

Лабораторная работа 11

Настройка безопасного удалённого доступа по протоколу SSH

Митрофанов Тимур Александрович

Содержание

| | |
|---|-----------|
| 1 Цель работы | 5 |
| 2 Задание | 6 |
| 3 Выполнение лабораторной работы | 7 |
| 4 Выводы | 21 |
| Список литературы | 22 |

Список иллюстраций

| | | |
|------|--|----|
| 3.1 | смена настройки | 7 |
| 3.2 | мониторинг | 8 |
| 3.3 | попытка входа под рутом | 8 |
| 3.4 | изменение файла | 9 |
| 3.5 | перезапуск службы | 9 |
| 3.6 | повторная попытка зайти под рутом и запрет сервера на это действие | 9 |
| 3.7 | подключение к пользователю на сервере | 10 |
| 3.8 | изменение конфига | 10 |
| 3.9 | попытка подключения к серверу | 10 |
| 3.10 | изменение файла | 11 |
| 3.11 | успешное подключение к серверу | 11 |
| 3.12 | измениаем кофиг | 12 |
| 3.13 | перезапуск служб | 12 |
| 3.14 | проверяяем наличие ошибки | 12 |
| 3.15 | настройка Postfix | 13 |
| 3.16 | обычное подключение к серверу | 13 |
| 3.17 | поключение через новый порт | 14 |
| 3.18 | меняем кофигурационный файл | 14 |
| 3.19 | перезапуск служб | 14 |
| 3.20 | создание ключа и копирование ключа на сервер | 15 |
| 3.21 | проверирем запущенные службы | 16 |
| 3.22 | перенаправление | 16 |
| 3.23 | проверирем запущенные службы | 17 |
| 3.24 | проверка работы перенаправления | 17 |
| 3.25 | проверка домтупа к серверу без пароля | 18 |
| 3.26 | изменения конф файла | 18 |
| 3.27 | ткываем удалённо браузер на сервере | 19 |
| 3.28 | сохранение файлов и их создание | 19 |
| 3.29 | новый скрипт | 20 |
| 3.30 | дополнение скрипта на основной системе | 20 |

Список таблиц

1 Цель работы

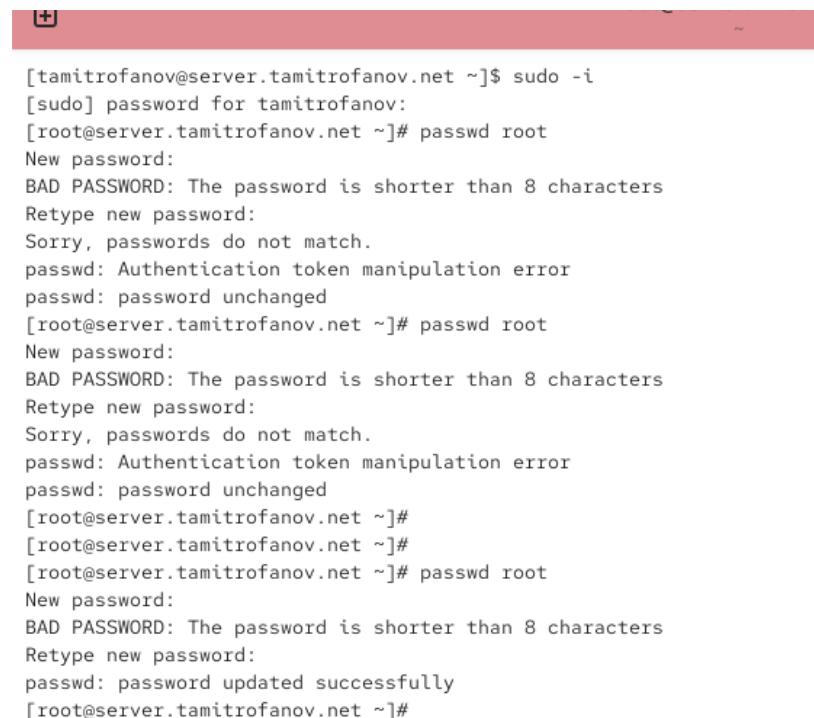
Приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

