Міністерство освіти і науки України

Центральноукраїнський національний технічний університет

**МЕХАНІКО-ТЕХНОЛОГІЧНИЙ ФАКУЛЬТЕТ**

Кафедра кібербезпеки та програмного забезпечення

**Звіт**

з виконаної лабораторної роботи № 7

Дисципліна: Комп'ютерні мережі

Виконав :

студент академічної групи КІ-15

Аннаєв А. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Перевірив :

Викладач

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кропивницкий- 2018

Лабораторная работа № 7

**Тема**: Использование сетевых анализаторов.

**Цель**: Получить практические навыки использования сетевых анализаторов

**Необходимо знать**: Основы сетевого взаимодействия.

**Задание** :

Используя свободно избранный сетевой анализатор (рекомендуется Wireshark) провести сканирование локальной сети во время работы разработанного клиент-серверного ПО в лабораторной работы №6.

Проанализировать трафик локальной сети, с помощью фильтров избранного сетевого анализатора, выделить пакеты разработанного клиент-серверного ПО. Сформировать отчет работы клиент-серверного ПО с комментариями.

Контрольные вопросы

1. Какими способами может осуществляться перехват трафика?

* Обычным «прослушиванием» сетевого интерфейса
* подключением снифера в разрыв канала;
* ответвлением трафика и направлением его копии на снифер;
* через анализ побочных электромагнитных излучений и восстановление трафика, таким образом прослушивается;
* через атаку на канальном (2) (MAC-spoofing) или сетевом (3) уровне (IP-spoofing)

1. Анализ трафика, прошедший через сетевой анализатор, позволяет?

* Выявить паразитный, вирусный и закольцованный трафик, наличие которого увеличивает загрузку сетевого оборудования и каналов связи (сниферы здесь малоэффективны; как правило, для этих целей используют сбор разнообразной статистики серверами и активным сетевым оборудованием и ее последующий анализ).
* Выявить в сети вредоносное и несанкционированное ПО , например, сетевые сканеры, флудеры, троянские программы, клиенты пиринговых сетей и другие (это обычно делают при помощи специализированных снифер - мониторов сетевой активности).
* Перехватить любой незашифрованный (а порой и зашифрованный) пользовательский трафик с целью получения паролей и другой информации.
* Локализовать неисправность сети или ошибку конфигурации сетевых агентов (для этой цели сниферы часто применяются системными администраторами )

1. Приведите наиболее распространенные существующие сетевые анализаторы?

* Wireshark
* tcpdump
* pcap - библиотека
* Iris

1. Какие преимущества использования сетевого анализатора Wireshark от существующих аналогов?

Wireshark — это приложение, которое «знает» структуру самых различных сетевых протоколов, и поэтому позволяет разобрать сетевой пакет, отображая значение каждого поля протокола любого уровня. Поскольку для захвата пакетов используется pcap, существует возможность захвата данных только из тех сетей, которые поддерживаются этой библиотекой. Тем не менее, Wireshark умеет работать с множеством форматов входных данных, соответственно, можно открывать файлы данных, захваченных другими программами, что расширяет возможности захвата.

1. С помощью каких средств можно снизить угрозу сетевого анализа трафика?

* Аутентификация.
* Коммутируемая инфраструктура
* Антиснифферы.
* Криптография