Отчет по лабораторной работе №6

«Набор инструментов для аудита беспроводных сетей AirCrack»

Выполнил студент: Греченко Л.В.

6.1 Цель работы

Изучить основные возможности пакета AirCrack и принципы взлома WPA/WPA2 PSK и WEP.

6.2 Ход работы

Изучение

1. Изучить документацию по основным утилитам пакета – airmon-ng, airodump-ng, aireplay-ng, aircrack-ng.

airmon-ng

Описание:

Этот сценарий может быть использован для включения режима монитора в беспроводных интерфейсах. Он также может быть использован, чтобы вернуться из режима мониторинга в режим управления. Ввод команды airmon-ng без параметров покажет статус интерфейсов.

Использование:

airmon-ng <start|stop> <interface> [channel] or airmon-ng <check|check kill>

- <start|stop> начать или остановить интерфейс. (Обязательный параметр)
- <interface> определяет интерфейс. (Обязательный параметр)
- [channel] настраиваем конкретный канал.
- <check|check kill> “check” покажет какие процессы могут быть помехой для aircrack-ng. Рекомендуется, чтобы эти процессы были устранены до использования aircrack-ng. “check kill” проверяют и убивают процессы, которые могли бы помешать aircrack-ng.

Типичное использование:

- Для старта wlan0 в режиме мониторинга: airmon-ng start wlan0
- Для старта wlan0 в режиме мониторинга канала 8: airmon-ng start wlan0 8
- Для остановки wlan0: airmon-ng stop wlan0
- Для проверки статуса: airmon-ng

airodump-ng

Описание:

Airodump-ng используется для захвата пакетов исходных 802.11 кадров и особенно подходит для сбора WEP IVs (вектор инициализации) для использования их с Aircrack-NG. Если есть приемник GPS, подключенный к компьютеру, Airodump-ng способен зафиксировать координаты обнаруженных точек доступа.

Использование:

Перед запуском airodump-ng необходимо запустить airmon-ng скрпит для обнаружения беспроводных интерфейсов.

airodump-ng <options> <interface>[,<interface>,...]

—ivs: Сохранять только отловленные IVы. Короткая форма -i.
—gpsd: Использовать GPS. Короткая форма -g.
—write: Префикс файла дампа. Короткая форма -w.
—beacons: Записывать все маяки в файл дампа. Короткая форма -e.
—netmask <netmask>: Фильтровать точки по маске. Короткая форма -m.
—bssid <bssid>: Фильтровать точки по BSSID. Короткая форма -d.
—encrypt <suite>: Фильтровать точки по типу шифрования. Короткая форма -t
-a: Фильтровать не асоциированых клиентов

По умолчанию, airodump-ng отслеживает каналы на частоте 2.4Ghz.
Можно заставить ее отслеживать пакеты на другом/определенном канале используя:
—channel <channels>: Определить канал. Короткая форма -c.
—band <abg>:Полоса на которой airodump-ng будет отлавливать пакеты. Короткая форма -b.
—cswitch <method>: Установить метод переключения каналов. Короткая форма -s.

Поле	**Описание**
BSSID	MAC адрес точки доступа.
PWR	Уровень сигнала о котором сообщает карта. Его значение зависит от драйвера, но поскольку уровень становится выше,вы можете определить что находитесь ближе к точке доступа. Если BSSID PWR равен −1, то драйвер не потдерживает уровень сигнала. Если PWR равен −1 для ограниченного числа станций тогда это для пакета который поступил от AP но возможностипередачи клиента вне возможностей вашей карты. Значит вы слышите только половину вей сети. Если все клиенты имееют PWR равный −1 драйвер не поддерживает заданный уровень сигнала.
RXQ	Качество Приема измеренное в процентах от пакетов (управляющие пакеты и пакеты данных) успешно полученных в течениипоследних 10 секунд. Смотрите примечание для получения более детальной информации.
Beacons	Число пакетов объявлений, посланных AP. Каждый пункт доступа посылает приблизительно десять маяков в секунду по самой низкой норме (1M), таким образом их может набираться очень много.
# Data	Количество отловленных пакетов (если WEP, только количество IV), включая широковещательные пакеты.

