Лабораторная работа №7

Расширенные настройки межсетевого экрана

Студент: Пакавира Арсениу Висенте Луиш

Группа: НФИбд 02–23

дисциплина: **Администрирование сетевых подсистем (Lab 7)**

Цель работы

Целью данной работы является получение навыков настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

Создание пользовательской службы firewalld

```
[root@server.user.net ~]# sudo -i
[root@server.user.net ~]# cp /usr/lib/firewalld/services/ssh.xml
/etc/firewalld/services/ssh-custom.xml
cp: missing destination file operand after '/usr/lib/firewalld/services/ssh.xml'
Try 'cp --help' for more information.
-bash: /etc/firewalld/services/ssh-custom.xml: No such file or directory
[root@server.user.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.user.net ~]# cd /etc/firewalld/services/
[root@server.user.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, ena
ble this option. You need the openssh-server package installed for this option to be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
[root@server.user.net services]#
```

Рис. 1.1. Создание файла с собственным описанием на основе существующего файла описания службы ssh. Просмотр содержимого файла службы.

Создание пользовательской службы firewalld

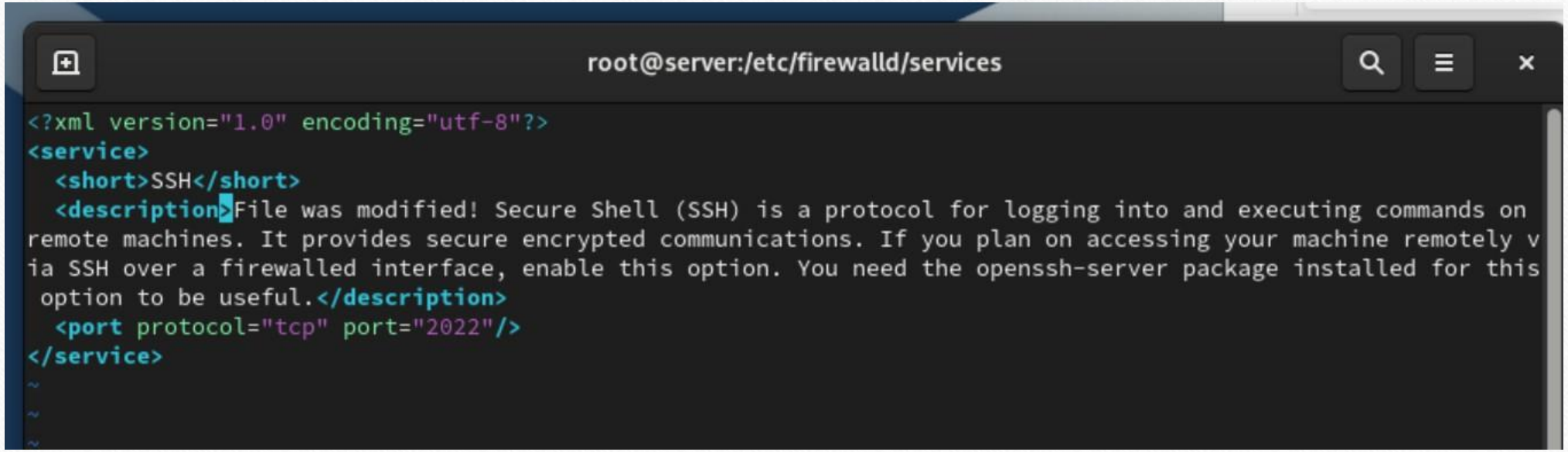

Рис. 1.2. Открытие файла описания службы на редактирование и замена порта 22 на новый порт (2022), корректирование описания службы для демонстрации, что это модифицированный файл службы.

Создание пользовательской службы firewalld

```
[user@server.user.net ~]$ firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bac
ula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-r
pc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dds
dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync
 elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replica
tion freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https iden
t imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpass
wd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager kube-contro
ller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kub
elet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix m
dns memcache minidlna mongodb mosh 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-vmconsole plex pmcd pmproxy pmwebapi
pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio
puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client sam
ba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squ
id 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-https wireguard ws-
discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp
-server zabbix-agent zabbix-server zerotier
[user@server.user.net ~]$
```

Рис. 1.3. Просмотр списка доступных FirewallD служб.

