INTRODUCCIÓN

El desarrollo y evolución de las comunicaciones en las últimas décadas han hecho más accesibles los sistemas informáticos, las redes de computadoras son ahora una herramienta necesaria para el desarrollo de las actividades de grandes empresas, gran parte del comercio se realiza mediante el uso de redes sofisticadas con grandes bases de datos, la información se genera de manera digital, al igual que su almacenamiento.

Las redes de computadoras comenzaron a implementarse a finales de los años 70 con el fin de compartir herramientas, recursos y datos para los usuarios. En aquél entonces la única preocupación que tenían las empresas era que alguien obtuviese acceso a una computadora o introdujera algún virus al sistema. El resguardo físico mediante personal o alarmas de seguridad era el único medio de defensa por el que tenían que preocuparse. Con la aparición de Internet y su enorme popularidad y crecimiento las cosas han cambiado, la Internet es una red de redes que proporciona múltiples y muy variados servicios y permite la comunicación a grandes distancias, el intercambio de datos, el comercio electrónico, entre otras actividades importantes. Sin embargo, así como Internet representa una serie de ventajas y servicios que una empresa puede aprovechar, también representa un riesgo ya que no se cuenta con una autoridad rectora que vigile el tipo de actividades se pueden realizar y que restringa los actos que puedan convertirse en una amenaza a las redes que se conectan a Internet.

Por otra parte, Internet no habría crecido de tal manera sin programas de libre distribución o *software libre*. Este concepto en el cual se pone a disposición de la comunidad programas y que a su vez permite la mejora de los mismos, debido a que también se proporciona el código fuente, ha permitido un enorme crecimiento de Internet.

Programas como SendMail y el popular servidor *Apache* Web, han servido de plataforma para la expansión y crecimiento de una red como Internet que sigue ofreciendo posibilidades ilimitadas gracias a programadores anónimos que desarrollan y mejoran los programas que se ejecutan en Internet.

Esta ventaja que nos ofrece el *software libre*, el gran crecimiento de programas de este tipo, y la facilidad con que accedemos a él, también significa un riesgo, pues cualquier persona puede tener acceso a programas y ejecutar ciertas tareas que constituyen amenazas a la seguridad de las redes. En Internet se pueden obtener de forma gratuita, programas que constituyen una amenaza para la seguridad de una red, entre estos, programas que dan acceso a la redes, hacen la negación de servicios, programas que tratan de obtener contraseñas de las cuentas de usuarios, programas que escalan privilegios y permiten el robo o la modificación de datos.

Por estas razones, la preocupación por mantener una red segura es mucho más grande ya que existen amenazas dentro y fuera de la red. Ahora un sistema puede ver vulnerada su seguridad por un ataque hecho desde miles de kilómetros de distancia por un individuo protegido por el anonimato y sin dejar rastro del ataque perpetuado. Aunque también existe la amenaza de un ataque a la seguridad perpetuado desde dentro del sistema, hecho por un administrador o por un usuario descuidado. El simple hecho de darle click a un archivo ejecutable puede vulnerar la seguridad de un sistema mal configurado.

Se ha convertido en práctica frecuente el ataque a empresas con redes de cualquier tamaño, no sólo las grandes redes de empresas. El objetivo ha cambiado y no sólo se centra en obtener información del sistema o datos importantes, sino que ahora utilizan los recursos de la red, como el ancho de banda, para perpetrar ataques desde nuestra red sin ser detectados. Las herramientas para hacer una intrusión en una red están disponibles en Internet y aprovechar cualquier vulnerabilidad de un sistema que por descuido o por desconocimiento del administrador, puedan ser explotadas.

Un ataque puede ser obra de un experto programador o de un principiante sin grandes conocimientos de programación pero con una herramienta poderosa, es por esto que no se debe correr ningún riesgo al momento de asegurar nuestro sistema.

A pesar de que Internet puede constituir una puerta de entrada a sujetos malintencionados a nuestra red, también es nuestra forma de comunicarnos hacia el exterior y brindar servicios a nuestros usuarios, y sin duda representa una mayor ventaja esto último, por lo que prescindir de una red conectada a Internet sólo porque puede significar una amenaza de seguridad es demasiado severo. Es mejor implementar medidas que nos permitan tener la suficiente certeza de que nuestro sistema está a salvo de dichas amenazas.

