Ethical Hacking: Hacking de Red Inalámbrica Wifi

Wilfredo Jesús Bellido Veizaga
Carrera de Informática
Análisis y diseño de Sistemas de Información
wilfred_bellido@hotmail.com
wilfredbellido@gmail.com

RESUMEN

El principal objetivo de este artículo es para informarse más sobre el hacking de red inalámbrica Wifi pero para ello no lo haremos a modo de receta de cocina, sino que les enseñaremos a fondo como hacerlo y tratando de explicar todos los conceptos necesarios, aun así es recomendable (aunque no necesario) tener conocimientos previos sobre el estándar 802.11 de las redes wifi.

El presente artículo no solo nos servirá para aprender a hackear sino también será de mucha ayuda para prevenir ser víctima de un hackeo de nuestro wifi.

PALABRAS CLAVE

Hacking, Wifi, Router, Network, Wirehark, wireless.

1. INTRODUCCION.

En la actualidad el uso de las Redes de Área Local (LAN) tradicionales es considerablemente amplio, sin embargo dicho uso ya no es únicamente parte elemental de las operaciones de las corporaciones transnacionales, sino se ha extendido al uso doméstico como en los hogares, centros de estudios, centros comerciales, etc.

Pero al tratar de implementar una red LAN, podemos encontrarnos con varios inconvenientes como por ejemplo:

- Costos de desplegar una red a larga distancia (Cableado, equipos).
- Impacto de la instalación de la misma.
- Falta de flexibilidad.

Es por esta razón que se diseñaron las WLAN, o Redes Inalámbricas de Área Local, las cuales ofrecen las comodidades y funcionalidades de las redes LAN tradicionales, sin tener los inconvenientes anteriormente mencionados y es dentro de este tipo de redes inalámbricas que se crea el sistema Wifi.

2. ¿QUÉ ES EL WIFI?

Wifi deriva de "Wireless Fidelity" (Fidelidad Inalámbrica) Es un sistema que establece la transmisión de paquetes de datos sobre redes computacionales para lo cual utiliza ondas de radio propagadas en el aire, en lugar de cables también podemos decir que es un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11, que fue creado con el fin de ser aplicado en redes locales inalámbricas y en la actualidad se lo utiliza también para poder acceder a internet.

2.1 ¿Qué es la norma IEEE.802.11?

Esta norma fue elaborada para sustituir dos capas del modelo OSI (capas físicas y MAC) de la norma 802.3, estándar de las redes LAN tradicionales que utilizan cables es por tal razón que existe solo una diferencia entre una red WiFi y una red Ethernet tradicional, dicha diferencia es la forma de acceso a la red de las terminales; el resto del proceso se realiza de la misma forma para los dos. Por tanto una red inalámbrica regida por el estándar 802.11 (WLAN) es completamente compatible con todos los servicios de las redes locales de cable 802.3 (Ethernet).

3. SEGURIDAD EN WIFI.

En la actualidad uno de los principales y problemas que enfrenta esta tecnología es la seguridad ya que su implementación es simple y la mayoría de las redes inalámbricas son instaladas por administradores de redes y/o sistemas sin tomar en cuenta la seguridad como factor clave. Por consiguiente convierten dichas redes en abiertas, sin proteger la información que por ellas circula.

Existen distintas alternativas para implementar la seguridad de estas redes, las más comunes son la utilización de protocolos de encriptación de datos para los estándares WiFi tales como el WEP y WPA que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los

propios dispositivos inalámbricos, o IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.
Para lo cual existen dos tipos de cifrado de contraseña para protegerla, estos cifrados son WEP y WPA. Se puede decir que es más seguro el cifrado WPA2 (implementación del estándar 802.11i), que es una versión mejorada del protocolo WPA y por tal se convirtió en el mejor protocolo de seguridad para WiFi en la actualidad, por lo tanto más difícil de desencriptar, sobre todo el WPA2 con cifrado AES, por ello en el presente artículo se explicara un poco más sobre los distintos cifrados:

- **WEP (Wired Equivalent Privacy)**: fue el primer estándar para redes wifi y al día de hoy está obsoleto puesto que la protección que ofrece es muy débil.
- **WPA (Wifi Protected Access)**: Este estándar apareció para subsanar las debilidades del WEP y mejorar así la seguridad. Una de las mejoras que introdujo fue el TKIP (Temporal Key Integrity Protocolo), que es capaz de variar automáticamente la contraseña Wifi cada cierto tiempo.
- **WPA2**: Este estándar es el más moderno para proteger redes inalámbricas y el más seguro por lo que se recomienda su uso. Hay que tener en cuenta que WPA2 es compatible con WPA, pero no con WEP. Esto significa que en tu red wifi puedes usar dispositivos WPA2 o WPA indistintamente pero no WEP.
  Este protocolo permite emplear para el cifrado dos posibilidades, TKIP y AES, se ha demostrado que AES es la alternativa más segura.

