

# РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

## ОТЧЕТ

### ПО ЛАБОРАТОРНОЙ РАБОТЕ № 11

*дисциплина:* Администрирование сетевых подсистем

Студент: Бакулин Никита 1032201747

Группа: НПИбд-01-20

МОСКВА

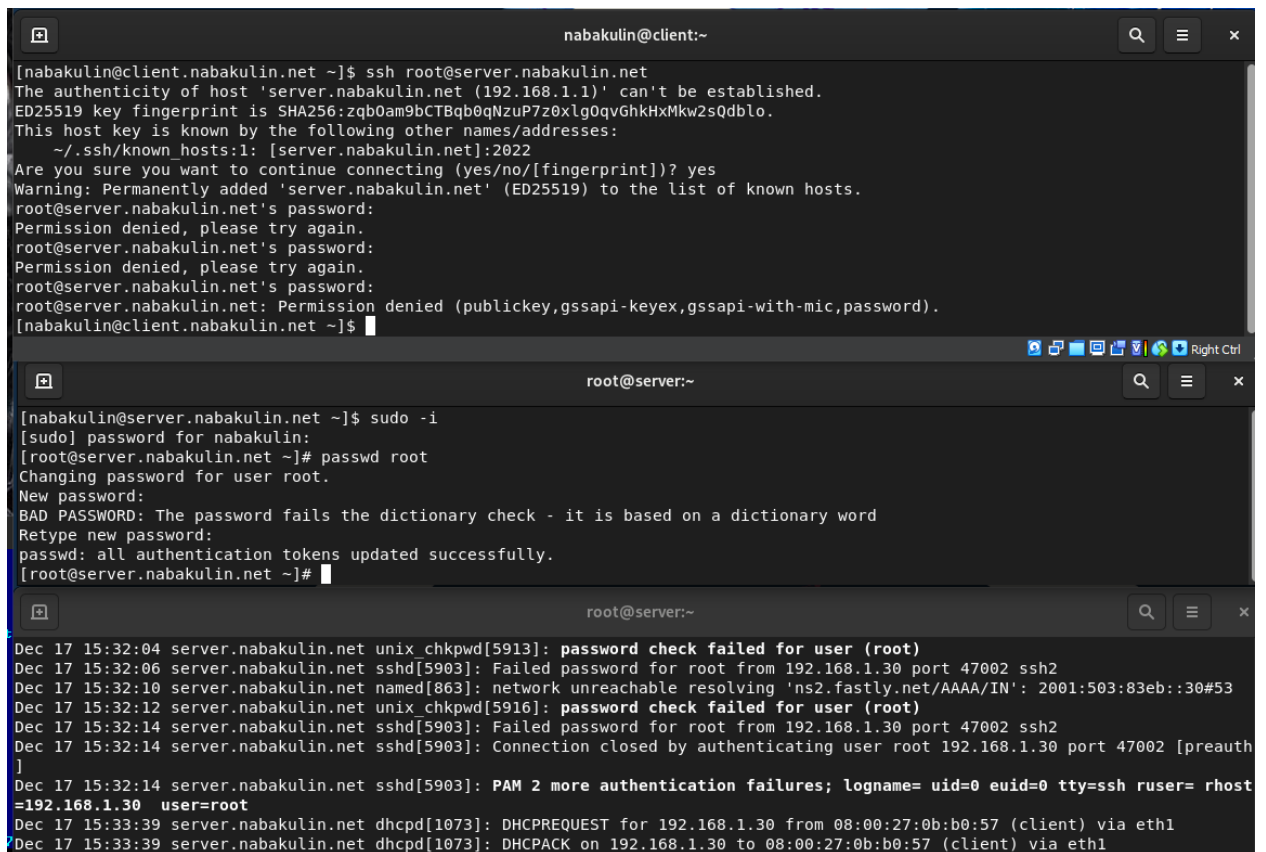
2022 г.

