CAPÍTULO 2

ANÁLISIS DE REQUERIMIENTOS DE SEGURIDAD DE LA RED

ANÁLISIS DE REQUERIMIENTOS DE SEGURIDAD DE LA RED

En toda red existe la necesidad de proteger la integridad y confidencialidad de la información y el uso de sus activos, para determinar el grado de confianza que se puede depositar en un sistema informático existen criterios y normas de seguridad, pero, si se requiere mejorar el nivel de seguridad que existe en una red, se tiene que realizar una evaluación de seguridad, con lo cuál se puede determinar el estado de un sistema y los cambios que se pueden realizar para mejorar dicho estado. Para realizar una evaluación de seguridad se pueden hacer pruebas de vulnerabilidad que incluyen el análisis de una red y sus políticas y controles de seguridad; pruebas de seguridad, en las que se realizan auditorías de seguridad, escaneo de vulnerabilidades y pruebas de penetración, y finalmente, el reporte de las vulnerabilidades encontradas y las sugerencias para la implementación de mejoras.

A continuación se describe una norma de evaluación reconocida para la evaluación de la seguridad en un sistema informático. El presente trabajo se desarrolla en la parte técnica de dicho proceso de evaluación, que es en sí, la parte práctica en la que se implementan herramientas para el descubrimiento de vulnerabilidades. Cabe mencionar que el proceso de documentación y el descubrimiento de hallazgos y reporte de recomendaciones es también un elemento importante en este tipo de análisis, pero que no se trata a fondo en el presente documento.

2.1 Normas de evaluación reconocidas

Para la evaluación de la seguridad de una red existen diferentes modelos que permiten tener una mayor certeza sobre evaluación, calificación y mejora de la misma, estos modelos permiten cuantificar de alguna manera, los resultados de las acciones emprendidas sobre una red, tanto si es un resultado tangible como si se trata de un intangible. Estándares de evaluación reconocidos como NSA IAM de la agencia de seguridad de Estados Unidos[7], CESG CHECK (Council of Registered Ethical Security Testers) y SPD (Site Data Protection) de Mastercard, nos brindan una metodología estructurada que permite desarrollar la evaluación de seguridad de una manera organizada.

NSA IAM

La metodología de evaluación de la red NSA IAM (National Security Agency -Information Security-Assessment Methodology) es un método detallado y sistemático para la evaluación de vulnerabilidades desde una perspectiva organizacional, en oposición a una perpectiva técnica. Generalmente se pasan por alto los procesos, documentación y actividades informales que impactan directamente en la postura de una organización de seguridad y no necesariamente de manera técnica. El IAM fue desarrollado por la Agencia

de Seguridad Nacional de los Estados Unidos y asesores de INFOSEC y ha estado en práctica dentro del gobierno de ese país desde 1997.

Modelo NSA

- Avalúo (“Assessment”)
- Evaluación (“Evaluation”)
- Penetración (“Red Team”)
- Informe de Hallazgos
- Recomendaciones

Fase de avalúo: En esta fase se realiza la recopilación y examen de las políticas de seguridad, procedimientos, de arquitectura de seguridad y de flujo de la información. También se hace un análisis colaborativo de alto nivel y se evalúan las funciones críticas de la organización.

Fase de Evaluación: Se realizan pruebas de seguridad del sistema, firewalls, routers, equipos. Se realiza un escaneado de la red y se utilizan herramientas de penetración.

Fase de Penetración: Una evaluación de nivel 3 es no cooperativa y externa a la red de destino, con la participación de pruebas de penetración para simular el adversario adecuado. La evaluación es no intrusiva, por lo que dentro de este marco, una evaluación de nivel 3 implica una calificación completa de las vulnerabilidades. Se realizan pruebas de ingeniería social, simulación de ataques y hackeo de sistemas.

- Informe modelo de hallazgos: Se realiza un informe técnico, operacional y gerencial de los hallazgos determinados durante las fases previas.
- Modelo análisis de hallazgos y recomendaciones: En esta etapa se prepara un informe con las recomendaciones para mitigar las vulnerabilidades.

El presente trabajo se sitúa en el nivel 2, “Fase de evaluación” y nivel 3 “Fase de Penetración”, en la que se realizan pruebas de seguridad del sistema, escaneado de la red y uso de herramientas de penetración, para determinar el estado de seguridad del sistema e implementar mecanismos de corrección y mejora de la seguridad.

