

Лабораторная работа №7

Расширенные настройки межсетевого экрана

Сахно Никита НФИбд-02-23

Содержание

1	Цель работы	1
2	Задание	1
3	Выполнение лабораторной работы.....	2
3.1	Создание пользовательской службы firewalld.....	2
3.2	Настройка Port Forwarding и Masquerading.....	4
3.3	Внесение изменений в настройки внутреннего окружения виртуальной машины	5
4	Выводы.....	6
5	Контрольные вопросы.....	6

1 Цель работы

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

2 Задание

1. Настроить межсетевой экран виртуальной машины server для доступа к серверу по протоколу SSH не через 22-й порт, а через порт 2022.
2. Настроить Port Forwarding на виртуальной машине server.
3. Настроить маскарадинг на виртуальной машине server для организации доступа клиента к сети Интернет.
4. Написать скрипт для Vagrant, фиксирующий действия по расширенной настройке межсетевого экрана. Соответствующим образом внести изменения в Vagrantfile.

3 Выполнение лабораторной работы

3.1 Создание пользовательской службы firewalld

На основе существующего файла описания службы ssh создадим файл с собственным описанием и посмотрим содержимое файла службы.

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

Создание файла с собственным описанием

В первой строчке указана версия xml и используемая кодировка - utf8. На второй строчке указан тег service, далее его тег-потомок short, внутри которого указан SSH. Затем указан тег description, внутри которого прописано описание протокола ssh, и указан протокол передачи порта tcp и номер порта.

Откроем файл описания службы на редактирование и заменим порт 22 на новый порт (2022):

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

В этом же файле скорректируем описание службы для демонстрации, что это модифицированный файл службы.



```
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>
```

Отредактированный файл описания службы

Посмотрим список доступных FirewallD служб:

```
firewall-cmd --get-services
```

Новая служба ещё не отображается в списке.

```

root@vbox:/etc/firewalld/services
eipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre hig
h-availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec i
rc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin k
passwd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-
plane-secure kube-controller-manager kube-controller-secure kube-nod
eport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kube
let-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network
llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache min
idlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula
netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry
openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy
pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus-node
-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel r
adius rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-m
aster samba samba-client samba-dc sane sip sips slp smtp smtp-submission smt
ps snmp snmpd snmpd-trap snmptrap spideroak-lansync spotify-sync squid s
sdp ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay sy
nergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmiss
ion-client upnp-client vdsm vnc-server warpinator wbem-http wbem-https wireg
uard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsma
n wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zab
bix-server zerotier
[root@vbox services]#

```

Список доступных FirewallD служб

Перегрузим правила межсетевого экрана с сохранением информации о состоянии и вновь выведем на экран список служб, а также список активных служб. Созданная служба отображается в списке доступных для FirewallD служб, но не активирована. Добавим новую службу в FirewallD и выведем на экран список активных служб:

```

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-rpc bittorrent-lsd ceph ceph-mon cfengine checkmk-ag
ent cockpit 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-ldap 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 iircs iscsi-target isns jellyfin jenkins kadmin kdeconnect
kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-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 manag
e sieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netdata-da
table nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmw
ebapi pmwebapis pop3 pop3s postgresql privoxy prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio pu
shticker 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 smptls smptls-trap snmptrap spideroak-lansync spotify-sync squid ssd
p ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-gui synergy 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 zab
bix-server zerotier

```

Список FirewallD служб и добавление новой службы в FirewallD

Организуем на сервере переадресацию с порта 2022 на порт 22:

```
firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
```

На клиенте попробуем получить доступ по SSH к серверу через порт 2022:

```
ssh -p 2022 nvsakhno@server.nvsakhno.net
```

3.2 Настройка Port Forwarding и Masquerading

На сервере посмотрим, активирована ли в ядре системы возможность перенаправления IPv4-пакетов пакетов:

```
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
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
```

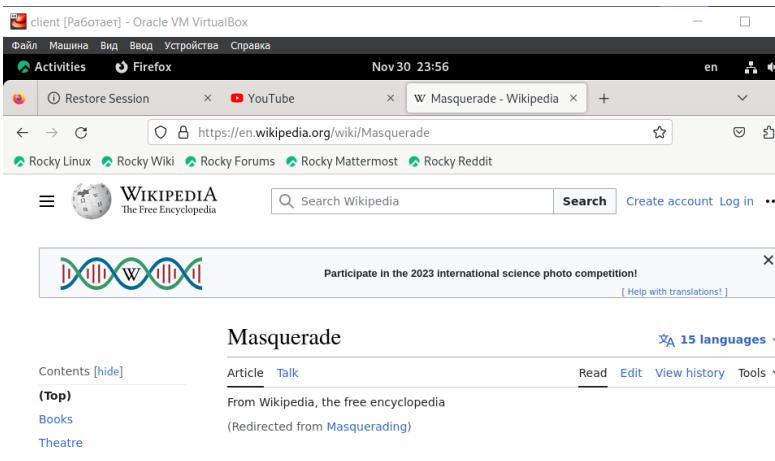
Проверка активации перенаправления IPv4-пакетов

Включим перенаправление IPv4-пакетов на сервере. Включим маскарадинг на сервере и перезапустим систему:

```
[root@vbox services]# firewall-cmd --list-services
cockpit dhcpcv6-client https ssh
[root@vbox services]# firewall-cmd --add-service=ssh-custom
success
[root@vbox services]# firewall-cmd --list-services
cockpit dhcpcv6-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]#
```

Включение перенаправление IPv4-пакетов и маскарадинга на сервере

На клиенте проверим доступность выхода в Интернет.



Проверка доступности выхода в Интернет

Выход в Интернет на клиенте доступен.

3.3 Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог firewall, в который поместим в соответствующие подкаталоги конфигурационные файлы FirewallD. В каталоге /vagrant/provision/server создадим файл firewall.sh.

```
# 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/* /vagrant/provision/server/firewall/etc/
cp -r /etc/sysctl.d/* /vagrant/provision/server/firewall/etc/
cd /vagrant/provision/server
touch firewall.sh
chmod +x firewall.sh
nano firewall.sh
```

Внесения изменений в настройки внутреннего окружения

Открыв его на редактирование, пропишите в нём следующий скрипт:

```
root@server:/vagrant/provision/server
GNU nano 5.6.1          firewall.sh
#!/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=2022:proto=tcp toport=22 --permanent
firewall-cmd --zone=public --add-masquerade --permanent
firewall-cmd --reload

restorecon -vR /etc
```

Редактирование файла

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера:

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

4 Выводы

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

5 Контрольные вопросы

- Где хранятся пользовательские файлы firewalld?

```
/usr/lib/firewalld/services
```

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

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

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

```
firewall-cmd --get-services
```

- 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).

- 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
```

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

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