

Отчет по лабораторной работе №11

Настройка безопасного удалённого доступа по протоколу SSH

Галацан Николай, НПИбд-01-22

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
2.1	Запрет удалённого доступа по SSH для пользователя root	5
2.2	Ограничение списка пользователей для удалённого доступа по SSH	6
2.3	Настройка дополнительных портов для удалённого доступа по SSH	8
2.4	Настройка удалённого доступа по SSH по ключу	11
2.5	Организация туннелей SSH, перенаправление TCP-портов	12
2.6	Запуск консольных приложений через SSH	13
2.7	Запуск графических приложений через SSH	14
2.8	Внесение изменений в настройки внутреннего окружения виртуальной машины	15
3	Выводы	17
4	Ответы на контрольные вопросы	18

Список иллюстраций

2.1	Попытка получения доступа к серверу через root: отказ	5
2.2	Запрет входа на сервер пользователю root	6
2.3	Попытка получения доступа к серверу через ngalacan: доступ получен	6
2.4	Добавление строки в конфигурационный файл	7
2.5	Попытка получения доступа к серверу через ngalacan: отказ	7
2.6	Попытка получения доступа к серверу через ngalacan: доступ получен	7
2.7	Добавление портов	8
2.8	Статус sshd: отказ в работе через порт 2022	8
2.9	Ошибки в журнале системных событий	9
2.10	Исправление меток SELinux, настройка межсетевого экрана, просмотр статуса sshd	10
2.11	Попытка получения доступа к серверу через ngalacan и через порт 2022: доступ получен	10
2.12	Разрешение аутентификации по ключу	11
2.13	Генерация SSH-ключа, копирование на сервер, попытка получения доступа: успешно	12
2.14	Перенаправление порта 80 на server.ngalacan.net на порт 8080 . .	12
2.15	localhost:8080 в браузере	13
2.16	Просмотр с клиента имени узла, файлов и почты на сервере	13
2.17	Разрешение отображения графических интерфейсов X11	14
2.18	Запуск firefox на сервере через клиент	15
2.19	Редактирование ssh.sh	16

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

Запускаю ВМ через рабочий каталог. На ВМ server вхожу под собственным пользователем и перехожу в режим суперпользователя. Задаю пароль для пользователя root. В дополнительном терминале запускаю мониторинг системных событий. С клиента пытаюсь получить доступ к серверу через SSH-соединение через пользователя root, однако в доступе отказано (рис. 2.1).



```
ngalacan@client:~  
[ngalacan@client.ngalacan.net ~]$ ssh root@server.ngalacan.net  
The authenticity of host 'server.ngalacan.net (192.168.1.1)' can't be established.  
ED25519 key fingerprint is SHA256:dtzsgQ2L/ztuBFw9Cy/q0lBhP0USYE31H707PUekdT8.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:1: [server.ngalacan.net]:2022  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'server.ngalacan.net' (ED25519) to the list of known  
hosts.  
root@server.ngalacan.net's password:  
Permission denied, please try again.  
root@server.ngalacan.net's password:  
Permission denied, please try again.  
root@server.ngalacan.net's password:  
root@server.ngalacan.net: Permission denied (publickey,gssapi-keyex,gssapi-with-  
mic,password).  
[ngalacan@client.ngalacan.net ~]$
```

Рис. 2.1: Попытка получения доступа к серверу через root: отказ

В конфигурационном файле `/etc/ssh/sshd_config` запрещаю вход на сервер пользователю root (рис. 2.2)

