

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования

Университет ИТМО

Факультет программной инженерии и компьютерной техники

Отчет по лабораторной работе №4
«Анализ трафика компьютерных сетей с помощью утилиты
Wireshark»
по дисциплине “Компьютерные сети”

Выполнил: студент группы
Р33131

Бусыгин Дмитрий Алексеевич

Преподаватель:

Мартынчук Илья Геннадьевич

Санкт-Петербург
2024

Цель и краткая характеристика работы:

Цель работы – изучить структуру протокольных блоков данных, анализируя реальный трафик на компьютере студента с помощью бесплатно распространяемой утилиты Wireshark. В процессе выполнения домашнего задания выполняются наблюдения за передаваемым трафиком с компьютера пользователя в Интернет и в обратном направлении.

Применение специализированной утилиты Wireshark позволяет наблюдать структуру передаваемых кадров, пакетов и сегментов данных различных сетевых протоколов. При выполнении УИР рекомендуется выполнить анализ последовательности команд и определить назначение служебных данных, используемых для организации обмена данными в протоколах: ARP, DNS, FTP, HTTP, DHCP.

Выполнение:

Выбранный сайт: <https://busygin.com>

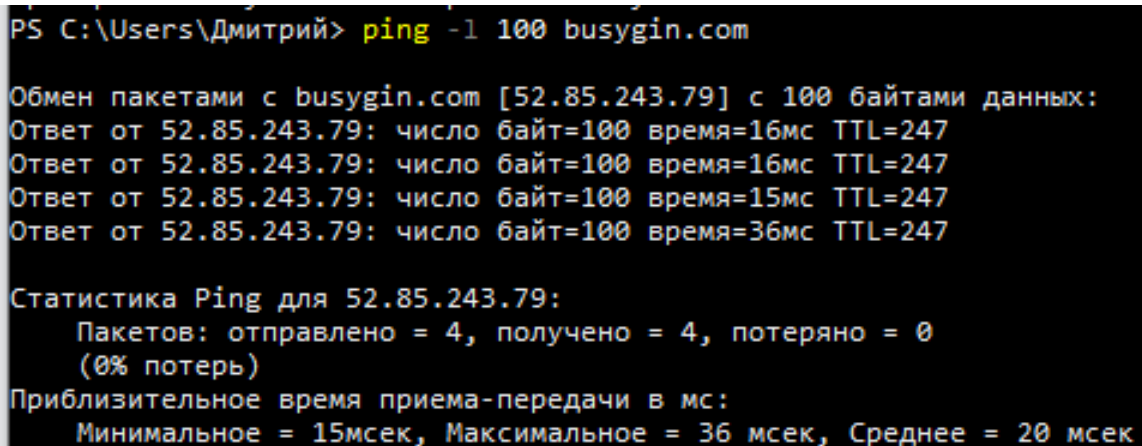
Этап 1. Анализ трафика утилиты ping.

Необходимо отследить и проанализировать трафик, создаваемой утилитой ping, запустив её следующим образом из командной строки:

“ping -l размер_пакета адрес_сайта_по_варианту”

В качестве размера пакета необходимо поочерёдно использовать различные значения от 100 до 10 000, самостоятельно выбрав шаг изменения. По результатам анализа собранной трассы, необходимо ответить на вопросы и выполнить задания.

Размер пакета 100:



```
PS C:\Users\Дмитрий> ping -l 100 busygin.com

Обмен пакетами с busygin.com [52.85.243.79] с 100 байтами данных:
Ответ от 52.85.243.79: число байт=100 время=16мс TTL=247
Ответ от 52.85.243.79: число байт=100 время=16мс TTL=247
Ответ от 52.85.243.79: число байт=100 время=15мс TTL=247
Ответ от 52.85.243.79: число байт=100 время=36мс TTL=247

Статистика Ping для 52.85.243.79:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 15мсек, Максимальное = 36 мсек, Среднее = 20 мсек
```

