CAPÍTULO 2: SISTEMAS DE DETECCIÓN DE INTRUSOS

En este capítulo se definen los sistemas de detección de intrusos y su relación con los ataques basados en el protocolo HTTP, así como los tipos de ataques posibles a redes de computadoras y los principales modelos de IDS para dar un contexto apropiado al desarrollo del programa basado en redes neuronales.

2.1 INTRODUCCIÓN

La seguridad en Internet se ha convertido en un tema muy importante para todos aquellos que dependen de los servicios de esta red de redes para realizar actividades personales y empresariales. La realidad de los ataques a sistemas de cómputo interconectados con el fin de obtener, suprimir o modificar información valiosa son cada vez más frecuentes y por consiguiente los sistemas de defensa contra todas estas intrusiones han evolucionado para enfrentar estos nuevos retos en términos de seguridad[8].

Todos los equipos de cómputo están equipados ya con *software* antivirus sin el cual serían blancos fáciles para programas dañinos que ingresan al equipo a través de la red a la que está conectado. Adicionalmente, una barrera de seguridad importante comprende los *firewalls*, conocidos filtros que impiden que equipos externos se conecten directamente al equipo *host* debido al riesgo que esto implica. Sin embargo, estos métodos de protección no son suficientes muchas veces, en especial enfocándonos en el protocolo HTTP y sus implicaciones. Los tipos de ataques que pueden sufrir los nodos de una red a través de este protocolo son muy variados y es por eso que se necesitan sistemas especializados para evitar estas intrusiones: los IDS [11].

Desde este punto de vista, los IDS tienen como principal función el identificar que un ataque se está realizando al equipo y alertar a otros sistemas del mismo para que

tomen una medida correctiva o emprendan un curso de acción que minimice el daño causado y al mismo tiempo impida que otros ataques de la misma índole tengan éxito en un futuro. Los IDS no están limitados a funcionar detrás del *firewall* como elementos individuales: múltiples IDS localizados en diferentes partes de la red y en las subredes correspondientes pueden funcionar de manera coordinada para alertarse entre sí en caso de que uno de ellos haya identificado un ataque; con esto la efectividad del sistema de protección completo se incrementa significativamente [12].

2.2 SISTEMAS HID Y SISTEMAS NID

Dentro de la evolución de los sistemas de detección de intrusos han existido dos enfoques importantes en términos de estos sistemas: IDS basados en la red e IDS basados en el *host.* Fueron desarrollados de forma cronológica, con el objetivo final de mejorar la calidad del servicio que se le ofrece al cliente y su seguridad.

Los sistemas NID (*Network Intrusion Detection)* se basan en la información misma que se transmite entre *hosts.* Este tipo de sistemas reciben el nombre de *packet-sniffers* porque analizan el contenido de los datos que pasan a través de la red interceptando paquetes de datos a través de protocolos tales como el TCP/IP. [12] Muchos de estos sistemas NID buscan anomalías o comparan el contenido de los paquetes con información previa almacenada en sus bases de datos en caso de que ciertos componentes de éste indiquen comportamiento típico de un intruso. Los sistemas NID son una buena opción para defensas perimetrales de la red, pero no les es posible trabajar en sistemas de redes de alta velocidad (más allá de 100Mbps) y redes encriptadas [11].

Los sistemas HID, por otro lado tienen la función de buscar y responder a ataques detectados en un servidor. Para estos sistemas no es importante qué información

se transmita por la red, sino qué sucede con un *host* en particular. Sus funciones incluyen análisis estadístico de datos, recopilación de evidencia, control de acceso y otros adicionales a las funciones básicas de todos ellos. Por su naturaleza, los sistemas HID son mucho mejores para asegurar el que no haya ataques de intrusos *dentro* de las redes mismas. Un ejemplo muy claro de esto son los empleados desleales que utilizan los privilegios de los que gozan dentro de la empresa en la que trabajan para invadir el sistema principal y modificar u obtener información confidencial y potencialmente desastrosa para el futuro de la compañía.

Hay otros tipos de sistemas desarrollados recientemente, como los sistemas híbridos y los sistemas NNID (*Network-Node Intrusion Detection)* que son una mejora de los sistemas NID. Los dos tipos de sistemas base, sin embargo, están bien adaptados a las necesidades de los administradores de redes y sus funciones son complementarias más que opuestas [11].