#/s	Число пакетов данных за последние 10 секунд.
CH	Номер канала (берется из пакетов-маяков). Примечание: иногда airodump-ng захватывает пакеты с других каналов даже если канал строго задан. Это происходитиз-за наложения радиочастот.
MB	Максимальная скорость поддерживаемая AP. Если MB = 11, это 802.11b, если MB = 22 это 802.11b+ и если больше то 802.11g. Точка (после того, как выше 54) указывает, что короткая преамбула поддержана.
ENC	Используемый алгоритм шифрования. OPN = нет шифрования,”WEP?” = WEP или выше (нет нужных данных для выбора между WEP или WPA/WPA2), WEP (без метки вопроса) показывает на статическое или динамическое WEP, и WPA или WPA2 если TKIP или CCMP тоже присутствует.
CIPHER	Обнаруженный шифр. Один из CCMP, WRAP, TKIP, WEP, WEP40, или WEP104. Не обязательно, но TKIP обычно используетсяс WPA, а CCMP обычно с WPA2.
AUTH	Используемый протокол аутентификации. Один из MGT (WPA/WPA2 использование выделенного сервера аутентификации), PSK (открытый ключ для WEP/ pre-shared ключ для WPA/WPA2), или OPN (открытый для WEP).
ESSID	Так называемый “SSID”, который может быть пустым если скрытие SSID активизировано. В этом случае, airodump-ngпопытается получить SSID исследуя ответы клиентов.
STATION	MAC адрес обнаруженной станции. В скриншоте выше были обнаружены две станции (00:09:5B:EB:C5:2B and 00:02:2D:C1:5D:1F).
Lost	Число пакетов потерянных за последние 10 секунд. Основывается на требованиях последовательности данных.
Packets	Количество данных посланных клиентом.
Probes	Проверка ESSIDов по клиентам.

Пример использования airodump-ng.

```
CH  9 ][ Elapsed: 1 min ][ 2007-04-26 17:41 ][ WPA handshake: 00:14:6C:7E:40:80

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:09:5B:1C:AA:1D   11  16       10        0    0  11  54.  OPN              NETGEAR
00:14:6C:7A:41:81   34 100       57       14    1   9  11e  WEP  WEP         bigbear
00:14:6C:7E:40:80   32 100      752       73    2   9  54   WPA  TKIP   PSK  teddy

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:14:6C:7A:41:81  00:0F:B5:32:31:31   51   36-24    2       14
(not associated)   00:14:A4:3F:8D:13   19    0-0     0        4    mossy
00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1   36-36    0        5
00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35   54-54    0       99    teddy
```

Чтобы ограничить сбор данных лишь одной точкой которая интересна, можно включить опцию “–bssid” и определить MAC адрес точки. Пример:

airodump-ng -c 8 –bssid 00:14:6C:7A:41:20 -w capture ath0

Для минимизации используемого под дампы дискового пространства, включите опцию “–ivs”. Пример:

airodump-ng -c 8 –bssid 00:14:6C:7A:41:20 -w capture –ivs ath0

Это заставит сохранять только вектора инициализации а не все пакеты. Это не может быть использовано если пытаетесь отлавливать WPA/WPA2 пакеты.

aireplay-ng

Aireplay-ng используется для генерации пакетов. Если к беспроводной точке доступа никто не подключен, соответственно нет трафика для захвата и последующего анализа (взлома).

Описание

Основная функция программы заключается в генерации трафика для последующего использования в aircrack-ng для взлома WEP и WPA-PSK ключей. Существуют несколько различных атак, с помощью которых можно совершить: реассоциацию узлов с целью получения данных WPA handshake, поддельные аутентификации, интерактивное повторение пакетов (Interactive packet replay), вручную произвести инжектирование ARP-запросов и повторных ARP-запросов. С помощью инструмента packetforge-ng можно создавать произвольные пакеты.

Большинство драйверов необходимо пропатчить, чтобы иметь возможность генерировать пакеты.

Использование атак

В настоящее время программа реализует несколько различных атак:

Атака 0: Реассоциация узлов

Атака 1: Фальшивая аутентификация

Атака 2: Интерактивная генерация пакетов

Атака 3: Повторение ARP запроса

Атака 4: KoreK chopchop (быстро-быстро) нападение

Атака 5: Фрагментация

Атака 6: Кофе-латте атака (Caffe-latte attack)

Атака 7: Клиент-ориентированная фрагментированная атака (Будет в следующем выпуске! Не доступна в данный момент.)