2.2 GENERALIDADES DE LA RED Y SERVICIOS A PROTEGER

De acuerdo con las necesidades de comunicación de los usuarios, los servicios mínimos que se requieren proteger en toda red son los siguientes:

2.2.1 Servicios Web

Las aplicaciones web son, por lo general, una colección de varios scripts de lenguajes como Javascript, PHP y HTML, que residen en un servidor Web e interactúan con una base de datos para la creación de una página Web con contenido dinámico[4]. Estas aplicaciones se implementan por la facilidad con que permiten la interacción entre clientes y proveedores de productos y servidico y porque permiten compartir y manipular información entre sí, mediante una interfaz Web que es usualmente independiente del sistema que se usa.

El servicio Web sigue el modelo cliente-servidor, por lo que se tiene un programa cliente Web instalado en el equipo del usuario que establece una conexión con el programa servidor que administra la presentación de la información en cada servicio Web. El programa cliente utiliza un número de puerto aleatorio con un valor superior a 1023 (entre 1024 y 65 535). El programa servidor usa por defecto el número de puerto 80 para el protocolo HTTP y el puerto 443 para el protocolo HTTPS. Pero un servidor puede configurarse para que utilice cualquier otro número de puerto. En este caso, el cliente tendría que introducir dicho puerto al indicar la dirección de destino. La gran mayoría usa el puerto 80 por lo que las reglas de filtrado a configurar en los *firewall* no consideran el tráfico Web a un número de puerto distinto.

2.2.2 Correo electrónico

El correo electrónico, junto con el Web, es el servicio más importante de los que ofrece Internet. La finalidad de este servicio es la de permitir el intercambio de mensajes entre usuarios. Para hacer uso del correo electrónico se utilizan unos programas conocidos como clientes de correo, aunque también existe la posibilidad de hacer uso de este servicio desde un servidor Web. A este servicio se le conoce como correo Web o Web mail.

Todos los mensajes de correo electrónico se mueven por Internet utilizando un formato especial llamado SMTP (Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo). Cuando se usa un programa cliente de correo, los mensajes que van recibiendo son guardados en el buzón de correo del servidor a la espera de que el usuario se conecte a Internet, ejecute su programa cliente y descargue los mensajes desde su buzón. La comunicación entre el programa cliente y servidor de correo para la descarga de mensajes se lleva a cabo con el protocolo POP (Post Office Protocol, Protocolo de la Oficina de

Correos, puerto 110). No obstante, cuando el programa cliente envía correos salientes a Internet lo hace directamente con el protocolo SMTP (puerto 25).

Aunque éstos son los protocolos comúnmente utilizados para el uso del correo electrónico, existen otros protocolos que aportan ciertas funcionalidades adicionales. El protocolo IMAP4 (Internet Mail Access Protocol, Protocolo de Acceso al Correo de Internet, versión 4) le da al usuario la posibilidad de acceder a otras carpetas de su buzón distintas a la carpeta Entrada (Inbox). Con POP3 el usuario sólo puede bajar los nuevos mensajes de la carpeta Entrada para posteriormente organizarlos localmente. Con IMAP4, el usuario puede acceder también a otras carpetas como Salida (Outbox), Enviado (Sent), Borrado (Deleted), etc., así como a carpetas de uso compartido. El protocolo IMAP4 utiliza una conexión *TCP* con el puerto 143 del servidor.

Otro protocolo de correo es el LDAP (Lightweight Directory Access Protocol, Protocolo Simple de Acceso al Directorio), que facilita la prestación de un servicio de directorio para que los usuarios puedan buscar las direcciones de correo desconocidas de los destinatarios de sus mensajes. El protocolo LDAP utiliza una conexión *TCP* sobre el puerto 389.

Si la conexión entre el programa cliente y el servidor de correo se realiza con el cifrado SSL, los puertos utilizados por el servidor suelen ser distintos: 995 para POP3, 993 para IMAP, 25 o 465 para SMTP y 636 para LDAP.

2.2.3 Mensajería instantánea

La mensajería instantánea es un servicio de Internet que permite a distintos usuarios estar en contacto permanente mientras están conectados a Internet. Ofrece herramientas de comunicación mediante texto escrito, voz o video. Adicionalmente se pueden realizar transferencias de archivos y compartir aplicaciones. Su relevancia en el entorno laboral es cada vez mayor, ya que permite que los trabajadores dispersos puedan trabajar en un entorno virtual como si todos estuviesen juntos en una sala. El inconveniente de los programas de mensajería es que son incompatibles entre sí al utilizar cada uno de ellos su propio sistema de comunicación.

