

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

ОТЧЕТ
по лабораторной работе №7
по дисциплине «Сети и телекоммуникации»
ТЕМА: СЕТЕВЫЕ ЭКРАНЫ. IPTABLES

Студентка гр. 2384

Соц Е.А.

Преподаватель

Борисенко К.А.

Санкт-Петербург

2024

Цель работы

Целью работы является изучение принципов работы с сетевыми экранами. Необходимо решить следующие задачи:

1. Создать три виртуальные машины (лаб. работа № 1).
2. Научиться блокировать и разрешать прием и отправку пакетов с помощью iptables, настраивать логирование событий

Задания

Для выполнения лабораторной работы необходимо настроить три виртуальные машины Ub1, Ub2 и Ub3 так, чтобы они находились в одной подсети. Кроме того, для некоторых пунктов необходимо установить дополнительные службы на виртуальные машины: apache2, ftpd – и выполнить следующие задачи:

1. Заблокировать доступ по IP-адресу ПК Ub1 к Ub3. Продемонстрировать результаты с попыткой подключения Ub1 и Ub2 к Ub3.
2. Заблокировать доступ по 21-му порту на Ub1. Продемонстрировать возможность доступа по ssh на Ub1 и невозможность доступа по 21-му порту.
3. Разрешить доступ только по ssh на Ub2. Предоставить результат.
4. Запретить ICMP-запросы на IP-адрес 8.8.8.8 двумя способами. Необходимо создать два правила: в цепочке INPUT и цепочке OUTPUT. С помощью Wireshark на хосте нужно продемонстрировать разницу между двумя способами блокировки и сделать вывод о том, какой вариант эффективнее.
5. Полностью запретить доступ к Ub3. Разрешить доступ по ICMP протоколу.

6. Запретить подключение к Ub1 по порту 80. Настроить логирование попыток подключения по 80-му порту. Продемонстрировать результаты логирования.

7. Заблокировать доступ по 80-му порту к Ub3 с Ub1 по его МАС-адресу. Продемонстрировать результат, сменить МАС-адрес на Ub3 и продемонстрировать успешное подключение к Ub3 по 80-му порту.

8. Полностью закрыть доступ к Ub1. Разрешить доступ для Ub3 к Ub1, используя диапазон портов 20–79. В результате необходимо показать невозможность подключения к 80 порту и возможность – к ssh или ftp.

9. Разрешить только одно ssh-подключение к Ub3. Продемонстрировать результат попытки подключения с Ub2 при наличии открытой ssh-сессии с Ub1 к Ub3.

Выполнение работы

На машинах были выполнены следующие сетевые настройки:

```
katya@katyavm:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:82:9a:84
        inet addr:172.20.10.13  Bcast:172.20.10.15  Mask:255.255.255.240
        inet6 addr: fe80::a00:27ff:fe82:9a84/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:13 errors:0 dropped:0 overruns:0 frame:0
        TX packets:17 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:2708 (2.7 KB)  TX bytes:1870 (1.8 KB)

lo      Link encap:Локальная петля (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:160 errors:0 dropped:0 overruns:0 frame:0
        TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)
```

Рис. 1 – UB1

```
katya@katyavm:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:ce:92:b3
        inet addr:172.20.10.12  Bcast:172.20.10.15  Mask:255.255.255.240
        inet6 addr: fe80::a00:27ff:fece:92b3/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:9 errors:0 dropped:0 overruns:0 frame:0
        TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1874 (1.8 KB)  TX bytes:1720 (1.7 KB)

lo      Link encap:Локальная петля (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:160 errors:0 dropped:0 overruns:0 frame:0
        TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)
```

Рис. 2 – UB2

```

katya@katyavm:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:a3:86:03
        inet addr:172.20.10.14 Bcast:172.20.10.15 Mask:255.255.255.240
        inet6 addr: fe80::a00:27ff:fea3:8603/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:242 errors:0 dropped:0 overruns:0 frame:0
        TX packets:171 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:307991 (307.9 KB)  TX bytes:12170 (12.1 KB)

lo      Link encap:Локальная петля (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:160 errors:0 dropped:0 overruns:0 frame:0
        TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)

katya@katyavm:~$

```

Рис. 3 – UB3

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

Для блокировки доступа по IP-адресу Ub1 к Ub3 с использованием iptables на Ub3, нужно добавить правило, которое отбрасывает все пакеты, приходящие с IP-адреса Ub1.

