CURSO DE HACKING ÉTICO

REDES INHALÁMBRICAS – TEORÍA I

Objetivos

- Describir los conceptos de una red WIFI
- Entender los diferentes tipos de encriptación
- Describir las amenazas en redes WIFI
- Entender la metodología para Hackear una red WIFI
- Conocer diferentes herramientas para redes WIFI

Conceptos de redes WIFI

Las redes inalámbricas han revolucionado la forma de trabajar de las personas. Han eliminado las limitaciones de las redes físicas a nivel de conectores y cableado, y han hecho que los datos sean portables, móviles y accesibles.

De forma muy sencilla, la redes inalámbricas son sistemas que permiten la comunicación entre un emisor y un receptor usando radiofrecuencia.

Terminología inalámbrica (WIFI)

Ancho de Banda (Bandwidth)

Describe la cantidad de información que puede ser enviada por una conexión. Normalmente, el ancho de banda se refiere a la tasa de transferencia medida en bps (bits por segundo)

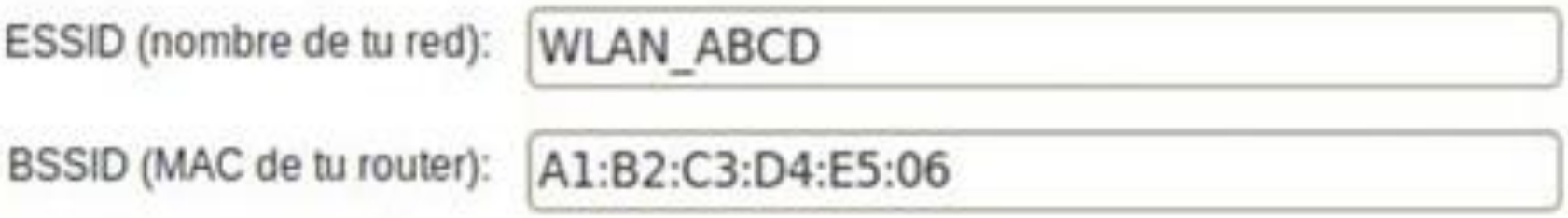
Estándares de Wi-Fi 802.11

Estándar	Velocidad máxima	Frecuencia	Compatibilidad con versiones anteriores
802.11a	54 Mbps	5 GHz	No
802.11b	11 Mbps	2,4 GHz	No
802.11g	54 Mbps	2,4 GHz	802.11b
802.11n	600 Mbps	2,4 GHz o 5 GHz	802.11b/g
802.11ac	1,3 Gbps (1300 Mbps)	2,4 GHz y 5,5 GHz	802.11b/g/n
802.11ad	7 Gbps (7000 Mbps)	2,4 GHz, 5 GHz y 60 GHz	802.11b/g/n/ac

Terminología inalámbrica (WIFI)

BSSID (Basic Service Set Identifer)

La MAC del punto de acceso (AP). Usualmente los usuarios no son conscientes de dicha información. Solo necesitan el nombre del punto de Acceso y la contraseña para poder utilizar la red inalámbrica.
Cuando un usuario se desplaza de un lugar a otro, el BSS podría cambiar dado que se cambio de AP, cambio que no debería afectar al usuario que sigue identificándose con Nombre y Contraseña.
Normalmente se expresa en formato hexadecimal: A1:B2:C3:D4:E5:06



Terminología inalámbrica (WIFI)

Punto de acceso – AP (Access Point)

Los puntos de acceso son utilizados para conectar los diferentes dispositivos a una red cableada o no.

Terminología inalámbrica (WIFI)

Hotspot

Lugares donde se dispone de redes inalámbricas de uso público. Importante tener presente la seguridad en lugares donde se disponga de redes WIFI gratuitas.

Se recomienda navegar cerrando túneles VPN para evitar comprometer la información con la que trabajamos.

Terminología inalámbrica (WIFI)

Asociación (Association)

El proceso de conexión de un dispositivo inalámbrico a un punto de acceso.

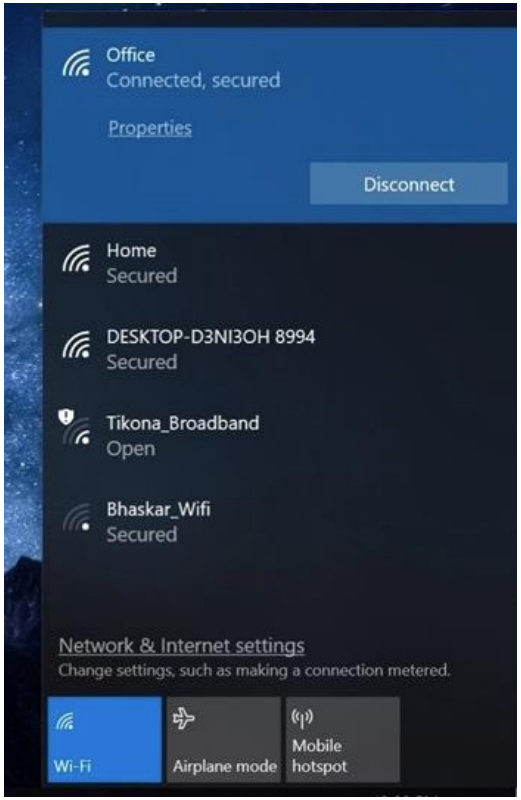
Normalmente este punto es clave en la obtención de contraseñas de puntos de acceso, dado que el token que permite la conexión entre el dispositivo WIFI y el Punto de Access es clave para poder obtener la contraseña de acceso.

Terminología inalámbrica (WIFI)

SSID – Service Set Identifier

Es una cadena alfanumérica de 32 caracteres de longitud que identifica al Punto de Acceso.