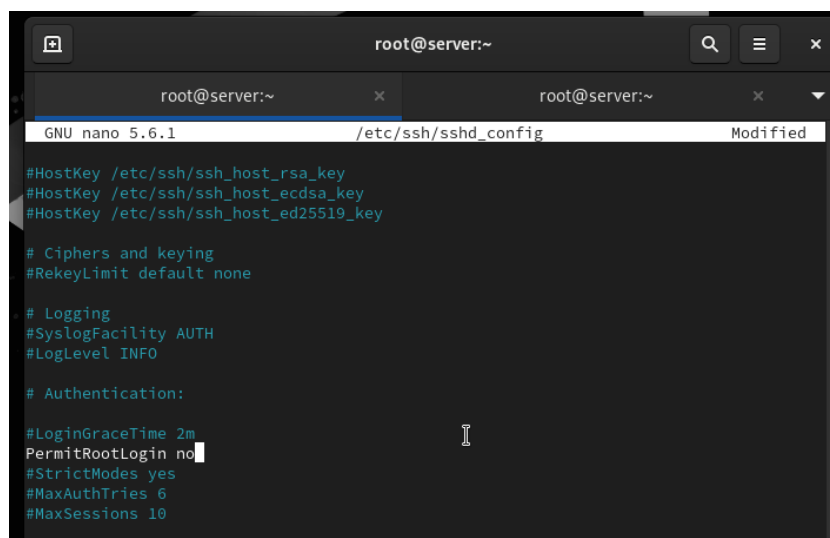


Рис. 2.2: Запрет входа на сервер пользователю root

Перезагружаю sshd. Повторяю попытку получения доступа через root, вновь получаю отказ в доступе.

2.2 Ограничение списка пользователей для удалённого доступа по SSH

клиента пытаюсь получить доступ к серверу через SSH-соединение через пользователя ngalacan, доступ получен (рис. 2.3)

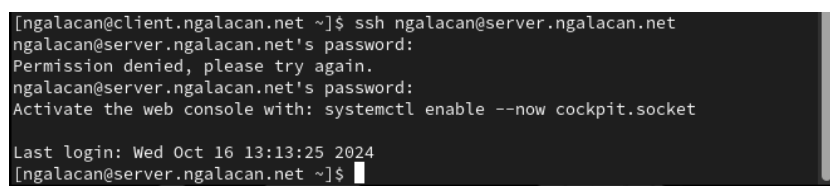
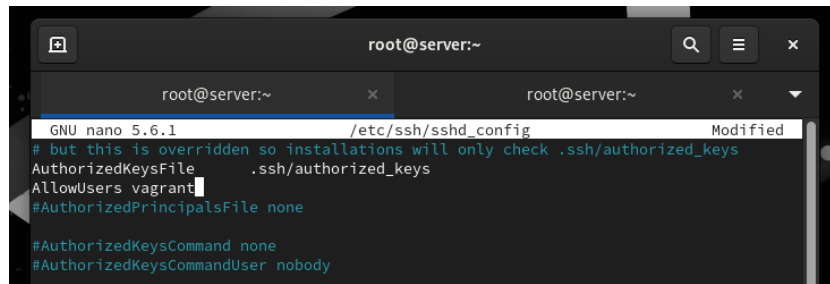


Рис. 2.3: Попытка получения доступа к серверу через ngalacan: доступ получен

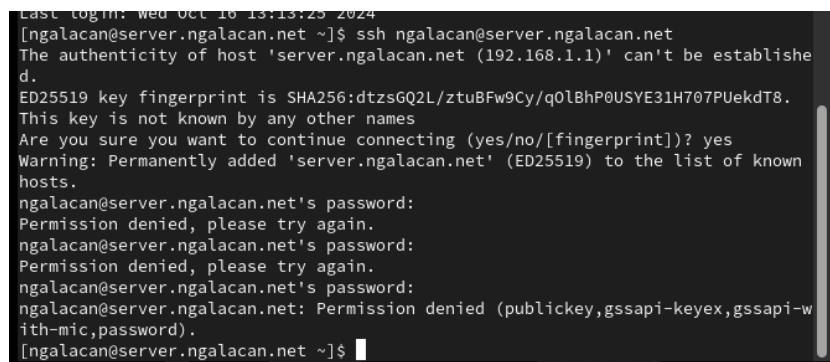
В конфигурационном файле /etc/ssh/sshd_config добавляю строку (рис. 2.4)



```
root@server:~  
GNU nano 5.6.1 /etc/ssh/sshd_config Modified  
# but this is overridden so installations will only check .ssh/authorized_keys  
AuthorizedKeysFile .ssh/authorized_keys  
AllowUsers vagrant  
#AuthorizedPrincipalsFile none  
#AuthorizedKeysCommand none  
#AuthorizedKeysCommandUser nobody
```

