Лабораторная работа №9. Изучение пакетов с помощью программы Wireshark

Топология

Задачи

Часть 1. Подготовка операционной системы компьютера

Часть 2. Захват поиск и изучение пакетов

Часть 3. Защита лабораторной работы (ответы на контрольные вопросы и вопросы преподавателя)

Необходимые ресурсы

- 1 ПК с доступом к командной строке, Интернету и установленному анализатору пакетов Wireshark.

Часть 1: Подготовка операционной системы компьютера

В части 1 потребуется подготовить операционную систему к захвату пакетов.

Шаг 1: Удаление результатов обращения к устройствам в сети.

a. Очистите кеш ARP на компьютере.

b. Очистите кеш DNS на компьютере.

Шаг 2: Узнайте адреса интерфейсов ПК.

a. Определите ip адрес компьютера.

b. Определите MAC адрес компьютера.

Часть 2: Захват, поиск и изучение пакетов

Шаг 1: Запустите программу Wireshark и выберите подходящий интерфейс.

Шаг 2: Захват пакетов.

a. Нажмите кнопку Start (Старт), чтобы начать захват данных.

b. Откройте веб-сайт www.yandex.ru в браузере.

c. 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 yandex.ru?

Шаг 3: Анализ пакетов ARP.

a. Отфильтруйте перехваченные данные оставив только кадры ARP.

Какой фильтр вы применили?

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

Для чего нужен протокол ARP?

Чей MAC адрес указан в кадре ARP?

Шаг 4: Анализ пакетов DNS.

a. Отфильтруйте перехваченные данные оставив только пакеты DNS.

Какой фильтр вы применили?

b. Изучите поля в пакете DNS идущем от сервера к компьютеру.

Для чего нужен протокол DNS?

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

Шаг 5: Изучите трафик между компьютером и веб сервером.

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

Какой фильтр вы применили?

b. Найдите первый пакет, отправленный с компьютера на сервер yandex.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?

c. Выберите следующий кадр в трёхстороннем рукопожатии.

Назовите значения портов источника и назначения.

Какие установлены флаги?

На какие значения настроены относительный последовательный номер и номер подтверждения?

d. Изучите третий и последний пакет трёхстороннего рукопожатия.

Какие установлены флаги?

Шаг 6: Восстановление сайта из собранных данных.

a. 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://

b. Сохраните перехваченные данные от веб-сервера (HTTP трафик) на жесткий диск.

c. Запустите сайт с жесткого диска.

Часть 3: Защита лабораторной работы (ответы на контрольные вопросы и вопросы преподавателя)

1. В программе Wireshark доступны сотни фильтров. В большой сети может быть множество фильтров и различных типов трафика. Какие три фильтра в списке будут наиболее полезны для сетевого администратора?
2. Как ещё можно использовать программу Wireshark в производственной сети?