2 Задание

1. Настройте запрет удалённого доступа на сервер по SSH для пользователя root (см. раздел 11.4.1).
2. Настройте разрешение удалённого доступа к серверу по SSH только для пользователей группы vagrant и вашего пользователя (см. раздел 11.4.2).
3. Настройте удалённый доступ к серверу по SSH через порт 2022 (см. раздел 11.4.3).
4. Настройте удалённый доступ к серверу по SSH по ключу (см. раздел 11.4.4).
5. Организуйте SSH-туннель с клиента на сервер, перенаправив локальное соединение с TCP-порта 80 на порт 8080 (см. раздел 11.4.5).
6. Используя удалённое SSH-соединение, выполните с клиента несколько команд на сервере (см. раздел 11.4.6).
7. Используя удалённое SSH-соединение, запустите с клиента графическое приложение на сервере (см. раздел 11.4.7).
8. Напишите скрипт для Vagrant, фиксирующий действия по настройке SSH-сервера во внутреннем окружении виртуальной машины server. Соответствующим образом внесите изменения в Vagrantfile (см. раздел 11.4.8).

3 Выполнение лабораторной работы

На сервере задайте пароль для пользователя root, если этого не было сделано ранее (рис. 3.1).



```
[+] ~

[tamitrofanov@server.tamitrofanov.net ~]$ sudo -i
[sudo] password for tamitrofanov:
[root@server.tamitrofanov.net ~]# passwd root
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
[root@server.tamitrofanov.net ~]# passwd root
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
[root@server.tamitrofanov.net ~]#
[root@server.tamitrofanov.net ~]#
[root@server.tamitrofanov.net ~]# passwd root
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
[root@server.tamitrofanov.net ~]#
```

Рисунок 3.1: смена настройки

На сервере в дополнительном терминале запустите мониторинг системных событий (рис. 3.2).

```

root@server:~ - sudo -i
The job identifier is 35029.
Nov 15 16:25:29 server.tamitrofanov.net systemd-coredump[20591]: [^] Process 20586 (VBoxClient) of user 1001 dumped core.

Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64
Module libXi.so.6 from rpm libXi-1.8.10-1.el10.x86_64
Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64
Module wayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64

Stack trace of thread 20589:
#0 0x000000000041db4b n/a (n/a + 0x0)
#1 0x000000000041dac4 n/a (n/a + 0x0)
#2 0x0000000000450a7c n/a (n/a + 0x0)
#3 0x0000000000423590 n/a (n/a + 0x0)
#4 0x00007f27099f6b68 start_thread (libc.so.6 + 0x94b68)
#5 0x00007f2709a676bc __clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 20586:
#0 0x00007f2709a654bd syscall (libc.so.6 + 0x1034bd)
#1 0x00000000004347a2 n/a (n/a + 0x0)
#2 0x0000000000450c66 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x00007f270998c30e __libc_start_main (libc.so.6 + 0x2a30e)

#5 0x00007f270998c3e9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)

Subject: Process 20586 (VBoxClient) dumped core
Defined-By: systemd
Support: https://wiki.rockylinux.org/rocky/support
Documentation: man:core(5)

Process 20586 (VBoxClient) crashed and dumped core.

This usually indicates a programming error in the crashing program and
should be reported to its vendor as a bug.
Nov 15 16:25:29 server.tamitrofanov.net systemd[1]: systemd-coredump@1384-20590-0.service: Deactivated successfully.
Subject: Unit succeeded
Defined-By: systemd
Support: https://wiki.rockylinux.org/rocky/support

The unit systemd-coredump@1384-20590-0.service has successfully entered the 'dead' state.

```

Рисунок 3.2: мониторинг

С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя root (рис. 3.3).

при поптке подключения создается отпечаток, но система запрещает войти под рутов в запись рут на сервере

```

[root@client.tamitrofanov.net ~]# ssh root@server.tamitrofanov.net
The authenticity of host 'server.tamitrofanov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:P5dS2DpuJpn/RRQavMA05prSyv96seCb42L+n7pX+Iw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'server.tamitrofanov.net' (ED25519) to the list of known hosts.
root@server.tamitrofanov.net's password:
Permission denied, please try again.
root@server.tamitrofanov.net's password:
Permission denied, please try again.
root@server.tamitrofanov.net's password:
root@server.tamitrofanov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@client.tamitrofanov.net ~]#

```

Рисунок 3.3: попытка входа под рутом

На сервере откройте файл /etc/ssh/sshd_config конфигурации sshd для редактирования и запретите вход на сервер пользователю root (рис. 3.4).

