ВЗЛОМ И ЗАЩИТА БЕСПРОВОДНЫХ СЕТЕЙ

ЧАСТЬ 1. БИБЛИЯ ВАРДРАЙВЕРА И ДЕФЕНДЕРА

Введение [00:06:42]

- идеология курса;
- современные реалии вардрайвинга;
- идея о создании курса;
- теория и практика;
- почему важно знать теорию;
- структура курса;
- виртуальная машина с нужными инструментами.

Урок №1. Основы беспроводной связи [00:29:07]

- природа WiFi сетей;
- WiFi с точки зрения физики;
- области применения радиоволн;
- свойства радиоволн;
- основные характеристики радиоволн;
- радиоволны используемые в радиотехнике;
- шкала электромагнитных излучений;
- распределение радиоволн по диапазонам;
- частоты используемые в беспроводных сетях;
- частота и длина волны;
- радиоволны и вода;
- свойства WiFi сигнала;
- факторы окружающей среды влияющие на дальность передачи сигнала;
- вреден ли WiFi;
- ограничения на мощность передатчика WiFi устройств;
- мифы о вреде WiFi сигнала;
- комментарии врача-рентгенолога о вредности WiFi.

Урок №2. Основы Wi-Fi сетей. Модуль 1 [00:27:58]

- что такое WiFi;
- основные стандарты WiFi;
- WiFi Alliance и IEEE 802.11;
- другие стандарты WiFi;
- частоты 2.4 и 5 ГГц;
- графическое представление каналов;
- интерференционное ослабление радиоволн;
- терминология в среде WiFi;
- аутентификация и шифрование в WiFi сетях;

- методы аутентификации;
- алгоритмы шифрования;
- WPA Personal и WPA Enterprise;
- режимы работы WiFi устройств.

Урок №2. Основы Wi-Fi сетей. Модуль 2 [00:28:50]

- скорости передачи данных в среде WiFi;
- почему роутер режет скорость;
- теоретическая и реальная скорости передачи данных;
- канальная скорость;
- факторы влияющие на скорость подключения:
  - служебный трафик;
  - производительность оборудования;
  - коммутация WLAN-WLAN;
  - обратная совместимость стандартов;
  - ширина канала;
  - шифрование;
  - Quality of Service (QoS);
  - WiFi Multimedia (WMM/WME);
  - ассиметрия сигнала;
  - драйвер и прошивка.

Урок №3. Установка ОС Kali Linux [23:35]

- чем обусловлен выбор ОС;
- варианты установки Kali;
- выбор образа для установки;
- подготовка для установки Kali на VMware;
- подготовка для установки Kali параллельно с Windows;
- создание загрузочной флешки для установки Kali на железо;
- пошаговая установка ОС на VMware или ПК;
- изменение порядка загружаемых ОС;
- обновление системы.

Урок №4. Выбор Wi-Fi адаптера [00:57:39]

- инструменты вардрайвера/пентестера;
- особенности аппаратных ревизий WiFi устройств;
- преимущества USB WiFi адаптеров;
- требования к WiFi устройствам для вардрайвинга;
- определение чипа WiFi устройства;
- маркировка WiFi устройств;
- федеральная комиссия по связи/FCCID;
- определение возможностей чипа;
- популярные чипы и адаптеры для вардрайвинга;
- как не ошибиться при выборе устройства для пентестинга;

- мои рекомендации по выбору девайса;
- где купить оригинальный адаптер ALFA Network;
- где взять спецификацию к устройству;
- как отличить подделку от оригинала ALFA;
- как проверить оригинальность устройства по MAC и SN.

Урок №5. Пакет программ Aircrack-NG [01:02:06]

