

Презентация по лабораторной работе №11

Настройка безопасного удалённого доступа по протоколу SSH

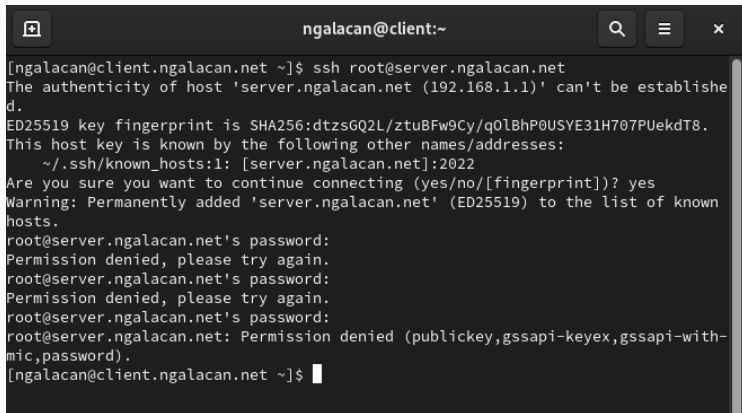
Галацан Николай

Российский университет дружбы народов, Москва, Россия

- Галацан Николай
- 1032225763
- уч. группа: НПИбд-01-22
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов

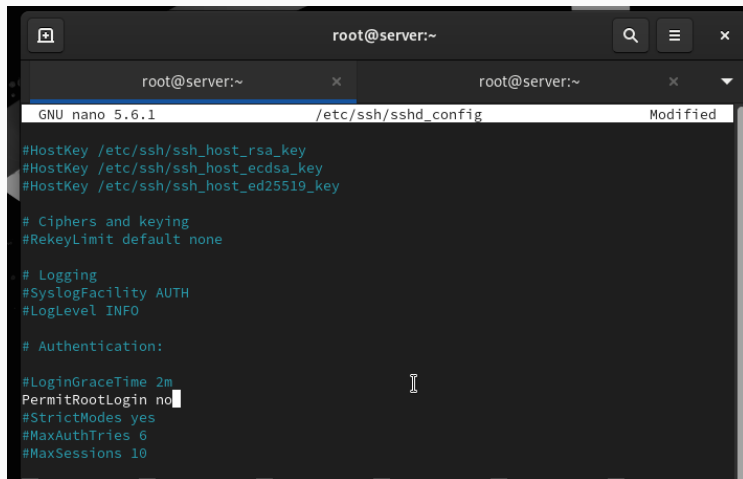
Приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

Запрет удалённого доступа по SSH для пользователя root



```
ngalacan@client:~  
[ngalacan@client.ngalacan.net ~]$ ssh root@server.ngalacan.net  
The authenticity of host 'server.ngalacan.net (192.168.1.1)' can't be established.  
ED25519 key fingerprint is SHA256:dtzsGQ2L/ztuBFw9Cy/q0lBhP0USYE31H707PUekdT8.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:1: [server.ngalacan.net]:2022  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'server.ngalacan.net' (ED25519) to the list of known hosts.  
root@server.ngalacan.net's password:  
Permission denied, please try again.  
root@server.ngalacan.net's password:  
Permission denied, please try again.  
root@server.ngalacan.net's password:  
root@server.ngalacan.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).  
[ngalacan@client.ngalacan.net ~]$
```

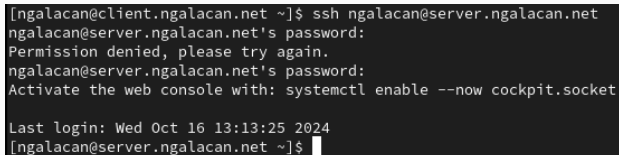
Рис. 1: Попытка получения доступа к серверу через root: отказ



```
root@server:~  
GNU nano 5.6.1 /etc/ssh/sshd_config Modified  
  
#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  
#MaxAuthTries 6  
#MaxSessions 10
```

