	sshd прослушивает порты 22 и 2022 . . . . .	11
2.15	Успешное SSH-подключение через порт 2022 . . . . .	11
2.16	Параметр PubkeyAuthentication yes в sshd_config . . . . .	12
2.17	Генерация пары SSH-ключей командой ssh-keygen . . . . .	12
2.18	Копирование открытого ключа на сервер с помощью ssh-copy-id . . . . .	12
2.19	Успешная SSH-аутентификация по ключу без ввода пароля . . . . .	13
2.20	Проверка активных TCP-соединений до создания SSH-туннеля . . . . .	13
2.21	Прослушивание локального порта 8080 процессом ssh . . . . .	14
2.22	Доступ к веб-серверу через SSH-туннель на localhost:8080 . . . . .	14
2.23	Удалённое выполнение команды hostname через SSH . . . . .	14
2.24	Удалённый вывод списка файлов командой ls -Al . . . . .	15
2.25	Удалённый просмотр почты через консольное приложение mail . . . . .	15
2.26	Параметр X11Forwarding yes в sshd_config . . . . .	16
2.27	Запуск Firefox на сервере с отображением на клиенте через SSH X11Forwarding . . . . .	16
2.28	Копирование файла sshd_config в каталог provision/server/ssh . . . . .	17
2.29	Содержимое скрипта ssh.sh для автоматической настройки SSH . . . . .	17
2.30	Добавление provision-блока для ssh.sh в Vagrantfile . . . . .	18

# **Список таблиц**

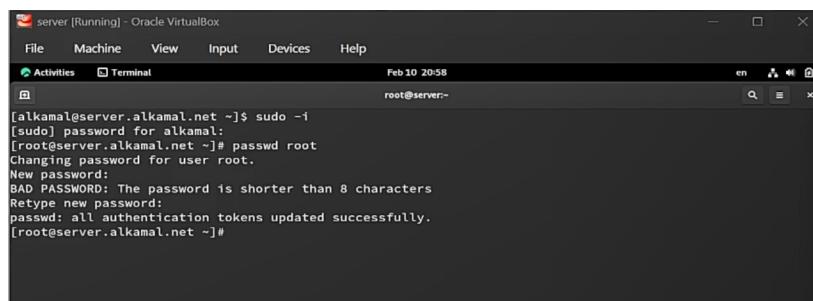
# **1 Цель работы**

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

## 2 Выполнение лабораторной работы

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

Выполнен вход на сервер под пользователем с административными привилегиями и задан пароль для пользователя root с помощью команд sudo -i и passwd root. В процессе изменения пароля система выдала предупреждение о недостаточной длине пароля, после чего пароль был успешно обновлён (рис. 2.1).

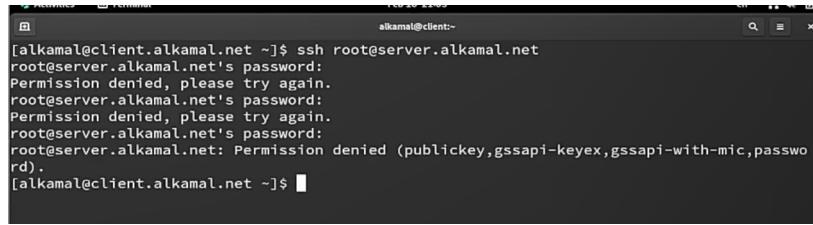


The screenshot shows a terminal window titled 'server [Running] - Oracle VirtualBox'. The window has a dark background and white text. At the top, there's a menu bar with 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help'. Below the menu is a toolbar with icons for 'Activities' and 'Terminal'. The status bar at the bottom shows 'Feb 10 20:58' and 'root@server:~'. The main area of the terminal shows the following command sequence:

```
[alkamal@server.alkamal.net ~]$ sudo -i  
[sudo] password for alkamal:  
[root@server.alkamal.net ~]# passwd root  
Changing password for user root.  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@server.alkamal.net ~]#
```

Рисунок 2.1: Изменение пароля пользователя root с помощью passwd

С клиента выполнена попытка подключения к серверу по SSH от имени пользователя root с помощью команды ssh root@server.alkamal.net. Аутентификация завершилась ошибкой Permission denied, что свидетельствует об отклонении доступа сервером (рис. 2.2).



