Лабораторная работа №7

Администрирование сетевых подсистем

Машков Илья Евгеньевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Задание

1. Настройте межсетевой экран виртуальной машины server для доступа к серверу по протоколу SSH не через 22-й порт, а через порт 2022.
2. Настройте Port Forwarding на виртуальной машине server.
3. Настройте маскарадинг на виртуальной машине server для организации доступа клиента к сети Интернет.
4. Напишите 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 уже существующего файла с описанием ssh создаю свой, но перед этим просматриваю изначальное содержание. Тут мы видим версию xml, кодировку utf-8, протокл tcp и порт 22, а также базовое описание SSH (рис. [3.1]).

```
[user@server ~]$ sudo -i
[sudo] password for user:
[root@server ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-cust
om.xml
[root@server ~]# /etc/firewalld/services/
-bash: /etc/firewalld/services/: Is a directory
[root@server ~]# cd /etc/firewalld/services/
[root@server 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 commands
on remote machines. It provides secure encrypted communications. If you plan on accessin
g your machine remotely via SSH over a firewalled interface, enable this option. You nee
d the openssh-server package installed for this option to be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
[root@server services]#
```

Рис. 3.1: Содержимое файла ssh-custom.xml

Затем меняю описание файла и меняю порт с 22-го на 2022-ой (рис. [3.2]).

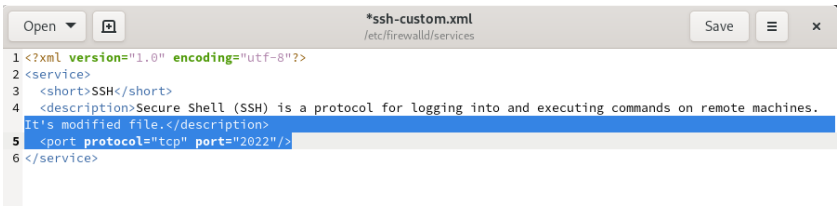

Рис. 3.2: Редактирование ssh-custom.xml

Просматриваю список доступных служб межсетевого экрана (рис. [3.3]).

```
[root@server services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcu
psd audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-stor
age bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph c
eph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb c
tdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls dock
er-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger fo
reman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-tru
st 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 jenkin
s kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver
kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-man
ager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kube
let kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llm
nr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb mo
sh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboar
d nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmcon
sole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prome
theus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel rad
ius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-cl
ient samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snm
ptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing
syncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc
 tor-socks transmission-client upnp-client vdsm vnc-server warpinator wbem-http wbem-htt
ps wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman ws
mans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerot
ier
[root@server services]#
```

Рис. 3.3: Список доступных служб

Перезагружаю правила и вновь вывожу список имеющихся и активных служб, где мы видим наши dhcp, dns, http, https, mysql и ssh службы (рис. [3.4]).

```
[root@server services]# firewall-cmd --reload
success
[root@server services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcu
psd audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-stor
age bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph c
eph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb c
tdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls dock
er-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger fo
reman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-tru
st 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 jenkin
s kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver
kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-man
ager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kube
let kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llm
nr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb mo
sh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboar
d nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmcon
sole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prome
theus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel rad
ius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-cl
ient samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snm
ptrap spideroak-lansync spotify-sync squid ssdp ssh ssh-custom steam-streaming svdrp svn
 syncthing syncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp
tile38 tinc tor-socks transmission-client upnp-client vdsm vnc-server warpinator wbem-ht
tp wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-u
dp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-s
erver zerotier
[root@server services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server services]#
```

Рис. 3.4: Список доступных и активных служб

Затем добавляем нашу модифицированную ssh-службу и выводим список активных служб, где можем увидеть, что она активна (рис. [3.5]).

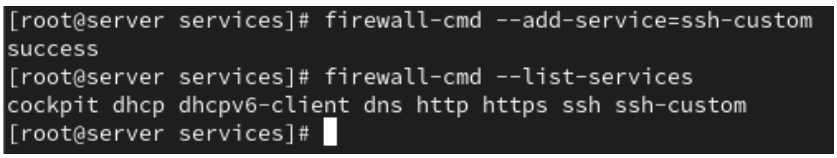

Рис. 3.5: Добавление кастомной ssh-службы

Презагружаем правила межсетевого экрана и добавляем переадресацию с порта 2022 на 22(рис. [3.6]).