Рис. 2.4: Добавление строки в конфигурационный файл

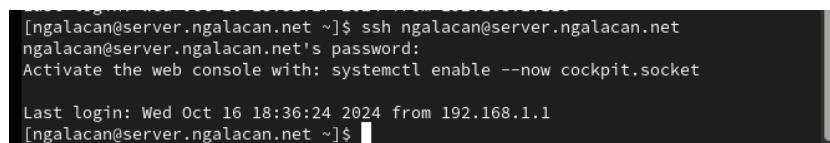
Перезагрузив sshd, вновь пытаюсь с клиента получить доступ через пользователя ngalacan, но в доступе отказано (рис. 2.5).



```
Last login: Wed Oct 16 13:13:25 2024  
[ngalacan@server.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net  
The authenticity of host 'server.ngalacan.net (192.168.1.1)' can't be established.  
ED25519 key fingerprint is SHA256:dtzsGQ2L/ztuBFw9Cy/q0lBhP0USYE31H707PUekdT8.  
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.ngalacan.net' (ED25519) to the list of known hosts.  
ngalacan@server.ngalacan.net's password:  
Permission denied, please try again.  
ngalacan@server.ngalacan.net's password:  
Permission denied, please try again.  
ngalacan@server.ngalacan.net's password:  
ngalacan@server.ngalacan.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).  
[ngalacan@server.ngalacan.net ~]$
```

Рис. 2.5: Попытка получения доступа к серверу через ngalacan: отказ

В файле /etc/ssh/sshd_config изменяю строку AllowUsers vagrant ngalacan. Пытаюсь с клиента получить доступ через пользователя ngalacan, доступ получен (рис. 2.6).



```
[ngalacan@server.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net  
ngalacan@server.ngalacan.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
Last login: Wed Oct 16 18:36:24 2024 from 192.168.1.1  
[ngalacan@server.ngalacan.net ~]$
```

Рис. 2.6: Попытка получения доступа к серверу через ngalacan: доступ получен

2.3 Настройка дополнительных портов для удалённого доступа по SSH

В файле `/etc/ssh/sshd_config` добавляю порты (рис. 2.7).

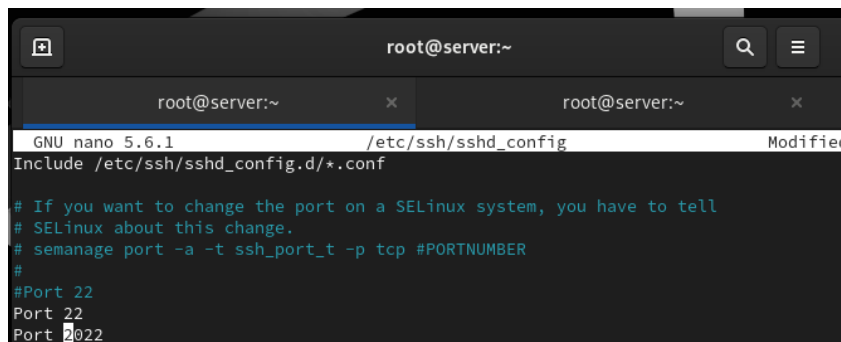


Рис. 2.7: Добавление портов

Перезапускаю `sshd` и просматриваю статус. Выводится отказ в работе через порт 2022 (рис. 2.8).

