CAPITULO 1

INTRODUCCIÓN

La seguridad en las redes de comunicaciones se ha convertido en un aspecto de importancia para los proveedores del Internet y para los clientes debido a la prioridad que ha tomado la información que viaja a través de este medio, surgiendo así la necesidad de crear sistemas que permitan asegurar al mismo tiempo la transferencia y privacidad de los datos desde su origen hasta el destino deseado, siendo requerida la implementación de los sistemas para detección de intrusos los cuales son elementos imprescindibles para la seguridad en una red de comunicaciones.

Por cuestiones prácticas y funcionales la eficiencia de los sistemas para detección de intrusos (*IDS, Intruder Detection System*) debe ser medida y analizada en un entorno real debido a los cambios constantes que se presentan. Dichos cambios son consecuencia de la constante generación de nuevos ataques o intrusiones que afectan el desempeño adecuado de los elementos que conforman a la red.

La detección de intrusos y ataques es el proceso de monitorear y detectar eventos que ocurren en una red, para analizarlos en búsqueda posibles de problemas que afecten a la seguridad, lo que permite el surgimiento de propuestas que intentan dar solución a este enfoque.

Con el objetivo de poder conocer el comportamiento y la eficiencia de estos sistemas de seguridad se emplean programas o software, tales como los simuladores para redes de comunicaciones en los cuales se realiza el diseño de una red y que una vez establecidos el tráfico y los intrusos sobre la misma se puede observar el comportamiento aproximado de estos sistemas para su implementación en un ambiente real.

1.1 Antecedentes

Cuando los usuarios se conectan a la red y logran comunicarse con el mundo exterior a través de ella, dicha red interactúa con el sistema del usuario y puesto que sobre ella puede viajar todo tipo de tráfico se requiere de la implementación de sistemas o barreras de protección que

ofrezcan seguridad al sistema de los usuarios, ya que si algún intruso intentara tener acceso a la red dichas barreras no permitiría un progreso de la intrusión o ataque.

En términos generales los sistemas para detección de intrusos realizan el análisis del tráfico con el propósito de evitar el acceso de atacantes que afecten el desempeño de los equipos usuarios sobre la red. Cabe recordar que el acceso o conexión a través de la red se debe al intercambio de la información a través del protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol*) el cual es un conjunto de protocolos de comunicaciones de datos y que permiten transportar la información de un equipo a otro.

Los ataques o intrusiones en las redes de comunicaciones ocurren rutinariamente y se han convertido en el mayor problema para el óptimo funcionamiento de la red a escala mundial, sin embargo cómo detectar a los intrusos sobre una red incluye el diseño apropiado de un IDS evaluando las ventajas y desventajas entre los factores riesgo y costo *[4]*.

Los ataques generados por intrusos sobre una red pueden dejar inoperativos los recursos de algún sistema y causar por lo tanto pérdidas económicas, además de exponer a dichos intrusos datos que pueden ser privados por medio de la recopilación de información sobre posibles puertos de acceso hacia redes que el atacante desee afectar *[2]*.

Dada la complejidad y variedad en el tráfico sobre la red surgen como sistemas de seguridad primarios los Firewall ya que funcionan como filtros evitando que los usuarios de Internet no autorizados tengan acceso a redes privadas y los cuales son efectivos empleando las firmas o códigos de reconocimiento ante usuarios e intrusos en la red *[1].*

Los IDS o Sistemas para Detección de Intrusos son sistemas utilizados para prevenir y detectar ataques hacia los equipos o nodos de interés en una red. Este funcionamiento se logra por medio de la recopilación de datos de un conjunto de sistemas los cuales han registrado las características de ataques anteriormente detectados y registrados, por lo que dicha información obtenida sugiere los posibles problemas de seguridad con los que otros sistemas se pueden enfrentar *[2]*.

