

Лабораторная работа №7

Шубина София Антоновна

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
3.1	Создание пользовательской службы firewalld	6
3.2	Настройка Port Forwarding и Masquerading	9
3.3	Внесение изменений в настройки внутреннего окружения виртуальной машины	11
4	Выводы	13
5	Контрольные вопросы	14

Список иллюстраций

3.1	<code>sudo -i</code>	6
3.2	Создание файла с собственным описанием	6
3.3	посмотр файла	6
3.4	просмотр файла	7
3.5	Отредактированный файл описания службы	7
3.6	Список доступных FirewallD служб	7
3.7	Список FirewallD служб и добавление новой службы в FirewallD . .	8
3.8	с порта 2022 на порт 22	8
3.9	Переадресация и получение доступа по SSh	8
3.10	Проверка активации перенаправления IPv4-пакетов	9
3.11	Включение перенаправление IPv4-пакетов и маскарadingа на сервере	9
3.12	<code>firewall-cmd--zone=public--add-masquerade--permanent</code> и <code>firewall-</code> <code>cmd--reload</code>	10
3.13	Проверка доступности выхода в Интернет	10
3.14	Проверка доступности выхода в Интернет	10
3.15	Внесения изменений в настройки внутреннего окружения	11
3.16	Внесения изменений в настройки внутреннего окружения	11
3.17	Редактирование файла	11
3.18	Редактирование файла	12

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 маскарading 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

Перейдем в режим суперпользователя

```
[sashubina@server.sashubina.net ~]$ sudo -i
[sudo] password for sashubina:
[root@server.sashubina.net ~]#
```

Рис. 3.1: sudo -i

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

```
[root@server.sashubina.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.sashubina.net ~]# cd /etc/firewalld/services/
[root@server.sashubina.net services]#
```

Рис. 3.2: Создание файла с собственным описанием

```
[root@server.sashubina.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 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>
[root@server.sashubina.net services]#
```

Рис. 3.3: просмотр файла

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"/>
```

Рис. 3.4: просмотр файла

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

Рис. 3.5: Отредактированный файл описания службы

Просмотрим список доступных FirewallD служб:

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

Новая служба ещё не отображается в списке.

Рис. 3.6: 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:

```
[root@server.sashubina.net services]# firewall-cmd --reload
success
[root@server.sashubina.net services]# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800 apcups
d aseqnet audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin
-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-
iv civilization-v cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client
distcc dns dns-over-qtcp dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-serve
r factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galer
a ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https ident imap imaps iperf2 iperf3 i
pfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshel
l kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-s
ecure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ld
ap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache m
incraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wa
nted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconso
le ovirt-vmconsole plex pncd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporte
r proxy-dhcp ps2link ps3netstrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind
rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp s
mtpp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh ssh-custom st
atsrv steam-lan-transfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn sync
thing syncthing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-so
cks transmission-client turn turns upnp-client vdsu vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discove
ry ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wssd wssd-http wsmn wsmans xdmcp xmpp-bosh x
mpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper zabbix-web-service zero
-k zerotier
[root@server.sashubina.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.sashubina.net services]#
```

Рис. 3.7: 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`

```
[root@server.sashubina.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
[root@server.sashubina.net services]#
```

Рис. 3.8: с порта 2022 на порт 22

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

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

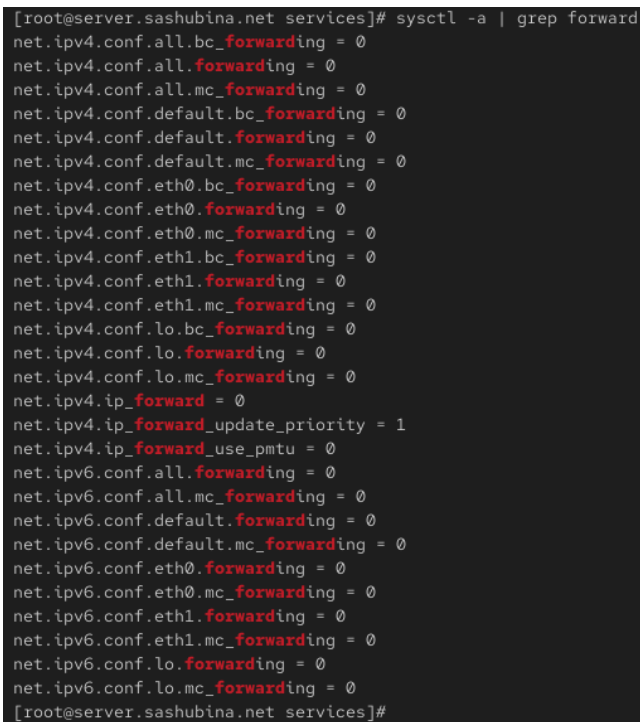
```
[sashubina@client.sashubina.net ~]$ ssh -p 2022 sashubina@server.sashubina.net
The authenticity of host '[server.sashubina.net]:2022 ([192.168.1.100]:2022)' can't be established.
ED25519 key fingerprint is SHA256:LjP5qM044iVZ+0Xnopuu/dN//5izIhYfJcVSZxbg00K.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[server.sashubina.net]:2022' (ED25519) to the list of known hosts.
Connection closed by 192.168.1.100 port 2022
[sashubina@client.sashubina.net ~]$
```

Рис. 3.9: Переадресация и получение доступа по SSH

3.2 Настройка Port Forwarding и Masquerading

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

