

МИНОБРНАУКИ РОССИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ИМ. Р.Е. АЛЕКСЕЕВА»
(НГТУ)**



Институт ИРИТ

Кафедра «Информатика и системы управления»

ОТЧЕТ

по лабораторной работе №5

Выполнил:

**Студент
группы 18-АС
Корнилов А.И**

Проверил:

Гай В.Е.

Отчет защищен с оценкой: _____

Дата защиты «___» _____ 20__ г.

Нижний Новгород

2021 год

Задание на лабораторную работу:

Работа с анализатором протоколов tcpdump

1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.

2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов воспользоваться утилитой ping.

4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Результат работы программы писать в файл.

5. Прочитать программой tcpdump созданный в предыдущем пункте файл.

6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

Работа с анализатором протоколов wireshark

1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.

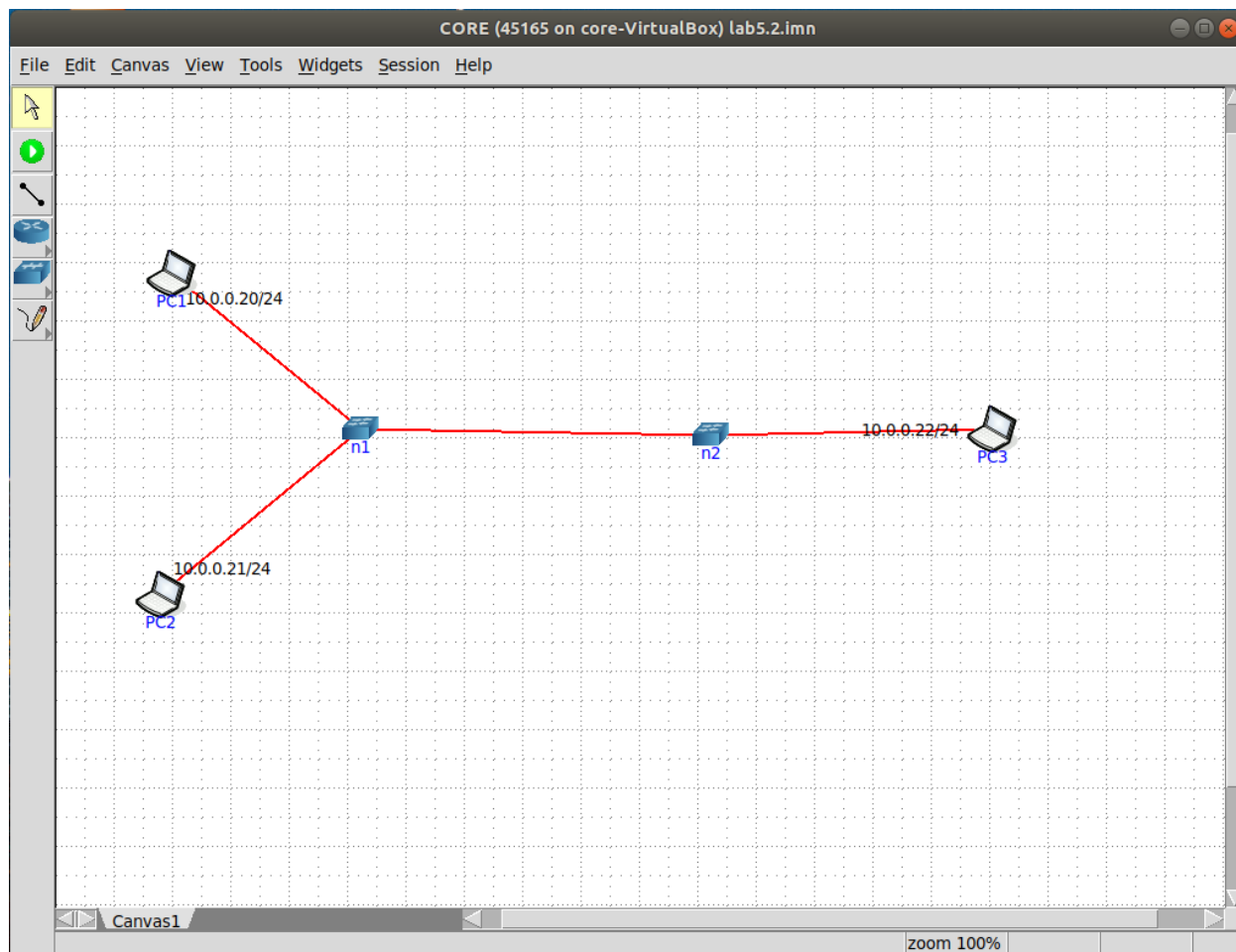
2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.

3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму

Flow Graph. Диаграмму сохранить либо в виде текстового файла либо в виде изображения.

4. Прочитать файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.