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

Рисунок 2.2: Отказ в аутентификации при SSH-подключении пользователя root

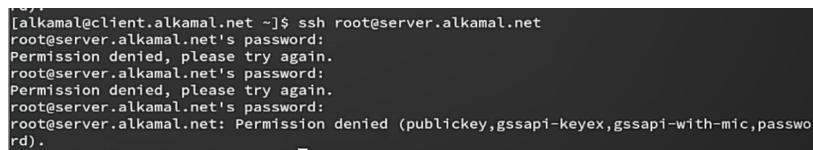
В конфигурационном файле `/etc/ssh/sshd_config` на сервере установлен параметр `PermitRootLogin no`, запрещающий удалённый вход пользователя root по SSH (рис. 2.3).



```
# Authentication:
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#RSAAuthentication yes
#PubkeyAuthentication yes
```

Рисунок 2.3: Параметр `PermitRootLogin no` в файле `sshd_config`

После перезапуска службы `sshd` повторная попытка подключения с клиента под пользователем root завершилась сообщением `Permission denied (publickey, gssapi-keyex, gssapi-with-mic, password)`, что подтверждает успешный запрет удалённого доступа для root (рис. 2.4).



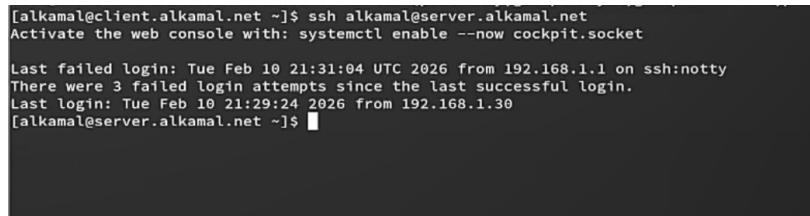
```
[alkamal@client.alkamal.net ~]$ ssh root@server.alkamal.net
root@server.alkamal.net's password:
Permission denied, please try again.
root@server.alkamal.net's password:
Permission denied, please try again.
root@server.alkamal.net's password:
root@server.alkamal.net: Permission denied (publickey,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

Рисунок 2.4: Повторная ошибка SSH-аутентификации после запрета входа root

## 2.2 Ограничение списка пользователей для удалённого доступа по SSH

С клиента выполнено SSH-подключение к серверу под пользователем alkamal с помощью команды `ssh alkamal@server.alkamal.net`. Аутентификация

прошла успешно, о чём свидетельствует вывод приглашения командной строки удалённой системы и информация о предыдущих входах (рис. 2.5).

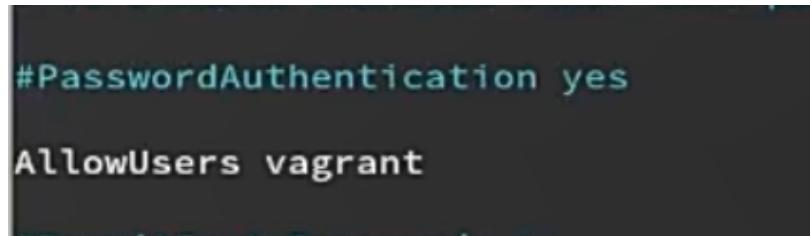


```
[alkamal@client.alkamal.net ~]$ ssh alkamal@server.alkamal.net
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Tue Feb 10 21:31:04 UTC 2026 from 192.168.1.1 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Tue Feb 10 21:29:24 2026 from 192.168.1.30
[alkamal@server.alkamal.net ~]$
```

Рисунок 2.5: Успешное SSH-подключение пользователя alkamal к серверу

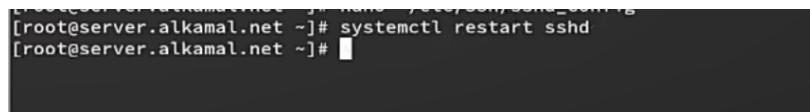
В конфигурационном файле `/etc/ssh/sshd_config` добавлена строка `AllowUsers vagrant`, ограничивающая список пользователей, которым разрешён удалённый доступ по SSH (рис. 2.6).



```
#PasswordAuthentication yes
AllowUsers vagrant
```

Рисунок 2.6: Добавление директивы `AllowUsers vagrant` в `sshd_config`

После внесения изменений выполнен перезапуск службы `sshd` командой `systemctl restart sshd` для применения новой конфигурации (рис. 2.7).