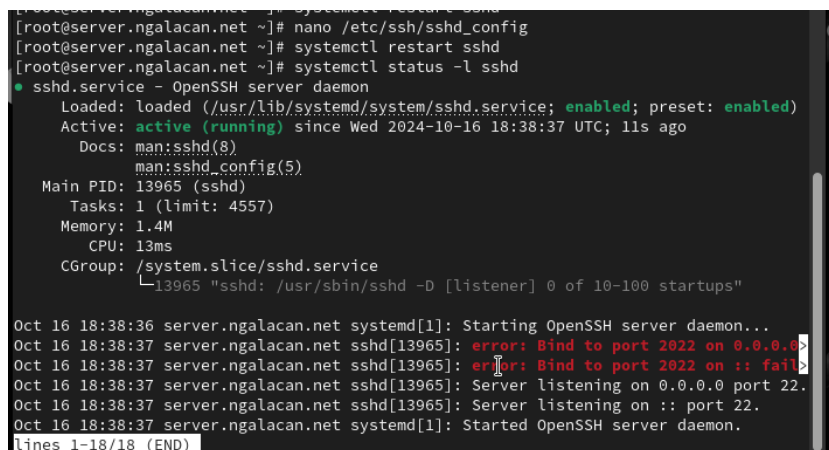
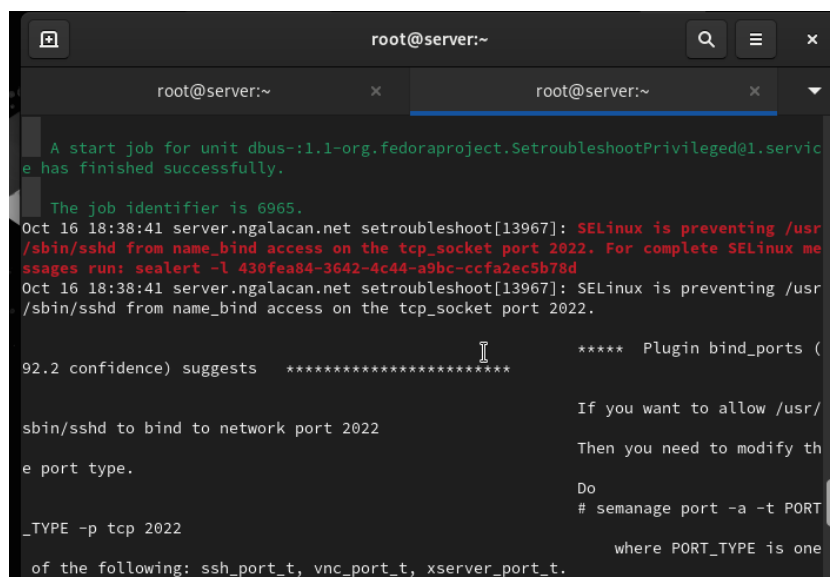


Рис. 2.8: Статус `sshd`: отказ в работе через порт 2022

Дополнительно просматриваю журнал системных событий и вижу сообщения об ошибках в SELinux (рис. 2.9).



```
root@server:~
A start job for unit dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@1.servic
e has finished successfully.
The job identifier is 6965.
Oct 16 18:38:41 server.ngalacan.net setroubleshoot[13967]: SELinux is preventing /usr
/sbin/sshd from name_bind access on the tcp_socket port 2022. For complete SELinux me
ssages run: sealert -l 430fea84-3642-4c44-a9bc-ccfa2ec5b78d
Oct 16 18:38:41 server.ngalacan.net setroubleshoot[13967]: SELinux is preventing /usr
/sbin/sshd from name_bind access on the tcp_socket port 2022.

92.2 confidence) suggests ***** Plugin bind_ports (
*****
If you want to allow /usr/
Then you need to modify th
Do
# semanage port -a -t PORT
where PORT_TYPE is one
of the following: ssh_port_t, vnc_port_t, xserver_port_t.
```

