Компьютерные сети

Лабораторная работа №3

Анализ пакетов в симуляции Cisco и реальных условиях Wireshark

Задачи:

- Установить программу для анализа трафика Wireshark и ознакомится с интефрейсом
- Построение топологии сети в симуляторе Cisco Packet Tracer с использованием сетевого анализатора
- Изучение содержания пакетов протоколов ICMP, ARP и STP внутри симулятора Cisco
- Изучение пакетов в сетевом анализаторе Wireshark на основе реальных примеров.

Ход работы:

- Установить симулятор Cisco Packet Tracer и сетевой анализатор Wireshark
- Построить простую топологию в симуляторе используя встроенный сетевой анализатор
- Отправить несколько пакетов через топологию для создания записи в сетевом анализаторе
- Проанализировать пакеты проходящие через сеть протоколов ICMP и ARP сделав записи.
- Ознакомится с интерфейсом программы Wireshark.
- При включённом анализаторе посетить предоставленную ссылку и заполнить фиктивные данные в поля логина и пароля.
- Проанализировать HTTP запрос на наличие незащищённых данных.
- Также при включённом анализаторе сетевого трафика заполнить фиктивные данные на странице имеющую приписку HTTPS в начале ссылки.
- Используя утилиту ping отправить несколько пакетов на адрес 8.8.8.8 для анализа протокола ICMP.
- Используя командную строку удалить ARP записи таблицы.
- Сделать вывод по проделанной работе.

Содержание отчёта:

- Титульный лист
- Задачи для выполнения

- Результаты проведения работы с комментариями, изображениями и объяснениями
- Выводы по проделанной работе

Введение

Анализ сетевого трафика является одной из ключевых задач в области компьютерных сетей. Понимание структуры сетевых пакетов, принципов их передачи и взаимодействия сетевых протоколов позволяет эффективно диагностировать неисправности, выявлять уязвимости и оптимизировать работу сети. В условиях роста объёмов передаваемых данных и усложнения сетевой инфраструктуры навыки анализа трафика становятся особенно актуальными.

В данной практической работе используются программные средства Cisco Packet Tracer и Wireshark. Cisco Packet Tracer представляет собой симулятор сетевого оборудования, позволяющий моделировать работу локальных и глобальных сетей, настраивать маршрутизаторы, коммутаторы и конечные устройства, а также отслеживать процесс передачи данных между ними. Использование режима симуляции даёт возможность визуально наблюдать прохождение пакетов по сети и анализировать работу различных протоколов.

Wireshark является мощным анализатором сетевых протоколов, предназначенным для перехвата и детального изучения сетевого трафика в реальном времени. Программа позволяет исследовать содержимое пакетов на различных уровнях модели OSI, анализировать заголовки протоколов, определять типы передаваемых данных и выявлять возможные аномалии.

Целью данной работы является изучение структуры сетевых пакетов, анализ их прохождения по сети и закрепление теоретических знаний о работе протоколов ICMP, ARP и HTTP на практике. В ходе выполнения работы планируется смоделировать сеть в Cisco Packet Tracer, сгенерировать сетевой трафик и выполнить его анализ встроенной компонентой симулятора sniffer. С помощью Wireshark, проанализровать трафик в реальном времени.

Реализуемые задачи

Первая часть 1. Анализ пакетов в симуляторе Cisco Packet Tracer.

В данной части необходимо провести анализов проходящих пакетов используя встроенные компоненты сетевого симулятора Cisco Packet Tracer. Для анализа пакетов будет использоваться встроенный sniffer, необходимо построить топологию сети по указанной схеме, переслать несколько пакетов через сетевой анализатор и по сохранённым записям проанализировать их содержимое. Необходимо проанализировать содержимое пакетов протоколов ICMP, ARP.

