

Лабораторная работа 11

Ярметов Камран

17 февраля, 2023., Москва, Россия

Российский Университет Дружбы Народов

Цель лабораторной работы

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

Выполнение лабораторной работы

Тестирование SSH-авторизации

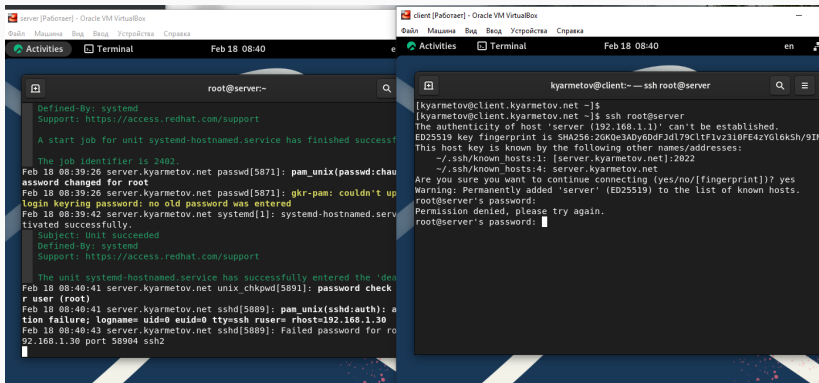
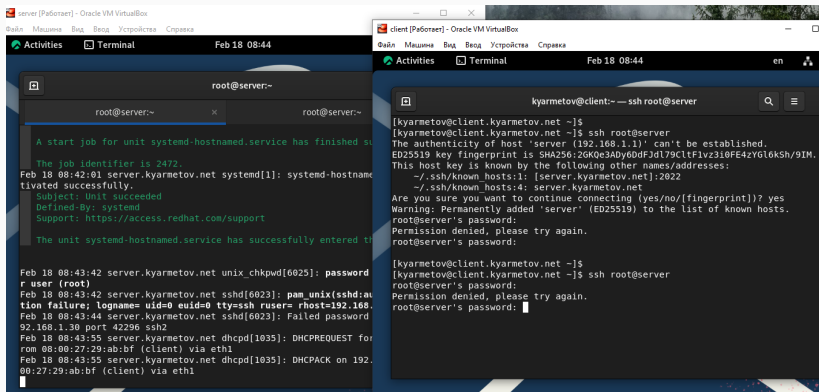


Figure 1: подключение суперпользователя

Тестирование SSH-авторизации

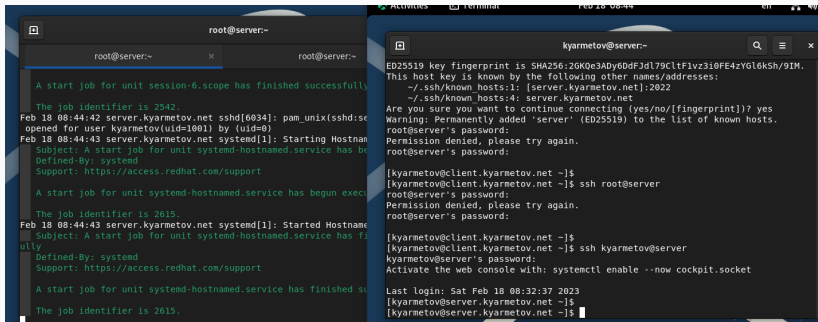


The image shows two terminal windows from Oracle VM VirtualBox. The left window, titled 'server [Работает] - Oracle VM VirtualBox', shows the server's perspective. It displays system logs for the systemd-hostnamed service starting at 08:42:01 and the sshd service starting at 08:43:44. The sshd log shows a failed password attempt from 192.168.1.30. The right window, titled 'client [Работает] - Oracle VM VirtualBox', shows the client's perspective. It shows the user 'kyarmetov' attempting to SSH into the server as 'root'. The terminal output shows the host key fingerprint, a warning about the host key, and two failed password attempts, both resulting in 'Permission denied, please try again.'

```
root@server:~  
root@server:~  
A start job for unit systemd-hostnamed.service has finished su  
The job identifier is 2472.  
Feb 18 08:42:01 server.kyarmetov.net systemd[1]: systemd-hostname  
tivated successfully.  
Subject: Unit succeeded  
Defined-By: systemd  
Support: https://access.redhat.com/support  
The unit systemd-hostnamed.service has successfully entered th  
  
Feb 18 08:43:42 server.kyarmetov.net unix_chkpwd[6025]: password  
r user (root)  
Feb 18 08:43:42 server.kyarmetov.net sshd[6023]: pam_unix(sshd:au  
tion failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.  
Feb 18 08:43:44 server.kyarmetov.net sshd[6023]: Failed password  
92.168.1.30 port 42296 ssh2  
Feb 18 08:43:55 server.kyarmetov.net dhcpd[1035]: DHCPREQUEST for  
rom 08:00:27:29:ab:bf (client) via eth1  
Feb 18 08:43:55 server.kyarmetov.net dhcpd[1035]: DHCPACK on 192.  
00:27:29:ab:bf (client) via eth1  
  
kyarmetov@client:~$ ssh root@server  
[kyarmetov@client.kyarmetov.net ~]$ ssh root@server  
The authenticity of host 'server (192.168.1.1)' can't be established.  
ED25519 key fingerprint is SHA256:2GKQe3ADy60dFjd179CltFlvz3i0FE4zYGl6kSh/9IM.  
This host key is known by the following other names/addresses:  
~/ssh/known_hosts:1: [server.kyarmetov.net]:2022  
~/ssh/known_hosts:4: server.kyarmetov.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:  
  
[kyarmetov@client.kyarmetov.net ~]$  
[kyarmetov@client.kyarmetov.net ~]$ ssh root@server  
root@server's password:  
Permission denied, please try again.  
root@server's password:
```