Было добавлено правило Ub3 в цепочку INPUT для блокировки всего трафика с IP-адреса Ub1:

```
sudo iptables -A INPUT -s 172.20.10.13 -j DROP
```

```

Обрабатываются триггеры для dnw (0.35-ubuntu12) ...
katya@katyavm:~$ ping 172.20.10.14
PING 172.20.10.14 (172.20.10.14) 56(84) bytes of data.
^C
--- 172.20.10.14 ping statistics ---
58 packets transmitted, 0 received, 100% packet loss, time 57455ms

katya@katyavm:~$

```

Рис. 4 – ub1 → ub3

```

Обрабатываются триггеры для iptw (0.35-Ubuntu2) ...
katya@katyavm:~$ ping 172.20.10.14
PING 172.20.10.14 (172.20.10.14) 56(84) bytes of data.
64 bytes from 172.20.10.14: icmp_seq=1 ttl=64 time=0.394 ms
64 bytes from 172.20.10.14: icmp_seq=2 ttl=64 time=0.247 ms
64 bytes from 172.20.10.14: icmp_seq=3 ttl=64 time=0.393 ms
64 bytes from 172.20.10.14: icmp_seq=4 ttl=64 time=0.298 ms
64 bytes from 172.20.10.14: icmp_seq=5 ttl=64 time=0.256 ms
^C
--- 172.20.10.14 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms

```

Рис. 5 – ub2 → ub3

2. Заблокировать доступ по 21-му порту на Ub1.

Продемонстрировать возможность доступа по ssh на Ub1 и невозможность доступа по 21-му порту.

На Ub1 применена следующая команда для блокировки доступа по 21-му порту:

```
sudo iptables -A INPUT -p tcp --dport 21 -j DROP
```

Эта команда добавляет правило в цепочку INPUT, которое отбрасывает все пакеты, приходящие на 21-й порт (FTP).

На другой машине (например, Ub2) попытка подключиться к Ub1 по 21-му порт:

```

katya@katyavm:~$ ftp 172.20.10.13
ftp: connect: Connection timed out
ftp>

```

Рис. 6 – Подключение к Ub1 по 21 порту

На другой машине (например, Ub2) попытка подключиться к Ub1 по SSH:

```
katya@katyavm:~$ ssh 172.20.10.13
The authenticity of host '172.20.10.13 (172.20.10.13)' can't be established.
ECDSA key fingerprint is SHA256:MkZCKFBjJL18Kvt+3kUCrkoeIieKqPs0LcGd6fFCmAE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.20.10.13' (ECDSA) to the list of known hosts.
katya@172.20.10.13's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-186-generic x86_64)

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

Могут быть обновлены 114 пакетов.
80 обновлений касаются безопасности системы.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Dec 17 22:27:48 2024
katya@katyavm:~$
```

Рис. 7 – Подключение к Ub1 по 22 порту

3. Разрешить доступ только по ssh на Ub2. Предоставить результат.

