

Лабораторная работа №11

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

2026-02-13

Содержание I

1 1. Цель работы

2 2. Выполнение лабораторной работы

3 3. Выводы

Раздел 1

1. Цель работы

1.1 Цель работы

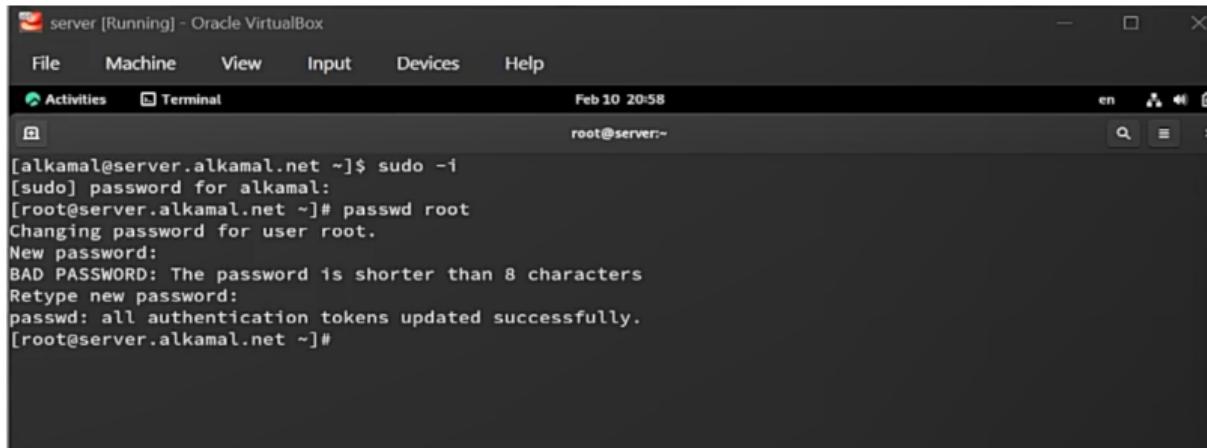
- Приобретение практических навыков настройки удалённого доступа по SSH
- Повышение безопасности доступа к серверу

Раздел 2

2. Выполнение лабораторной работы

2.1 Запрет удалённого доступа по SSH для пользователя root

- Выполнен вход с административными привилегиями
- Задан пароль пользователю root (`passwd root`)
- Получено предупреждение о длине пароля
- Пароль успешно обновлён

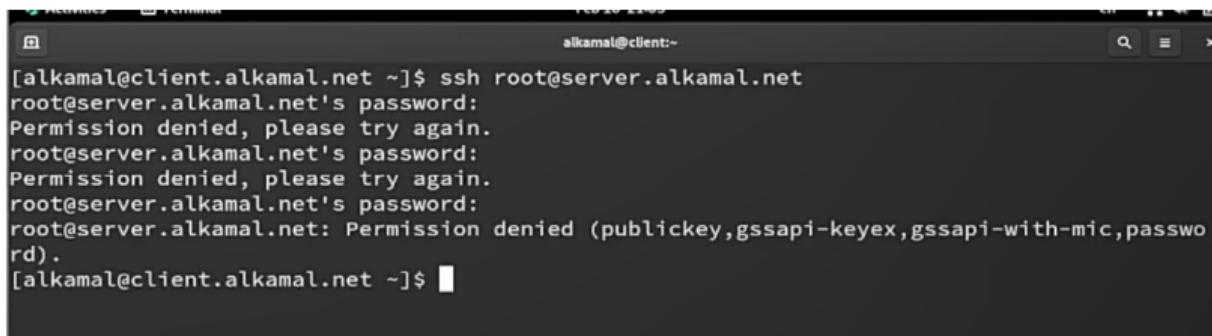


The screenshot shows a terminal window titled "server [Running] - Oracle VirtualBox". The window has a dark theme with white text. At the top, there are menu options: File, Machine, View, Input, Devices, Help. Below the menu is a toolbar with icons for Activities and Terminal. The status bar at the top right shows the date and time: "Feb 10 20:58". The main terminal area displays the following command-line session:

```
[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 1: Изменение пароля пользователя root с помощью `passwd`

- С клиента выполнено ssh root@server.alkamal.net
- Получена ошибка Permission denied
- Доступ отклонён сервером



The screenshot shows a terminal window titled "Terminal" with the command "ssh root@server.alkamal.net" entered. The user is prompted for the password three times, but each attempt results in a "Permission denied" error. After the third attempt, the server returns a message about publickey authentication being disabled. The terminal window has a dark background and light-colored text.