Ход работы:



Работа с анализатором протоколов tcpdump

1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.

```
Терминал
Файл Правка Вид Поиск Терминал Справка
root@PC2:/tmp/pycore.43933/PC2.conf# ping 10.0.0.20
PING 10.0.0.20 (10.0.0.20) 56(84) bytes of data.
64 bytes from 10.0.0.20: icmp_seq=1 ttl=63 time=0.101 ms
64 bytes from 10.0.0.20: icmp_seq=2 ttl=63 time=0.049 ms
64 bytes from 10.0.0.20: icmp_seq=3 ttl=63 time=0.050 ms
64 bytes from 10.0.0.20: icmp_seq=4 ttl=63 time=0.067 ms
64 bytes from 10.0.0.20: icmp_seq=5 ttl=63 time=0.054 ms
64 bytes from 10.0.0.20: icmp_seq=6 ttl=63 time=0.049 ms
64 bytes from 10.0.0.20: icmp_seq=7 ttl=63 time=0.046 ms
64 bytes from 10.0.0.20: icmp_seq=8 ttl=63 time=0.074 ms
64 bytes from 10.0.0.20: icmp_seq=9 ttl=63 time=0.052 ms
64 bytes from 10.0.0.20: icmp_seq=10 ttl=63 time=0.037 ms
64 bytes from 10.0.0.20: icmp_seq=11 ttl=63 time=0.053 ms

Терминал
Файл Правка Вид Поиск Терминал Справка
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10 packets captured
10 packets received by filter
0 packets dropped by kernel
root@PC1:/tmp/pycore.43933/PC1.conf# tcpdump -c 10 -w out.txt
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10 packets captured
11 packets received by filter
0 packets dropped by kernel
root@PC1:/tmp/pycore.43933/PC1.conf# tcpdump -c 10 -r out.txt
reading from file out.txt, link-type EN10MB (Ethernet)
19:13:43.572843 IP 10.0.3.20 > PC1: ICMP echo request, id 27, seq 9, length 64
19:13:43.572856 IP PC1 > 10.0.3.20: ICMP echo reply, id 27, seq 9, length 64
19:13:44.570689 IP _gateway > 224.0.0.5: OSPFv2, Hello, length 44
19:13:44.586378 IP 10.0.3.20 > PC1: ICMP echo request, id 27, seq 10, length 64
19:13:44.586388 IP PC1 > 10.0.3.20: ICMP echo reply, id 27, seq 10, length 64
19:13:45.298765 IP6 fe80::68e1:84ff:fe19:ce2a > ip6-allrouters: ICMP6, router soli
citation, length 16
19:13:45.615158 IP 10.0.3.20 > PC1: ICMP echo request, id 27, seq 11, length 64
19:13:45.615170 IP PC1 > 10.0.3.20: ICMP echo reply, id 27, seq 11, length 64
19:13:46.581021 IP _gateway > 224.0.0.5: OSPFv2, Hello, length 44
19:13:46.644836 IP 10.0.3.20 > PC1: ICMP echo request, id 27, seq 12, length 64
root@PC1:/tmp/pycore.43933/PC1.conf#
```

2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

-e	Отображает данные канального уровня (MAC-адрес, протокол, длина пакета). Вместо IP-адресов будут отображаться mac-адреса компьютеров.
----	---

-x	Делает распечатку пакета в шестнадцатеричной системе, полезно для более детального анализа пакета. Количество отображаемых данных зависит от опции -s
-xx	Тоже, что и предыдущий параметр, но включает в себя заголовок канального уровня.

The screenshot shows a terminal window titled "Терминал" with a menu bar: "Файл Правка Вид Поиск Терминал Справка".

The first terminal session shows the execution of the command: `<PC1.conf# tcpdump -c 5 -e -xx 'ether dst ff:ff:ff:ff:ff:ff'`. The output indicates that verbose output is suppressed and provides details about the capture on interface `eth0`, including the link type (EN10MB), capture size (262144 bytes), and the details of a captured packet: `20:35:36.641282 00:00:00:aa:00:02 (oui Ethernet) > Broadcast, ethertype IPv4 (0x0800), length 98: 10.0.0.22 > 10.0.0.255: ICMP echo request, id 27, seq 1, length 64`. Below this, a hex dump of the packet data is shown:

```

0x0000:  ffff ffff ffff 0000 00aa 0002 0800 4500
0x0010:  0054 0000 4000 4001 2595 0a00 0016 0a00
0x0020:  00ff 0800 929d 001b 0001 684a 6b60 0000
0x0030:  0000 c9c8 0900 0000 0000 1011 1213 1415
0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425

```

The second terminal session shows the execution of the command: `root@PC3:/tmp/pycore.45165/PC3.conf# ping 10.0.0.255 -b`. The output shows a warning: `WARNING: pinging broadcast address`, followed by the command's execution: `PING 10.0.0.255 (10.0.0.255) 56(84) bytes of data.` After pressing `^C`, the ping statistics are displayed: `--- 10.0.0.255 ping statistics ---`, `12 packets transmitted, 0 received, 100% packet loss, time 11271ms`. The prompt returns to `root@PC3:/tmp/pycore.45165/PC3.conf#`.

3. Запустить `tcpdump` так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов воспользоваться утилитой `ping`.

