Лабораторная работа № 11. Настройка безопасного удалённого доступа по протоколу SSH

Данила Стариков
НПИбд-02-22

Российский университет дружбы народов имени Патриса Лумумбы

2024

Цель работы

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

Запрет удалённого доступа по SSH для пользователя root

```
[root@server.dastarikov.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.dastarikov.net ~]#
```

Рис.: Задание пароля для пользователя root.

Запрет удалённого доступа по SSH для пользователя root

Запретили пользователю root подключение к серверу через SSH:

```
PermitRootLogin no
```

```
[root@client.dastarikov.net ~]# ssh root@server.dastarikov.net
The authenticity of host 'server.dastarikov.net (192.168.1.1)' can't be established
.
ED25519 key fingerprint is SHA256:wPNWROdsR7WQ4jisOU7+9Wpt3obVIYN5cqrQNHuJ9gw.
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.dastarikov.net' (ED25519) to the list of known h
osts.
root@server.dastarikov.net's password:
Permission denied, please try again.
root@server.dastarikov.net's password:
Permission denied, please try again.
root@server.dastarikov.net's password:
root@server.dastarikov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-m
ic,password).
[root@client.dastarikov.net ~]#
```

Рис.: Подключение к серверу через SSH-соединение.

Ограничение списка пользователей для удалённого доступа по SSH

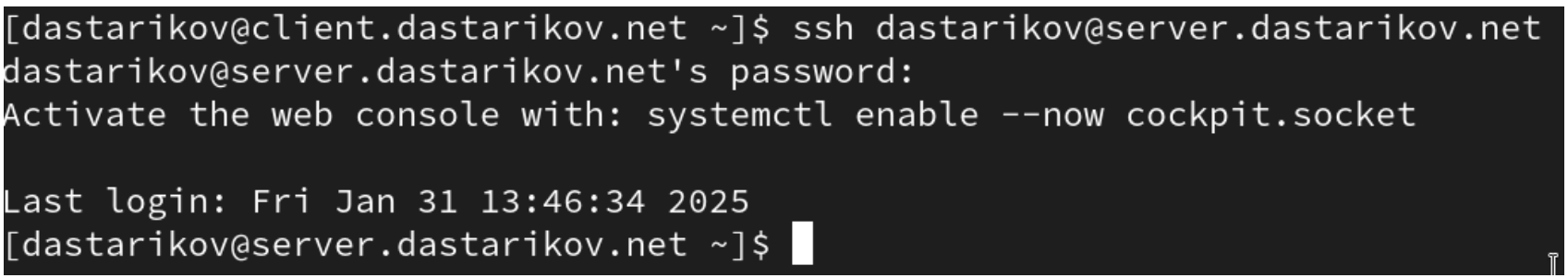

Рис.: Успешное подключение к серверу пользователем dastarikov.

Ограничение списка пользователей для удалённого доступа по SSH

Явно указали разрешенных к подключению пользователей:

```
AllowUsers vagrant
```

```
[dastarikov@client.dastarikov.net ~]$ ssh dastarikov@server.dastarikov.net
dastarikov@server.dastarikov.net's password:
Permission denied, please try again.
dastarikov@server.dastarikov.net's password:
```

Рис.: Отказ в доступе на сервер пользователю dastarikov.

Ограничение списка пользователей для удалённого доступа по SSH

Обновили список разрешенных пользователей:

```
AllowUsers vagrant dastarikov
```

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

Last failed login: Fri Jan 31 15:28:16 UTC 2025 from 192.168.1.30 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Fri Jan 31 15:26:27 2025 from 192.168.1.30
[dastarikov@server.dastarikov.net ~]$
```

Рис.: Восстановление доступа на сервер пользователю dastarikov.

Настройка дополнительных портов для удалённого доступа по SSH

В файле конфигурации `sshd_config` добавили строки:

```
Port 22
Port 2022
```

```
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-01-31 15:30:13 UTC; 10s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 48340 (sshd)
      Tasks: 1 (limit: 4555)
     Memory: 1.4M
        CPU: 17ms
     CGroup: /system.slice/sshd.service
             └─48340 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jan 31 15:30:13 server.dastarikov.net systemd[1]: Starting OpenSSH server daemon...
Jan 31 15:30:13 server.dastarikov.net sshd[48340]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
Jan 31 15:30:13 server.dastarikov.net sshd[48340]: error: Bind to port 2022 on :: failed: Permission denied.
Jan 31 15:30:13 server.dastarikov.net sshd[48340]: Server listening on 0.0.0.0 port 22.
Jan 31 15:30:13 server.dastarikov.net sshd[48340]: Server listening on :: port 22.
Jan 31 15:30:13 server.dastarikov.net systemd[1]: Started OpenSSH server daemon.
```

Рис.: Проверка расширенного статуса работы sshd.

Настройка дополнительных портов для удалённого доступа по SSH