2.2.4 Servicios de terminal

El servicio de terminal permite que un usuario haga un uso remoto de otra computadora (servicio central de terminal) en modo compartido. De esta manera no es necesario estar físicamente presente en el lugar donde se encuentra el servidor para hacer uso de sus recursos. *Secure shell* (SSH) es una herramienta muy popular y muy segura para comunicación en canales inseguros, que permite realizar conexiones remotas en otro host desde una estación de trabajo. Además de la conexión, SSH permite copiar datos de forma

segura y pasar datos de otra aplicación por un canal seguro tunelizado mediante SSH. *Secure shell* utiliza el puerto 22. Cabe mencionar que la mayoría de los sistemas operativos de libre distribución ya incluyen esta herramienta, por lo que no es necesario realizar su instalación.

2.2.5 Bases de datos

Una base de datos es una entidad que puede almacenar datos de forma estructurada. Se trata de una serie de datos organizados y relacionados entre sí, con la finalidad de ser usados de de una manera específica en beneficio de una persona u organización. Generalmente, una base de datos interactúa con diferentes programas y usuarios, los cuales utilizan los datos almacenados para sus tareas cotidianas, razón por la cual una base de datos es un servicio indispensable en una red que comparte información.

Una base de datos proporciona a sus usuarios el acceso simultáneo a los datos almacenados, quienes pueden hacer consultas de los registros existentes, ingresos o altas, bajas o eliminación de registros y modificaciones a los mismos, todo de acuerdo con los privilegios establecidos para cada usuario. Los puertos utilizados por las bases de datos varían de acuerdo con el sistema manejador de bases de datos.

2.3 MODELADO DE AMENAZAS Y GESTIÓN DE RIESGOS

De una forma simple, un riesgo es la relación entre los activos y las vulnerabilidades que cualquier atacante aprovecharía para adueñarse o interferir sobre estos[8].

Existen dos métodos para llevar a cabo el modelado de amenazas y gestión de riesgos, el método cuantitativo y el cualitativo. En el método cuantitativo se expresa el valor de cada activo en términos monetarios, tanto las medidas a implementar, como el presupuesto destinado a la seguridad está basado en análisis confiables y siempre determinados mediante el análisis de costo-beneficio.

En el método cualitativo no es necesario determinar el valor monetario de la información ni el costo de las medidas a tomar; no requiere una actualización constante de los valores de los activos que se evalúan, en su lugar, se consideran factores generales que afectan el desempeño del sistema, como son, las amenazas, las vulnerabilidades, el nivel de riesgo a que se expone el sistema y el posible tratamiento correctivo. En adelante se implementará este tipo de metodología ya que se adapta a todo tipo de sistema. Debido a que el presente trabajo está orientado a la parte lógica, no se analizarán los aspectos relativos a la parte física o seguridad de hardware, aspecto muy importante pero que no forma parte del

presente trabajo, por lo tanto en el siguiente análisis se consideran solamente las amenazas al software.

Las siguientes tablas muestran un análisis de las posibles amenazas a la red (tabla 2.1), al servidor (tabla 2.2) y a las aplicaciones (tabla 2.3), implementadas en el servidor. Se trata de un análisis global de las amenazas, las vulnerabilidades, nivel de riesgo, dependiendo del grado de daño que puedan provocar en los recursos y su tratamiento. No contiene todas las amenazas existentes o posibles, ya que un estudio de tal magnitud requiere también un tratamiento específico, bastante extenso y que escapa a los alcances de este trabajo, pero permite definir en forma básica cómo crear una respuesta ante un ataque a los recursos de la red. Asimismo, cabe mencionar que las tablas en cuestión son producto de una recopilación, análisis, y selección de las que he considerado las más sobresalientes de los documentos revisados.

Tabla 2.1, Amenazas a la red

Amenaza	Vulnerabilidad	Nivel de riesgo	Tratamiento
Ataque a los dispositivos de acceso a la red	Escaneo de puertos y consultas remotas.	**Alto**	Filtrar el tráfico entrante para aislar los puertos específicos en el host. Implementar un sistema de detección de intrusos. Implementar un *sniffer* de red para verificar la entrada de tráfico autorizado. Deshabilitar los servicios innecesarios con base en las políticas de seguridad de la institución.
Ataque a los dispositivos de monitoreo de la red	Mala configuración del *firewall* y/o del Sistema de Detección de Intrusos.	**Alto**	Verificar la configuración del Sistema de Detección de Intrusos en línea para normalizar el tráfico. Verificar la configuración del *firewall* y realizar pruebas de filtrado. Permitir el mínimo paso posible de paquetes al sistema. Revisar que las políticas de seguridad sean adecuadas para el nivel de seguridad

			requerido.
Banners	Brindar información mediante las pancartas de ingreso al sistema.	**Bajo**	Cambiar las pancartas que ofrecen información del sistema. Realizar las actualizaciones pertinentes al sistema operativo.
Rastreo de puertos	Puertos innecesarios abiertos.	**Alto**	Usar un detector de rastreadores, para descubrir actividades de escaneo. Revisar puertos abiertos en el sistema y determinar si son indispensables en ese momento. Usar protocolos cifrados para todas las comunicaciones que tengan contenido confidencial. Segmentar lo más posible servicios y accesos para evitar la divulgación de información.