## **Постановка задачи**

1. Настройте запрет удалённого доступа на сервер по SSH для пользователя root
2. Настройте разрешение удалённого доступа к серверу по SSH только для пользователей группы vagrant и вашего пользователя
3. Настройте удалённый доступ к серверу по SSH через порт 2022
4. Настройте удалённый доступ к серверу по SSH по ключу
5. Организуйте SSH-туннель с клиента на сервер, перенаправив локальное соединение с TCP-порта 80 на порт 8080
6. Используя удалённое SSH-соединение, выполните с клиента несколько команд на сервере
7. Используя удалённое SSH-соединение, запустите с клиента графическое приложение на сервере
8. Напишите скрипт для Vagrant, фиксирующий действия по настройке SSH-сервера во внутреннем окружении виртуальной машины server. Соответствующим образом внесите изменения в Vagrantfile

## **Выполнение работы**

1.
  - 1.1. На сервере задайте пароль для пользователя root, если этого не было сделано ранее
  - 1.2. На сервере в дополнительном терминале запустите мониторинг системных событий
  - 1.3. С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя root – Failed password for root

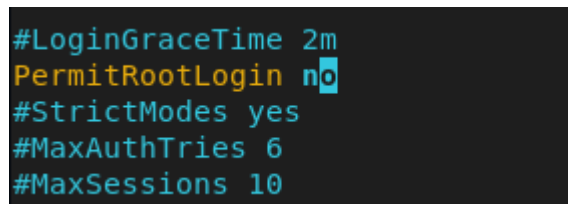


The image consists of three terminal window screenshots. The top window shows a user 'nabakulin' at a client machine attempting to SSH into a server 'server.nabakulin.net' as 'root'. It displays host key fingerprint information and a warning about adding the host to the known hosts list. The user is prompted for a password but is denied access three times. The middle window shows the user 'nabakulin' on the server using 'sudo -i' to become 'root'. They are prompted for a password and then asked to change their password. The new password is rejected as it is a dictionary word, and they are prompted to retype it. The bottom window shows system logs for the server, including failed password attempts for 'root' and a DHCP request from the client.

```
nabakulin@client:~  
[nabakulin@client.nabakulin.net ~]$ ssh root@server.nabakulin.net  
The authenticity of host 'server.nabakulin.net (192.168.1.1)' can't be established.  
ED25519 key fingerprint is SHA256:zqb0am9bCTBqb0qNzuP7z0xlg0qvGhkHxMkw2sQdblo.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:1: [server.nabakulin.net]:2022  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'server.nabakulin.net' (ED25519) to the list of known hosts.  
root@server.nabakulin.net's password:  
Permission denied, please try again.  
root@server.nabakulin.net's password:  
Permission denied, please try again.  
root@server.nabakulin.net's password:  
root@server.nabakulin.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).  
[nabakulin@client.nabakulin.net ~]$  
  
root@server:~  
[nabakulin@server.nabakulin.net ~]$ sudo -i  
[sudo] password for nabakulin:  
[root@server.nabakulin.net ~]# passwd root  
Changing password for user root.  
New password:  
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@server.nabakulin.net ~]#  
  
root@server:~  
Dec 17 15:32:04 server.nabakulin.net unix_chkpwd[5913]: password check failed for user (root)  
Dec 17 15:32:06 server.nabakulin.net sshd[5903]: Failed password for root from 192.168.1.30 port 47002 ssh2  
Dec 17 15:32:10 server.nabakulin.net named[863]: network unreachable resolving 'ns2.fastly.net/AAAA/IN': 2001:503:83eb::30#53  
Dec 17 15:32:12 server.nabakulin.net unix_chkpwd[5916]: password check failed for user (root)  
Dec 17 15:32:14 server.nabakulin.net sshd[5903]: Failed password for root from 192.168.1.30 port 47002 ssh2  
Dec 17 15:32:14 server.nabakulin.net sshd[5903]: Connection closed by authenticating user root 192.168.1.30 port 47002 [preauth]  
Dec 17 15:32:14 server.nabakulin.net sshd[5903]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=  
=192.168.1.30 user=root  
Dec 17 15:33:39 server.nabakulin.net dhcpcd[1073]: DHCPREQUEST for 192.168.1.30 from 08:00:27:0b:b0:57 (client) via eth1  
Dec 17 15:33:39 server.nabakulin.net dhcpcd[1073]: DHCPACK on 192.168.1.30 to 08:00:27:0b:b0:57 (client) via eth1
```

Рисунок 1

1.4. На сервере откройте файл `/etc/ssh/sshd_config` конфигурации `sshd` для редактирования и запретите вход на сервер пользователю `root`, установив



A terminal snippet showing the configuration file `/etc/ssh/sshd_config`. The lines `PermitRootLogin` and `StrictModes` are highlighted in yellow. The value for `PermitRootLogin` is being changed from `yes` to `no`.