На Ub2 выполнены следующие команды для разрешения доступа только по SSH (22-й порт) и блокировки всех остальных портов:

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

```
sudo iptables -A INPUT -j DROP
```

На другой машине (например, Ub1) попытка подключиться к Ub2 по SSH:

```

katya@katyavm:~$ sudo iptables -F
katya@katyavm:~$ ssh 172.20.10.12
The authenticity of host '172.20.10.12 (172.20.10.12)' can't be established.
ECDSA key fingerprint is SHA256:MkZCKFBjJL18KVt+3kUCrkoeIieKqPs0LcGd6fFCmAE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.20.10.12' (ECDSA) to the list of known hosts.
katya@172.20.10.12's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-186-generic x86_64)

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

Могут быть обновлены 114 пакетов.
80 обновлений касаются безопасности системы.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Dec 17 23:03:15 2024
katya@katyavm:~$

```

Рис. 9 – Подключение к Ub2 по ssh

На другой машине (например, Ub3) попытка подключиться к Ub2 по другим портам, например, по 80-му порту (HTTP):

```

katya@katyavm:~$ curl http://172.20.10.12
^C
katya@katyavm:~$ ping 172.20.10.12
PING 172.20.10.12 (172.20.10.12) 56(84) bytes of data.
^C
--- 172.20.10.12 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4032ms

```

Рис. 10 – Подключение к Ub2 по 80 порту

4. Запретить ICMP-запросы на IP-адрес 8.8.8.8 двумя способами. Необходимо создать два правила: в цепочке INPUT и цепочке OUTPUT. С помощью Wireshark на хосте нужно продемонстрировать разницу между двумя способами блокировки и сделать вывод о том, какой вариант эффективнее.

Добавлено правило для блокировки исходящих ICMP-запросов:

sudo iptables -A OUTPUT -p icmp -d 8.8.8.8 -j DROP


```

katya@katyavm:~$ sudo iptables -A OUTPUT -p icmp -d 8.8.8.8 -j DROP
katya@katyavm:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 4999ms

```

Рис. 11 – Блокировка исходящих

Вторым способом было добавлено правило для блокировки входящих ICMP-ответов:

sudo iptables -A INPUT -p icmp -s 8.8.8.8 -j DROP

```

Last login: Tue Dec 17 23:04:05 2024 from 172.20.10.12
katya@katyavm:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
19 packets transmitted, 0 received, 100% packet loss, time 18144ms
katya@katyavm:~$ _

```

```

katya@katyavm:~$ sudo tcpdump -p icmp -i enp0s3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
3:32:04.882781 IP 172.20.10.13 > dns.google: ICMP echo request, id 12188, seq 6, length 64
3:32:04.915811 IP dns.google > 172.20.10.13: ICMP echo reply, id 12188, seq 6, length 64
3:32:05.890476 IP 172.20.10.13 > dns.google: ICMP echo request, id 12188, seq 7, length 64
3:32:06.231910 IP dns.google > 172.20.10.13: ICMP echo reply, id 12188, seq 7, length 64
3:32:06.898580 IP 172.20.10.13 > dns.google: ICMP echo request, id 12188, seq 8, length 64
3:32:06.925875 IP dns.google > 172.20.10.13: ICMP echo reply, id 12188, seq 8, length 64
3:32:07.906556 IP 172.20.10.13 > dns.google: ICMP echo request, id 12188, seq 9, length 64
3:32:07.936954 IP dns.google > 172.20.10.13: ICMP echo reply, id 12188, seq 9, length 64
3:32:08.914226 IP 172.20.10.13 > dns.google: ICMP echo request, id 12188, seq 10, length 64
3:32:08.932617 IP dns.google > 172.20.10.13: ICMP echo reply, id 12188, seq 10, length 64
3:32:09.922301 IP 172.20.10.13 > dns.google: ICMP echo request, id 12188, seq 11, length 64
3:32:09.963614 IP dns.google > 172.20.10.13: ICMP echo reply, id 12188, seq 11, length 64
3:32:10.930550 IP 172.20.10.13 > dns.google: ICMP echo request, id 12188, seq 12, length 64
3:32:10.964570 IP dns.google > 172.20.10.13: ICMP echo reply, id 12188, seq 12, length 64
3:32:11.938477 IP 172.20.10.13 > dns.google: ICMP echo request, id 12188, seq 13, length 64
3:32:11.965608 IP dns.google > 172.20.10.13: ICMP echo reply, id 12188, seq 13, length 64
3:32:12.946344 IP 172.20.10.13 > dns.google: ICMP echo request, id 12188, seq 14, length 64
3:32:12.968559 IP dns.google > 172.20.10.13: ICMP echo reply, id 12188, seq 14, length 64
3:32:13.954459 IP 172.20.10.13 > dns.google: ICMP echo request, id 12188, seq 15, length 64
3:32:13.972670 IP dns.google > 172.20.10.13: ICMP echo reply, id 12188, seq 15, length 64
^C
0 packets captured

