

Лаборатория работа 11

Настройка безопасного удалённого доступа по
протоколу SSH

ПОДГОТОВИЛА: КИМ РЕАЧНА
ГРУППА: НПИБД-02-20

Цель работы:

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

Задание:

- Запрет удалённого доступа по SSH для пользователя root
- Ограничение списка пользователей для удалённого доступа по SSH
- Настройка дополнительных портов для удалённого доступа по SSH
- Настройка удалённого доступа по SSH по ключу
- Организация туннелей SSH, перенаправление TCP-портов
- Запуск консольных приложений через SSH
- Запуск графических приложений через SSH (X11 Forwarding)
- Внесение изменений в настройки внутреннего окружения виртуальной машины

Запрет удалённого доступа по SSH для пользователя root

```
[kreachna@server.kreachna.net ~]$ sudo -i
[sudo] password for kreachna:
[root@server.kreachna.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.
```

```
[kreachna@client.kreachna.net ~]$ ssh root@server.kreachna.net
The authenticity of host 'server.kreachna.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:/2uvDHfM1QlaLTeqPJTnsRSAYzizIaAix/x7vXlm2m4.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [server.kreachna.net]:2022
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.kreachna.net' (ED25519) to the list of known hosts.
root@server.kreachna.net's password:
Permission denied, please try again.
root@server.kreachna.net's password:
Permission denied, please try again.
root@server.kreachna.net's password:
root@server.kreachna.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
```

Ограничение списка пользователей для удалённого доступа по SSH

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

Last login: Fri Dec 16 12:50:27 2022
```

```
# Example of overriding settings on a per-user basis
#Match User anoncvs
#<----->X11Forwarding no
#<----->AllowTcpForwarding no
#<----->PermitTTY no
#<----->ForceCommand cvs server
AllowUsers vagrant
```

```
#           AllowTcpForwarding no
#           PermitTTY no
#           ForceCommand cvs server
AllowUsers vagrant kreachna
```


Настройка дополнительных портов для удалённого доступа по SSH

```
[root@server.kreachna.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 Fri 2022-12-16 13:18:14 UTC; 16s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 7231 (sshd)
    Tasks: 1 (limit: 5748)
   Memory: 1.7M
      CPU: 12ms
   CGroup: /system.slice/sshd.service
           └─7231 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

```
Dec 16 13:18:14 server.kreachna.net systemd[1]: Starting OpenSSH server daemon...
```

```
Dec 16 13:18:14 server.kreachna.net sshd[7231]: ----- Bind to port 2022 -- A 0.0.0.0 failed. Operation denied
```

```
Dec 16 13:18:14 server.kreachna.net sshd[7231]: [root@server.kreachna.net ~]# systemctl status -l sshd
```

```
Dec 16 13:18:14 server.kreachna.net sshd[7231]: ● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-12-16 13:21:20 UTC; 20s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 7292 (sshd)
    Tasks: 1 (limit: 5748)
   Memory: 1.7M
      CPU: 15ms
   CGroup: /system.slice/sshd.service
           └─7292 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

```
Dec 16 13:21:19 server.kreachna.net systemd[1]: Starting OpenSSH server daemon...
```

```
Dec 16 13:21:20 server.kreachna.net sshd[7292]: Server listening on 0.0.0.0 port 2022.
```

```
Dec 16 13:21:20 server.kreachna.net sshd[7292]: Server listening on :: port 2022.
```

```
Dec 16 13:21:20 server.kreachna.net sshd[7292]: Server listening on 0.0.0.0 port 22.
```

```
Dec 16 13:21:20 server.kreachna.net sshd[7292]: Server listening on :: port 22.
```

```
Dec 16 13:21:20 server.kreachna.net systemd[1]: Started OpenSSH server daemon.
```

Настройка удалённого доступа по SSH по ключу

```
[kreachna@client.kreachna.net ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kreachna/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kreachna/.ssh/id_rsa
Your public key has been saved in /home/kreachna/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:AX8Q6cDj+GsCZeJKsU/0CMsoXHYPuILZPVqHuJnNpvI kreachna@client.kreachna.net
The key's randomart image is:
+---[RSA 3072]-----+
|      ... 00      |
|      . +0..      |
|.o o.+.+o .      |
|o++=000 .o       |
|+.X%++. S        |
|o*B0+..          |
|o.o+ .           |
|o ... o          |
| oE  o           |
+-----[SHA256]-----+
```

```
[kreachna@client.kreachna.net ~]$ ssh-copy-id kreachna@server.kreachna.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
kreachna@server.kreachna.net's password:
\
Number of key(s) added: 1

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

Организация туннелей SSH, перенаправление TCP-портов

```
[kreachna@client.kreachna.net ~]$ lsof | grep TCP
ssh          7308          kreachna    3u      IPv4        48582      0t0      TCP client.kreachna.
net:32966->server.kreachna.net:ssh (ESTABLISHED)
ssh          7308          kreachna    4u      IPv6        48602      0t0      TCP localhost:webcac
he (LISTEN)
ssh          7308          kreachna    5u      IPv4        48603      0t0      TCP localhost:webcac
he (LISTEN)
```

```
[kreachna@client.kreachna.net ~]$ lsof | grep TCP
```

