Recuperación de la clave WiFi con cifrado WEP

Guillermo López Leal, 2IM1
Introducción a la Seguridad
Universidad Nebrija

Avisos

- Sólo es una demostración con fines educativos [en serio, en España no es ilegal, pero en otros países sí]
- No hagáis nada que Bill Gates no haría [por ejemplo no terminar la carrera]
- Si os preguntan cómo hacerlo: “No soy la persona más adecuada para responder eso”
- … y si os preguntan por mi: “Pues me han dicho que es un tío cojonudo pero no le conozco”

Glosario de términos

- Backtrack 3: Distribución LiveCD (en nuestro caso USB) basada en Slackware Linux. Su principal objetivo es la seguridad informática, tanto WiFi, como Ethernet, como GPS, bluetooth…
- Wi-Fi: ***Wi****reless* ***Fi****delity*. Capa de transmisión de la pila TCP/IP. Es inalámbrico y se transmite por el espectro de los 2.4Ghz. Hay diferentes estándares, "b", "g", "n"… cada uno con un radio y capacidad de transmisión determinado.
  - ARP: Address Resolution Protocol. Un protocolo TCP/IP (RFC 826) usado para convertir una dirección IP a una dirección MAC.
  - IV (+ Data): es un bloque de bits que es requerido para permitir un cifrado en flujo o un cifrado por bloques, en uno de los modos de cifrado, con un resultado independiente de otros cifrados producidos por la misma clave.
  - MAC: Identificación digital de un punto de acceso, tarjeta de Red, tarjeta WiFi, son 6 pares de caracteres hexadecimales como por ejemplo:

    `0A:3D:1F:67:43:FD`
  - (E)SSID: Nombre de la red.
  - BSSID: Mac de la red (es única).
  - WEP: ***W****ired* ***E****quivalent* ***P****rivacy*. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación *IV*) o de 128 bits (104 bits más 24 bits del IV).

Backtrack 3

- Arrancamos el ordenador con Backtrack 3 previamente cargado en un dispositivo USB (podría estarlo en un CD, pero es más engorroso, ruidoso y lento).
  Cambiamos el idioma del teclado al español desde el inglés para trabajar mejor en consola y no tener problemas con la distribución del teclado.
- Hay que tener cuidado porque se entra como root y se tiene acceso a TODOS los datos de particiones en el sistema operativo, por lo que se podrían destruir datos de forma accidental.

Comprobaciones previas

- Comprobamos que nuestra tarjeta inalámbrica está enchufada (con los típicos botones) y que está soportada por la distribución, para ello abrimos una terminal, y escribimos:

```
airmon-ng
```

- Si sale algo como esto…

```
[ver demo]
```

- …vamos bien: nos dice el interfaz de red que poseemos, y el driver (esto es informativo).
- También tenemos que apuntar la MAC de nuestra tarjeta WiFi. Son los primeros seis pares hexadecimales en:

```
ifconfig INTERFAZ
```

En mi caso…

- Debido a que los drivers que vienen por defecto en BT3 para mi tarjeta inalámbrica no permiten inyección, tenemos que cargar los que lo permiten:

```
modprobe -r iwl3945
modprobe ipwraw
```

- Comprobamos de nuevo con airmon-ng para ver si ha cargado bien los drivers.

Ver qué redes y clientes hay

- Es un paso básico, necesitamos saber qué redes hay a nuestro alcance, qué potencia tienen y los posibles clientes que hay conectados a ellas (o si no hay).
- En consola, escribir (acorde a nuestra interfaz):

```
airodump-ng wifi0
```

- Veremos las redes (con su MAC, nombre, canal, IV's [Data#], beacons a parte de más cosas).
- Además tenemos que poner la tarjeta en modo monitor en el canal de la red que queremos abrir:

```
airmon-ng start wifi0 CANAL
```

- Parte analógica: apuntar en un papel la MAC del punto de acceso y su nombre, así como el canal de transmisión, los clientes conectados y dónde lo están.

