**Evaluación Contínua 1.2 - Seguridad Wireless**

**Chequeado**

Alumno: Gonzalo Benito

Email: [gu4n4rt@gmail.com](mailto:gu4n4rt@gmail.com)

• Crear una tabla con los nombres de las diferentes redes WiFi. Indicar qué tipo de protocolo de seguridad tienen configurado (redes abiertas, WEP, WPA/WPA2 Personal o Enterprise). Además, el alumno debe evaluar la seguridad del cifrado indicando por qué es seguro o por qué no.

• En la tabla anterior añadir una columna con la información del BSSID de los puntos de acceso.

• En la tabla añadir una columna para indicar en qué canal se emite la red inalámbrica. Responder si existe algún canal en el que haya una gran población de redes inalámbricas, ¿Qué recomendaríais?

• Añadir a la tabla una columna con la intensidad de la red. En función de la intensidad responder: ¿Se encuentra cerca o lejos el punto de acceso?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Protocolo de Seguridad | BSSID | Canal | Intensidad  de la  Red |
| Fibertel WiFi195 2.4GHz | WPA/WPA2-PSK | E8:D2:FF:AC:5F:06 | 11 | -60dBm |
| Speedy-0698B3 | WPA/WPA2-PSK | 50:68:0A:06:98:BC | 11 (9) | -61dBm |
| CoopenetULTRA-1706601 | WPA/WPA2-PSK | 72:02:71:8C:3E:29 | 1 | -63dBm |
| Fibertel WiFi554 2.4GHz | WPA/WPA2-PSK | B0:BB:E5:42:C5:EA | 6 | -65dBm |

***“Evaluar la seguridad del cifrado indicando por qué es seguro o por qué no”***

En todas las redes observadas pude observar que se utiliza el protocolo de seguridad recomendado, WPA2-PSK. Por el contrario, no encontré ninguna red que emplee el cifrado WEP, actualmente obsoleto dada la facilidad de interceptar y descifrar el tráfico con métodos ampliamente conocidos.

WPA2-PSK es el sistema más utilizado y seguro (aunque aún así vulnerable) para las redes domésticas que pude encontrar con el análisis. La razón de su seguridad se debe, principalmente, a que utiliza un algoritmo de cifrado más seguro que WPA y WEP, que es CCMP (Counter-mode/CBC-MAC Protocol), basado en AES (Advanced Encryption System).

Esto supone un gran avance en materia de seguridad, dificultando a un atacante el ataque, más no imposibilitándolo, puesto que aún posee métodos conocidos para vulnerarlo.

Los diversos métodos se basan en monitorizar el tráfico en el aire e interceptar el 4-way-handshake para utilizar cracking y obtener la clave de la red.

***“Responder si existe algún canal en el que haya una gran población de redes inalámbricas ¿Qué recomendarías?”***

Existe una mayor cantidad de redes en el canal 1, 6 y 11. Mi recomendación (o la de la aplicación de análisis WiFi) es utilizar el menos poblado (marcado con mejor puntuación).

La razón es sencilla, cada canal es una determinada banda de frecuencia sobre la que funcionarán las redes inalámbricas. A mayor población en un canal, mayores interferencias entre redes habrá, lo que se traduce a un peor rendimiento general.

***“En función de la intensidad responder: ¿Se encuentra cerca o lejos el punto de acceso?”***

La fuerza de señal se representa en formato -dBm (0 a -100). Mientras más cercano sea el valor a 0, más fuerte será la señal.

Teniendo en cuenta esto (la misma aplicación de análisis nos muestra un valor aproximado), el primer punto de acceso de mi tabla (Fibertel WiFi195 2.4GHz) se encuentra más cerca que el último AP (Fibertel WiFi554 2.4GHz).