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

Рисунок 3.4: изменение файла

После сохранения изменений в файле конфигурации перезапустите sshd (рис. 3.5).

```
@server.tamitrofanov.net ~]# systemctl restart sshd
@server.tamitrofanov.net ~]#
```

Рисунок 3.5: перезапуск службы

Повторите попытку получения доступа с клиента к серверу посредством SSHсоединения через пользователя root (рис. 3.6).

```
Last login: Sat Nov 15 16:41:58 2025 from 192.168.1.1
[tamitrofanov@server.tamitrofanov.net ~]$ 
[tamitrofanov@server.tamitrofanov.net ~]$ 
[tamitrofanov@server.tamitrofanov.net ~]$ 
[tamitrofanov@server.tamitrofanov.net ~]$ 
[tamitrofanov@server.tamitrofanov.net ~]$ ssh root@server.tamitrofanov.net
root@server.tamitrofanov.net's password:
Permission denied, please try again.
root@server.tamitrofanov.net's password:
Permission denied, please try again.
root@server.tamitrofanov.net's password:
root@server.tamitrofanov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[tamitrofanov@server.tamitrofanov.net ~]$
```

Рисунок 3.6: повторная попытка зайти под рутом и запрет сервера на это действие

П. С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя user (вместо user укажите вашего пользователя) (рис. 3.7).

система нас пускает

```

[tamitrofanov@client.tamitrofanov.net ~]$ ssh tamitrofanov@server.tamitrofanov.net
The authenticity of host 'server.tamitrofanov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:PSd52DpuJpn/RRQaVMAQ5prSyv96seCb42L+n7pX+Iw.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [server.tamitrofanov.net]:2022
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'server.tamitrofanov.net' (ED25519) to the list of known hosts.
tamitrofanov@server.tamitrofanov.net's password:
Web console: https://server.tamitrofanov.net:9090/ or https://10.0.2.15:9090/
Last login: Sat Nov 15 16:41:58 2025 from 192.168.1.1
[tamitrofanov@server.tamitrofanov.net ~]$

```

Рисунок 3.7: подключение к пользователю на сервере

На сервере откройте файл /etc/ssh/sshd_config конфигурации sshd на редактирование и добавьте строку (рис. 3.8).

```

# Authentication:
#LoginGraceTime 2m
PermitRootLogin no
AllowUsers vagrant
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

```

Рисунок 3.8: изменение конфига

После сохранения изменений в файле конфигурации перезапустите sshd Повторите попытку получения доступа с клиента к серверу посредством (рис. 3.9).

так как мы запретили иным пользователям кроме вгранта подключение на сервере перестаёт пускать

```

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

```

Рисунок 3.9: попытка подключения к серверу

В файле /etc/ssh/sshd_config конфигурации sshd внесите следующее изменение (рис. 3.10).

```
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
AllowUsers vagrant tamitrofanov
#StrictModes yes
```

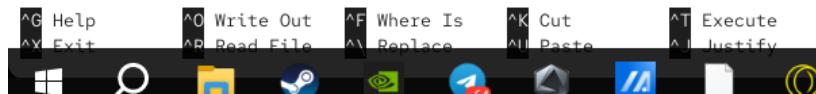


Рисунок 3.10: изменение файла

После сохранения изменений в файле конфигурации перезапустите sshd и вновь попытайтесь получить доступ с клиента к серверу посредством SSH-соединения через пользователя user. В отчёте поясните, что при этом происходит (рис. 3.11).

так как мы прописали разрешение нашему пользователю на подключение нас пускает

```
[tamitrofanov@client.tamitrofanov.net ~]$ ssh tamitrofanov@server.tamitrofanov.net
tamitrofanov@server.tamitrofanov.net's password:
Web console: https://server.tamitrofanov.net:9090/ or https://10.0.2.15:9090/
Last login: Sat Nov 15 16:49:09 2025 from 192.168.1.30
[tamitrofanov@server.tamitrofanov.net ~]$
```

Рисунок 3.11: успешное подключение к серверу

На сервере в файле конфигурации sshd /etc/ssh/sshd_config найдите строку Port и ниже этой строки добавьте (рис. 3.12).

```

# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22

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

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key

```

Рисунок 3.12: изменияем конфиг

После сохранения изменений в файле конфигурации перезапустите sshd (рис. 3.13).

```

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