Tener una red de cualquier tipo conectada a Internet requiere de una arquitectura debidamente protegida por políticas de seguridad, una estrategia que nos permita en cada parte de nuestro sistema, controlar, monitorear y supervisar el funcionamiento adecuado de servicios, programas y herramientas. Para asegurar nuestra red es necesario conocer las características de nuestro sistema operativo, que es el primer elemento donde se instrumentan las medidas de seguridad. Además se requiere determinar aquellas herramientas que podemos implementar en nuestro sistema y los servicios que vamos a ofrecer a los usuarios, así como la información trascendental y los puntos débiles de nuestra red.

De esta manera, el administrador de una red deberá establecer criterios en áreas como las cuentas de usuario, el control de acceso, el control de acceso a la red, el cifrado de datos y el tipo de conexiones permitidas, registro, auditoría y control de red y finalmente la detección de intrusos.

Ciertas áreas se desarrollan desde dentro de la red y su control está enfocado a delimitar accesos y el uso de recursos por usuarios del sistema, como el correcto manejo de cuentas de usuarios y control de accesos. Otras áreas están enfocadas a la interacción entre nuestra red y redes externas, como el control de acceso a la red y el cifrado de datos. Entre otros, la implementación de un *firewall* entra en esta etapa.

Un *firewall* es un elemento fundamental para la protección del acceso a una red; se trata de una aplicación conectada entre Internet y la red a proteger, que tiene implementadas las directivas de seguridad, entre éstas, los servicios accesibles a nuestras terminales, los servicios que se ofrecen hacia fuera de la red, conexiones remotas y los programas que se van a ejecutar localmente. Estas decisiones se refieren principalmente al control de acceso y el uso autenticado de los servicios y programas en la red.

Un *firewall* es una herramienta importante y necesaria para filtrar y analizar paquetes de varios protocolos y realizar evaluaciones condicionales, si una petición se ajusta a una directiva predefinida, se realiza cierta acción, permitir el acceso o ejecución de cierto servicio o el bloqueo de protocolo y contenido. Un *firewall* bien implementado representa una puerta de control efectiva para la autenticación y correcto uso de sesiones en nuestra red, así como un obstáculo contra usuarios no deseados y software malicioso.

Un *firewall* puede mantener fuera de la red amenazas específicas, pero aún cuando están bien configurados, dejan algún tráfico de aplicación que puede ser peligroso. Si algún ataque logra entrar a través de él, se requiere de otro dispositivo de seguridad complementario que proteja al sistema desde el interior, que detecte a los intrusos que incursionan en la red. La detección de intrusiones es la práctica de utilizar herramientas inteligentes y automáticas para detectar intentos de intrusión, estas herramientas se llaman Sistemas de Detección de Intrusos.

Una vez que se traspasa la barrera del *firewall*, las herramientas implementadas para detectar intrusos se convierten en el último y más importante recurso para defender al sistema desde el interior. Estas herramientas permiten el análisis detallado del tráfico en la red y el comportamiento sospechoso como el escaneo de puertos. No sólo permiten el análisis del tipo de tráfico, sino que, además se revisa el contenido y su comportamiento. Un Sistema de Detección de Intrusos es una herramienta que funciona en forma complementaria con el *firewall*, uniendo dos capacidades distintas, la inteligencia de la detección y el poder de bloqueo del *firewall*.

Para realizar el monitoreo, se requiere de una base de datos actualizada que permita reconocer los ataques más recientes y se necesita un mantenimiento constante. Algunos sistemas emplean técnicas más avanzadas que pretender hacer que el mismo sistema aprenda de un ataque y responda en consecuencia. Pueden actuar de manera preventiva,

escuchando el tráfico en la red y tomando las medidas implementadas para las amenazas detectadas, o de manera reactiva, consultando sus bitácoras y respondiendo en consecuencia.

Los Sistemas de Detección de Intrusos pueden ser pasivos y activos; los pasivos únicamente detectan una posible intrusión, almacenan la información y mandan una señal de alerta al administrador de la red para que él se encargue de tomar acciones contra la intrusión. Por el contrario, los activos o reactivos, son aquellos que ante una amenaza generan algún tipo de respuesta como el cierre de la conexión o la reconfiguración del *firewall* para bloquear el tráfico que proviene de la red atacante.

Snort es un Sistema de Detección de Intrusos basado en red de libre distribución que puede funcionar tanto de manera pasiva como activa; implementa un motor de detección de ataques y barrido de puertos, esto permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos aprovechar alguna vulnerabilidad, análisis de protocolos, entre otros.

