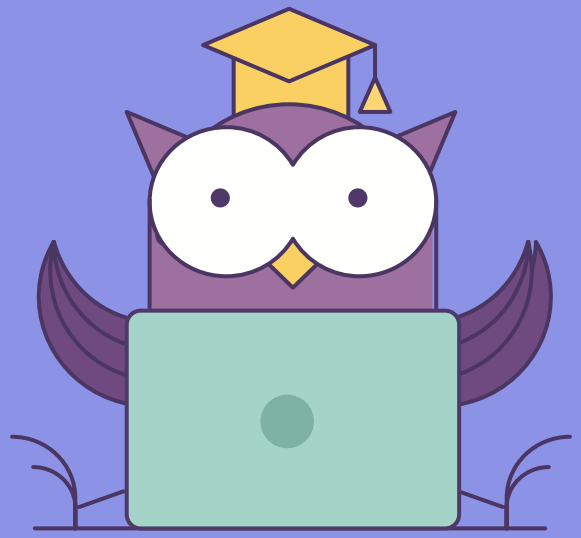
ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

Сканирование и идентификация сервисов. Как это работает.

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

- **Сканирование сети**
- **nmap**
  - Функциональные возможности
  - Стандартные сканирования
  - Скриптовый движок

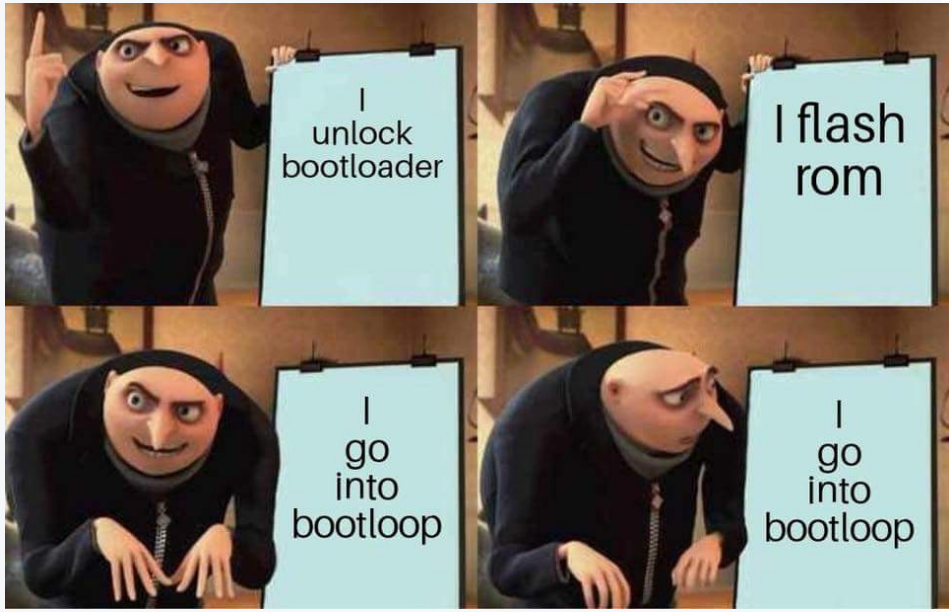
- **Практика**
  - Сканирование сети

Цели занятия

1. Разобраться со стеком протоколов сетевого взаимодействия

2. Разобраться с принципом работы методик сканирования

3. Получить навыки работы с утилитами для сканирования сети



00

Сканирование сети

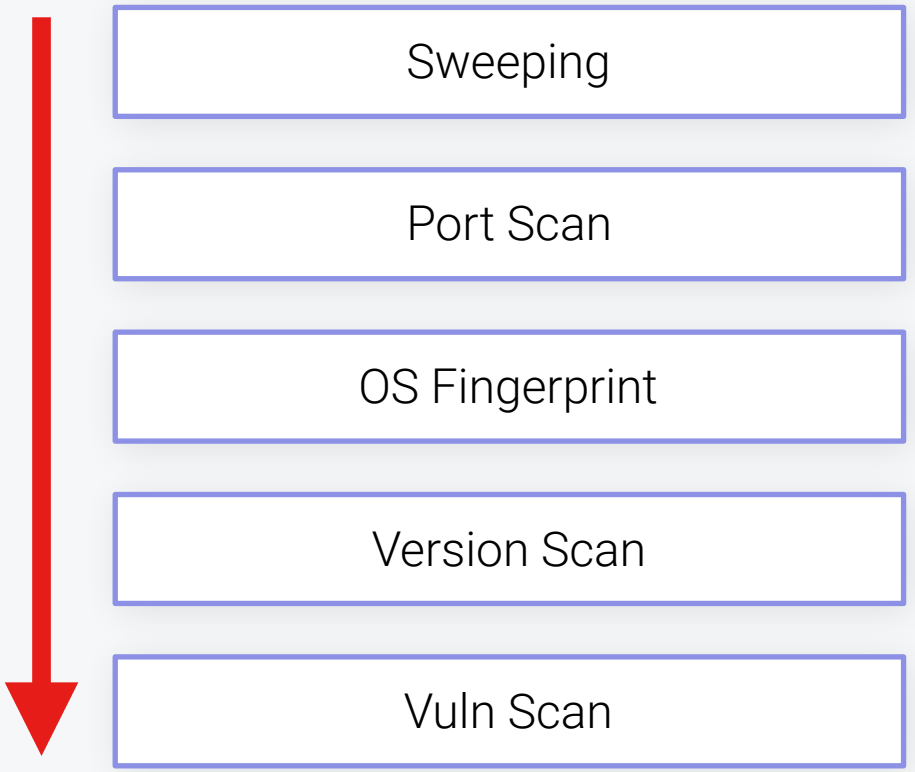
Сканирование

Сканирование:

- Процесс сбора информации о хостах и установленных на них сервисах

Типы:

- Sweeping
- Port Scan
- OS Fingerprint
- Version Scan
- Vuln Scan



01

NMAP

NMAP

Основные данные:

- Утилита для сканирования сети и проведения аудита безопасности
- Создана в 1997 году
- Кросплатформенная
- Использует сырые сокеты для определения характеристик сервисов
- Имеет встроенный движок для скриптования действий производимых с данными