Рис. 2: Запрет входа на сервер пользователю root

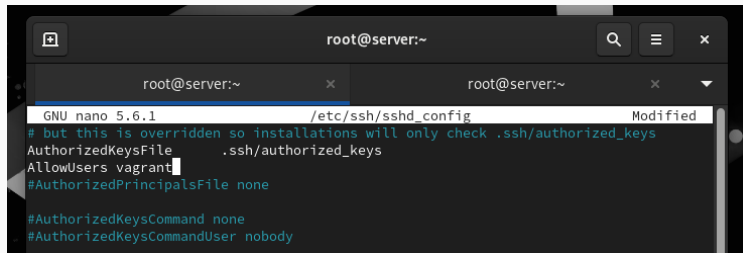
Ограничение списка пользователей для удалённого доступа по SSH



```
[ngalacan@client.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net
ngalacan@server.ngalacan.net's password:
Permission denied, please try again.
ngalacan@server.ngalacan.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Wed Oct 16 13:13:25 2024
[ngalacan@server.ngalacan.net ~]$
```

Рис. 3: Попытка получения доступа к серверу через ngalacan: доступ получен

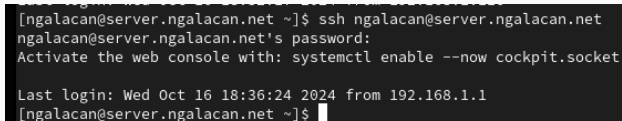


```
root@server:~  
GNU nano 5.6.1 /etc/ssh/sshd_config Modified  
# but this is overridden so installations will only check .ssh/authorized_keys  
AuthorizedKeysFile .ssh/authorized_keys  
AllowUsers vagrant  
#AuthorizedPrincipalsFile none  
  
#AuthorizedKeysCommand none  
#AuthorizedKeysCommandUser nobody
```

Рис. 4: Добавление строки в конфигурационный файл

```
Last login: wed Oct 16 13:13:23 2024
[ngalacan@server.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net
The authenticity of host 'server.ngalacan.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:dtzsGQ2L/ztuBFw9Cy/q0lBhP0USYE31H707PUekdT8.
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.ngalacan.net' (ED25519) to the list of known hosts.
ngalacan@server.ngalacan.net's password:
Permission denied, please try again.
ngalacan@server.ngalacan.net's password:
Permission denied, please try again.
ngalacan@server.ngalacan.net's password:
ngalacan@server.ngalacan.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[ngalacan@server.ngalacan.net ~]$
```

Рис. 5: Попытка получения доступа к серверу через ngalacan: отказ

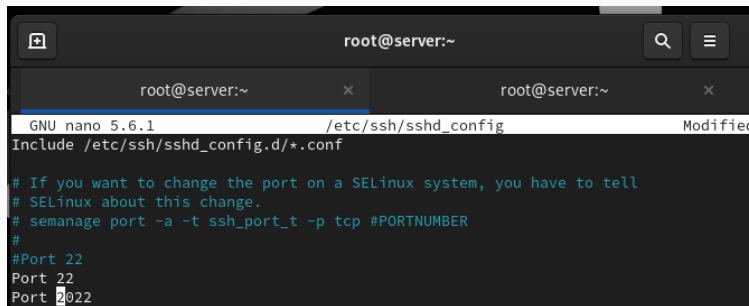


```
[ngalacan@server.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net
ngalacan@server.ngalacan.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Wed Oct 16 18:36:24 2024 from 192.168.1.1
[ngalacan@server.ngalacan.net ~]$
```

Рис. 6: Попытка получения доступа к серверу через ngalacan: доступ получен

Настройка дополнительных портов для удалённого доступа по SSH



```
root@server:~  
GNU nano 5.6.1 /etc/ssh/sshd_config Modified  
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 22  
Port 2022
```

