Министерство образования и науки
Санкт-Петербургский политехнический университет Петра Великого
Институт компьютерных наук и кибербезопасности
Высшая школа технологий искусственного интеллекта
Направление 02.03.01 Математика и компьютерные науки

Л А Б О Р А Т О Р Н А Я Р А Б О Т А № 2

Анализ пакетного трафика

по дисциплине «Сети ЭВМ и телекоммуникации компьютерных сетей»

Выполнил студент гр. 5130201/10101 _____ Кондраев Дмитрий Евгеньевич
Проверил _____ Мулюха Владимир Александрович

Санкт-Петербург
2024

1 Постановка задачи

В процессе снятия дампа (`tcpdump`), выполнить следующие команды:

1. пропинговать указанный адрес,
2. выполнить трассировку к указанному адресу,
3. выполнить вход на указанный сайт.

Остановить снятие дампа. В отчете привести фрагменты дампа, содержащие запросы с объяснениями, почему именно такие фрагменты привели.

Выполнять `tcpdump` с ключами `-xx`, иначе будет слишком мало данных, чтобы понять, что это за пакеты в некоторых случаях. Записывать данные лучше или в raw файл (ключ `-w`), а потом читать оттуда (ключ `-r`), или перенаправлением вывода в файл, а уже потом "вырезать" из файла нужные фрагменты.

Привести схему сети, на которой выполнялась работа (свой ip-адрес, mac-адрес; mac-адрес и ip-адрес шлюза по умолчанию, а также ip-адреса всех серверов, к которым обращаетесь).

Вариант 8:

ping	tracert	web-доступ
ok.ru	google.com	spbstu.ru

2 Схема сети

Чтобы узнать требуемые адреса в локальной сети, используем команду `ip`:

```
$ ip -4 address show wlo1
2: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
 ↪  qlen 1000
    altname wlp0s12f0
    inet 192.168.1.164/24 brd 192.168.1.255 scope global dynamic noprefixroute wlo1
       valid_lft 40689sec preferred_lft 40689sec
$ ip -0 address show wlo1
2: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
 ↪  qlen 1000
    link/ether 6c:94:66:cb:ca:73 brd ff:ff:ff:ff:ff:ff
    altname wlp0s12f0
$ ip neigh
192.168.1.1 dev wlo1 lladdr d4:6e:0e:a9:04:ef REACHABLE
192.168.1.173 dev wlo1 lladdr 7c:f6:66:77:77:b9 STALE
fe80::d66e:eff:fea9:4ef dev wlo1 lladdr d4:6e:0e:a9:04:ef router STALE
```

Чтобы узнать адреса серверов, используем команду dig:

```
$ dig +short ok.ru
217.20.147.1
217.20.155.13
5.61.23.11
$ dig +short google.com
173.194.222.113
173.194.222.138
173.194.222.139
173.194.222.100
173.194.222.102
173.194.222.101
```

```
$ dig +short www.spbstu.ru
new.spbstu.ru.
portal-c.spbstu.ru.
178.154.244.120
```

Схема сети изображена на рисунке 1.