```

Рис. 12 – Блокировка входящих

Блокировка в цепочке OUTPUT:

- Пакеты ICMP не отправляются вообще.

- В tcpdump пакеты не покидают машину.
- Этот способ эффективен, если необходимо запретить отправку ICMP-запросов на конкретный IP-адрес.

Блокировка в цепочке INPUT:

- Пакеты ICMP отправляются, но ответы блокируются.
- В tcpdump пакеты отправляются и получают ответ, но ответы не доходят до машины.
- Этот способ эффективен, если необходимо разрешить отправку запросов, но запретить получение ответов.

5. Полностью запретить доступ к Ub3. Разрешить доступ по ICMP протоколу.

Разрешение доступа по ICMP-протоколу:

```
sudo iptables -A INPUT -p icmp -j ACCEPT
```

Блокировка всех остальных входящих соединений:

```
sudo iptables -A INPUT -j DROP
```

```
katya@katyavm:~$ sudo iptables -F
katya@katyavm:~$ ping 172.20.10.14
PING 172.20.10.14 (172.20.10.14) 56(84) bytes of data.
64 bytes from 172.20.10.14: icmp_seq=1 ttl=64 time=0.229 ms
64 bytes from 172.20.10.14: icmp_seq=2 ttl=64 time=0.396 ms
64 bytes from 172.20.10.14: icmp_seq=3 ttl=64 time=0.377 ms
64 bytes from 172.20.10.14: icmp_seq=4 ttl=64 time=0.256 ms
64 bytes from 172.20.10.14: icmp_seq=5 ttl=64 time=0.836 ms
64 bytes from 172.20.10.14: icmp_seq=6 ttl=64 time=0.215 ms
^C
--- 172.20.10.14 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.215/0.384/0.836/0.214 ms
katya@katyavm:~$ _
```

Рис. 13 – Прохождение icmp

```
katya@katyavm:~$ ssh katya@172.20.10.14
^C
katya@katyavm:~$
```

```
katya@katyavm:~$ ftp 172.20.10.14
ftp: connect: Connection timed out
ftp> _
```

Рис. 14 – Блокировка остальных

6. Запретить подключение к Ub1 по порту 80. Настроить логирование попыток подключения по 80-му порту. Продемонстрировать результаты логирования.

Настройка логирования попыток подключения по 80-му порту:

```
sudo iptables -A INPUT -p tcp --dport 80 -j LOG --log-prefix
```

"HTTP_DROP: "

Запрет подключения по 80-му порту:

```
sudo iptables -A INPUT -p tcp --dport 80 -j DROP
```

Попробуем подключиться к порту с другой машины:

```
katya@katyavm:~$ sudo iptables -F
katya@katyavm:~$ curl 172.20.10.13
curl: (7) Failed to connect to 172.20.10.13 port 80: Время ожидания соединения истекло
katya@katyavm:~$ _
```