Рис. 2.9: Ошибки в журнале системных событий

Исправляю метки SELinux к порту 2022, настраиваю межсетевой экран, перезапускаю sshd и вновь просматриваю статус. Прослушиваются оба порта (рис. 2.10).

```
root@server:~  
[root@server.ngalacan.net ~]# semanage port -a -t ssh_port_t -p tcp 2022  
[root@server.ngalacan.net ~]# firewall-cmd add-port=2022/tcp  
usage: 'firewall-cmd --help' for usage information or see firewall-cmd(1) man page  
firewall-cmd: error: unrecognized arguments: add-port=2022/tcp  
[root@server.ngalacan.net ~]# firewall-cmd --add-port=2022/tcp  
success  
[root@server.ngalacan.net ~]# firewall-cmd --add-port=2022/tcp --permanent  
success  
[root@server.ngalacan.net ~]# systemctl restart sshd  
[root@server.ngalacan.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 Wed 2024-10-16 18:41:40 UTC; 6s ago  
     Docs: man:sshd(8)  
           man:sshd_config(5)  
  Main PID: 13998 (sshd)  
    Tasks: 1 (limit: 4557)  
  Memory: 1.7M  
    CPU: 13ms  
  CGroup: /system.slice/sshd.service  
          └─13998 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"  
  
Oct 16 18:41:40 server.ngalacan.net systemd[1]: Starting OpenSSH server daemon...  
Oct 16 18:41:40 server.ngalacan.net sshd[13998]: Server listening on 0.0.0.0 port 2022.  
Oct 16 18:41:40 server.ngalacan.net sshd[13998]: Server listening on :: port 2022.  
Oct 16 18:41:40 server.ngalacan.net sshd[13998]: Server listening on 0.0.0.0 port 22.  
Oct 16 18:41:40 server.ngalacan.net sshd[13998]: Server listening on :: port 22.  
Oct 16 18:41:40 server.ngalacan.net systemd[1]: Started OpenSSH server daemon.  
lines 1-18/18 (END)...skipping...  
● sshd.service - OpenSSH server daemon
```

Рис. 2.10: Исправление меток SELinux, настройка межсетевого экрана, просмотр статуса sshd

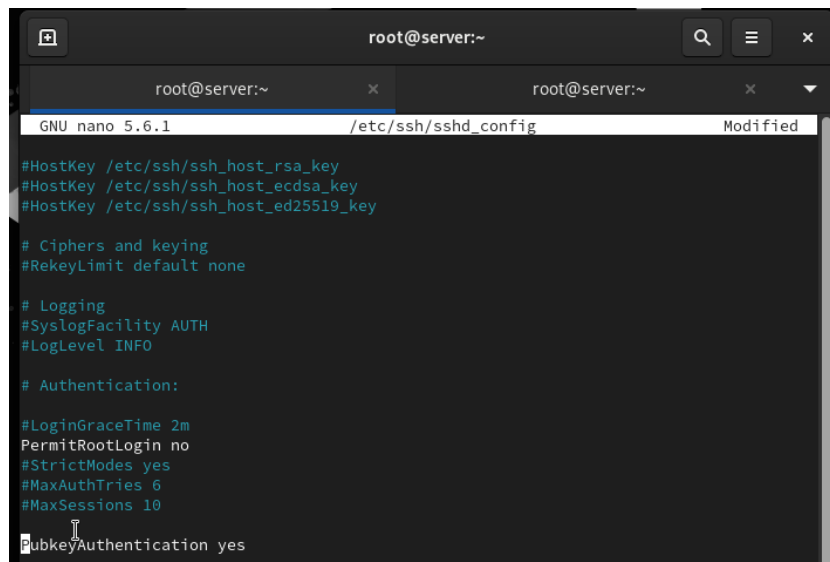
С клиента пытаюсь получить доступ через пользователя. После открытия оболочки получаю доступ в root. Отлогиниваюсь от root и от пользователя на сервере. Повторяю попытку получения доступа через порт 2022, повторяю те же самые действия (рис. 2.11).

```
[ngalacan@client.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net  
ngalacan@server.ngalacan.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Wed Oct 16 18:45:25 2024 from 192.168.1.1  
[ngalacan@server.ngalacan.net ~]$ sudo -i  
[sudo] password for ngalacan:  
[root@server.ngalacan.net ~]# logout  
[ngalacan@server.ngalacan.net ~]$ logout  
Connection to server.ngalacan.net closed.  
[ngalacan@client.ngalacan.net ~]$ ssh -p2022 ngalacan@server.ngalacan.net  
ngalacan@server.ngalacan.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Wed Oct 16 18:47:12 2024 from 192.168.1.116  
[ngalacan@server.ngalacan.net ~]$ sudo -i  
[sudo] password for ngalacan:  
[root@server.ngalacan.net ~]# logout  
[ngalacan@server.ngalacan.net ~]$ logout  
Connection to server.ngalacan.net closed.  
[ngalacan@client.ngalacan.net ~]$
```

Рис. 2.11: Попытка получения доступа к серверу через ngalacan и через порт 2022: доступ получен