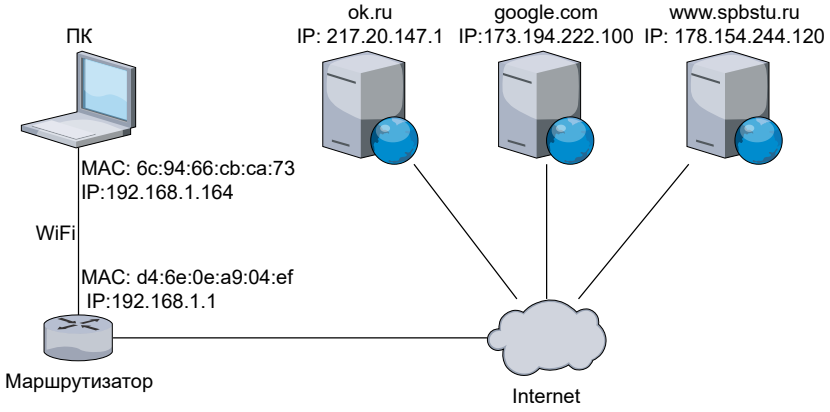

Рис. 1: Схема сети

3 Ход работы

Код скрипта для ping и traceroute:

```
#!/usr/bin/env bash
# не буферизовать пакеты, записывать в файл
tcpdump -U -w raw.pcap &
# запомнить номер процесса
pid=$!
# 2 echo-запроса
ping ok.ru -c 2
# Посылать одновременно 1 пакет, 1 пакет на хоп, использовать ICMP echo
traceroute --icmp --sim-queries=1 --queries=1 -n google.com
# завершить снятие дампа
kill $pid
```

Код скрипта для доступа к веб-серверу:

```
#!/usr/bin/env bash
tcpdump -U -w raw2.pcap &
pid=$!
sleep 1
curl www.spbstu.ru
sleep 2
kill $pid
```

Вывод скриптов:

```
$ chmod +x lab2.sh
$ sudo ./lab2.sh
dropped privs to tcpdump
tcpdump: listening on wlo1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
PING OK.ru (217.20.147.1) 56(84) bytes of data.
64 bytes from ip1.147.odnoklassniki.ru (217.20.147.1): icmp_seq=1 ttl=56 time=11.9 ms
64 bytes from ip1.147.odnoklassniki.ru (217.20.147.1): icmp_seq=2 ttl=56 time=13.8 ms

--- OK.ru ping statistics ---
```

```
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 11.852/12.801/13.751/0.949 ms
traceroute to google.com (173.194.222.100), 30 hops max, 60 byte packets
 1  192.168.1.1  1.187 ms
 2  *
 3  *
 4  93.100.0.122  3.177 ms
 5  *
 6  *
 7  72.14.216.110  3.865 ms
 8  74.125.244.129  3.441 ms
 9  74.125.244.133  1.952 ms
10  142.251.51.187  5.389 ms
11  172.253.51.187  6.115 ms
12  *
13  *
14  *
15  *
16  *
17  *
18  *
19  *
20  *
21  173.194.222.100  7.434 ms
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
117 packets captured
129 packets received by filter
0 packets dropped by kernel
```

4 Фильтрация захваченного трафика

Пакеты ICMP echo request и reply (команда `ping`):

```
$ tcpdump -n -r raw.pcap host ok.ru -XX
reading from file raw.pcap, link-type EN10MB (Ethernet), snapshot length 262144
22:31:01.829330 IP 192.168.1.164 > 217.20.147.1: ICMP echo request, id 4, seq 2, length 64
    0x0000:  d46e 0ea9 04ef 6c94 66cb ca73 0800 4500  .n....l.f..s..E.
    0x0010:  0054 8d25 4000 4001 7f21 c0a8 01a4 d914  .T.%@.@..!......
    0x0020:  9301 0800 c719 0004 0002 f5ff 0e66 0000  .............f..
    0x0030:  0000 61a7 0c00 0000 0000 1011 1213 1415  ..a.............
    0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  ...........!"#$%
    0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
    0x0060:  3637                                     67
22:31:01.843032 IP 217.20.147.1 > 192.168.1.164: ICMP echo reply, id 4, seq 2, length 64
    0x0000:  6c94 66cb ca73 d46e 0ea9 04ef 0800 4500  l.f..s.n......E.
    0x0010:  0054 07c7 0000 3801 4c80 d914 9301 c0a8  .T....8.L.......
    0x0020:  01a4 0000 cf19 0004 0002 f5ff 0e66 0000  .............f..
    0x0030:  0000 61a7 0c00 0000 0000 1011 1213 1415  ..a.............
    0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  ...........!"#$%
    0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
    0x0060:  3637                                     67
```

Приведены эти пакеты, т.к. у них совпадает адрес сервера 217.20.147.1 и протокол ICMP.