```
[root@server.alkamal.net ~]# systemctl restart sshd
[root@server.alkamal.net ~]#
```

Рисунок 2.7: Перезапуск службы `sshd` после изменения конфигурации

Повторная попытка подключения с клиента под пользователем `alkamal` завершилась ошибкой `Permission denied`, что связано с отсутствием данного пользователя в списке, указанном в директиве `AllowUsers` (рис. 2.8).

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

Рисунок 2.8: Отказ в SSH-доступе пользователю alkamal после ограничения AllowUsers

В файл /etc/ssh/sshd\_config внесено изменение: строка AllowUsers vagrant заменена на AllowUsers vagrant alkamal, что добавляет пользователя alkamal в разрешённый список (рис. 2.9).

```
# 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
AllowUsers  vagrant alkamal
#AuthorizedPrincipalsFile none
```

Рисунок 2.9: Расширение списка AllowUsers: vagrant alkamal

После повторного перезапуска службы sshd выполнена новая попытка подключения с клиента под пользователем alkamal, которая завершилась успешно, что подтверждается появлением приглашения командной строки сервера (рис. 2.10).

```
alkamal@server.alkamal.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password)
[alkamal@client.alkamal.net ~]$ ssh alkamal@server.alkamal.net
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Tue Feb 10 22:29:40 UTC 2026 from 192.168.1.30 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Tue Feb 10 22:24:51 2026 from 192.168.1.30
[alkamal@server.alkamal.net ~]$
```

Рисунок 2.10: Успешное SSH-подключение после добавления пользователя в AllowUsers

## 2.3 Настройка дополнительных портов для

### удалённого доступа по SSH

В конфигурационном файле /etc/ssh/sshd\_config добавлена дополнительная строка Port 2022 ниже существующей строки Port 22, что задаёт

прослушивание двух TCP-портов процессом sshd (рис. 2.11).

```
#  
Port 22  
Port 2022  
#AddressFamily any  
#ListenAddress 0.0.0.0  
#ListenAddress ::
```

Рисунок 2.11: Добавление порта 2022 в конфигурацию sshd

После перезапуска службы выполнена проверка расширенного статуса systemctl status -l sshd. В журнале зафиксированы сообщения error: Bind to port 2022 ... failed: Permission denied, что указывает на запрет использования данного порта механизмом SELinux. При этом служба продолжила работу на порту 22 (рис. 2.12).

```
[root@server.alkamal.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 Tue 2026-02-10 21:16:15 UTC; 5s ago  
    Docs: man:sshd(8)  
          man:sshd_config(5)  
   Main PID: 11813 (sshd)  
     Tasks: 1 (limit: 4493)  
    Memory: 1.7M (peak: 2.0M)  
      CPU: 4ms  
     CGroup: /system.slice/sshd.service  
             └─11813 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"  
  
Feb 10 21:16:15 server.alkamal.net systemd[1]: Starting OpenSSH server daemon..  
Feb 10 21:16:15 server.alkamal.net sshd[11813]: error: Bind to port 2022 on 0.0.0.0 failed: Permission >  
Feb 10 21:16:15 server.alkamal.net sshd[11813]: error: Bind to port 2022 on :: failed: Permission deni >  
Feb 10 21:16:15 server.alkamal.net sshd[11813]: Server listening on 0.0.0.0 port 22.  
Feb 10 21:16:15 server.alkamal.net systemd[1]: Started OpenSSH server daemon.  
Feb 10 21:16:15 server.alkamal.net sshd[11813]: Server listening on :: port 22.  
[lines 1-18/18. (END)]
```

Рисунок 2.12: Ошибка привязки к порту 2022 в статусе sshd

Для разрешения использования порта 2022 выполнено добавление соответствующей метки SELinux командой semanage port -a -t ssh\_port\_t -p tcp 2022, а также открыт порт в межсетевом экране с помощью firewall-cmd. После этого служба sshd перезапущена (рис. 2.13).

```
[root@server.alkamal.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.alkamal.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.alkamal.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.alkamal.net ~]# systemctl restart sshd
[root@server.alkamal.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 Tue 2026-02-10 21:19:32 UTC; 4s ago
      Docs: man:sshd(8)
             man:sshd_config(5)
      Main PID: 11844 (sshd)
         Tasks: 1 (limit: 4493)
        Memory: 2.2M (peak: 2.4M)
          CPU: 6ms
         CGroup: /system.slice/sshd.service
                   └─11844 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Feb 10 21:19:32 server.alkamal.net systemd[1]: Starting OpenSSH server daemon...
Feb 10 21:19:32 server.alkamal.net sshd[11844]: Server listening on 0.0.0.0 port 2022.
Feb 10 21:19:32 server.alkamal.net sshd[11844]: Server listening on :: port 2022.
Feb 10 21:19:32 server.alkamal.net sshd[11844]: Server listening on 0.0.0.0 port 22.
Feb 10 21:19:32 server.alkamal.net sshd[11844]: Server listening on :: port 22.
Feb 10 21:19:32 server.alkamal.net systemd[1]: Started OpenSSH server daemon.
[root@server.alkamal.net ~]#
```

Рисунок 2.13: Настройка SELinux и firewall для порта 2022

Повторная проверка статуса службы показала, что `sshd` прослушивает порты 22 и 2022 на адресах 0.0.0.0 и ::, что подтверждает корректную настройку (рис. 2.14).

