GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Seminario web: Reforzando la seguridad wifi

Ejercicio de investigación

017 TU AYUDA EN CIBERSEGURIDAD
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

ÍNDICE DE FIGURAS

1. AUDITORÍAS INALÁMBRICAS

Una auditoría de una red inalámbrica implica poner a prueba la seguridad de la red, y en el caso de que sea vulnerable, se deben de realizar las recomendaciones necesarias para solventar dicha vulnerabilidad.

En este caso presentaremos la realización de una auditoría sobre el protocolo WPA, y para ello necesitaremos la distribución "Wifiway" junto con el *hardware* específico que pueda ponerse en modo monitor y soporte el modo AP. Para ello, utilizaremos un "pincho" wifi con *chipset* que soporte dicho modo. El modo monitor también es conocido como modo promiscuo o modo de escucha, donde la tarjeta es capaz de capturar todos los paquetes "wifi". De esta manera, no solamente se ven los puntos de acceso sino también los dispositivos clientes.

El primer paso sería poner el USB wifi en modo monitor; para ello, ejecutaremos desde la shell el siguiente comando donde "wlan0" sera nuestro adaptador inalambrico:

- airmon-ng start wlan0

A continuación, comprobaremos que el modo monitor funciona correctamente gracias al modo monitor, por lo que ejecutamos:

- airodump-ng wlan0.

Figura 1 Redes inalámbricas encontradas

El BSSID es la dirección MAC de los puntos de accesos y el ESSID es el nombre de las redes que emiten los puntos de acceso en cuestión.

Este BSSID, al ser un nombre de identificación único de todos los paquetes de una red inalámbrica, nos permite identificarlos como parte de esa red y asociarlos al punto de acceso.

Nuestro objetivo sería el punto de acceso con WPA2.

Figura 2 Punto de acceso con WPA2

Como podemos ver en la imagen hay un “cliente conectado”. Es indispensable que esté conectado para poder capturar los *handshakes*. Para ello, el primer paso es desautenticarlo mediante el siguiente comando:

Le enviaremos 5 des autenticaciones.

- aireplay-ng -0 5 -a MAC_CLIENTE -c MAC_PUNTO_ACCESO wlan0.

En este paso capturaremos el *handshake* para posteriormente someterlos a un ataque por diccionario mediante el siguiente comando:

- aircrack-ng -w diccionario_preparado.txt captura_hansdhake_de_aireplay.cap.

En el ejemplo de arriba del fichero “captura_handshake_de_aireplay.cap” sería el fichero que ha sido obtenido previamente por el comando “AirePlay”, y el otro fichero, “diccionario_preparado.txt”, puede ser creado con el Bloc de Notas, incluyendo en un fichero nuevo varias líneas con palabras aleatorias y en medio de ellas escribir la clave de nuestra wifi.

Al ser una prueba preparada como tal para este tipo de ejercicio de investigación el tiempo sería de 10 minutos, al estar en el diccionario la contraseña.

En un escenario real, dependería la calidad de nuestro diccionario y de la potencia para des autenticar al cliente.