Рис. 15 – Подключение к 80 порту с другой машины

```
katya@katyavm:~$ ssh katya@172.20.10.14
^C
katya@katyavm:~$ sudo iptables -F
katya@katyavm:~$ sudo iptables -A INPUT -p tcp --dport 80 -j LOG --log-prefix "HTTP_DROP:"
katya@katyavm:~$ sudo iptables -A INPUT -p tcp --dport 80 -j DROP
katya@katyavm:~$ sudo tail -f /var/log/syslog | grep "HTTP_DROP"
Dec 17 23:48:53 katyavm kernel: [ 4972.811716] HTTP_DROP:IN=enp0s3 OUT= MAC=08:00:27:82:9a:84:08:00:
27:a3:86:03:08:00 SRC=172.20.10.14 DST=172.20.10.13 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=42 DF PROTO=
TCP SPT=37176 DPT=80 WINDOW=29200 RES=0x00 SYN URG=0
Dec 17 23:48:57 katyavm kernel: [ 4976.819864] HTTP_DROP:IN=enp0s3 OUT= MAC=08:00:27:82:9a:84:08:00:
27:a3:86:03:08:00 SRC=172.20.10.14 DST=172.20.10.13 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=43 DF PROTO=
TCP SPT=37176 DPT=80 WINDOW=29200 RES=0x00 SYN URG=0
Dec 17 23:49:05 katyavm kernel: [ 4984.835625] HTTP_DROP:IN=enp0s3 OUT= MAC=08:00:27:82:9a:84:08:00:
27:a3:86:03:08:00 SRC=172.20.10.14 DST=172.20.10.13 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=44 DF PROTO=
TCP SPT=37176 DPT=80 WINDOW=29200 RES=0x00 SYN URG=0
Dec 17 23:49:18 katyavm kernel: [ 4997.877230] HTTP_DROP:IN=enp0s3 OUT= MAC=08:00:27:82:9a:84:08:00:
27:a3:86:03:08:00 SRC=172.20.10.14 DST=172.20.10.13 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=9357 DF PROTO=
TCP SPT=37178 DPT=80 WINDOW=29200 RES=0x00 SYN URG=0
Dec 17 23:49:19 katyavm kernel: [ 4998.875158] HTTP_DROP:IN=enp0s3 OUT= MAC=08:00:27:82:9a:84:08:00:
27:a3:86:03:08:00 SRC=172.20.10.14 DST=172.20.10.13 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=9358 DF PROTO=
TCP SPT=37178 DPT=80 WINDOW=29200 RES=0x00 SYN URG=0
Dec 17 23:49:21 katyavm kernel: [ 5000.879181] HTTP_DROP:IN=enp0s3 OUT= MAC=08:00:27:82:9a:84:08:00:
27:a3:86:03:08:00 SRC=172.20.10.14 DST=172.20.10.13 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=9359 DF PROTO=
TCP SPT=37178 DPT=80 WINDOW=29200 RES=0x00 SYN URG=0
Dec 17 23:49:25 katyavm kernel: [ 5004.883023] HTTP_DROP:IN=enp0s3 OUT= MAC=08:00:27:82:9a:84:08:00:
27:a3:86:03:08:00 SRC=172.20.10.14 DST=172.20.10.13 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=9360 DF PROTO=
TCP SPT=37178 DPT=80 WINDOW=29200 RES=0x00 SYN URG=0
Dec 17 23:49:33 katyavm kernel: [ 5012.898818] HTTP_DROP:IN=enp0s3 OUT= MAC=08:00:27:82:9a:84:08:00:
27:a3:86:03:08:00 SRC=172.20.10.14 DST=172.20.10.13 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=9361 DF PROTO=
TCP SPT=37178 DPT=80 WINDOW=29200 RES=0x00 SYN URG=0
Dec 17 23:49:49 katyavm kernel: [ 5028.914321] HTTP_DROP:IN=enp0s3 OUT= MAC=08:00:27:82:9a:84:08:00:
27:a3:86:03:08:00 SRC=172.20.10.14 DST=172.20.10.13 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=9362 DF PROTO=
TCP SPT=37178 DPT=80 WINDOW=29200 RES=0x00 SYN URG=0
Dec 17 23:50:21 katyavm kernel: [ 5060.977341] HTTP_DROP:IN=enp0s3 OUT= MAC=08:00:27:82:9a:84:08:00:
27:a3:86:03:08:00 SRC=172.20.10.14 DST=172.20.10.13 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=9363 DF PROTO=
TCP SPT=37178 DPT=80 WINDOW=29200 RES=0x00 SYN URG=0
```

Рис. 16 – Лог Ub1

7. Заблокировать доступ по 80-му порту к Ub3 с Ub1 по его MAC адресу. Продемонстрировать результат, сменить MAC-адрес на Ub3 и продемонстрировать успешное подключение к Ub3 по 80-му порту.