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

Рисунок 2

1.5. После сохранения изменений в файле конфигурации перезапустите `sshd`

1.6. Повторите попытку получения доступа с клиента к серверу посредством SSH соединения через пользователя `root` – нет доступа

```
[nabakulin@client.nabakulin.net ~]$ ssh root@server
The authenticity of host 'server (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:zqb0am9bCTBqb0gNzuP7z0xlG0qvGhkHxMkw2sQdblo.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [server.nabakulin.net]:2022
  ~/.ssh/known_hosts:4: server.nabakulin.net
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server' (ED25519) to the list of known hosts.
root@server's password:
Permission denied, please try again.
root@server's password:
Permission denied, please try again.
root@server's password:
root@server: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[nabakulin@client.nabakulin.net ~]$
```

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

```
root@server:~
=192.168.1.30 user=root
Dec 17 15:41:14 server.nabakulin.net unix_chkpwd[6013]: password check failed for user (root)
Dec 17 15:41:14 server.nabakulin.net sshd[6009]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30 user=root
Dec 17 15:41:17 server.nabakulin.net sshd[6009]: Failed password for root from 192.168.1.30 port 44532 ssh2
Dec 17 15:41:24 server.nabakulin.net unix_chkpwd[6014]: password check failed for user (root)
Dec 17 15:41:25 server.nabakulin.net sshd[6009]: Failed password for root from 192.168.1.30 port 44532 ssh2
Dec 17 15:41:28 server.nabakulin.net unix_chkpwd[6015]: password check failed for user (root)
Dec 17 15:41:31 server.nabakulin.net sshd[6009]: Failed password for root from 192.168.1.30 port 44532 ssh2
Dec 17 15:41:31 server.nabakulin.net sshd[6009]: Connection closed by authenticating user root 192.168.1.30 port 44532 [preauth]
Dec 17 15:41:31 server.nabakulin.net sshd[6009]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30 user=root
```

Рисунок 3

2.

2.1. С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя user – доступ есть

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

Last login: Sat Dec 17 15:26:23 2022
[nabakulin@server.nabakulin.net ~]$
```

```
Dec 17 15:44:10 server.nabakulin.net sshd[6038]: Accepted password for nabakulin from 192.168.1.30 port 39200 ssh2
Dec 17 15:44:10 server.nabakulin.net systemd-logind[603]: New session 6 of user nabakulin.
Subject: A new session 6 has been created for user nabakulin
Defined-By: systemd
Support: https://access.redhat.com/support
Documentation: sd-login(3)

A new session with the ID 6 has been created for the user nabakulin.

The leading process of the session is 6038.
Dec 17 15:44:10 server.nabakulin.net systemd[1]: Started Session 6 of User nabakulin.
Subject: A start job for unit session-6.scope has finished successfully
Defined-By: systemd
Support: https://access.redhat.com/support

A start job for unit session-6.scope has finished successfully.

The job identifier is 2476.
Dec 17 15:44:10 server.nabakulin.net sshd[6038]: pam_unix(sshd:session): session opened for user nabakulin(uid=1001) by (uid=0)
Dec 17 15:44:11 server.nabakulin.net systemd[1]: Starting Hostname Service...
Subject: A start job for unit systemd-hostnamed.service has begun execution
Defined-By: systemd
Support: https://access.redhat.com/support

A start job for unit systemd-hostnamed.service has begun execution.