Рис. 7: Добавление портов

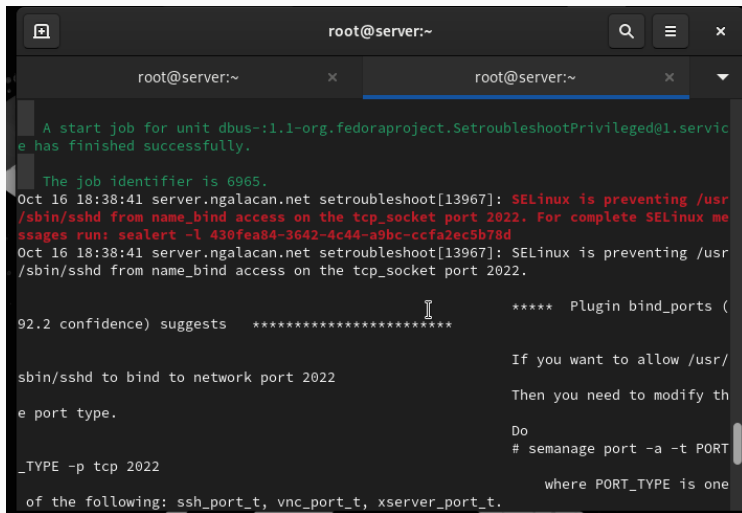
Выполнение лабораторной работы

```
[root@server.ngalacan.net ~]# nano /etc/ssh/sshd_config
[root@server.ngalacan.net ~]# systemctl restart sshd
[root@server.ngalacan.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Wed 2024-10-16 18:38:37 UTC; 11s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 13965 (sshd)
     Tasks: 1 (limit: 4557)
    Memory: 1.4M
         CPU: 13ms
    CGroup: /system.slice/ssh.service
            └─13965 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 16 18:38:36 server.ngalacan.net systemd[1]: Starting OpenSSH server daemon...
Oct 16 18:38:37 server.ngalacan.net sshd[13965]: error: Bind to port 2022 on 0.0.0.0>
Oct 16 18:38:37 server.ngalacan.net sshd[13965]: error: Bind to port 2022 on :: fail>
Oct 16 18:38:37 server.ngalacan.net sshd[13965]: Server listening on 0.0.0.0 port 22.
Oct 16 18:38:37 server.ngalacan.net sshd[13965]: Server listening on :: port 22.
Oct 16 18:38:37 server.ngalacan.net systemd[1]: Started OpenSSH server daemon.
lines 1-18/18 (END)
```

Рис. 8: Статус sshd: отказ в работе через порт 2022

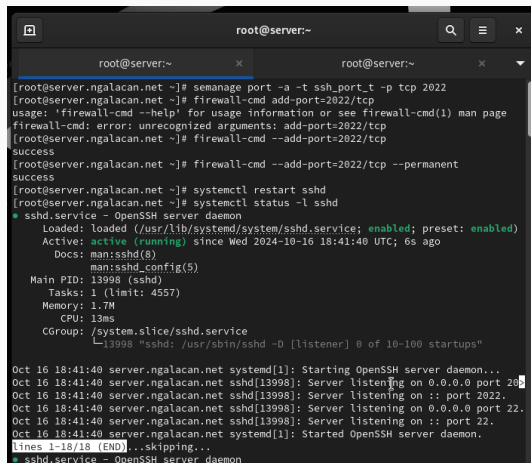
Выполнение лабораторной работы



```
root@server:~  
A start job for unit dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@1.service has finished successfully.  
The job identifier is 6965.  
Oct 16 18:38:41 server.ngalacan.net setroubleshoot[13967]: SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2022. For complete SELinux messages run: sealert -l 430fea84-3642-4c44-a9bc-ccfa2ec5b78d  
Oct 16 18:38:41 server.ngalacan.net setroubleshoot[13967]: SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2022.  
  
92.2 confidence) suggests *****  
  
sbin/sshd to bind to network port 2022  
  
e port type.  
  
Do  
# semanage port -a -t PORT  
_TYPE -p tcp 2022  
where PORT_TYPE is one  
of the following: ssh_port_t, vnc_port_t, xserver_port_t.
```