Dado esto en algunos casos se logra obtener una respuesta en tiempo real a las violaciones o ataques sobre la red. A continuación se presentan las funciones esenciales de un IDS:

- Monitoreo y Análisis del usuario y actividad en la red.
- Detección de los sistemas de configuración y posibles vulnerabilidades.
- Reconocimiento de los patrones que reflejen ataques sobre el sistema.
- Análisis estadístico de patrones de actividad anormal en la red *[3]*.

La combinación de estas características permiten a los controladores o administradores de los servicios en la red un monitoreo sobre los sistemas incrementando prácticamente la seguridad sobre la misma.

Cabe mencionar que es de suma importancia considerar los niveles de seguridad de los sistemas que contrarrestan el progreso de un ataque, es por eso que se ha establecido un comparativo por medio de estándares de seguridad de computadoras desarrollado por el Departamento de Defensa de los Estados Unidos y cuyo criterio de evaluación de seguridad es usado con el propósito de proteger los sistemas dentro de la red *[5]*.

A continuación se presentan los niveles que describen los diferentes tipos de seguridad física, autenticación del usuario y confiabilidad del software tanto del sistema operativo como de las aplicaciones (véase la Figura 1.1) *[5]*.

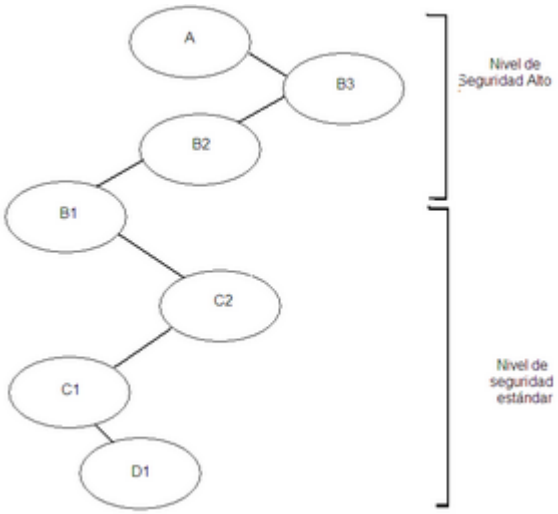

Figura 1.1: Niveles de seguridad para la protección de la red.

Nivel A

El nivel A o *nivel de diseño verificado* es el nivel más elevado de seguridad. Cuenta con un estricto diseño, control y verificación en su estructura. Se incluyen todos los componentes de los niveles inferiores de seguridad. Se cuenta con una *distribución confiable,* lo que significa que el hardware y el software han estado protegidos durante su expedición para evitar violaciones a los sistemas de seguridad *[5]*.

Nivel B1

El nivel B1 o mejor conocido como *protección de seguridad etiquetada,* soporta una seguridad multinivel y en el que se parte de un principio en el que un objeto bajo control de acceso obligatorio no puede aceptar cambios en los permisos hechos por el dueño del archivo, de acuerdo a Siyan Karajit, en su libro Internet y Seguridad en Redes *[5]*.

Nivel B2

Conocido como *protección estructurada*. Cada objeto que navegue en la red debe ser etiquetado a través de un *Tag* (*Etiqueta de información del paquete*), mientras que a nivel de hardware los dispositivos como discos duros, cintas o terminales podrán tener asignado un nivel sencillo o múltiple de seguridad *[5]*.

Nivel B3

El nivel B3 o *nivel de dominios de seguridad* refuerza los dominios del hardware al realizar su instalación. Un hardware de administración de memoria se utiliza para proteger el dominio de seguridad de un acceso no autorizado. Dicho nivel requiere que la terminal del usuario se conecte al sistema por medio de una ruta de acceso *[5]*.

