МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра вычислительные системы и технологии

Отчет

по лабораторной работе № 1

по дисциплине

Сети и телекоммуникации

«Работа с утилитами ping, tracert, tcpdump, wireshark»

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Гай В.Е. (подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ибо Эднан

(подпись) (фамилия, и.,о.)

17-АС

(шифр группы)

Работа защищена «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород, 2020

**Цель**:

Получение базовых навыков по работе с утилитами ping, tracert, tcpdump, wireshark.

**Вариант 5**

**Работа с ping, tracert**

Исследуемые узлы:

tv.sut.ru

www.iana.org

slashdot.jp

Число отправляемых запросов - 5

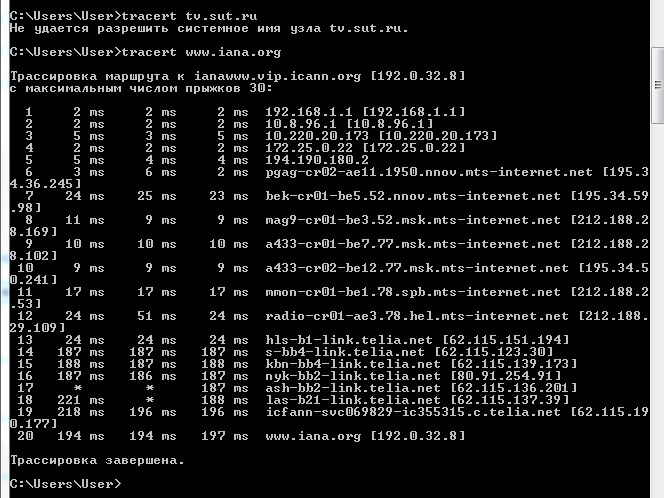
1. Проверка состояния связи с узлами с помощью утилиты ping.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Доменное имя | IP-адрес | Страна | Число потерянных запросов | Среднее время прохождения запроса, мс | TTL |
| tv.sut.ru | Не удалось найти IP-адрес | \_ | \_ | \_ | \_ |
| www.iana.org | 192.0.32.8 | США | 0 | 218 | 239 |
| slashdot.jp | 202.221.179.13 | Япония | 0 | 231 | 48 |

**Результаты выполнения ping.**

|  |
| --- |
| C:\Users\User\Desktop\прав1.PNG  C:\Users\User\Desktop\прав2.PNG |
|  |
|  |

1. **Трассировка узлов при помощи tracert:**





|  |
| --- |
| **Графики времени прохождения шлюзов для двух узлов (для 3-х пакетов).** |





1. **Работа с анализаторами протоколов tcpdump и wireshark.**

**Цель работы:**

Получение базовых навыков по работе с анализаторами протоколов tcpdump и wireshark.

1.1. Запускаем tcpdump в режиме захвата всех пакетов:

12:22:14.600758 IP 192.168.3.253.49611 > 239.255.255.250.1900: UDP, length 173

12:22:14.936087 IP 5412-v6.137 > 239.255.255.250.137: UDP, length 50

12:22:15.600343 IP 192.168.3.253.49611 > 239.255.255.250.1900: UDP, length 173

12:22:16.448818 IP 5412-v6.137 > 239.255.255.250.137: UDP, length 50

12:22:16.637773 IP 192.168.3.253.49611 > 239.255.255.250.1900: UDP, length 173

12:22:16.705497 arp who-has 192.168.3.145 tell 192.168.3.1

12:22:17.371602 IP 192.168.3.253.17500 > 192.168.3.255.17500: UDP, length 166

12:22:17.715529 IP 192.168.3.253.49611 > 239.255.255.250.1900: UDP, length 173

12:22:17.963186 IP 5412-v6.137 > 239.255.255.250.137: UDP, length 50

12:22:19.482271 arp who-has 192.168.12.100 tell 5412-v6

1.2. Запускаем tcpdump в режиме захвата широковещательного трафика, количество перехватываемых пакетов - 5, распечатка в шестнадцатеричной системе.