Рис. 9: Ошибки в журнале системных событий

Выполнение лабораторной работы



```
root@server:~
[root@server.ngalacan.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.ngalacan.net ~]# firewall-cmd add-port=2022/tcp
usage: 'firewall-cmd --help' for usage information or see firewall-cmd(1) man page
firewall-cmd: error: unrecognized arguments: add-port=2022/tcp
[root@server.ngalacan.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.ngalacan.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.ngalacan.net ~]# systemctl restart sshd
[root@server.ngalacan.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Wed 2024-10-16 18:41:40 UTC; 6s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
    Main PID: 13998 (sshd)
      Tasks: 1 (limit: 4557)
     Memory: 1.7M
        CPU: 13ms
    CGroup: /system.slice/ssh.service
            └─13998 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 16 18:41:40 server.ngalacan.net systemd[1]: Starting OpenSSH server daemon...
Oct 16 18:41:40 server.ngalacan.net sshd[13998]: Server listening on 0.0.0.0 port 2022.
Oct 16 18:41:40 server.ngalacan.net sshd[13998]: Server listening on :: port 2022.
Oct 16 18:41:40 server.ngalacan.net sshd[13998]: Server listening on 0.0.0.0 port 22.
Oct 16 18:41:40 server.ngalacan.net sshd[13998]: Server listening on :: port 22.
Oct 16 18:41:40 server.ngalacan.net systemd[1]: Started OpenSSH server daemon.
lines 1-18/18 (END)...skipping...
● sshd.service - OpenSSH server daemon
```

Рис. 10: Исправление меток SELinux, настройка межсетевого экрана, просмотр статуса sshd

Выполнение лабораторной работы

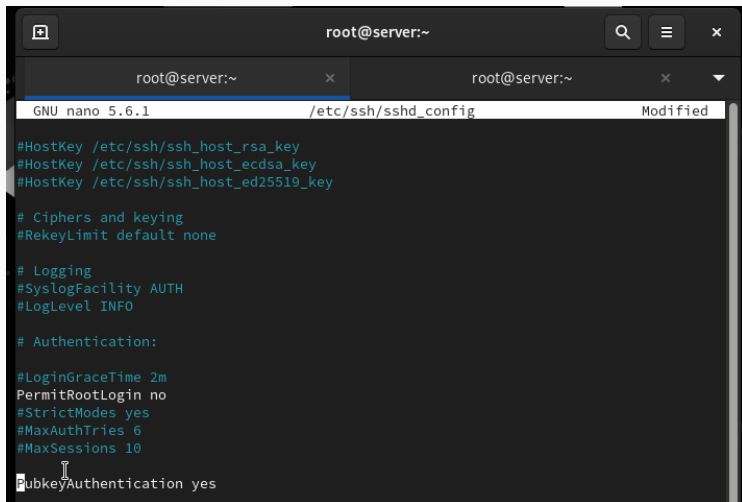
```
[ngalacan@client.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net
ngalacan@server.ngalacan.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Wed Oct 16 18:45:25 2024 from 192.168.1.1
[ngalacan@server.ngalacan.net ~]$ sudo -i
[sudo] password for ngalacan:
[root@server.ngalacan.net ~]# logout
[ngalacan@server.ngalacan.net ~]$ logout
Connection to server.ngalacan.net closed.
[ngalacan@client.ngalacan.net ~]$ ssh -p2022 ngalacan@server.ngalacan.net
ngalacan@server.ngalacan.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Wed Oct 16 18:47:12 2024 from 192.168.1.116
[ngalacan@server.ngalacan.net ~]$ sudo -i
[sudo] password for ngalacan:
[root@server.ngalacan.net ~]# logout
[ngalacan@server.ngalacan.net ~]$ logout
Connection to server.ngalacan.net closed.
[ngalacan@client.ngalacan.net ~]$
```

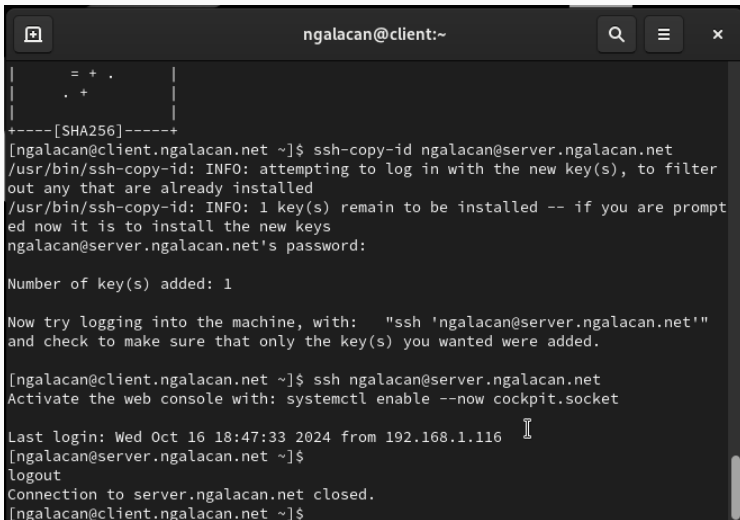
Рис. 11: Попытка получения доступа к серверу через ngalacan и через порт 2022: доступ получен