2.3 CATEGORÍAS DE ATAQUES BASADOS EN HTTP

Como ya se ha mencionado, los ataques basados en HTTP son muy variados. Existen muchas formas de alterar, borrar o copiar información valiosa de otros equipos de cómputo aprovechando las ventanas de oportunidad que ofrece dicho protocolo. Los ataques que se han considerado en esta tesis y en los cuales se basó el IDS desarrollado, sin embargo, son cuatro: ataques de *Cross-Site Scripting* (XSS), *Path*, *Structured Query Language (SQL),* y *Code Injection.*

El primer tipo de ataque estudiado y clasificado por el IDS desarrollado en esta tesis es el ataque XSS. En los primeros años de desarrollo de los navegadores de Internet, se descubrió que ciertas características de los mismos permitían interacción entre objetos y páginas del mismo navegador independientemente de tener el mismo

origen o no, siempre y cuando se introdujera cierto código en el navegador que lo hiciera posible. Como medida preventiva a esta ventana a posibles ataques se desarrolló la política del 'mismo origen', en el que dos sitios o ventanas de un navegador pueden interactuar sólo si provienen de la misma fuente.

Desafortunadamente, aún con esta política hay muchas formas posibles de realizar ataques a redes de computadoras. Existen tres categorías principales de ataques XSS: Tipo 0, Tipo 1 y Tipo 2; también conocidos como XSS local, no persistente y persistente respectivamente. En el XSS local, si un usuario ingresa un URL (*Uniform Resource Locator)* que tenga código JavaScript capaz de acceder a una página HTML vulnerable instalada en el equipo, el intruso puede acceder a esta misma página con los privilegios de ingreso del usuario. Esto tiene la inevitable consecuencia de que, si el equipo víctima del ataque contaba con privilegios altos dentro de una organización, el intruso tenga acceso a todos aquellos archivos importantes o sesiones privadas a los que el usuario original tenía acceso directo por sí mismo [12].

A diferencia de este tipo de ataque, el XSS no persistente permite que un intruso obtenga información confidencial *(username, password)* del usuario si éste abre un correo electrónico del atacante mientras está registrado en el sitio de interés. Para lograrlo se necesita, evidentemente, un poco de lo que es conocido como ingeniería social: las técnicas y métodos necesarios para lograr que personas desconocidas exhiban patrones de comportamiento que cumplan con ciertos parámetros deseables. Los intrusos pueden mandar mensajes de correo electrónico cuidadosamente estructurados para lograr este propósito.

El último tipo de ataque es quizá el más peligroso por su capacidad de diseminarse rápidamente. En los foros en línea, un intruso puede ingresar un mensaje con código corrupto que, al ser visitado por otros usuarios, obtenga todas las *cookies* y

otros datos de autenticación de estos usuarios, permitiendo al intruso utilizarlos para su conveniencia. Un atentando masivo de esta naturaleza podría ocasionar el colapso de bases de datos enteras pertenecientes a muchas personas diferentes, y si por casualidad esos datos proporcionan acceso a información confidencial y valiosa es entonces posible para el intruso realizar cualquier tipo de acciones deshonestas basado en esta información falsa, ya sea para borrar datos u obtener otro tipo de información [8].

El segundo tipo de ataques basados en HTTP se refiere a la modificación de *path.* En este caso, los *paths* o direcciones relativas o absolutos dentro de un equipo pueden ser vistos y modificados por el intruso a la red mediante código diseñado para este fin. De esta manera, los directorios y archivos individuales del usuario se ven en un estado de vulnerabilidad que origina su posible alteración por parte de la persona que ha logrado introducirse a la red.

Los privilegios de acceso son evidentemente requeridos para que una modificación de *path* tenga éxito; pero el atacante puede obtener este tipo de privilegios valiéndose de otro método complementario de código que le permita sobrepasar las barreras impuestas a usuarios externos. Si un ataque de este tipo no es detectado a tiempo, directorios enteros de una computadora o un servidor estarán a disposición de quien haya logrado infiltrar el sistema de seguridad para propósitos deshonestos. Este tipo de ataques por lo general se usan en conjunción con otros para tener mayores beneficios para el intruso; por ejemplo, mediante XSS tipo 1 se pueden obtener las credenciales de autenticación de usuario y una vez validado el ingreso al equipo víctima del ataque, tendrá lugar la modificación de *path* obstruyendo o desviando el flujo normal de información desde su fuente hasta su destino final [9].

