Лабораторная работа
Номер 7

Кобзев Д. К.
Российский университет дружбы народов, Москва, Россия
5 декабря 2025

Информация

Докладчик

- Кобзев Дмитрий Константинович
- Студент
- Российский университет дружбы народов
- НПИбд-01-23

Цель работы

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

Создание пользовательской службы firewalld

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. 1: Создание пользовательской службы firewalld

Создание пользовательской службы firewalld

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

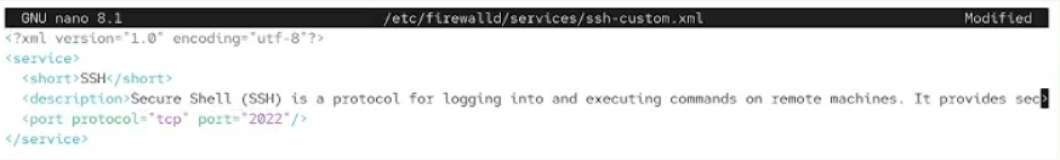

Рис. 2: Файл ssh-custom.xml

Создание пользовательской службы firewalld

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).

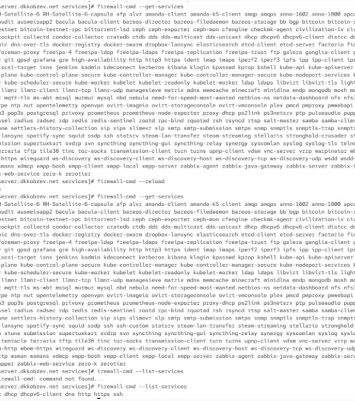

Рис. 3: FirewallD

Создание пользовательской службы 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. 4: Новая служба FirewallD

Перенаправление портов

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

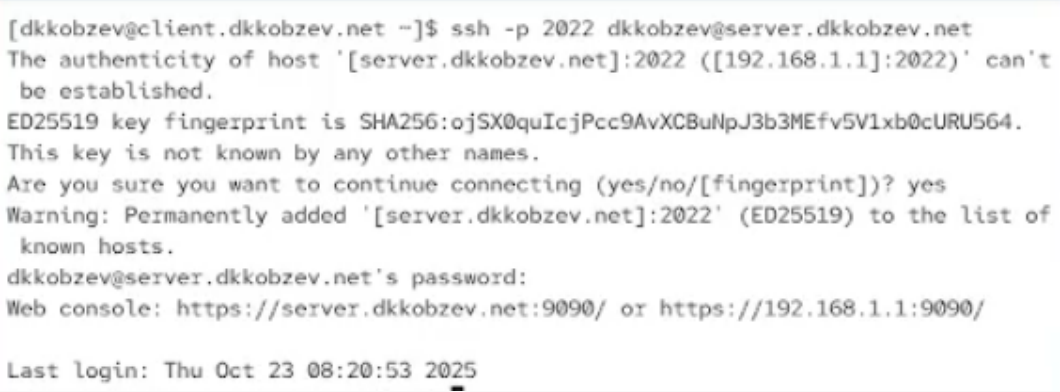

Рис. 5: Попытка получить доступ по SSH к серверу через порт 2022

Настройка Port Forwarding и Masquerading

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).

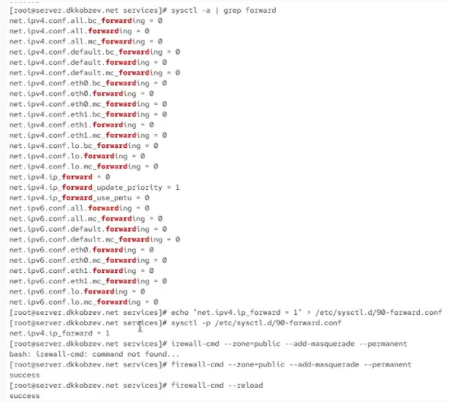

Рис. 6: Настройка Port Forwarding и Masquerading

Внесение изменений в настройки внутреннего окружения виртуальной машины

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. 7: Внесение изменений в настройки внутреннего окружения виртуальной машины

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. 8: Файл firewall.sh

Внесение изменений в настройки внутреннего окружения виртуальной машины

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

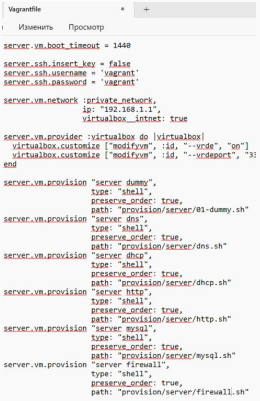

Рис. 9: Vagrantfile

Выводы

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