РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ №7

дисциплина: администрирование локальных подсистем

Студент: Саинт-Амур Измаэль

Группа: НПИбд-02-20

МОСКВА

2022 г.

Постановка задачи

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

Выполнение работы

7.4.1. Создание пользовательской службы firewalld

1. На основе существующего файла описания службы ssh создал файл с собственным описанием

2. Посмотрел содержимое файла службы:

```
[root@server.saismael.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewa
lld/services/ssh-custom.xml
[root@server.saismael.net ~]#
[root@server.saismael.net ~]# cd /etc/firewalld/services/
[root@server.saismael.net services]#
[root@server.saismael.net services]# cat /etc/firewalld/services/ssh-custom.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>Secure Shell (SSH) is a protocol for logging into and executing c
ommands on remote machines. It provides secure encrypted communications. If you
plan on accessing your machine remotely via SSH over a firewalled interface, ena
ble this option. You need the openssh-server package installed for this option t
o be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
[root@server.saismael.net services]#
```

3. Открыл файл описания службы на редактирование и заменил порт 22 на новый порт (2022). В этом же файле скорректировал описание службы для демонстрации, что это модифицированный файл службы.

```
ssh-custom.xml     [-M--] 32 L:[  1+ 4   5/  7] *(449 / 465b) 0050 0x032  [*][X]
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>Secure Shell (SSH) is a protocol for logging into and executing c
  <port protocol="tcp" port="2022"/>
</service>
```

4. Просмотрел список доступных FirewallD служб:

```
[root@server.saismael.net services]#
[root@server.saismael.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps
apcupsd audit bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bi
tcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine cockpit collectd condor-
collector ctdb dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry
 docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger forem
an foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeip
a-trust ftp galera ganglia-client ganglia-master git grafana gre high-availabili
ty http https imap imaps ipp ipp-client ipsec irc ircs iscsi-target isns jenkins
 kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-api
server kube-control-plane kube-controller-manager kube-scheduler kubelet-worker
ldap ldaps libvirt libvirt-tls lightning-network llmnr managesieve matrix mdns m
emcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd
 netbios-ns nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storagec
onsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresq
l privoxy prometheus proxy-dhcp ptp pulseaudio puppetmaster quassel radius rdp r
edis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-cli
ent samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroa
k-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncth
ing-gui synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks tra
nsmission-client upnp-client vdsm vnc-server wbem-http wbem-https wireguard wsma
n wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-
server
```

5. Перегрузил правила межсетевого экрана с сохранением информации о состоянии и вновь вывел на экран список служб, а также список активных служб:

6. Добавил новую службу в FirewallD и вывел на экран список активных служб:

7.4.2. Перенаправление портов

1. Организовал на сервере переадресацию с порта 2022 на порт 22:

2. На клиенте попробовал получить доступ по SSH к серверу через порт 2022:

```
[root@server.saismael.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.saismael.net services]#
[root@server.saismael.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.saismael.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.saismael.net services]#
[root@server.saismael.net services]# firewall-cmd --add-forward-port=port=2022:p
roto=tcp:toport=22
success
[root@server.saismael.net services]# ssh -p 2022 saismael@server.saisamel.net
```

7.4.3. Настройка Port Forwarding и Masquerading

1. На сервере посмотрел, активирована ли в ядре системы возможность перенаправления IPv4-пакетов пакетов:

```
[root@server.saismael.net services]# sysctl -a | grep forward
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
```