```
[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: Отказ в аутентификации при SSH-подключении пользователя root

- В sshd_config установлен PermitRootLogin no
- Запрещён удалённый вход root

```
# Authentication:  
  
#LoginGraceTime 2m  
PermitRootLogin no  
#StrictModes yes  
#MaxAuthTries 6
```

Рисунок 3: Параметр PermitRootLogin no в файле sshd_config

- Выполнен перезапуск sshd
- Повторная попытка входа завершилась ошибкой
- Подтверждён запрет доступа root

```
[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 4: Повторная ошибка SSH-аутентификации после запрета входа root

2.2 Ограничение списка пользователей для удалённого доступа по SSH

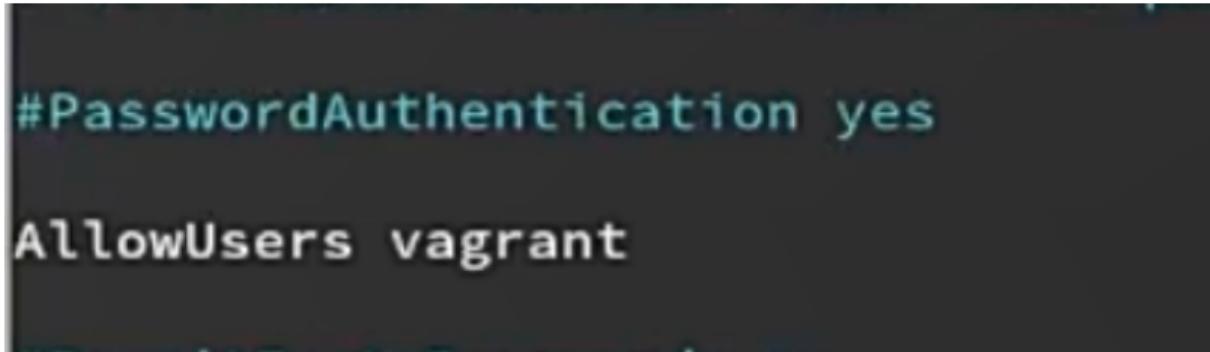
- Выполнено подключение ssh alkamal@server.alkamal.net
- Аутентификация прошла успешно

```
[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 5: Успешное SSH-подключение пользователя alkamal к серверу

- В sshd_config добавлена строка AllowUsers vagrant
- Ограничен список разрешённых пользователей



The screenshot shows a terminal window with a dark background. It displays two lines of configuration text:
#PasswordAuthentication yes
AllowUsers vagrant

Рисунок 6: Добавление директивы AllowUsers vagrant в sshd_config

- Выполнен `systemctl restart sshd`
- Применена новая конфигурация

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

Рисунок 7: Перезапуск службы `sshd` после изменения конфигурации

- Повторное подключение alkamal завершилось ошибкой
- Пользователь отсутствует в AllowUsers

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

Рисунок 8: Отказ в SSH-доступе пользователю alkamal после ограничения AllowUsers

- Стока изменена на `AllowUsers vagrant alkamal`
- Пользователь добавлен в разрешённый список

```
# 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 9: Расширение списка AllowUsers: vagrant alkamal

- После перезапуска sshd подключение успешно
- Подтверждён доступ alkamal

```
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 10: Успешное SSH-подключение после добавления пользователя в AllowUsers

2.3 Настройка дополнительных портов для удалённого доступа по SSH

- В sshd_config добавлена строка Port 2022
- Настроено прослушивание портов 22 и 2022

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

Рисунок 11: Добавление порта 2022 в конфигурацию sshd

- После перезапуска зафиксирована ошибка привязки
- Permission denied из-за SELinux
- Служба работала на порту 22

```
[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 failed: Permission >
Feb 10 21:16:15 server.alkamal.net sshd[11813]: error: Bind to port 2022 on :: failed: Permission denie>
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 12: Ошибка привязки к порту 2022 в статусе sshd

- Выполнено semanage port -a -t ssh_port_t -p tcp 2022
- Порт открыт в firewalld
- Перезапущен sshd