No.	Time	Source	Destination	Protocol	Length	Info
252	37.319395	18.165.171.34	192.168.0.105	ICMP	142	Echo (ping) reply id=0x0001, seq=17/4352, ttl=245 (request in 251)
255	38.333651	18.165.171.34	192.168.0.105	ICMP	142	Echo (ping) reply id=0x0001, seq=18/4608, ttl=245 (request in 253)
265	39.343759	18.165.171.34	192.168.0.105	ICMP	142	Echo (ping) reply id=0x0001, seq=19/4864, ttl=245 (request in 264)
270	40.351245	18.165.171.34	192.168.0.105	ICMP	142	Echo (ping) reply id=0x0001, seq=20/5120, ttl=245 (request in 269)
759	91.973585	18.165.171.34	192.168.0.105	ICMP	142	Echo (ping) reply id=0x0001, seq=21/5376, ttl=245 (request in 756)
769	92.999090	18.165.171.34	192.168.0.105	ICMP	142	Echo (ping) reply id=0x0001, seq=22/5632, ttl=245 (request in 768)
773	94.005085	18.165.171.34	192.168.0.105	ICMP	142	Echo (ping) reply id=0x0001, seq=23/5888, ttl=245 (request in 772)
803	95.020834	18.165.171.34	192.168.0.105	ICMP	142	Echo (ping) reply id=0x0001, seq=24/6144, ttl=245 (request in 800)

Увидеть есть ли фрагментация можно, посмотрев на флаг More fragments

```

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 128
Identification: 0x3812 (14354)
▼ 000. .... = Flags: 0x0
  0... .... = Reserved bit: Not set
  .0... .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 245
Protocol: ICMP (1)

```

Поле More fragments: 1 - промежуточный, 0 - последний

Количество фрагментов зависит от размера пакета и MTU (Maximum Transmission Unit) соединения, который обычно равен 1500 байт.

График, на котором на оси абсцисс находится размер пакета, а по оси ординат - количество фрагментов, на которое был разделён каждый ping-пакет:



Как изменить поле TTL с помощью утилиты ping?

добавить ключ `-i <TTL>` - значение указывается в хопх

Что содержится в поле data в ping-пакетах? - ASCII-символы

Этап 2. Анализ трафика утилиты `tracert`

Необходимо отследить и проанализировать трафик, создаваемой утилитой `tracert`, запустив её следующим образом из командной строки:

`“tracert -d адрес_сайта_по_варианту”`

По результатам анализа собранной трассы, необходимо ответить на вопросы.

```
PS C:\Users\Дмитрий> tracert -d busygin.com

Трассировка маршрута к busygin.com [18.245.86.32]
с максимальным числом прыжков 30:

 1      1 ms      1 ms      2 ms  192.168.0.1
 2      5 ms      3 ms      4 ms  10.180.224.1
 3     21 ms     21 ms     9 ms  5.19.0.205
 4      *        *        *    Превышен интервал ожидания для запроса.
 5      *        *        *    Превышен интервал ожидания для запроса.
 6      *        *        *    Превышен интервал ожидания для запроса.
 7      *        *        *    Превышен интервал ожидания для запроса.
 8      *        *        *    Превышен интервал ожидания для запроса.
 9      *        *        *    Превышен интервал ожидания для запроса.
10     *        *        *    Превышен интервал ожидания для запроса.
11     *        *        *    Превышен интервал ожидания для запроса.
12    35 ms     33 ms     34 ms  18.245.86.32
```

С помощью этой утилиты мы смогли отследить маршрут пакетов от источника к хосту назначения. До хоста дошли за 12 "хопов".

Сколько байт содержится в заголовке IP? Сколько байт содержится в поле данных? - В заголовке — 20 байт. В поле данных — 64 байта.

Errorg посылает промежуточный узел, когда TTL становится равен 0, ну и в случае любой ошибки. Reply посылает конечный узел, когда пакет успешно доходит до него.

Что изменится в работе tracert, если убрать ключ “-d”? Какой дополнительный трафик при этом будет генерироваться?

Произойдет попытка определить имя узла по его IP адресу, т.е. будут произведены дополнительные запросы к DNS-серверу.

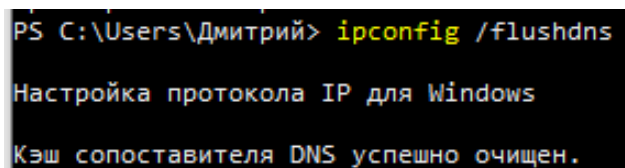
Этап 3. Анализ DNS трафика

Необходимо отследить и проанализировать трафик протокола DNS, сгенерированный в результате выполнения следующих действий:

- очистить кэш DNS с помощью команды ipconfig в командной строке:
`ipconfig /flushdns`
- очистить кэш браузера;
- зайти на Интернет-сайт, заданный по варианту.

По результатам анализа собранной трассы, ответьте на следующие вопросы.

