Crackeando WPA2 con un Half-Handshake

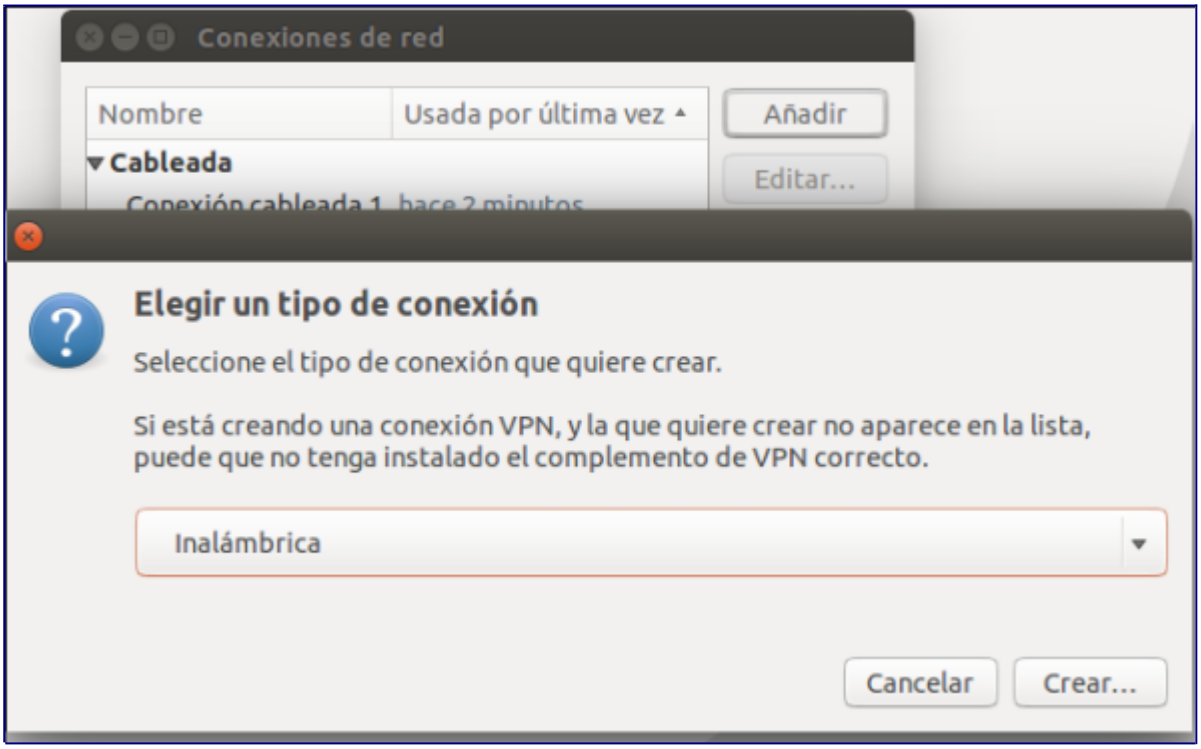
marzo 10, 2015 adastra Deja un comentario Go to comments

Las redes wifi con WPA/WPA2 activado suelen ser suficientemente seguras y dadas sus características, a la fecha de redactar este articulo, la única forma de atacar directamente una red con este mecanismo de protección es intentando capturar un 4way-handshake entre el cliente y un AP. Un 4way-handshake en la terminología de WPA se refiere a los paquetes de datos intercambiados entre AP y cliente a la hora de realizar el proceso de autenticación mutuo. No obstante, aunque un handshake completo es lo deseado para poder iniciar un ataque por diccionario, también es posible hacerlo con un handshake "a medias", es decir, cuando el cliente inicia el proceso de autenticación con un AP y dicho proceso ha fallado. Ahora bien, seguramente el lector ya lo sabe, pero cuando un dispositivo tiene registrado un AP con el que suele conectarse con frecuencia (como por ejemplo una red wifi domestica), dicho dispositivo envía de forma constante paquetes del tipo "PROBE_REQUEST" con la esperanza de que el AP se encuentre en en la zona de alcance. Cuando un AP con el SSID especificado responde con un "PROBE_RESPONSE", el proceso de autenticación en ambos sentidos comienza inmediatamente, dando lugar a una serie de peticiones que identifican tanto al cliente como al AP y determinan si ambos son quienes dicen ser. Se trata de un procedimiento robusto en el que la relación de confianza en ambos sentidos es vital para que la conexión se pueda realizar correctamente. No obstante, es posible que solamente una de las dos partes se pueda identificar con la otra de forma correcta, en este caso hablamos de un handshake a medias, ya que solamente una de las dos entidades ha podido reconocer a la otra. Con un handshake a medias también es posible realizar el mismo ataque por diccionario que con un handshake completo y por este motivo, también es un vector de ataque valido en este tipo de entornos.
Ahora, ¿Cuándo y cómo se debe llevar a cabo este tipo de ataque? Cuando se capturan los paquetes "PROBE_REQUEST" de un cliente, dichos mensajes contienen el SSID del AP que el cliente busca y en este punto, un atacante puede levantar un AP falso con dicho SSID para responder a las peticiones enviadas por el cliente. Para responder al "cómo" de la pregunta anterior, pueden haber varios mecanismos validos, como por ejemplo utilizando la herramienta "ap-hotspot". Por simplicidad y porque es una solución rápida de implementar, se puede utilizar la herramienta "KDE NetworkManager" o el "NetworkManager de Gnome", a efectos prácticos utilizar cualquiera de los dos resulta equivalente.