Сначала был определен MAC-адрес Ub1:

```
ip link show
```

MAC-адрес Ub1

```
link/ether 08:00:27:82:9a:84 brd ff:ff:ff:ff:ff:ff
```

Блокировка доступа по 80-му порту с Ub1 по его MAC-адресу:

Выполнена следующая команда на Ub3:

```
sudo iptables -A INPUT -p tcp --dport 80 -m mac --mac-source  
08:00:27:82:9a:84 -j DROP
```

Проверка доступа по 80-му порту:

```
katya@katyavm:~$ curl 172.20.10.14  
curl: (7) Failed to connect to 172.20.10.14 port 80: Время ожидания соединения истекло  
katya@katyavm:~$ _
```

Рис. 17 – Доступность порта 80

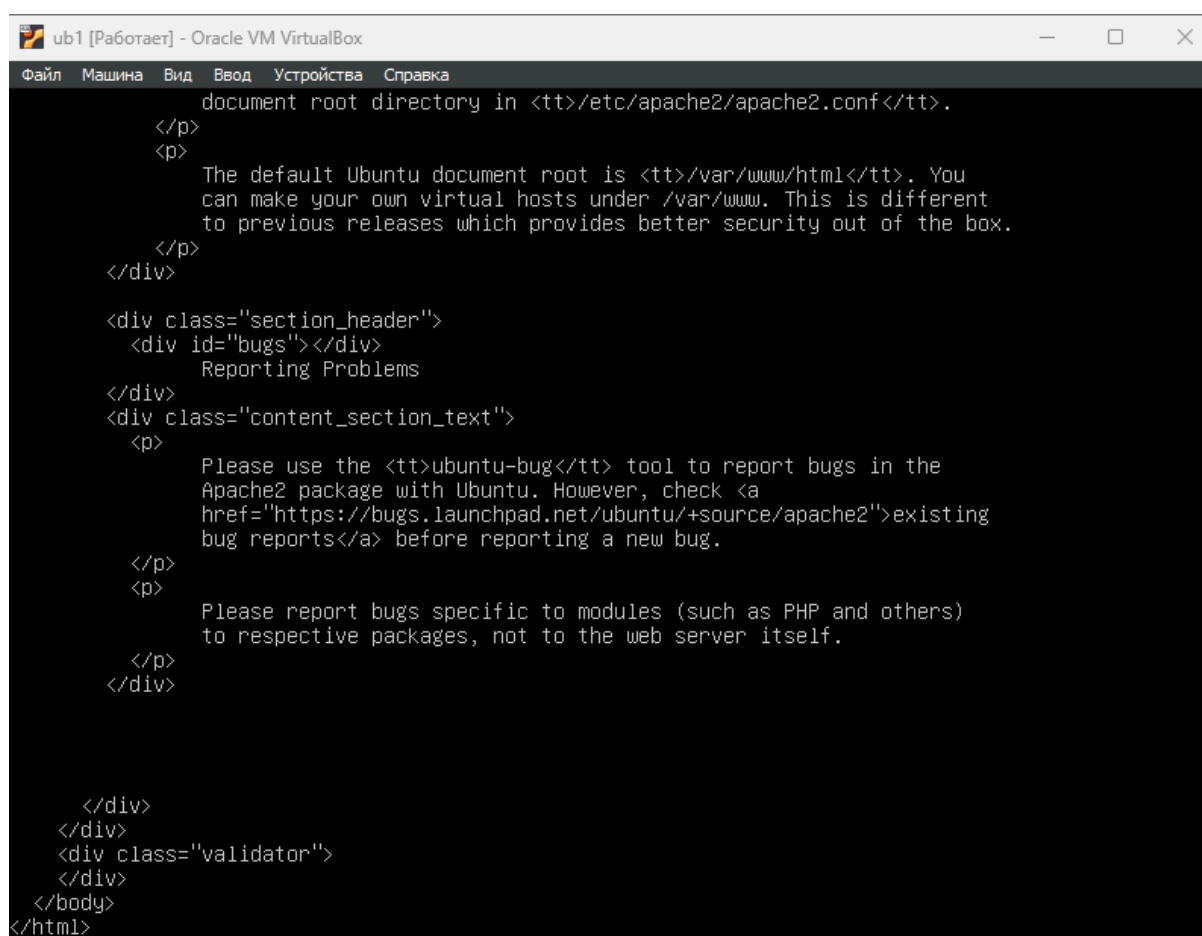
Теперь же сменим mac address ub1:

```
sudo ifconfig enp0s3 down
```

```
sudo ifconfig enp0s3 hw ether 08:00:27:00:00:01
```

```
sudo ifconfig enp0s3 up
```