```
[root@server.alkamal.net ~]# ss -tnlp | grep sshd
alkamal@server.alkamal.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Feb 10 21:14:37 2026 from 192.168.1.1
[alkamal@server.alkamal.net ~]$ sudo -i
[sudo] password for alkamal:
[root@server.alkamal.net ~]# logout
[alkamal@server.alkamal.net ~]$ logout
Connection to server.alkamal.net closed.
[alkamal@server.alkamal.net ~]$ logout
Connection to server.alkamal.net closed.
[alkamal@server.alkamal.net ~]$ exit
logout
Connection to server.alkamal.net closed.
```

Рисунок 2.14: sshd прослушивает порты 22 и 2022

С клиента выполнено подключение к серверу с указанием альтернативного порта `ssh -p2022 alkamal@server.alkamal.net`. Аутентификация прошла успешно, после чего выполнен переход в режим суперпользователя `sudo -i` и корректный выход из сеанса (рис. 2.15).

```
[root@client.alkamal.net ~]$ ssh -p2022 alkamal@server.alkamal.net
alkamal@server.alkamal.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Feb 10 21:20:20 2026 from 192.168.1.1
[alkamal@server.alkamal.net ~]$ sudo -i
[sudo] password for alkamal:
[root@server.alkamal.net ~]#
logout
[alkamal@server.alkamal.net ~]$ logout
Connection to server.alkamal.net closed.
[alkamal@client.alkamal.net ~]$ █
```

Рисунок 2.15: Успешное SSH-подключение через порт 2022

## 2.4 Настройка удалённого доступа по SSH по ключу

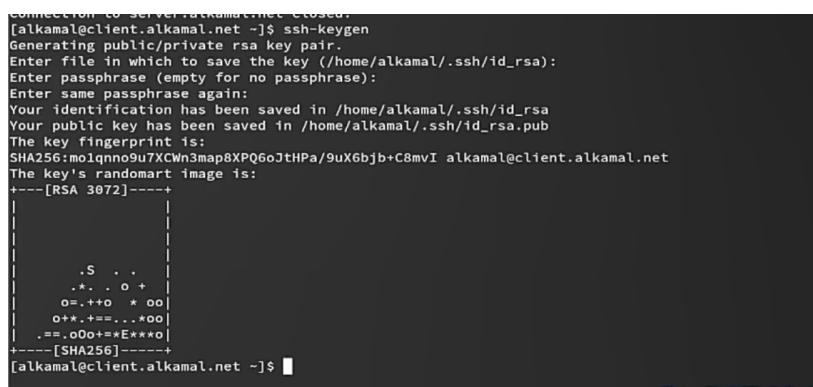
В конфигурационном файле `/etc/ssh/sshd_config` на сервере установлен параметр `PubkeyAuthentication yes`, разрешающий аутентификацию по открытому ключу (рис. 2.16).



```
PubkeyAuthentication yes
# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
```

Рисунок 2.16: Параметр `PubkeyAuthentication yes` в `sshd_config`

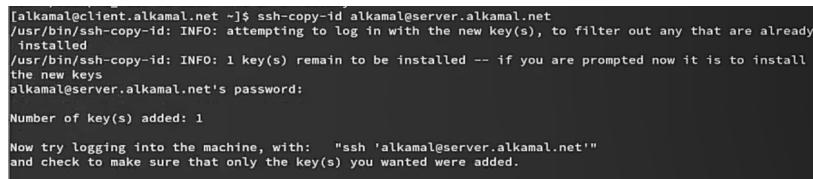
На клиенте под пользователем `alkamal` выполнена генерация пары RSA-ключей с помощью команды `ssh-keygen`. Закрытый ключ сохранён в файл `~/.ssh/id_rsa`, открытый – в `~/.ssh/id_rsa.pub`, что подтверждается выводом утилиты (рис. 2.17).



