Национальный исследовательский университет информационных технологий,
механики и оптики
Кафедра вычислительной техники
Сети ЭВМ и телекоммуникации

Лабораторная работа №4
«Основы сетевого администрирования локальной сети»

Работу выполнил студент группы P3315
Халанский Дмитрий

2016

1. Цели работы

- Изучить основные сетевые утилиты GNU/Linux;
- Изучить основные понятия маршрутизации;
- Научиться создавать простые брендмауэры на основе `iptables(8)`.

2. Исходные данные

Количество букв в фамилии 9

Количество букв в имени 7

Количество букв в отчестве 12

Суммарное Количество букв в ФИО $9 + 7 + 12 = 28$

IP-адрес А `10.9.7.12`

IP-адрес Б `10.9.7.34`

Порт netcat $20000 + 28 = 20028$

Протокол netcat $9 \equiv 1 \mod 2 \Rightarrow$ TCP

Максимальный размер $700 + 28 = 728$

Максимальный TTL 28

3. Ход работы

3.1. Создание и запуск

Машина А:

```
root@host01:~# uname -a
Linux host01 3.16.0-4-586 #1 Debian 3.16.7-ckt25-2 (2016-04-08) i686 GNU/Linux
```

Машина Б:

```
root@host02:~# uname -a
Linux host02 3.16.0-4-586 #1 Debian 3.16.7-ckt25-2 (2016-04-08) i686 GNU/Linux
```

3.2. Установка адресов

После создания NAT-сети `10.9.7.0/24` и добавления в неё машин в Virtualbox,

```
root@host01:~# ip a show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:92:13:a5 brd ff:ff:ff:ff:ff:ff
    inet 10.9.7.4/24 brd 10.9.7.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe92:13a5/64 scope link
       valid_lft forever preferred_lft forever
root@host01:~# ip a del 10.9.7.4/24 dev eth0
root@host01:~# ip a add 10.9.7.12/24 dev eth0
root@host01:~# ip a show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:92:13:a5 brd ff:ff:ff:ff:ff:ff
    inet 10.9.7.12/24 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe92:13a5/64 scope link
       valid_lft forever preferred_lft forever
```

После проведения аналогичных действий на машине Б,

```
root@host01:~# ping -c 5 10.9.7.34
PING 10.9.7.34 (10.9.7.34) 56(84) bytes of data.
64 bytes from 10.9.7.34: icmp_seq=1 ttl=64 time=0.669 ms
64 bytes from 10.9.7.34: icmp_seq=2 ttl=64 time=0.585 ms
64 bytes from 10.9.7.34: icmp_seq=3 ttl=64 time=0.633 ms
64 bytes from 10.9.7.34: icmp_seq=4 ttl=64 time=0.703 ms
64 bytes from 10.9.7.34: icmp_seq=5 ttl=64 time=0.778 ms

--- 10.9.7.34 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.585/0.673/0.778/0.071 ms
```

3.3. Проверка путей маршрутизации

Машина А:

```
root@host01:~# ip r show dev eth0
10.9.7.0/24  proto kernel  scope link  src 10.9.7.12
```

Машина Б:

```
root@host02:~# ip r show dev eth0
10.9.7.0/24  proto kernel  scope link  src 10.9.7.34
```

3.4. Редактирование путей маршрутизации

Машина А:

```
root@host01:~# ip r add 192.169.0.35 via 10.9.7.34 src 10.9.7.12 dev eth0
root@host01:~# ip r
10.9.7.0/24 dev eth0  proto kernel  scope link  src 10.9.7.12
192.168.56.0/24 dev eth1  proto kernel  scope link  src 192.168.56.10
192.169.0.35 via 10.9.7.34 dev eth0  src 10.9.7.12
root@host01:~# ip r del 192.169.0.35 via 10.9.7.34 src 10.9.7.12 dev eth0
```

Предположим, что машина Б имеет доступ к внешней сети — к примеру, к адресу `192.169.0.35` — а машина А не имеет. Прописав такой путь, мы позволяем ей обращаться к требуемой машине, передавая запрос через машину Б.

3.5. Работа с `netcat`

3.5.1. «Б» как сервер

Машина Б в роли сервера:

```
root@host02:~# nc -lp 20028
Халанский
```

Машина А в роли клиента:

```
root@host01:~# nc 10.9.7.12 20028
Халанский
```

3.5.2. «А» как сервер

Машина А в роли сервера:

```
root@host01:~# nc -lp 20028
Дмитрий
```

Машина Б в роли клиента:

```
root@host02:~# nc 10.9.7.12 20028
Дмитрий
```

3.6. Настройка firewall

После каждого подраздела на обеих машинах выполняется `iptables -F`.

3.6.1. Запрет передачи на порт 20028

На машине Б:

```
root@host02:~# nc -lp 20028
```

На машине А:

```
root@host01:~# iptables -I OUTPUT -p tcp --dport 20028 -j DROP
root@host01:~# nc 10.9.7.34 20028
Халанский
```

На машине Б в консоли не должно появиться моей фамилии.

3.6.2. Запрет приёма с порта 20028

На машине А:

```
root@host01:~# iptables -I INPUT -p tcp --sport 20028 -j DROP
root@host01:~# nc -lp 20028
Халанский
root@host01:~# nc -lp 20028
```

На машине Б:

```
root@host02:~# nc -p 20027 10.9.7.12 20028
Халанский
root@host02:~# nc -p 20028 10.9.7.12 20028
Халанский?
```

3.6.3. Запрет приёма от А

На машине Б:

```
root@host02:~# iptables -I INPUT -s 10.9.7.12 -j DROP
```

Тогда на машине А:

```
root@host01:~# ping -c 5 10.9.7.34
PING 10.9.7.34 (10.9.7.34) 56(84) bytes of data.

--- 10.9.7.34 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4000ms
```

3.6.4. Запрет отсылки на Б

На машине А:

```
root@host01:~# iptables -I OUTPUT -d 10.9.7.34 -j DROP
root@host01:~# ping -c 5 10.9.7.34
PING 10.9.7.34 (10.9.7.34) 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

--- 10.9.7.34 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 3999ms
```

3.6.5. Сложное задание

На машине А:

```
root@host01:~# iptables -I INPUT  -m ttl --ttl-gt 28 \
        -m length --length 728:65535
root@host01:~# iptables -I OUTPUT -m ttl --ttl-gt 28 \
        -m length --length 728:65535
```

4. Анекдот

Сидит мать программиста, смотрит телевизор. Вдруг она осознаёт, что её сын сидит в ванной уже больше часа. Её это насторожило. Через полчаса она начала паниковать. Стучится в дверь — оттуда молчание. Дёргает за ручку — закрыто. Мать в ужасе зовёт отца, тот выламывает дверь.

Картина: сидит программист, волос на голове почти не осталось, и сосредоточенно намыливает шампунем голову.

Мать его спрашивает:

— Ты что делаешь, дурак?

Тот оскорблённо говорит:

— Голову мою.

Показывает на бутылку шампуня, где написано:

1. Взять небольшое количество шампуня;
2. 3-5 минут намыливать волосы;
3. Тщательно смыть шампунь;
4. Повторить.