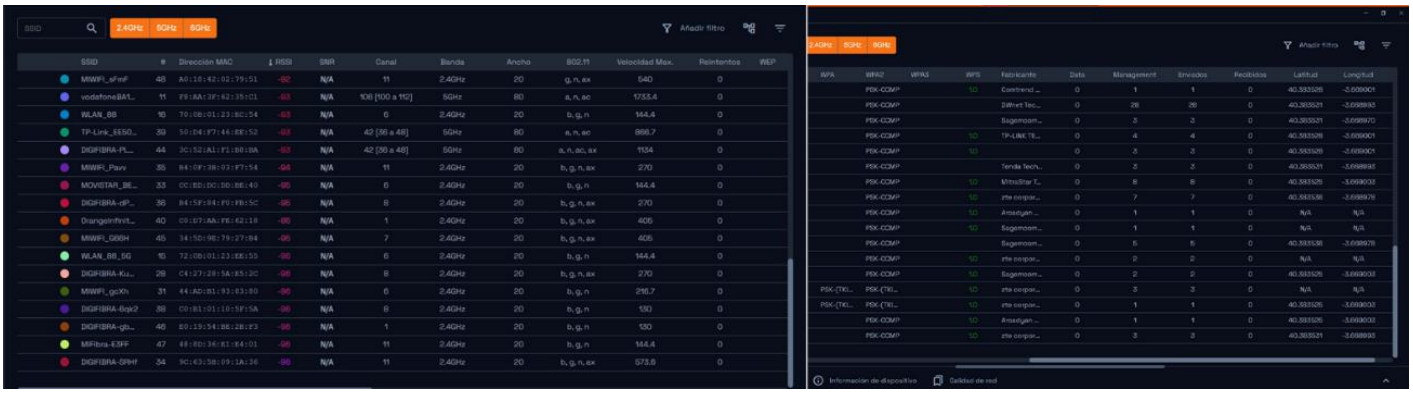
RETO 10 SEGURIDAD EN SISTEMAS Y REDES

CIM31-G11

Imágenes observadas en el estudio



Mecanismos de Seguridad Observados

1. **PSK-CCMP (WPA2)**
   WPA2 (la evolución a WPA) es un mecanismo bastante seguro; sin embargo, presenta ciertas debilidades o ataques realizados a este tiempo atrás. WPA2 utiliza el algoritmo AES para encriptar. A pesar de las vulnerabilidades detectadas, se pueden resolver mediante el uso de configuraciones adecuadas.

2. **WPA**
   WPA es la evolución de WEP (cifrado mediante RC4 con claves de 64 o 128 bits), siendo más seguro, pero obviamente menos resistente que WPA2. Este, a diferencia de WEP, usa claves dinámicas. Sin duda es recomendable elegir WPA2 si se encuentra disponible para su uso.

Para asegurarse de un buen uso, se recomienda, como anteriormente se ha mencionado, **mantener WPA2 como mecanismo principal de seguridad y actualizar regularmente el firmware,** ya que protege contra la mayoría de los ataques. Por otro lado, conviene (si no es necesario) desactivar WPS ya que pueden entorpecer la seguridad aun con WPA2.

Estudio Geográfico

El estudio fue realizado en una zona residencial tensionada de clase baja, provocando que ciertas redes usen WPA como mecanismo de seguridad, así como un uso inexistente de WPA3. Esto puede ser por diversos motivos:

1. **Falta de conexión con ciertos proveedores**
   Normalmente, los equipos que se suelen tener en barrios de clase obrera suelen ser los proporcionados por las operadoras. Es por ello que esto puede provocar que los routers, al ser bastante básicos, solo soporten como máximo WPA2 y no WPA3.

2. **Acceso limitado a dispositivos y conocimiento**
   En barrios humildes puede ser más obvio el carecer de la economía suficiente para renovar los equipos tecnólogicos, teniendo que producirse cada 5-10 años.

Diego Espinosa, Manuel Neto, Lucía González y Paul Rodríguez

Es por esto que esos equipos pueden no ser compatibles con una seguridad más avanzada y provocar el uso de WPA, así como un desconocimiento total sobre la seguridad en redes.

3. **Falta de empresas**
   Uniéndose al punto 1, donde los proveedores suelen “prestar” los dispositivos a sus compradores, también puede ser que no todas las operadoras puedan llegar a todas las zonas de una ciudad, provocando mayor desinterés por la seguridad en esos lugares. Por ejemplo, si una zona solo tiene la red de Movistar con Wi-Fi 5, es innecesario dotarla con una seguridad tan alta que sea de uso para redes como por ejemplo Wi-Fi 6. Si hubiera mayor competencia de empresas en esa zona, se implementaría mayor seguridad en redes.