```
[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 13: Настройка SELinux и firewall для порта 2022

- Проверка статуса показала прослушивание 22 и 2022
- Подтверждена корректная настройка

```
[root@server.alkamal.net ~]# netstat -an | grep 22
 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 14: sshd прослушивает порты 22 и 2022

- Выполнено ssh -p2022 alkamal@server.alkamal.net
- Аутентификация успешна
- Выполнен вход и выход из системы

```
[connection to server.alkamal.net closed.  
[alkamal@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 15: Успешное SSH-подключение через порт 2022

2.4 Настройка удалённого доступа по SSH по ключу

- В `sshd_config` установлено `PubkeyAuthentication yes`
- Разрешена аутентификация по ключу

```
...maxsessions 10

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

Рисунок 16: Параметр `PubkeyAuthentication yes` в `sshd_config`

- На клиенте выполнено ssh-keygen
- Созданы id_rsa и id_rsa.pub

```
[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:m01qnno9u7XCWn3map8XPQ6oJtHPa/9uX6bjb+C8mvI alkamal@client.alkamal.net
The key's randomart image is:
+---[RSA 3072]---+
|                               |
|                               |
|                               |
|                               |
| .S . . |
| .*. . o + |
| o=.=++o * oo|
| o+*.+=...*oo|
| .==.oOo+=**E***o|
+---[SHA256]---+
[alkamal@client.alkamal.net ~]$ █
```

Рисунок 17: Генерация пары SSH-ключей командой ssh-keygen

- Выполнено `ssh-copy-id alkamal@server.alkamal.net`
- Ключ добавлен в `authorized_keys`

```
[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 18: Копирование открытого ключа на сервер с помощью `ssh-copy-id`

- Повторное подключение без запроса пароля
- Подтверждена аутентификация по ключу

```
[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 19: Успешная SSH-аутентификация по ключу без ввода пароля

2.5 Организация туннелей SSH, перенаправление TCP-портов

- До туннеля отсутствовал порт 8080
- Проверка lsof | grep TCP

```
[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 20: Проверка активных TCP-соединений до создания SSH-туннеля

- Выполнено `ssh -fNL 8080:localhost:80 ...`
- Создан локальный туннель `8080 → 80`
- Процесс `ssh` прослушивает порт `8080`
- Установлено соединение `ESTABLISHED`

```
[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 21: Прослушивание локального порта 8080 процессом `ssh`

- В браузере открыт `http://localhost:8080`
- Отображена страница сервера
- Подтверждено корректное перенаправление

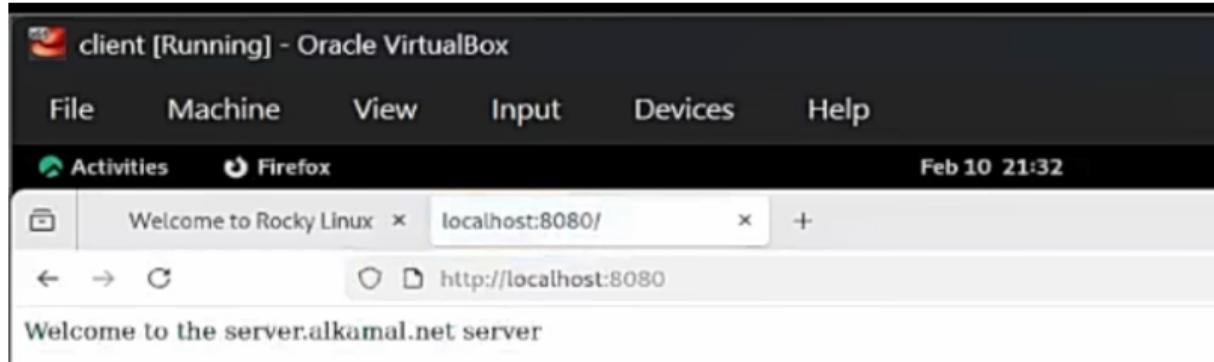


Рисунок 22: Доступ к веб-серверу через SSH-туннель на localhost:8080

2.6 Запуск консольных приложений через SSH

- Выполнено `ssh ... hostname`
- Получено имя узла сервера

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

Рисунок 23: Удалённое выполнение команды `hostname` через SSH

- Выполнено ssh ... ls -Al
- Получен список файлов каталога

