Практическая работа № 8. Изучение пакетов с помощью программы Wireshark

Топология сети:

Задание:

Проведите анализ захваченных пакетов при помощи программы Wireshark и восстановите на жестком диске сайт, выполнив запрос в браузере к данному сайту по протоколу HTTP.

Решение:

1. Алгоритм работы для приложения Wireshark

1.1. Зайдите в удаленное рабочее место через Termidesk Client, где установлена ОС Astra Linux. Обратите внимание, что в PNETLab в данной практической работе входить не требуется!

1.2. Откройте браузер Firefox.

1.3. Запустите программу Wireshark и выберите интерфейс eth0 для захвата пакетов.

1.4. Откройте командную строку вашего рабочего места (можно вбить в поиске Терминал Fly) и чистите кеш ARP.

```
ip neigh flush all
```

Примечание:

`netsh interface ip delete arpcache` (для ОС Windows, требуется запустить командную строку от администратора)

`sudo arp -d` (для ОС MAC OS)

Для очистки кеша DNS на компьютере можно воспользоваться следующими командами (в данной практической работе они не используются):

`ipconfig /flushdns` (для ОС Windows)

`sudo /etc/init.d/nscd restart` (для ОС Linux)

`sudo dscacheutil -flushcache` (для ОС MAC OS)

1.5. Определите IP-адрес и MAC-адрес компьютера.

`ip a`

Примечание:

`ipconfig /all` (для ОС Windows)

`sudo ifconfig` (для ОС MAC OS)

2. Захват, поиск и изучение пакетов

2.1. Откройте веб-сайт dzen.ru в браузере.

2.2. Сверните окно браузера и вернитесь в программу Wireshark. Остановите процесс захвата данных. Вы увидите захваченный трафик.

Какие запросы выполнил компьютер, прежде чем обратился к серверу dzen.ru?

2.3. Отфильтруйте перехваченные данные, оставив только кадры ARP.

Какой фильтр вы применили?

2.4. Изучите поля в кадре ARP, MAC адрес назначения которого является адресом компьютера.

Для чего нужен протокол ARP?

Чей MAC адрес указан в кадре ARP?

2.5. Отфильтруйте перехваченные данные, оставив только пакеты DNS.

Какой фильтр вы применили?

2.6. Изучите поля в пакете DNS, идущем от сервера к компьютеру.

Для чего нужен протокол DNS?

Какой IP-адрес указан в поле протокола DNS и чему он принадлежит?

2.7. Отсортируйте данные таким образом, чтобы отображался только поток между компьютером и веб сервером.

Какой фильтр вы применили?

2.8. Найдите первый пакет, отправленный с компьютера на сервер dzen.ru.

Какую роль выполняет данный пакет?

Назовите номер порта источника TCP.

Как бы вы классифицировали порт источника?

Назовите номер порта назначения TCP.

Как бы вы классифицировали порт назначения?

Какие установлены флаги?

На какое значение настроен относительный последовательный номер?

2.9. Выберите следующий кадр в трехстороннем рукопожатии.

Назовите значения портов источника и назначения.

Какие установлены флаги?

На какие значения настроены относительный последовательный номер и номер подтверждения?

2.10. Изучите третий и последний пакет трехстороннего рукопожатия.

Какие установлены флаги?

3. Восстановление сайта из собранных данных

3.1. Повторите захват пакетов, выполнив запрос в браузере к сайту по протоколу HTTP: http://termilab.ru/ или http://mirea.org/ или любой другой сайт, доступный по http://

3.2. Сохраните перехваченные данные от веб-сервера (HTTP трафик) на жесткий диск (файл → экспортировать объекты → HTTP).

3.3. Запустите сайт с жесткого диска. Для этого можно указать расширение файла – .html.

Результат практической работы: показать восстановленный сайт с жесткого диска и ответы на вопросы, которые встречаются по ходу выполнения практической работы.