Tabla 2.2, Amenazas al servidor

Amenaza	Vulnerabilidad	Nivel de riesgo	Tratamiento
Explotación de errores de configuración del sistema operativo.	Sobrecargas de búfer.	**Alto**	Establecer límites de uso de procesador. Realizar pruebas frecuentes con un software de escaneado de vulnerabilidades. Realizar las actualizaciones de software necesarias.
Administración abierta de usuarios y archivos	Errores en la configuración de cuentas de usuarios y	**Alto**	Establecimiento de cuotas. Acceso sistemas y programas indispensables.

	permisos de archivos.		Privilegio mínimo para usuarios y ejecución de aplicaciones. Realizar pruebas frecuentes con un software de escaneado de vulnerabilidades. Verificar que todas las contraseñas sean robustas. Eliminar cuentas no utilizadas. Establecer adecuados controles de acceso a personal autorizado.
Ataques a cuentas del sistema	Cuentas predeterminadas del fabricante.	**Medio**	Eliminar cuentas predeterminadas y cuentas no utilizadas. Verificar que las contraseñas sean actualizadas periódicamente. En su caso, cambiar contraseñas predeterminadas.
	Contraseñas en blanco o vulnerables.	**Alto**	Implementar un software de detección de contraseñas vulnerables. Establecer políticas de contraseñas para evitar contraseñas vulnerables e implementarlas mediante el uso de un software. Requerir que las contraseñas se cambien regularmente y eliminar las cuentas que no hayan iniciados nunca una sesión en la red. Escaneado de vulnerabilidades.
Puertos abiertos	Ejecución de servicios innecesarios.	**Bajo**	Eliminar aplicaciones que se ejecutan en nuestras máquinas que ya no sirven a ningún propósito útil, para evitar que se tengan puertos abiertos. Configurar el *firewall* para cerrar dichos puertos.
Bitácoras accesibles a	Mala configuración de	**Medio**	Verificar los permisos de las bitácoras y evitar el acceso mediante permisos de

usuarios.	las bitácoras y libre acceso a ellas.		administrador.
Ataques de fuerza bruta	Ataques a contraseñas.	**Alto**	Establecer un número máximo de intentos de autenticación. Revisión periódica a los intentos de acceso monitoreando los archivos /var/log/messages y /var/log/secure. Bloqueo de las direcciones *IP* de las que se reciben intentos de ataque en el archivo /etc/host.deny. Evitar el logeo como administrador en el servicio *secure shell*. Usar protocolos cifrados para todas las comunicaciones que tengan contenido confidencial.
Intrusiones	Acceso a cuentas de usuario no root.		Verificar que los archivos en el servidor no son alterados. Revisión periódica a los intentos de acceso monitoreando los archivos /var/log/messages y /var/log/secure.
	Acceso a cuentas root.		Revisión de los archivos de sistema. Realizar respaldos a las aplicaciones y bases de datos necesarias y considerar reinstalación del sistema. Análisis forense.
	Aumento de privilegios y puertas traseras.		Escaneo para revisar vulnerabilidades aprovechadas. Revisión de las bitácoras para descubrir actividades dañinas. Escaneo para ubicar y eliminar puertas traseras.

Tabla 2.3 Amenazas a las aplicaciones

Amenaza	Vulnerabilidad	Nivel de riesgo	Tratamiento
Ataque a base de datos	Saturación del búfer.	**Medio**	Corregir aplicaciones con vulnerabilidades. Eliminar las cuentas de usuario que no se usen y especialmente las predeterminadas. No aceptar cuentas sin contraseñas. Eliminar en la medida de lo posible los procedimientos almacenados.
Ataque a aplicaciones web	Ataques de inyección a SQL.	**Medio**	Validar entradas para el tamaño y tipo correctos, en particular si hay caracteres especiales. Revisar y corregir aplicaciones basadas en el Web. No permitir que se vean mensajes de error explícitos que muestren la consulta o parte de la consulta de SQL. No aceptar cuentas sin contraseñas. Mantener al mínimo los privilegios de las cuentas.
	Manipulación de URL y cruce de directorios.	**Medio**	Deshabilitar la visualización de los archivos de un directorio que no contiene un archivo índice. Eliminar directorios y archivos inservibles, así como secuencias de comandos innecesarios. Proteger el acceso a directorios que contienen datos importantes. Eliminar las opciones de configuración

