Лабораторная работа №7

Тема: Создание простой конфигурации сети. IP -адресация. Мониторинг сети. Анализ трафика. Использование сниферов для анализа сетевых пакетов.

Цель работы: изучить принципы анализа сетевого трафика.

Методические рекомендации по выполнению лабораторной работы:

В начале 1990 -х годов он широко использовался хакерами для захвата пользовательских входов и паролей. Широкое использование концентраторов позволило вам захватить трафик без особых усилий в больших сегментах сети.

Снифферы:

https://www.anti-malware.ru/threats/sniffers

https://trends.rbc.ru/trends/industry/60f6c2af9a7947fc32ae0a91

Сниферы используются как для хороших, так и для разрушительных целей. Анализ трафика, пройденного сквозь снифер, позволяет вам:

1) Мониторинг сетевой активности приложений.

2) Протоколы отладки сети.

3) Найдите ошибку неисправности или конфигурации.

4) Обнаружение паразитического, вирусного и петлевого трафика, присутствие которого увеличивает нагрузку сетевого оборудования и каналов связи.

5) Определите злонамеренное и несанкционированное программное обеспечение в сети, например, сетевые сканеры, ливни, трояны, клиенты одноранговых сетей и других.

Перехватите любой незашифрованный (а иногда и зашифрованный) пользовательский трафик с целью работы по распознаванию паролей и другой информации.

Задание:

1. Изучите интерфейс Wireshark (\\ corp.mgkit.ru \ dfs \ work \ wireshark)

2. Захватить 100 произвольных пакетов. Определите статистические данные:

- процент трафика различных протоколов в сети;

- средняя частота кадров / сек;

- средняя скорость байтов/сек;

- минимальные, максимальные и средние размеры пакета;

- степень использования пропускной способности канала (загрузка сети).

3. Исправьте 20 IP -пакетов. Определите статистические данные:

- процент трафика различных протоколов стека TCP / IP в сети;

- Средний, минимальный, максимальный размер упаковки.

4. Выполните анализ ARP-протокола, следуя примеру из руководящих принципов.

5. Для примера IP -пакета укажите структуры протокола Ethernet и IP, отметьте поля заголовка и опишите их.

Проанализируйте и опишите принцип эксплуатации утилиты Ping. В этом случае опишите все протоколы, используемые утилитой. Опишите все поля протоколов. Создайте диаграмму взаимодействия ПК при запуске утилиты Ping.

Контрольные вопросы:

1. Каковы основные цели мониторинга сетевого трафика?

2. В чем разница между мониторингом трафика и фильтрацией?

3. Какова цель класса программ Sniffer?

4. Каковы основные функции снижения?

5. Почему используются фильтры Wireshark Sniffer и фильтры захвата? В чем их отличие?

6. Какие основные функции статистической обработки захваченных пакетов - Wireshark Sniffer?

7. Какие задачи предназначены для решения протокола ARP?

8. Назовите задачи протокола ARP.

Форма отчетности: электронная версия заданий, ответы на контрольные вопросы в письменной форме.