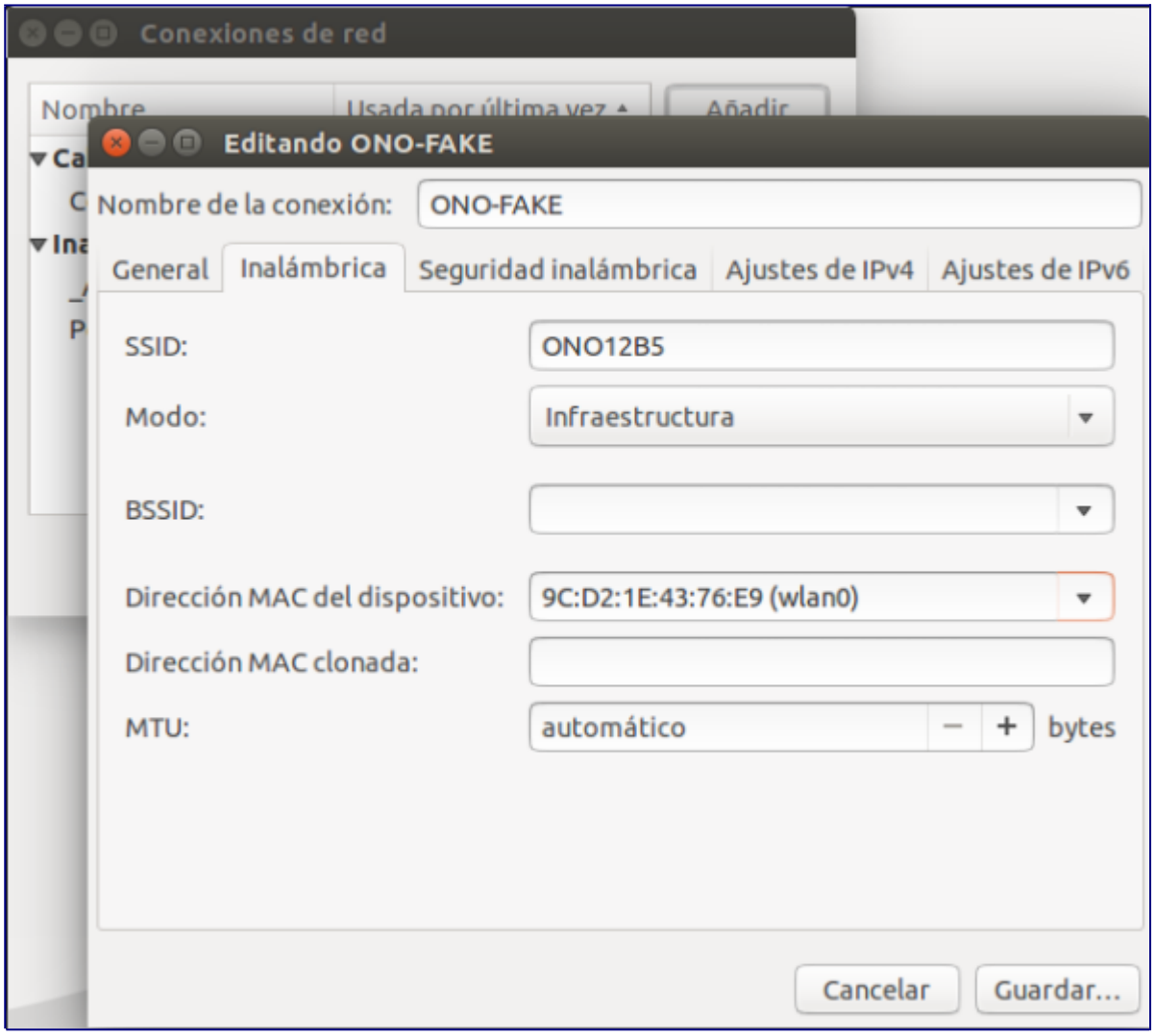
Configurando un AP inalámbrico con el NetworkManager