			innecesarias. Impedir la visualización HTTP en páginas HTTPS accesibles.
Ataque Dos	DoS múltiple.	**Medio**	Bloquear redifusiones dirigidas. Considerar el bloqueo a los paquetes *ICMP*.
	Privación de recursos.	**Bajo**	Aplicar las últimas actualizaciones al sistema operativo y aplicaciones. Establecer cuotas de disco.
	Interrupción de servicios.	**Medio**	Aplicar actualizaciones constantes al sistema operativo. Probar las actualizaciones antes de aplicarlas a los sistemas de producción. Deshabilitar los servicios innecesarios

Las siguientes páginas Web también son útiles para investigar vulnerabilidades potenciales en los servicios de red:
http://www.securityfocus.com
http://www.milw0rm.com
http://www.packetstormsecurity.com
http://www.frsirt.com
http://www.mitre.org

2.4 DISEÑO DEL PERÍMETRO DE LA RED

El diseño del perímetro de la red permite determinar la posición de los elementos de seguridad implementados en toda la red con respecto a su exterior. Constituye la planeación física del sistema de defensa y se trata de la primera medida de seguridad que va a tener resultados importantes en la forma de administrar la red.

Existen diferentes configuraciones o arquitecturas que varían tanto en elementos como en el nivel de seguridad que pueden proveer a la red, a continuación se describen las características de algunas configuraciones básicas de acuerdo con la descripción hecha por Michael D. Bauer[8].

2.4.1 Arquitectura interna contra externa

La arquitectura más simple y la que se utiliza comúnmente es aquella en que se emplea en primer término un enrutador con filtrado de paquetes, pero no como única línea de defensa. Directamente detrás se sitúa un *firewall*, en este caso una estación ejecutando el sistema operativo Linux con iptables (filtrado de paquetes). No hay conexión directa con Internet o desde el enrutador externo con la red interna; todo el tráfico que entra o sale, pasa por el *firewall*. Una desventaja de esta configuración es que todo el tráfico de servicios públicos como SMTP (email) o HTTP (www) debe ser enviado a través del *firewall* a servidores internos. El paso de este tráfico no expone directamente a los servidores internos a algún ataque, pero si magnifica las consecuencias de servidores internos comprometidos.

El establecer una arquitectura en la que se controlan todos los servicios públicos en un *firewall* no parece tan malo a simple vista, pero resulta fácil deducir que el rendimiento podría resultar diferente al esperado; el *firewall* tiene que emplear todos los recursos disponibles para inspeccionar y mover paquetes, así que la seguridad podría verse afectada cuando algún servicio se ejecute en el *firewall*.

2.4.2 Arquitectura de zona desmilitarizada con tres interfaces de red en el *firewall.*

En esta configuración se tiene una zona desmilitarizada (*DMZ*, DeMilitarized Zone) para acceso a los servicios públicos. Una zona desmilitarizada es aquella red que contiene servicios públicamente accesibles, aislados de la red interna. De preferencia aislada de la red externa.

En este caso se cuenta con un enrutador y detrás del enrutador se coloca el *firewall* protegiendo la zona desmilitarizada, a su vez un switch o un enrutador filtra el acceso a la red local. Si se configura adecuadamente, el *firewall* usa diferentes reglas para evaluar el tráfico:

- De Internet a la zona desmilitarizada
- De la zona desmilitarizada
- De Internet a la red interna
- De la red interna a Internet
- De la zona desmilitarizada a la red interna
- De la red interna a la zona desmilitarizada

En este caso se simplifica la administración de la seguridad, ya que se toma a la zona desmilitarizada como una sola entidad con diferentes servicios internos como SMTP, FTP, Web, DNS.

2.4.3 Arquitectura débil de subred protegida

En esta arquitectura se utilizan dos enrutadores que actúan como *firewalls* filtrando paquetes, uno entre Internet y la zona desmilitarizada y otro enrutador entre la zona desmilitarizada y la red interna. Para tener acceso a la zona desmilitarizada o a la red interna vía el enrutador de protección, se utiliza un switch o un hub.

Este tipo de arquitectura tenía sentido cuando los enrutadores eran meros copiadores de grandes cantidades de datos en lugar de host con varias interfaces de red. Tiene algunos inconvenientes importantes como son: los enrutadores generalmente se encuentran bajo el control de una persona diferente que la encargada del *firewall*; los enrutadores tienden a tener un control administrativo más débil que los *firewalls*; y los enrutadores tienden a ser más vulnerables a ataques que una computadora bien configurada.