Атака 9: Тест инжекции

Использование

aireplay-ng <опции> <интерфейс>

Для всех атак, за исключением реассоциации узлов и фальшивой аутентификации,
можно использовать следующие фильтры, чтобы ограничить пакеты, которые будут участвовать в конкретной атаке. Наиболее часто используется фильтр-опция «-b», чтобы выбрать конкретную точку доступа. Обычно опция «-b» является единственным ключем, который вы используете.

Параметры фильтрации:

Опция	Парам.	Описание
-b	bssid	MAC-адрес точки доступа
-d	dmac	MAC-адрес, адресат
-s	smac	MAC-адрес, источник
-m	len	Минимальный размер пакета
-n	len	Максимальный размер пакета
-u	type	Контроль кадра, тип поля (type field)
-v	subt	Контроль кадра, подтип поля (subtype field)

-t	tods	Контроль кадра, To DS bit
-f	fromds	Контроль кадра, From DS bit
-w	iswep	Контроль кадра, WEP bit

При генерации пакетов (путем инжекции), применяются следующие варианты параметров. Имейте в виду, что не каждый параметр имеет отношение к каждому нападению. Для каждой атаки ниже будут приведены примеры возможных опций.

Параметры генерации (повторения) пакетов:

Опция	Парам.	Описание
-x	nbpps	количество пакетов в секунду
-p	fctrl	установить контрольное слово кадра (hex)
-a	bssid	установить MAC-адрес точки доступа
-c	dmac	установить MAC-адрес Получателя
-h	smac	установить MAC-адрес Источника
-e	essid	атака «фальшивая аутентификация»: установить SSID (идентификатор сети) точки доступа
-j	arpreplay атака	генерация FromDS пакетов
-g	значение	изменить размер кольцевого буфера (по умолчанию: 8)
-k	IP	установить IP адрес назначения в фрагментах
-l	IP	установить IP адрес источника в фрагментах
-o	npckts	количество пакетов в пачке (-1)
-q	sec	количество секунд между посылкой keep-alive пакетов (сообщений, подтверждающих активность) (-1)

-y	prga	поток ключей (keystream) для авторизации открытым ключем

При атаках есть возможность получать пакеты для генерации из двух источников. Первый источник — поток пакетов в реальном временис вашей беспроводной карты. Второй источник — из pcap файла. Стандартный формат Pcap (Packet CAPture, связанный с libpcap библиотекой http://www.tcpdump.org), признается большинством коммерческих и открытых (open-source) программ для захвата и анализа пакетов.При чтении из файла зачастую игнорируются особенности aireplay-ng. Это позволяет читать пакеты из других сессий захвата пакетов и довольночасто генерировать различные нападения в pcap файлы для удобного повторного использования.

Параметры для выбора источника:

iface: захват пакетов с этого интерфейса

-r file: получение пакетов из этого файла формата pcap

Здесь вы указываете способ, в каком режиме будет работать программа. В зависимости от указанного способа не все опции будут доступны.

Режимы атаки (для выбора режима могут быть использованы цифры):

Атака	Описание
- -deauth count	Реассоциация одной или всех станций (пользователей) (-0)
- -fakeauth delay	Фальшивая аутентификация к точке доступа (-1)
- -interactive	Интерактивный выбор кадров (-2)
- -arpreplay	Стандартное повторение ARP-запроса (-3)
- -chopchop	Дешифровка/chopchop WEP пакета (-4)
- -fragment	Генерирует действительный поток ключей (keystream) (-5)
- -test	Тест инжекции (-9)

aircrack-ng

Описание

Aircrack-ng — программа для взлома 802.11 WEP and WPA/WPA2-PSK ключей. Aircrack-ng может восстановить WEP ключ как только будет захвачено достаточно много пакетов с помощью программы

airodump-ng. Эта часть набора программ от aircrack-ng предназначена для выполнения статических атак на беспроводные сети и для обнаружения WEP ключа методом грубого подбора. Также можно использовать подбор по словарю. Для взлома WPA/WPA2 pre-shared ключей, можно использовать ТОЛЬКО подбор по словарю.