```

Рисунок 3.13: перезапуск службы

Посмотрите расширенный статус работы sshd (рис. 3.14).
проблема в том что нам надо шифрованное подключение на порту для безопасного подключения, но мы не указывали tcp на указанный порт

```

[root@server.tamitrofanov.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 Sat 2025-11-15 17:03:41 UTC; 25s ago
    Invocation-ID: ae2d53f98a5d4536825af75129548fe
      Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 25482 (sshd)
     Tasks: 1 (limit: 10366)
    Memory: 1M (peak: 1.2M)
       CPU: 14ms
      CGroup: /system.slice/sshd.service
              └─25482 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Nov 15 17:03:41 server.tamitrofanov.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
Nov 15 17:03:41 server.tamitrofanov.net (sshd)[25482]: sshd.service: Referenced but unset environment variable evaluates to
Nov 15 17:03:41 server.tamitrofanov.net sshd[25482]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
Nov 15 17:03:41 server.tamitrofanov.net sshd[25482]: error: Bind to port 2022 on :: failed: Permission denied.
Nov 15 17:03:41 server.tamitrofanov.net sshd[25482]: Server listening on 0.0.0.0 port 22.
Nov 15 17:03:41 server.tamitrofanov.net sshd[25482]: Server listening on :: port 22.
Nov 15 17:03:41 server.tamitrofanov.net systemd[1]: Started sshd.service - OpenSSH server daemon.
lines 1-20/20 (END)

```

Рисунок 3.14: проверяя наличие ошибки

Исправьте на сервере метки SELinux к порту 2022. В настройках межсетевого экрана откройте порт 2022 протокола TCP. Вновь перезапустите sshd и посмотрите

расширенный статус его работы. Статус должен показать, что процесс sshd теперь прослушивает два порта. (рис. 3.15).

```
[root@server.tamitrofanov.net ~]# [root@server.tamitrofanov.net ~]# semanage port -a -t ssh_port_t -p tcp 2022 [root@server.tamitrofanov.net ~]# [root@server.tamitrofanov.net ~]# [root@server.tamitrofanov.net ~]# i firewall-cmd --add-port=2022/tcp firewall-cmd --add-port=2022/tcp --permanent bash: i: command not found... success [root@server.tamitrofanov.net ~]# firewall-cmd --add-port=2022/tcp firewall-cmd --add-port=2022/tcp --permanent success Warning: ALREADY_ENABLED: 2022:tcp success [root@server.tamitrofanov.net ~]# systemctl restart sshd [root@server.tamitrofanov.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 Sat 2025-11-15 17:06:56 UTC; 3s ago Invocation: 1a26112a5e04e5ca03deb19a4ca0b27 Docs: man:sshd(8) man:sshd_config(5) Main PID: 25933 (sshd) Tasks: 1 (limit: 10366) Memory: 1M (peak: 1.3M) CPU: 15ms CGroup: /system.slice/sshd.service └─25933 "sshd: /usr/sbin/sshd -D [listener]" 0 of 10-100 startups Nov 15 17:06:56 server.tamitrofanov.net systemd[1]: Starting sshd.service - OpenSSH server daemon... Nov 15 17:06:56 server.tamitrofanov.net (sshd)[25933]: sshd.service: Referenced but unset environment variable evaluates to Nov 15 17:06:56 server.tamitrofanov.net sshd[25933]: Server listening on 0.0.0.0 port 2022. Nov 15 17:06:56 server.tamitrofanov.net sshd[25933]: Server listening on :: port 2022. Nov 15 17:06:56 server.tamitrofanov.net sshd[25933]: Server listening on 0.0.0.0 port 22. Nov 15 17:06:56 server.tamitrofanov.net sshd[25933]: Server listening on :: port 22. Nov 15 17:06:56 server.tamitrofanov.net systemd[1]: Started sshd.service - OpenSSH server daemon.
```