-X	Выводит пакет в ASCII- и hex-формате. Полезно в случае анализа инцидента связанного со взломом, так как позволяет просмотреть какая текстовая информация передавалась во время соединения.
----	--


```
Терминал
Файл Правка Вид Поиск Терминал Справка
<PC1.conf# tcpdump -c 3 -xx -X 'dst host 10.0.0.20 and ip proto \icmp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:13:16.207974 IP 10.0.2.20 > PC1: ICMP echo request, id 27, seq 41, length 64
    0x0000: 4500 0054 fe23 4000 3e01 285e 0a00 0214 E..T.#@.>.(^....
    0x0010: 0a00 0014 0800 e0c9 001b 0029 cc92 5060 .....).P'
    0x0020: 0000 0000 382c 0300 0000 0000 1011 1213 .....8.....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!"#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
    0x0050: 3435 3637 4567
14:13:17.232287 IP 10.0.2.20 > PC1: ICMP echo request, id 27, seq 42, length 64
    0x0000: 4500 0054 ff0b 4000 3e01 2776 0a00 0214 E..T..@.>.'v....
    0x0010: 0a00 0014 0800 df69 001b 002a cd92 5060 .....i...*.P'
    0x0020: 0000 0000 388b 0300 0000 0000 1011 1213 .....8.....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!"#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
    0x0050: 3435 3637 4567
14:13:18.256224 IP 10.0.2.20 > PC1: ICMP echo request, id 27, seq 43, length 64
    0x0000: 4500 0054 ff97 4000 3e01 26ea 0a00 0214 E..T..@.>.&.....
    0x0010: 0a00 0014 0800 5d0b 001b 002b ce92 5060 .....].....+.P'
    0x0020: 0000 0000 b9e8 0300 0000 0000 1011 1213 .....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!"#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
    0x0050: 3435 3637 4567
3 packets captured
3 packets received by filter
0 packets dropped by kernel
root@PC1:/tmp/pycore.33117/PC1.conf#
```

4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Результат работы программы писать в файл.

```
Терминал
Файл Правка Вид Поиск Терминал Справка
<PC1.conf# tcpdump -c 7 'src host 10.0.0.22' -w traceroute.txt
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
7 packets captured
16 packets received by filter
0 packets dropped by kernel
root@PC1:/tmp/pycore.45165/PC1.conf#

Терминал
Файл Правка Вид Поиск Терминал Справка
root@PC3:/tmp/pycore.45165/PC3.conf# traceroute -q 10 10.0.0.20
traceroute to 10.0.0.20 (10.0.0.20), 30 hops max, 60 byte packets
 1  10.0.0.20 (10.0.0.20)  0.264 ms  0.218 ms  0.203 ms  0.189 ms  0.175 ms  0.162 ms * * * *
root@PC3:/tmp/pycore.45165/PC3.conf#
```

```
Терминал
Файл Правка Вид Поиск Терминал Справка
root@PC1:/tmp/pycore.45165/PC1.conf# tcpdump -c 7 -xx -X -r traceroute.txt
reading from file traceroute.txt, link-type EN10MB (Ethernet)
21:11:57.287120 IP 10.0.0.22.60154 > PC1.33434: UDP, length 32
    0x0000:  4500 003c 595f 0000 0111 4c29 0a00 0016  E..<Y_....L)....
    0x0010:  0a00 0014 eafa 829a 0028 88da 4041 4243  .....(..@ABC
    0x0020:  4445 4647 4849 4a4b 4c4d 4e4f 5051 5253  DEFGHIJKLMNOPQRS
    0x0030:  5455 5657 5859 5a5b 5c5d 5e5f          TUVWXYZ[\]^_
21:11:57.287154 IP 10.0.0.22.51327 > PC1.33435: UDP, length 32
    0x0000:  4500 003c 5960 0000 0111 4c28 0a00 0016  E..<Y`....L(....
    0x0010:  0a00 0014 c87f 829b 0028 ab54 4041 4243  .....(.T@ABC
    0x0020:  4445 4647 4849 4a4b 4c4d 4e4f 5051 5253  DEFGHIJKLMNOPQRS
    0x0030:  5455 5657 5859 5a5b 5c5d 5e5f          TUVWXYZ[\]^_
21:11:57.287171 IP 10.0.0.22.46902 > PC1.33436: UDP, length 32
    0x0000:  4500 003c 5961 0000 0111 4c27 0a00 0016  E..<Ya....L'....
    0x0010:  0a00 0014 b736 829c 0028 bc9c 4041 4243  .....6...(..@ABC
    0x0020:  4445 4647 4849 4a4b 4c4d 4e4f 5051 5253  DEFGHIJKLMNOPQRS
    0x0030:  5455 5657 5859 5a5b 5c5d 5e5f          TUVWXYZ[\]^_
21:11:57.287187 IP 10.0.0.22.40558 > PC1.33437: UDP, length 32
    0x0000:  4500 003c 5962 0000 0111 4c26 0a00 0016  E..<Yb....L&....
    0x0010:  0a00 0014 9e6e 829d 0028 d563 4041 4243  .....n...(.c@ABC
    0x0020:  4445 4647 4849 4a4b 4c4d 4e4f 5051 5253  DEFGHIJKLMNOPQRS
    0x0030:  5455 5657 5859 5a5b 5c5d 5e5f          TUVWXYZ[\]^_
21:11:57.287204 IP 10.0.0.22.35679 > PC1.33438: UDP, length 32
    0x0000:  4500 003c 5963 0000 0111 4c25 0a00 0016  E..<Yc....L%. ....
```