2 пакета, относящихся к `traceroute`:

```
$ $ tcpdump -r raw.pcap icmp and not host ok.ru -XX -c 2 -n
reading from file raw.pcap, link-type EN10MB (Ethernet), snapshot length 262144
22:31:01.848971 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 1,
 ↪  length 40
    0x0000:  d46e 0ea9 04ef 6c94 66cb ca73 0800 4500  .n....l.f..s..E.
    0x0010:  003c b309 0000 0101 b844 c0a8 01a4 adc2  .<.......D......
    0x0020:  de64 0800 51fc 307d 0001 4849 4a4b 4c4d  .d..Q.0}..HIJKLM
    0x0030:  4e4f 5051 5253 5455 5657 5859 5a5b 5c5d  NOPQRSTUVWXYZ[\]
    0x0040:  5e5f 6061 6263 6465 6667                 ^_`abcdefg
22:31:01.850111 IP 192.168.1.1 > 192.168.1.164: ICMP time exceeded in-transit, length 68
    0x0000:  6c94 66cb ca73 d46e 0ea9 04ef 0800 45c0  l.f..s.n......E.
    0x0010:  0058 5f38 0000 4001 96b7 c0a8 0101 c0a8  .X_8..@.........
    0x0020:  01a4 0b00 f4ff 0000 0000 4500 003c b309  ..........E··<..
    0x0030:  0000 0101 b844 c0a8 01a4 adc2 de64 0800  .....D.......d..
    0x0040:  51fc 307d 0001 4849 4a4b 4c4d 4e4f 5051  Q.0}..HIJKLMNOPQ
    0x0050:  5253 5455 5657 5859 5a5b 5c5d 5e5f 6061  RSTUVWXYZ[\]^_`a
    0x0060:  6263 6465 6667                           bcdefg
```

Приведены эти пакеты, т.к. у них совпадает адрес сервера 173.194.222.100 и протокол ICMP.

Краткий вывод по всем пакетам, относящимся к traceroute:

```
$ tcpdump -r raw.pcap icmp and not host ok.ru -n
reading from file raw.pcap, link-type EN10MB (Ethernet), snapshot length 262144
22:31:01.848971 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 1,
 ↪  length 40
22:31:01.850111 IP 192.168.1.1 > 192.168.1.164: ICMP time exceeded in-transit, length 68
22:31:01.850278 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 2,
 ↪  length 40
22:31:06.855578 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 3,
 ↪  length 40
22:31:11.860725 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 4,
 ↪  length 40
22:31:11.863772 IP 93.100.0.122 > 192.168.1.164: ICMP time exceeded in-transit, length 36
22:31:11.863953 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 5,
 ↪  length 40
22:31:16.868652 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 6,
 ↪  length 40
22:31:21.874201 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 7,
 ↪  length 40
22:31:21.877972 IP 72.14.216.110 > 192.168.1.164: ICMP time exceeded in-transit, length 68
22:31:21.878250 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 8,
 ↪  length 40
22:31:21.881651 IP 74.125.244.129 > 192.168.1.164: ICMP time exceeded in-transit, length 76
22:31:21.881866 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 9,
 ↪  length 40
22:31:21.883788 IP 74.125.244.133 > 192.168.1.164: ICMP time exceeded in-transit, length 36
22:31:21.884005 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 10,
 ↪  length 40
22:31:21.889364 IP 142.251.51.187 > 192.168.1.164: ICMP time exceeded in-transit, length 36
22:31:21.889623 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 11,
 ↪  length 40
22:31:21.895679 IP 172.253.51.187 > 192.168.1.164: ICMP time exceeded in-transit, length 76
22:31:21.895896 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 12,
 ↪  length 40
22:31:26.901436 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 13,
 ↪  length 40
22:31:31.906852 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 14,
 ↪  length 40
```

```
22:31:36.911674 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 15,
 ↪  length 40
22:31:41.916668 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 16,
 ↪  length 40
22:31:46.921770 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 17,
 ↪  length 40
22:31:51.927138 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 18,
 ↪  length 40
22:31:56.931553 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 19,
 ↪  length 40
22:31:58.325200 IP 185.37.128.62 > 192.168.1.164: ICMP time exceeded in-transit, length 36
22:32:01.935434 IP 192.168.1.164 > 173.194.222.100: ICMP echo request, id 12413, seq 20,
 ↪  length 40
```