```
[root@server.dastarikov.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.dastarikov.net ~]# firewall-cmd --add-port=2022/tcp
firewall-cmd --add-port=2022/tcp --permanent
success
success
```

Рис.: Настройка межсетевого экрана.

Настройка дополнительных портов для удалённого доступа по SSH

```
[root@server.dastarikov.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 Fri 2025-01-31 15:31:37 UTC; 1s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 48367 (sshd)
      Tasks: 1 (limit: 4555)
     Memory: 1.8M
        CPU: 23ms
     CGroup: /system.slice/sshd.service
             └─48367 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jan 31 15:31:37 server.dastarikov.net systemd[1]: Starting OpenSSH server daemon...
Jan 31 15:31:37 server.dastarikov.net sshd[48367]: Server listening on 0.0.0.0 port 2022.
Jan 31 15:31:37 server.dastarikov.net sshd[48367]: Server listening on :: port 2022.
Jan 31 15:31:37 server.dastarikov.net sshd[48367]: Server listening on 0.0.0.0 port 22.
Jan 31 15:31:37 server.dastarikov.net sshd[48367]: Server listening on :: port 22.
Jan 31 15:31:37 server.dastarikov.net systemd[1]: Started OpenSSH server daemon.
```

Рис.: Просмотр расширенного статуса sshd после настройки работы с портом 2022.

Настройка дополнительных портов для удалённого доступа по SSH

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

Last login: Fri Jan 31 15:28:51 2025 from 192.168.1.30
[dastarikov@server.dastarikov.net ~]$ sudo -i
[sudo] password for dastarikov:
[root@server.dastarikov.net ~]#
```

Рис.: Успешное подключение к серверу.

Настройка дополнительных портов для удалённого доступа по SSH

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

Last login: Fri Jan 31 15:32:01 2025 from 192.168.1.30
[dastarikov@server.dastarikov.net ~]$ sudo -i
[sudo] password for dastarikov:
[root@server.dastarikov.net ~]#
logout
[dastarikov@server.dastarikov.net ~]$
logout
Connection to server.dastarikov.net closed.
[dastarikov@client.dastarikov.net ~]$
```

Рис.: Успешное подключение к серверу по порту 2022.

Настройка удалённого доступа по SSH по ключу

```
[dastarikov@client.dastarikov.net ~]$ ssh-copy-id dastarikov@server.dastarikov.net
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are alre
ady installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to insta
ll the new keys
dastarikov@server.dastarikov.net's password:

Number of key(s) added: 1

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

Рис.: Копирование открытого ключа на сервер.

Настройка удалённого доступа по SSH по ключу

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

Last login: Fri Jan 31 15:32:40 2025 from 192.168.1.30
[dastarikov@server.dastarikov.net ~]$
```

Рис.: Успешное подключение к серверу с использованием SSH-ключа.

Организация туннелей SSH, перенаправление TCP-портов

```
[dastarikov@client.dastarikov.net ~]$ lsof | grep TCP
[dastarikov@client.dastarikov.net ~]$ ssh -fNL 8080:localhost:80 dastarikov@server.dastarikov.net
[dastarikov@client.dastarikov.net ~]$ lsof | grep TCP
ssh       50461                    dastarikov    3u     IPv4             143183       0t0        TCP
 client.dastarikov.net:32936->ns.dastarikov.net:ssh (ESTABLISHED)
ssh       50461                    dastarikov    4u     IPv6             143202       0t0        TCP
 localhost:webcache (LISTEN)
ssh       50461                    dastarikov    5u     IPv4             143203       0t0        TCP
 localhost:webcache (LISTEN)
[dastarikov@client.dastarikov.net ~]$
```

Рис.: Перенаправление TCP-портов.

Запуск консольных приложений через SSH

