RESUMEN

La seguridad en las redes de comunicación se ha convertido en un factor de suma importancia debido a la presencia constante de intrusos en la red ya que son elementos que afectan la Calidad de Servicio *(QoS, Quality of Service)* y que se define como un parámetro para establecer el óptimo funcionamiento de la red a través de protocolos establecidos tal como el TCP (*Transmission Control Protocol*). Dicho protocolo está orientado a crear conexiones lógicas entre los nodos o equipos que integran a la red para comunicarse entre ellos a través del flujo de datos.

Debido al crecimiento exponencial de usuarios en el Internet, éste se ha convertido en un medio importante e indispensable para la comunicación puesto que la mayoría de usuarios hacen uso de la red con el fin de efectuar sus operaciones. Esto obliga a los proveedores de Internet a emplear sistemas de seguridad que ofrezcan protección a los clientes para mantener la disponibilidad de los recursos y servicios en la red.

El trabajo reportado en esta tesis tiene como objetivo realizar el diseño y simulación de un sistema de detección de intrusos para redes de comunicaciones utilizando OMNET++. A través de simulaciones se detectarán los ataques o amenazas que afecten el desempeño de los elementos sobre la red diseñada. OMNET++ es una herramienta de simulación para redes de comunicaciones, el cual permite modelar protocolos, sistemas multiprocesadores o redes de telecomunicaciones.

Para realizar el diseño del IDS (*Intruder Detection System*) fueron considerados cinco ataques: DoS (*Denial of Service*), DDoS (*Distributed Denial of Service*), Ping of Death, XSS (*Cross Site Scripting*) y el MiTM (*Man in the Middle*). Los ataques mencionados se emplearon por el desempeño que tienen en un ambiente real siendo amenazas que causan la denegación de servicios a clientes legítimos en una red.

En la simulación se utilizaron estos ataques como las principales amenazas en la red diseñada afectando el ancho de banda de ciertos elementos, ya que es un recurso importante para la comunicación entre ellos. Posteriormente se obtuvieron resultados que muestran el daño provocado en las "víctimas" por los ataques utilizados.

Para la simulación inicialmente se emplearon como parámetros el ancho de banda de los elementos en la red, el cual fue de 250 Mbps (*Megabits por segundo*) para los servidores y 80 Mbps para las PCs. Estos valores fueron establecidos en función a la generación de tráfico de paquetes y ataques sobre la red, la cual es de 250 ms (*milisegundos*) para el tráfico de ataques y 100 ms para datos que no afectan como ataques a los elementos de la red considerados, tal como el correo eléctrónico o simples paquetes de texto.

Finalmente los resultados obtenidos representan el desempeño del IDS diseñado ante los ataques utilizados. Durante su detección se presentaron los falsos negativos siendo tomados como parámetros para mostrar la eficiencia dicho sistema. En la ejecución de la simulación se programaron ciertos ataques que los IDS pueden detectar de manera que se pudiera observar el paso de algunos de estos ataques a través de los sistemas de seguridad y afectar a ciertas víctimas en el escenario simulado, representando así a los falsos negativos.

En la simulación presentada en este trabajo de tesis, la eficiencia del sistema de seguridad compuesto por los IDS en la red se basó en el registro de los ataques que afectaron a ciertas víctimas y los que fueron detectados por el mismo sistema durante la simulación, siendo de un 93 % efectivo. Cabe recordar que en la programación de la simulación este desempeño puede variar de acuerdo a la activación para la detección de los ataques en los IDS.