

Лабораторная работа

Номер 7

Кобзев Д. К.

Содержание

1 Цель работы	5
2 Выполнение лабораторной работы	6
3 Выводы	12
Список литературы	13

Список иллюстраций

2.1	Создание пользовательской службы firewalld	6
2.2	Файл ssh-custom.xml	6
2.3	FirewallD	7
2.4	Новая служба FirewallD	7
2.5	Попытка получить доступ по SSH к серверу через порт 2022	8
2.6	Настройка Port Forwarding и Masquerading	9
2.7	Внесение изменений в настройки внутреннего окружения виртуальной машины	9
2.8	Файл firewall.sh	10
2.9	Vagrantfile	11

Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

На виртуальной машине server переходим в режим суперпользователя. На основе существующего файла описания службы ssh создаем файл с собственным описанием. Смотрим содержимое файла службы (Рис. 12.1).

```
[dkkobzev@server.dkkobzev.net ~]$ sudo -i
[sudo] password for dkkobzev:
[root@server.dkkobzev.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.dkkobzev.net ~]# cd /etc/firewalld/services/
[root@server.dkkobzev.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>
```

Рис. 2.1: Создание пользовательской службы firewalld

Открываем файл описания службы на редактирование и заменяем порт 22 на новый порт (2022) (Рис. 12.2).

```
GNU nano 8.1                               /etc/firewalld/services/ssh-custom.xml                         Modified
<?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="2022"/>
</service>
```

Рис. 2.2: Файл ssh-custom.xml

Смотрим список доступных FirewallD служб. Перегружаем правила межсетевого экрана с сохранением информации о состоянии и вновь выводим на экран список служб, а также список активных служб (Рис. 12.3).

```
[root@server.dkkobzev.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-1600 anno-1800 apcupsd as
eqnet audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bit
coin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilizat
ion-v cockpit collected condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpcv6 dhcpcv6-client distcc dns dns-
over-quic dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger fo
reman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia
-master git gpd grafana gre high-availability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc
ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-c
ontrol-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-sc
heduler kube-scheduler-secure kube-worker kubelite kubelite-readonly kubelite-worker ldap ldaps libvirt libvirt-tls lightning-n
etwork llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft minidlna mnbspd mongodb mosh mountd m
pd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-
0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmweba
pis pop3 pop3s postgresql privoxy prometheus-prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmast
er quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samb
a-dc sane settlers-history-collection sip sips slimevr slp smtp smtp-submission smtpev snmp snmpstls snmpstls-trap snmptrap spi
deroak-lansync spotify-sync squid ssdp ssh statsrv steam-steam-transfer steam-streaming stellaris stronghold-crusader stun stu
ns submission supertuxkart svdp svn syncthing syncthing-gui syncthing-relay synergy sysconlan syslog syslog-tls telnet tent
acle terraria tftp tile38 tinc tor-socks transmission-client turn turns upnp-client vdsm vnc-server vrrp warpinator wbem-htt
p wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd wsdd-http w
sman wsmans xmpp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper
zabbix-web-service zero-k zerotier
[root@server.dkkobzev.net services]# firewall-cmd --reload
success
[root@server.dkkobzev.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-1600 anno-1800 apcupsd as
eqnet audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bit
coin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilizat
ion-v cockpit collected condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpcv6 dhcpcv6-client distcc dns dns-
over-quic dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger fo
reman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia
-master git gpd grafana gre high-availability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc
ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-c
ontrol-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-sc
heduler kube-scheduler-secure kube-worker kubelite kubelite-readonly kubelite-worker ldap ldaps libvirt libvirt-tls lightning-n
etwork llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft minidlna mnbspd mongodb mosh mountd m
pd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-
0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmweba
pis pop3 pop3s postgresql privoxy prometheus-prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmast
er quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samb
a-dc sane settlers-history-collection sip sips slimevr slp smtp smtp-submission smtpev snmp snmpstls snmpstls-trap snmptrap spi
deroak-lansync spotify-sync squid ssdp ssh ssh-custom statsrv steam-steam-transfer steam-streaming stellaris stronghold-crusader stun stu
ns submission supertuxkart svdp svn syncthing syncthing-gui syncthing-relay synergy sysconlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmission-client turn turns upnp-client vdsm vnc-server vrrp warpinat
or wbem-https wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd
wsdd-http wsmans wsmans xmpp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zab
bix-trapper zabbix-web-service zero-k zerotier
[root@server.dkkobzev.net services]# firewall-cmd --list-services
bash: i firewall-cmd: command not found...
[root@server.dkkobzev.net services]# firewall-cmd --list-services
cockpit dhcp dhcpcv6-client dns http https ssh ssh-custom
```

Рис. 2.3: FirewallD

Добавляем новую службу в FirewallD и выводим на экран список активных служб.