2.4.4 Arquitectura fuerte de subred protegida

En esta arquitectura se utilizan dos *firewalls* propiamente hechos, que son más sofisticados que los enrutadores. El *firewall* externo filtra las peticiones desde el exterior hacia el interior de nuestra red, inmediatamente después del *firewall* se encuentra un switch o un hub que redirige el tráfico hacia los servicios públicos o hacia el *firewall* interno. El *firewall* interno filtra el tráfico dirigido hacia la red interna.

Esta arquitectura es útil cuando hay que soportar grandes volúmenes de tráfico y en entornos de *firewalls* heterogéneos.

2.4.5 El Sistema de Detección de Intrusos

No existen reglas fijas para situar el Sistema de Detección de Intrusos, pero dependiendo de la ubicación de éste en la red, serán los resultados que se obtengan y el aprovechamiento que tendremos del mismo. Dependiendo de la estructura de la red, un SDI (Sistema de Detección de Intrusos) puede situarse:

a) Delante del *firewall*
b) Detrás del *firewall*
c) Combinación de las dos anteriores
d) En el *firewall*
e) Configuraciones avanzadas

a) Delante del *firewall*:

El SDI comprobará todos los ataques que se produzcan y le evitará una gran carga al *firewall*, que se encargará de bloquear ataques efectivos, a su vez esto generará una gran

cantidad de logs y un exceso de información que podría resultar contraproducente. Debido a la excesiva carga de información se puede perder de vista información vital sobre ataques importantes a nuestra red.

b) Detrás del *firewall*:

El SDI no analizará todos los ataques se dirijan a la red, sino únicamente el tráfico que haya sido permitido por el *firewall*, es decir, que haya sido previamente filtrado, con lo que se genera una menor cantidad de logs y de información y se enfoca realmente en ataques potencialmente más peligrosos.

c) Combinación de las dos anteriores:

Con esta configuración se tiene un mejor control de los eventos que se monitorizan en ambos lados del *firewall*, se mejora la seguridad porque se puede establecer una correlación entre los ataques detectados en ambos lados del *firewall*. La desventaja es que se requieren dos máquinas para implementar este tipo de configuración.

d) En el *firewall*:

En esta configuración una máquina opera como *firewall* y de SDI a la vez, al igual que en el caso del SDI delante del *firewall*, se monitoriza todo el tráfico de la red, por lo que se genera una gran cantidad de logs y se pueden llegar a perder de vista los ataques efectivos dirigidos hacia nuestra red.

e) Combinaciones avanzadas:

Surgen de la necesidad de tener un mayor control y seguridad en áreas específicas de la red, segmentos o hosts individuales, dependiendo de la arquitectura o diseño del perímetro de red implementado.

2.5 CARACTERÍSTICAS DEL SISTEMA OPERATIVO

La elección del sistema operativo para el sistema de seguridad es una parte fundamental de lo que se conoce como la base informática de confianza, una lista de elementos que proporcionan seguridad, entre los que destacan el sistema operativo, los programas, el hardware de la red, las protecciones físicas e incluso los procedimientos.

Anteriormente un sistema operativo tenía un número limitado de entradas posibles, eran pocos los programas de aplicación implementados. Sin embargo, ahora con Internet y la diversidad de programas que se usan en las computadoras, los sistemas operativos se han vuelto menos seguros y más susceptibles a fallas. Además, la tendencia de los proveedores

de software es intentar que el usuario tenga todo preparado una vez que instala su sistema operativo, esto puede parecer muy bueno pero representa un problema muy grande en cuanto a seguridad; ya que la mayoría de las opciones de seguridad están desactivadas de forma predeterminada, muchos programas y servicios se cargan automáticamente, tanto si las necesita el usuario como si no, y se introducen muchos "extras" en el sistema en un esfuerzo por ganar la competencia entre desarrolladores de software.

El sistema operativo que se va a instalar y sobre el cuál se va a implementar el Sistema de Detección de Intrusos es GNU/Linux. Este sistema, implementación de libre distribución tipo Unix, es usado en una amplia variedad de plataformas de hardware y computadoras, incluyendo las computadoras de escritorio, servidores, supercomputadoras, mainframes y teléfonos celulares. Se encuentra protegido con la licencia GNU.

