**Лабораторная работа № 2. Сетевая безопасность**

**Рассматриваемые вопросы:**

* Проведение сетевых атак
* Детектирование сетевых атак

**Справочный материал:**

* Nmap
* Wireshark
* Snort

**Задание на лабораторную работу:**

Запускам Nmap с опцией  определения версии ОС

Анализируем отправленные пакеты используя Wireshark

Разбираемся в том какие именно пакеты были использованы для определения версии ОС

Устанавливаем систему обнаружения атак Snort

Пишем правила обнаружения атак (сигнатуры) для Snort которые позволят определить факт работы Nmap определяющего версию операционной системы

Демонстрируем что сканирование обнаруживается

Сигнатура должна быть такой чтоб у нее не было ложных срабатываний. То есть чтобы в обычной жизни она не говорила на нормальные пакеты что это попытка сканирования попадаться в реальной жизни когда не происходит сканирования)

.