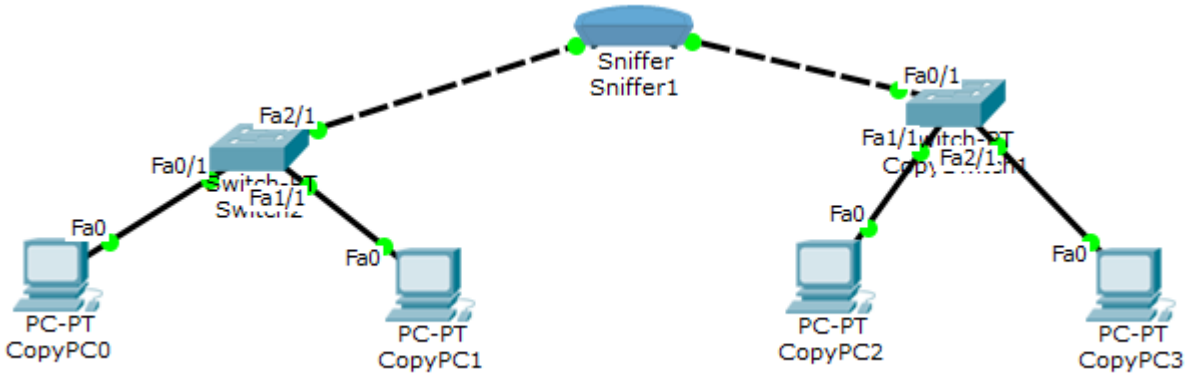

Схема 1. Топология с использованием сниффера.

Основные шаги:

1. Построить топологию сети как на представленной схеме. Для построения сети использовать 2 x Switch-PT (Generic), 4 x Компьютера, 1 x Sniffer (Категория End devices).

2. Для подключения к Sniffer использовать кабель Copper Cross-Over.

3. Распределить IP адреса используя сеть 192.168.X.0 (X – номер в группе) и маску 255.255.255.0.

4. Зайти в интерфейс Sniffer раздел GUI и посмотреть изначальный список.

5. После распределения IP адресов отправить пакет типа ICMP (Simple PDU) с PC 1 на PC 3.

6. Зайти в интерфейс Sniffer и проверить какие пакеты были переданы в сети.

Какие пакеты появились после отправки одного пакета ICMP? Какие адреса получателя и отправителя? Какой показатель TTL (Time to Live)?

7. Проанализировать содержимое пакетов ARP и ICMP.

   Зачем в сети используется протоколы ARP и ICMP? Сколько количество информации отправляет каждый? Что из себя представляет Ethernet Frame? На каких уровнях модели OSI работают данные протоколы?

Вторая часть 2. Анализ пакетов в режиме реального времени используя Wireshark.

В данной части необходимо провести анализ пакетов проходящих через сеть в режиме реального времени используя программный сетевой анализатор Wireshark. Для проведения анализа пакетов необходимо установить сетевой анализатор и применить фильтры для получения необходимых результатов.

1. Установить сетевой анализатор Wireshark.
2. В открытом интерфейсе программы установить сетевой фильтр на интерфейс «Беспроводная сеть».
3. В верхней строке возможно использовать фильтры для определения необходимых пакетов протоколов.
4. В включённым анализатором пакетов и выставленным фильтром «icmp» зайти в командную строку (CMD) и используя утилиту ping отправить несколько пакетов типа ICMP на адрес 8.8.8.8.
5. Проверить что выдаёт сетевой анализатор.

   Отличаются ли пакеты от тех что в симуляторе? Какая информация содержится в пакетах протокола ICMP?

6. Для проверки действия протокола ARP понадобится очистить таблицу записей ARP. Запустите командную строку от имени администратора.
7. Используя команду «arp -a». Какой результат получен?
8. Не выключая сетевой анализатор. Пропишите команду «netsh interface IP

delete arpcache» для очистки таблицы.

9. В сетевом анализаторе примените сетевой фильтр «arp».

   Что появилось в результате ваших действий? Проанализировать результат работы сетевого анализатора и пакеты ARP.

10. Запустите Wireshark, откройте веб-браузер и подключитесь к незащищенному http-серверу (например, http://www.vbsca.ca/login/login.asp) , введите информацию на экране входа (вымышленное имя и пароль) и отправьте ее на сервер.

11. Остановите захват и проанализируйте содержимое пакетов, применив фильтры отображения.

12. Найдите в захватах пакетов введенную информацию для входа.

    Какой IP адрес ваш и какой сервера? Какой MAC адрес ваш и сервера?

13. Произведите те же самые действия, но используя сайт с сертификатом безопасности (HTTPS).

    Какая разница в HTTPS и HTTP? Почему некоторые данные не видны?