```
[dastarikov@client.dastarikov.net ~]$ ssh dastarikov@server.dastarikov.net hostname
server.dastarikov.net
[dastarikov@client.dastarikov.net ~]$ ssh dastarikov@server.dastarikov.net ls -Al
total 80
-rw-------.  1 dastarikov dastarikov 2257 Jan 31 15:33 .bash_history
-rw-r--r--.  1 dastarikov dastarikov   18 Apr 30  2024 .bash_logout
-rw-r--r--.  1 dastarikov dastarikov  141 Apr 30  2024 .bash_profile
-rw-r--r--.  1 dastarikov dastarikov  546 Oct  2 07:09 .bashrc
drwx------. 15 dastarikov dastarikov 4096 Dec  7 13:47 .cache
drwx------.  2 dastarikov dastarikov   64 Nov 30 20:48 common
drwx------. 13 dastarikov dastarikov 4096 Jan  7 20:05 .config
-rw-r--r--.  1 dastarikov dastarikov    0 Jan  7 20:06 dastarikov@server.txt
drwxr-xr-x.  2 dastarikov dastarikov    6 Oct 19 10:24 Desktop
drwxr-xr-x.  2 dastarikov dastarikov    6 Oct 19 10:24 Documents
drwxr-xr-x.  2 dastarikov dastarikov    6 Oct 19 10:24 Downloads
drwx------.  2 dastarikov dastarikov    6 Jan 31 12:56 .emacs.d
-rw-------.  1 dastarikov dastarikov   20 Jan  7 20:03 .lesshst
drwx------.  4 dastarikov dastarikov   32 Oct 19 10:24 .local
```

Рис.: Просмотр имени узла сервера и списка файлов через ssh.

Запуск консольных приложений через SSH

```
[dastarikov@client.dastarikov.net ~]$ ssh dastarikov@server.dastarikov.net MAIL=~/Maildir/ mail
s-nail version v14.9.22.  Type `?' for help
/home/dastarikov/Maildir: 3 messages
▸   1 Danila Starikov       2025-01-31 13:19   18/684   "test                "
    2 dastarikov@client.da  2025-01-31 13:45   21/855   "LMTP test           "
    3 Danila Starikov       2025-01-31 14:59   24/905   "Changed port        "

quit
Held 3 messages in /home/dastarikov/Maildir
```

Рис.: Просмотр почты на сервере через ssh.

Запуск графических приложений через SSH (X11Forwarding)

Разрешили отображать на локальном клиентском компьютере графические интерфейсы X11:

```
X11Forwarding yes
```

Запустили графическое приложение на сервере:

```
ssh -YC dastarikov@server.dastarikov.net firefox
```

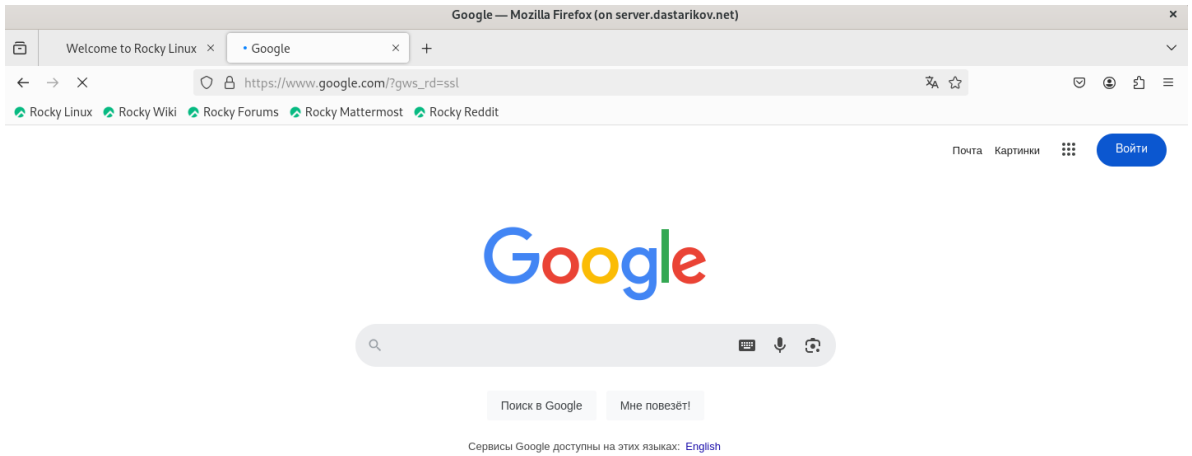

Рис.: Просмотр графического приложения (firefox) через ssh.

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/ssh/etc/ssh
cp -R /etc/ssh/sshd_config
 ↪  /vagrant/provision/server/ssh/etc/ssh/
cd /vagrant/provision/server
touch ssh.sh
chmod +x ssh.sh
```

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
#!/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
```

Внесение изменений в настройки внутреннего окружения виртуальной машины

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

Выводы

- В результате выполнения лабораторной работы приобрели практические навыки по настройке удалённого доступа к серверу с помощью SSH.