```
connection to server alkamal.net closed.
[alkamal@client.alkamal.net ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/alkamal/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/alkamal/.ssh/id_rsa
Your public key has been saved in /home/alkamal/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:moiQnno9u7xCWn3map8XPQ6oJtHPa/9uX6bjb+C8mvI alkamal@client.alkamal.net
The key's randomart image is:
+---[RSA 3072]----+
| |
| |
| |
| .S . .
| .. . o +
| o=.=+o * oo
| o+*.+=...*oo
| .==.oo+=**E**o
+---[SHA256]----+
[alkamal@client.alkamal.net ~]$
```

Рисунок 2.17: Генерация пары SSH-ключей командой `ssh-keygen`

Открытый ключ скопирован на сервер командой `ssh-copy-id alkamal@server.alkamal.net`. После ввода пароля пользователя ключ добавлен в файл `~/.ssh/authorized_keys` на сервере (рис. 2.18).



```
[alkamal@client.alkamal.net ~]$ ssh-copy-id alkamal@server.alkamal.net
/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
alkamal@server.alkamal.net's password:
Number of key(s) added: 1

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

Рисунок 2.18: Копирование открытого ключа на сервер с помощью `ssh-copy-id`

Повторное подключение к серверу выполнено командой `ssh alkamal@server.alkamal.net`. Аутентификация прошла без запроса пароля, что подтверждается непосредственным входом в оболочку удалённой системы (рис. 2.19).

```
[alkamal@client.alkamal.net ~]$ ssh alkamal@server.alkamal.net
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Feb 10 21:24:52 2026 from 192.168.1.30
[alkamal@server.alkamal.net ~]$ █
```

Рисунок 2.19: Успешная SSH-аутентификация по ключу без ввода пароля

## 2.5 Организация туннелей SSH, перенаправление TCP-портов

На клиенте выполнена проверка активных TCP-соединений командой `lsof | grep TCP`. До организации туннеля отсутствовали локальные прослушивающие сокеты на порту 8080 (рис. 2.21).

```
[alkamal@client.alkamal.net ~]$ lsof | grep TCP
[alkamal@client.alkamal.net ~]$ ssh -fNL 8080:localhost:80 alkamal@server.alkamal.net
[alkamal@client.alkamal.net ~]$ lsof | grep TCP
ssh          11483      alkamal    3u      IPv4          74098      0t0      TCP  client.alkamal.net:48060->mail.alkamal.net:ssh (ESTABLISHED)
ssh          11483      alkamal    4u      IPv6          74117      0t0      TCP  localhost:webcache (LISTEN)
ssh          11483      alkamal    5u      IPv4          74118      0t0      TCP  localhost:webcache (LISTEN)
[alkamal@client.alkamal.net ~]$ █
```

Рисунок 2.20: Проверка активных TCP-соединений до создания SSH-туннеля

Выполнена команда `ssh -fNL 8080:localhost:80 alkamal@server.alkamal.net` создающая локальный SSH-туннель. Параметр `-L 8080:localhost:80` организует перенаправление: локальный порт 8080 клиента связывается с портом 80 сервера через защищённое SSH-соединение. Повторный вывод `lsof | grep TCP` показывает процесс `ssh`, прослушивающий порт `localhost:8080` (`web-cache`), а также установленное SSH-соединение в состоянии `ESTABLISHED`, что подтверждает успешное создание туннеля (рис. 2.21).

```
[alkamal@client.alkamal.net ~]$ lsof | grep TCP
[alkamal@client.alkamal.net ~]$ ssh -NL 8080:localhost:80 alkamal@server.alkamal.net
[alkamal@client.alkamal.net ~]$ lsof | grep TCP
ssh      11483          alkamal  3u    IPv4          74098      0t0      TCP  client.alkamal.net:48660->mail.alkamal.net:ssh (ESTABLISHED)
ssh      11483          alkamal  4u    IPv6          74117      0t0      TCP  client.alkamal.net:48660->mail.alkamal.net:ssh (ESTABLISHED)
ssh      11483          alkamal  5u    IPv4          74118      0t0      TCP  client.alkamal.net:48660->mail.alkamal.net:ssh (ESTABLISHED)
[alkamal@client.alkamal.net ~]$
```

Рисунок 2.21: Прослушивание локального порта 8080 процессом ssh

На клиенте в браузере открыт адрес `http://localhost:8080`. Отображается страница приветствия «Welcome to the server.alkamal.net server», что подтверждает корректное перенаправление HTTP-трафика через SSH-туннель на веб-сервер, работающий на сервере (рис. 2.22).