Centrarnos en una red…

- Es preferible centrarse en una sola red, debido a que "el que mucho abarca poco aprieta". Si nos centramos en una sola red, podremos inyectar paquetes y "engañar" al router, pudiendo recibir muchos paquetes en poco tiempo (minutos), algo que no se puede hacer si monitoreamos todas las redes.
- Ahora tenemos que guardar **SÓLO** los datos recibidos desde una red en concreto:

```
airodump-ng -e NOMBRE_RED -c CANAL -w ARCH_GUARDAR
                                    INTERFAZ
```

Si hay un cliente conectado…

- Si hay un cliente conectado la WiFi está abierta en segundos:

1. Cambiamos nuestra MAC a la del cliente conectado, nos asociamos al router, y debido al diseño del protocolo, nos empieza a repetir a nosotros también todos los datos (los datos se envían a MACs, no a nombres ni IP's, y si la MAC (que es de UN SOLO ORDENADOR en teoría) está recibiendo, nosotros por extensión también).
2. Simplemente encontrar un paquete auténtico, y reenviarle con mucha frecuencia para que nos responda el router (un "paquete de datos" o "IV"(y ver paso de descifrado de la contraseña)).

- Pero nosotros vamos a hacerlo sin un cliente conectado (muchas veces es esto lo que se encuentra). Sólo tenemos el router y nosotros… (aunque nos ayudaremos de un cliente conectado por cable o un intento de conexión wifi para acelerar el proceso)

Si no hay un cliente conectado…

- Nos tenemos que asociar al punto de acceso, para ello escribimos.

```
aireplay-ng --fakeauth wifi0
```

- Y esperamos a que se asocie, si lo hemos hecho bien y funciona, nos saldrá esto:

```
18:18:20 Sending Authentication Request
18:18:20 Authentication successful
18:18:20 Sending Association Request
18:18:20 Association successful :-)
```

- También podemos hacer que se asocie y recompruebe que seguimos asociados:

```
aireplay-ng --fakeauth 6000 -o 1 -q 10 -e
 NOMBRE_RED -a MAC_RED -h MAC_PROPIA wifi0
```

Capturar 1 ARP

- Una vez nos hemos asociado, lo que necesitamos es un paquete de datos auténticos: Data, que no Beacons (que son parecidos a los pings), ya que estos llevan la "clave" en su interior.
- Para ello no nos queda más remedio que esperar a que router envíe un ARP de broadcast, un "ey, aquí estoy yo, conectaos conmigo si queréis", lo que puede tardar minutos u horas, o bien forzándole/engañándole a que lo haga a través de un cliente conectado por cable o un intento por wifi.

```
ping 192.168.1.x
```

Reenviar ARPs

- Una vez hemos conseguido un ARP lo que tenemos que hacer es reenviar al router ese paquete auténtico capturado.

```
aireplay-ng --arpreplay -e NOMBRE_RED -h
                MAC_ORIGEN INTERFAZ
```

- Veremos como en la pantalla abierta en la diapositiva 7 empiezan a subir los IV (Data#) rápidamente.
- Tenemos que esperar hasta tener unos 40 o 50k.

Crackear la contraseña

- Es el paso más fácil. En una consola escribimos:

```
aircrack-ptw *.cap
```

…o bien…

```
aircrack-ng *.cap
```

- Y veremos como el programa va haciendo una lectura de todos los paquetes. En segundos tendremos nuestra contraseña, tanto en ASCII como en hexadecimal.

Otros ataques

- Hemos hecho el ataque del ARP replay, pero hay otros como por ejemplo el ChopChop, que se basa en el problema del IV con su operación XOR para crear un paquete verdadero que se usa para reenviar y recibir paquetes.
- También está el de fragmentación, que busca un Data para generar miles de paquetes iguales y recibir respuesta.
- De "deautenticación" que se hace cuando hay un cliente conectado **pero** que no genera tráfico (o Data).
- -p 0841 (reenvía cualquier dato que llega del AP, incluso los beacons. Útil cuando no hay ARP requests desde el AP e intentamos que venga uno)

Conclusiones

- Obviamente NO utilizar bajo ningún concepto el cifrado WEP, ya que hemos visto cómo es crackeable en segundos.
- Usar un cifrado WPA o su evolución WPA2, aunque también es “crackeable”, si encontramos el handshake y lo comparamos con un diccionario (avances muy grandes con GPUs), sacamos la pass, aunque tarda bastante.
- Además ha habido fallos de seguridad en WPA y WPA2 últimamente.

Bibliografía

- Página oficial de aircrack-ng, con multitud de tutoriales, ejemplos y una documentación maravillosa.
- Foros de el-hacker.net
- Foros de seguridad-wireless (donde tienen una distribución Wifiway 1.0b2 que junto al script airoway.sh incluido automatiza mucho el proceso para ordenadores portátiles con el chip Intel 3945abg (driver iwl3945 o ipwraw) enormemente)
- Juegos propios
- Documentación propia en http://www.pijusmagnificus.com/wiki/