```
[alkamal@client.alkamal.net ~]$ ssh alkamal@server.alkamal.net ls -Al
total 72
-rw-----. 1 alkamal alkamal 1896 Feb 10 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 10 13:09 .cache
drwx-----. 11 alkamal alkamal 4096 Feb 10 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 20 Feb 10 13:41 .lessht
drwx-----. 4 alkamal alkamal 32 Feb 6 13:50 .local
drwx-----. 5 alkamal alkamal 4096 Feb 10 16:00 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
drwx-----. 2 alkamal alkamal 71 Feb 10 21:28 .ssh
drwxr-xr-x. 2 alkamal alkamal 6 Feb 6 13:50 Templates
-rw-r-----. 1 alkamal alkamal 6 Feb 10 19:41 .vboxclient-clipboard-tty1-control.pid
-rw-r-----. 1 alkamal alkamal 6 Feb 10 19:41 .vboxclient-clipboard-tty1-service.pid
-rw-r-----. 1 alkamal alkamal 6 Feb 10 19:41 .vboxclient-draganddrop-tty1-control.pid
-rw-r-----. 1 alkamal alkamal 6 Feb 10 19:41 .vboxclient-draganddrop-tty1-service.pid
-rw-r-----. 1 alkamal alkamal 6 Feb 10 19:41 .vboxclient-hostversion-tty1-control.pid
-rw-r-----. 1 alkamal alkamal 6 Feb 10 19:41 .vboxclient-seamless-tty1-control.pid
-rw-r-----. 1 alkamal alkamal 6 Feb 10 19:41 .vboxclient-seamless-tty1-service.pid
-rw-r-----. 1 alkamal alkamal 6 Feb 10 19:41 .vboxclient-vmsvga-session-tty1-control.pid
-rw-r-----. 1 alkamal alkamal 6 Feb 10 19:41 .vboxclient-vmsvga-session-tty1-service.pid
drwxr-xr-x. 2 alkamal alkamal 6 Feb 6 13:50 Videos
-rw-----. 1 alkamal alkamal 0 Feb 10 19:41 .xsession-errors
-rw-----. 1 alkamal alkamal 0 Feb 10 13:09 .xsession-errors.old
```

Рисунок 24: Удалённый вывод списка файлов командой ls -Al

- Выполнено ssh ... MAIL=~/Maildir/ mail
- Отображены 4 почтовых сообщения

```
[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  "LMTMP 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 25: Удалённый просмотр почты через консольное приложение mail

2.7 Запуск графических приложений через SSH (X11Forwarding)

