Лабораторная работа №7

СТУДЕНТ: САХНО

ГРУППА: НФИБД-02-23

Цель

Получить навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

Задания

Настроить межсетевой экран виртуальной машины server для доступа к серверу по протоколу SSH не через 22-й порт, а через порт 2022.

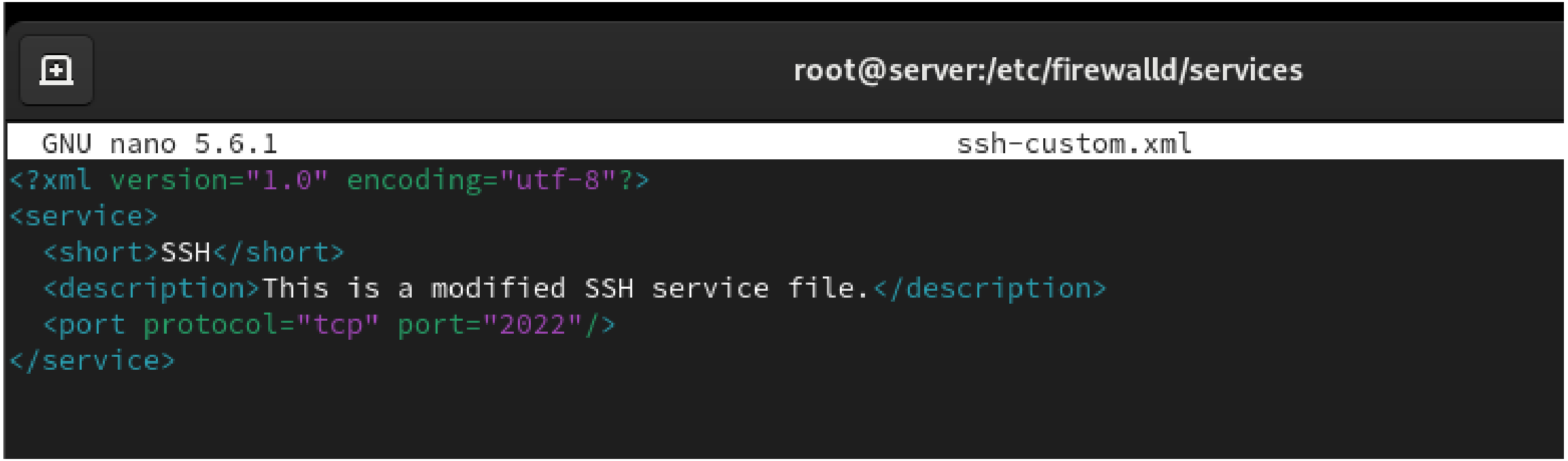
Настроить Port Forwarding на виртуальной машине server.

Настроить маскарадинг на виртуальной машине server для организации доступа клиента к сети Интернет.

Написать скрипт для Vagrant, фиксирующий действия по расширенной настройке межсетевого экрана. Соответствующим образом внести изменения в Vagrantfile.

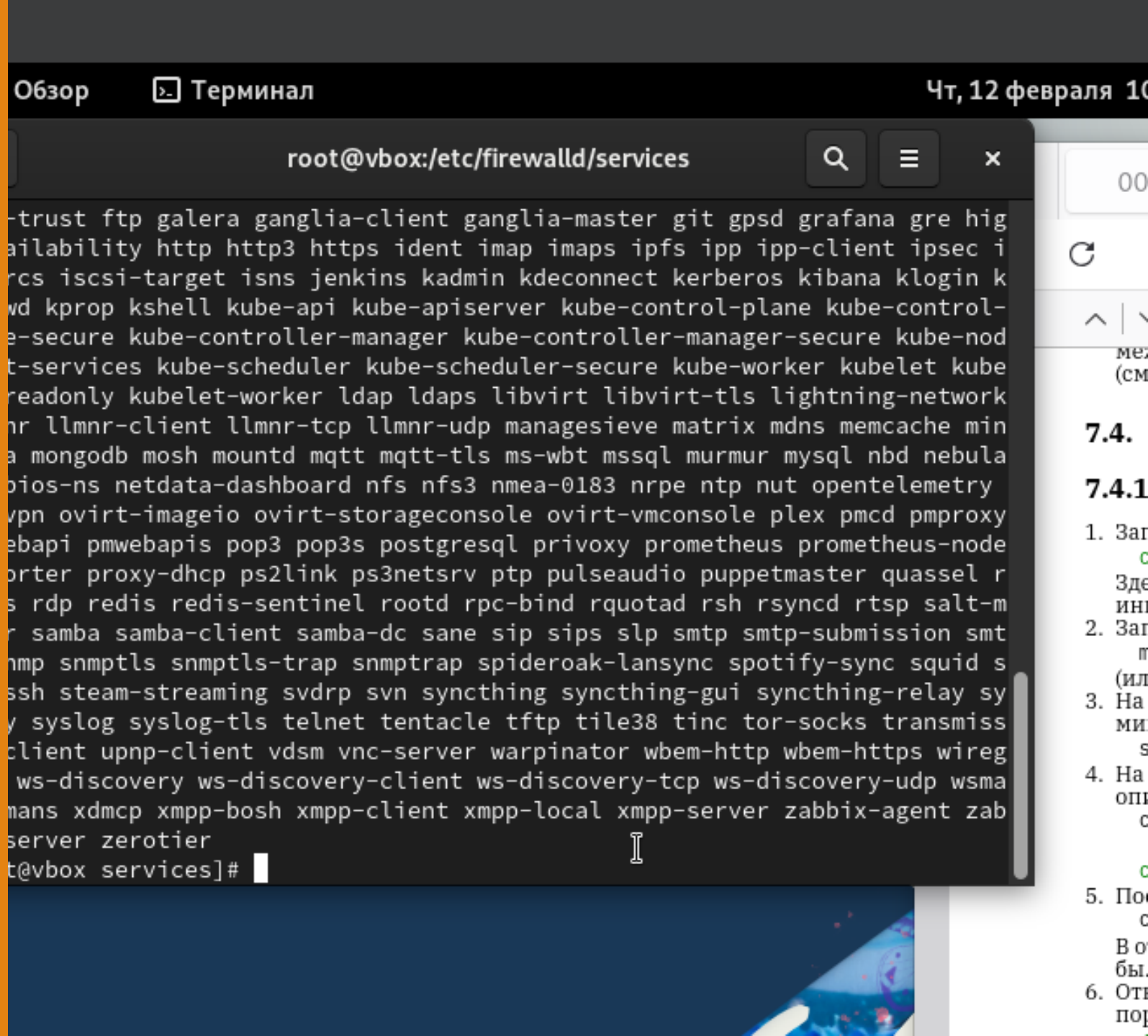
```
<service>
  <short>SSH</short>
  <description>Secure Shell (SSH) is a protocol for logging into and executing commands on remote machines. It provides sec
ure encrypted communications. If you plan on accessing your machine remotely via SSH over a firewalled interface, enable th
is option. You need the openssh-server package installed for this option to be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
```