Рисунок 3.15: настройка Postfix

С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя user (вместо user укажите вашего пользователя). После открытия оболочки пользователя введите sudo -i для получения доступа root. Отлогиньтесь от root и вашего пользователя на сервере, введя дважды logout или используя дважды комбинацию клавиш Ctrl + d . (рис. 3.16).

```
[tamitrofanov@client.tamitrofanov.net ~]$ [tamitrofanov@client.tamitrofanov.net ~]$ ssh tamitrofanov@server.tamitrofanov.net tamitrofanov@server.tamitrofanov.net's password: Web console: https://server.tamitrofanov.net:9090/ or https://10.0.2.15:9090/ Last login: Sat Nov 15 17:01:23 2025 from 192.168.1.30 [tamitrofanov@server.tamitrofanov.net ~]$ sudo -i [sudo] password for tamitrofanov: [root@server.tamitrofanov.net ~]# logout [tamitrofanov@server.tamitrofanov.net ~]$ logout Connection to server.tamitrofanov.net closed. [tamitrofanov@client.tamitrofanov.net ~]$
```

Рисунок 3.16: обычное подключение к серверу

Повторите попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя user, указав порт 2022: ssh -p2022 user@server.user.net После открытия оболочки пользователя введите sudo -i для получения доступа root.

Отлогиньтесь от root и вашего пользователя на сервере, введя дважды logout или используя дважды комбинацию клавиш Ctrl + d . (рис. 3.17).

```
[tmitrofanov@client.tmitrofanov.net ~]$  
[tmitrofanov@client.tmitrofanov.net ~]$ ssh -p2022 tmitrofanov@server.tmitrofanov.net  
tmitrofanov@server.tmitrofanov.net's password:  
Web console: https://server.tmitrofanov.net:9090/ or https://10.0.2.15:9090/  
  
Last login: Sat Nov 15 17:07:54 2025 from 192.168.1.30  
[tmitrofanov@server.tmitrofanov.net ~]$ root  
bash: root: command not found..  
Install package 'root' to provide command 'root'? [N/y] ^C  
[tmitrofanov@server.tmitrofanov.net ~]$ sudo -i  
[sudo] password for tmitrofanov:  
[root@server.tmitrofanov.net ~]# logout  
[tmitrofanov@server.tmitrofanov.net ~]$ logout  
Connection to server.tmitrofanov.net closed.  
[tmitrofanov@client.tmitrofanov.net ~]$
```

Рисунок 3.17: поключение через новый порт

На сервере в конфигурационном файле /etc/ssh/sshd_config задайте параметр, разрешающий аутентификацию по ключу (рис. 3.18).

```
#MaxSessions 10  
  
PubkeyAuthentication yes  
  
# The default is to check both .ssh/authorized_keys  
# but this is overridden so installations will  
AuthorizedKeysFile      .ssh/authorized_keys
```

Рисунок 3.18: меняем кофигурационный файл

После сохранения изменений в файле конфигурации перезапустите sshd (рис. 3.19).

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

Рисунок 3.19: перезапуск служб

На клиенте сформируйте SSH-ключ, введя в терминале под пользователем user (вместо user используйте ваш логин): ssh-keygen Когда вас спросят, хотите ли вы

использовать кодовую фразу, нажмите Enter , чтобы использовать установку без пароля. При запросе имени файла, в котором будет храниться закрытый ключ, примите предлагаемое по умолчанию имя файла (~/.ssh/id_rsa). Когда вас попросят ввести кодовую фразу, нажмите Enter дважды. Скопируйте открытый ключ на сервер, введя на клиенте (вместо user укажите вашего пользователя) Попробуйте получить доступ с клиента к серверу посредством SSH-соединения (вместо user используйте ваш логин): ssh user@server.user.net Теперь вы должны пройти аутентификацию без ввода пароля для учётной записи удалённого пользователя. Отлогиньтесь с сервера, используя комбинацию клавиш Ctrl + d .(рис. 3.20).

```
[tamtrofanov@client.tamtrofanov.net ~]$ ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/tamtrofanov/.ssh/id_ed25519):
Enter passphrase for '/home/tamtrofanov/.ssh/id_ed25519' (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/tamtrofanov/.ssh/id_ed25519
Your public key has been saved in /home/tamtrofanov/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:00m7NYYT05BW5Nk5ETqtFaAvkneY4bCd91RC2gm0A tamitrofanov@client.tamtrofanov.net
The key's randomart image is:
+--[ED25519 256]--+
| ..E *B.. |
| .O..+o+.o . |
| o*** o . |
| . *Xoo. . |
| o*XS. . |
| ..B.o |
| O.o |
| *=. |
| o. o. |
+---[SHA256]----+
[tamtrofanov@client.tamtrofanov.net ~]$ ssh-copy-id tamitrofanov@server.tamtrofanov.net
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ssh-add -l
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
tamtrofanov@server.tamtrofanov.net's password:

Number of key(s) added: 1

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

[tamtrofanov@client.tamtrofanov.net ~]$ ssh tamitrofanov@server.tamtrofanov.net
Web console: https://server.tamtrofanov.net:9090/ or https://10.0.2.15:9090/

Last login: Sat Nov 15 17:09:17 2025 from 192.168.1.30
[tamtrofanov@server.tamtrofanov.net ~]$ logout
Connection to server.tamtrofanov.net closed.
[tamtrofanov@client.tamtrofanov.net ~]$
```

