Q-WiFi®

El **Q-WiFi**® es una amalgama de una serie de paquetes de software de código abierto que se ejecutan en un dispositivo de red de consumo extremadamente pequeño diseñado para detectar y frustrar los puntos de acceso inalámbricos "Evil Twin" (WAP). El **Q-WiFi** evita que los Evil Twin APs engañen a los usuarios al mismo tiempo que monitorean los dispositivos y servicios de red y proporcionan detección y prevención de intrusiones. La protección WiFi incluida bloquea activamente el "Evil Twin" en su detección al desencadenar un ataque de denegación de servicio (DoS) para evitar que los usuarios inicien sesión en él. El diseño ultra compacto permite opciones de implementación excepcionalmente flexibles y creativas, así como ahorros significativos de electricidad y espacio.

- *Especificaciones de Hardware **Q-WiFi:***
- 108 mm x 64 mm x 26 mm – 170 gramos (4.25" x 2.50" x 1.125" – 6 oz)
- Consumo de energía a plena carga: 8 watts, 120v-240v
- No hay ventilador ni ninguna pieza móvil. Debe instalarse en un espacio bien ventilado.
- Funciona de 0°C a 70°C (32°F–158°F)

Indicadores LED:

- Energia electrica
- Enlace (conexión física a la red)
- Actividad (tráfico de red)
- FDX (duplex completo)
- 100 (10/100 mbps conexión)

El dispositivo de red **Q-WiFi** incluye:

- **EvilAP_Defender** – **EvilAP_Defender** es la principal herramienta de código abierto y de clase empresarial para descubrir y evitar que los puntos de acceso Twin (AP) de Malvados ataquen a los usuarios inalámbricos. El **Q-WiFi** puede descubrir y proporcionar una alerta de correo electrónico cuando se descubre un Evil Twin. Además, puede realizar un ataque de Denegación de Servicio ("DoS") para evitar que los usuarios legítimos de WiFi se conecten al AP de Twin Evil. Esto puede dar a los administradores de red y / o tiempo de aplicación de la ley para localizar y eliminar el AP Malvado. ***N.B.*** La función DoS sólo funciona si el Evil Twin y el AP legítimo tienen el mismo SSID pero diferentes BSSID, o están ejecutándose en un canal diferente. (El BSSID - Basic Service Set Identifier - es la dirección MAC del AP.) Esto evita accidentalmente paralizar un AP legítimo. La lista blanca se realiza a través de un asistente durante la instalación para reconocer y permitir puntos de acceso inalámbricos (AP) legítimos.
- **Aircrack-ng – Aircrack-ng** permite al **Q-WiFi** capturar y monitorizar el tráfico WiFi. **Aircrack-ng** alimenta estos datos a **EvilAP_Defender**.
- **qAircrack-ng – qAircrack-ng** es la GUI basada en la web para **Aircrack-ng**.
- **ModSecurity**® **– ModSecurity**® ("**ModSec**") es el principal paquete de protección contra ataques de scripts cruzados de código abierto para endurecer el servidor web Apache de **Q-WiFi** y prevenir ataques concebibles.
- **Tiny Honeypot (THP) - THP** engaña a los atacantes haciendo que parezca que el

Quantalytics, Inc.
220 Henley Rd.
Woodmere, NY 11598

Contacto: Richard Avery
+1 646-449-7810
q-wifi@quantalytics.com

ataque está funcionando, mientras que mientras registra la información de ataque. **THP** desperdicia el tiempo de un atacante y crea una oportunidad para detectar la intrusión de red ofreciendo al atacante lo que parece ser miles de servicios.

- **HA Proxy – HA Proxy** es el paquete líder de código abierto para la conmutación automática y el equilibrio de carga. Se pueden conectar hasta 32 dispositivos **Q-WiFi** para la conmutación automática o el equilibrio de carga para la cobertura de redes extremadamente grandes. La administración se realiza a través de una GUI Web.
- **ClamAV® – ClamAV®** es el paquete de software antivirus de código abierto líder.
- **Webmin – Webmin** es el principal paquete de GUI Web de código abierto para la configuración y el mantenimiento del servidor. **Webmin** también permite la vinculación de múltiples dispositivos **Q-VUL** para la administración simplificada.

El dispositivo de red **Q-WiFi** se administra completamente a través de una GUI Web. Esto hace que todas las funciones estén fácilmente disponibles incluso para los administradores de redes principiantes. No se requiere ninguna habilidad de interfaz de línea de comandos (CLI) o Linux.

El dispositivo de red **Q-WiFi** tiene un NIC 10/100 y un 802.11 b / g / n WiFi. El **Q-WiFi** está destinado a ser desplegado dondequiera que exista el riesgo de un ataque de Evil Twin. E.G. Espacios públicos donde se ofrece WiFi gratuito, además de redes WiFi privadas.

Usando el módulo **Webmin** proporcionado, la autenticación de dos factores se puede agregar usando **Google Authenticator** o **Authy**, un servicio comercial con su propia aplicación. **Google Authenticator** se ejecuta en dispositivos Android, IOS y Blackberry y utiliza el protocolo TOTP estándar.

Las notificaciones se proporcionan por correo electrónico utilizando **SendMail**, que está configurado con un módulo en **Webmin**, y las entradas de syslog. El dispositivo de red **Q-WiFi** se puede integrar con **Nagios®** en el **Q-Box®** como otra ruta de notificación. La notificación por SMS está disponible como opción. El dispositivo de red **Q-WiFi** también se puede integrar con el dispositivo de red **Q-Log®** o cualquier otra solución Syslog o SEIM.

Quantalytics, Inc.
220 Henley Rd.
Woodmere, NY 11598

Contacto: Richard Avery
+1 646-449-7810
q-wifi@quantalytics.com