Создание пользовательской службы firewalld

Рис. 1.4. Перегрузка правил межсетевого экрана с сохранением информации о состоянии, вывод на экран списка служб, а также списка активных служб.

Создание пользовательской службы firewalld

```
[user@server.user.net ~]$ firewall-cmd --add-service=ssh-custom
success
[user@server.user.net ~]$ firewall-cmd --list-services
cockpit dhcpv6-client ntp samba smtp ssh ssh-custom
[user@server.user.net ~]$
```

Рис. 1.5. Добавление новой службы в FirewallD и вывод на экран списка активных служб.

Перенаправление портов

```
[user@server.user.net ~]$ firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
```

Рис. 2.1. Организация переадресации на сервере с порта 2022 на порт 22.

Перенаправление портов

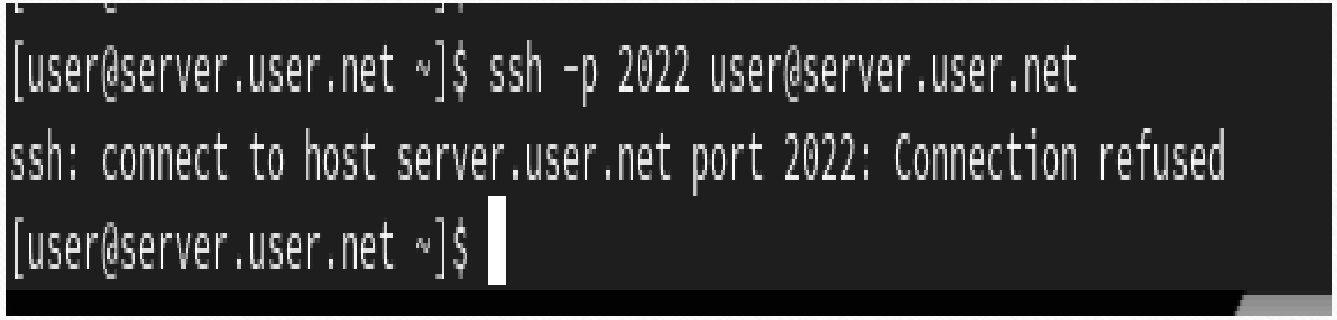

Рис. 2.2.Попытка получить на клиенте доступ по SSH к серверу через порт 2022.

Настройка Port Forwarding и Masquerading

```
[user@server.user.net ~]$ sysctl -a | grep forward
sysctl: permission denied on key 'fs.protected_fifos'
sysctl: permission denied on key 'fs.protected_hardlinks'
sysctl: permission denied on key 'fs.protected_regular'
sysctl: permission denied on key 'fs.protected_symlinks'
sysctl: permission denied on key 'kernel.cad_pid'
sysctl: permission denied on key 'kernel.usermodehelper.bset'
sysctl: permission denied on key 'kernel.usermodehelper.inheritable'
sysctl: permission denied on key 'net.core.bpf_jit_harden'
sysctl: permission denied on key 'net.core.bpf_jit_kallsyms'
sysctl: permission denied on key 'net.core.bpf_jit_limit'
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
sysctl: permission denied on key 'net.ipv4.tcp_fastopen_key'
sysctl: net.ipv6.conf.all.forwarding = 0
permission denied on key 'net.ipv6.conf.all.stable_secret'net.ipv6.conf.all.mc_forwarding = 0

sysctl: net.ipv6.conf.default.forwarding = 0
permission denied on key 'net.ipv6.conf.default.stable_secret'
net.ipv6.conf.default.mc_forwarding = 0
sysctl: permission denied on key 'net.ipv6.conf.eth0.stable_secret'
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth0.mc_forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
sysctl: permission denied on key 'net.ipv6.conf.eth1.stable_secret'
net.ipv6.conf.eth1.mc_forwarding = 0
sysctl: permission denied on key 'net.ipv6.conf.lo.stable_secret'
net.ipv6.conf.lo.forwarding = 0
net.ipv6.conf.lo.mc_forwarding = 0
sysctl: permission denied on key 'vm.mmap_rnd_bits'
sysctl: permission denied on key 'vm.mmap_rnd_compat_bits'
sysctl: permission denied on key 'vm.stat_refresh'
[user@server.user.net ~]$
```