Linux contiene todas las funciones y características necesarias de cualquier sistema operativo; pero en especial implementa características que lo definen como un sistema operativo de alto rendimiento en servidores; entre ellas: es multitarea, es decir, puede ejecutar varios programas al mismo tiempo; tiene capacidad multiusuario, varios usuarios pueden estar trabajando al mismo tiempo en la computadora; es multiplataforma, es multiproceso, se puede hacer una implementación de varios procesadores para realizar objetivos comunes; tiene protección de memoria entre procesos; permite usar bibliotecas enlazadas tanto estática como dinámicamente; es compatible con *Posix*, System V y BSD a nivel fuente; y por el amplio desarrollo, tiene cada vez más soporte para nuevo hardware, todo el código fuente está disponible, incluyendo el núcleo completo y todos los drivers, las herramientas de desarrollo y todos los programas de usuario.

Existen numerosas distribuciones Linux, también conocidas como "distros". Entre ellas destacan el proyecto Debian/GNU y Fedora, ambos sistemas de propósitos generales usados frecuentemente en servidores de aplicaciones, ambos cuentan con el respaldo del movimiento de *software libre* y de todas las ventajas de que muchos programadores están trabajando continuamente para mejorar el código fuente continuamente.

2.6 REQUERIMIENTOS DE SEGURIDAD DEL SERVIDOR

Fortalecer un sistema Linux después de su instalación básica no es una tarea trivial, se deben determinar todas las vulnerabilidades ofrecidas por la instalación por default y modificarlas de manera que no signifiquen un peligro para la seguridad del sistema. Una tarea importante es mantener actualizado al sistema con parches de seguridad con cierta regularidad y deshabilitar todos los servicios que no sean necesarios.

La computadora en que estén instaladas las herramientas de seguridad requiere de una serie de medidas de seguridad bien definidas tanto en aplicaciones como en servicios, para

evitar al máximo las vulnerabilidades y amenazas que den lugar a algún ataque y puedan poner en riesgo la seguridad del servidor y por tanto de la red que éste defiende.

2.6.1 Políticas sobre contraseñas

La importancia que tienen las contraseñas en cualquier sistema es muy grande; una contraseña permite identificar a un usuario y saber de acuerdo con sus estatus qué tiene permitido hacer en el sistema. Es de vital importancia por tanto, asegurar que este sistema de identificación básico no pueda ser fácilmente vulnerado por cualquier persona que quiera usurpar una identidad. Para ello se tiene que hacer una revisión contínua de contraseñas, a fin de verificar que son fuertes, deben contener caracteres alfanuméricos, y caracteres especiales; además dichas contraseñas deben estar en uso y tener un tiempo de expiración. El archivo /etc/shadow debe ser legible únicamente por el administrador.

2.6.2 Políticas sobre cuentas de usuario

Se deben crear cuentas de usuario solamente en los casos necesarios y con establecimiento de cuotas, es decir, con cierto espacio de disco y determinados privilegios, tener un control estricto de los usuarios y grupos creados en el sistema y sus privilegios. Desactivar o remover cuentas innecesarias que se crean para servicios que no estarán en uso y limitar el uso del procesador para evitar el desbordamiento de buffer.

Hacer la asignación adecuada de permisos a cada directorio para asegurar que los usuarios únicamente puedan tener acceso a los archivos que les pertenecen y puedan ejecutar los programas permitidos.

2.6.3 Políticas de acceso remoto

El acceso remoto tiene que realizarse mediante una herramienta segura como *secure shell*, que nos permitirá realizar conexiones remotas hacia el servidor con la finalidad de administrar los recursos instalados en el mismo. No debe permitirse el acceso como usuario root y debe estipularse un número máximo de intentos de autenticación para evitar el ataque por fuerza bruta. Además se debe estar muy atentos a los intentos de acceso monitoreando permanentemente los archivos /var/log/messages y /var/log/secure y bloquear definitivamente las direcciones *IP* de las que se reciben intentos de ataque en el archivo /etc/host.deny.

2.6.4 Políticas de respaldos

Es indispensable crear, conservar y proteger los recursos de información de la red, del sistema y de las aplicaciones; para ello se requieren políticas para crear respaldos de todos los elementos participantes en el desarrollo fundamental de la red.

Estos respaldos proporcionan la seguridad de recuperación ante algún incidente dañino, imprevisto o poco usual que modifique alguna característica de nuestra red perjudicando su funcionamiento. La información a respaldar incluye a los archivos de sistema de los equipos de la red, bitácoras del Sistema de Detección de Intrusos, resultados de escaneo de vulnerabilidades, archivos de información sobre conexión remota a las máquinas, respaldo de bases de datos, de aplicaciones y de programas desarrollados para el servicio de la red.

2.7 HERRAMIENTAS DE FILTRADO Y MONITOREO

Existen muchos elementos que permiten mantener un sistema seguro, entre ellos el *firewall* y el Sistema de Detección de Intrusos, que aunque son elementos importantes en el ámbito de la seguridad, no constituyen una garantía de fiabilidad si no se implementan otras herramientas, componentes y medidas de seguridad que forman parte de las estrategias de protección de un sistema.

