

МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра МО ЭВМ

ОТЧЕТ
по лабораторной работе №3
по дисциплине «Сети и телекоммуникации»
Тема: Использование межсетевого экрана ОС Linux

Студент гр. 7383

Левкович Д.В.

Преподаватель

Фирсов М.А.

Санкт-Петербург

2019

Цель работы.

Научиться создавать, удалять и изменять правила межсетевого экрана iptables (настройка блокировки трафика, разрешения принятия трафика, логгирования приходящих пакетов).

Задачи.

0. На всех машинах запустить скрипт toscrath.sh. Проверить, что таблицы ядра пусты.

1. Заблокировать доступ по IP-адресу Ub1 к Ub3.

2. Заблокировать доступ по порту X на Ub1.

3. Заблокировать доступ к порту X на Ub3 от UbR. Проверить возможность доступа с Ub1.

4. Полностью запретить доступ к Ub3. Разрешить доступ к порту X.

5. С помощью правила по умолчанию обеспечить блокировку всех входящих и исходящих пакетов узла Ub3, исключая пакеты управления сетью (протокол ICMP). Убедиться, что Ub3 принимает и отвечает на запросы команды ping, но не отвечает на запросы протокола TCP.

6. Запретить подключение к Ub1 по порту X. Настроить логгирование попыток подключения по порту X.

7. Заблокировать доступ по порту X к Ub3 с Ub1 по его MAC-адресу.

8. Полностью закрыть доступ к Ub1. Разрешить доступ для Ub3 к Ub1, используя диапазон портов X.

9. Разрешить только одно ssh подключение к UbR.

Вариант заданий.

Вариант заданий указан в табл. 1.

Таблица 1 – Вариант заданий

Вар.\Задание	2	3	4	6	7	8
	X=	X=	X=	X=	X=	X=
10	30	80	30	80	20	20-80

Ход работы.

0. На каждой машине был запущен скрипт toscratch.sh. Для проверки того, что таблицы каждой машины пусты, была введена команда:

iptables -L

Вывод в консоли представлен на рис.1. По нему видно, что таблицы пусты.

```
ubuntu1 login: stud
Password:
Last login: Sun Nov  3 04:08:58 EST 2019 on tty1
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

55 packages can be updated.
27 updates are security updates.

stud@ubuntu1:~$ sudo su ubuntu1:~$
[sudo] password for stud:
root@ubuntu1:/home/stud# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
root@ubuntu1:/home/stud# ping 192.168.56.107
PING 192.168.56.107 (192.168.56.107) 56(84) bytes of data.
^C
--- 192.168.56.107 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5000ms
root@ubuntu1:/home/stud# _

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:820 errors:0 dropped:0 overruns:0 frame:0
TX packets:820 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:61100 (61.1 KB) TX bytes:61100 (61.1 KB)

root@ubuntu3:/home/stud#
192.168.1.3 gw reboot
192.168.172.0/30 ifconfig REJECT
192.168.175.189 INPUT route
192.168.56.106 IP -s
192.169.56.106 iptables -t
-A -j sudo
add -L -t
cd ls tcpdump
default nano ./toscratch.sh
DROP -net ./ULAN/task3/ub3/task3-v1.sh
/etc/network/interfaces -p ULAN/task3/ub3/task3-v1.sh
filter ping
root@ubuntu3:/home/stud# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
DROP all -- 192.168.56.106 anywhere
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
root@ubuntu3:/home/stud#
```

Рисунок 1 – Вывод консоли после выполнения команды чтения таблиц ядра

1. Для блокировки доступа по IP-адресу Ub1 к Ub3 на Ub3 была введена команда:

iptables -t filter -A INPUT -s 192.168.56.106 -j DROP,

где 192.168.56.106 – IP-адрес Ub1, который можно узнать с помощью команды ifconfig. В результате этой команды Ub1 не имеет доступа к Ub3, что видно при попытке отправить пакет с Ub1 на Ub3 командой ping, как показано на рис. 2.

```
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:22 errors:0 dropped:0 overruns:0 frame:0
TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:8405 (8.4 KB) TX bytes:2058 (2.0 KB)

lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:65536 Metric:1
      RX packets:5792 errors:0 dropped:0 overruns:0 frame:0
      TX packets:5792 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1
      RX bytes:429344 (429.3 KB) TX bytes:429344 (429.3 KB)

root@ubuntu1:/home/stud#
192.168.1.0/30      exit          -netmask
192.168.1.3         gw           ping
192.168.1.4         ifconfig     reboot
192.168.174.3       iptables     route
255.255.252.0       -I           tcpdump
add                ls           ./tscratch.sh
default            nano
/etc/network/interfaces -net
root@ubuntu1:/home/stud# ping 192.168.56.107
PING 192.168.56.107 (192.168.56.107) 56(84) bytes of data.
From 192.168.56.107: icmp_seq=1 Destination Port Unreachable
From 192.168.56.107: icmp_seq=2 Destination Port Unreachable
From 192.168.56.107: icmp_seq=3 Destination Port Unreachable
From 192.168.56.107: icmp_seq=4 Destination Port Unreachable
From 192.168.56.107: icmp_seq=5 Destination Port Unreachable
From 192.168.56.107: icmp_seq=6 Destination Port Unreachable
^C
--- 192.168.56.107 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5012ms

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

root@ubuntu3:/home/stud# ifconfig
emp0s3  Link encap:Ethernet HWaddr 08:00:27:94:da:76
        inet addr:192.168.56.107 Bcast:192.168.56.255 Mask:255.255.255.0
        inet6 addr: fe80:a00:27ff:fe94:da76/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:35 errors:0 dropped:0 overruns:0 frame:0
        TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:12752 (12.7 KB) TX bytes:2058 (2.0 KB)

lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:65536 Metric:1
      RX packets:7076 errors:0 dropped:0 overruns:0 frame:0
      TX packets:7076 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1
      RX bytes:524412 (524.4 KB) TX bytes:524412 (524.4 KB)
```