4. PROGRAMAS PARA HACKEAR.

Para proceder a realizar el hackeo de una red wifi se tiene que saber que esta se divide en dos fases, primero capturar el paquete con la clave correspondiente encriptada y segundo y último paso desencriptar esta clave.
Los programas necesarios para el proceso son "Commview For WIFI" y "Aircrack", los cuales trataremos a fondo en el presente artículo:

- **Commview For WIFI**: es una herramienta para la vigilancia inalámbrica 802.11 a/b/g/n de redes, que nos permite analizar de forma detallada el trafico WLAN.
- **Aircrack**: programa que nos permite analizar los paquetes capturados para descifrar las contraseñas.

Ahora se configura el programa "Commview For WIFI", para los propósitos del hackeo.

- Pestaña "Registros", activar "Guardar automáticamente" y emplear los valores para "Tamaño máximo de directorio" de 600 y para "Tamaño promedio de archivo" de 50.

- A continuación hacemos click en el botón "Play" (el primero del menú empezando por la izquierda) y nos saldrá una ventana para poder ajustar las opciones de exploración de AP (access points, en español, puntos de acceso).

- Ajustamos las opciones y elegimos un AP con clave WEP y pulsas "Capturar", y así lo dejaremos durante un tiempo capturando.

He elegido una red con clave WEP ya que es más sencilla de hackear, para esta parte es suficiente, podemosintentar con Commview y familiarizarnos con el entorno. Aclarar que la versión de evaluación de "Commview For WIFI" solo permite capturar un número limitado de paquetes, tomando en cuenta las dos alternativas que se tiene para saltar esta limitación.

Descifrar las contraseñas de las redes wifi.
Una vez que se hayan capturado suficientes paquetes, se pasa al siguiente paso que es emplear esos archivos que contienen datos de los paquetes para proceder a descifrar la clave. Para ello lo primero será convertir con el propio Commview los archivos de paquetes volcados a formato .cap, para ello hay que elegir la opción de "Archivo -> Visor de registros" y después click a "Exportar Registros" seleccionando la opción "Wirehark Tcpdump".

Una vez que el archivo ya esta listo, se procede a abrirlo abrirlo con Aircrack, se seleccionael archivo .cap y en las opciones se elige "Encryption -> WEP" y "Key Size -> 128 bits". El key size que se elige es el de 128bits porque es el más empleado en la actualidad, hace años se empleaban claves de 64bits, pero hoy en día sería muy raro dar con

una. De todas formas seleccionando 128bits se quedancubiertoslas claves de 64bits también.
Luego aparecerá una pantalla de consola con el mensaje "Index number of target network" , pero se empleara un comando para que efectué el cifrado en función de los IV´s obtenidos. El comando a introducir es "-a 1" y si todo ha salido bien se mostrará en pantalla la clave de la red wifi.
Si se selecciona un índice manualmente, hay que tener en cuenta que debe contener varios IVs, cuantos más mejor.
En caso de que no se muestre la contraseña en pantalla por algún motivo, se debe proceder de la siguiente forma: Iniciar Commview y capturar más paquetes, para conseguir más IVs y proceder otra vez como los anteriores pasos explicados anteriormente con el Air Crack.

5. CONCLUSIONES

En el desarrollo del presente articulo pudimos observar que la utilización de redes inalámbricas de área local ha incrementado debido a la facilidad de su implementación y su costo accesible, también por la comodidad que representa para el usuario mantener la comunicación sin tener ninguna conexión física pero sin embargo debemos tener en cuenta que muchas redes inalámbricas se instalan por personas no conscientes del tema de seguridad, por lo que generalmente las redes instaladas son abiertas, exponiendo toda la información que transmiten
o convirtiéndolas vulnerables al dejar el equipo con las condiciones de seguridad por defecto.

Por ser este un tema muy amplio es que no se abarco un contenido más completo y solo se hizo énfasis en pequeñas introducciones y procesos sobre el hackeo de una red wifi es por tal motivo que en caso de querer estudiar más a profundidad sobre este tema se recomienda visitar los enlaces mencionados en las referencias ya que el presente artículo fue elaborado en base a investigaciones y resúmenes de estos.

6. REFERENCIAS

[1]*http://walhez.com/2008/06/como- hackear-una-red-wifi-wep-en-5-min/*
Visto 24/04/13 16:30

[2]*http://walhez.com/2012/07/hackeo-de-redes-wifi*
Visto 24/04/13 17:30

- [3]*http://biblioteca.usac.edu.gt/tesis/08/08_0466_CS.pdf*

Visto 27/04/13 20:00