

Tarea: Herramientas de cracking
Asignatura: Criptografía
Alumno: Jaime Navarro

He elegido la herramienta Aircrack-ng, la cual está integrada en cualquier distribución de Kali Linux, el cual está basado en Debian.

Está enfocada a romper los cifrados de las contraseñas Wi-Fi, como lo son WEP, WPA y WPA2 (aunque el reciente WPA3 se rumorea que también ya ha sido comprometido, ver :

<https://www.adslzone.net/2019/04/10/wifi-wpa3-hack-dragonblood/>). En este caso, usé un ataque de diccionario contra unos paquetes del handshake que capturé de un equipo cualquiera.

El proceso es el siguiente: primero expulso a un equipo de la red Wi-Fi de la ufv, en concreto "zona_ufv", pues no es fácil romper el cifrado de la red "eduroam" al estar basado en RADIUS. Después, con "airodump-ng" capturo los paquetes que intenta mandar infinitamente el PC en cuestión hasta que se reconecte a dicha red. Esos paquetes son el anterior mencionado handshake, de manera que cuando los tengo cierro el comando y reviso el archivo donde está escrito. Con Aircrack-ng creo un nuevo archivo ".hccapx" a partir del ".cap", con la opción "-j"

```
james@ANON: ~  
  
generic  
avx512  
avx2  
avx  
sse2  
altivec  
power8  
asimd  
neon  
  
Other options:  
  
-u      : Displays # of CPUs & SIMD support  
--help  : Displays this usage screen  
  
(james@ANON)-[~]  
$ aircrack-ng --help | grep -i hccap  
-j <file> : create Hashcat v3.6+ file (HCCAPX)  
-J <file> : create Hashcat file (HCCAP)  
  
(james@ANON)-[~]  
$
```

En esta captura, se puede ver la ayuda del comando, pero sólo muestro lo que coincida con la expresión "hccap". Una vez escrito este archivo clave, se puede usar Aircrack-ng para un ataque de diccionario, fuerza bruta, rainbow table, o incluso de expresión regular. Pero en este caso, al ser una prueba, construí con "Crunch", otra herramienta integrada en esta distribución de Linux, un diccionario, que entre las 5 posibilidades se encuentra la contraseña que es de dominio público "zonawifiufv".

```
Aircrack-ng 1.7
[00:00:00] 6/6 keys tested (426.50 k/s)

Time left: --

KEY FOUND! [ zonawifiufv ]

Master Key      : C2 3E 12 D0 65 2F EF AB D5 B9 A5 D6 AF 40 84 52
                  8A 32 F4 8F 90 93 77 D4 68 21 96 F3 7B C0 90 E8

Transient Key   : 44 72 0A 3C 99 A4 56 7A CA 80 71 BD DC EE F3 BF
                  3A 3F 52 2F A5 54 21 22 4C 65 77 EC C5 60 C6 12
                  98 46 8C DE BD 8B E8 89 D6 D8 F3 7E 1F 80 5A 64
                  93 AC 73 86 F9 F6 20 4F 00 0D 81 DC B5 00 00 00

EAPOL HMAC     : 32 CD BD D0 BB 5F 7E BD 33 A7 37 9C 51 DD 6D E8

(root@ANON)-[/home/james]
# cat zonawifiufv.txt
ufvwifizona
ufvzonawifi
wifiufvzona
wifizonaufv
zonaufvwifi
zonawifiufv

(root@ANON)-[/home/james]
# 
hccapx
```

Se puede apreciar el resultado que arroja esta herramienta cuando encuentra la contraseña adecuada. En la terminal de la derecha, muestro el contenido del diccionario que utilicé a modo de prueba.

A la izquierda, el resultado de lanzar la herramienta, con su comando escrito otra vez a continuación para que se pueda apreciar cómo se usa, por entrada parametrizada especificando tanto el archivo con el handshake, el diccionario, y el archivo donde queremos que nos escriba la contraseña encontrada.