CAPITULO 7

CONCLUSIONES Y TRABAJO A FUTURO

Con este capítulo se concluye el trabajo de tesis realizado además de presentar las conclusiones en relación al objetivo propuesto y a los resultados que se obtuvieron en las simulaciones realizadas con OMNET++. Por otra parte se presenta la propuesta para trabajos a futuro, tomando este trabajo de tesis como una base para el desarrollo del mismo.

7.1 Conclusiones

Actualmente el Internet es el medio de comunicación por el cual transita toda clase de información. Debido a que existe información que requiere la mayor privacidad posible, tales como las transferencias bancarias o simplemente información de correo electrónico, el administrador de red crea sistemas de seguridad en la red y el cual es un servicio que garantiza la transferencia segura al usuario final del a información de forma lo más transparente posible. Ejemplo de este tipo de planteamiento es el establecimiento de un nivel de transporte seguro tal como *MTA (Mails Transport Agents)* *[9]* el cual ofrece un servicio de mensajería segura.

Para conocer y subsanar las vulnerabilidades de un sistema es necesario profundizar en las características de los ataques a los que puede ser sometido. No obstante, muchos administradores únicamente logran alcanzar los límites de sus sistemas de forma casual, por lo que para la detección oportuna de estos ataques en redes, se requiere de estrategias que anticipen a los demás elementos de seguridad en la red tales como los *IDS* y que al momento de ser detectado algún ataque o intento del mismo, el Sistema de Detección de Intrusos permita monitorear, identificar y determinar los riesgos existentes en las redes informáticas.

Dado el objetivo de realizar el diseño de un *IDS* y evaluar su desempeño en una red de comunicaciones, se empleó como herramienta OMNET++ el cual es un programa útil para la simulación de redes de comunicaciones y que con el uso de sus herramientas de programación, simulación y graficación, este programa brinda resultados que pueden llegar a ser similares a los obtenidos en una red de comunicaciones real, ya que cuenta con la interfaz

GUI la cual permite visualizar el comportamiento programado de una red por medio de las disposiciones gráficas con las que cuenta el programa.

Con este programa se mostró el funcionamiento de una red de comunicaciones y la vulnerabilidad de los elementos de la red, al haber la presencia de generadores de ataques tanto externos como internos de la misma. Se demostró la eficiencia de un sistema de seguridad compuesto por *IDS* diseñados, ubicados en puntos estratégicos, y cuya eficiencia fue medida en base a los falsos negativos y positivos, y de los ataques detectados por el mismo sistema de seguridad.

El IDS implementado en la simulación es un sistema diseñado en función de reglas para la detección de amenazas y basado en Red, ya que se monitorean los paquetes o datos que transitan en la red lo que le permite alertar de manera oportuna la detección de ataques que pueden afectar a los elementos o computadoras que componen a la red.

En cuanto a la comparación del IDS diseñado con otros sistemas de seguridad comerciales se puede comentar que nuestro sistema para la detección de intrusos puede ser implementado en distintas tasas de procesamiento de tráfico (en Mbps), pues como se presenta en la simulación esta tasa es de 50 Mbps y que posteriormente puede ser variable.

Por otra parte se pueden establecer las características de los medios de comunicación conectados hacia los IDS, es decir, ya sea a través de fibra óptica o por cable de red variando la tasa de transferencia o el BW del medio.

En cuanto a su desempeño, el IDS diseñado realiza la oportuna detección de los ataques a través del análisis de paquetes lo que le permite detectar e identificar el tipo de intrusión que transitó por el sistema de seguridad por lo que el IDS es eficiente y funcional ante las características del funcionamiento de otros equipos comercialmente distribuidos.

7.2 Trabajo a Futuro

Dadas las características presentadas en el diseño del *IDS* y los resultados obtenidos, como a trabajo a futuro se propone que el diseño propuesto para este sistema de seguridad, sea implementado a través de un *Appliance o dispositivo integrado de seguridad*, los cuales son

elementos robustos que integran tanto el hardware de conexión como un sólido sistema operativo, sobre el cual se colocan diversos bloques de seguridad *[19]*, como por ejemplo el antivirus, anti spam, *VPN (Virtual Private Network)*. Para el desempeño del *IDS* en esta implementación se tendría un equipo primario de mantenimiento de seguridad con un panel que cuente con sensores y controles de advertencia en función del *IDS* para una detección preventiva de posibles amenazas *[19]*.

Por otra parte la implementación del *IDS* se puede llevar acabo en un *FPGA* instalado en una red real y que por consiguiente se tendría un sistema para detección de intrusos sin la necesidad de recurrir a equipos que requieran un mayor gasto, tales como los *Appliances.* En cuanto al nivel software y diseño del mismo *IDS* se puede incrementar la eficiencia, realizando la respectiva programación en la que se incluyan otras cualidades que distinguen a los ataques, ya sean los presentados en este trabajo de tesis u otros lo que permitiría hallar nuevos patrones que hagan más eficiente al sistema.