Лабораторная работа № 10

Тема: "Знакомство с анализаторами трафика. Wireshark.

Цель: Ознакомиться с использованием программы Wireshark для анализа сетевого трафика и основными принципами работы анализаторов трафика.

Необходимое оборудование/программное обеспечение:

- компьютеры с установленной операционной системой Windows или Linux - программа Wireshark.

Задание:

1. Захватите трафик во время выполнения ARP-запросов и ответов. Изучите структуру и содержимое ARP-пакетов. Определите процесс разрешения MAC-адресов на IP-адреса и обратно.

2. Захватите трафик во время процесса назначения IP-адреса DHCP-клиенту. Изучите структуру и содержимое DHCP-пакетов. Определите различные типы сообщений DHCP, такие как DHCP Discover, DHCP Offer, DHCP Request и т. д. Проанализируйте процесс назначения IP-адреса.

3. Захватите трафик между клиентом и сервером во время выполнения TCP-соединения. Изучите процесс установления, поддержки и завершения соединения TCP. Определите флаги TCP, такие как SYN, ACK, FIN и т. д., и их использование в различных этапах соединения.

4. Захватите трафик во время просмотра веб-страницы в браузере. Исследуйте HTTPзапросы и ответы, чтобы понять структуру и содержимое протокола. Определите заголовки запросов и ответов, а также параметры, передаваемые в URL и тела сообщений. Сравните различные методы HTTP (GET, POST, PUT и т. д.) и их использование в разных сценариях.

5. Захватите трафик во время выполнения DNS-запросов, например, попробуйте открыть веб-сайт в браузере. Когда DNS-запрос выполнен остановите запись трафика и изучите структуру и содержимое DNS-пакетов и проанализируйте следующую информацию:

   - Query Name: Имя домена, запрошенного у DNS-сервера.
   - Query Type: Тип DNS-запроса (например, A, AAAA, MX).
   - Response: Ответ DNS-сервера, включая IP-адреса или другие данные.

Отчет должен содержать:

- скриншоты Wireshark, подтверждающие выполнение заданий.
- выводы.