Настройка удалённого доступа по SSH по ключу



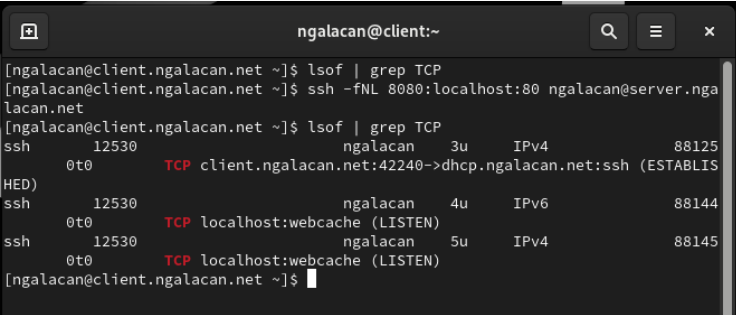
```
root@server:~  
GNU nano 5.6.1 /etc/ssh/sshd_config Modified  
  
#HostKey /etc/ssh/ssh_host_rsa_key  
#HostKey /etc/ssh/ssh_host_ecdsa_key  
#HostKey /etc/ssh/ssh_host_ed25519_key  
  
# Ciphers and keying  
#RekeyLimit default none  
  
# Logging  
#SyslogFacility AUTH  
#LogLevel INFO  
  
# Authentication:  
  
#LoginGraceTime 2m  
PermitRootLogin no  
#StrictModes yes  
#MaxAuthTries 6  
#MaxSessions 10  
  
PubkeyAuthentication yes
```

Рис. 12: Разрешение аутентификации по ключу



```
ngalacan@client:~  
|      = + .      |  
|      . +      |  
|      |      |  
+-----[SHA256]-----+  
[ngalacan@client.ngalacan.net ~]$ ssh-copy-id ngalacan@server.ngalacan.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  
ngalacan@server.ngalacan.net's password:  
  
Number of key(s) added: 1  
  
Now try logging into the machine, with:  "ssh 'ngalacan@server.ngalacan.net'"  
and check to make sure that only the key(s) you wanted were added.  
  
[ngalacan@client.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Wed Oct 16 18:47:33 2024 from 192.168.1.116  
[ngalacan@server.ngalacan.net ~]$  
logout  
Connection to server.ngalacan.net closed.  
[ngalacan@client.ngalacan.net ~]$
```

Организация туннелей SSH, перенаправление TCP-портов



```
ngalacan@client:~  
[ngalacan@client.ngalacan.net ~]$ lsof | grep TCP  
[ngalacan@client.ngalacan.net ~]$ ssh -fNL 8080:localhost:80 ngalacan@server.ngalacan.net  
[ngalacan@client.ngalacan.net ~]$ lsof | grep TCP  
ssh          12530          ngalacan      3u      IPv4          88125  
    0t0      TCP client.ngalacan.net:42240->dhcp.ngalacan.net:ssh (ESTABLISHED)  
ssh          12530          ngalacan      4u      IPv6          88144  
    0t0      TCP localhost:webcache (LISTEN)  
ssh          12530          ngalacan      5u      IPv4          88145  
    0t0      TCP localhost:webcache (LISTEN)  
[ngalacan@client.ngalacan.net ~]$
```

