Лабораторная работа

Номер 7

Кобзев Д. К.

Содержание

Список иллюстраций

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 secu
re 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 sec
  <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).

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 dhcpv6-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]# irewall-cmd --zone=public --add-masquerade --permanent
bash: irewall-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/firew
alld/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).

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).

Vagrantfile

Изменить Просмотр

```
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", "33
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