И попробуем еще раз получить доступ к 80 порту:



```
document root directory in <tt>/etc/apache2/apache2.conf</tt>.
</p>
<p>
  The default Ubuntu document root is <tt>/var/www/html</tt>. You
  can make your own virtual hosts under /var/www. This is different
  to previous releases which provides better security out of the box.
</p>
</div>

<div class="section_header">
  <div id="bugs"></div>
  Reporting Problems
</div>
<div class="content_section_text">
  <p>
    Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
    Apache2 package with Ubuntu. However, check <a
    href="https://bugs.launchpad.net/ubuntu/+source/apache2">existing
    bug reports</a> before reporting a new bug.
  </p>
  <p>
    Please report bugs specific to modules (such as PHP and others)
    to respective packages, not to the web server itself.
  </p>
</div>

</div>
</div>
<div class="validator">
</div>
</body>
</html>
```

Рис. 18 – Доступность порта 80 с другого адреса

8. Полностью закрыть доступ к Ub1. Разрешить доступ для Ub3 к Ub1, используя диапазон портов 20–79. В результате необходимо показать невозможность подключения к 80 порту и возможность – к ssh или ftp.

Разрешение доступа для Ub3 в диапазоне портов 20–79:

IP-адрес Ub3 — 172.20.10.14 Выполнена следующая команда на Ub1:

```
sudo iptables -A INPUT -s 172.20.10.14 -p tcp --dport 20:79 -j ACCEPT
```

Блокировка всех входящих соединений:

```
sudo iptables -A INPUT -j DROP
```

Проверка доступа к портам 20–79 с Ub3:

```
katya@katyavm:~$ ssh 172.20.10.13
katya@172.20.10.13's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-186-generic x86_64)

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

Могут быть обновлены 114 пакетов.
80 обновлений касаются безопасности системы.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Dec 17 23:31:34 2024 from 172.20.10.12
katya@katyavm:~$
```

Рис. 19 – Доступность портов

Проверка доступа к порту 80 с Ub3:

```
katya@katyavm:~$ curl 172.20.10.13
curl: (7) Failed to connect to 172.20.10.13 port 80: Время ожидания соединения истекло
katya@katyavm:~$
```

Рис. 20 – Доступность 80 порта

Проверка доступа с других машин:

На другой машине (например, Ub2) попытка подключиться к Ub1 по порту 22 (SSH):

```
[sadas] пароль для katya
katya@katyavm:~$ ssh 172.20.10.13
ssh: connect to host 172.20.10.13 port 22: Connection timed out
katya@katyavm:~$
```

Рис. 21 – Доступность ssh с другой машины

9. Разрешить только одно ssh-подключение к Ub3.