5. Прочсть программой tcpdump созданный в предыдущем пункте файл.

```
Терминал
Файл Правка Вид Поиск Терминал Справка
21:11:57.287120 IP 10.0.0.22.60154 > PC1.33434: UDP, length 32
21:11:57.287154 IP 10.0.0.22.51327 > PC1.33435: UDP, length 32
21:11:57.287171 IP 10.0.0.22.46902 > PC1.33436: UDP, length 32
21:11:57.287187 IP 10.0.0.22.40558 > PC1.33437: UDP, length 32
21:11:57.287204 IP 10.0.0.22.35679 > PC1.33438: UDP, length 32
21:11:57.287220 IP 10.0.0.22.47245 > PC1.33439: UDP, length 32
21:11:57.287236 IP 10.0.0.22.38098 > PC1.33440: UDP, length 32
root@PC1:/tmp/pycore.45165/PC1.conf#
```

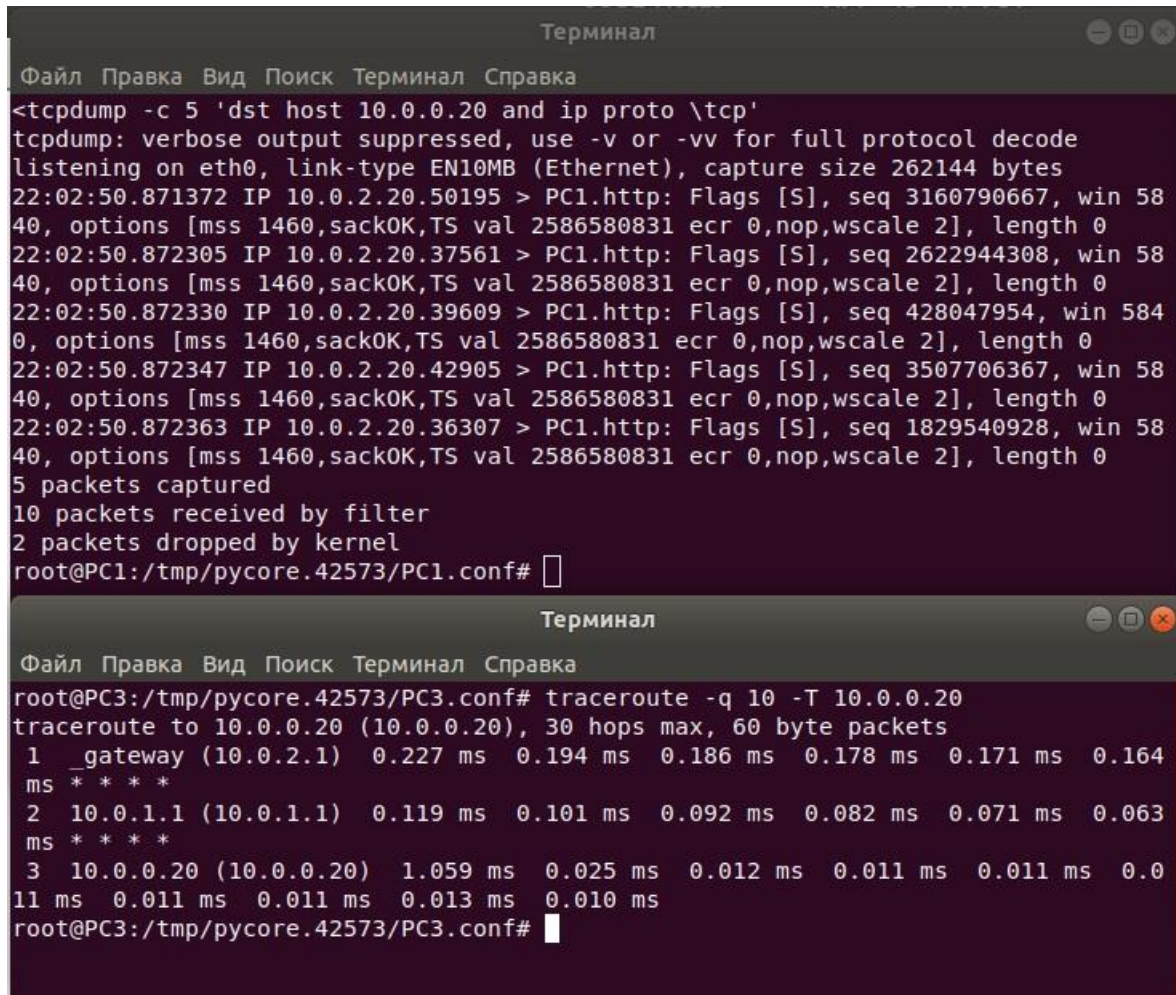
6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

Запустить tcpdump так, чтобы он перехватывал только пакеты протокола UDP, отправленные на определенный IP-адрес. Количество захватываемых пакетов ограничить 5. Для генерирования пакетов воспользоваться утилитой traceroute.

```
Терминал
Файл Правка Вид Поиск Терминал Справка
<tcpdump -c 5 'dst host 10.0.0.20 and ip proto \udp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
22:01:13.029914 IP 10.0.2.20.35223 > PC1.33454: UDP, length 32
22:01:13.029946 IP 10.0.2.20.58042 > PC1.33455: UDP, length 32
22:01:13.029966 IP 10.0.2.20.43554 > PC1.33456: UDP, length 32
22:01:13.029986 IP 10.0.2.20.36374 > PC1.33457: UDP, length 32
22:01:13.030005 IP 10.0.2.20.46822 > PC1.33458: UDP, length 32
5 packets captured
10 packets received by filter
3 packets dropped by kernel
root@PC1:/tmp/pycore.42573/PC1.conf#

Терминал
Файл Правка Вид Поиск Терминал Справка
root@PC3:/tmp/pycore.42573/PC3.conf# traceroute -q 10 10.0.0.20
traceroute to 10.0.0.20 (10.0.0.20), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.1)  0.296 ms  0.237 ms  0.220 ms  0.207 ms  0.195 ms  0.184
ms * * * *
 2 10.0.1.1 (10.0.1.1)  0.129 ms  0.107 ms  0.093 ms  0.080 ms  0.065 ms  0.051
ms * * * *
 3 10.0.0.20 (10.0.0.20)  0.162 ms  0.131 ms  0.113 ms  0.096 ms  0.079 ms  0.0
61 ms * * * *
root@PC3:/tmp/pycore.42573/PC3.conf#
```

