

**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

**ОТЧЕТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №11**

*дисциплина: администрирование локальных подсистем*

Студент: Саинт-Амур Измаэль

Группа: НПИбд-02-20

**МОСКВА**

2023 г.

## Постановка задачи

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

## Выполнение работы

### 11.4.1. Запрет удалённого доступа по SSH для пользователя root

1. На сервере задал пароль для пользователя root

```
[saismael@server.saismael.net ~]$ sudo -i
[sudo] password for saismael:
[root@server.saismael.net ~]# passwd root
Changing password for user root.
New password:
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

2. На сервере в дополнительном терминале запустил мониторинг системных событий

```
[saismael@server.saismael.net ~]$ sudo -i
[sudo] password for saismael:
[root@server.saismael.net ~]# journalctl -x -f
Dec 31 11:14:53 server.saismael.net sudo[6423]: pam_unix(sudo-i:session): session opened for user root(uid=0) by (uid=1001)
Dec 31 11:14:53 server.saismael.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 4756.
Dec 31 11:14:53 server.saismael.net systemd[1]: Started Hostname Service.
Subject: A start job for unit systemd-hostnamed.service has finished successfully
Defined-By: systemd
Support: https://access.redhat.com/support

A start job for unit systemd-hostnamed.service has finished successfully.

The job identifier is 4756.
Dec 31 11:15:23 server.saismael.net systemd[1]: systemd-hostnamed.service: Deactivated successfully.
```

3. С клиента попытался получить доступ к серверу посредством SSH-соединения через пользователя root:

```
[saismael@client.saismael.net ~]$ ssh saismael@server.saismael.net
The authenticity of host 'server.saismael.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.saismael.net' (ED25519) to the list of known hosts.
saismael@server.saismael.net's password:
Permission denied, please try again.
saismael@server.saismael.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Sat Dec 31 11:44:56 UTC 2022 from 192.168.1.30 on ssh:notty
There were 4 failed login attempts since the last successful login.
Last login: Sat Dec 31 10:24:29 2022 from 192.168.1.1
```

4. На сервере открыл файл `/etc/ssh/sshd_config` конфигурации `sshd` для редактирования и запретил вход на сервер пользователю `root`, установив:

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

#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
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn
```

5. После сохранения изменений в файле конфигурации перезапустил `sshd`

6. Повторил попытку получения доступа с клиента к серверу посредством SSH соединения через пользователя `root`:

```
[root@server.saismael.net ~]# systemctl restart sshd
[root@server.saismael.net ~]# ssh root@server.saismael.net
root@server.saismael.net's password:
Permission denied, please try again.
root@server.saismael.net's password:
Permission denied, please try again.
root@server.saismael.net's password:
root@server.saismael.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
```

### 11.4.2. Ограничение списка пользователей для удалённого доступа по SSH

1. С клиента попытался получить доступ к серверу посредством SSH-соединения через пользователя user

```
saismael@client.saismael.net ~]$ ssh saismael@server.saismael.net
Warning: The authenticity of host 'server.saismael.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:zqb0am9bCTBqb0qNzuP7z0xlq0qvGhkHxMkw2sQdblo.
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.saismael.net' (ED25519) to the list of known hosts
saismael@server.saismael.net's password:
Permission denied, please try again.
saismael@server.saismael.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Sat Dec 31 11:44:56 UTC 2022 from 192.168.1.30 on ssh:notty
There were 4 failed login attempts since the last successful login.
Last login: Sat Dec 31 10:24:29 2022 from 192.168.1.1
```

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

```
sshd config [-M--] 18 L:[ 30+14 44/131] *(1222/3671b) 0010
# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile<---->.ssh/authorized_keys

#AuthorizedPrincipalsFile none
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9
```

3. После сохранения изменений в файле конфигурации перезапустил sshd:

4. Повторил попытку получения доступа с клиента к серверу посредством



SSHсоединения через пользователя user:

```
[root@server.saismael.net ~]# systemctl restart sshd
[root@server.saismael.net ~]# ssh root@server.saismael.net
root@server.saismael.net's password:
Permission denied, please try again.
root@server.saismael.net's password:
Permission denied, please try again.
root@server.saismael.net's password:
root@server.saismael.net: Permission denied (publickey,gssapi-keyex,gssapi-with-
mic,password).
```

5. В файле /etc/ssh/sshd\_config конфигурации sshd внес следующее изменение:

```
sshd config [-M--] 2/ L:[ 34/10 44/131] + (1231/36800) 0010 0x00A
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
AllowUsers vagrant saismael
#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_
# but this is overridden so installations will only check .ssh/authorize
AuthorizedKeysFile<---->.ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
```

6. После сохранения изменений в файле конфигурации перезапустил sshd и вновь попытался получить доступ с клиента к серверу посредством SSH-соединения через пользователя user.

```
[root@server.saismael.net ~]# systemctl restart sshd
[root@server.saismael.net ~]# ssh root@server.saismael.net
root@server.saismael.net's password:
Permission denied, please try again.
root@server.saismael.net's password:
Permission denied, please try again.
root@server.saismael.net's password:
root@server.saismael.net: Permission denied (publickey,gssapi-keyex,gssapi-with-
mic,password).
```

### 11.4.3. Настройка дополнительных портов для удалённого доступа по SSH

1. На сервере в файле конфигурации sshd /etc/ssh/sshd\_config добавил:

```
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

# To modify the system-wide sshd configuration, create a *.conf file under
# /etc/ssh/sshd_config.d/ which will be automatically included below
Include /etc/ssh/sshd_config.d/*.conf

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22
Port 2022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

2. После сохранения изменений в файле конфигурации перезапустил sshd:

3. Посмотрел расширенный статус работы sshd:

```
[root@server.saismael.net ~]# systemctl restart sshd
[root@server.saismael.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor pres>
   Active: active (running) since Sat 2022-12-31 11:40:14 UTC; 16s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 6871 (sshd)
     Tasks: 1 (limit: 5789)
    Memory: 1.7M
       CPU: 82ms
    CGroup: /system.slice/sshd.service
            └─6871 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 31 11:40:14 server.saismael.net systemd[1]: Starting OpenSSH server daemon.>
Dec 31 11:40:14 server.saismael.net sshd[6871]: error: Bind to port 2022 on 0.0>
Dec 31 11:40:14 server.saismael.net sshd[6871]: error: Bind to port 2022 on ::>
Dec 31 11:40:14 server.saismael.net sshd[6871]: Server listening on 0.0.0.0 por>
Dec 31 11:40:14 server.saismael.net sshd[6871]: Server listening on :: port 22.
```

4. Исправил на сервере метки SELinux к порту 2022:

5. В настройках межсетевого экрана открыл порт 2022 протокола TCP:

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

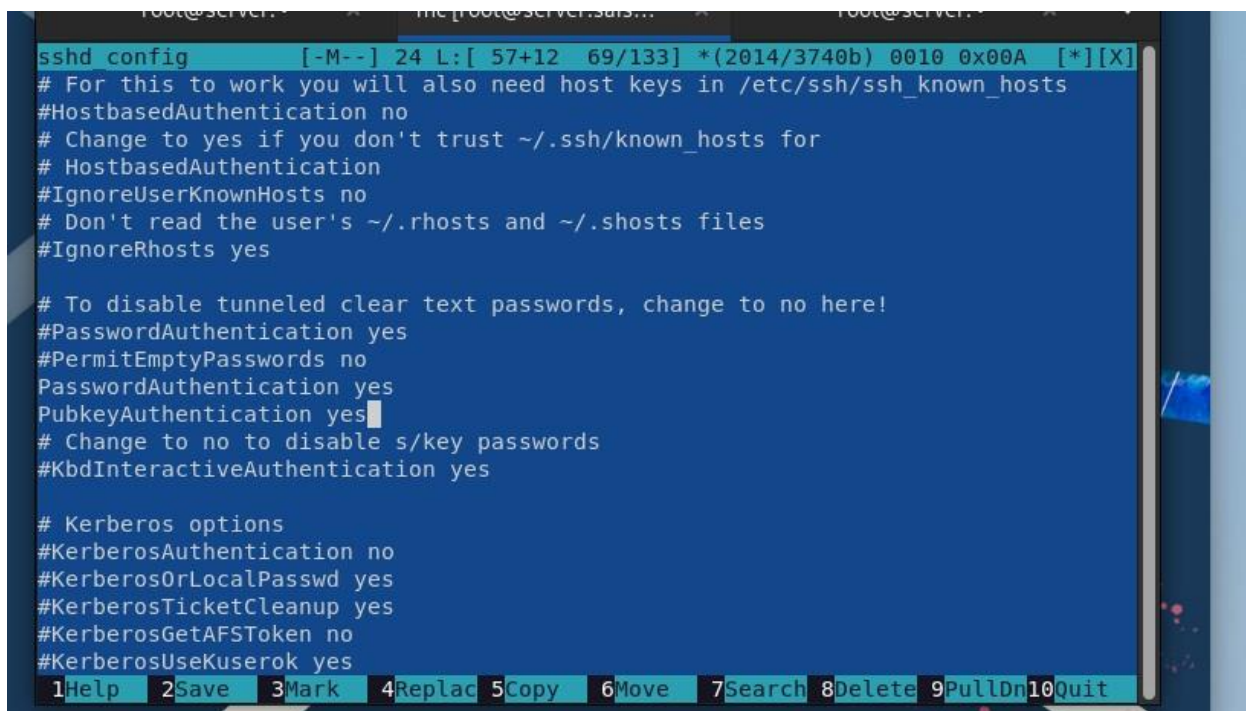
6. Вновь перезапустил sshd и посмотрел расширенный статус его работы.
7. С клиента попытался получить доступ к серверу посредством SSH-соединения через пользователя user
8. Повторил попытку получения доступа с клиента к серверу посредством SSHсоединения через пользователя user, указав порт 2022:

```
[saismael@client.saismael.net ~]$ ssh saismael@server.saismael.net
The authenticity of host 'server.saismael.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.saismael.net' (ED25519) to the list of known hosts.
saismael@server.saismael.net's password:
Permission denied, please try again.
saismael@server.saismael.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Sat Dec 31 11:44:56 UTC 2022 from 192.168.1.30 on ssh:notty
There were 4 failed login attempts since the last successful login.
Last login: Sat Dec 31 10:24:29 2022 from 192.168.1.1
[saismael@server.saismael.net ~]$ sudo -i
[sudo] password for saismael:
```

#### 11.4.4. Настройка удалённого доступа по SSH по ключу

1. На сервере в конфигурационном файле /etc/ssh/sshd\_config задал параметр, разрешающий аутентификацию по ключу:



```
sshd config [-M--] 24 L: [ 57+12 69/133] *(2014/3740b) 0010 0x00A [*][X]
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes
PubkeyAuthentication yes
# Change to no to disable s/key passwords
#KbdInteractiveAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn10Quit
```

2. После сохранения изменений в файле конфигурации перезапустил sshd.
3. На клиенте сформировал SSH-ключ



```
[root@server.saismael.net ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:ESsvE36hM+kgtcPeEfK6xjp/sRPYC3rvVpfl7kIs014 root@server.saismael.net
The key's randomart image is:
+---[RSA 3072]-----+
|
|      .
|    o + +
|  o = B o
| . =o@oS .
| oo**B= E
| oo.o@ + .
| o +.* o o
| .*o=o. +o
|
+-----[SHA256]-----+
[root@server.saismael.net ~]#
```

4. Закрытый ключ теперь будет записан в файл ~/.ssh/id\_rsa, а открытый ключ записывается в файл ~/.ssh/id\_rsa.pub.

5. Скопировал открытый ключ на сервер