- установка VMware Tools для виртуалки Kali Linux;
- установка сетевых инструментов;
- устойчивые имена сетевых интерфейсов;
- режимы работы WiFi адаптера;
- особенности режима мониторинга/airmon-ng;
- перехват трафика/airodump-ng;
- детальный анализ отображаемых данных;
- разбор понятия "уровень сигнала";
- от чего зависит мощность сигнала;
- дополнительные опции airodump-ng;
- что такое Probe Request;
- непроассоциированные клиенты;
- сортировка и маркировка сетей;
- перехват трафика на конкретной точке доступа;
- по каким данным можно ориентироваться об уровне и качестве связи;
- что такое 4-way handshake;
- принцип взлома хендшейка "на пальцах";
- отключение WiFi клиентов от сети/aireplay-ng;
- директивы aireplay-ng;
- что такое ACK пакеты и о чём они говорят;
- как сохранить перехваченные данные;
- как увеличть мощность адаптера;
- как узнать ESSID скрытой сети;
- взлом WPA 4-way hanshake/aircrack-ng;
- подбор пароля к хендшейку на виртуалке;
- подбор пароля к хендшейку в среде Windows;
- итоги по набору инструментов aircrack-ng.

Урок №6. Брутфорс WPA хендшейка с помощью Hashcat [01:28:47]

- введение в Hashcat;
- факторы влияющие на скорость перебора;
- что такое свободные драйвера/nouveau;
- как быбрать правильный драйвер для Linux;
- установка Hashcat в Linux;
- почему Hashcat не видит видеокарту;
- как отключить драйвера nouveau;
- установка правильных драйверов для видеоадаптера;

- запуск и проверка работоспособности Hashcat;
- конвертация хендшейка в формат Hashcat средствами aircrack-ng;
- конвертация хендшейка в формат Hashcat средствами hashcat-utils;
- как посмотреть результаты по взломанным сетям;
- как удалить файл с сохраненными результатами/.pot файл;
- hashcat-utils для Windows;
- подбор пароля по группе словарей;
- совместный перебор CPU+GPU;
- групповой перебор: несколько словарей+несколько хешей;
- разновидности брутфорса в Hashcat;
- принцип и применение комбинированной атаки;
- брутфорс по маске/как создать шаблон пароля;
- сгорела видеокарта/сравнение производительности карт;
- подбор пароля основанного на кастомном наборе символов;
- перебор по списку масок/.hcmask
- гибридная атака/словарь+маска;
- создаем собственный словарь для гибридной атаки;
- гибридная атака/маска+словарь;
- атаки Hashcat основанные на правилах;
- генератор словарей crunch;
- генерация словаря из нескольких других;
- разбор инструментов hashcat-utils;
- применение правил к сформированному словарю.

Урок №7. Pairwise Master Key Identifier [00:47:44]

- что такое PMKID;
- трудности перевода или как друг у друга воруют контент;
- развод от разработчиков по стандарту 802.11q;
- инструмент для захвата PMKID/hcxdumptool;
- особенности запуска hcxdumptool;
- сканирование доступных сетей средствами hcxdumptool;
- дополнительные опции для запуска hcxdumptool;
- увеличение мощности адаптера с целью получения лучших результатов;
- получение PMKID из перехваченных данных/hcxtools;
- структура PMKID/как узнать имя сети;
- брут PMKID средствами Hashcat;
- получение PMKID от конкретной сети;
- конвертация формата hcxdumptool в читабельный для aircrack-ng;
- брут PMKID с помощью aircrack-ng;
- анализ роутеров отдавших PMKID;
- дублирование PMKID;
- объединение нескольких .hccapx файлов в один;
- организация упорядоченного брутфорса.

Урок №8. Брутфорс в Windows. EWSA и WIFIPR [01:17:33]

- Elcomsoft Wireless Security Auditor;
  - описание и особенности EWSA;
  - вводный обзор по функционалу и начальным настройкам;
  - разбор статистики;
  - встроенный WiFi сниффер;
  - атака по словарю/мутации паролей;
  - детальный разбор/пояснение по каждому виду мутаций;
  - атаку по слову;
  - атака по маске;
  - комбинированная атака;
  - гибридная атака;
  - настраиваемая атака;
  - настройка очереди для подбора хеша;
- Passcape Wireless Password Recovery;
  - описание и особенности WIFIPR;
  - обзор базовых возможностей;
  - предварительная атака;
  - разбор статистики;
  - особенности тонкой настройки GPU;
  - идентификационная атака;
  - генератор словарей и сетевые словари;
  - атака прямым перебором;
  - детальный разбор атаки по словарю;
  - атака по маске;
  - атака по ключевому слову;
  - комбинированная атака;
  - атака по фразе;
  - гибридная атака;
  - групповая атака;
  - анализ словарных паролей/отчёты;
  - подробный разбор "пароле-метра";
  - слияние словарей;
  - чистка и оптимизация словарей;
  - сжатие словарей.