Перегружаем правила межсетевого экрана с сохранением информации о состоянии.

Организовываем на сервере переадресацию с порта 2022 на порт 22 (Рис. 12.4).

```
[root@server.dkkobzev.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.dkkobzev.net services]# firewall-cmd --list-services
cockpit dhcp dhcpcv6-client dns http https ssh ssh-custom
[root@server.dkkobzev.net services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server.dkkobzev.net services]# firewall-cmd --reload
success
[root@server.dkkobzev.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
```

Рис. 2.4: Новая служба FirewallD

На клиенте пробуем получить доступ по SSH к серверу через порт 2022 (Рис. 12.5).

```
[dkkobzev@client.dkkobzev.net ~]$ ssh -p 2022 dkkobzev@server.dkkobzev.net
The authenticity of host '[server.dkkobzev.net]:2022 ([192.168.1.1]:2022)' can't
be established.
ED25519 key fingerprint is SHA256:ojSX0quIcjPcc9AvXCBuNpJ3b3MEfv5V1xb0cURU564.
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.dkkobzev.net]:2022' (ED25519) to the list of
known hosts.
dkkobzev@server.dkkobzev.net's password:
Web console: https://server.dkkobzev.net:9090/ or https://192.168.1.1:9090/
Last login: Thu Oct 23 08:20:53 2025
```

Рис. 2.5: Попытка получить доступ по SSH к серверу через порт 2022

На сервере смотрим, активирована ли в ядре системы возможность перенаправления IPv4-пакетов пакетов. Включаем перенаправление IPv4-пакетов на сервере. Включаем маскарадинг на сервере (Рис. 12.6).

```

-----
[root@server.dkkobzev.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.dkkobzev.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.dkkobzev.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.dkkobzev.net services]# i firewall-cmd --zone=public --add-masquerade --permanent
bash: i firewall-cmd: command not found...
[root@server.dkkobzev.net services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.dkkobzev.net services]# firewall-cmd --reload
success

```

Рис. 2.6: Настройка Port Forwarding и Masquerading

На виртуальной машине server переходим в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создаем в нём каталог `firewall`, в который помещаем в соответствующие подкаталоги конфигурационные файлы `FirewallD`. В каталоге `/vagrant/provision/server` создаем файл `firewall.sh` (Рис. 12.7).

```

[root@server.dkkobzev.net services]# cd /vagrant/provision/server
[root@server.dkkobzev.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@server.dkkobzev.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server.dkkobzev.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewall/etc/firewalld/services/
[root@server.dkkobzev.net server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sysctl.d/
[root@server.dkkobzev.net server]# cd /vagrant/provision/server
[root@server.dkkobzev.net server]# touch firewall.sh
[root@server.dkkobzev.net server]# chmod +x firewall.sh

```

Рис. 2.7: Внесение изменений в настройки внутреннего окружения виртуальной машины

Прописываем скрипт в firewall.sh (Рис. 12.8).

```
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
```

Рис. 2.8: Файл firewall.sh

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавляем в разделе конфигурации для сервер (Рис. 12.9).

The screenshot shows a code editor window titled "Vagrantfile". The file contains configuration for a virtual machine named "server". It includes settings for boot timeout, SSH, network, provider (VirtualBox), and various provisioning scripts for dummy, dns, dhcp, http, mysql, and firewall services.

```
server.vm.boot_timeout = 1440

server.ssh.insert_key = false
server.ssh.username = 'vagrant'
server.ssh.password = 'vagrant'

server.vm.network :private_network,
  ip: "192.168.1.1",
  virtualbox_intnet: true

server.vm.provider :virtualbox do |virtualbox|
  virtualbox.customize ["modifyvm", :id, "--vrde", "on"]
  virtualbox.customize ["modifyvm", :id, "--vrdeport", "3344"]
end

server.vm.provision "server dummy",
  type: "shell",
  preserve_order: true,
  path: "provision/server/01-dummy.sh"
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"
```

Рис. 2.9: Vagrantfile

3 Выводы

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

Список литературы