The job identifier is 2549.
Dec 17 15:44:11 server.nabakulin.net systemd[1]: Started Hostname Service.
```

Рисунок 4

2.2. На сервере откройте файл /etc/ssh/sshd\_config конфигурации sshd на редактирование и добавьте строку

```
#LoginGraceTime 2m
PermitRootLogin no
AllowUsers vagrant
```

Рисунок 5

2.3. После сохранения изменений в файле конфигурации перезапустите sshd

2.4. Повторите попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя user – Invalid user (пользователь не входит в список разрешенных)

```
[root@client.nabakulin.net vagrant]# ssh nabakulin@server.nabakulin.net
The authenticity of host 'server.nabakulin.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:zqb0am9bCTBqb0qNzuP7z0xlg0qvGhkHxMkw2sQdblo.
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.nabakulin.net' (ED25519) to the list of known hosts.
nabakulin@server.nabakulin.net's password:
Permission denied, please try again.
nabakulin@server.nabakulin.net's password:
Permission denied, please try again.
nabakulin@server.nabakulin.net's password:
nabakulin@server.nabakulin.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@client.nabakulin.net vagrant]#
```

```
nabakulin@server:~ — journalctl -x -f
Dec 17 18:09:19 server.nabakulin.net unix_chkpwd[9767]: password check failed for user (nabakulin)
Dec 17 18:09:19 server.nabakulin.net sshd[9761]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30 user=nabakulin
Dec 17 18:09:21 server.nabakulin.net sshd[9761]: Failed password for invalid user nabakulin from 192.168.1.30 port 37090 ssh2
Dec 17 18:09:24 server.nabakulin.net unix_chkpwd[9768]: password check failed for user (nabakulin)
Dec 17 18:09:26 server.nabakulin.net sshd[9761]: Failed password for invalid user nabakulin from 192.168.1.30 port 37090 ssh2
Dec 17 18:09:29 server.nabakulin.net unix_chkpwd[9769]: password check failed for user (nabakulin)
Dec 17 18:09:31 server.nabakulin.net sshd[9761]: Failed password for invalid user nabakulin from 192.168.1.30 port 37090 ssh2
Dec 17 18:09:31 server.nabakulin.net sshd[9761]: Connection closed by invalid user nabakulin 192.168.1.30 port 37090 [preauth]
Dec 17 18:09:31 server.nabakulin.net sshd[9761]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30 user=nabakulin
```

Рисунок 6

2.5. В файле /etc/ssh/sshd\_config конфигурации sshd внесите следующее изменение

```
#LoginGraceTime 2m
PermitRootLogin no
AllowUsers vagrant nabakulin
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Рисунок 7

2.6. После сохранения изменений в файле конфигурации перезапустите sshd и вновь попытайтесь получить доступ с клиента к серверу посредством SSH-соединения через пользователя user – доступ есть

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

Last login: Sat Dec 17 15:44:11 2022 from 192.168.1.30
[nabakulin@server.nabakulin.net ~]$

Dec 17 15:49:24 server.nabakulin.net sshd[6188]: Accepted password for nabakulin from 192.168.1.30 port 55960 ssh2
Dec 17 15:49:24 server.nabakulin.net systemd-logind[603]: New session 7 of user nabakulin.
  Subject: A new session 7 has been created for user nabakulin
  Defined-By: systemd
  Support: https://access.redhat.com/support
  Documentation: sd-login(3)

  A new session with the ID 7 has been created for the user nabakulin.

  The leading process of the session is 6188.
Dec 17 15:49:24 server.nabakulin.net systemd[1]: Started Session 7 of User nabakulin.
  Subject: A start job for unit session-7.scope has finished successfully
  Defined-By: systemd
  Support: https://access.redhat.com/support

  A start job for unit session-7.scope has finished successfully.

  The job identifier is 2763.
Dec 17 15:49:24 server.nabakulin.net sshd[6188]: pam_unix(sshd:session): session opened for user nabakulin(uid=1001) by (uid=0)
Dec 17 15:49:25 server.nabakulin.net systemd[1]: Starting Hostname Service...
  Subject: A start job for unit systemd-hostnamed.service has begun execution
  Defined-By: systemd
  Support: https://access.redhat.com/support

  A start job for unit systemd-hostnamed.service has begun execution.