```
sysctl -a | grep forward
```



```
[root@server.sashubina.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
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.sashubina.net services]#
```

Рис. 3.10: Проверка активации перенаправления IPv4-пакетов

Возможность не активирована

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



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

Рис. 3.11: Включение перенаправление IPv4-пакетов и маскардинга на сервере

Включим маскардинг на сервере:

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

Рис. 3.12: firewall-cmd--zone=public--add-masquerade--permanent
firewall-cmd--reload

ifirewall-

На клиенте проверим доступность выхода в Интернет.

```
[sashubina@client.sashubina.net ~]$ ping -c 3 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=255 time=29.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=255 time=19.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=255 time=23.6 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 19.917/24.275/29.341/3.879 ms
[sashubina@client.sashubina.net ~]$
```

Рис. 3.13: Проверка доступности выхода в Интернет

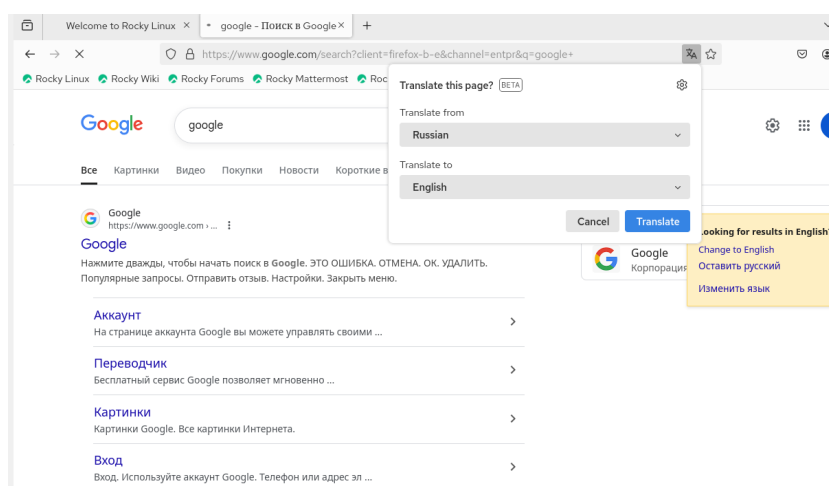


Рис. 3.14: Проверка доступности выхода в Интернет

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`.

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

Рис. 3.15: Внесения изменений в настройки внутреннего окружения

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

Рис. 3.16: Внесения изменений в настройки внутреннего окружения

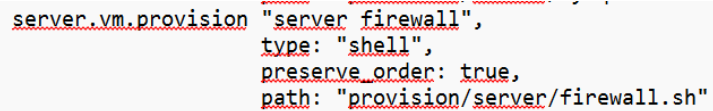
Открыв его на редактирование, пропишите в нём следующий скрипт:

```
GNU nano 8.1 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=port=2022:proto=tcp:toport=22 --permanent
firewall-cmd --zone=public --add-masquerade --permanent
firewall-cmd --reload
restorecon -vR /etc
```

Рис. 3.17: 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"
```



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

Рис. 3.18: Редактирование файла

4 Выводы

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

5 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 маскарadingом (masquerading)?

При маскарadingе 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 маскарadingа IP-пакетов для всех пакетов, выходящих в зону public?

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