2.4 Настройка удалённого доступа по SSH по ключу

В файле `/etc/ssh/sshd_config` разрешаю аутентификацию по ключу, перезапускаю сервис (рис. 2.12)



```
root@server:~  
GNU nano 5.6.1 /etc/ssh/sshd_config Modified  
#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
```

Рис. 2.12: Разрешение аутентификации по ключу

На клиенте генерирую SSH-ключ и копирую его на сервер. Пробую получить доступ к серверу через пользователя. Доступ получен, теперь не запрашивается пароль. Отлогиниваюсь с помощью `ctrl+d` (рис. 2.13).

```
ngalacan@client:~  
+-----[SHA256]-----+  
[ngalacan@client.ngalacan.net ~]$ ssh-copy-id ngalacan@server.ngalacan.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 prompt  
ed now it is to install the new keys  
ngalacan@server.ngalacan.net's password:  
  
Number of key(s) added: 1  
  
Now try logging into the machine, with: "ssh 'ngalacan@server.ngalacan.net'"  
and check to make sure that only the key(s) you wanted were added.  
  
[ngalacan@client.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Wed Oct 16 18:47:33 2024 from 192.168.1.116  
[ngalacan@server.ngalacan.net ~]$  
logout  
Connection to server.ngalacan.net closed.  
[ngalacan@client.ngalacan.net ~]$
```

Рис. 2.13: Генерация SSH-ключа, копирование на сервер, попытка получения доступа: успешно

2.5 Организация туннелей SSH, перенаправление

TCP-портов

На клиенте просматриваю, запущены ли какие-то службы с протоколом TCP (не запущены). Перенаправляю порт 80 на server.ngalacan.net на порт 8080. Вновь просматриваю службы с TCP (службы запущены) (рис. 2.14).

```
ngalacan@client:~  
[ngalacan@client.ngalacan.net ~]$ lsof | grep TCP  
[ngalacan@client.ngalacan.net ~]$ ssh -fNL 8080:localhost:80 ngalacan@server.nga  
lacan.net  
[ngalacan@client.ngalacan.net ~]$ lsof | grep TCP  
ssh      12530      ngalacan    3u  IPv4        88125  
0t0      TCP client.ngalacan.net:42240->dhcp.ngalacan.net:ssh (ESTABLIS  
HED)  
ssh      12530      ngalacan    4u  IPv6        88144  
0t0      TCP localhost:webcache (LISTEN)  
ssh      12530      ngalacan    5u  IPv4        88145  
0t0      TCP localhost:webcache (LISTEN)  
[ngalacan@client.ngalacan.net ~]$
```

Рис. 2.14: Перенаправление порта 80 на server.ngalacan.net на порт 8080

Запускаю браузер и ввожу localhost:8080. Вижу приветственное сообщение

сервера (рис. 2.15).