Задание №1


root@server:/etc/firewalld/services
GNU nano 5.6.1
ssh-custom.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
<short>SSH</short>
<description>This is a modified SSH service file.</description>
<port protocol="tcp" port="2022"/>
</service>

Задание №1

Задание №1


Обзор
Терминал
Чт, 12 февраля 10
root@vbox:/etc/firewalld/services
-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre hig
ailability http http3 https ident imap imaps ipfs ipp ipp-client ipsec i
rcs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin k
wd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-
e-secure kube-controller-manager kube-controller-manager-secure kube-nod
t-services kube-scheduler kube-scheduler-secure kube-worker kubelet kube
readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network
nr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache min
a mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula
bios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry
vpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy
ebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node
orter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel r
s rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-m
r samba samba-client samba-dc sane sip sips slp smtp smtp-submission smt
nmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid s
ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay sy
y syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmiss
client upnp-client vdsm vnc-server warpinator wbem-http wbem-https wireg
ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsma
mans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zab
server zerotier
t@vbox services]#
7.4.
7.4.1

```
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacu
la-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine checkmk-ag
ent cockpit collectd condor-collector cratedb ctdb dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry dock
er-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeip
a-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability
 http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jellyfin jenkins kadmin kdeconnec
t kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-c
ontroller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker
kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-tcp llmnr-udp manage
sieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns netdata-da
shboard nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwe
bapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps3netsrv ptp pulseaudio pupp
etmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc
 sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssd
p ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tile38
tinc tor-socks transmission-client upnp-client vdsm vnc-server wbem-http wbem-https wireguard ws-discovery ws-discovery-c
lient ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabb
ix-server zerotier
```