Figure 2: подключение суперпользователя

Тестирование SSH-авторизации



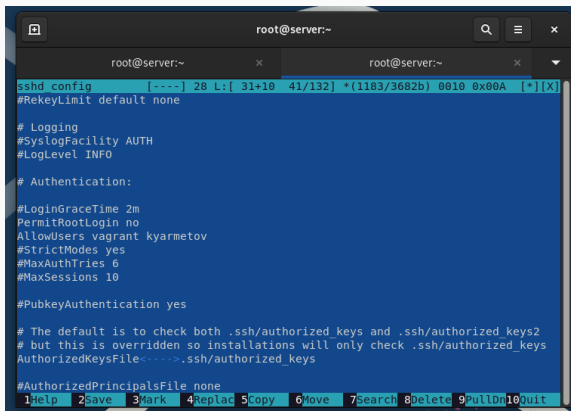
The image shows two terminal windows side-by-side. The left window is titled 'root@server:~' and shows system messages from the systemd journal, including a successful login for 'kyarmetov' and the start of the 'systemd-hostnamed.service'. The right window is titled 'kyarmetov@server:~' and shows the user's perspective of logging in via SSH, including the host key fingerprint, a confirmation to add the host to the known hosts list, and the user's password being rejected twice.

```
root@server:~  
root@server:~  
A start job for unit session-6.scope has finished successfully.  
The job identifier is 2542.  
Feb 18 08:44:42 server.kyarmetov.net sshd[6034]: pam_unix(sshd:session) opened for user kyarmetov(uid=1001) by (uid=0)  
Feb 18 08:44:43 server.kyarmetov.net systemd[1]: Starting Hostnamed.  
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 2615.  
Feb 18 08:44:43 server.kyarmetov.net systemd[1]: Started Hostnamed.  
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 2615.
```

```
kyarmetov@server:~  
ED25519 key fingerprint is SHA256:2GKQe3ADy6DdFJdL79CltFlvz3i0FE4zYGL6kSh/9IM.  
This host key is known by the following other names/addresses:  
~/.ssh/known_hosts:1: [server.kyarmetov.net]:2022  
~/.ssh/known_hosts:4: server.kyarmetov.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:  
[kyarmetov@client.kyarmetov.net ~]$  
[kyarmetov@client.kyarmetov.net ~]$ ssh root@server  
root@server's password:  
Permission denied, please try again.  
root@server's password:  
[kyarmetov@client.kyarmetov.net ~]$  
[kyarmetov@client.kyarmetov.net ~]$ ssh kyarmetov@server  
kyarmetov@server's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Sat Feb 18 08:32:37 2023  
[kyarmetov@server.kyarmetov.net ~]$  
[kyarmetov@server.kyarmetov.net ~]$
```