11:58:37.011550 arp who-has 192.168.12.100 tell 5412

0x0000: ffff ffff ffff 5435 30b3 4d1d 0806 0001

0x0010: 0800 0604 0001 5435 30b3 4d1d c0a8 0c67

0x0020: 0000 0000 0000 c0a8 0c64 0000 0000 0000

0x0030: 0000 0000 0000 0000 0000 0000

11:58:37.701161 arp who-has 192.168.12.100 tell 5412-v6

0x0000: ffff ffff ffff 000c 2968 4b3e 0806 0001

0x0010: 0800 0604 0001 000c 2968 4b3e c0a8 0c6a

0x0020: 0000 0000 0000 c0a8 0c64

11:58:37.933248 arp who-has 192.168.12.100 tell 5412

0x0000: ffff ffff ffff 5435 30b3 4d1d 0806 0001

0x0010: 0800 0604 0001 5435 30b3 4d1d c0a8 0c67

0x0020: 0000 0000 0000 c0a8 0c64 0000 0000 0000

0x0030: 0000 0000 0000 0000 0000 0000

11:58:38.716714 arp who-has 192.168.12.100 tell 5412-v6

0x0000: ffff ffff ffff 000c 2968 4b3e 0806 0001

0x0010: 0800 0604 0001 000c 2968 4b3e c0a8 0c6a

0x0020: 0000 0000 0000 c0a8 0c64

11:58:38.854903 arp who-has 192.168.12.100 tell 5412

0x0000: ffff ffff ffff 5435 30b3 4d1d 0806 0001

0x0010: 0800 0604 0001 5435 30b3 4d1d c0a8 0c67

0x0020: 0000 0000 0000 c0a8 0c64 0000 0000 0000

0x0030: 0000 0000 0000 0000 0000 0000

1.3. Запускаем tcpdump в режиме захвата пакетов протокола ICMP, отправленных на определенный адрес, количество перехватываемых пакетов - 3, распечатка в шестнадцатеричной системе и ASCII формате.

12:19:15.144312 IP 5412-v6 > 5412-V7: ICMP echo reply, id 1, seq 9, length 40

0x0000: 4500 003c 0163 0000 8001 0000 c0a8 0c6a E..<.c.........j

0x0010: c0a8 0c6b 0000 5552 0001 0009 6162 6364 ...k..UR....abcd

0x0020: 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst

0x0030: 7576 7761 6263 6465 6667 6869 uvwabcdefghi

12:19:16.146494 IP 5412-v6 > 5412-V7: ICMP echo reply, id 1, seq 10, length 40

0x0000: 4500 003c 0165 0000 8001 0000 c0a8 0c6a E..<.e.........j

0x0010: c0a8 0c6b 0000 5551 0001 000a 6162 6364 ...k..UQ....abcd

0x0020: 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst

0x0030: 7576 7761 6263 6465 6667 6869 uvwabcdefghi

12:19:17.146653 IP 5412-v6 > 5412-V7: ICMP echo reply, id 1, seq 11, length 40

0x0000: 4500 003c 0166 0000 8001 0000 c0a8 0c6a E..<.f.........j

0x0010: c0a8 0c6b 0000 5550 0001 000b 6162 6364 ...k..UP....abcd

0x0020: 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst

0x0030: 7576 7761 6263 6465 6667 6869 uvwabcdefghi

1.4. Запускаем tcpdump в режиме сохранения данных в двоичном режиме, распечатка в шестнадцатеричной системе и ASCII формате, количество перехватываемых пакетов - 3.

12:32:38.408521 arp who-has 5412 tell 5412-V1

0x0000: ffff ffff ffff 5435 30b3 2c19 0806 0001 ......T50.,.....

0x0010: 0800 0604 0001 5435 30b3 2c19 c0a8 0c65 ......T50.,....e

0x0020: 0000 0000 0000 c0a8 0c66 0000 0000 0000 .........f......

0x0030: 0000 0000 0000 0000 0000 0000 ............