Los ataques basados en SQL están enfocados en las bases de datos almacenadas en las computadoras destino. El lenguaje estructurado en cuestión posee comandos de

manipulación de datos, control de transacciones y definición de datos que se usan dentro de la operación normal de las bases de datos, pero un intruso puede hacer uso de estas herramientas para otros propósitos. Si una base de datos es vulnerable al ataque de un intruso utilizando SQL, los contenidos de las bases de datos podrán ser vistos, proporcionando información potencialmente confidencial a terceros. Si el intruso está interesado en modificar los contenidos de dicha base o hasta borrarlos, también es posible dependiendo del enfoque de su código.

Debido a que el SQL es ya considerado un estándar por el Instituto de Estándares Nacionales Americanos (ANSI) y por la Organización Internacional para la Estandarización (OSI), un gran número de usuarios a nivel mundial lo utilizan para el manejo y administración de sus bases de datos y es por eso que es un tipo de ataque importante contra el cual protegerse [9]. Las consecuencias de este tipo de ataques podrían llegar a ser desastrosas si la víctima del intruso fuera un sitio de Internet importante o encargado de almacenar y administrar información de muchos otros usuarios. En ese caso, una falla total del sistema podría ocasionar que se borre el sitio mismo y se pierdan todos los datos que ahí se guardaban. Para ciertas comunidades virtuales, en especial en el ramo empresarial, esto significaría una catástrofe financiera completa.

El último tipo de ataques es conocido como ataque de inyección de código. Este tipo de ataques se aprovechan de ciertas suposiciones que se hacen al crear programas, sitios de Internet o navegadores acerca de los datos que ingresarán al mismo. Los errores más comunes tienen que ver con el tipo de caracteres, la longitud y veracidad de los mismos que serán proporcionados por los usuarios (por ejemplo, los mensajes en un foro en línea). Un intruso puede utilizar estas debilidades para introducir código propio

al sistema, el cual puede tener efectos diversos dependiendo del tipo de objetivo que tenga en mente en ese momento.

Las consecuencias más importantes de este tipo de ataques son las siguientes: instalar *malware* (programas dañinos) en una computadora o en un servidor que ejecutará el código del atacante al visitar sitios específicos; incremento de los privilegios de acceso a directorios locales y raíz; y también modificar de manera aleatoria los contenidos de los archivos de datos del equipo víctima con el fin de corromper o destruir la información que ahí está almacenada [11] .

La naturaleza dinámica de los mecanismos de inyección de código los hace el tipo de intrusión a una red de computadoras más difícil de combatir, ya que gran parte de la vulnerabilidad de un *end system* a dichos ataques es la programación previa realizada durante la creación del sistema mismo. Los errores de código que creen ventanas para que otro usuario introduzca cadenas de caracteres cuyo propósito es alterar el desempeño normal del flujo de información se convierte en serios problemas en las barreras de seguridad que, al no haber sido planeados, necesitan de un sistema de detección de intrusos que complemente las funciones de los demás sistemas de seguridad.

2.4 RESUMEN

Como puede verse, las redes de computadoras tienen muchas áreas vulnerables que un intruso puede aprovechar si así lo desea. Los tipos de ataques son diversos y es imposible estar protegido contra todos ellos al mismo tiempo. Es por eso que, en adición a todos los sistemas que ya existen como el *software* antivirus y los *firewalls*, es necesario utilizar IDS para asegurar que un sistema no será atacado o que si lo es al menos se identificará la trasgresión para evitar que suceda de nuevo. Los atacantes

siempre están pensando y desarrollando nuevas formas de encontrar fallas en los sistemas de seguridad existentes, y aquellos basados en HTTP requieren de especial atención debido a que la conectividad que ofrecen dan a los intrusos más oportunidades de acceder a otros equipos a través de la red.

Las consecuencias de los ataques basados en XSS, SQL, *path* e inyección de código van desde el borrar una página de Internet hasta un posible fraude bancario si cierta información confidencial cae en las manos equivocadas. Los IDS deben ser entonces adaptables y versátiles para enfrentar estos retos, y así permitir el seguro intercambio de información entre equipos y servidores.