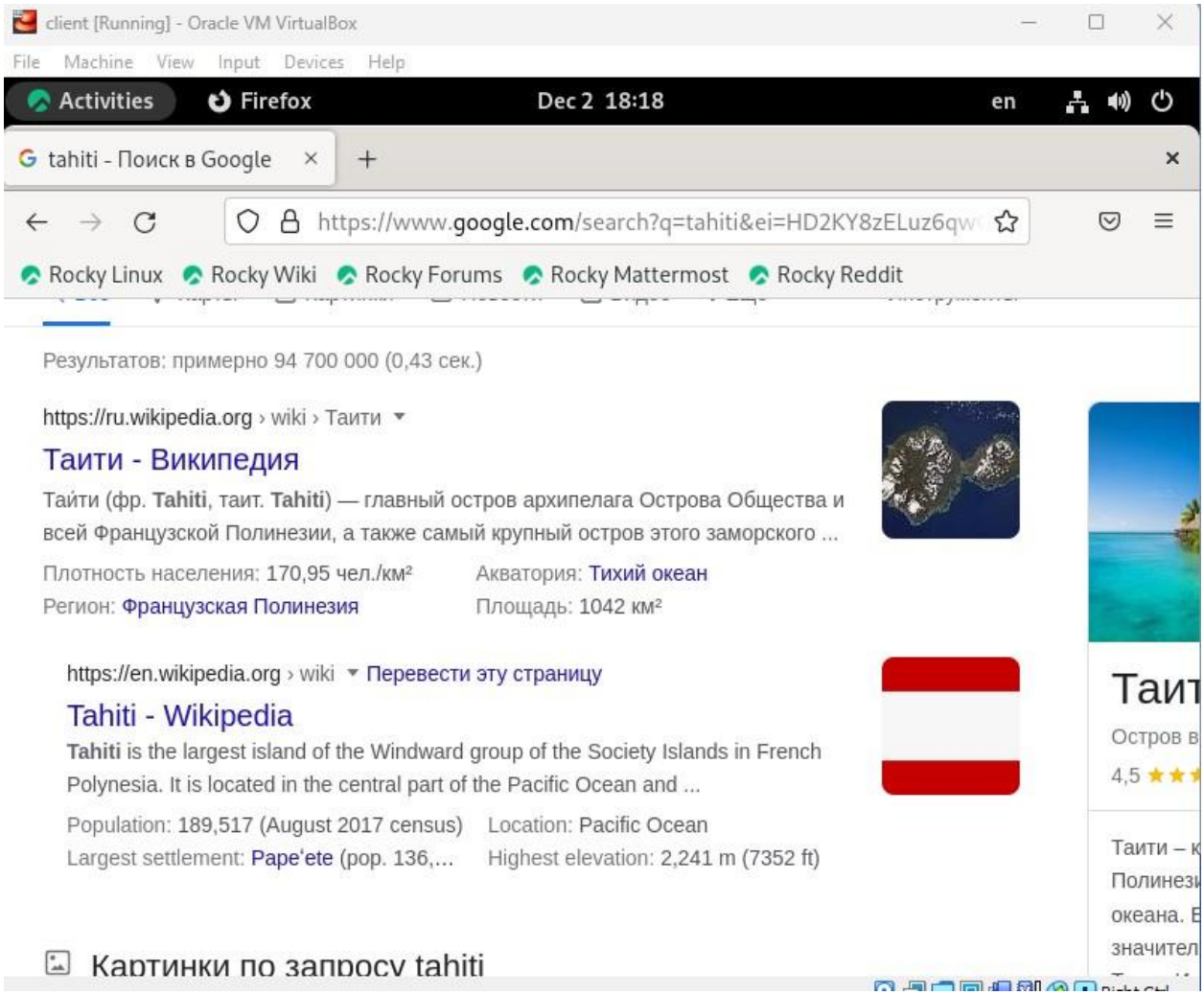
2. Включил перенаправление IPv4-пакетов на сервере

3. Включил маскарадинг на сервере:

```
[root@server.saismael.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysct
l.d/90-forward.conf
[root@server.saismael.net services]#
[root@server.saismael.net services]#
[root@server.saismael.net services]# sysctl -p /etc/systcl.d/90-forward.conf
sysctl: cannot open "/etc/systcl.d/90-forward.conf": No such file or directory
[root@server.saismael.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
```

```
[root@server.saismael.net services]# firewall-cmd --zone=public --add-masquerade
 --permanent
success
[root@server.saismael.net services]# firewall-cmd --reload
success
```

4. На клиенте проверил доступность выхода в Интернет.



7.4.4. 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 firewall, в который поместил в соответствующие подкаталоги конфигурационные файлы FirewallD:

2. В каталоге /vagrant/provision/server создал файл firewall.sh:

```
[root@server.saismael.net services]# cd /vagrant/provision/server
[root@server.saismael.net server]# mkdir -p /vagrant/provision/server/firewall/e
tc/firewalld/services
[root@server.saismael.net server]#
[root@server.saismael.net server]# mkdir -p /vagrant/provision/server/firewall/e
tc/sysctl.d
[root@server.saismael.net server]#
```

