RESUMEN

Wi Fi es una tecnología que ha ido fascinando y consolidándose en las infraestructuras de red; pero su seguridad fue y sigue siendo una debilidad para las redes inalámbricas; porque el medio inclina la balanza hacia los atacantes. Mucho antes de su primer paso; a WEP, ya se le presentaban sus opositores, luego en la lucha por mejorar esta situación nacen consecuentemente WPA y WPA2. No obstante no sólo los protocolos iban evolucionando también las habilidades y herramientas de los hackers toman fuerza; inclusive la gran herramienta llamada Internet permitió que no sólo personas con gran conocimiento lograran sus ataques, ahora cualquiera con acceso a Internet puede adquirir herramientas tan fascinantes y efectivas en la realización de ataques. Pero también surgen y van madurando, herramientas tan valiosas como los IDSs, permitiendo no sólo dar un plus más de seguridad con la emisión de sus alertas; también brindan una forma de aprendizaje de la ejecución de un ataque. Cabe la necesidad de una evaluación de las mismas para determinar que tan desarrolladas están en el tema de Seguridad Inalámbrica, así los Benchmarks, agrupados en las herramientas de ataque de Backtrack ayudan a medir la efectividad de los sistemas Kismet y Snort, popularmente conocidos, para así dejar al descubierto fortalezas y debilidades de los IDSs; en el importante campo de la tecnología Wi Fi.

Palabras clave:

Wi Fi, Ataques, Backtrack, Snort, Kismet.