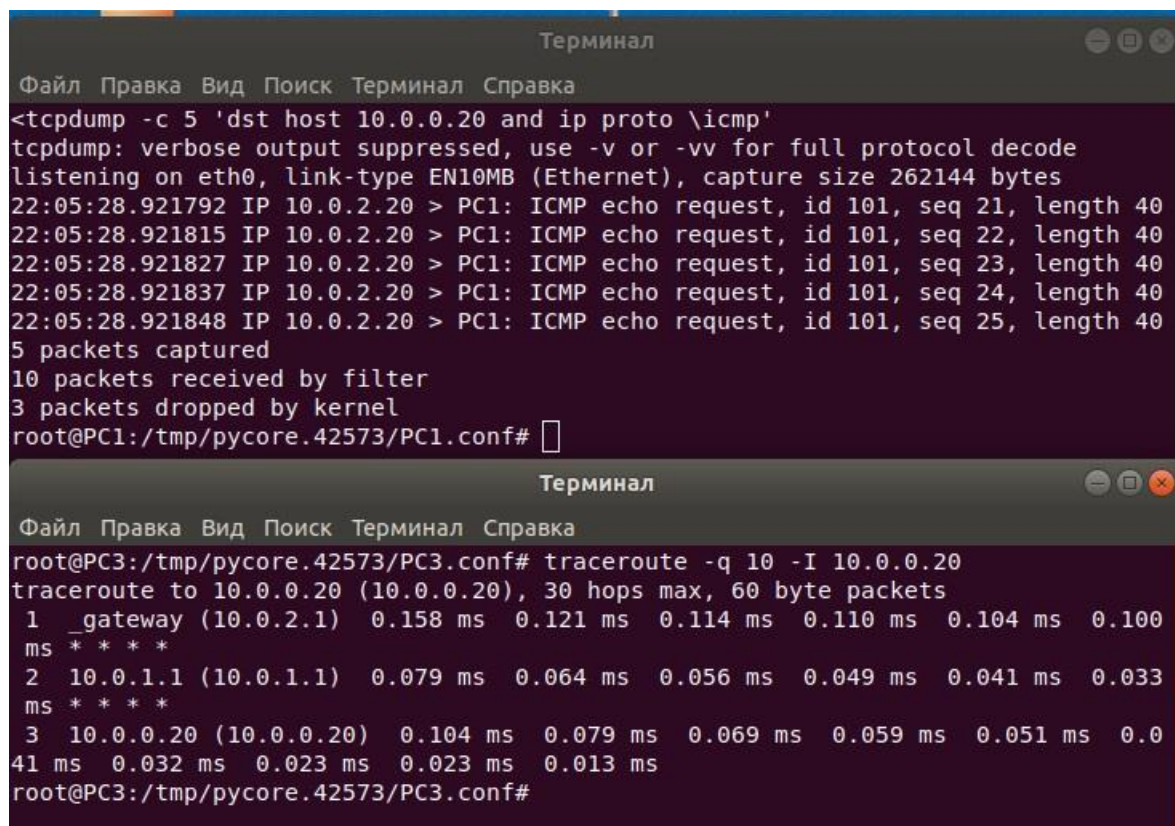

Запустить tcpdump так, чтобы он перехватывал только пакеты протокола TCP, отправленные на определенный IP-адрес. Количество захватываемых пакетов ограничить 5. Для генерирования пакетов воспользоваться утилитой traceroute.



```
Терминал
Файл Правка Вид Поиск Терминал Справка
<tcpdump -c 5 'dst host 10.0.0.20 and ip proto \tcp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
22:02:50.871372 IP 10.0.2.20.50195 > PC1.http: Flags [S], seq 3160790667, win 58
40, options [mss 1460,sackOK,TS val 2586580831 ecr 0,nop,wscale 2], length 0
22:02:50.872305 IP 10.0.2.20.37561 > PC1.http: Flags [S], seq 2622944308, win 58
40, options [mss 1460,sackOK,TS val 2586580831 ecr 0,nop,wscale 2], length 0
22:02:50.872330 IP 10.0.2.20.39609 > PC1.http: Flags [S], seq 428047954, win 584
0, options [mss 1460,sackOK,TS val 2586580831 ecr 0,nop,wscale 2], length 0
22:02:50.872347 IP 10.0.2.20.42905 > PC1.http: Flags [S], seq 3507706367, win 58
40, options [mss 1460,sackOK,TS val 2586580831 ecr 0,nop,wscale 2], length 0
22:02:50.872363 IP 10.0.2.20.36307 > PC1.http: Flags [S], seq 1829540928, win 58
40, options [mss 1460,sackOK,TS val 2586580831 ecr 0,nop,wscale 2], length 0
5 packets captured
10 packets received by filter
2 packets dropped by kernel
root@PC1:/tmp/pycore.42573/PC1.conf#

Терминал
Файл Правка Вид Поиск Терминал Справка
root@PC3:/tmp/pycore.42573/PC3.conf# traceroute -q 10 -T 10.0.0.20
traceroute to 10.0.0.20 (10.0.0.20), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.1)  0.227 ms  0.194 ms  0.186 ms  0.178 ms  0.171 ms  0.164
ms  * * * *
 2 10.0.1.1 (10.0.1.1)  0.119 ms  0.101 ms  0.092 ms  0.082 ms  0.071 ms  0.063
ms  * * * *
 3 10.0.0.20 (10.0.0.20)  1.059 ms  0.025 ms  0.012 ms  0.011 ms  0.011 ms  0.0
11 ms  0.011 ms  0.011 ms  0.013 ms  0.010 ms
root@PC3:/tmp/pycore.42573/PC3.conf#
```

Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. Количество захватываемых пакетов ограничить 5. Для генерирования пакетов воспользоваться утилитой traceroute.



The image shows two terminal windows. The top window, titled 'Терминал', shows the execution of the `<tcpdump -c 5 'dst host 10.0.0.20 and ip proto \icmp'` command. It displays five captured ICMP echo requests from 10.0.2.20 to 10.0.0.20 with sequence numbers 21 through 25. The bottom window, also titled 'Терминал', shows the execution of the `tracert -q 10 -I 10.0.0.20` command. It displays a traceroute path from 10.0.2.1 to 10.0.1.1 to 10.0.0.20, with round-trip times for each hop.

```
Терминал
Файл Правка Вид Поиск Терминал Справка
<tcpdump -c 5 'dst host 10.0.0.20 and ip proto \icmp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
22:05:28.921792 IP 10.0.2.20 > PC1: ICMP echo request, id 101, seq 21, length 40
22:05:28.921815 IP 10.0.2.20 > PC1: ICMP echo request, id 101, seq 22, length 40
22:05:28.921827 IP 10.0.2.20 > PC1: ICMP echo request, id 101, seq 23, length 40
22:05:28.921837 IP 10.0.2.20 > PC1: ICMP echo request, id 101, seq 24, length 40
22:05:28.921848 IP 10.0.2.20 > PC1: ICMP echo request, id 101, seq 25, length 40
5 packets captured
10 packets received by filter
3 packets dropped by kernel
root@PC1:/tmp/pycore.42573/PC1.conf#

Терминал
Файл Правка Вид Поиск Терминал Справка
root@PC3:/tmp/pycore.42573/PC3.conf# traceroute -q 10 -I 10.0.0.20
traceroute to 10.0.0.20 (10.0.0.20), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.1)  0.158 ms  0.121 ms  0.114 ms  0.110 ms  0.104 ms  0.100
ms * * * *
 2 10.0.1.1 (10.0.1.1)  0.079 ms  0.064 ms  0.056 ms  0.049 ms  0.041 ms  0.033
ms * * * *
 3 10.0.0.20 (10.0.0.20)  0.104 ms  0.079 ms  0.069 ms  0.059 ms  0.051 ms  0.0
41 ms  0.032 ms  0.023 ms  0.023 ms  0.013 ms
root@PC3:/tmp/pycore.42573/PC3.conf#
```

Работа с анализатором протоколов wireshark

1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.

Терминал

Файл Правка Вид Поиск Терминал Справка

```
root@PC3:/tmp/pycore.45165/PC3.conf# ping 10.0.0.255 -b
WARNING: pinging broadcast address
PING 10.0.0.255 (10.0.0.255) 56(84) bytes of data.
```

*veth3.0.dd

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 10.0.0.255

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.22	10.0.0.255	ICMP	98	Echo (ping) request
2	1.023317304	10.0.0.22	10.0.0.255	ICMP	98	Echo (ping) request
3	2.062674752	10.0.0.22	10.0.0.255	ICMP	98	Echo (ping) request
4	3.072465750	10.0.0.22	10.0.0.255	ICMP	98	Echo (ping) request
5	4.100309200	10.0.0.22	10.0.0.255	ICMP	98	Echo (ping) request
6	5.120150603	10.0.0.22	10.0.0.255	ICMP	98	Echo (ping) request

Timestamp from icmp data: Apr 5, 2021 21:20:27.000000000 MSK
[Timestamp from icmp data (relative): 0.689067635 seconds]

▼ Data (48 bytes)

2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.

