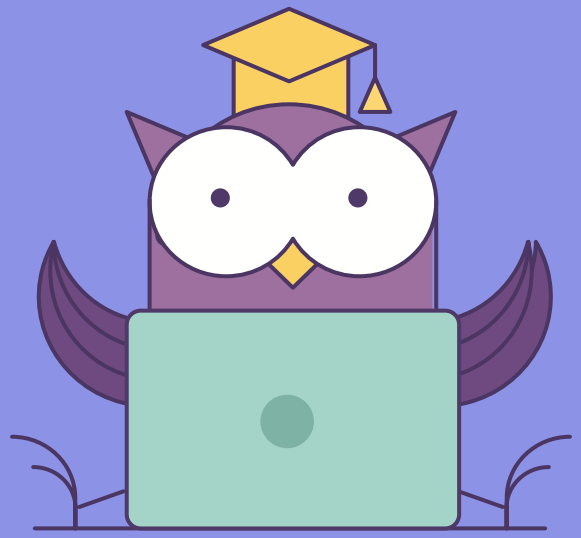
ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

«Инструментарий для проведения Pentest»

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

- Инструментарий
  - Рекомендации
  - Возможные дистрибутивы
- Kali Linux
  - Основные группы инструментов и их использование
  - Что поставить дополнительно

01

Инструментарий

02

Рекомендации

Рекомендации

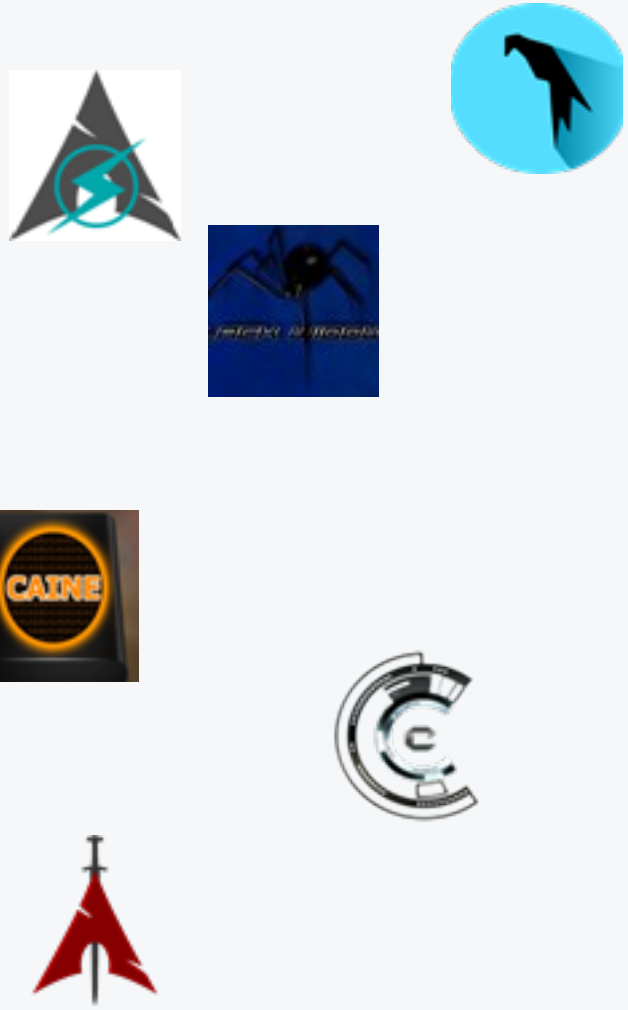
- Проведение легального Pentest всегда регламентируется в соответствии со стандартом или рекомендацией
- Известные рекомендации:
  - PTES
  - OWASP

03

Возможные дистрибутивы

Дистрибутивы

- Дистрибутивы для проведения тестирования:
  - BlackArch
  - Parrot Security
  - Kali Linux
  - Santoku Linux
  - Cyborg Linux
  - Caine
  - ArchStrike
  - BugTraq



04

Kali Linux

05

Основные группы инструментов

06

Что поставить дополнительно

Docker

- Приложение для управления контейнерами
  - Зачем нужно нам:
    - Виртуализация исследуемого сервиса
    - Простота развертывания на новом сервере

BetterCap

- Фреймворк, который включает в себя множество атак на сети.
- Список атак:
  - WiFi:
    - Deauthentication attack
    - Clienteles PMKID association attack
    - Automatic WPA/WPA2 handshake capture
  - Bluetooth scanning
  - ARP spoofing
  - DNS spoofing
  - DHCPv6 spoofing
  - Sniffing

01

Metasploit

Колесников Александр

Спасибо
за внимание!