  The job identifier is 2836.
Dec 17 15:49:25 server.nabakulin.net systemd[1]: Started Hostname Service.
```

Рисунок 8

3.

3.1. На сервере в файле конфигурации sshd /etc/ssh/sshd\_config найдите строку Port и ниже этой строки добавьте

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

Рисунок 9

3.2. После сохранения изменений в файле конфигурации перезапустите sshd

3.3. Посмотрите расширенный статус работы sshd – ошибка бинда на порте 2022 из-за SELinux

```
[root@server.nabakulin.net ~]# systemctl restart sshd
[root@server.nabakulin.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2022-12-17 15:52:23 UTC; 5s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 6262 (sshd)
    Tasks: 1 (limit: 5788)
   Memory: 1.7M
      CPU: 14ms
   CGroup: /system.slice/sshd.service
           └─6262 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 17 15:52:23 server.nabakulin.net systemd[1]: Starting OpenSSH server daemon...
Dec 17 15:52:23 server.nabakulin.net sshd[6262]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
Dec 17 15:52:23 server.nabakulin.net sshd[6262]: error: Bind to port 2022 on :: failed: Permission denied.
Dec 17 15:52:23 server.nabakulin.net sshd[6262]: Server listening on 0.0.0.0 port 22.
Dec 17 15:52:23 server.nabakulin.net sshd[6262]: Server listening on :: port 22.
Dec 17 15:52:23 server.nabakulin.net systemd[1]: Started OpenSSH server daemon.
[root@server.nabakulin.net ~]#
```

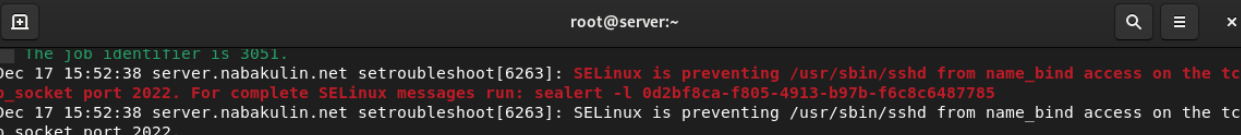


Рисунок 10

3.4. Исправьте на сервере метки SELinux к порту 2022

3.5. В настройках межсетевого экрана откройте порт 2022 протокола TCP

3.6. Вновь перезапустите sshd и посмотрите расширенный статус его работы.

Статус показывает, что процесс sshd теперь прослушивает два порта

```
[root@server.nabakulin.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.nabakulin.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.nabakulin.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.nabakulin.net ~]# systemctl restart sshd
[root@server.nabakulin.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2022-12-17 15:54:36 UTC; 3s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 6309 (sshd)
    Tasks: 1 (limit: 5788)
   Memory: 1.7M
      CPU: 13ms
   CGroup: /system.slice/sshd.service
           └─6309 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 17 15:54:36 server.nabakulin.net systemd[1]: Starting OpenSSH server daemon...
Dec 17 15:54:36 server.nabakulin.net sshd[6309]: Server listening on 0.0.0.0 port 2022.
Dec 17 15:54:36 server.nabakulin.net sshd[6309]: Server listening on :: port 2022.
Dec 17 15:54:36 server.nabakulin.net sshd[6309]: Server listening on 0.0.0.0 port 22.
Dec 17 15:54:36 server.nabakulin.net systemd[1]: Started OpenSSH server daemon.
Dec 17 15:54:36 server.nabakulin.net sshd[6309]: Server listening on :: port 22.
```

Рисунок 11

3.7. С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя user

3.8. Повторите попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя user, указав порт 2022

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

Last login: Sat Dec 17 15:49:24 2022 from 192.168.1.30
[nabakulin@server.nabakulin.net ~]$ sudo -i
[sudo] password for nabakulin:
[root@server.nabakulin.net ~]# exit
logout
[nabakulin@server.nabakulin.net ~]$ exit
logout
Connection to server.nabakulin.net closed.
[nabakulin@client.nabakulin.net ~]$ ssh -p2022 nabakulin@server.nabakulin.net
nabakulin@server.nabakulin.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Dec 17 15:55:34 2022 from 192.168.1.30
[nabakulin@server.nabakulin.net ~]$ sudo -i
[sudo] password for nabakulin:
[root@server.nabakulin.net ~]#
```

Рисунок 12

4.

