RESUMEN

En la actualidad existen ataques a las redes de instituciones, bancos, empresas entre otros, las cuales tienen información preciada y personal que es sensible a que personas malintencionadas quieran invadir y robar la misma. El objetivo del presente proyecto es realizar el análisis de la red utilizando la técnica Sniffing mediante la herramienta Open Source Wireshark, para lo cual se siguió una metodología que permite conocer las potencialidades del programa, inspeccionar el sistema a estudiar y realizar las capturas para luego analizar el tráfico real de los paquetes que viajan a través de la red: tiempo de ingreso del paquete al canal, dirección fuente y destino, longitud promedio de paquete, utilización promedio del canal, etc. Para llevar a cabo nuestro propósito se comenzó a capturar datos en la red y así detectar si existen intrusos para tomar medidas pertinentes para evitar la fuga o manipulación de información y mejorar el rendimiento de la red mediante el monitoreo y el análisis del tráfico, se observó que los estudiantes solo ingresan a páginas de consultas y es muy poco probable que en el momento de capturar el tráfico alguna persona esté realizando ataques por lo que se realizaron simulaciones de los mismos como son SYN Flooding, Envenenamiento ARP, ICMP Flooding y DNS Spoofing. Los beneficios que se obtuvo al realizar el proyecto es que se evidencio que los usuarios son vulnerables y pueden ser víctimas de ataques que pueden dejar al usuario sin servicio de internet, redireccionar información que debe llegar a un usuario o al router hacia la computadora del atacante y así modificar información confidencial.

Palabras Claves

WIRESHARK
REDES INSTITUCIONALES
SPOOFING
FLOODING