Терминал

Файл Правка Вид Поиск Терминал Справка

```
root@PC3:/tmp/pycore.45165/PC3.conf# ping 10.0.0.20
PING 10.0.0.20 (10.0.0.20) 56(84) bytes of data.
64 bytes from 10.0.0.20: icmp_seq=1 ttl=64 time=0.050 ms
64 bytes from 10.0.0.20: icmp_seq=2 ttl=64 time=0.039 ms
64 bytes from 10.0.0.20: icmp_seq=3 ttl=64 time=0.040 ms
```

Capturing from veth3.0.dd

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp and ip.src == 10.0.0.22

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.22	10.0.0.20	ICMP	98	Echo (ping) request
3	1.022565355	10.0.0.22	10.0.0.20	ICMP	98	Echo (ping) request
5	2.046402460	10.0.0.22	10.0.0.20	ICMP	98	Echo (ping) request
7	3.069799885	10.0.0.22	10.0.0.20	ICMP	98	Echo (ping) request

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
 ▶ Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
 ▶ Internet Protocol Version 4, Src: 10.0.0.22, Dst: 10.0.0.20
 ▶ Internet Control Message Protocol

```
123.txt [Только для чтения]
~/Рабочий стол

Открыть Сохранить

+-----+
18:47:10,122,588 ETHER
|0|00|00|00|aa|00|00|00|00|00|aa|00|02|08|00|45|00|00|54|7c|be|40|00|40|01|a9|
c1|0a|00|00|16|0a|00|00|14|08|00|f1|28|00|60|00|0a|2e|5b|6b|60|00|00|00|00|ac|de|
01|00|00|00|00|00|10|11|12|13|14|15|16|17|18|19|1a|1b|1c|1d|1e|1f|20|21|22|23|24|
25|26|27|28|29|2a|2b|2c|2d|2e|2f|30|31|32|33|34|35|36|37|

+-----+
18:47:10,122,604 ETHER
|0|00|00|00|aa|00|02|00|00|00|aa|00|00|08|00|45|00|00|54|76|b5|00|00|40|01|ef|
ca|0a|00|00|14|0a|00|00|16|00|00|f9|28|00|60|00|0a|2e|5b|6b|60|00|00|00|00|ac|de|
01|00|00|00|00|00|10|11|12|13|14|15|16|17|18|19|1a|1b|1c|1d|1e|1f|20|21|22|23|24|
25|26|27|28|29|2a|2b|2c|2d|2e|2f|30|31|32|33|34|35|36|37|

+-----+
18:47:11,145,154 ETHER
|0|00|00|00|aa|00|00|00|00|00|aa|00|02|08|00|45|00|00|54|7d|54|40|00|40|01|a9|
2b|0a|00|00|16|0a|00|00|14|08|00|b5|cf|00|60|00|0b|2f|5b|6b|60|00|00|00|00|e6|36|
02|00|00|00|00|00|10|11|12|13|14|15|16|17|18|19|1a|1b|1c|1d|1e|1f|20|21|22|23|24|
25|26|27|28|29|2a|2b|2c|2d|2e|2f|30|31|32|33|34|35|36|37|

+-----+
18:47:11,145,168 ETHER
|0|00|00|00|aa|00|02|00|00|00|aa|00|00|08|00|45|00|00|54|77|20|00|00|40|01|ef|
5f|0a|00|00|14|0a|00|00|16|00|00|bd|cf|00|60|00|0b|2f|5b|6b|60|00|00|00|00|e6|36|
02|00|00|00|00|00|10|11|12|13|14|15|16|17|18|19|1a|1b|1c|1d|1e|1f|20|21|22|23|24|
25|26|27|28|29|2a|2b|2c|2d|2e|2f|30|31|32|33|34|35|36|37|

Текст Ширина табуляции: 8 Стр 1, Стлб 1 ВСТ
```

3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла либо в виде изображения.

Capturing from veth3.0.dd

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 10.0.0.22

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.22	10.0.0.20	UDP	74	40440 → 33434 Len=32
2	0.000016243	10.0.0.20	10.0.0.22	ICMP	102	Destination unreachable
3	0.000043457	10.0.0.22	10.0.0.20	UDP	74	49276 → 33435 Len=32
4	0.000047058	10.0.0.20	10.0.0.22	ICMP	102	Destination unreachable
5	0.000062056	10.0.0.22	10.0.0.20	UDP	74	51871 → 33436 Len=32
6	0.000065352	10.0.0.20	10.0.0.22	ICMP	102	Destination unreachable
7	0.000079799	10.0.0.22	10.0.0.20	UDP	74	54684 → 33437 Len=32
8	0.000083060	10.0.0.20	10.0.0.22	ICMP	102	Destination unreachable
9	0.000097586	10.0.0.22	10.0.0.20	UDP	74	44678 → 33438 Len=32
10	0.000100877	10.0.0.20	10.0.0.22	ICMP	102	Destination unreachable

Терминал

Файл Правка Вид Поиск Терминал Справка

```

root@PC3:/tmp/pycore.45165/PC3.conf# traceroute -q 10 10.0.0.20
traceroute to 10.0.0.20 (10.0.0.20), 30 hops max, 60 byte packets
 1 10.0.0.20 (10.0.0.20) 0.049 ms 0.008 ms 0.007 ms 0.007 ms 0.008 ms 0.0
08 ms * * * *
root@PC3:/tmp/pycore.45165/PC3.conf#