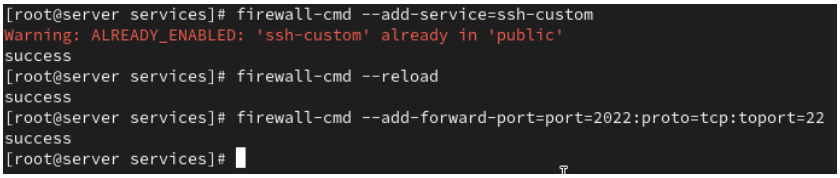

Рис. 3.6: Перезагрузка правил и перенаправление портов

С машины client пытаюсь выйти в интернет, но получаю отказ (рис. [3.7]).

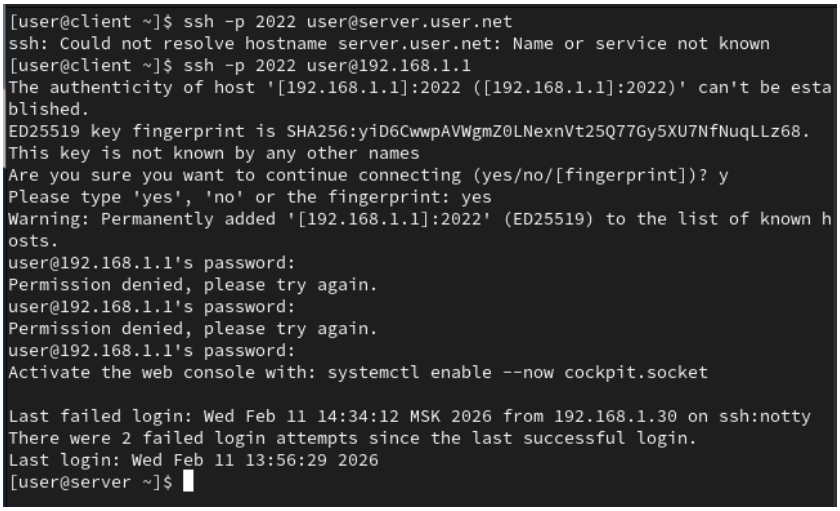

Рис. 3.7: Попытка выхода в сеть с клиента

3.2 Настройка Port Forwarding и Masquerading

Смотрю, активирована ли функция перенаправления IPv4-пакетов. Вижу, что она не активирована на уровне ядра (рис. [3.8]).

```
[root@server 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
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
[root@server services]#
```

Рис. 3.8: Перенаправление IPv4-пакетов

Включаю эту функцию и проверяю, что она работает (рис. [3.9]).

```
[root@server services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server services]#
```

Рис. 3.9: Включение перенаправления IPv4-пакетов

Затем включаю маскарадинг на сервере (рис. [3.10]).

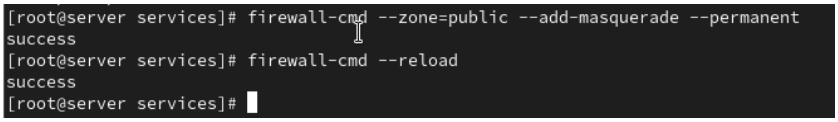

Рис. 3.10: Включение маскарадинга на сервере

После этого снова совершаю попытку выхода в интернет, но в доступе мне отказано (рис. [3.11]).

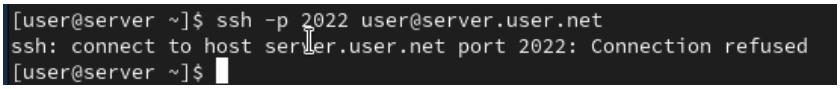

Рис. 3.11: Попытка выхода в интернет №2

3.3 Внесение изменений в настройки внутреннего окружения виртуальной машины

Вношу изменения в настройки внутреннего окружения путём добавления конфиговских файлов межсетевого экрана (рис. [3.12]).

Рис. 3.12: Коррекция настроек внутреннего окружения

Создаю файл скрипта firewall.sh (рис. [3.13]).

```
root@server server]# cd /vagrant/provision/server
root@server server]# touch firewall.sh
root@server server]# chmod +x firewall.sh
root@server server]# gedit firewall.sh
```

Рис. 3.13: Создание скрипта

Заполняю файл скриптом, который будет повторять все действия из этой лабы при запуске машины server (рис. [3.14]).

Open *firewall.sh /vagrant/provision/server

```
#!/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
```

Рис. 3.14: firewall.sh

Для отработки скрипта вношу изменения в Vagrantfile (рис. [3.15]).

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

Рис. 3.15: Vagrantfile

4 Выводы

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

Список литературы

Администрирование сетевых подсисем