Рисунок 2 – Запрет входящий пакетов от Ub1 на Ub3

2. Для блокировки доступа по порту 30 на Ub1 была выполнена команда `iptables -A INPUT -p tcp -dport 30 -j REJECT`. Результат показан на рис. 3.

```
root@ubuntu1:/home/stud# iptables -A INPUT -p tcp --dport 30 -j REJECT
root@ubuntu1:/home/stud# telnet localhost 30
Trying ::1...
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
root@ubuntu1:/home/stud# _

n: Command not found
root@ubuntu3:/home/stud# telnet 192.168.56.106 30
Trying 192.168.56.106...
telnet: Unable to connect to remote host: Connection timed out
root@ubuntu3:/home/stud#
root@ubuntu3:/home/stud#
```

Рисунок 3 – Блокировка по порту 30 на Ub1.

3. Для блокировки доступа по порту 80 UbR к Ub3 была выполнена команда, показанная на рис. 4. Также на рис. 4 показано, что доступа от UbR нет, однако у Ub1 к Ub3 доступ есть.

```
Chain OUTPUT (policy ACCEPT)
target prot opt source destination

root@ubuntu3:/home/stud# nc -l -p 80
nc: Address already in use
root@ubuntu3:/home/stud#

?Invalid command
telnet> quit
Connection closed.
root@ubuntu1:/home/stud# nc -zv 192.168.56.107 80
Connection to 192.168.56.107 port [tcp/http] succeeded!
root@ubuntu1:/home/stud# _

RX bytes:3595856 (3.5 MB) TX bytes:3595856 (3.5 MB)
root@ubuntu1:/home/stud#
root@ubuntu1:/home/stud# nc -zv 192.168.56.107 80
nc: connect to 192.168.56.107 port 80 (tcp) failed: Connection refused
root@ubuntu1:/home/stud#
```

Рисунок 4 – Запрет доступа UbR к Ub3 по порту 80

4. Для полной блокировки доступа на Ub3 была введена команда:

`Iptables -t filter -P INPUT DROP`.

Для разрешения доступа по порту 30 была введена команда:

`Iptables -t filter -A INPUT -p tcp --dport 30 -j ACCEPT`.

Таблица ядра и проверка соединения представлены на рис. 5.

```
root@ubuntu3:/home/stud# iptables -L
Chain INPUT (policy DROP)
target prot opt source destination
ACCEPT tcp -- anywhere anywhere tcp dpt:30

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
root@ubuntu3:/home/stud# _

root@ubuntu1:/home/stud# nc -zv 192.168.56.107 30
Connection to 192.168.56.107 30 port [tcp/*] succeeded!
root@ubuntu1:/home/stud#
root@ubuntu1:/home/stud#
root@ubuntu1:/home/stud#
root@ubuntu1:/home/stud#
root@ubuntu1:/home/stud#
root@ubuntu1:/home/stud#
root@ubuntu1:/home/stud#
root@ubuntu1:/home/stud#
```

Рисунок 5 – Запрет доступа на Ub3 и разрешение по порту 30

Рисунок 8 – Запрет доступа и разрешения по диапазону портов

9. Для запрета более 1 подключения по ssh, была введена команда, показанная на рис 9.

```
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
LOG        tcp  -- anywhere             anywhere
REJECT     tcp  -- anywhere             anywhere
--
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
--
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@ubuntu1:/home/stud# ssh stud@192.168.56.108
The authenticity of host '192.168.56.108 (192.168.56.108)' can't be established.
LOG ECDSA key fingerprint is SHA256:4JsbUSxW15d197h+am185F3dK0KosL/rev8Sdvz4UYY.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.56.108' (ECDSA) to the list of known hosts.
stud@192.168.56.108's password:
Permission denied, please try again.
stud@192.168.56.108's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

55 packages can be updated.
27 updates are security updates.

Last login: Sun Nov  3 13:14:03 2019
stud@ubuntu1:/home/stud#
```

Рисунок 9 – Запрет более одного соединения по ssh

Выводы.

В процессе выполнения данной лабораторной работы были изучены создание, удаление и изменение правил межсетевого экрана iptables (настройка блокировки трафика, разрешения принятия трафика, логгирования приходящих пакетов).