```

Wireshark · Flow · veth3.0.dd

Time	10.0.0.22	10.0.0.20	Comment
0.000000000	40440	40440 → 33434 Len=32	UDP: 40440 → 33434 Len=32
0.000016243	33434	Destination unreachable (Port unreachable)	ICMP: Destination unreachable (Port unreachable)
0.000043457	49276	49276 → 33435 Len=32	UDP: 49276 → 33435 Len=32
0.000047058	33435	Destination unreachable (Port unreachable)	ICMP: Destination unreachable (Port unreachable)
0.000062056	51871	51871 → 33436 Len=32	UDP: 51871 → 33436 Len=32
0.000065352	33436	Destination unreachable (Port unreachable)	ICMP: Destination unreachable (Port unreachable)
0.000079799	54684	54684 → 33437 Len=32	UDP: 54684 → 33437 Len=32
0.000083060	33437	Destination unreachable (Port unreachable)	ICMP: Destination unreachable (Port unreachable)
0.000097586	44678	44678 → 33438 Len=32	UDP: 44678 → 33438 Len=32
0.000100877	33438	Destination unreachable (Port unreachable)	ICMP: Destination unreachable (Port unreachable)
0.000114776	32822	32822 → 33439 Len=32	UDP: 32822 → 33439 Len=32
0.000118045	33439	Destination unreachable (Port unreachable)	ICMP: Destination unreachable (Port unreachable)
0.000132305	49458	49458 → 33440 Len=32	UDP: 49458 → 33440 Len=32
0.000146333	47717	47717 → 33441 Len=32	UDP: 47717 → 33441 Len=32
0.000163035	35989	35989 → 33442 Len=32	UDP: 35989 → 33442 Len=32

Packet 16: UDP: 55322 → 33443 Len=32

☐ Limit to display filter

Flow type: All Flows

Addresses: Any

Reset

Save As... Заккрыть Справка

4. Прочсть файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.

*veth3.0.dd

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 10.0.0.22 and ip.dst == 10.0.0.20 Expression...

No.	Time	Source	Destination	Protocol	Length	Info
22	0.000256306	10.0.0.22	10.0.0.20	UDP	74	57761 → 33449 Len=32
21	0.000243159	10.0.0.22	10.0.0.20	UDP	74	54992 → 33448 Len=32
20	0.000229844	10.0.0.22	10.0.0.20	UDP	74	49348 → 33447 Len=32
19	0.000217093	10.0.0.22	10.0.0.20	UDP	74	40986 → 33446 Len=32
18	0.000203855	10.0.0.22	10.0.0.20	UDP	74	52736 → 33445 Len=32
17	0.000190221	10.0.0.22	10.0.0.20	UDP	74	45686 → 33444 Len=32
16	0.000176763	10.0.0.22	10.0.0.20	UDP	74	55322 → 33443 Len=32
15	0.000163035	10.0.0.22	10.0.0.20	UDP	74	35989 → 33442 Len=32

Терминал

Файл Правка Вид Поиск Терминал Справка

```
root@PC3:/tmp/pycore.45165/PC3.conf# traceroute -q 10 10.0.0.20
traceroute to 10.0.0.20 (10.0.0.20), 30 hops max, 60 byte packets
 1 10.0.0.20 (10.0.0.20) 0.049 ms 0.008 ms 0.007 ms 0.007 ms 0.008 ms 0.008 ms * * * *
```

root@PC3:/tmp/pycore.45165/PC3.conf#

Терминал

Файл Правка Вид Поиск Терминал Справка

```
root@PC1:/tmp/pycore.45165/PC1.conf# tcpdump -c 7 -xx -X -r traceroute.txt
reading from file traceroute.txt, link-type EN10MB (Ethernet)
21:11:57.287120 IP 10.0.0.22.60154 > PC1.33434: UDP, length 32
    0x0000: 4500 003c 595f 0000 0111 4c29 0a00 0016  E...<Y_....L)....
    0x0010: 0a00 0014 eafa 829a 0028 88da 4041 4243  .....(..@ABC
    0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253  DEFGHIJKLMNOPQRS
    0x0030: 5455 5657 5859 5a5b 5c5d 5e5f          TUVWXYZ[\]^_
21:11:57.287154 IP 10.0.0.22.51327 > PC1.33435: UDP, length 32
    0x0000: 4500 003c 5960 0000 0111 4c28 0a00 0016  E...<Y`....L(....
    0x0010: 0a00 0014 c87f 829b 0028 ab54 4041 4243  .....(.T@ABC
    0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253  DEFGHIJKLMNOPQRS
    0x0030: 5455 5657 5859 5a5b 5c5d 5e5f          TUVWXYZ[\]^_
21:11:57.287171 IP 10.0.0.22.46902 > PC1.33436: UDP, length 32
    0x0000: 4500 003c 5961 0000 0111 4c27 0a00 0016  E...<Ya....L'....
    0x0010: 0a00 0014 b736 829c 0028 bc9c 4041 4243  .....6...(..@ABC
    0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253  DEFGHIJKLMNOPQRS
    0x0030: 5455 5657 5859 5a5b 5c5d 5e5f          TUVWXYZ[\]^_
21:11:57.287187 IP 10.0.0.22.40558 > PC1.33437: UDP, length 32
    0x0000: 4500 003c 5962 0000 0111 4c26 0a00 0016  E...<Yb....L&....
    0x0010: 0a00 0014 9e6e 829d 0028 d563 4041 4243  .....n...(.c@ABC
    0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253  DEFGHIJKLMNOPQRS
    0x0030: 5455 5657 5859 5a5b 5c5d 5e5f          TUVWXYZ[\]^_
21:11:57.287204 IP 10.0.0.22.35679 > PC1.33438: UDP, length 32
    0x0000: 4500 003c 5963 0000 0111 4c25 0a00 0016  E...<Yc....L%....
```