- В sshd_config установлено X11Forwarding yes
- Разрешена пересылка X11

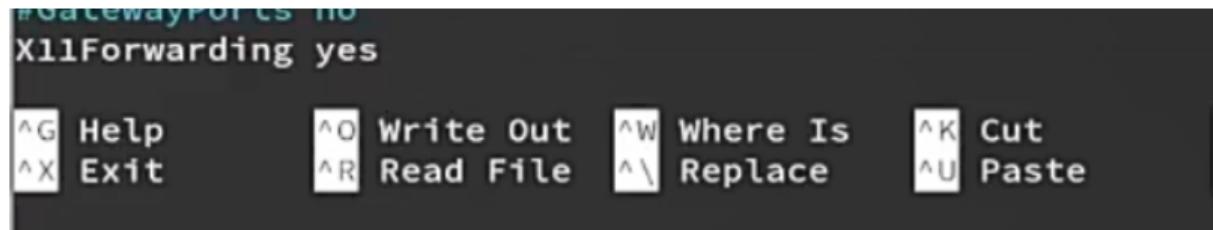
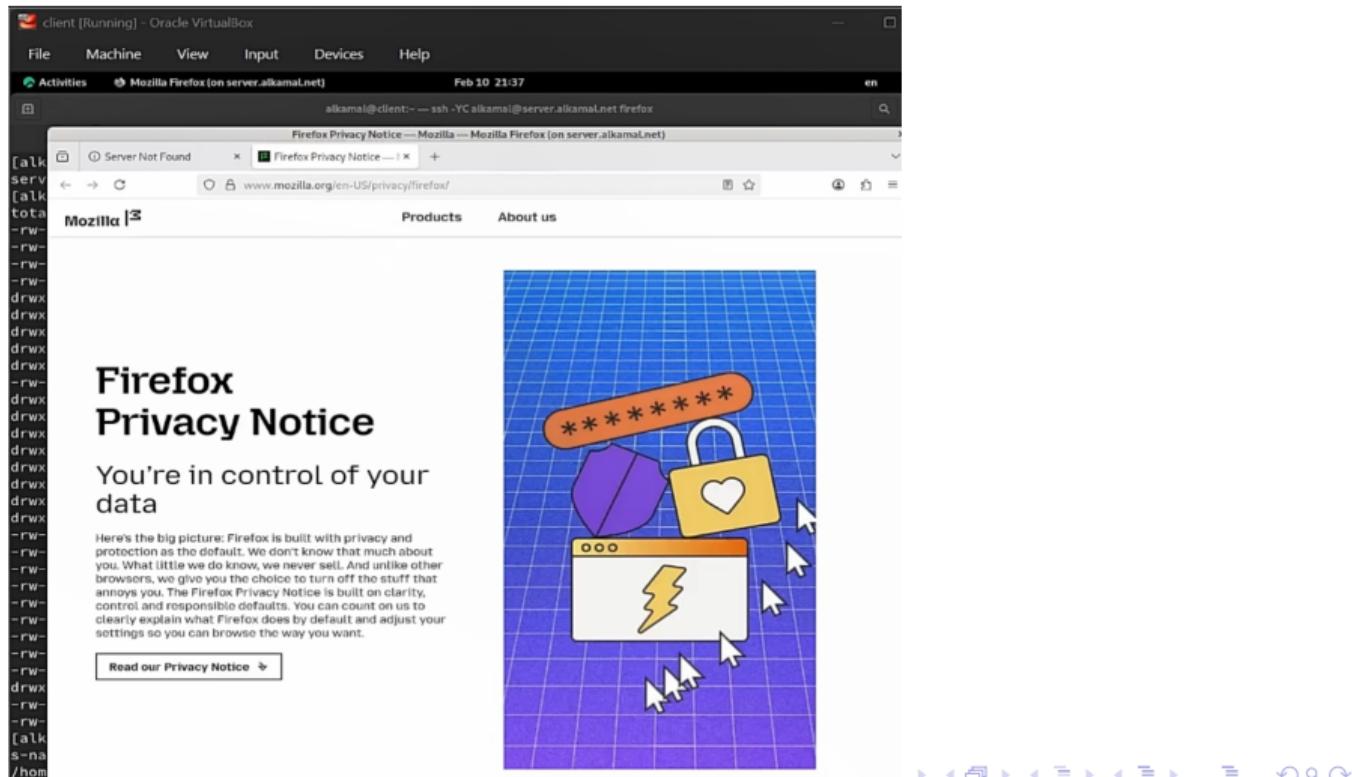


Рисунок 26: Параметр X11Forwarding yes в sshd_config

- Выполнено ssh -YC ... firefox
 - Включено X11-перенаправление и сжатие
 - Firefox запущен на сервере и отображён на клиенте



2.8 Внесение изменений в настройки внутреннего

- В `/vagrant/provision/server` создан каталог `ssh/etc/ssh`
- Скопирован файл `sshd_config`

```
[root@server.alkamal.net ~]# systemctl restart sshd
[root@server.alkamal.net ~]# 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 28: Копирование файла `sshd_config` в каталог `provision/server/ssh`

- Создан скрипт ssh.sh
- Реализовано копирование конфигурации
- Выполнены restorecon, semanage, настройка firewall
- Перезапущен sshd

```
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 29: Содержимое скрипта ssh.sh для автоматической настройки SSH

- В Vagrantfile добавлен provision-блок shell
- Указан путь provision/server/ssh.sh
- Обеспечено автоматическое выполнение при запуске VM

```
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 30: Добавление provision-блока для ssh.sh в Vagrantfile

Раздел 3

3. Выводы

3.1 Выводы

- Запрещён удалённый вход пользователя root
- Ограничен список пользователей через AllowUsers
- Настроен альтернативный порт 2022 с учётом SELinux и firewall
- Реализована аутентификация по ключу
- Настроено SSH-туннелирование и перенаправление портов
- Проверен запуск консольных и графических приложений
- Конфигурация интегрирована в provisioning Vagrant
- Обеспечена воспроизводимость и безопасность SSH-доступа