Урок №9. Онлайн ресурсы для брутфорса WPA хешей [00:44:52]

- введение;
- принцип работы сервисов;
- особенности выгрузки хендшейков;
- особенности при регистрации на некоторых ресурсах;
- чистка перехваченных данных с помощью Wireshark;
- применение фильтров Wireshark для конкретной сети;
- "больше сетей - меньше паролей";

- выбираем на сервисе свои словари и правила для брута;
- выбираем на сервисе свои условия для брутфорса хэша;
- от чего зависит скорость получения результата.

Урок №10. Взлом протокола WPS [01:12:24]

- виды WiFi Protected Setup;
- почему возможен взлом WPS;
- установка требуемых инструментов;
- анализ доступных сетей с помощью wash;
- разбор реализаций WPS через airodump-ng;
- основные аргументы для работы с reaver;
- атака на первую сеть/WPS Locked;
- порядок выполнения атак на WPS;
- атака Pixie Dust;
- получение WPA PSK по WPS PIN;
- получение WPA PSK по пустому пину;
- базы и генераторы пинов для WPS;
- считаем время на взлом сети через WPS;
- восстановление сохраненной сессии в reaver;
- важные директивы --no-nacks/--ignore-locks и др.
- применение связки reaver+aireplay-ng;
- как сохранить отсканированные сети/файлы csv;
- проверяем соответствие WPS и PSK.

Урок №11. Автоматизация процесса взлома. Wifite [00:54:09]

- вводный обзор по программе;
- перечень атак выполняемых скриптом;
- особенности установки и запука Wifite;
- разбор отображаемых колонок;
- уровень сигнала SNR;
- как работать с атаками;
- тонкие настройки Wifite;
- детальный разбор дополнительных опций;
- применяем к Wifite навыки из прошлых уроков;
- инструменты для брута хендшейка в Wifite;
- глюки и недоработки.

Урок №12. MITM атаки | Wifiphisher | Fluxion [00:55:19]

- введение по атакам "человек по середине";
- как работает "MITM" атака;
- атаки типа "Evil Twin";
- зачем для полноценнной атаки иметь 2 или 3 WiFi адаптера;
- организовываем атаку с помощью Wifiphisher;
  - установка и запуск Wifiphisher;

- как работает Wifiphisher;
- выбор фишинговых сценариев;
- назначение ролей WiFi адаптерам;
- тонкие настройки Wifiphisher;
- тест на инъекции пакетов;
- как создать виртуальный интерфейс;
- как поднять виртуальную точку доступа;
- имитируем атаку "Evil Twin" своими руками;
- организовываем атаку с помощью Fluxion;
- установка и запуск Fluxion;
- захват хендшейка и интерфейс для отслеживания цели;
- создание фейковой точки доступа и фишингового портала;
- детальный разбор атаки;
- изменяем фишинговую страницу под себя;
- меры предосторожности от атаки "злой двойник".

Урок №13. Media Access Control | MAC [01:13:52]

- что такое аппаратный адрес и для чего он нужен;
- подмена mac-адреса на простом примере;
- фильтрация по mac-адресам в роутерах/черный и белый списки;
- подмена mac-адреса в среде Windows;
- стандартный метод замены mac;
- почему на WiFi карте/адаптере MAC не меняется;
- программы для mac-спуфинга/ TMAC|SMAC;
- ограничения в Windows на mac-адреса;
- что означает в mac-адресе первый октет "02";
- шаблоны mac-адресов для ОС Windows;
- как работает софт по подмене mac-адресов;
- меняем mac-адрес в реестре вручную;
- подмена mac-адреса в среде Linux;
- почему Kali показывает "левый" mac-адрес WiFi адаптера;
- служба NetworkManager и её поведенческие сценарии;
- режимы сканирования и клонирования/NetworkManager;
- изменяем поведение NetworkManager;
- отключаем автоматическую подмену mac-адреса;
- macchanger или серьёзная альтернатива для NetworkManager;
- детальный разбор функционала macchanger;
- что такое ARP протокол;
- принцип ARP спуфинга/отравление ARP протокола;
- как скрыть своё присутсвие на роутере жертвы.