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


Запуск консольных приложений через SSH

```
[kreachna@client.kreachna.net ~]$ ssh kreachna@server.kreachna.net ls -Al
```

```
total 48
```

```
-rw-----. 1 kreachna kreachna 310 Dec 16 13:35 .bash_history
-rw-r--r--. 1 kreachna kreachna 18 May 16 2022 .bash_logout
-rw-r--r--. 1 kreachna kreachna 141 May 16 2022 .bash_profile
-rw-r--r--. 1 kreachna kreachna 519 Nov 12 16:46 .bashrc
drwxr-xr-x. 9 kreachna kreachna 4096 Nov 12 16:47 .cache
drwx-----. 9 kreachna kreachna 4096 Dec 2 10:30 .config
drwxr-xr-x. 2 kreachna kreachna 6 Nov 12 16:46 Desktop
drwxr-xr-x. 2 kreachna kreachna 6 Nov 12 16:46 Documents
drwxr-xr-x. 2 kreachna kreachna 6 Nov 12 16:46 Downloads
drwx-----. 4 kreachna kreachna 32 Nov 12 16:46 .local
drwx-----. 5 kreachna kreachna 4096 Dec 10 13:53 Maildir
drwxr-xr-x. 4 kreachna kreachna 39 Nov 12 13:19 .mozilla
drwxr-xr-x. 2 kreachna kreachna 6 Nov 12 16:46 Music
drwxr-xr-x. 2 kreachna kreachna 4096 Nov 26 13:16 Pictures
drwxr-xr-x. 2 kreachna kreachna 6 Nov 12 16:46 Public
drwx-----. 2 kreachna kreachna 71 Dec 16 13:42 .ssh
drwxr-xr-x. 2 kreachna kreachna 6 Nov 12 16:46 Templates
-rw-r-----. 1 kreachna kreachna 5 Dec 16 12:50 .vboxclient-clipboard.pid
-rw-r-----. 1 kreachna kreachna 5 Dec 16 12:50 .vboxclient-display-svgx-x11.pid
-rw-r-----. 1 kreachna kreachna 5 Dec 16 12:50 .vboxclient-draganddrop.pid
-rw-r-----. 1 kreachna kreachna 5 Dec 16 12:50 .vboxclient-seamless.pid
drwxr-xr-x. 2 kreachna kreachna 6 Nov 12 16:46 Videos
-rw-----. 1 kreachna kreachna 0 Dec 16 13:42 .Xauthority
-rw-----. 1 kreachna kreachna 0 Dec 16 13:42 .Xresources
```

```
[kreachna@client.kreachna.net ~]$ ssh kreachna@server.kreachna.net MAIL=~/.Maildir/ mail
```

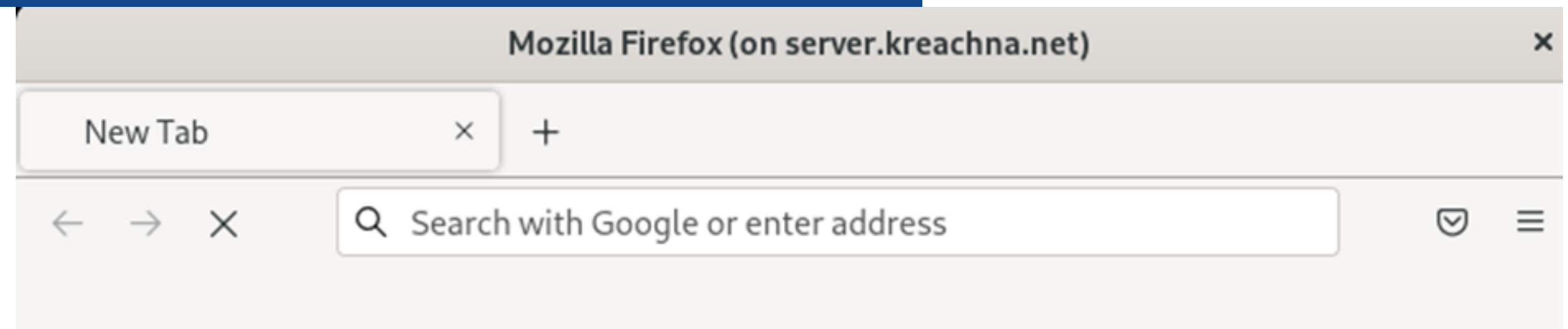
```
ss-nail version v14.9.22. Type '?' for help
```

```
/home/kreachna/Maildir: 3 messages
```

```
► 1 kreachna 2022-12-09 11:34 18/646 "example1"
2 kreachna@client.krea 2022-12-10 12:34 21/814 "LMTP test"
3 kreachna 2022-12-10 13:52 22/832 "Checking the correcti"
```


Запуск графических приложений через SSH (X11Forwarding)

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



Внесение изменений в настройки внутреннего окружения виртуальной машины

```
Vagrantfile x mail.sh x mail.sh x ssh.sh x
1  #!/bin/bash
2
3  echo "Provisioning script $0"
4
5  echo "Copy configuration files"
6  cp -R /vagrant/provision/server/ssh/etc/* /etc
7
8  restorecon -vR /etc
9
10 echo "Configure firewall"
11 firewall-cmd --add-port=2022/tcp
12 firewall-cmd --add-port=2022/tcp --permanent
13
14 echo "Tuning SELinux"
15 semanage port -a -t ssh_port_t -p tcp 2022
16
17 echo "Restart sshd service"
18 systemctl restart sshd
```

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

Вывод

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

Спасибо за внимание!