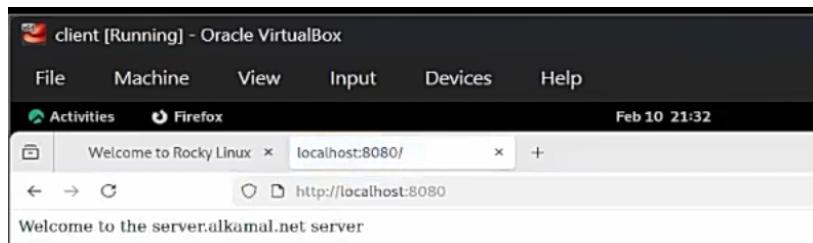


Рисунок 2.22: Доступ к веб-серверу через SSH-туннель на localhost:8080

## 2.6 Запуск консольных приложений через SSH

С клиента под пользователем `alkamal` выполнена команда `ssh alkamal@server.alkamal hostname`, которая запускает на удалённом сервере консольную утилиту `hostname`. В ответ получено имя узла `server.alkamal.net`, что подтверждает удалённое выполнение команды через SSH (рис. 2.23).

```
[alkamal@client.alkamal.net ~]$ ssh alkamal@server.alkamal.net hostname
server.alkamal.net
```

Рисунок 2.23: Удалённое выполнение команды `hostname` через SSH

Командой `ssh alkamal@server.alkamal.net ls -Al` получен подробный список файлов домашнего каталога пользователя на сервере. Вывод содержит права доступа, владельца, размер и дату изменения файлов, что подтверждает корректное удалённое выполнение команды `ls` (рис. 2.24).

```
[alkamal@client.alkamal.net ~]$ ssh alkamal@server.alkamal.net ls -Al
total 72
-rw-----. 1 alkamal alkamal 1896 Feb 18 21:31 .bash_history
-rw-r--r--. 1 alkamal alkamal 18 Apr 30 2024 .bash_logout
-rw-r--r--. 1 alkamal alkamal 141 Apr 30 2024 .bash_profile
-rw-r--r--. 1 alkamal alkamal 546 Feb 6 13:50 .bashrc
drwx----- 11 alkamal alkamal 4096 Feb 18 13:09 .cache
drwx----- 11 alkamal alkamal 4096 Feb 18 13:09 .config
drwxr-xr-x. 2 alkamal alkamal 6 Feb 6 13:50 Desktop
drwxr-xr-x. 2 alkamal alkamal 6 Feb 6 13:50 Documents
drwxr-xr-x. 2 alkamal alkamal 6 Feb 6 13:50 Downloads
-rw----- 1 alkamal alkamal 28 Feb 18 13:41 .lessht
drwx----- 4 alkamal alkamal 32 Feb 6 13:50 .local
drwx----- 5 alkamal alkamal 4096 Feb 18 16:08 Maildir
drwxr-xr-x. 4 alkamal alkamal 39 Feb 6 02:09 .mozilla
drwxr-xr-x. 2 alkamal alkamal 6 Feb 6 13:50 Music
drwxr-xr-x. 2 alkamal alkamal 4096 Feb 9 20:57 Pictures
drwxr-xr-x. 2 alkamal alkamal 6 Feb 6 13:50 Public
drwxr-xr-x. 2 alkamal alkamal 71 Feb 18 21:28 .ssh
drwxr-xr-x. 2 alkamal alkamal 6 Feb 6 13:50 Templates
-rw-r----- 1 alkamal alkamal 6 Feb 18 19:41 .vboxclient-clipboard-tty1-control.pid
-rw-r----- 1 alkamal alkamal 6 Feb 18 19:41 .vboxclient-clipboard-tty1-service.pid
-rw-r----- 1 alkamal alkamal 6 Feb 18 19:41 .vboxclient-draganddrop-tty1-control.pid
-rw-r----- 1 alkamal alkamal 6 Feb 18 19:41 .vboxclient-draganddrop-tty1-service.pid
-rw-r----- 1 alkamal alkamal 6 Feb 18 19:41 .vboxclient-hostversion-tty1-control.pid
-rw-r----- 1 alkamal alkamal 6 Feb 18 19:41 .vboxclient-seamless-tty1-control.pid
-rw-r----- 1 alkamal alkamal 6 Feb 18 19:41 .vboxclient-seamless-tty1-service.pid
-rw-r----- 1 alkamal alkamal 6 Feb 18 19:41 .vboxclient-vmsvga-session-tty1-control.pid
-rw-r----- 1 alkamal alkamal 6 Feb 18 19:41 .vboxclient-vmsvga-session-tty1-service.pid
drwxr-xr-x. 2 alkamal alkamal 6 Feb 6 13:50 Videos
-rw-----. 1 alkamal alkamal 6 Feb 18 19:41 .xsession-errors
-rw-----. 1 alkamal alkamal 6 Feb 18 13:09 .xsession-errors.old
```