4.1. На сервере в конфигурационном файле `/etc/ssh/sshd_config` задайте параметр, разрешающий аутентификацию по ключу

```
#LoginGraceTime 2m
PermitRootLogin no
AllowUsers vagrant nabakulin
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes
```

Рисунок 13

4.2. После сохранения изменений в файле конфигурации перезапустите `sshd`

4.3. На клиенте сформируйте SSH-ключ, введя в терминале под пользователем `user`

4.4. Закрытый ключ теперь будет записан в файл `~/.ssh/id_rsa`, а открытый ключ записывается в файл `~/.ssh/id_rsa.pub`

4.5. Попробуйте получить доступ с клиента к серверу посредством SSH-соединения – подключаемся без ввода пароля



```
[nabakulin@client.nabakulin.net ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/nabakulin/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/nabakulin/.ssh/id_rsa
Your public key has been saved in /home/nabakulin/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:7rYx0wGjMKZyNxrRm5Tmre4VNNq8DUQk8I8x6B4vsM nabakulin@client.nabakulin.net
The key's randomart image is:
+---[RSA 3072]-----+
|  +.ooo |
|  .B *  |
|  . o= B o |
|  o= 0 * + |
|  o.+ 0 BS. |
|  o.o.* =.. |
|  ..E= + +. |
|  ... .O+ |
|  .+o |
+---[SHA256]-----+
[nabakulin@client.nabakulin.net ~]$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDQDRD2QUf8N0kboAYVcgZ0M7tv8c2HBZwLwt2fe6t/kt07XZ69fioKrQXWhIH7br51URNi+gn0RHISvZ7pl2WS0eTK
o5msZUryruJ2rNjEtZwoik2siHRwDBi/C/j4Az7sC5qjiHK/+SN4SlgjCq9DdzIspoLPHFc0gdTpWwulw0x0oqRIucU5nXFicDgZI7wU04WzXaNPULQuYqHZab4da
4EWcbPWVsoxn0kLhdigsj3YxyrhX26yVEXV1HGtg0B2t90hgmWmw86jEmJPwt6TZCV92+qj719uk+cuI4EIPGcY6ZrdKaiRpV7pqJa6xXv4P39qfYRxmA3whkRlj+
Hs3izrpzVteVsZj5kfMTDseRBvXDT9a8IU0HTK+n0Jst4aAl+0H+dRq/b/1UolAbsSjTRqxj8pkB7kwxli0hosUde9+h0NrYbykv0IahV6z11V7zFQK47TX07bnL7R
QUbRsyIXs9Q5vmkRE4GYEwMMXY76kJOtPF2ycW6zNcYFGE= nabakulin@client.nabakulin.net
[nabakulin@client.nabakulin.net ~]$ ssh-copy-id nabakulin@server.nabakulin.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
nabakulin@server.nabakulin.net's password:

Number of key(s) added: 1

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

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

Last login: Sat Dec 17 15:56:16 2022 from 192.168.1.30
[nabakulin@server.nabakulin.net ~]$
```

Рисунок 14

5.
  - 5.1. На клиенте посмотрите, запущены ли какие-то службы с протоколом TCP
  - 5.2. Перенаправьте порт 80 на server.user.net на порт 8080 на локальной машине
  - 5.3. Вновь на клиенте посмотрите, запущены ли какие-то службы с протоколом TCP
  - 5.4. На клиенте запустите браузер и в адресной строке введите localhost:8080.  
Убедитесь, что отобразится страница с приветствием «Welcome to the server.user.net server»

