FORTINET
NSE Training Institute

NSE 2 WiFi Scripts—Spanish Version

¡Hola! En esta clase, definiremos qué es el Wi-Fi y veremos algunos aspectos sobre la seguridad de las redes inalámbricas.

El Wi-Fi es una tecnología para conectar dispositivos a una red de área local inalámbrica, basada en la norma estándar IEEE 802.11. Diseñado sobre todo para uso industrial, comenzó a pequeña escala. Sin embargo, creció y hoy es la principal forma de conexión para los dispositivos electrónicos de uso personal, ya sea en el hogar o en la oficina.

El desarrollo del Wi-Fi se basó en muchos de los protocolos y tecnologías de Ethernet, con una diferencia sustancial. Todas las transmisiones son a través del aire, por lo que, al igual que en una conversación oral, cualquiera podía escuchar lo que se decía.

Al principio, los mecanismos de autenticación y de privacidad para el Wi-Fi eran muy débiles. El estándar tenía una opción simple de cifrado, llamada "privacidad equivalente a cableado" (*Wired Equivalent Privacy*, WEP). Este sistema utilizaba una clave para cifrar el tráfico mediante el cifrado de tipo RC4. No obstante, el WEP era bastante fácil de vulnerar si se disponía de las herramientas adecuadas y de un equipo con una potencia razonable. Así, se corrió la voz de que el Wi-Fi era inseguro y de que la tecnología, que apenas estaba empezando a desarrollarse, presentaba graves problemas.

Las partes interesadas se reunieron con el Instituto de Ingeniería Eléctrica y Electrónica (*Institute of Electrical and Electronics Engineers*, IEEE) y con la organización Wi-Fi Alliance para diseñar el sistema de acceso inalámbrico protegido (*Wi-Fi Protected Access*, WPA). Este añadía características de seguridad adicionales, pero conservaba el algoritmo RC4, por lo que los usuarios podían actualizar los dispositivos anteriores de manera sencilla. Sin embargo, no resolvía el problema fundamental de la seguridad.

Además, se introdujo una nueva versión del acceso inalámbrico protegido, el WPA2. Este nuevo estándar estaba basado en el algoritmo AES (*Advanced Encryption Standard*), creado por el Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology*, NIST). Era mucho más seguro que el WEP. Además, la tecnología incorporó una autenticación

para empresas y se crearon dos opciones para cada estilo de seguridad. La de tipo personal continuó utilizando una frase de contraseña compartida para la autenticación de red y el intercambio de claves. La seguridad para empresas, en cambio, utilizaba los mecanismos de autenticación 802.1x, similares a los de las redes cableadas, para autenticar usuarios y establecer el cifrado. Aun así, si la frase de contraseña elegida era débil o no era adecuada, la red seguía siendo vulnerable.

En 2018 se lanzó la tercera versión del acceso inalámbrico protegido o WPA3, que introdujo un protocolo nuevo y más seguro para establecer conexiones, un método más sencillo para agregar dispositivos a la red y una longitud de clave mayor, entre otras características de seguridad.

Podría pensarse que eso era suficiente, que el Wi-Fi era seguro y no había nada por lo que preocuparse. Por desgracia, no fue así. Los atacantes han encontrado varias formas de aprovechar el comportamiento humano y obtener acceso a la información que desean.

Cuando estamos en lugares públicos, buscamos un cartel que ofrezca Wi-Fi gratuito, pero este conlleva sus riesgos. Los atacantes establecen puntos de acceso en áreas públicas, que actúan como sistemas señuelo o *honeypots*. Los usuarios se confían y se conectan a estas supuestas redes gratuitas, sin darse cuenta de que el atacante puede ver todo lo que hacen en línea. Por ejemplo, si ingresamos las credenciales de una cuenta o la información de una tarjeta de crédito, puede acceder a ellas. Debemos ser prudentes, incluso si el nombre de una red parece legítimo.

Además, los dispositivos portátiles recuerdan las redes a las que nos hemos conectado en el pasado. Por cuestiones de simplicidad, buscan esas redes de manera automática y se reconectan cuando las encuentran. De este modo, un atacante puede espiar nuestro teléfono y buscar la red de Wi-Fi legítima a la que nos conectamos el año pasado en un hotel, crear un punto de acceso falso con ese mismo nombre y, así, engañarnos para que nos conectemos. A menos que notemos que el dispositivo está conectado al Wi-Fi, podemos brindar información a través del punto de acceso falso y revelar todo lo que hacemos.

Pero no solo corremos un riesgo cuando estamos fuera de casa. Muchas personas configuran una red doméstica, pero no activan la seguridad. Si lo hicieron, fue hace mucho: posiblemente, utilizaron el sistema WEP o WPA, y nunca lo actualizaron con una frase de contraseña más sólida. Los *firmware* más recientes para enrutadores inalámbricos domésticos ofrecen características adicionales, como el WPA3 o la visibilidad de los dispositivos conectados a la red. Siempre es conveniente mantener la seguridad actualizada y elegir frases de contraseña que sean complejas y difíciles de averiguar. Cuanto mínimo, debemos cambiar el identificador SSID (*service set identifier*), además del nombre de usuario y la contraseña de administrador que vienen de fábrica. También debemos controlar la red doméstica y asegurarnos de que reconocemos todos los dispositivos que están conectados. Si un atacante accede a una red, puede ver **todo** lo que sucede en ella. En esta instancia, ya no se trata del tráfico inalámbrico que enviamos, sino de los dispositivos que pueden quedar en riesgo y de la información que puede obtenerse a través de ellos.

Los retos relacionados con las conexiones de Wi-Fi para empresas son cada vez mayores. Con la internet de las cosas, la tendencia de llevar los dispositivos personales al trabajo y la gran cantidad de trabajadores remotos, es fundamental administrar los puntos de acceso. Al mismo tiempo, hay que ocuparse de las crecientes amenazas de seguridad, ya sea en la empresa, en puestos remotos o en el hogar.

Fortinet le ofrece el producto inalámbrico FortiAP™. Es compatible con las tecnologías de Wi-Fi más recientes, y puede integrarse y administrarse con FortiGate®, el firewall de última generación.

Gracias por su tiempo, y no olvide responder las preguntas a continuación.