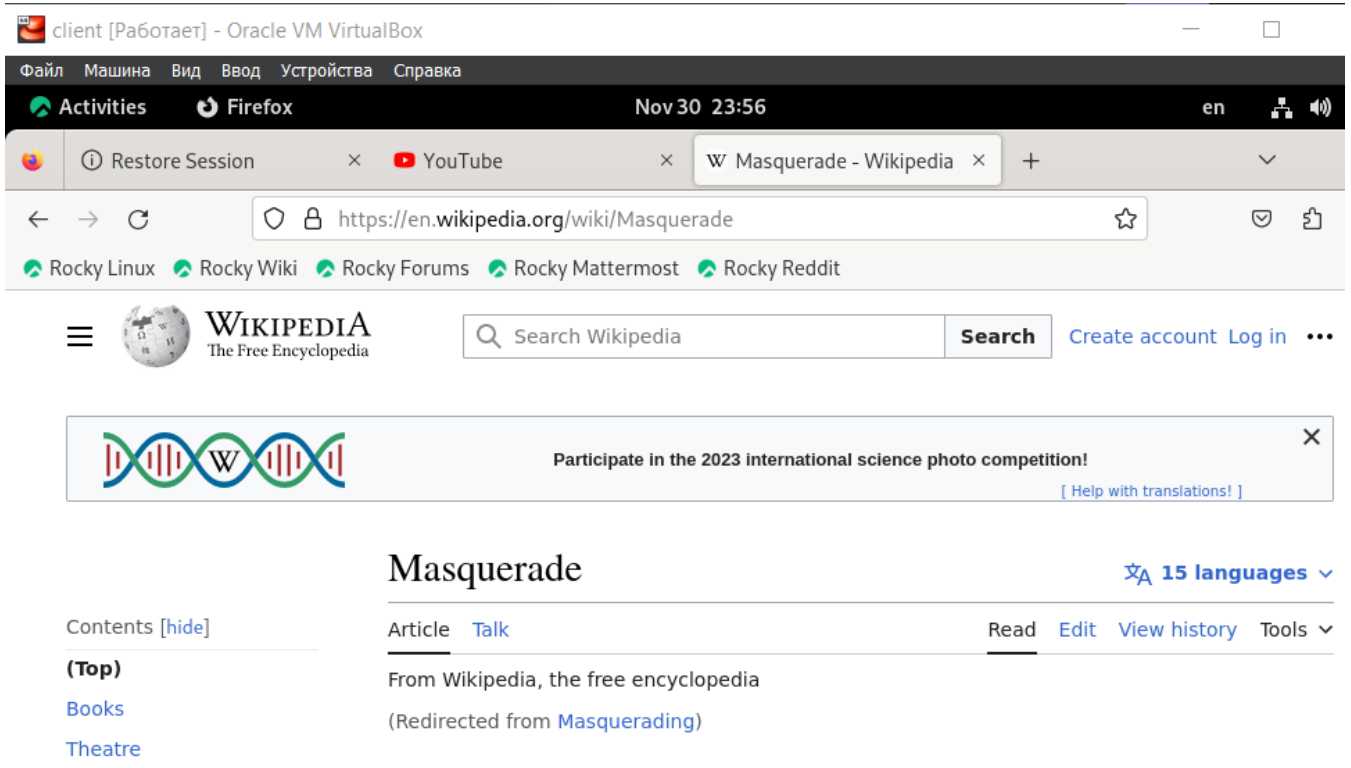
Задание №1


net.ipv4.conf.all.bc_forwarding = 0
net.ipv4.conf.all.forwarding = 0
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.default.bc_forwarding = 0
net.ipv4.conf.default.forwarding = 0
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.eth0.bc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 0
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth1.bc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 0
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.lo.bc_forwarding = 0
net.ipv4.conf.lo.forwarding = 0
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.ip_forward = 0
net.ipv4.ip_forward_update_priority = 1
net.ipv4.ip_forward_use_pmtu = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.all.mc_forwarding = 0
net.ipv6.conf.default.forwarding = 0
net.ipv6.conf.default.mc_forwarding = 0
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth0.mc_forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
net.ipv6.conf.eth1.mc_forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv6.conf.lo.mc_forwarding = 0

Задание №1

```
[root@vbox services]# firewall-cmd --list-services
cockpit dhcpv6-client https ssh
[root@vbox services]# firewall-cmd --add-service=ssh-custom
success
[root@vbox services]# firewall-cmd --list-services
cockpit dhcpv6-client https ssh ssh-custom
[root@vbox services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@vbox services]# firewall-cmd --reload
success
[root@vbox services]#
```

Задание №2


client [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Activities Firefox Nov 30 23:56 en
Restore Session
YouTube
Masquerade - Wikipedia
https://en.wikipedia.org/wiki/Masquerade
Rocky Linux Rocky Wiki Rocky Forums Rocky Mattermost Rocky Reddit
WIKIPEDIA
The Free Encyclopedia
Search Wikipedia
Search
Create account Log in
Participate in the 2023 international science photo competition!
[Help with translations!]
Masquerade
15 languages
Contents [hide]
(Top)
Books
Theatre
Article Talk
Read Edit View history Tools
From Wikipedia, the free encyclopedia
(Redirected from Masquerading)

Задание №2

```
]# cd /vagrant/provision/server
# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewall/etc

# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sysctl.d

# cd /vagrant/provision/server
# touch firewall.sh
# chmod +x firewall.sh
# nano firewall.sh
#
```

Задание №2

Контрольные вопросы

1. Где хранятся пользовательские файлы firewalld?

/usr/lib/firewalld/services

2. Какую строку надо включить в пользовательский файл службы, чтобы указать порт TCP 2022?

<port protocol="tcp" port="2022"/>

3. Какая команда позволяет вам перечислить все службы, доступные в настоящее время на вашем сервере?

firewall-cmd --get-services

4. В чем разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading)?

При маскарадинге вместо адреса отправителя(как делается это в NAT) динамически подставляется адрес назначенного интерфейса (сетевой адрес + порт).

5. Какая команда разрешает входящий трафик на порт 4404 и перенаправляет его в службу ssh по IP-адресу 10.0.0.10?

sudo firewall-cmd --add-forward-port=port=4404:proto=tcp:toport=22:toaddr=10.0.0.10

6. Какая команда используется для включения маскарадинга IP-пакетов для всех пакетов, выходящих в зону public?

firewall-cmd --zone=public --add-masquerade --permanent

Вывод:

В процессе выполнения данной лабораторной работы я получил навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.