Herramientas pasivas y activas para encontrar SSIDs ocultos

Publicado por Vicente Motos on lunes, 2 de febrero de 2015 Etiquetas: herramientas , wi-fi

Por defecto, los puntos de acceso retransmiten su **SSID (service set identifier)** o nombre de red en *beacon frames* aunque, hoy en día, la mayoría también permite ocultarlo: es lo que se denomina '**network cloaking**' y no debe llevarnos a una sensación de falsa seguridad. Me explico, siempre está bien ocultar nuestro SSID de miradas indiscretas pero **cualquier sniffer inalámbrico seguirá siendo capaz de leer los frames cuando un cliente se conecte.**.. ¿por qué? porque el SSID va en texto claro y bastaría con leer los paquetes '*Probe Request*' y '*Probe Response*' (tipo=0x00, subtipo=0x05).

Y ahora seguro que dirás... "pues puedo eternizarme esperando a que un cliente se conecte al SSID objetivo"... no necesariamente. Existe un método más rápido (aunque más detectable) enviando **frames de desautenticación** a todos los clientes para forzarles a desconectarse y reconectarse, revelando así sus SSIDs.

Por ejemplo con aireplay-ng sería así de sencillo:

```
aireplay-ng --deauth 5 -a 00:14:6C:7E:40:80 mon0
```

donde '5' es el nº de paquetes de desautenticación enviados y la MAC la dirección física del punto de acceso.

Es decir, **podemos averiguar el SSID oculto de forma pasiva o de forma activa**, y tanto para una u otra forma tenemos herramientas que nos facilitan la vida:

Pasivas:

- KisMAC: herramienta libre y gratuita para OS X que puede auditar por completo conexiones a nuestro alrededor, recibir sus paquetes de datos y, por supuesto,

realizar inyecciones de estos mismos paquetes para lograr la contraseña de acceso a la red.

- Kismet: Kismet es un sniffer, un husmeador de paquetes, y un sistema de detección de intrusiones para redes inalámbricas 802.11.

- PRADS: sistema pasivo de detección de activos que puede usarse para mapear la red y hacer inventario o, junto con un IDS/IPS, para la correlación de eventos con hosts/servicios.

- ESSID-Jack: o airjack, fue utilizada originalmente como una herramienta de desarrollo para aplicaciones y controladores de captura, inyección o recepción de paquetes que se transmiten de forma inalámbrica.

- CommView para WiFi: potente monitor de red inalámbrico y analizador de 802.11. Cargado con muchas funciones, CommView para WiFi combina rendimiento y flexibilidad con facilidad de uso.

Activas:

- NetStumbler: NetStumbler es un programa para Windows que permite detectar redes inalámbricas (WLAN) usando estándares 802.11a, 802.11b y 802.11g. Existe una versión para Windows CE (PDA) llamada MiniStumbler.

- inSSIDer: es un escáner Wi-Fi para Microsoft Windows y Apple OS X desarrollado por MetaGeek, LLC. Ha recibido premios como el Bossie Infoworld 2008 al "Mejor Software libre de red" pero ya no es libre en la versión 3.

- Acrylic WiFi: innovador escáner WiFi para realizar un análisis de cobertura y seguridad WiFi detallado en redes de comunicaciones WiFi en un tiempo muy reducido y con un coste insuperable.

Fuentes:

- Uncovering Hidden SSIDs
- How to Detect a Non-Broadcasted (Hidden) SSID in Linux and Windows
- Wireless Pentesting on the Cheap (Kali + TL-WN722N) - Hidden SSID
- How to Find Hidden Wireless Networks & their SSID, in Windows
- Debunking Myths: Is Hiding Your Wireless SSID Really More Secure?

3 comentarios :

1. *Anónimo*3 de febrero de 2015, 9:27

   Y no mencionáis a Acrylic WiFi? Herramienta española presentada en RootedCON 2013 con versión gratuíta y profesional por ~15€, que incluye un driver para capturar en modo monitor en Windows.

   Responder
   Respuestas

   1. 

      *Vicente Motos*3 de febrero de 2015, 10:33

      este post no es estático, de hecho, la idea siempre es añadir el máximo número de herramientas a este tipo de repositorios. Añado Acrylic y si conoces alguno más interesante ya sabes ;)

      Responder

2. *Anónimo*3 de febrero de 2015, 21:50

   y tampoco mencionáis las de android (wifi analyzer, fing, etc) y las que mencionais son las más comunes. hay otras mejores