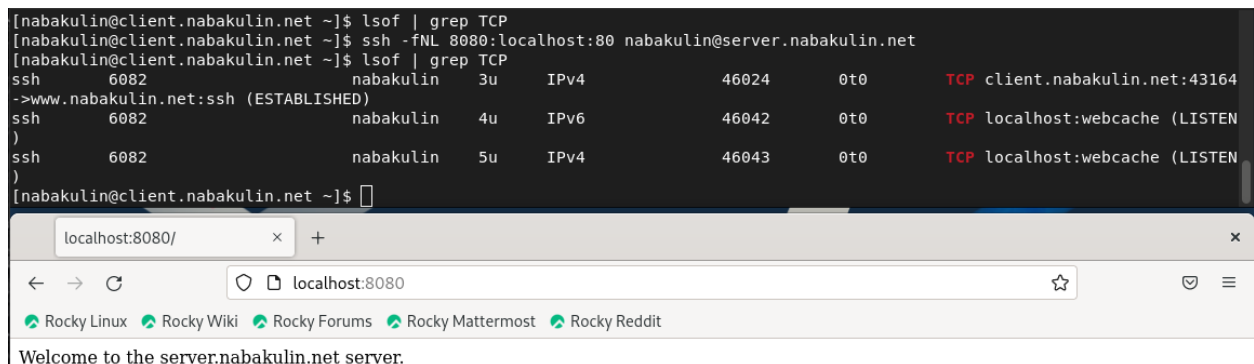


Рисунок 15

- 6.

6.1. На клиенте откройте терминал под пользователем user

6.2. Посмотрите с клиента имя узла сервера

6.3. Посмотрите с клиента список файлов на сервере

6.4. Посмотрите с клиента почту на сервере

```
[nabakulin@client.nabakulin.net ~]$ ssh nabakulin@server.nabakulin.net hostname
server.nabakulin.net
[nabakulin@client.nabakulin.net ~]$ ssh nabakulin@server.nabakulin.net ls -Al
total 60
-rw-----. 1 nabakulin nabakulin   768 Dec 17 15:57 .bash_history
-rw-r--r--. 1 nabakulin nabakulin   18 May 16 2022 .bash_logout
-rw-r--r--. 1 nabakulin nabakulin  141 May 16 2022 .bash_profile
-rw-r--r--. 1 nabakulin nabakulin   546 Dec 10 16:02 .bashrc
drwxr-xr-x. 9 nabakulin nabakulin 4096 Nov 12 18:00 .cache
drwx-----. 8 nabakulin nabakulin  169 Nov 12 18:00 .config
drwxr-xr-x. 2 nabakulin nabakulin    6 Nov 12 17:58 Desktop
drwxr-xr-x. 2 nabakulin nabakulin    6 Nov 12 17:58 Documents
drwxr-xr-x. 2 nabakulin nabakulin    6 Nov 12 17:58 Downloads
drwx-----. 4 nabakulin nabakulin    32 Nov 12 17:58 .local
drwx-----. 5 nabakulin nabakulin 4096 Dec 11 00:40 Maildir
drwxr-xr-x. 4 nabakulin nabakulin   39 Nov 1 09:32 .mozilla
drwxr-xr-x. 2 nabakulin nabakulin    6 Nov 12 17:58 Music
drwxr-xr-x. 2 nabakulin nabakulin    6 Nov 12 17:58 Pictures
drwxr-xr-x. 2 nabakulin nabakulin    6 Nov 12 17:58 Public
drwx-----. 2 nabakulin nabakulin   29 Dec 17 16:04 .ssh
drwxr-xr-x. 2 nabakulin nabakulin    6 Nov 12 17:58 Templates
-rw-r-----. 1 nabakulin nabakulin    5 Dec 17 15:26 .vboxclient-clipboard.pid
-rw-r-----. 1 nabakulin nabakulin    5 Dec 17 15:26 .vboxclient-display-svga-x11.pid
-rw-r-----. 1 nabakulin nabakulin    5 Dec 17 15:26 .vboxclient-draganddrop.pid
-rw-r-----. 1 nabakulin nabakulin    5 Dec 17 15:26 .vboxclient-seamless.pid
drwxr-xr-x. 2 nabakulin nabakulin    6 Nov 12 17:58 Videos
-rw-----. 1 nabakulin nabakulin 10022 Dec 11 00:22 .viminfo
-rw-----. 1 nabakulin nabakulin   314 Dec 17 15:26 .xsession-errors
-rw-----. 1 nabakulin nabakulin   314 Dec 10 18:54 .xsession-errors.old
[nabakulin@client.nabakulin.net ~]$ ssh nabakulin@server.nabakulin.net MAIL=~/.Maildir/ mail
s-nail version v14.9.22. Type '?' for help
/home/nabakulin/Maildir: 6 messages 2 unread 3 deleted
 4 nabakulin          2022-12-10 19:48 18/645 "test"
U 5 nabakulin@nabakulin. 2022-12-11 00:20 18/608 "LMTP test"
U 6 nabakulin          2022-12-11 00:39 22/821 "test tls"
```