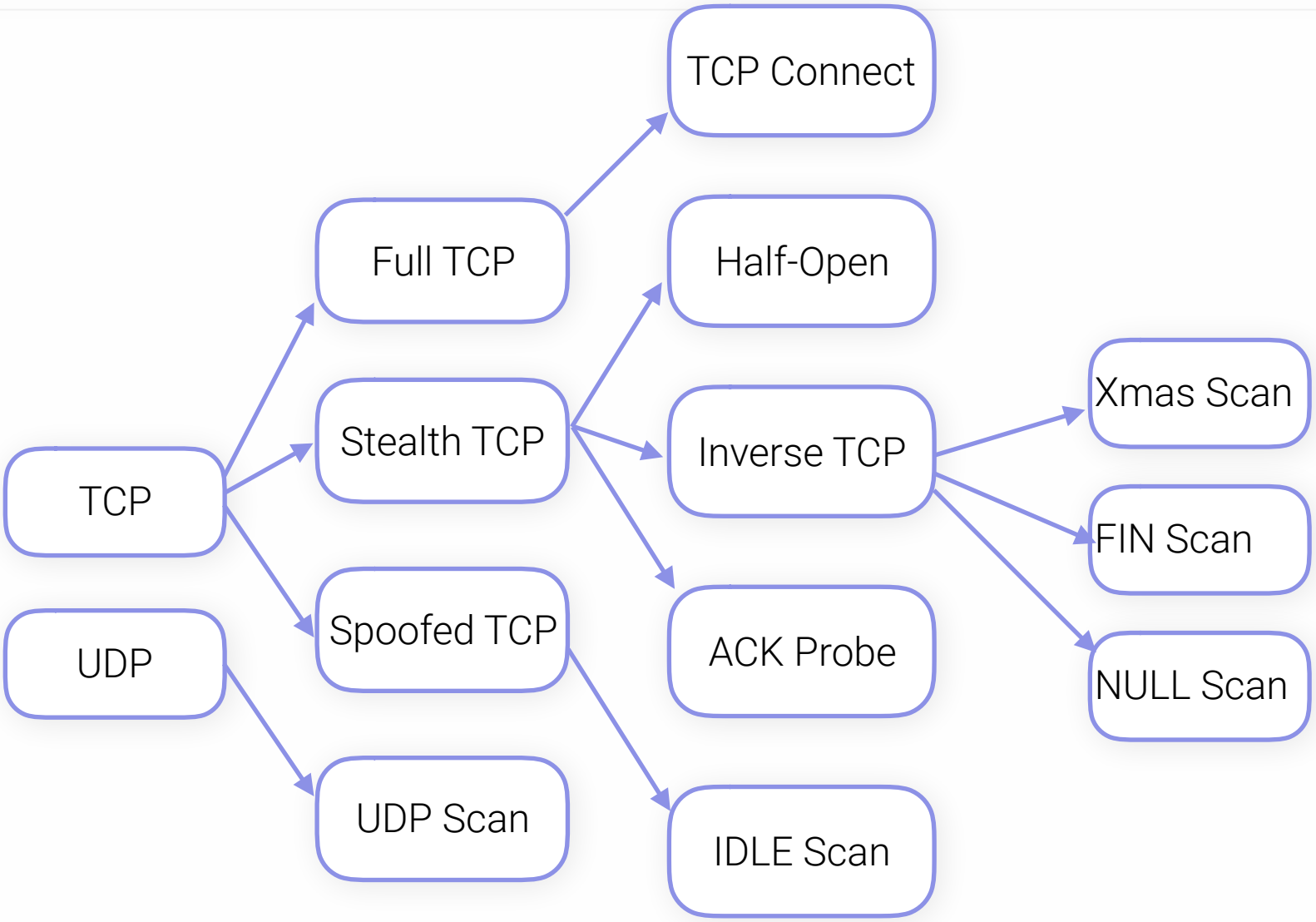
02

Функциональные возможности

03

Стандартные сканирования

Типы сканирований и протоколы

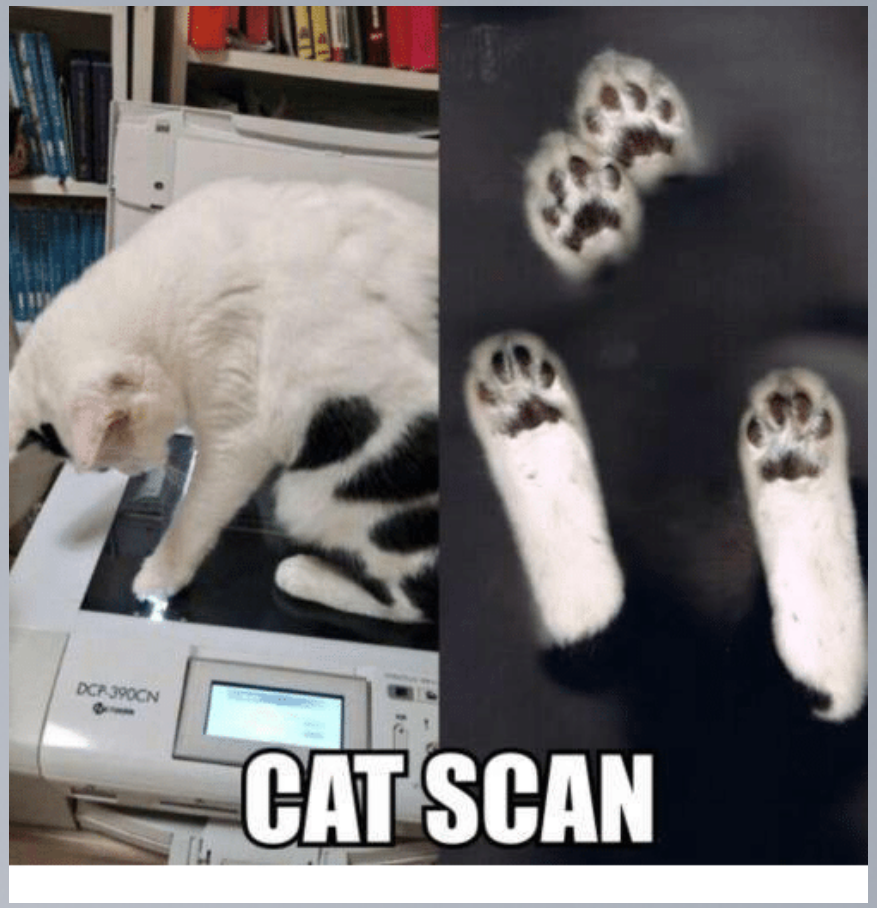


nmap

Сканирование:

Типы сканирования:

1. Syn, Fin, Ack, Xmas, Mainmon
2. Ping scan
3. Zombie Scan



Александр Колесников

Спасибо
за внимание!