Nivel C1

El nivel C se compone de dos subniveles de seguridad: C1 y C2. El nivel C1 o mejor conocido como *sistema de protección de seguridad discrecional* describe la eficiencia en un sistema típico UNIX y en el que existe cierto nivel de seguridad en el hardware. Los usuarios se identifican con el sistema por medio de un nombre de registro y una contraseña y así determinar los derechos de acceso del usuario. Dichos derechos son permisos para archivos y directorios *[5]*.

Nivel C2

Incluye características adicionales de seguridad para crear un medio de acceso controlado que tiene la capacidad de reforzar la restricción a los usuarios en la ejecución de algunos comandos o el acceso a archivos que requieren autorización especial. Por lo que se crea un registro de auditoría para cada evento en el sistema y que al mantener los eventos relacionados con la seguridad sólo ciertos usuarios pueden hacer manejo del sistema *[5]*.

Nivel D1

En cuanto a los niveles de seguridad es el más elemental, dado este estándar se demuestra que un sistema no es confiable puesto que no hay protección disponible para el hardware y no hay autenticación con respecto a los usuarios. Se carece de un sistema definido para determinar entre un usuario normal y un intruso *[5]*.

Una vez establecido el tema a exponer en éste proyecto de tesis se tienen como antecedentes los siguientes trabajos: *Seguridad en redes inalámbricas IEEE 802.11 (WLAN, Wireless Local Area Network) con WEP (Wired Equivalent Privacy) mejorado, simulado en MATLAB,* por Jibran De La Rosa Ramos, de la Universidad de las Américas Puebla, el cual se basa en el estándar IEEE 802.11 y que empleando redes Ethernet o LAN se incluye el protocolo de seguridad WEP para ofrecer seguridad en una red, en el que a través del WEP busca establecer una protección encriptando los datos que circulan por la WLAN protegiendo la vulnerabilidad del enlace inalámbrico *[7].*

El siguiente trabajo realizado por Carlos Alberto Oropeza Clavel y que tiene por título *Modelado y Simulación de un Sistema de Detección de Intrusos Utilizando Redes Neuronales Recurrentes,* también de la Universidad de las Américas Puebla es un trabajo de tesis en el que se emplearon las redes neuronales como el medio de comunicación para la implementación del IDS diseñado, además de que la red neuronal debe ser capaz de actualizarse en tiempo real para que el IDS surtiera efecto ante un ataque *[8]*.

Network Intrusion Simulation Using OPNET es un trabajo realizado por Razak Shabana y Zhou Mian de la escuela de Ingeniería Eléctrica y Computación de la Universidad de Orlando, Fl, *[11]*. En este trabajo se presenta la simulación de intrusos en una red de comunicaciones para posteriormente realizar el diseño de un IDS en base al tráfico y ataques

generados en la red tal como el DoSnuke, un ataque que provoca la denegación de servicio afectando el ancho de banda de la víctima sobre el mismo programa simulador.

1.2 Planteamiento del Problema

Las redes de comunicaciones son sistemas en los cuales existe el intercambio de información de un nodo o equipo a otro a través de recursos y protocolos establecidos mencionados anteriormente, siendo en ocasiones afectados por la presencia de intrusos que generan ataques alterando el desempeño óptimo de la red ya que existen equipos que se conectan a través de ella sin estar protegidos ante las amenazas.

Dichos ataques se pueden reflejar en el acceso del intruso hacia archivos confidenciales o causando la denegación del servicio a clientes legítimos para comunicarse con otros puntos en la red. Por otra parte siendo implementados los sistemas para detección de Intrusos se pueden detectar amenazas registradas anteriormente, pero que dada la complejidad del tráfico el mismo sistema puede no estar listo ante ciertas vulnerabilidades siendo un enfoque de prioridad la actualización de los sistemas.