Рисунок 16

7.

7.1. На сервере в конфигурационном файле /etc/ssh/sshd\_config разрешите отображать на локальном клиентском компьютере графические интерфейсы X11

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

Рисунок 17

7.2. После сохранения изменения в конфигурационном файле перезапустите sshd

7.3. Попробуйте с клиента удалённо подключиться к серверу и запустить графическое приложение, например firefox

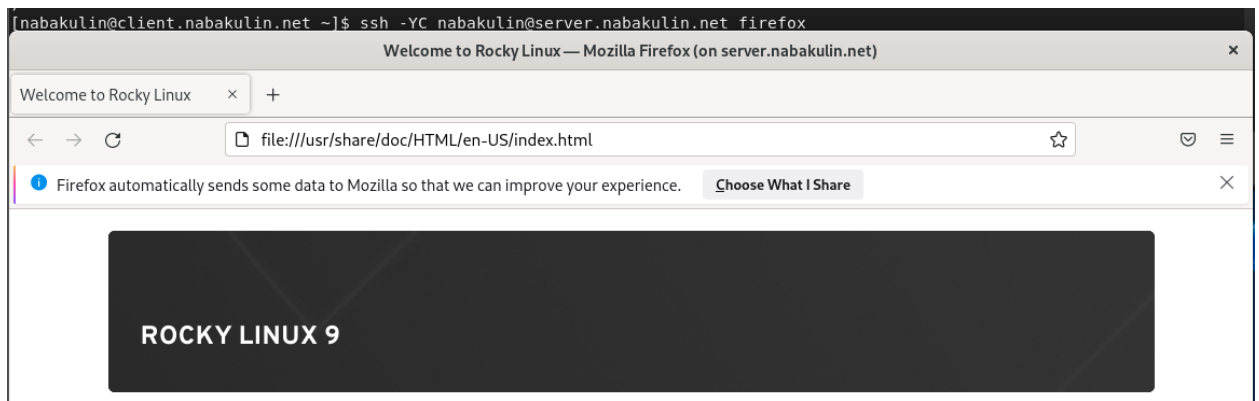


Рисунок 18

8.

8.1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создайте в нём каталог `ssh`, в который поместите в соответствующие подкаталоги конфигурационный файл `sshd_config`

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

Рисунок 19

8.2. В каталоге `/vagrant/provision/server` создайте исполняемый файл `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 20

8.3. Для отработки созданного скрипта во время загрузки виртуальной машины

server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера

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

*Рисунок 21*

### Контрольные вопросы

1. Вы хотите запретить удалённый доступ по SSH на сервер пользователю root и разрешить доступ пользователю alice. Как это сделать?  
В /etc/ssh/sshd\_config указать PermitRootLogin No и AllowUsers alice
2. Как настроить удалённый доступ по SSH через несколько портов? Для чего это может потребоваться?  
В /etc/ssh/sshd\_config указать Port 22 Port 2022 для портов 22 и 2022. Даёт гарантию возможности открыть сеансы SSH, даже если была сделана ошибка в конфигурации
3. Какие параметры используются для создания туннеля SSH, когда команда ssh устанавливает фоновое соединение и не ожидает какой-либо конкретной команды?  
Из /etc/ssh/sshd\_config
4. Как настроить локальную переадресацию с локального порта 5555 на порт 80 сервера server2.example.com?  
ssh -fNL 5555:localhost:80 user@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 и firewall-cmd --add-port=2022/tcp --permanent