Algunas herramientas de seguridad para filtrado y monitoreo son distribuidas con los sistemas operativos, otras se producen especialmente para reforzar la seguridad en una parte específica de la red o del servidor. El control de acceso, los mecanismos de identificación y autenticación, el cifrado de la comunicación, y diversos comandos de monitoreo del sistema, son elementos que se distribuyen comúnmente con el sistema operativo.

Ciertas herramientas se han diseñado para abordar problemas específicos, entre ellas destacan los programas para el reforzamiento del sistema operativo, los escáners de vulnerabilidades, los *sniffers* de red, los programas seguros de conexiones remotas, descifradores de contraseñas, los programas antivirus, herramientas de filtrado de paquetes y de detección de intrusiones. Se trata de herramientas para diversos problemas de seguridad de la red, muchas de ellas de libre distribución y generalmente disponibles para los sistemas Linux.

Como se dijo anteriormente, un elemento importante es el *firewall*, un dispositivo que actúa en la primera línea de defensa frente a cualquier ataque entrante, que puede desviar o suavizar el efecto de muchos tipos de ataques y proteger los servidores y estaciones de trabajo. Un *firewall* también puede evitar el acceso a las máquinas internas desde fuera de

la red. Correctamente configurado, un *firewall* nos ayuda a estar más seguros frente a los ataques exteriores.

Existen dos formas de configurar un *firewall*, una de ellas es permitir todo el tráfico y después añadir el comportamiento que deseamos bloquear. La otra forma es denegar todo y añadir después lo que deseamos permitir. Este último método es más fácil de mantener con seguridad que la otra solución, ya que nos permite tener cerrado el sistema a ataques desconocidos e identificar y abrir el sistema únicamente a los servicios inofensivos y conocidos.

El *firewall* debe respetar el mapa de servicios internos y externos de la red, es decir, permitir la conexión a los servidores que necesitan hacerlo desde el exterior, en los puertos correspondientes, por ejemplo, abrir los puertos 80 y 443 para web, el puerto 22 para *Secure Shell*, y así sucesivamente, de acuerdo con la arquitectura definida para la red y las políticas de seguridad de la institución.

El núcleo de Linux incluye la facilidad del filtrado de paquetes desde la versión 1.1.x. A mediados de 1999 apareció una nueva generación de *firewall* de Linux desarrollada por Rusty Russel, y que tiene como nombre iptables. Esta aplicación implementa la inspección dinámica de paquetes y utiliza de forma más eficiente la cadena de reglas que maneja el tráfico que se enruta a otras redes. El *firewall* de Linux forma parte del núcleo del sistema operativo, y por tanto, está siempre presente en la mayoría de las distribuciones, aunque puede que no esté instalado. *Iptables* es una herramienta muy eficaz pero compleja, y normalmente se recomienda para usuarios que están familiarizados con los *firewalls* y la forma de configurarlos.

La otra herramienta importante en la seguridad de una red es el Sistema de Detección de Intrusos, una herramienta de seguridad que ayuda a supervisar los eventos ocurridos en una red comparándolos con patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa para la red. Un SDI alerta y previene de manera anticipada sobre cualquier actividad sospechosa en la red pues está diseñado para detectar las primeras etapas de un ataque como es el barrido de puertos.

El SDI configurado correctamente sirve para encontrar usos indebidos de los recursos de la red, esto se hace comparando las firmas con la información recogida en busca de coincidencias; además puede detectar anomalías mediante el uso de técnicas estadísticas que definen de forma aproximada lo que debería ser el comportamiento normal o usual.

Uno de los Sistemas de Detección de Intrusos más populares y efectivo es Snort, un detector de intrusos disponible bajo la licencia GPL, de libre distribución que funciona bajo

plataformas Unix/Linux y Windows. Snort contiene una gran cantidad de patrones definidos y actualizaciones ante ataques, barridos y vulnerabilidades detectadas en boletines de seguridad. Incluye un lenguaje flexible y potente para la creación de reglas e incluye filtros predefinidos contra ataques frecuentes; se puede utilizar como *sniffer* de red, registro de paquetes o como un SDI normal.

En el siguiente capítulo se explica la funcionalidad de algunas herramientas de libre distribución que se implementan en sistemas Linux y el uso de dichas herramientas para obtener el sistema de seguridad tanto de un servidor como de la red. Entre las herramientas descritas adelante, se encuentran herramientas para el escaneo de vulnerabilidades, el análisis de paquetes, descifrado de contraseñas, filtrado de paquetes y monitoreo de la red.