Grado en Ingeniería Informática

Seguridad en Tecnologías de la Información
Curso 2017/18

Trabajo de Seguridad:
Redes Wifi

UNIVERSIDAD DE JAÉN

Autor: Manuel Alférez Ruiz

Índice

Introducción

En este informe se pretende hablar sobre las ***características*** del Wi-Fi, su ***funcionamiento*** y las posibilidades de seguridad que presenta.

Por otro lado, se realizará un análisis en cuanto a las medidas que se pueden realizar para mantenernos ***seguros*** y evitar que los intrusos entren en nuestra red, accediendo así a toda nuestra información.

Finalmente, si seguimos los ***consejos*** y las ***pautas*** que se presentaran conseguiremos un sistema de red seguro, y tendremos más controlada la red personal.

¿Qué es Wi-Fi?

Antes de nada, procedemos a definir el ***concepto*** de Wi-Fi y un poco sobre su ***historia***.

Wi-Fi es una tecnología de comunicación inalámbrica que permite conectar a ***Internet*** dispositivos electrónicos, como computadoras, móviles, etc. Originalmente es una abreviación de ***Wireless Fidelity***, es decir, fidelidad sin cables.

Esta tecnología se basa en el uso de ***radiofrecuencias*** para la transmisión de la información. Comprende un conjunto de estándares basados en las especificaciones de IEE 802.11.

Para que funcione, como ya es bien sabido, se necesita un equipo conectado a Internet y dotado de una antena para que ***redistribuya*** esta señal que capta de manera ***inalámbrica***. De esta manera, satisface a todos los usuarios que se ***conecten*** a dicha conexión.

Sobre su historia, hay que decir que la primera transmisión sin cables con ondas electromagnéticas se realizó en ***1888*** a manos de ***Rudolf Hertz***.

Poco después, en ***1899 Marconi*** realizó una comunicación inalámbrica a través del canal de la mancha. Y en ***1971*** la ***Universidad de Hawaii***, creó el sistema de conmutación de paquetes mediante una red de comunicación de radio. Fue la primera red local inalámbrica ***(WLAN***).

A finales de ***1990*** empresas como Nokia crearon ***WECA***, que pasó a llamarse ***Wi-Fi Alliance***, cuya finalidad era el ***fomento*** de la tecnología Wi-Fi y la creación de estándares para que los equipos fueran compatibles entre sí.

Actualmente, se han vendido más de ***2,5 billones*** de dispositivos que incorporar Wi-Fi como medio de comunicación inalámbrica.

Tipos de seguridad Wi-Fi

En esta sección se van a hablar sobre los distintos protocolos de seguridad empleados por la redes Wifi. Dependiendo de si se elige una u otra se podría estar más expuesto a un ataque.

WEP

La encriptación WEP (***Wired Equivalence Privacy***), es sin duda la más ***básica***, ***vulnerable*** y ***fácil*** de ser víctima de un ataque. Apareció en ***1999***, y pese que apareció con muchos agujeros y fallas, se le siguieron aplicando mejoras pero sigue siendo un cifrado ***poco fiable***. Pero aún así, hay muchos usuarios que aún la usan pese a que se van a ver expuestos seriamente. Emplea una clave de 128 bits.

WPA

El cifrado WPA (***Wifi Protected Access***) fue la respuesta que se dio a los problemas del cifrado anterior. Se empezó a usar a partir del año 2003, y usaba claves de ***256 bits.*** Por otro lado, hace una comprobación de contenido e ***integridad*** de mensajes para evitar la intercepción de tráfico.

WPA2

Este cifrado hace uso del algoritmo de ***AES***, el cual es un cifrado por bloques adoptado como estándar de cifrado de los estados unidos. Dicho algoritmo emplea claves más largas y más seguras y además implementa el ***CCMP***, es decir, un protocolo mejorado de encriptación que sustituye al que venia utilizando el WPA.

Consideración final

Finalmente, a modo de reflexión, en base al análisis visto, la mejor opción es el cifrado ***WPA2***, ya que estaríamos limitando los ataques recibidos debido a su ***dificultad.*** La única manera de atacarlo sería tener acceso a red protegida y hacer uso de la fuerza bruta. Por ello, sería conveniente tener activado el cifrado AES y ***desactivado la opción WPS*** para evitar ataques.

Seguridad en red personal

En esta sección se va a tratar la seguridad en un ***ámbito personal***, es decir, cómo saber si alguien está conectado a nuestra red y actuar en consecuencia.