12:32:38.422365 arp who-has 5412-V1 tell 5412

0x0000: ffff ffff ffff 5435 30b3 275f 0806 0001 ......T50.'\_....

0x0010: 0800 0604 0001 5435 30b3 275f c0a8 0c66 ......T50.'\_...f

0x0020: 0000 0000 0000 c0a8 0c65 0000 0000 0000 .........e......

0x0030: 0000 0000 0000 0000 0000 0000 ............

12:32:38.682979 IP6 fe80::d8ea:6e72:b0fe:60ef.546 > ff02::1:2.547: dhcp6 solicit

0x0000: 3333 0001 0002 5435 30b3 4d41 86dd 6000 33....T50.MA..`.

0x0010: 0000 005f 1101 fe80 0000 0000 0000 d8ea ...\_............

0x0020: 6e72 b0fe 60ef ff02 0000 0000 0000 0000 nr..`...........

0x0030: 0000 0001 0002 0222 0223 005f bdc4 0145 .......".#.\_...E

0x0040: 32a6 0008 0002 0ce4 0001 000e 0001 0001 2...............

0x0050: 1c57 d36a 000c 2952 cb1a 0003 000c 0e00 .W.j..)R........

12:32:38.753610 arp who-has 5412 tell 5412-v6

0x0000: ffff ffff ffff 000c 2968 4b3e 0806 0001 ........)hK>....

0x0010: 0800 0604 0001 000c 2968 4b3e c0a8 0c6a ........)hK>...j

0x0020: 0000 0000 0000 c0a8 0c66 .........f

12:32:38.756894 arp reply 5412 is-at 54:35:30:b3:27:5f (oui Unknown)

0x0000: 000c 2968 4b3e 5435 30b3 275f 0806 0001 ..)hK>T50.'\_....

0x0010: 0800 0604 0002 5435 30b3 275f c0a8 0c66 ......T50.'\_...f

0x0020: 000c 2968 4b3e c0a8 0c6a 0000 0000 0000 ..)hK>...j......

0x0030: 0000 0000 0000 0000 0000 0000 ............

12:32:38.757059 IP 5412-v6.137 > 5412.137: UDP, length 50

0x0000: 5435 30b3 275f 000c 2968 4b3e 0800 4500 T50.'\_..)hK>..E.

0x0010: 004e 01bf 0000 8011 0000 c0a8 0c6a c0a8 .N...........j..

0x0020: 0c66 0089 0089 003a 9a6c 8bd6 0000 0001 .f.....:.l......

0x0030: 0000 0000 0000 2043 4b41 4141 4141 4141 .......CKAAAAAAA

0x0040: 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAA

0x0050: 4141 4141 4141 4100 0021 0001 AAAAAAA..!..

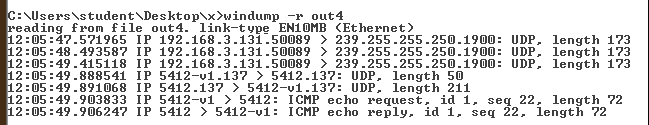
12:32:38.766253 arp who-has 5412-v6 tell 5412

0x0000: ffff ffff ffff 5435 30b3 275f 0806 0001 ......T50.'\_....

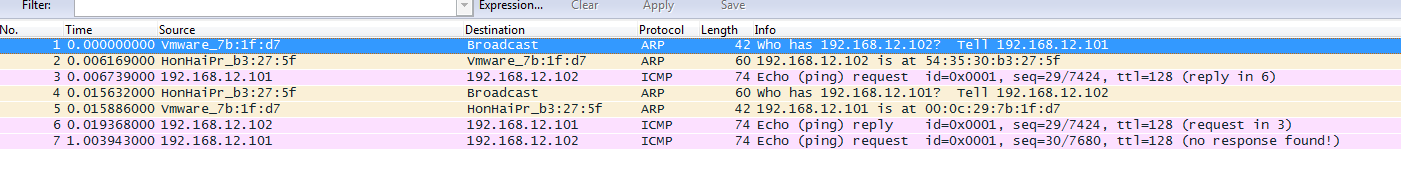
0x0010: 0800 0604 0001 5435 30b3 275f c0a8 0c66 ......T50.'\_...f

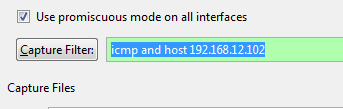
0x0020: 0000 0000 0000 c0a8 0c6a 0000 0000 0000 .........j......