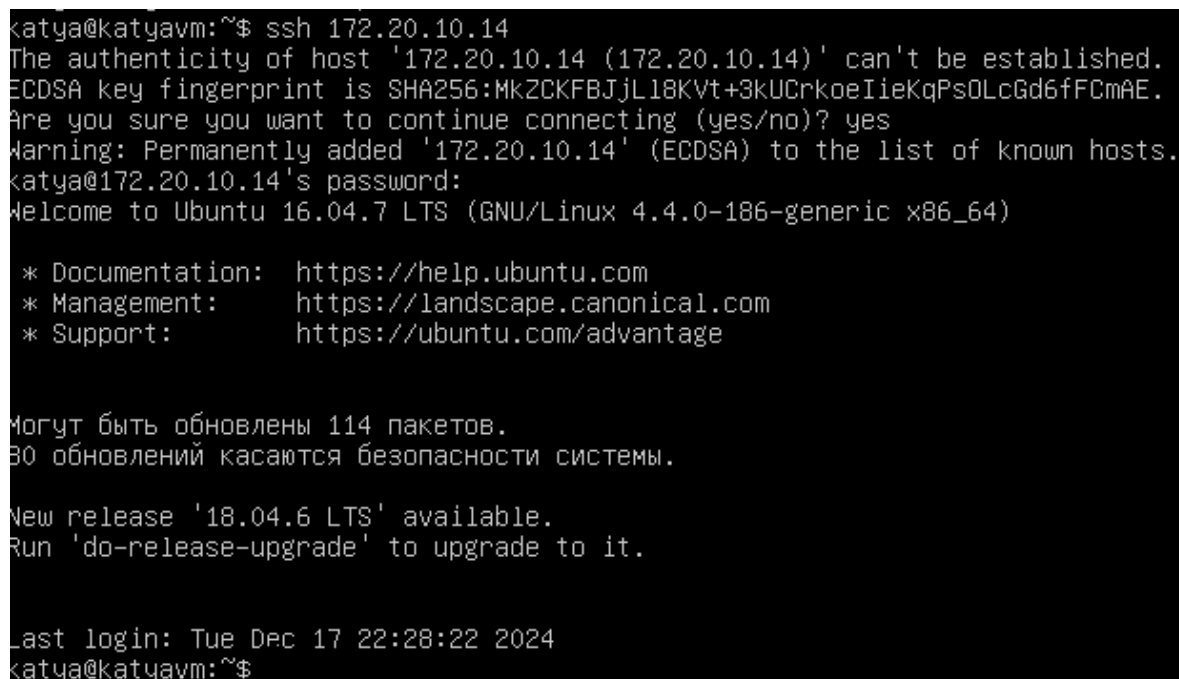
Продемонстрировать результат попытки подключения с Ub2 при наличии открытой ssh-сессии с Ub1 к Ub3.

Разрешение только одного SSH-подключения:

Выполнена следующая команда на Ub3, чтобы разрешить только одно SSH-подключение:

```
sudo iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m connlimit --connlimit-above 1 -j REJECT
```

Проверка SSH-подключения с Ub1:



```
katya@katyavm:~$ ssh 172.20.10.14
The authenticity of host '172.20.10.14 (172.20.10.14)' can't be established.
ECDSA key fingerprint is SHA256:MkZCKFBJjL18Kvt+3kUCrkoeIieKqPsOLcGd6fFCmAE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.20.10.14' (ECDSA) to the list of known hosts.
katya@172.20.10.14's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-186-generic x86_64)

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

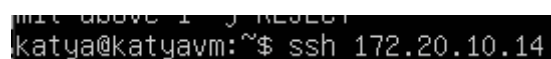
Могут быть обновлены 114 пакетов.
30 обновлений касаются безопасности системы.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Dec 17 22:28:22 2024
katya@katyavm:~$
```

Рис. 21 – Первое ssh подключение

Проверка SSH-подключения с Ub2:



```
katya@katyavm:~$ ssh 172.20.10.14
```

Рис. 22 – Второе ssh подключение

Вывод

В ходе лабораторной работы были изучены принципы работы с сетевыми экранами. На практике были созданы три виртуальные машины, на которых была продемонстрирована непосредственная работа настроек iptables при приеме и отправке пакетов.