Рисунок 3.20: создание ключа и копирование ключа на сервер

На клиенте посмотрите, запущены ли какие-то службы с протоколом TCP (рис. 3.21).

```
[tamitrofanov@client.tamitrofanov.net ~]$ lsof | grep TCP
^C
[tamitrofanov@client.tamitrofanov.net ~]$ sudo lsof | grep TCP
[sudo] password for tamitrofanov:
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
        Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
        Output information may be incomplete.
systemd      1          root    8u    IPv6          8506    0t0      TCP *:websm (LISTEN
)
cupsd     1219          root    7u    IPv6          9902    0t0      TCP localhost:ipp (
LISTEN)
cupsd     1219          root    8u    IPv4          9903    0t0      TCP localhost:ipp (
LISTEN)
sshd      1223          root    7u    IPv4          10871   0t0      TCP *:ssh (LISTEN)
sshd      1223          root    8u    IPv6          10873   0t0      TCP *:ssh (LISTEN)
master    1354          root   13u    IPv4          10183   0t0      TCP localhost:smtp
(ListEN)
firefox   3352      tamitrofanov  62u    IPv4          341260  0t0      TCP client.tamitrof
anov.net:52192->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox   3352      tamitrofanov  65u    IPv4          340595  0t0      TCP client.tamitrof
anov.net:52206->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox   3352      tamitrofanov  88u    IPv4          340598  0t0      TCP client.tamitrof
anov.net:43278->146.75.117.91:https (ESTABLISHED)
firefox   3352      tamitrofanov  62u    IPv4          341260  0t0      TCP client.tamitrof
anov.net:52192->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox   3352      tamitrofanov  65u    IPv4          340595  0t0      TCP client.tamitrof
anov.net:52206->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox   3352      tamitrofanov  88u    IPv4          340598  0t0      TCP client.tamitrof
anov.net:43278->146.75.117.91:https (ESTABLISHED)
firefox   3352      WaylandPr  tamitrofanov  62u    IPv4          341260  0t0      TCP client.tamitrof
anov.net:52192->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox   3352      WaylandPr  tamitrofanov  65u    IPv4          340595  0t0      TCP client.tamitrof
anov.net:52206->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox   3352      WaylandPr  tamitrofanov  88u    IPv4          340598  0t0      TCP client.tamitrof
anov.net:43278->146.75.117.91:https (ESTABLISHED)
firefox   3352      3374 pool-spaw tamitrofanov  62u    IPv4          341260  0t0      TCP client.tamitrof
anov.net:52192->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox   3352      3374 pool-spaw tamitrofanov  65u    IPv4          340595  0t0      TCP client.tamitrof
anov.net:52206->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox   3352      3374 pool-spaw tamitrofanov  88u    IPv4          340598  0t0      TCP client.tamitrof
anon.net:43278->146.75.117.91:https (ESTABLISHED)
```

Рисунок 3.21: проверием запущенные службы

Перенаправьте порт 80 на server.user.net на порт 8080 на локальной машине (вместо user используйте ваш логин) (рис. 3.22).

```
[tamitrofanov@client.tamitrofanov.net ~]$ ssh -fNL 8080:localhost:80 tamitrofanov@server.tamitrofanov.net
[tamitrofanov@client.tamitrofanov.net ~]$
```

Рисунок 3.22: перенаправление

Вновь на клиенте посмотрите, запущены ли какие-то службы с протоколом TCP (рис. 3.23).

