МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ ФГБОУ ВО «АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт цифровых технологий, электроники и физики Кафедра вычислительной техники и электроники (ВТиЭ)

Лабораторная работа № 7

Доступность информации. Анализ сетевого трафика. Снифферы.

Выполнил студент 595 гр.
А.В. Лаптев
Проверил:
П.С. Ладыгин
Лабораторная работа защищена
«»2023 г.
Оценка

Цель работы: рассмотрение методов обеспечения доступности информации, а также возможности анализа сетевого трафика на примере снифферов.

Задачи:

- 1. Работа с Wireshark.
 - 1.1. Запустите анализатор трафика Wireshark.
 - 1.2. Включите захват пакетов на вашей рабочей станции.
 - 1.3. Зайдите на сайт с HTTP соединением, например http://phys.asu.ru.
 - 1.4. Проанализируйте полученный трафик, найдите пакеты протокола НТТР.
 - 1.5. Вставьте в отчет скриншот одного из пакетов. В каком виде передаются данные?

В протоколе НТТР данные передаются в незашифрованном формате.

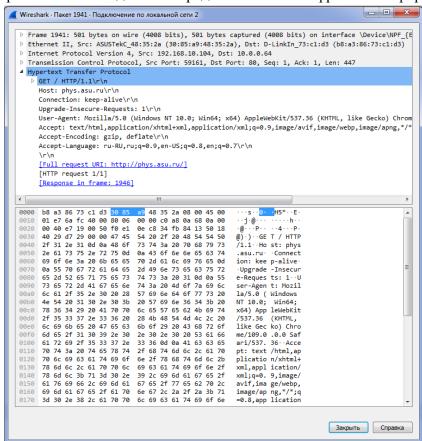


Рис. 1. Содержимое НТТР-пакета.

- 1.6. Перейдите на сайт с HTTPS соединением.
- 1.7. Вставьте в отчет скриншот одного из пакетов. В каком виде передаются данные?

В протоколе HTTPS данные передаются в зашифрованном виде.

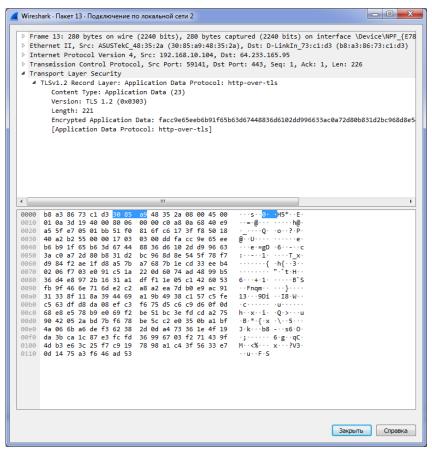
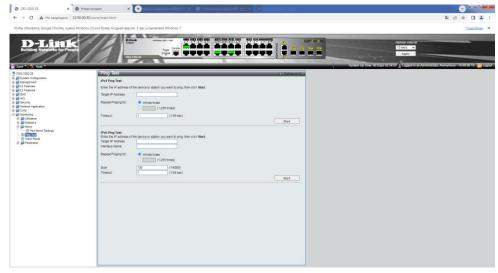


Рис. 2. Содержимое HTTPS-пакета.

- 2. Работа с коммутатором.
 - 2.1. Зайдите через браузер в web-интерфейс коммутатора D-Link DES 3200. По умолчанию коммутатор имеет IP адрес 10.90.90.90. Первоначально дайте своему компьютеру адрес в диапазоне 10.90.90.1-255 с маской подсети 255.255.255.0.
 - 2.2. Изучите настройки коммутатора, вставьте в отчет описание не менее двух пунктов меню со скриншотами.

Один из пунктов меню – Ping Test. Он нужен для проверки соединения между ПК в одной сети.



Puc. 3. Пункт меню – Ping Test.

В верхнее поле вводим IP-адрес, к которому хотим постучаться. Ниже устанавливаем количество пакетов для передачи и таймаут передачи.

Еще один пункт меню – настройка зеркалирования.