Figure 3: подключение пользователя

Конфигурация SSH



The image shows a terminal window titled 'root@server:~'. The terminal displays the contents of the `/etc/ssh/sshd_config` file. The text is as follows:

```
sshd config [---] 28 L:[ 31+10 41/132] *(1183/3682b) 0010 0x00A [*][X]
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

#PubkeyAuthentication yes

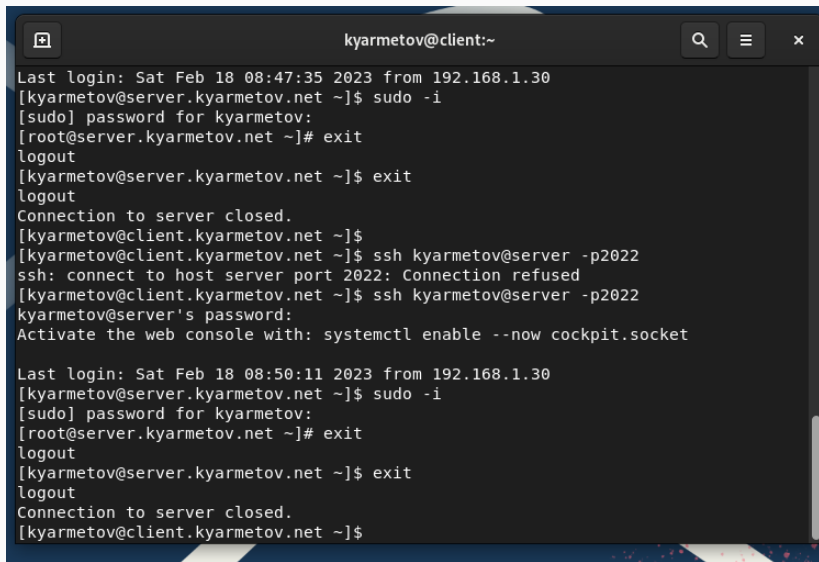
# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile----->.ssh/authorized_keys

#AuthorizedPrincipalsFile none
```

At the bottom of the terminal, there is a status bar with the following text: 1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit.

Figure 4: файл /etc/ssh/sshd_config

Настройка дополнительных портов

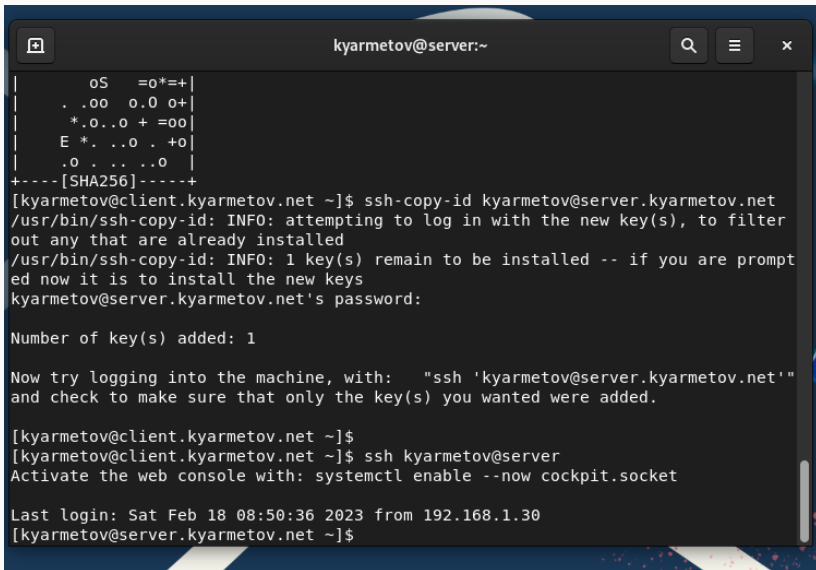
A terminal window titled 'kyarmetov@client:~' with search, menu, and close icons in the title bar. The terminal shows two identical sequences of commands and output. The first sequence shows a successful login to 'server.kyarmetov.net' as 'root' via 'sudo -i', followed by 'exit' and 'logout'. The second sequence shows an attempt to connect to the same host on port 2022, which is refused. The user then enters the password and the prompt changes to root. The terminal ends with the command 'systemctl enable --now cockpit.socket'.

```
kyarmetov@client:~
Last login: Sat Feb 18 08:47:35 2023 from 192.168.1.30
[kyarmetov@server.kyarmetov.net ~]$ sudo -i
[sudo] password for kyarmetov:
[root@server.kyarmetov.net ~]# exit
logout
[kyarmetov@server.kyarmetov.net ~]$ exit
logout
Connection to server closed.
[kyarmetov@client.kyarmetov.net ~]$
[kyarmetov@client.kyarmetov.net ~]$ ssh kyarmetov@server -p2022
ssh: connect to host server port 2022: Connection refused
[kyarmetov@client.kyarmetov.net ~]$ ssh kyarmetov@server -p2022
kyarmetov@server's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Feb 18 08:50:11 2023 from 192.168.1.30
[kyarmetov@server.kyarmetov.net ~]$ sudo -i
[sudo] password for kyarmetov:
[root@server.kyarmetov.net ~]# exit
logout
[kyarmetov@server.kyarmetov.net ~]$ exit
logout
Connection to server closed.
[kyarmetov@client.kyarmetov.net ~]$
```