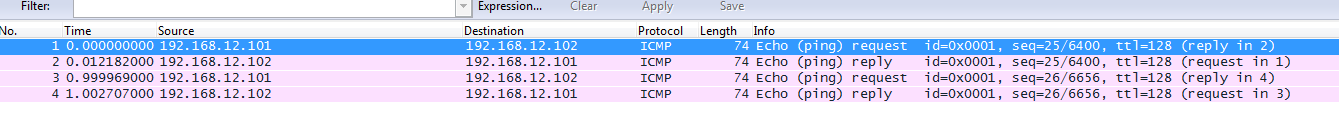
0x0030: 0000 0000 0000 0000 0000 0000 ...........

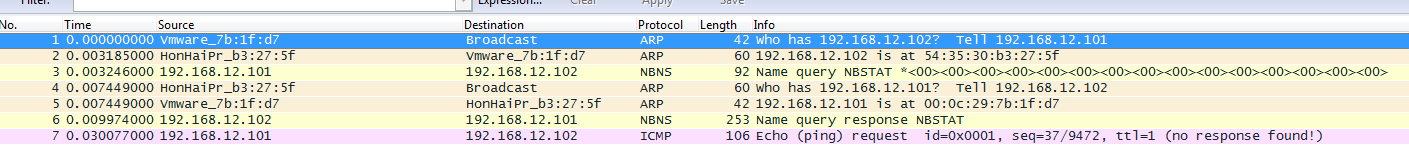
1.5. Прочтем файлы, созданные tcpdump.

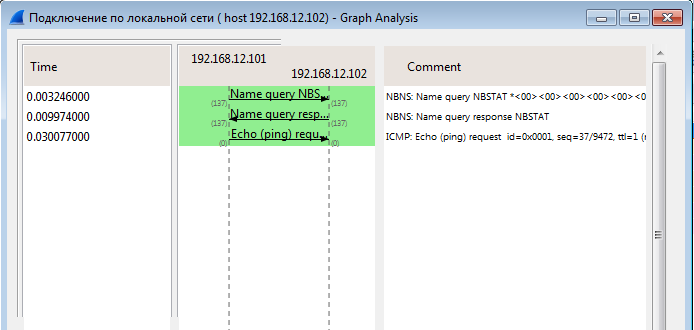
2. Работа с анализатором протоколов Wireshark

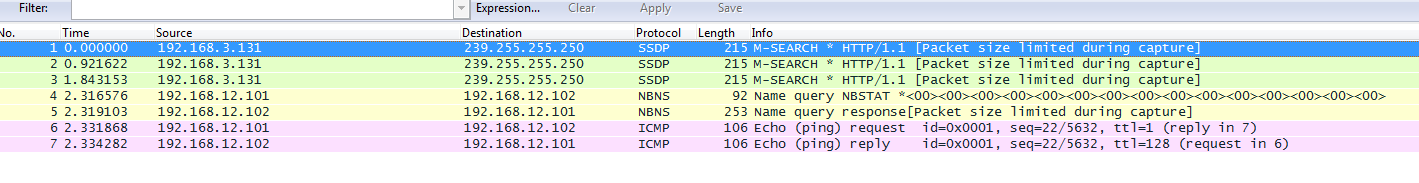
2.1. Захватим 7 пакетов широковещательного трафика.

2.2. Захватим 4 пакета ICMP, полученных от определенного узла



2.3. Перехватим пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построим диаграмму Flow Graph.



2.4. Прочтем файл, созданный программой tcpdump.