Рисунок 2.24: Удалённый вывод списка файлов командой ls -Al

Командой ssh alkamal@server.alkamal.net MAIL=~/Maildir/mail выполнен запуск почтового клиента mail на сервере с указанием каталога Maildir. В выводе отображены 4 почтовых сообщения с указанием отправителя, даты и темы, что подтверждает успешный запуск консольного приложения на удалённой системе (рис. 2.25).

```
[alkamal@client.alkamal.net ~]$ ssh alkamal@server.alkamal.net MAIL=~/Maildir/ mail
s-mail version v14.9.22. Type `?' for help
/home/alkamal/Maildir: 4 messages
• 1 alkamal 2026-02-09 19:59 18/603 "Test 1"
  2 alkamal 2026-02-09 20:48 18/620 "test3"
  3 alkamal@client.alkam 2026-02-10 14:47 21/789 "LMTP test"
  4 alkamal 2026-02-10 15:58 22/802 "test 5"

quit
Held 4 messages in /home/alkamal/Maildir
[alkamal@client.alkamal.net ~]$ █
```

Рисунок 2.25: Удалённый просмотр почты через консольное приложение mail

## 2.7 Запуск графических приложений через SSH (X11Forwarding)

В конфигурационном файле /etc/ssh/sshd\_config на сервере установлен параметр X11Forwarding yes, разрешающий пересылку графического трафика X11 через SSH-соединение (рис. 2.26).

```
#GatewayPorts no
X11Forwarding yes

^G Help      ^O Write Out  ^W Where Is  ^K Cut
^X Exit      ^R Read File  ^\ Replace  ^U Paste
```

Рисунок 2.26: Параметр X11Forwarding yes в sshd\_config

С клиента выполнено подключение с поддержкой X11-перенаправления командой `ssh -YC alkamal@server.alkamal.net firefox`. Параметр `-Y` включает доверенное X11-перенаправление, `-C` активирует сжатие трафика. В результате графическое приложение Firefox, запущенное на сервере, отобразилось на клиентской машине, что подтверждает корректную работу X11Forwarding (рис. 2.27).

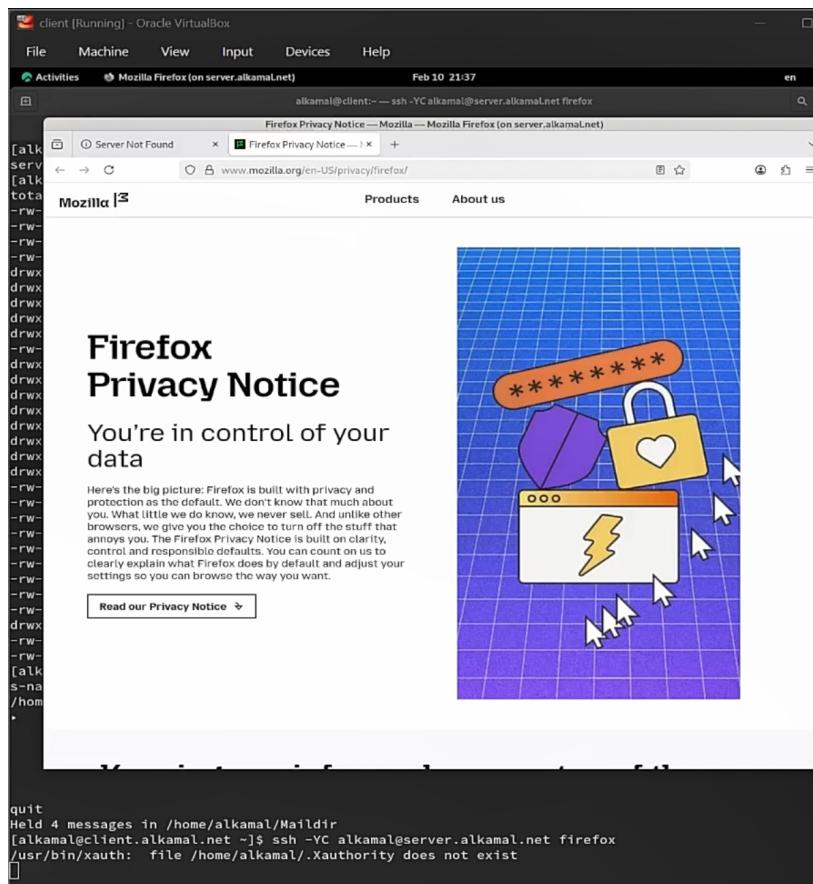


Рисунок 2.27: Запуск Firefox на сервере с отображением на клиенте через SSH X11Forwarding