Un Sistema de Detección de Intrusos es muy útil para protegernos contra ataques externos y además nos da la ventaja de localizar los ataques y actividades sospechosas de orígenes internos y responder ante ambas situaciones de manera casi inmediata. Aunque se requiere de un conocimiento más a fondo, este tipo de sistemas de detección, resultan fundamentales para cualquier tipo de redes que compartan servicios, recursos e información y tengan un punto de conexión a Internet.

Con base en esto, el objetivo del presente trabajo de tesis es *Crear Un Sistema De Defensa Con Herramientas De Software Libre* que pueda ser utilizado como esquema general básico, para todos aquellos entornos que requieran seguridad en sus redes de datos.

Asi, los objetivos particulares del proyecto son:

- Hacer uso de las herramientas que permitan conocer los puntos vulnerables de una red para controlar el acceso y proteger tanto los servicios como los recursos compartidos de la misma y sentar bases para el estudio de los sistemas de seguridad de las redes.

- Obtener el conocimiento necesario para el correcto uso de las herramientas de seguridad que permiten proteger una red.

- Verificar que el sistema defensa funcione correctamente en un entorno simulado, para ello, se considera que el sistema contendrá:

- Sistema operativo con seguridad reforzada
- Protección de contraseñas
- Escáner de vulnerabilidades
- Escáner de vulnerabilidades web
- Cortafuegos
- Sistema de detección de intrusos

Aunado a esto, considerando que la seguridad de la información es una necesidad de hoy día en todos los sistemas que generan, procesan, almacenan y transmiten información, y que los profesionales del cuidado de ésta deben estar preparados y contar con las habilidades prácticas para cuidar de ella es que adicionalmente se considera también como un objetivo *desarrollar una práctica sobre hardening* (reforzamiento de la seguridad) para el laboratorio de redes y seguridad de la Facultad de Ingeniería a fin de que los futuros Ingenieros en Computación adquieran los conocimientos básicos que les permitan reforzar la seguridad de los sistemas de información.

Para ello el documento se estructura en 6 capítulos. En el primero se describe la historia del *software libre* y de la libre distribución, además se analizan conceptos fundamentales relacionados con las redes de computadoras, los modelos de referencia *OSI* y TCP/IP, protocolos de red y los tipos de amenazas en una red.

El capítulo 2 contiene un análisis de los requerimientos de seguridad de la red que se va a proteger, se enumeran las posibles amenazas y los riesgos que afectan la red, el tipo de diseño que se puede implementar para una mejor protección de la red y los requerimientos de seguridad del servidor.

En el capítulo 3 se hace una descripción de las herramientas que se van a implementar como parte del sistema de defensa de la red, se detalla el tipo de herramienta a utilizar, el alcance de dicha herramienta, las opciones que se pueden implementar con la misma y la parte del sistema que protege.

Para las herramientas que se utilizan en el sistema de defensa se requiere hacer las instalaciones y configuraciones correspondientes, este proceso se describe paso a paso en el capítulo 4, además se realizan las instalaciones de las librerías y software adicional necesario para crear el sistema de defensa de la red y se realizan las configuraciones que permiten un correcto funcionamiento del sistema.

En el capítulo 5 se hace la prueba de los diferentes elementos del sistema de defensa, se detalla el tipo de prueba a realizar, los resultados esperados y las condiciones en que se va a llevar a cabo cada prueba. En este capítulo se obtienen los resultados de los elementos del sistema bajo condiciones simuladas.

El capítulo 6 es una práctica de reforzamiento de la seguridad con Bastille, una herramienta muy eficaz que permite, mediante una interfaz intuitiva, realizar el aseguramiento de los elementos importantes más vulnerables en un sistema operativo tipo Linux. Uno de los objetivos de esta práctica es que el estudiante comprenda la importancia del reforzamiento de la seguridad y que pueda realizarlo mediante el uso de esta herramienta.

Finalmente, en las conclusiones se definen los alcances logrados en este trabajo de acuerdo con los objetivos planteados inicialmente y se analizan los resultados obtenidos en forma general con el uso de herramientas de *software libre* implementadas como un sistema de defensa para una red.

Cabe mencionar que la parte práctica del presente trabajo, esto es, el desarrollo del sistema de defensa se recreó en el Laboratorio de Redes y Seguridad de la Facultad de Ingeniería de la UNAM, con la finalidad de poner en práctica las diferentes herramientas que permitan levantar el sistema de defensa y hacer las pruebas necesarias a fin de que los interesados en poner en práctica el sistema aquí sugerido, como base para resguardar redes de datos, cuenten con la información y consideraciones necesarias que les permitan implementar un sistema de defensa con herramientas de software libre.