Figure 5: подключение на 2022 порт

Настройка удалённого доступа по SSH по ключу

A terminal window titled 'kyarmetov@server:~' with standard macOS window controls. The terminal shows the output of 'ssh-copy-id' and the execution of 'ssh' to connect to a remote server. The output includes a visual representation of the key being added, status messages from ssh-copy-id, a password prompt, and the final successful connection to the remote host.

```
|      oS    =o*=+|
|      . .oo  o.o o+|
|      *.o..o + =oo|
|      E *.  ..o . +o|
|      .o . . . .o |
+-----[SHA256]-----+
[kyarmetov@client.kyarmetov.net ~]$ ssh-copy-id kyarmetov@server.kyarmetov.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 prompt
ed now it is to install the new keys
kyarmetov@server.kyarmetov.net's password:
Number of key(s) added: 1

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

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

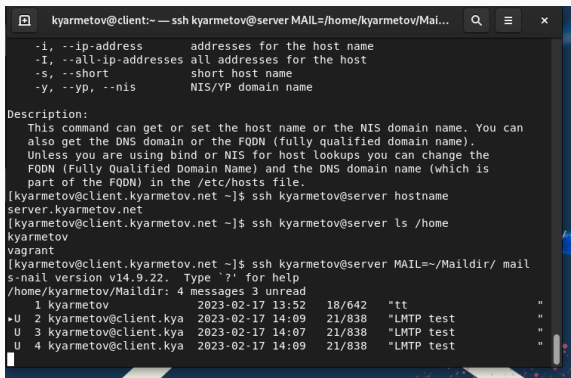
Last login: Sat Feb 18 08:50:36 2023 from 192.168.1.30
[kyarmetov@server.kyarmetov.net ~]$
```

Перенаправление портов

```
kyarmetov@client.kyarmetov.net ~]$  
kyarmetov@client.kyarmetov.net ~]$  
kyarmetov@client.kyarmetov.net ~]$ lsof | grep TCP  
kyarmetov@client.kyarmetov.net ~]$ ssh -fNL 8080:localhost:80 kyarmetov@server  
kyarmetov@client.kyarmetov.net ~]$ lsof | grep TCP  
ssh        6496      kyarmetov    3u      IPv4        40736  
0t0        TCP      client.kyarmetov.net:50080->www.kyarmetov.net:ssh (ESTABLISH  
ED)  
ssh        6496      kyarmetov    4u      IPv6        54124  
0t0        TCP      localhost:webcache (LISTEN)  
ssh        6496      kyarmetov    5u      IPv4        54125  
0t0        TCP      localhost:webcache (LISTEN)  
kyarmetov@client.kyarmetov.net ~]$
```

Figure 7: перенаправлен порт 8080

Удаленное выполнение команд



```
kyarmetov@client:~ — ssh kyarmetov@server MAIL=/home/kyarmetov/Mail...  
-i, --ip-address      addresses for the host name  
-I, --all-ip-addresses all addresses for the host  
-s, --short           short host name  
-y, --yp, --nis       NIS/YP domain name  
  
Description:  
  This command can get or set the host name or the NIS domain name. You can  
  also get the DNS domain or the FQDN (fully qualified domain name).  
  Unless you are using bind or NIS for host lookups you can change the  
  FQDN (Fully Qualified Domain Name) and the DNS domain name (which is  
  part of the FQDN) in the /etc/hosts file.  
[kyarmetov@client.kyarmetov.net ~]$ ssh kyarmetov@server hostname  
server.kyarmetov.net  
[kyarmetov@client.kyarmetov.net ~]$ ssh kyarmetov@server ls /home  
kyarmetov  
vagrant  
[kyarmetov@client.kyarmetov.net ~]$ ssh kyarmetov@server MAIL=~/.Maildir/ mail  
s-nail version v14.9.22. Type '?' for help  
/home/kyarmetov/Maildir: 4 messages 3 unread  
 1 kyarmetov          2023-02-17 13:52    18/642    "tt" "  
+U 2 kyarmetov@client.kya 2023-02-17 14:09    21/838    "LMTP test" "  
U 3 kyarmetov@client.kya 2023-02-17 14:07    21/838    "LMTP test" "  
U 4 kyarmetov@client.kya 2023-02-17 14:09    21/838    "LMTP test" "
```

Figure 8: выполнение команд hostname и ls

Удаленный запуск приложения

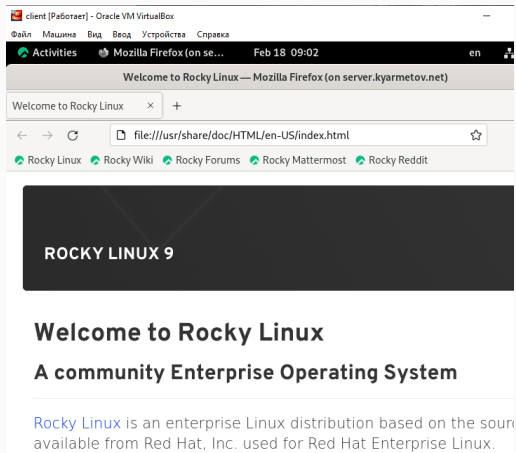


Figure 9: запуск firefox по ssh

Приобретены практические навыки по работе с ssh и перенаправлением портов.