Теперь у нас всё ёрремя шифрованный протокол на порту 80

```
[tmitrofanov@client.tmitrofanov.net ~]$ lsof | grep TCP
^C
[tmitrofanov@client.tmitrofanov.net ~]$ sudo lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
        Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
        Output information may be incomplete.

systemd      1          root    80u   IPv6          8506    0t0      TCP *:websm (LISTEN)
cupsd     1219          root    7u   IPv6          9902    0t0      TCP localhost:ipp (LISTEN)
cupsd     1219          root    8u   IPv4          9903    0t0      TCP localhost:ipp (LISTEN)
sshd      1223          root    7u   IPv4          10871    0t0      TCP *:ssh (LISTEN)
sshd      1223          root    8u   IPv6          10873    0t0      TCP *:ssh (LISTEN)
master    1354          root   13u   IPv4          10183    0t0      TCP localhost:smtp (LISTEN)
firefox   3352      tamitrofanov  65u   IPv4          340595   0t0      TCP client.tmitrof
anov.net:52206->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox   3352  3372 firefox      tamitrofanov  65u   IPv4          340595   0t0      TCP client.tmitrof
anov.net:52206->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox   3352  3373 WaylandPr  tamitrofanov  65u   IPv4          340595   0t0      TCP client.tmitrof
anov.net:52206->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox   3352  3374 pool-spaw  tamitrofanov  65u   IPv4          340595   0t0      TCP client.tmitrof
anov.net:52206->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox   3352  3375 gmain      tamitrofanov  65u   IPv4          340595   0t0      TCP client.tmitrof
anov.net:52206->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox   3352  3377 dconf\x20  tamitrofanov  65u   IPv4          340595   0t0      TCP client.tmitrof
anov.net:52206->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
```

Рисунок 3.23: проверием запущенные службы

На клиенте запустите браузер и в адресной строке введите localhost:8080. Убедитесь, что отобразится страница с приветствием «Welcome to the server.user.net server». (рис. 3.24).



Рисунок 3.24: проверка работы перенаправления

1. На клиенте откройте терминал под пользователем user (вместо user используйте ваш логин).
2. Посмотрите с клиента имя узла сервера: ssh user@server.user.net hostname
3. Посмотрите с клиента список файлов на сервере: ssh user@server.user.net ls -Al
4. Посмотрите с клиента почту на сервере: ssh user@server.user.net MAIL=~/Maildir/mail (рис. 3.25).

```
[tamitrofanov@client.tamitrofanov.net ~]$ ssh tamitrofanov@server.tamitrofanov.net hostname
server.tamitrofanov.net
[tamitrofanov@client.tamitrofanov.net ~]$ ssh tamitrofanov@server.tamitrofanov.net ls -Al
total 60
-rw-----. 1 tamitrofanov tamitrofanov 1525 Nov 15 17:10 .bash_history
-rw-r--r--. 1 tamitrofanov tamitrofanov 18 Oct 29 2024 .bash_logout
-rw-r--r--. 1 tamitrofanov tamitrofanov 144 Oct 29 2024 .bash_profile
-rw-r--r--. 1 tamitrofanov tamitrofanov 549 Sep 20 18:24 .bashrc
drwx-----. 12 tamitrofanov tamitrofanov 4096 Sep 27 18:10 .cache
drwx-----. 13 tamitrofanov tamitrofanov 4096 Sep 27 18:10 .config
drwxr-xr-x. 2 tamitrofanov tamitrofanov 6 Sep 27 13:25 Desktop
-rw-r--r--. 1 tamitrofanov tamitrofanov 574 Sep 27 13:29 DiG 9 18 33 www yandex.txt
drwxr-xr-x. 2 tamitrofanov tamitrofanov 78 Sep 27 15:22 Documents
drwxr-xr-x. 2 tamitrofanov tamitrofanov 6 Sep 27 13:25 Downloads
drwx-----. 4 tamitrofanov tamitrofanov 32 Sep 27 13:25 .local
drwx-----. 5 tamitrofanov tamitrofanov 4096 Nov 15 14:55 Maildir
drwxr-xr-x. 5 tamitrofanov tamitrofanov 54 Sep 27 13:33 .mozilla
drwxr-xr-x. 2 tamitrofanov tamitrofanov 6 Sep 27 13:25 Music
drwxr-xr-x. 2 tamitrofanov tamitrofanov 6 Sep 27 13:25 Pictures
drwxr-xr-x. 2 tamitrofanov tamitrofanov 6 Sep 27 13:25 Public
drwx-----. 2 tamitrofanov tamitrofanov 71 Nov 15 17:14 .ssh
drwxr-xr-x. 2 tamitrofanov tamitrofanov 6 Sep 27 13:25 Templates
-rw-r-----. 1 tamitrofanov tamitrofanov 6 Nov 15 14:25 .vboxclient-clipboard-tty2-control.pid
-rw-r-----. 1 tamitrofanov tamitrofanov 6 Nov 15 17:23 .vboxclient-clipboard-tty2-service.pid
-rw-r-----. 1 tamitrofanov tamitrofanov 6 Nov 15 14:25 .vboxclient-draganddrop-tty2-control.pid
-rw-r-----. 1 tamitrofanov tamitrofanov 6 Nov 15 14:25 .vboxclient-hostversion-tty2-control.pid
-rw-r-----. 1 tamitrofanov tamitrofanov 6 Nov 15 14:25 .vboxclient-seamless-tty2-control.pid
-rw-r-----. 1 tamitrofanov tamitrofanov 6 Nov 15 14:25 .vboxclient-vmsvga-session-tty2-control.pid
-rw-r-----. 1 tamitrofanov tamitrofanov 5 Nov 15 14:25 .vboxclient-vmsvga-session-tty2-service.pid
drwxr-xr-x. 2 tamitrofanov tamitrofanov 6 Sep 27 13:25 Videos
[+] [tamitrofanov@client.tamitrofanov.net ~]$ ssh tamitrofanov@server.tamitrofanov.net MAIL=-/Maildir/mail
s-nail version v14.9.24. Type '?' for help
/home/tamitrofanov/Maildir: 2 messages 1 new
  1 tamitrofanov@tamitro 2025-11-01 16:26 23/832 "test" *
  ▶N 2 tamitrofanov@client. 2025-11-15 14:55 21/901 "LMTP test" *
```

