Maestría en

CIBERSEGURIDAD

Trabajo final de Maestría previa a la obtención del título de Magíster en Ciberseguridad

AUTORES:

Ing. Castro Robles Fernando

Ing. Ganán Flores Ronald

Ing. Pillajo Morocho José

TUTOR:

Ing. Cortés Lopez Alejandro

TEMA:

Análisis de tráfico wifi y estudio de seguridad

RESUMEN

El presente trabajo final de maestría aborda el análisis de tráfico en redes Wi-Fi y su relación con la seguridad de la información en entornos inalámbricos. El estudio se centra en la identificación de patrones de tráfico, la evaluación de posibles vulnerabilidades en los protocolos de seguridad más comunes, y la exploración de técnicas utilizadas por atacantes para comprometer redes las redes inalámbricas mediante ataques.

A lo largo del estudio, se utilizaron herramientas especializadas para monitorear el tráfico de red y se realizaron pruebas sobre los protocolos WEP, WPA y WPA2, con el fin de evaluar su resistencia frente a diversos tipos de ataques, como el man-in-the-middle y wps. El análisis revela las principales debilidades de cada protocolo y ofrece una visión sobre las amenazas más relevantes en entornos inalámbricos.

Además, se proponen una serie de recomendaciones orientadas a mejorar la seguridad de las redes Wi-Fi, basadas en el uso de métodos de encriptación robustos, la correcta configuración de los puntos de acceso y la implementación de medidas de prevención para detectar y mitigar ataques. El trabajo final de maestría concluye que, aunque las redes Wi-Fi siguen siendo vulnerables a ciertos tipos de ataques, una adecuada gestión de seguridad puede reducir significativamente los riesgos.

Palabras claves: Wi-Fi, Análisis de red, Vulnerabilidad, Seguridad, Wireshark.

ABSTRACT

This master's thesis deals with traffic analysis in Wi-Fi networks and its relationship with information security in wireless environments. The study focuses on the identification of traffic patterns, the evaluation of possible vulnerabilities in the most common security protocols, and the exploration of techniques used by attackers to compromise wireless networks through attacks.

Throughout the study, specialized tools were used to monitor network traffic and tests were performed on the WEP, WPA and WPA2 protocols, in order to evaluate their resistance to various types of attacks, such as man-in-the-middle and wps. The analysis reveals the main weaknesses of each protocol and provides insight into the most relevant threats in wireless environments.

In addition, a series of recommendations aimed at improving the security of Wi-Fi networks are proposed, based on the use of robust encryption methods, the correct configuration of access points and the implementation of prevention measures to detect and mitigate attacks. The final master's thesis concludes that, although Wi-Fi networks are still vulnerable to certain types of attacks, proper security management can significantly reduce the risks.

Keywords: Wi-Fi, Network analysis, Vulnerability, Security, Wireshark.