Рис. 14: Перенаправление порта 80 на server.ngalacan.net на порт 8080

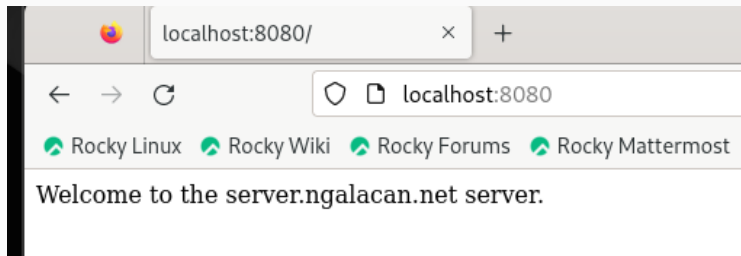
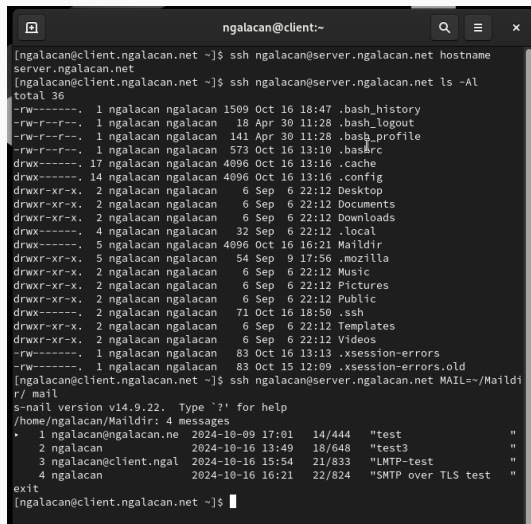


Рис. 15: localhost:8080 в браузере

Запуск консольных приложений через SSH

Выполнение лабораторной работы

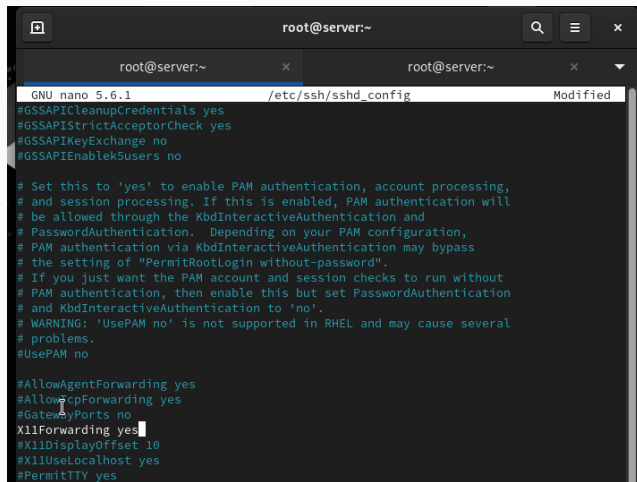


```
ngalacan@client:~  
[ngalacan@client.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net hostname  
server.ngalacan.net  
[ngalacan@client.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net ls -Al  
total 36  
-rw-----. 1 ngalacan ngalacan 1509 Oct 16 18:47 .bash_history  
-rw-r--r--. 1 ngalacan ngalacan 18 Apr 30 11:28 .bash_logout  
-rw-r--r--. 1 ngalacan ngalacan 141 Apr 30 11:28 .bash_profile  
-rw-r--r--. 1 ngalacan ngalacan 573 Oct 16 13:10 .bashrc  
drwx-----. 17 ngalacan ngalacan 4096 Oct 16 13:16 .cache  
drwx-----. 14 ngalacan ngalacan 4096 Oct 16 13:16 .config  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Desktop  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Documents  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Downloads  
drwx-----. 4 ngalacan ngalacan 32 Sep 6 22:12 .local  
drwx-----. 5 ngalacan ngalacan 4096 Oct 16 16:21 Maildir  
drwxr-xr-x. 5 ngalacan ngalacan 54 Sep 9 17:56 .mozilla  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Music  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Pictures  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Public  
drwx-----. 2 ngalacan ngalacan 71 Oct 16 18:50 .ssh  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Templates  
drwxr-xr-x. 2 ngalacan ngalacan 6 Sep 6 22:12 Videos  
-rw-----. 1 ngalacan ngalacan 83 Oct 16 13:13 .xsession-errors  
-rw-----. 1 ngalacan ngalacan 83 Oct 15 12:09 .xsession-errors.old  
[ngalacan@client.ngalacan.net ~]$ ssh ngalacan@server.ngalacan.net MAIL=~/.Maildir/  
r/ mail  
s-nail version v14.9.22. Type '?' for help  
/home/ngalacan/Maildir: 4 messages  
* 1 ngalacan@ngalacan.ne 2024-10-09 17:01 14/444 "test "  
2 ngalacan 2024-10-16 13:49 18/648 "test3 "  
3 ngalacan@client.ngal 2024-10-16 15:54 21/833 "LMTP-test "  
4 ngalacan 2024-10-16 16:21 22/824 "SMTP over TLS test "  
exit  
[ngalacan@client.ngalacan.net ~]$
```