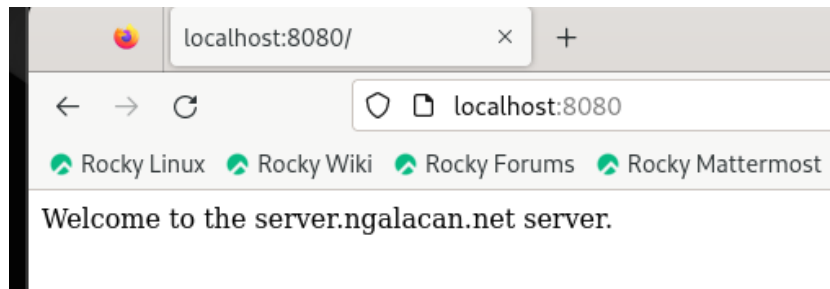


Рис. 2.15: localhost:8080 в браузере

2.6 Запуск консольных приложений через SSH

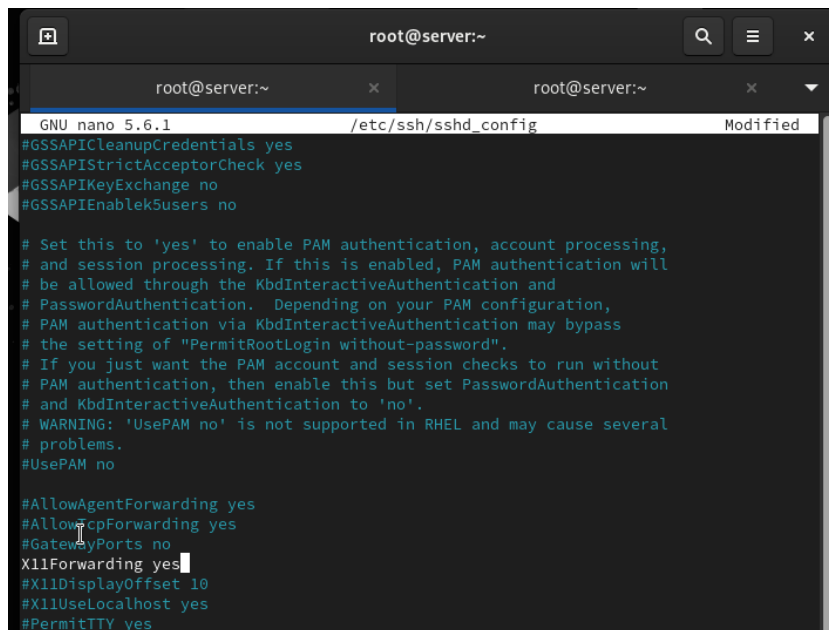
С клиента просматриваю имя узла, список файлов на сервере, почту (рис. 2.16).

```
ngalacan@client:~  
[ngalacan@client.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net hostname  
server.ngalacan.net  
[ngalacan@client.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net ls -Al  
total 36  
-rw-----. 1 ngalacan ngalacan 1509 Oct 16 18:47 .bash_history  
-rw-r--r--. 1 ngalacan ngalacan 18 Apr 30 11:28 .bash_logout  
-rw-r--r--. 1 ngalacan ngalacan 141 Apr 30 11:28 .bash_profile  
-rw-r--r--. 1 ngalacan ngalacan 573 Oct 16 13:10 .bashrc  
drwx----- 17 ngalacan ngalacan 4096 Oct 16 13:16 .cache  
drwx----- 14 ngalacan ngalacan 4096 Oct 16 13:16 .config  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Desktop  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Documents  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Downloads  
drwx----- 4 ngalacan ngalacan 32 Sep 6 22:12 .local  
drwx----- 5 ngalacan ngalacan 4096 Oct 16 16:21 Maildir  
drwxr-xr-x. 5 ngalacan ngalacan 54 Sep 9 17:56 .mozilla  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Music  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Pictures  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Public  
drwx----- 2 ngalacan ngalacan 71 Oct 16 18:50 .ssh  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Templates  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Videos  
-rw----- 1 ngalacan ngalacan 83 Oct 16 13:13 .xsession-errors  
-rw----- 1 ngalacan ngalacan 83 Oct 15 12:09 .xsession-errors.old  
[ngalacan@client.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net MAIL=~/.Maildir/  
r/ mail  
s-nail version v14.9.22. Type '?' for help  
/home/ngalacan/Maildir: 4 messages  
• 1 ngalacan@ngalacan.ne 2024-10-09 17:01 14/444 "test"  
2 ngalacan 2024-10-16 13:49 18/648 "test3"  
3 ngalacan@client.ngal 2024-10-16 15:54 21/833 "LMTP-test"  
4 ngalacan 2024-10-16 16:21 22/824 "SMTP over TLS test"  
exit  
[ngalacan@client.ngalacan.net ~]$
```

Рис. 2.16: Просмотр с клиента имени узла, файлов и почты на сервере

2.7 Запуск графических приложений через SSH

В файле `/etc/ssh/sshd_config` разрешаю отображать на локальном клиентском компьютере графические интерфейсы X11 и перезапускаю сервис (рис. 2.17).



```
GNU nano 5.6.1 /etc/ssh/sshd_config Modified
#GSSAPICleanupCredentials yes
#GSSAPIStrictAccepterCheck yes
#GSSAPIKeyExchange no
#GSSAPIEnableK5Users no

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

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
```

Рис. 2.17: Разрешение отображения графических интерфейсов X11

С клиента удаленно подключаюсь к серверу и запускаю `firefox` (рис. 2.18).