En sistemas Debian el paquete que incluye el KDE NetworkManager es el "

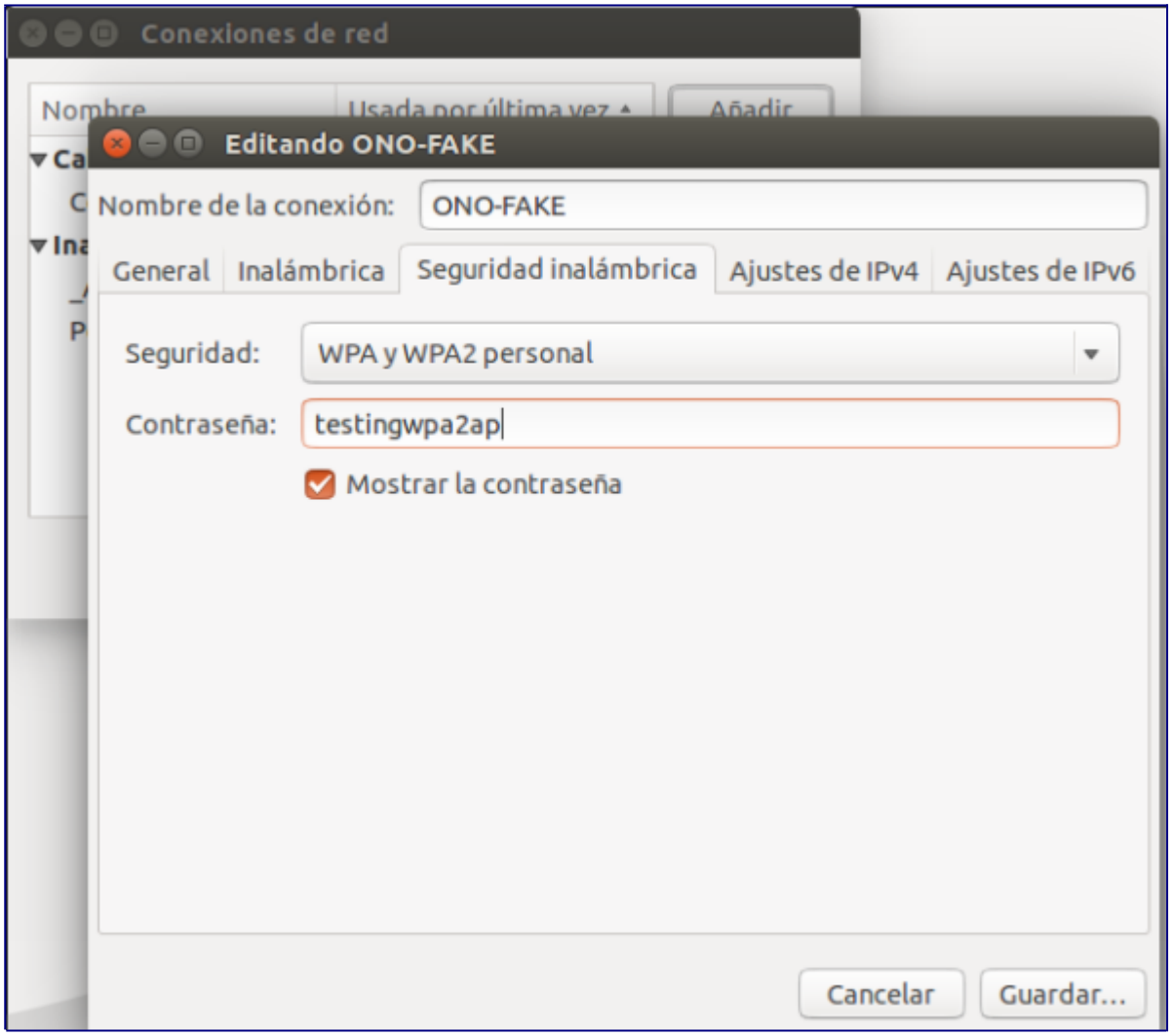
" y en sistemas Ubuntu el "plasma-nm". Como es acostumbrado en este tipo de sistemas, se puede instalar muy fácilmente utilizando herramientas como "apt-get". Por otro lado, en sistemas Debian y Ubuntu con GNOME, el NetworkManager viene incluido por defecto y se puede ver en el panel lateral en donde se encuentran otras herramientas del escritorio. En ambos casos, crear un AP es bastante simple, las imágenes que se enseñan a continuación muestran cómo crear un AP con un SSID y una contraseña. (Antes de crear la conexión, asegurarse de que la red wifi se encuentra desactivada).