Рис. 3.1. Просмотр на сервере, активирована ли в ядре системы возможность перенаправления IPv4-пакетов.

Настройка Port Forwarding и Masquerading

```
sysctl: permission denied on key 'vm.stat_refresh'
[user@server.user.net ~]$ echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
bash: /etc/sysctl.d/90-forward.conf: Permission denied
[user@server.user.net ~]$ sysctl -p /etc/sysctl.d/90-forward.conf
sysctl: cannot open "/etc/sysctl.d/90-forward.conf": No such file or directory
[user@server.user.net ~]$
```

Рис. 3.2. Включение перенаправления IPv4-пакетов на сервере и маскарадинга на сервере.

Настройка Port Forwarding и Masquerading

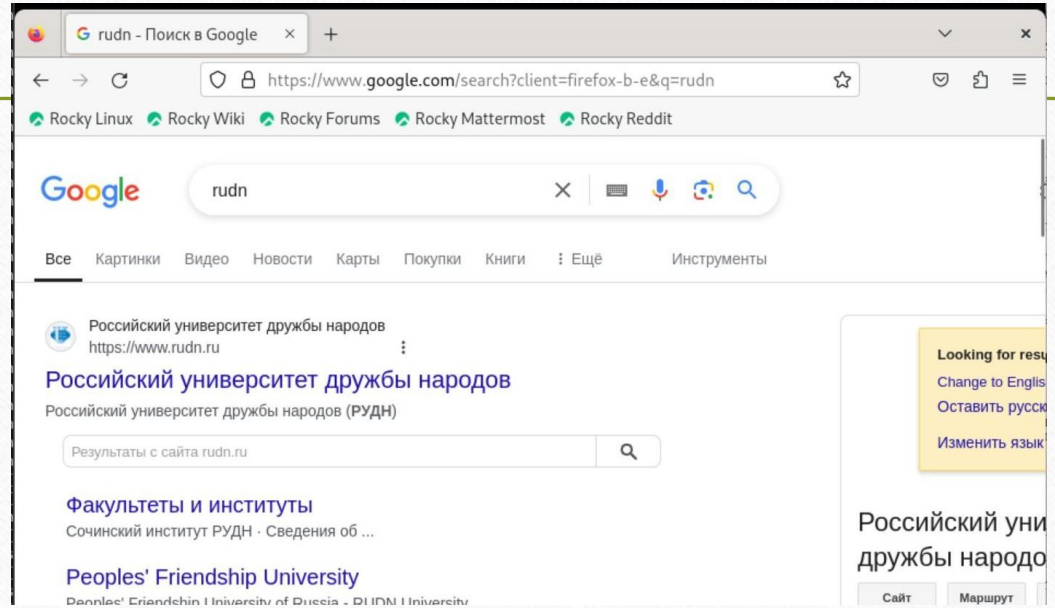

Рис. 3.3. Проверка доступности выхода в Интернет на клиенте.