```
[root@server.saismael.net ~]#
[root@server.saismael.net ~]# ssh-copy-id saismael@server.saismael.net
/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any tha
t are already installed
/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it i
s to install the new keys
saismael@server.saismael.net's password:

Number of key(s) added: 1

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

[root@server.saismael.net ~]# ssh saismael@server.saismael.net
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Dec 31 11:45:10 2022 from 192.168.1.30
[saismael@server.saismael.net ~]$
```

6. Попробовал получить доступ с клиента к серверу посредством SSH-соединения

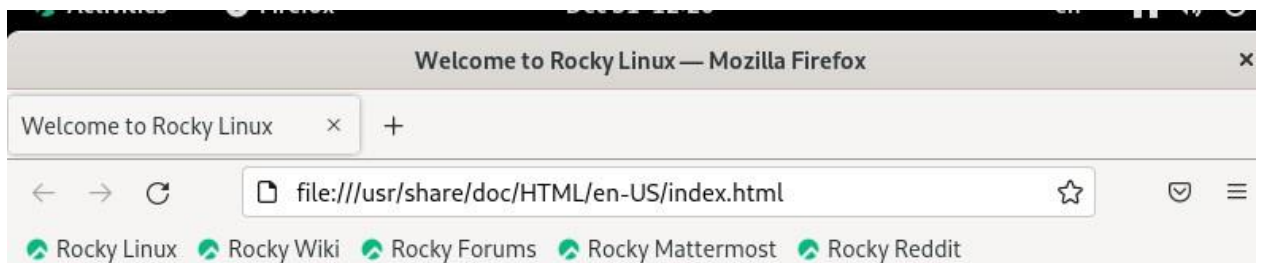
#### 11.4.5. Организация туннелей SSH, перенаправление TCP-портов

1. На клиенте посмотрите, запущены ли какие-то службы с протоколом TCP:
2. Перенаправил порт 80 на server.rmkipchakbaev.net на порт 8080 на локальной машине
3. Вновь на клиенте посмотрел, запущены ли какие-то службы с протоколом TCP:



```
[root@server.saismael.net ~]# 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    246u    IPv4        16950      0t
0      TCP *:sunrpc (LISTEN)
systemd      1      root    248u    IPv6        16966      0t
0      TCP *:sunrpc (LISTEN)
rpcbind     515      rpc       4u    IPv4        16950      0t
0      TCP *:sunrpc (LISTEN)
rpcbind     515      rpc       6u    IPv6        16966      0t
0      TCP *:sunrpc (LISTEN)
cupsd       789      root       6u    IPv6       20977      0t
0      TCP localhost:ipp (LISTEN)
cupsd       789      root       7u    IPv4       20978      0t
0      TCP localhost:ipp (LISTEN)
named       837      named     17u    IPv4       21245      0t
0      TCP localhost:domain (LISTEN)
named       837      named     21u    IPv6       21247      0t
0      TCP localhost:domain (LISTEN)
```

4. На клиенте запустил браузер и в адресной строке введите localhost:8080.



#### 11.4.6. Запуск консольных приложений через SSH

1. На клиенте открыл терминал под пользователем
2. Посмотрел с клиента имя узла сервера:
3. Посмотрел с клиента список файлов на сервере:

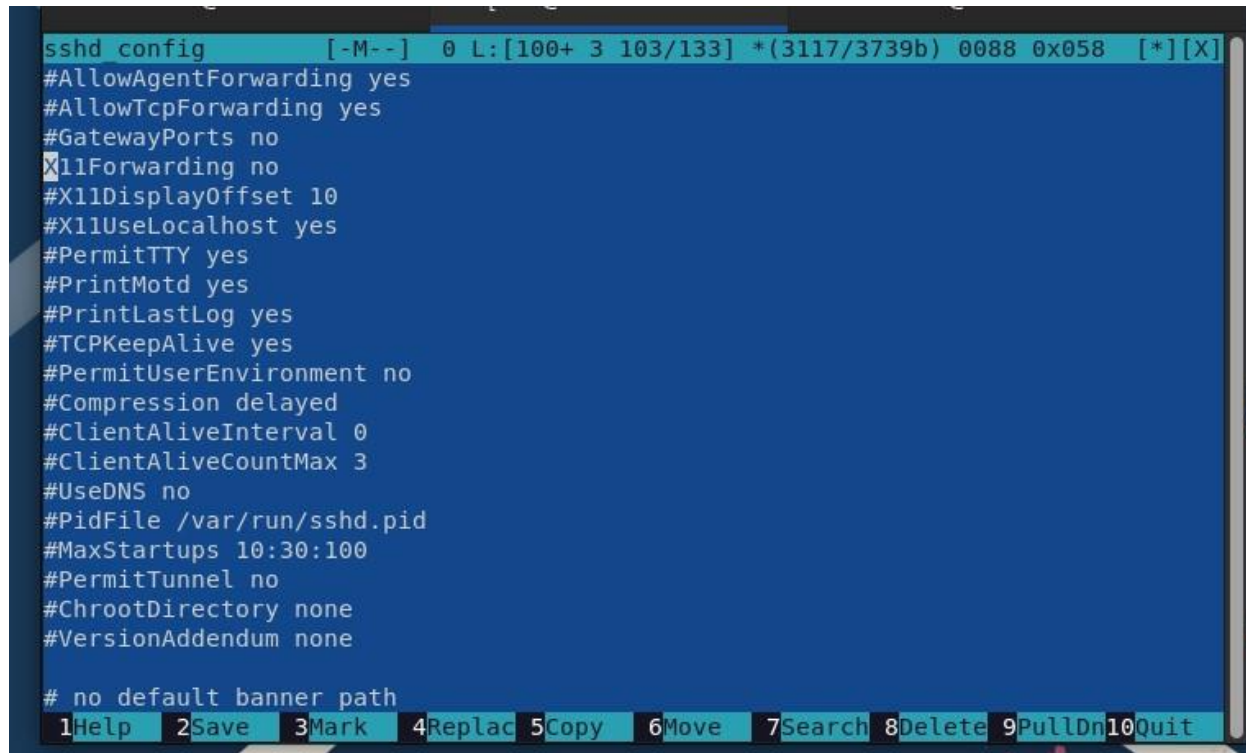
```
[root@server.saismael.net ~]# ssh saismael@server.saismael.net ls -Al
total 44
-rw-----. 1 saismael saismael 460 Dec 31 11:12 .bash_history
-rw-r--r--. 1 saismael saismael 18 May 16 2022 .bash_logout
-rw-r--r--. 1 saismael saismael 141 May 16 2022 .bash_profile
-rw-r--r--. 1 saismael saismael 546 Nov 26 14:23 .bashrc
drwxr-xr-x. 14 saismael saismael 4096 Dec 24 17:45 .cache
drwxr-xr-x. 2 root      root          6 Dec 31 08:04 common
drwx-----. 11 saismael saismael 4096 Dec 24 17:45 .config
drwxr-xr-x. 2 saismael saismael   6 Nov 26 14:30 Desktop
drwxr-xr-x. 2 saismael saismael   6 Nov 26 14:30 Documents
drwxr-xr-x. 2 saismael saismael   6 Nov 26 14:30 Downloads
drwx-----. 4 saismael saismael  32 Nov 26 14:31 .local
drwx-----. 5 saismael saismael 180 Dec  8 08:06 Maildir
drwxr-xr-x. 5 saismael saismael  54 Nov 27 14:14 .mozilla
drwxr-xr-x. 2 saismael saismael   6 Nov 26 14:30 Music
drwxr-xr-x. 2 saismael saismael   6 Nov 26 14:30 Pictures
drwxr-xr-x. 2 saismael saismael   6 Nov 26 14:30 Public
drwx-----. 2 saismael saismael  29 Dec 31 11:54 .ssh
drwxr-xr-x. 2 saismael saismael   6 Nov 26 14:30 Templates
-rw-r-----. 1 saismael saismael   5 Dec 31 08:07 .vboxclient-clipboard.pid
-rw-r-----. 1 saismael saismael   5 Dec 31 08:07 .vboxclient-display-svga-x11.
pid
```

4. Посмотрел с клиента почту на сервере:

```
[root@server.saismael.net ~]# ssh saismael@server.saismael.net hostname
server.saismael.net
[root@server.saismael.net ~]# S
```

#### 1.4.7. Запуск графических приложений через SSH (X11Forwarding)

1. На сервере в конфигурационном файле `/etc/ssh/sshd_config` разрешил отображать на локальном клиентском компьютере графические интерфейсы X11:



```
sshd_config [-M--] 0 L:[100+ 3 103/133] *(3117/3739b) 0088 0x058 [*][X]
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

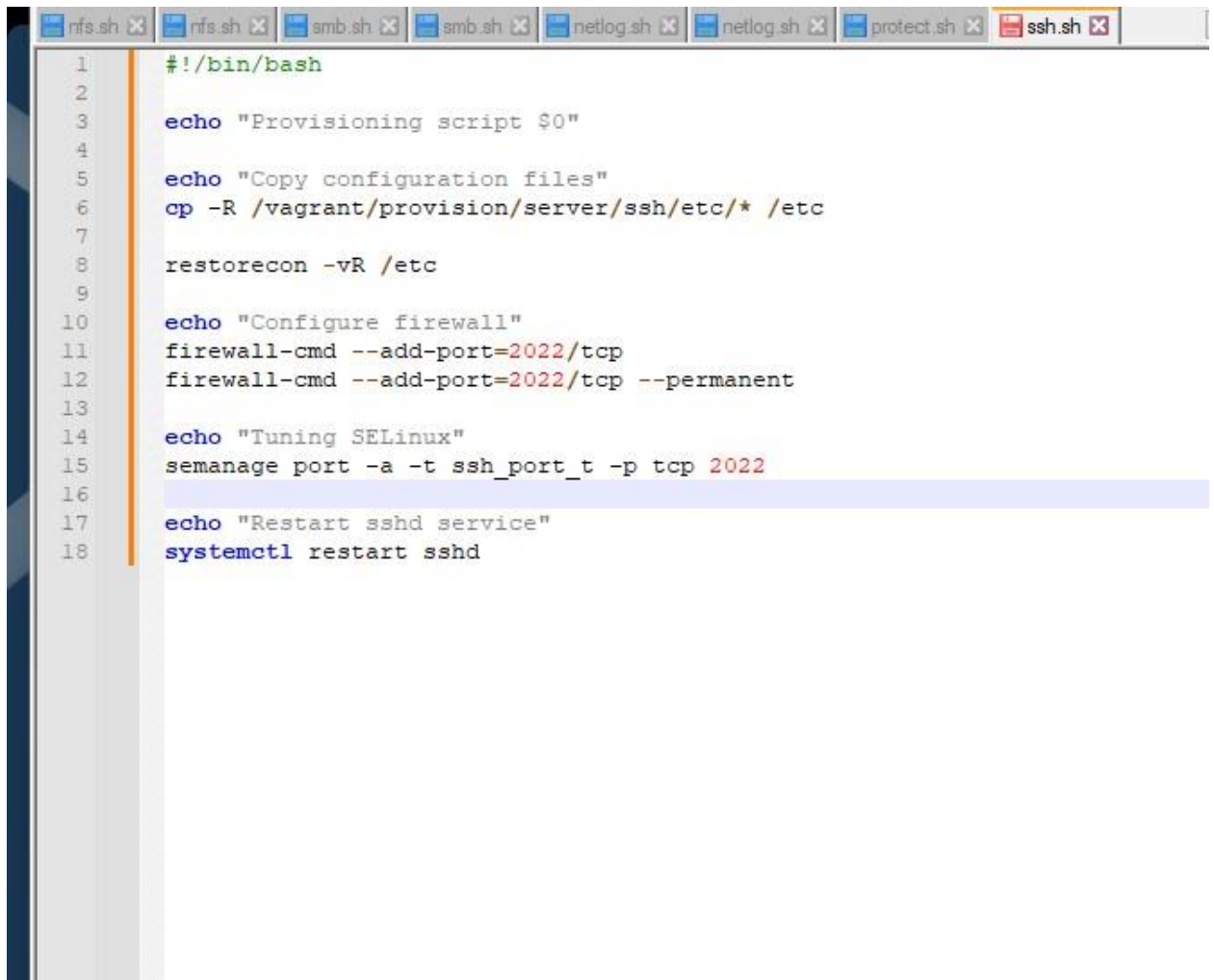
# no default banner path
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn10Quit
```

2. После сохранения изменения в конфигурационном файле перезапустил `sshd`.
3. Попробовал с клиента удалённо подключиться к серверу и запустить графическое приложение, например `firefox`

#### 11.4.8. Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине `server` перешел в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создал в нём каталог `ssh`, в который поместил в соответствующие подкаталоги конфигурационный файл `sshd_config`:
2. В каталоге `/vagrant/provision/server` создал исполняемый файл `ssh.sh`:  
Открыв его на редактирование, пропишите в нём следующий скрипт:

```
[root@server.saismael.net ~]# ssh -YC saismael@server.saismael.net firefox
/usr/bin/xauth: file /home/saismael/.Xauthority does not exist
Crash Annotation GraphicsCriticalError: |[0][GFX1-]: glxtest: X error, error_code=1, request_code=154, minor_code=1 (t=12.9792) [GFX1-]: glxtest: X error, error_code=1, request_code=154, minor_code=1
Crash Annotation GraphicsCriticalError: |[0][GFX1-]: glxtest: X error, error_code=1, request_code=154, minor_code=1 (t=12.9792) |[1][GFX1-]: glxtest: process failed (exited with status 1) (t=12.9818) [GFX1-]: glxtest: process failed (exited with status 1)
Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.mjs
Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.mjs
[root@server.saismael.net ~]#
[root@server.saismael.net ~]# cd /vagrant/provision/server
[root@server.saismael.net server]# mkdir -p /vagrant/provision/server/ssh/etc/ssh
[root@server.saismael.net server]# cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/
[root@server.saismael.net server]# cd /vagrant/provision/server
[root@server.saismael.net server]# touch ssh.sh
[root@server.saismael.net server]# chmod +x ssh.sh
[root@server.saismael.net server]#
```



```
rfs.sh x rfs.sh x smb.sh x smb.sh x netlog.sh x netlog.sh x protect.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
```

3. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавил в разделе конфигурации для сервера:



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

server.vm.provision "SMB server",
  type: "shell",
  preserve_order: true,
  path: "provision/server/smb.sh"

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

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

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

## Вывод

Приобрел практические навыки по настройке удалённого доступа к серверу с помощью SSH.

## Контрольные вопросы:

1. Вы хотите запретить удалённый доступ по SSH на сервер пользователю root и разрешить доступ пользователю alice. Как это сделать?

- Для запрета удаленного доступа пользователю root требуется в конфигурационном файле sshd\_config выставить значение поля «PermitRootLogin» в «no», для того, чтобы разрешить доступ пользователю alice, в том же файле нужно добавить данного пользователя в поле AllowUsers через запятую.

2. Как настроить удалённый доступ по SSH через несколько портов? Для чего это может потребоваться?

- В конфигурационном файле sshd\_config прописываем Port <номер порта> на все порты, которые потребуются. Это 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?*

- Все настройки SSH находятся в файле `sshd_config`, поэтому при подключении используются параметры, описанные в нем, такие как номер порта, версия протокола, названия файлов ключей и их расположение, и т.д.

4. *Как настроить локальную переадресацию с локального порта 5555 на порт 80 сервера `server2.example.com`?*

- `ssh -fNL 8080:localhost:80 server2.example.com`

5. *Как настроить SELinux, чтобы позволить SSH связываться с портом 2022?*

- Следующей командой: `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?*

- Следующей командой: `firewall-cmd --add-port=2022/tcp`