En mi caso, uso ***Linux*** como sistema operativo por defecto. Ahora bien, instalando los paquetes necesarios en nuestro sistema:

```
sudo apt-get install nast nmap
```

Tendríamos instaladas las herramientas. Ahora escribiríamos:

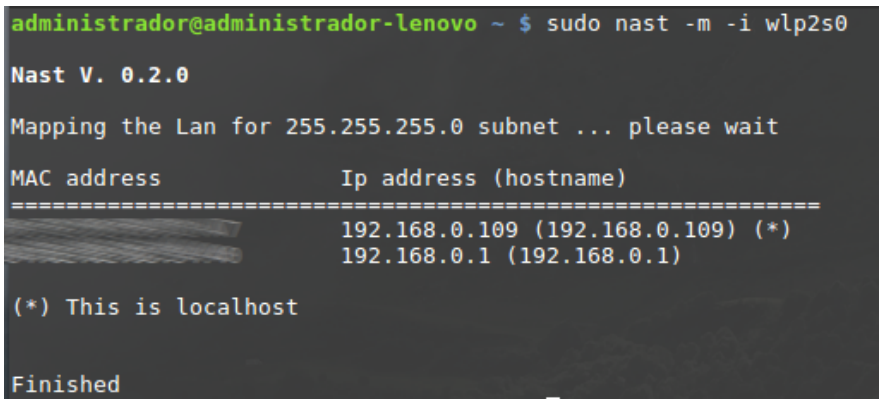
```
sudo nast -m -i (nuestra_tarjeta_de_red)
```

Una manera de saber la ***tarjeta de red*** que estamos usando es escribir en la terminal:

```
ifconfig
```

Y esto nos devolvería algo como esto:

Tras escribir el segundo comando nos aparecería por la terminal los terminales que se encuentran conectados a la red:



En este caso aparecen dos, yo mismo y la del router. También se puede observar la ***advertencia*** en forma de asterisco de que dicho cliente es ***ajeno*** al sistema.

En la siguiente sección se plantean algunas medidas más para aumentar la seguridad de nuestra red Wifi.

Aumentando la seguridad

Aunque la seguridad total no existe, existen alguna pautas con las que se consiguen una mayor privacidad y grado de seguridad.

La primera de ellas es ***cambiar la contraseña*** y dirección IP por defecto del router. Ya que en muchos casos, los router que distribuyen las distintas compañías usan una seria de contraseñas conocidas y mediante un ataque de diccionario se podría acceder a la red.

Por otro lado, como ya hemos dicho es elegir el sistema de cifrado como WPA2 y una clave preferiblemente ***alfanumérica*** larga. Cuanto más larga sea esta clave y aleatoria mejor.

Si se utiliza un filtrado por ***MAC*** y usamos una lista de los ordenadores que se conectan a nuestra red es mejor ya que denegamos el acceso a la red a los usuarios que no están en dicha lista (aún teniendo la clave).

Por otro lado, si limitamos la ***potencia de emisión*** podemos evitar que un atacante situado a más distancia de nuestro hogar le sea más difícil de atacarnos. Con tal de que dicha señal llegue a todos los puntos del hogar es suficiente.

Si por alguna circunstancia nos ausentamos del hogar durante mucho tiempo es mejor dejar ***apagado*** el Wifi, ya que conseguimos un ahorro de energía y evitamos que se aprovechen de nuestra conexión.

Por otro lado, algunos router incorporan la nueva tecnología del ***5G***, pues bien dicha tecnología en ocasiones no nos permite cambiar la clave y crea una puerta trasera. Por tanto, lo mejor es apagarlo.

Finalmente, una buena práctica es ***verificar*** regularmente quien se conecta a nuestra red, de esta manera realizamos un control periódicamente disminuyendo las posibilidad de que alguien se encuentre conectado por demasiado tiempo.

Referencias

- https://www.significados.com/wifi/
- http://pleasenetworks.com/blog/post/13/historia-y-evolucin-de-las-redes-wifi-de-tecnologa-inalmbrica-a-aplicacin-ligera-para-retailers
- http://wifihacker.es/tipos-de-seguridad-wifi/
- https://www.redeszone.net/2015/01/01/comprueba-los-usuarios-conectados-tu-red-wi-fi-con-nmap-y-nast/
- https://www.xataka.com/ordenadores/como-proteger-tu-wifi-por-completo
- https://www.osi.es/es/protege-tu-wifi