Лабораторная работа №7

Администрирование сетевых подсистем

Ищенко Ирина НПИбд-02-22

Российский университет дружбы народов, Москва, Россия

Цель работы

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

Выполнение лабораторной работы

```
root@server:/etc/firewalld/services

[ioithenko@server ~]$ sudo -i
[sudo] password for ioithenko:
[root@server ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom
.xml
[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 accessing yo
ur 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 services]#
```

Рис. 1: Создание собственного файла описания службы и просмотр

Рис. 2: Редактирование файла описания службы

root@server:/etc/firewalld/services

```
-server zabbix-agent zabbix-server zerotier
[root@server services]# firewall-cmd --get-services | grep ssh
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcups
d 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-ex
porter 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-registr
y docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman forema
n-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication 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 kdeconnec
t kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane k
ube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodep
ort-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 mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-w
bt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard 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 ps2
link ps3netsrv ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bin
d rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp s
mtp-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 sysl
og syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client v
dsm 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
[root@server services]#
```

Рис. 3: Список доступных служб

```
root@server:/etc/firewalld/services
success
[root@server services]# firewall-cmd --get-services | grep ssh
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcups
d 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-ex
porter 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-registr
y docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman forema
n-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication 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 kdeconnec
t kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane k
ube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodep
ort-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 mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-w
bt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard 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 ps2
link ps3netsrv ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bin
d rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp s
mtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squ
id ssdp ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay s
ynergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client up
np-client vdsm vnc-server warpinator wbem-http wbem-https wireguard ws-discovery ws-discov
ery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp
-local xmpp-server zabbix-agent zabbix-server zerotier
[root@server services]#
```

Рис. 4: Новая служба в списке доступных служб

```
[root@server services]# firewall-cmd --list-services | grep ssh
cockpit dhcp dhcpv6-client dns http https ssh
[root@server services]# firewall-cmd --add-service=ssh-custom
success
[root@server services]# firewall-cmd --list-services | grep ssh
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server services]# firewall-cmd --reload
success
[root@server services]#
```

Рис. 5: Добавление новой службы и просмотр списка активных служб, сохранение информации о состоянии

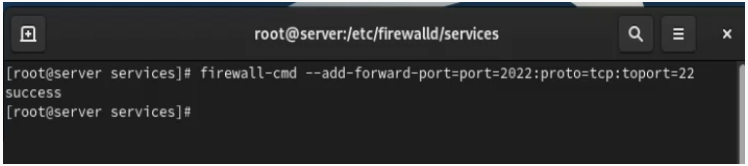

Рис. 6: Переадресация

```
ioithenko@server:~
[ioithenko@client ~]$ ssh -p 2022 ioithenko@server.ioithenko.net
The authenticity of host '[server.ioithenko.net]:2022 ([192.168.1.1]:2022)' can'
t be established.
ED25519 key fingerprint is SHA256:Thye46E17svni0fMP0tToWzEFseVN0KvqNQRg3jfWCY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[server.ioithenko.net]:2022' (ED25519) to the list o
f known hosts.
ioithenko@server.ioithenko.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Wed Oct 16 16:12:26 2024
[ioithenko@server ~]$
```

Рис. 7: Доступ по SSH к серверу через порт 2022 на клиенте

root@server:/etc/firewalld/services

```
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
```

Рис. 8: Возможность перенаправления пакетов

Рис. 9: Включение перенаправления пакетов и включение маскарадинга

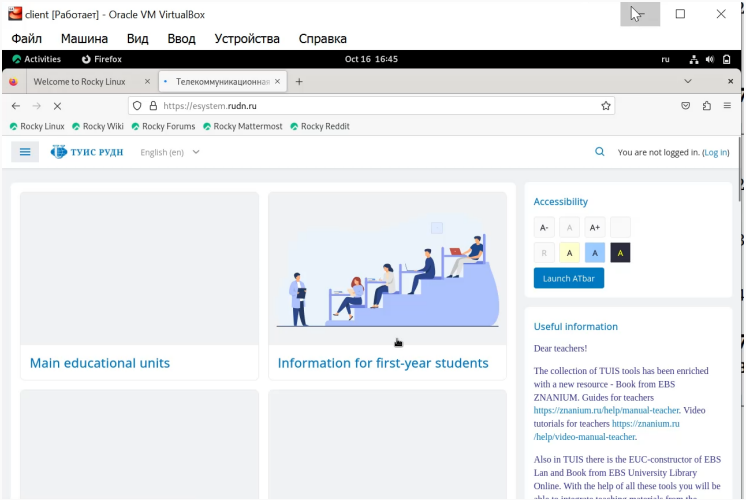

Рис. 10: Браузер клиента

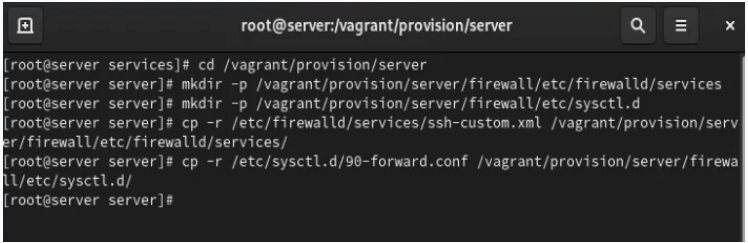

Рис. 11: Внесение изменений в настройки внутреннего окружения

firewall – Блокнот

Файл Правка Формат Вид Справка

```
#!/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. 12: Создание скрипта firewall.sh

*Vagrantfile – Блокнот

Файл Правка Формат Вид Справка

```
    server.vm.provision "server dns",
                        type: "shell",
                        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"


    server.vm.provider :virtualbox do |v|
      v.linked_clone = true
```

Рис. 13: Vagrantfile

Вывод

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