## 2.8 Внесение изменений в настройки внутреннего

На виртуальной машине **server** выполнен переход в каталог `/vagrant/provision/server`, создан каталог `ssh/etc/ssh` и в него скопирован конфигурационный файл `sshd_config`, что обеспечивает сохранение настроек SSH во внутреннем окружении Vagrant (рис. 2.28).

```
[root@server.alkamal.net ~]# systemctl restore sshd
[root@server.alkamal.net server]# cd /vagrant/provision/server
[root@server.alkamal.net server]# mkdir -p /vagrant/provision/server/ssh/etc/ssh
[root@server.alkamal.net server]# cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/
[root@server.alkamal.net server]# cd /vagrant/provision/server
[root@server.alkamal.net server]# touch ssh.sh
[root@server.alkamal.net server]# chmod +x ssh.sh
[root@server.alkamal.net server]# nano ssh.sh
```

Рисунок 2.28: Копирование файла `sshd_config` в каталог `provision/server/ssh`

В каталоге `/vagrant/provision/server` создан исполняемый файл `ssh.sh`, в котором реализован сценарий автоматической настройки: копирование конфигурационных файлов в `/etc`, восстановление контекстов SELinux (`restorecon`), открытие порта 2022 в `firewalld`, добавление порта 2022 в тип `ssh_port_t` с помощью `semanage`, а также перезапуск службы `sshd` (рис. 2.29).

```
GNU nano 5.6.1                                         ssh.sh
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/ssh/etc/* /etc
restorecon -vR /etc
echo "Configure firewall"
firewall-cmd --add-port=2022/tcp
firewall-cmd --add-port=2022/tcp --permanent
echo "Tuning SELinux"
semanage port -a -t ssh_port_t -p tcp 2022
echo "Restart sshd service"
systemctl restart sshd
```

Рисунок 2.29: Содержимое скрипта `ssh.sh` для автоматической настройки SSH

В файле `Vagrantfile` в разделе конфигурации виртуальной машины **server** добавлен provision-блок типа `shell` с указанием пути `provision/server/ssh.sh` и параметром `preserve_order: true`, что обеспечивает автоматическое выполнение созданного скрипта при загрузке виртуальной машины (рис. 2.30).

```
C: > work > alkamal > vagrant > Vagrantfile
58   server.vm.provision "server ssh",
59     type: "shell",
60     preserve_order: true,
61     path: "provision/server/ssh.sh"
```

Рисунок 2.30: Добавление provision-блока для ssh.sh в Vagrantfile

## 3 Выводы

В ходе работы выполнена комплексная настройка службы OpenSSH на виртуальной машине server. Реализованы меры повышения безопасности: запрещён удалённый вход пользователя root, ограничен список пользователей с помощью директивы `AllowUsers`, настроена аутентификация по ключу вместо пароля, а также организован доступ через альтернативный порт 2022 с корректной настройкой SELinux и межсетевого экрана.

Дополнительно реализованы механизмы SSH-туннелирования и X11-перенаправления, что позволило безопасно передавать TCP-трафик и запускать графические приложения удалённо. Проверена возможность выполнения консольных команд на сервере без интерактивного входа в систему.

Изменения интегрированы во внутреннее окружение виртуальной машины посредством provisioning-скрипта Vagrant, что обеспечивает автоматическое применение конфигурации и воспроизводимость настроенной среды.

## 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` конфигурации прописать `PermitRootLogin no` и `AllowUsers alice`.

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

Для настройки удалённого доступа по SSH через несколько портов нужно отредактировать файл конфигурации SSH и добавить строку `Port <XXXX>`.

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

Для установки фонового соединения без команды используется параметр `-N` при использовании команды ssh: `ssh -N <hostname>`

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

```
ssh -fNL 80:localhost:55555 server2.example.com
```

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

```
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?

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