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
[user@server.user.net server]$ cd /vagrant/provision/server
[user@server.user.net server]$ touch firewall.sh
[user@server.user.net server]$ chmod +x firewall.sh
[user@server.user.net server]$
```

Рис. 4.1. Открытие каталога для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога firewall, в который помещаем в соответствующие подкаталоги конфигурационные файлы FirewallD. Создание в каталоге /vagrant/provision/server файла firewall.sh.

Внесение изменений в настройки внутреннего окружения виртуальной машины

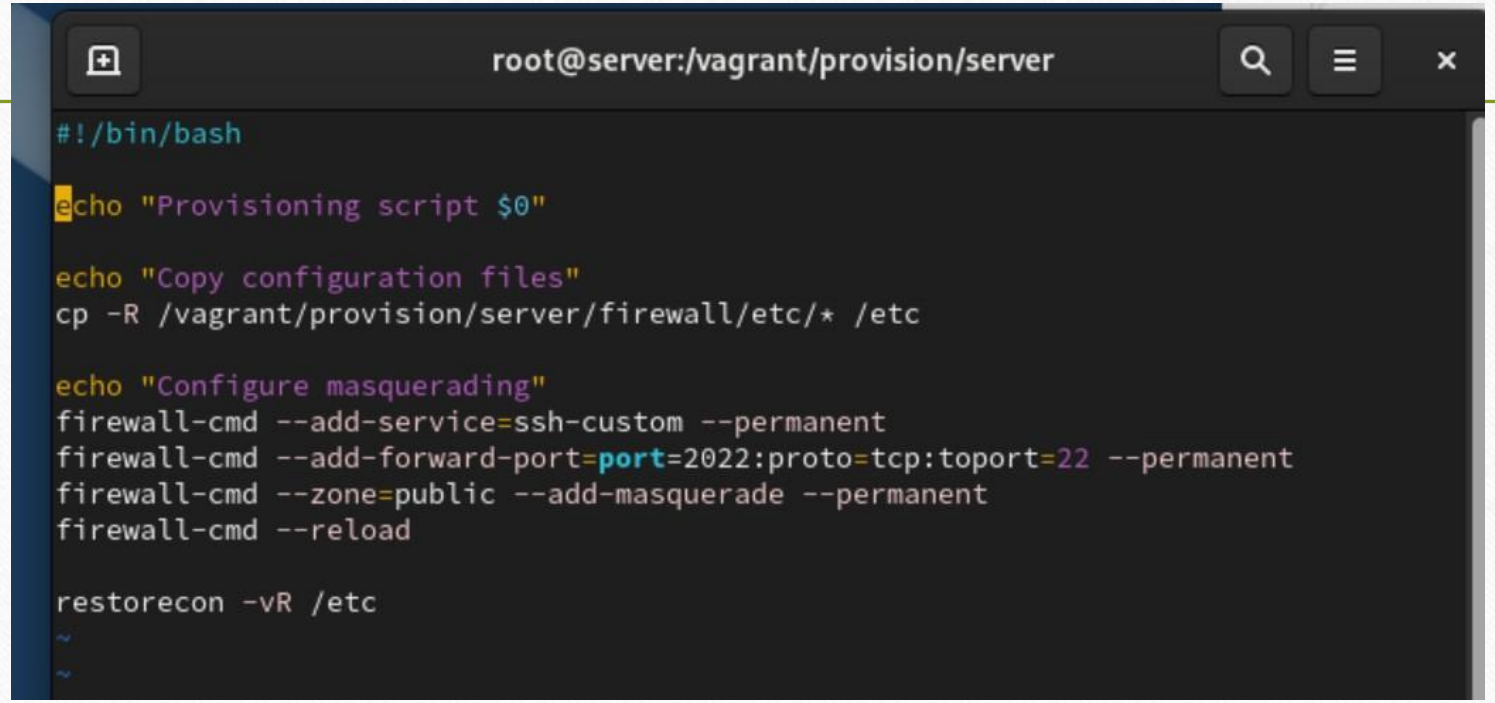

Рис. 4.2. Открытие файла на редактирование и прописывание в нём скрипта из лабораторной работы.

Внесение изменений в настройки внутреннего окружения виртуальной машины

Fichier Modifier Affichage

```
                    preserve_order: true,
                    path: "provision/server/dns.sh"

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

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

Рис. 4.3. Добавление записи в конфигурационном файле Vagrantfile.

Вывод

В ходе выполнения лабораторной работы были получены навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

Спасибо за внимание!