Los dispositivos conectamos a una misma red WLAN, deben usar el mismo SSID para establecer la conexión.

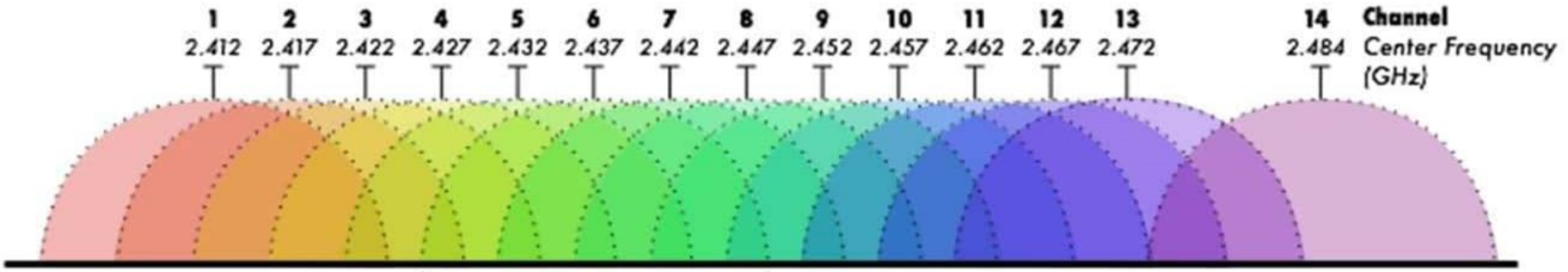


Terminología inalámbrica (WIFI)

Canales WIFI

Cuando nos conectamos de forma inalámbrica lo hacemos en una frecuencia determinada asignada por el “punto de acceso”. El dispositivo se “engancha” a su frecuencia y enviamos y recibimos los datos por la “autopista” creada en la conexión.

El éxito del wifi ha hecho que se masifique en muchas zonas, coincidiendo muchos puntos de acceso en la misma zona de emisión, provocando numerosos conflictos de frecuencias. La conectividad wifi en la frecuencia de 2,4Ghz trabaja con 13 “canales”, siendo teóricamente los más bajos los que dan más alcance. Con este gráfico podemos ver su distribución y solapamiento.



Terminología inalámbrica (WIFI)

Limitaciones de 2.4GHz

Durante muchos años las redes inalámbricas se han creado utilizando la frecuencia 2.4GHz. A medida que estas redes han ido creciendo, el número de estas redes y usuarios han ido creciendo, y por tanto los problemas de interferencias han empezado a aparecer. En zonas con muchas antenas, los conflictos e interferencias entre ellas empiezan a ser un problema.

Otro problema con las redes 2.4GHz es que la frecuencia también es usada, entre otras cosas, por algunos radares, los teléfonos móviles, los walkie-talkie y los microondas, causando más interferencias de las generadas por las antenas. Todo este tráfico y señales que interfieren reducen la velocidad de la red inalámbrica. Podemos encontrarnos en una zona con máxima cobertura, pero el “ruido” nos va a impedir trabajar.

Terminología inalámbrica (WIFI)

Redes 5GHz

Las redes de 5GHz pueden ser un alivio para la saturación de la 2.4GHz. Tiene una señal más limpia y más canales que pueden ser combinados para mayor velocidad. Actualmente las redes WiFi 5GHz tienen menos tráfico, con lo que pueden manejar mayores velocidades.

Operan en un espectro mucho más amplio, con canales no compartidos con ninguna otra red. Cada canal tiene 20MHz de ancho de banda, lo que garantiza mejor velocidad si comparamos con las wifi 2.4GHz (la banda completa sólo tiene 80MHz de ancho).

Permiten trabajar hasta 400 Mbps

Terminología inalámbrica (WIFI)

Estándares inalámbricos

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

Tipos de encriptación inalámbrica

PROTOCOLO	Descripción
WEP de 64 bits	Es el estándar de encriptación WEP más viejo, altamente vulnerable y no es recomendable utilizarlo
WEP de 128 bits	Mantiene la base del WEP anterior sólo que con un cifrado de mayor tamaño, igualmente inseguro y nada recomendable.
WPA-PSK (TKIP):	En esencia es básicamente el cifrado estándar WPA o WPA1, que ya ha sido ampliamente superado y no es seguro.

Tipos de encriptación inalámbrica

PROTOCOLO	Descripción
WPA-PSK (AES)	Elige el protocolo inalámbrico WPA con el cifrado más moderno AES. Los dispositivos que soportan AES casi siempre soportarán WPA2, mientras que los dispositivos que requieran WPA1 casi nunca admitirán el cifrado AES, por lo que es un sin sentido que añadimos más que nada como curiosidad.
WPA2-PSK (TKIP)	Utiliza el estándar WPA2 con cifrado TKIP. Como vimos esta opción no es segura, pero si tenemos dispositivos antiguos que no soportan una red WPA2-PSK (AES) es necesario para poder seguir utilizándolos.

Tipos de encriptación inalámbrica

PROTOCOLO	Descripción
WPA2-PSK (AES)	La opción más segura. Utiliza WPA2, el último estándar de encriptación Wi-Fi, y el más reciente protocolo de encriptación AES. Ya lo dijimos en su momento y lo reiteramos, ***salvo por razones de fuerza mayor debería ser nuestra única opción***.
WPA2-PSK (TKIP / AES):	Utiliza WPA y WPA2 con TKIP y AES, proporcionando la máxima compatibilidad con todos los dispositivos antiguos y es la opción predeterminada de muchos routers para evitar problemas, pero termina ralentizando el tráfico y siendo insegura, por lo que no es recomendable.