СЛАЙД 1:

Здравствуйте, меня зовут Мышкин Артем Евгеньевич. Тема моей курсовой работы «Метод обнаружения сетевых атак» научный руководитель старший преподаватель Кожекина Елена Николаевна

СЛАЙД 2: Предотвращение сетевых атак – одна из самых сложных задач в области защиты информационных систем. Большинство современных систем имеет распределенную структуру, в основе их архитектуры лежит использование сетевых технологий. И обеспечение работоспособности таких систем зависит от способности противостоять злонамеренным действиям, которые направлены на нарушение работы как самой сети, так и информационной системы, функционирующей в ее рамках. Одним из наиболее опасных видов преступной деятельности в сети Интернет являются так называемые сетевые атаки. Как свидетельствует статистика, количество сетевых атак продолжает расти, методы, которыми пользуются преступники, постоянно развиваются и совершенствуются

СЛАЙД 3:  
**Цель работы -** повышение эффективности обнаружения атак и принятия решений на основе утилиты wireshark, nmap.

**Объектом исследования -** алгоритмическое и программное обеспечение защиты информации.

**Предмет исследования** – практические примеры как результат применения того или иного метода.

СЛАЙД 4:

Для изучения были выбраны следующие утилиты

* Wireshark
* Nmap
* Встроенные системные утилиты Windows

СЛАЙД 5:

Я использовал свою основную Windows 10 и Kali Linux  
Возникли проблемы с настройкой Kali linux. Для их устранения нужно правильно определить сеть в VirtualBOX.  
1. Откроем параметры машины

2. Сеть

3. Стандартно стоит параметр NAT- это общая сеть. Он нам не подходит.

4. Меняем на Сетевой мост и выбираем имя устройства(в моем случае, отдельная сетевая карта WIFI)

Я выбрал Kali Linux, т.к все утилиты которые нам понадобятся уже есть в самой системе и ничего настраивать в самой системе не нужно.

СЛАЙД 6: Вошли в Kali и запустили там программу nmap, провел сканирование моей основной системы, с профилем Intense scan.

А в Windows, в это время, я включить Wireshark, которым “прослушивал” сеть. Результаты на слайде: 7

СЛАЙД 7: В это время, в Windows я включить Wireshark, которым “прослушивал” сеть. Получил такие результаты

Видно, что была куча запросов на мою сеть. Проверка разных портов и поиск любой информации

СЛАЙД 8:

Но т.к человек не способен за всем уследить я использовал script, написанный на python

Файл который я сохранил на windows wireshark, не заметил ничего подозрительного   
А вот тот который я взял из linux, script обнаружил угрозу и флаг SYN-ACKs

СЛАЙД 9: Я зашел в wireshark. Показать что человек способен увидеть угрозу

СЛАЙД 10: В данном случае рассмотрена статистика NMAP сканирования, по которой ясно, что если в сети мощного Warning и Error флагов, то происходит что то нетипичное (но это не является однозначным критерием того, что сеть сканируют).

СЛАЙД 11: Можно заметить, что в случае нормального поведения количество данных по отношению к пакетам, переданным за секунду несколько разнится. Но опять-таки это не стопроцентный показатель того, что сеть подверглась сканированию

СЛАЙД 12: Сканирование можно определять и в режиме реального времени.

Есть такие способы:

1. Мониторить Wireshark (но это делается человеком и высока вероятность пропуска важной информации).
2. Использовать специальные скрипты снифферы-анализаторы.
3. Использовать IDS (системы обнаружения вторжений), апример Snort, в котором выставлен флаг обнаружения сканирования в конфигурационном файле.