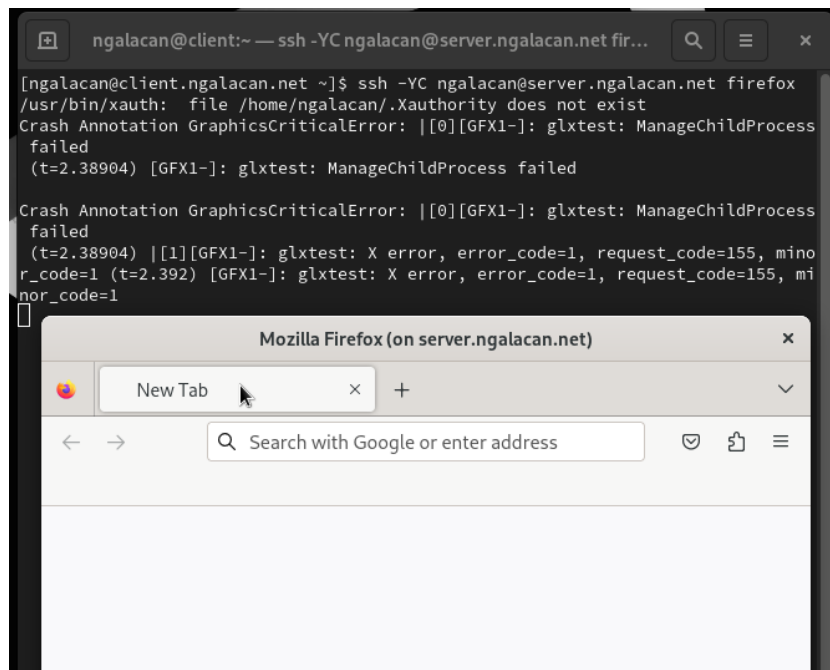


Рис. 2.18: Запуск firefox на сервере через клиент

2.8 Внесение изменений в настройки внутреннего окружения виртуальной машины

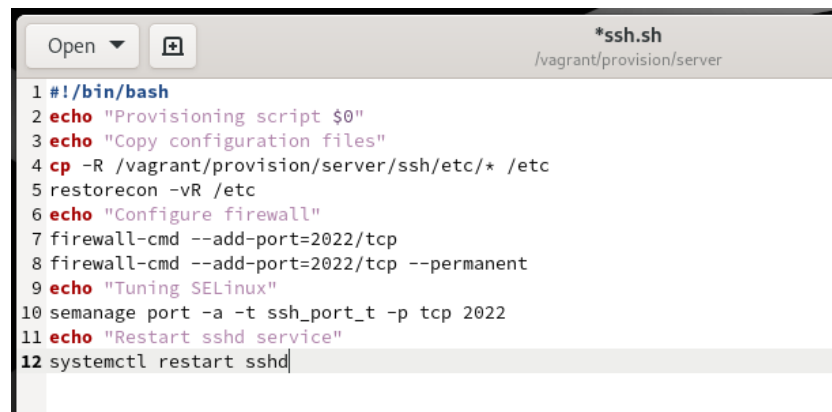
На VM server перехожу в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/` и копирую в соответствующие каталоги конфигурационные файлы:

```
cd /vagrant/provision/server
```

```
mkdir -p /vagrant/provision/server/ssh/etc/ssh
```

```
cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/
```

Создаю файл `/vagrant/provision/server/ssh.sh` (рис. 2.19).

A screenshot of a terminal window with a title bar that says '*ssh.sh' and '/vagrant/provision/server'. The terminal shows a bash script with 12 lines of code. The code includes echo statements for provisioning, copying files, configuring firewall, tuning SELinux, and restarting sshd. The last line is 'systemctl restart sshd' followed by a cursor.

```
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. 2.19: Редактирование ssh.sh

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавляю следующую запись:

```
server.vm.provision "server ssh",
  type: "shell",
  preserve_order: true,
  path: "provision/server/ssh.sh"
```


3 Выводы

В результате выполнения работы были приобретены практические навыки по настройке удалённого доступа к серверу с помощью SSH.

4 Ответы на 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 <порт>`.

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:5555 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
```