

Resumen

En las últimas décadas con el avance tecnológico y la necesidad de comunicarse para intercambiar información ha generado que las personas recurran al uso masivo de redes inalámbricas tanto a nivel empresarial, así como en sus hogares; éste incremento en el uso de redes inalámbricas ha provocado que sean más susceptibles a ataques y que estos sean perjudiciales para el desempeño de la red, así como para la seguridad de la información de los usuarios. El presente proyecto se desarrolla un aplicativo compatible con el sistema operativo Windows que permite caracterizar y mostrar las tramas 802.11 de una red inalámbrica en tiempo real, de manera sencilla y automatizada. Para poder realizar la captura de tráfico se utilizaron los chipsets compatibles con Windows y con el controlador de Acrylic, el cual permite colocar la tarjeta de red en modo monitor al igual que módulos AirPcap NX tanto en mono canal como multicanal y así obtener información sobre los protocolos inalámbricos. La implementación del algoritmo utiliza la técnica de sniffing que permite en modo de ataque pasivo capturar el tráfico generado en conexiones locales, así como el tráfico generado por las conexiones de los otros usuarios. Los resultados obtenidos mediante la captura del tráfico proporcionan tramas de administración, datos, control y direcciones MAC/IP; mismos que serán analizados para comprobar la eficiencia del aplicativo desarrollado, comparando sus resultados con otro software llamado Wireshark y de este modo exponer conclusiones sobre su uso, desempeño y eficiencia.

Palabras Clave

- **TRAMA 802.11**
- **SNIFFER**
- **WIRESHARK**
- **ANALIZADOR DE TRÁFICO**

Abstract

In recent decades, with technological advancement and need to communicate to exchange information, people have resorted to the massive use of wireless networks both at the business level, as well as at home; This increase of the wireless networks has made them more susceptible to attacks and that these are detrimental to the performance of the network, as well as to the security of users' information. This project develops an application compatible with the Windows operating system that allows characterizing and displaying 802.11 frames of a wireless network in real time, in a simple and automated way. In order to capture the traffic, chipsets compatible with Windows and with the Acrylic driver were used, which allows the network card to be placed in monitor mode as well as AirPcap NX modules in both single and multi-channel channels and thus obtain information about the wireless protocols. The implementation of the algorithm uses the sniffing technique that allows, in passive attack mode, to capture the traffic generated in local connections, as well as the traffic generated by the connections of other users. The results obtained by capturing the traffic provide management frames, data, control and MAC/IP addresses. They will be analyzed to check the efficiency of the application developed, comparing its results with other software called Wireshark and thus present conclusions about its use, performance and efficiency.

Keywords

- **FRAME 802.11**
- **SNIFFER**
- **WIRESHARK**
- **TRAFFIC ANALYZER**