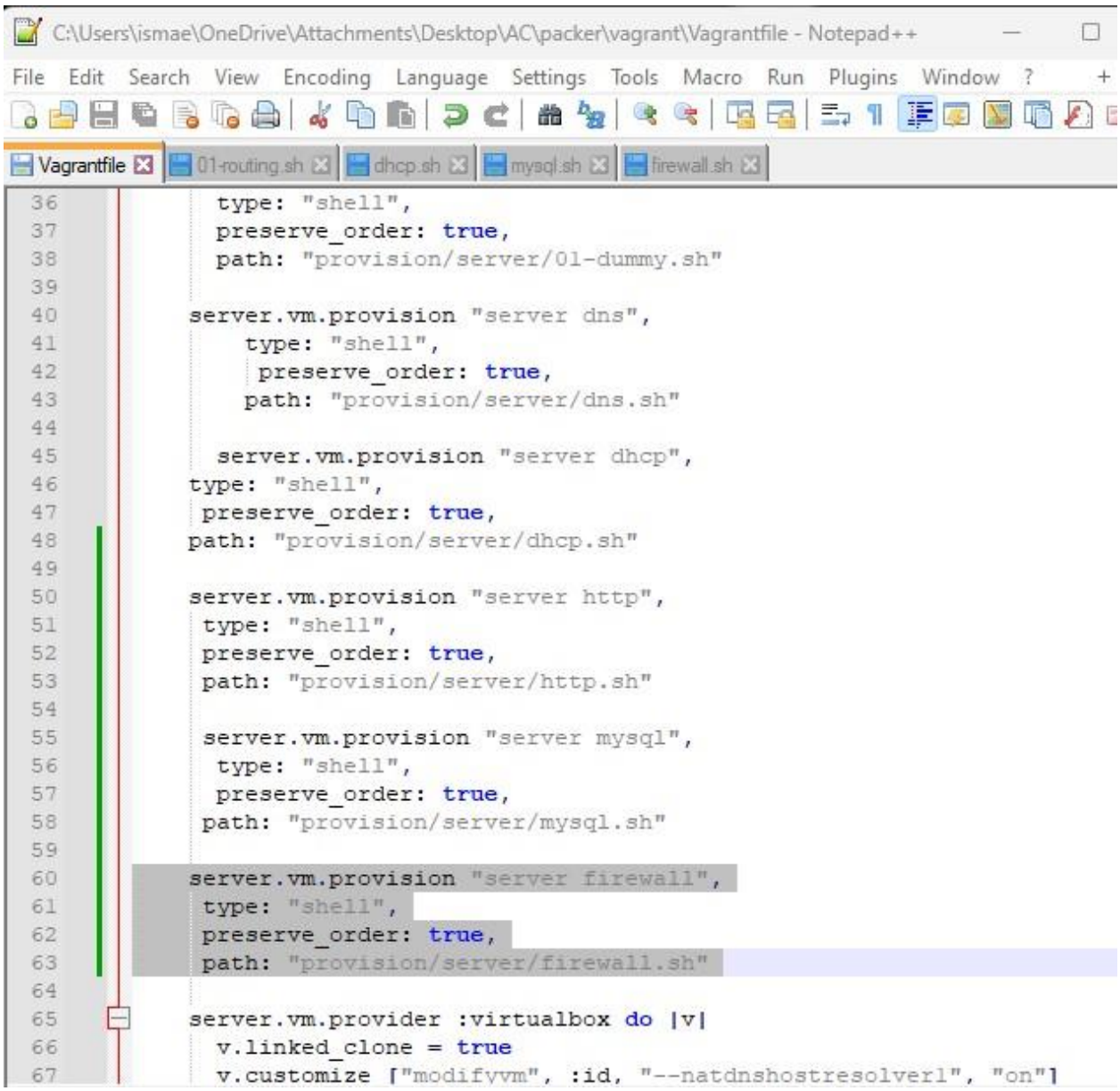
```
[root@server.saismael.net server]# cp -r /etc/firewalld/services/ssh-custom.xml
/vagrant/provision/server/firewall/etc/firewalld/services/
[root@server.saismael.net server]#
[root@server.saismael.net server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/
provision/server/firewall/etc/sysctl.d/
[root@server.saismael.net server]#
[root@server.saismael.net server]# cd /vagrant/provision/server
[root@server.saismael.net server]# touch firewall.sh
[root@server.saismael.net server]#
```

```
[root@server.saismael.net server]# chmod +x firewall.sh
[root@server.saismael.net server]#
```

Открыв его на редактирование, прописал в нём следующий скрипт

```
firewall.sh        [----] 19 L:[  1+13  14/ 14] *(381 / 381b) <EOF>        [*]
#!/bin/bash

echo "Provisioning script $0"

echo "Copy configuration files"
cp -R /vagrant/provision/server/firewall/etc/* /etc

echo "Configure masquerading"
firewall-cmd --add-service=ssh-custom --permanent
firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22 --permanent
firewall-cmd --zone=public --add-masquerade --permanent
firewall-cmd --reload

restorecon -vR /etc
```

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



Вывод:

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

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)?

- Маскарад - замена адреса на адрес машины, выполняющей маскарад. для перенаправления узлу локальной сети ответного пакета из внешней сети узел-шлюз обратно заменяет не только сетевой адрес, но и указывает порт отправителя

Трансляция адресов - замена адреса на любой указанный.

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