Пакеты, относящиеся к доступу к web-серверу:

```
$ tcpdump -r raw2.pcap -n port http -S
reading from file raw2.pcap, link-type EN10MB (Ethernet), snapshot length 262144
00:01:42.821790 IP 192.168.1.164.33692 > 178.154.244.120.http: Flags [S], seq 2984481249,
 ↪  win 32120, options [mss 1460,sackOK,TS val 308150528 ecr 0,nop,wscale 7], length 0
00:01:42.841626 IP 178.154.244.120.http > 192.168.1.164.33692: Flags [S.], seq 68055806, ack
 ↪  2984481250, win 27960, options [mss 1410,sackOK,TS val 1649994911 ecr
 ↪  308150528,nop,wscale 9], length 0
00:01:42.841750 IP 192.168.1.164.33692 > 178.154.244.120.http: Flags [.], ack 68055807, win
 ↪  251, options [nop,nop,TS val 308150548 ecr 1649994911], length 0
00:01:42.841885 IP 192.168.1.164.33692 > 178.154.244.120.http: Flags [P.], seq
 ↪  2984481250:2984481326, ack 68055807, win 251, options [nop,nop,TS val 308150548 ecr
 ↪  1649994911], length 76: HTTP: GET / HTTP/1.1
00:01:42.861551 IP 178.154.244.120.http > 192.168.1.164.33692: Flags [.], ack 2984481326,
 ↪  win 55, options [nop,nop,TS val 1649994931 ecr 308150548], length 0
00:01:42.861654 IP 178.154.244.120.http > 192.168.1.164.33692: Flags [P.], seq
 ↪  68055807:68056221, ack 2984481326, win 55, options [nop,nop,TS val 1649994931 ecr
 ↪  308150548], length 414: HTTP: HTTP/1.1 301 Moved Permanently
00:01:42.861728 IP 192.168.1.164.33692 > 178.154.244.120.http: Flags [.], ack 68056221, win
 ↪  249, options [nop,nop,TS val 308150568 ecr 1649994931], length 0
00:01:42.862023 IP 192.168.1.164.33692 > 178.154.244.120.http: Flags [F.], seq 2984481326,
 ↪  ack 68056221, win 249, options [nop,nop,TS val 308150568 ecr 1649994931], length 0
00:01:42.881570 IP 178.154.244.120.http > 192.168.1.164.33692: Flags [F.], seq 68056221, ack
 ↪  2984481327, win 55, options [nop,nop,TS val 1649994951 ecr 308150568], length 0
00:01:42.881690 IP 192.168.1.164.33692 > 178.154.244.120.http: Flags [.], ack 68056222, win
 ↪  249, options [nop,nop,TS val 308150588 ecr 1649994951], length 0
```

Приведены эти пакеты, т.к. у них совпадает адрес сервера 178.154.244.120, используется порт 80 = http. Приведенные пакеты демонстрируют двухстороннее TCP подключение: трехстороннее рукопожатие (первые 3 пакета), передача запроса с подтверждением (следующие 2), передача ответа клиенту (следующие 2), четырехстороннее рукопожатие для закрытия соединений (последние 4).

Заключение

В ходе лабораторной работы были изучены команды для определения параметров сети, проверки наличия подключения (`ping`) и трассировки маршрутов (`traceroute`), а также получены навыки работы с программой сбора и анализа трафика `tcpdump`.

Для решения поставленых задач разработан bash-скрипт, выполняющий сбор трафика. Затем сохраненный в файл дамп прочитан и отфильтрован с помощью программы `traceroute -r`.