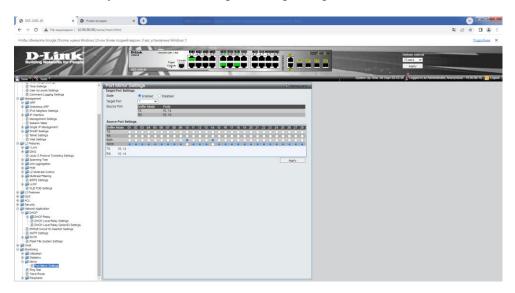


Рис. 4. Пункт меню – настройка зеркалирования.

Здесь выбираем порт, который будет зеркалом (выпадающий список). И выбираем номера портов, с которых будет перехватываться трафик.

- 2.3. Подключите к коммутатору ещё два компьютера, присвойте им адреса из того же диапазона.
- 2.4. Настройте на первый ПК «зералирование», например, подключившись к нему через консоль (возможна команда telnet), можно попробовать настройку через Web-интерфейс.
- 2.5. Включите на первом ПК Wireshark.
- 2.6. На втором ПК попробуйте команду ріпд к третьему ПК.
- 2.7. Проследите за появлением новых пакетов в программе Wireshark. Пакеты какого протокола захвачены анализатором? Вставьте скриншот в отчёт.

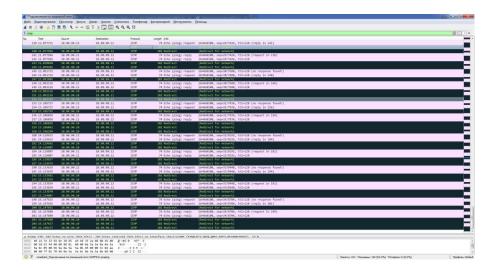


Рис. 5. Пакеты, захваченные Wireshark.

В результате перехвата были захвачены пакеты ІСМР (на приведенном скриншоте применен фильтр, поэтому видны только эти пакеты).

Ниже приведен пример содержимого таких пакетов.

```
Wireshark · Пакет 158 · Подключение по локальной сети 2
   Frame 158: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{E:
     Interface id: 0 (\Device\NPF_{E784CFC3-3074-4051-B3F7-0F2989CDE816})
      Encapsulation type: Ethernet (1)
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1679900926.316552000 seconds
      [Time delta from previous captured frame: 0.000000000 seconds]
      [Time delta from previous displayed frame: 0.000000000 seconds]
      [Time since reference or first frame: 13.106036000 seconds]
      Frame Number: 158
      Frame Length: 102 bytes (816 bits)
      Capture Length: 102 bytes (816 bits)
      [Frame is marked: False]
[Frame is ignored: False]
      [Protocols in frame: eth:ethertype:ip:icmp:ip:icmp]
      [Coloring Rule Name: ICMP errors]
   [Coloring Rule String: icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 ||

Fthernet TI Sec. ASHSTEAC 48:35:2a (30:85:a9:48:35:2a)

III | Dist. ASHSTEAC 23:69:8a (40:16:7a:23:69:8a)
      40 16 7e 23 69 8e 30 85 a9 48 35 2a 08 00 45 00 00 58 63 51 00 00 80 01 0e 8a 0a 5a 5a 0a 0a 5a
                                                                XcQ-
0030
0040
0050
                                                                                          Закрыть Справка
```

Рис. 6. Пример содержимого ІСМР-пакета.

Вывод: в ходе выполнения лабораторной работы были рассмотрены методы обеспечения доступности информации, а также возможности анализа сетевого трафика на примере снифферов.

Ответы на контрольные вопросы:

- 1. «Человек посередине» это кто?
 - О: «Человек посередине» вид атаки в криптографии и компьютерной безопасности, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом.
 - Является методом компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию.
- 2. Какие снифферы бывают?
 - О: Снифферы пакетов, снифферы Wi-Fi, снифферы сетевого трафика и снифферы пакетов IP.
- 3. Возможен ли перехват трафика в беспроводной сети?

О: Да, конечно. Для этого существует специальный вид снифферов – Wi-Fi снифферы.