Очистим кэш DNS:



```
PS C:\Users\Дмитрий> ipconfig /flushdns
Настройка протокола IP для Windows
Кэш сопоставителя DNS успешно очищен.
```

start <https://busygin.com>

351	8.861470	192.168.0.102	192.168.0.1	DNS	71 Standard query 0x4da1 HTTPS.busygin.com
352	8.861628	192.168.0.102	192.168.0.1	DNS	71 Standard query 0x0101 A busygin.com
353	8.872053	192.168.0.1	192.168.0.102	DNS	131 Standard query response 0x4da1 HTTPS.busygin.com SOA ns1.gandi.net
354	8.969805	192.168.0.1	192.168.0.102	DNS	135 Standard query response 0x0101 A busygin.com A 18.245.86.22 A 18.245.86.7 A 18.245.86.32 A 18.245.86.11

Почему адрес, на который отправлен DNS-запрос, не совпадает с адресом посещаемого сайта?

Так как были очищены записи о DNS, поэтому необходимо обратиться к DNS-серверу и получить адрес, запрашиваемого сайта.

Какие бывают типы DNS-запросов?

Прямой: преобразование домена в IP-адрес.

Обратный: преобразование IP-адреса в домен.

Рекурсивный: выполняется DNS-сервером, пока не будет найден домен или не будет получен ответ, что домен не существует. Рекурсия выполняется сервером.

Итеративный: Запрос посылает доменное имя DNS серверу и просит вернуть либо IP адрес этого домена, либо имя DNS сервера, авторитетного для этого домена. Так работают корневые и TLD-сервера.

В какой ситуации нужно выполнять независимые DNS-запросы для получения содержащихся на сайте изображений?

Если адрес, на котором хранится изображение отличается от адреса сайта.

Этап 4. Анализ ARP-трафика

Необходимо отследить и проанализировать трафик протокола ARP, сгенерированный в результате выполнения следующих действий:

- очистить ARP-таблицу командой “netsh interface ip delete arpccache”;
- очистить кэш браузера;
- зайти на Интернет-сайт, заданный по варианту.

По результатам анализа собранной трассы, ответьте на следующие вопросы.

Администратор: Командная строка

Microsoft Windows [Version 10.0.19045.4412]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.
C:\Windows\system32>netsh interface ip delete arpccache
OK.

1042...	10298.140908	TuyaSmart_ca:a0:ea	Broadcast	ARP	42 ARP Announcement for 192.168.0.100
1042...	10308.176345	TuyaSmart_ca:a0:ea	Broadcast	ARP	42 ARP Announcement for 192.168.0.100
1042...	10308.764527	TpLinkTechno_ce:07:...	Intel_71:56:e2	ARP	42 Who has 192.168.0.105? Tell 192.168.0.1
1042...	10308.764543	Intel_71:56:e2	TpLinkTechno_ce:07:...	ARP	42 192.168.0.105 is at dc:71:96:71:56:e2
1043...	10318.108861	TuyaSmart_ca:a0:ea	Broadcast	ARP	42 ARP Announcement for 192.168.0.100
1044...	10328.144119	TuyaSmart_ca:a0:ea	Broadcast	ARP	42 ARP Announcement for 192.168.0.100
1044...	10330.089740	IntertechSer_6b:7c:...	Broadcast	ARP	42 ARP Announcement for 192.168.0.101

> Frame 104242: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface
> Ethernet II, Src: TuyaSmart_ca:a0:ea (70:89:76:ca:a0:ea), Dst: Broadcast (ff:ff:ff:f
▼ Address Resolution Protocol (ARP Announcement)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
[Is gratuitous: True]
[Is announcement: True]
Sender MAC address: TuyaSmart_ca:a0:ea (70:89:76:ca:a0:ea)
Sender IP address: 192.168.0.100
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.0.100

0000 ff ff ff ff ff ff 70 89
0010 08 00 06 04 00 01 70 89
0020 00 00 00 00 00 00 c0 a8

Какие MAC-адреса присутствуют в захваченных пакетах ARP-протокола? Что означают эти адреса? Какие устройства они идентифицируют?

70:89:76:ca:a0:ea - адрес отправителя

00:00:00:00:00:00 - broadcast

Какие MAC-адреса присутствуют в захваченных HTTP-пакетах и что означают эти адреса? Какие устройства они идентифицируют?

Присутствует MAC-адрес устройства, с которого производится http запрос и MAC-адрес маршрутизатора

Для чего ARP-запрос содержит IP-адрес источника?

Чтобы узел-получатель мог добавить информацию об узле-отправителе в свою ARP-таблицу.

Вывод:

В процессе выполнения работы я ознакомился с приложением Wireshark, на примере предоставленного ресурса понаблюдал за “трейсами” запросов разных типов, а также проанализировал назначение и особенности каждого из них