Использование Aircrack-ng

aircrack-ng [options] <capture file (s)>

Вы можете определять множество файлов для ввода (в формате.cap или.ivs). Также вы можете запускать airodump-ng и aircrack-ngодновременно. aircrack-ng автоматически обновит свои данные при поступлении новых IV в файл дампа.

Вот список возможных опций:

Опция	**Парам.**	**Описание**
-a	amode	Режим атаки (1 = статичный WEP, 2 = WPA/WPA2-PSK).
-e	essid	Если установлено, будут использоваться все IVы от сети с указанным ESSID. Эта опция также требуется для подбора WPA/WPA2-PSK если ESSID не широковещательный (скрытый).
-b	bssid	Выбор целевой сети основанный на MAC адресе точки доступа.
-p	nbcpu	На SMP системах: # CPU для использования.
-q	*none*	Включить «тихий» режим (не выводить статическую информацию пока не будет найден ключ).
-c	*none*	(взлом WEP) Ограничить поиск только алфавитноцифровыми кодами (0?20 — 0?7F).
-t	*none*	(взлом WEP) Ограничить поиск двоичнодесятичными кодами.
-h	*none*	(взлом WEP) Ограничить поиск цифровыми кодами (0?30-0?39) Такие ключи используются по умолчаниюна большинстве Fritz!BOXes.
-d	start	(взлом WEP) Установить начало ключа WEP (в шестн.) для того чтобы

		отладить цели.
-m	maddr	(взлом WEP) MAC адрес для фильтрации WEP данных. Определите -m ff:ff:ff:ff:ff:ff для использования всех IVs, независимо от сети.
-n	nbits	(взлом WEP) Установка длинны ключа: 64 для 40-bit WEP, 128 для 104-bit WEP, и т. д. По умолчанию — 128.
-i	index	(взлом WEP) Поддерживать только введенный ключевой индекс (1 to 4). Значение по умолчанию — игнорировать ключевой индекс.
-f	fudge	(взлом WEP) По умолчанию этот параметр установлен в 2 для 104-bit WEP и в 5 для 40-bit WEP. Определяет значение фактора вероятности.
-k	korek	(взлом WEP) Есть 17 статических атак KoreKa. Иногда одна атака создает огромное кол-во ложных голосов которые препятствуют нахождению верного ключа даже с большим кол-вом IVов. Попробуйте -k 1, -k 2, … -k 17 для проверки каждого типа атаки выборочно.
-x/-x0	*none*	(взлом WEP) Отключает последний брутфорс.
-x1	*none*	(взлом WEP) Включает последний брутфорс (по умолчанию).
-x2	*none*	(взлом WEP) Включает два последних брутфорса.
-X	*none*	(взлом WEP) Отключает многопроцессорный брутфорс (только для SMP).
-y	*none*	(взлом WEP) Это экспериментальное нападение которое должно использоваться когда обычный метод терпит неудачу с более чем миллионом IVов
-w	words	(взлом WPA) Путь к словарю или «-» без ковычек для стандартного ввода (stdin).

Практическое задание

На лабораторной работе были проделаны следующие действия по взлому WPA2 PSK сети (описание по ссылке "Руководство по взлому WPA"в материалах)

1. Запущен режим мониторинга на беспроводном интерфейсе

2. Запущен сбор трафика для получения аутентификационных сообщений

3. Аутентификация в сети не происходила в разумный промежуток времени, и была произведена деаутентификацию одного из клиентов, до тех пор, пока не удалось собрать необходимых для взлома аутентификационных сообщений

4. Произвели взлом используя словарь паролей

Вывод:

В данной лабораторной работе был изучены основные возможности пакета AirCrack и принципы взлома WPA/WPA2 PSK и WEP. AirCrack популярен и предназначен для обнаружения беспроводных сетей, перехвата передаваемого через беспроводных сетей, перехвата передаваемого через беспроводные сети трафика, аудита WEP и WPA/WPA2-PSK ключей шифрования (проверка стойкости), в том числе пентеста (Penetration test) беспроводных сетей (подверженность атакам на оборудование и атакам на алгоритмы шифрования).