Tal es la demanda de servicio que actualmente tiene el Internet que si existiera alguna incidencia en él probablemente muchos de los sistemas que conforman a la red dejarían de funcionar. En muchos casos estas incidencias se pueden deber a fallos en el propio equipamiento pero por otra parte son provocados por la falta de seguridad en la misma red y en el que la confianza o el desconocimiento de los usuarios pueden provocar la pérdida irremediable de información. Es por eso que toda red debe contar con un sistema de seguridad constituido por los IDS, IPS (*Intruder Prevention System*) y Firewall, asegurando que sólo los clientes tendrán acceso a los recursos que la misma red ofrezca manteniendo el correcto desempeño y funcionamiento de los sistemas que la conforman.

1.3 Objetivo de la Tesis

El planteamiento de este trabajo de tesis se basa en el diseño y la simulación de un sistema para la detección de intrusos en redes de comunicaciones utilizando OMNET + +. OMNET++

es un programa para simular y analizar redes de comunicaciones. Con el objetivo establecido se hará el diseño de una red LAN en la cual se conectarán generadores de ataques o intrusos, uno proveniente de una red externa y el segundo dentro de la red generando ataques de forma aleatoria sobre los elementos en la red.

Durante la simulación se considerará como estudio el monitoreo y análisis del tráfico en la red en un medio sin ataques y con ataques. Dados los datos de la simulación se tomarán en cuenta los patrones de actividad en ambos casos con el objetivo de diseñar un IDS que detecte y registre los ataques presentes en el tráfico. Una vez diseñado el IDS, el sistema realizará un monitoreo del tráfico que pase a través de los sistemas colocados sobre la red a fin de identificar y detectar los ataques de manera oportuna a través del análisis de gráficas que reproduzcan los valores que se desean conocer.

1.4 Organización de la Tesis

El trabajo reportado en esta tesis se organiza en 7 capítulos y dos apéndices.

Capítulo 2. Sistemas para Detección de Intrusos: En este capítulo se explica la importancia de los sistemas de seguridad que se emplean para las redes de comunicaciones tales como los IDS, los Firewall e IPS. También se exponen el funcionamiento y la jerarquía de seguridad que se debe seguir para preservar una transferencia de datos que asegure la privacidad y llegada de la información al destino deseado.

Capítulo 3. OMNET++: Se describe el programa para la simulación del IDS en una red de comunicaciones. Se presentan los elementos de simulación y el ambiente en el que se puede desarrollar y ejecutar la simulación para redes de comunicaciones.

Capítulo 4. Diseño del IDS: Se describe el diseño del IDS presentado para este trabajo de tesis explicando las consideraciones que se tomaron para realizar el diseño del mismo sistema tales como los ataques que se emplearon para la simulación y la jerarquía de seguridad que debe seguir el sistema simulado para tener una eficiencia óptima.

Capítulo 5. Implementación del IDS en OMNET++: En este capítulo se describe la implementación del IDS diseñado, con el propósito de obtener resultados que permitan medir su desempeño y eficiencia en base a los ataques empleados para la simulación utilizando OMNET++.

Capítulo 6. Pruebas y Resultados: Una vez concluida la programación y las simulaciones, OMNET++ brinda al usuario datos acerca de ciertos eventos ocurridos en la red durante la simulación. Con base en estos datos se analiza el comportamiento que se tuvo en la red para así comparar el resultado obtenido por cada esquema de ataque simulado y posteriormente comprobar la efectividad del diseño para el IDS. Se exponen los ataques que se utilizaron para la simulación ofreciendo al usuario un resultado que le permita comprender de manera analítica el comportamiento de una red en el enfoque de seguridad.

Capítulo 7. Conclusiones y Trabajo a Futuro: Finalizados la simulación y el análisis de la red con sus respectivos datos, se concluye este trabajo de tesis presentando trabajos a futuro para realizar con base en los resultados obtenidos.

Apéndice A: Contiene en un CD el código del diseño del IDS, en base a la plataforma de programación C++.

Apéndice B: Contiene la Implementación de los ataques en OMNET++ a través de una breve presentación del código empleado, mostrando el desempeño de los ataques utilizados para llevar acabo la simulación.