Урок №14. Airgeddon [01:09:57]

- особенности установки и запуска;
- разбор меню, интерфейса и базовые настройки;

- анализ эффективности атак деаунтификации/mdk4|aireplay|wds;
- подробный разбор инструментов для работы с хендшейками и PMKID;
- полный брутфорс по шаблонам и маскам с использованием crunch;
- меню атак "Злой Двойник";
- что такое sslstrip и как он работает;
- как реализована полноценная атака "Evil Twin";
- атака "Злой Двойник" с перехватывающим порталом;
- меню атак на WPS;
- офлайн генерация пин-кода, используя алгоритмы и базу данных/WPS;
- атака на основе базы данных известных и сгенерированных пинов/WPS;
- атака на WEP "Все в одном".

Урок №15. Портативные ОС. Kali Live/AirSlax|WifiSlax [00:41:27]

- обзор портативных/мобильных ОС для вардрайвинга;
- **обзор Kali Live;**
  - установка Kali Live USB на флешку;
  - особенности установки Kali на USB накопители;
  - проверяем работу persitence раздела Kali;
- **обзор AirSlax;**
  - установка AirSlax на флешку;
  - основы и принцип работы ОС;
  - как обойти ограничения базовой версии;
  - особенности сохранения результатов;
  - взлом протокола WPS;
  - автоматический поиск и перехват хендшейков;
  - автоматизация взлома WPS;
  - где взять версию PRO;
- **обзор WifiSlax;**
  - установка и запуск ОС;
  - где найти и как установить дополнительные модули;
  - обзор инструментов WifiSlax;
- заключение.

Урок №16. Альтернативные прошивки | OpenWRT [00:54:10]

- прошивка и аппаратные компоненты роутеров;
- различия стоковых и альтернативных прошивок;
- преимущества альтернативных прошивок;
- OpenWRT как родоначальник других альтернативных ОС;
- OpenWRT или DD-WRT;
- рекомендации к выбору девайса для прошивки;
- обоснование выбора роутера для прошивки;
- риски при прошивке устройства;
- выбор правильной ОС для маршрутизатора;
- алгоритм установки OpenWRT;

- особенности и нюансы при прошивке;
- базовые настройки по LAN и WiFi сети в OpenWRT;
- установка дополнительных пакетов;
- как вернуться на стоковую прошивку;
- особенности прошивки для возврата в сток;
- обязательные действия после возврата на оригинальную прошивку;
- итоговые выводы по выше выполненным манипуляциям.

Урок №17. Локальные сети провайдеров [01:38:50]

- внешние и внутренние подсети провайдеров;
- вас могут взломать не только через WiFi;
- уязвимости роутеров и чем это чревато;
- программа RouterScan и её назначение;
- расширенные настройки и опции RouterScan;
- IP адреса и маски подсетей;
- как пользоваться IP калькулятором;
- определяем диапазон сканируемых IP на примере домашней сети;
- определяем внешний IP адрес шлюза своего провайдера;
- что такое реальный IP адрес и для чего он нужен;
- узнаем диапазон внешних IP адресов провайдера;
- сканируем роутеры своего провайдера с реальными IP адресами;
- почему сканирование внешних IP адресов не эффективно;
- диапазоны частных IP адресов;
- как узнать диапазон внутренних IP адресов своего провайдера;
- сканируем внутренний диапазон моего провайдера;
- анализируем статистику по паролям и роутерам;
- получаем доступ к локальной сети жертвы через LAN провайдера;
- подключаемся к медиа-ресурсу жертвы;
- как защитить свой роутер от атак снаружи.

Урок №18. Защита WiFi сетей | Резюме [00:47:15]

- идеология курса;
- правильная настройка роутеров на примере стоковой прошивки и OpenWRT;
- как узнать загруженность радиоэфира;
- нюансы OpenWRT при фильтрации MAC-адресов.
- особенности настройки моего роутера;
- список ARP List в OpenWRT;
- дополнительные меры защиты своей сети;
- получение админ логина/пароля роутера путём отравления протокола ARP;
- получаем в роутере скрытый пароль VPN подключения;
-что будет во 2 части курса;
- заключение.