Рисунок 3.25: проверка домтупа к серверу без пароля

На сервере в конфигурационном файле /etc/ssh/sshd_config разрешите отображать на локальном клиентском компьютере графические интерфейсы X11(рис. 3.26).

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

Рисунок 3.26: изменения конф файла

Попробуйте с клиента удалённо подключиться к серверу и запустить графическое приложение, например firefox (вместо user используйте ваш логин) (рис. 3.27).

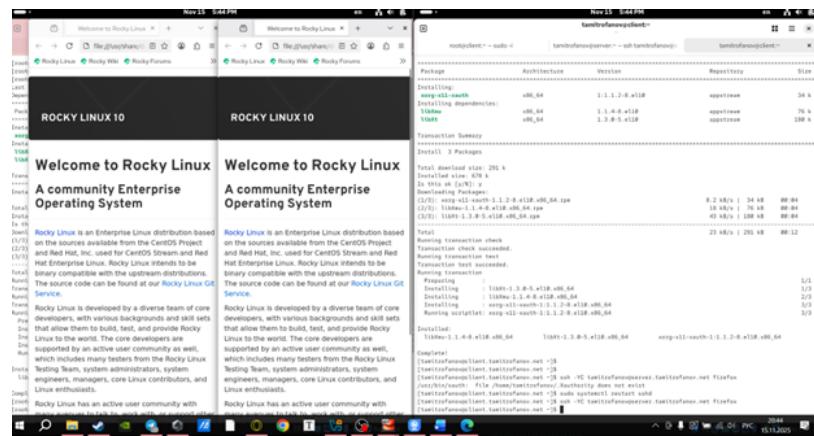


Рисунок 3.27: скрываем удалённо браузер на сервере

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 В каталоге /vagrant/provision/server создайте исполняемый файл ssh.sh (рис. 3.28).

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

Рисунок 3.28: сохранение файлов и их создание

ДОткрыв его на редактирование, пропишите в нём следующий скрипт (рис. 3.29).

```
GNU nano 8.1
#!/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 3.29: новый скрипт

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера (рис. 3.30).

```
111
112   server.vm.provision "server ssh",
113     type: "shell",
114     preserve_order: true,
115     path: "provision/server/ssh.sh"
116
117
```

Рисунок 3.30: дополнение скрипта на основной системе

4 Выводы

Сегодня я приобрёл практические навыки по настройке удалённого доступа к серверу с помощью SSH.

Список литературы