Рис. 16: Просмотр с клиента имени узла, файлов и почты на сервере

Запуск графических приложений через SSH

Выполнение лабораторной работы



```
root@server:~  
GNU nano 5.6.1 /etc/ssh/sshd_config Modified  
#GSSAPICleanupCredentials yes  
#GSSAPIStrictAcceptorCheck yes  
#GSSAPIKeyExchange no  
#GSSAPIEnablek5users no  
  
# Set this to 'yes' to enable PAM authentication, account processing,  
# and session processing. If this is enabled, PAM authentication will  
# be allowed through the KbdInteractiveAuthentication and  
# PasswordAuthentication. Depending on your PAM configuration,  
# PAM authentication via KbdInteractiveAuthentication may bypass  
# the setting of "PermitRootLogin without-password".  
# If you just want the PAM account and session checks to run without  
# PAM authentication, then enable this but set PasswordAuthentication  
# and KbdInteractiveAuthentication to 'no'.  
# WARNING: 'UsePAM no' is not supported in RHEL and may cause several  
# problems.  
#UsePAM no  
  
#AllowAgentForwarding yes  
#AllowTcpForwarding yes  
#GatewayPorts no  
X11Forwarding yes  
#X11DisplayOffset 10  
#X11UseLocalhost yes  
#PermitTTY yes
```

Рис. 17: Разрешение отображения графических интерфейсов X11

Выполнение лабораторной работы

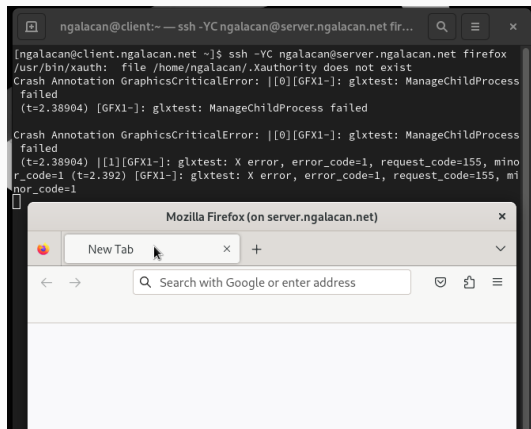
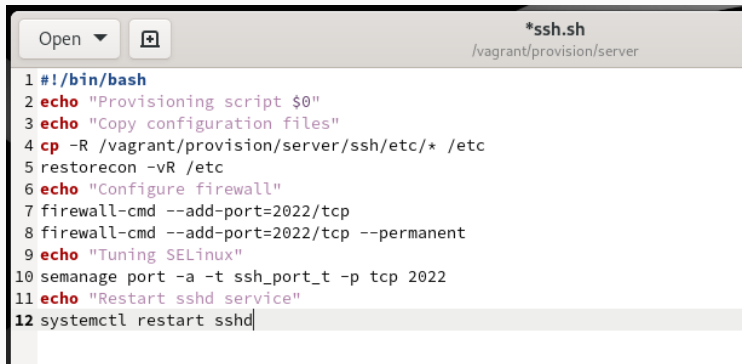


Рис. 18: Запуск firefox на сервере через клиент

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/
```



The screenshot shows a terminal window with a title bar. On the left, there is an 'Open' button with a dropdown arrow and a file icon button. On the right, the title bar indicates the file is '*ssh.sh' located at '/vagrant/provision/server'. The terminal content shows a script being edited line by line, with line numbers 1 through 12 on the left. The script includes comments and commands for provisioning a server, such as copying files, restoring repositories, configuring a firewall, and restarting the sshd service.

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

Рис. 19: Редактирование ssh.sh

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


В результате выполнения работы были приобретены практические навыки по настройке удалённого доступа к серверу с помощью SSH.