Creando conexión inalámbrica con NetworkManager de Gnome



Estableciendo los detalles básicos de conexión



Estableciendo credenciales de acceso a la conexión.

Después de crear la conexión, aun es necesario cambiar el modo de la conexión, de esta forma actuará como AP. Para ello, es necesario editar el siguiente fichero de configuración.

```
sudo gedit /etc/NetworkManager/system-connections/ONO-FAKE
```

Donde “ONO-FAKE” es el nombre que se le ha dado a la conexión. Al abrir dicho fichero de configuración, es necesario cambiar la línea “mode=infrastructure” por “mode=ap”. El contenido del fichero será similar al siguiente:

```
[connection]

id=ONO-FAKE

uuid=c3704266-e143-4705-a3c0-9511fc2d37eb

type=802-11-wireless
```

```
[802-11-wireless]

ssid=ONO12B5

mode=infrastructure

mac-address=9C:D2:1E:43:76:E9

security=802-11-wireless-security

[802-11-wireless-security]

key-mgmt=wpa-psk

psk=testingwpa2ap

[ipv4]

method=auto

[ipv6]

method=auto
```

Con todo lo anterior, ahora se puede activar la red wifi y el dispositivo actuará como un AP con el SSID indicado.

El siguiente paso consiste en capturar todo el trafico correspondiente a las conexiones que realizarán los clientes contra el AP recién creado. Para ello, se puede utilizar Wireshark, TCPDump o airodump-ng para capturar el handshake a medias.

```
sudo tcpdump -i wlan0 -s 65535 -w half-handshake.cap
```

Una forma de conseguir trafico, es utilizando herramientas como aircrack-ng para ejecutar ataques de “deauthenticación” contra los clientes de una red determinada. En el caso de que no exista un AP con el SSID especificado en la zona de acción, pero que se tenga la plena seguridad de que en algún momento habrá clientes que busquen dicho SSID, solamente será cuestión de paciencia y esperar a que dichos clientes ejecuten las peticiones “PROBE_REQUEST”.

Finalmente, es el momento de realizar el ataque por diccionario y para ello, se puede utilizar una herramienta llamada “WPA2-HalfHandshake-Crack”

Utilizando WPA2-HalfHandshake-Crack

“WPA2-HalfHandshake-Crack” es una herramienta que se encarga de realizar ataques por diccionario contra ficheros PCAP con un handshake completo o uno a medias. El proyecto se encuentra ubicado en el siguiente repositorio de GitHub: https://github.com/dxa4481/WPA2-HalfHandshake-Crack.git

Es necesario instalar todas las dependencias para poder ejecutar el script y para ello, se puede lanzar el script setup.py con el argumento “install”. La utilidad principal del proyecto es “halfHandshake.py” y recibe como argumento las siguientes opciones:

-r: Fichero PCAP con el handshake o el handshake a medias que se ha capturado previamente

-m: Dirección MAC del AP.

-s: El SSID del AP.

-d: Ubicación del diccionario para realizar el ataque. Si no se especifica un valor, se lee el diccionario por defecto de la herramienta.

Usando el fichero PCAP capturado en el paso anterior y un diccionario que contiene la contraseña, se puede ejecutar la utilidad para intentar obtener el passphrase.

```
python halfHandshake.py -r half-handshake.cap -m FC15B4FCF606 -s “ONOB4387” -d dictONOFAKE

loading dictionary…

0.02212665655% done. 700.23228772 hashes per second

0.0431311549654% done. 713.574044375 hashes per second

0.0637903739549% done. 714.927209317 hashes per second

0.0851689250818% done. 721.570195251 hashes per second

0.105885690642% done. 721.111075404 hashes per second

Passphrase found! testingwpa2ap
```

Como se puede apreciar, ha sido rápido y limpio, evidentemente porque el diccionario especificado ya contenía la passphrase del AP, sin embargo es bastante ilustrativo para probar el uso de esta herramienta y verificar que aunque no se cuente con un handshake completo, aun sigue siendo posible realizar un ataque por diccionario con un handshake a medias.

Un saludo y Happy Hack!
Adastra