HERRAMIENTAS DE SEGURIDAD

Siempre es conveniente instalar herramientas de seguridad y es aconsejable que éstas sean las que se consideren necesarias después de haber realizado un análisis de seguridad para el entorno correspondiente, y que según los requerimientos determinados así como las amenazas y vulnerabilidades identificadas será pertinente instalar a fin de que dichas herramientas puedan utilizarse para hacer cumplir las políticas de seguridad de la organización.

Entre las herramientas indispensables de uso cotidiano que se requieren para la comunicación de redes están:

a) Telnet: abre una sesión en una máquina remota.

b) FTP: transfiere archivos desde una máquina remota.

Sin embargo, estas herramientas son muy inseguras ya que a su paso por Internet existen programas que pueden identificar todo el flujo de información de manera textual desde una máquina hacia otra incluyendo el nombre y la contraseña del usuario. Para evitarlo, se crearon las siguientes herramientas:

a) Ssh (Secure shell): es un programa para conectarse a otros equipos a través de una red, ejecutar comandos en una máquina remota y mover archivos de una máquina a otra. Proporciona una exhaustiva autenticación y comunicaciones seguras en redes inseguras ya que comunica una máquina con otra, transfiere archivos y directorios con copia de seguridad, la información pasa cifrada a lo largo de la red, por lo que algunos programas sólo aprecian datos con caracteres que no tienen ninguna lógica de secuencia de información.

b) OpenSSH (Open secure shell): se encarga de cifrar el tráfico incluyendo las contraseñas, para eliminar de un modo efectivo el espionaje, los secuestros de las conexiones y otros ataques a nivel de red, de tal manera que permite realizar la comunicación y transferencia de información de forma cifrada pues proporciona fuerte autenticación sobre un medio inseguro. OpenSSH ofrece amplias posibilidades para la creación de túneles seguros, aparte de una variedad de métodos de autenticación.

c) SSL (Secure socket layer): sistema de protocolos de carácter general diseñado en 1994 por la empresa Nestcape Communications Co., está basado en la aplicación conjunta de criptografía simétrica, criptografía asimétrica, certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través de Internet,

es idóneo para transferir información personal o relacionada con transacciones financieras a través de Internet de forma segura y privada. SSL implementa un protocolo de negociación para establecer una comunicación segura a nivel de socket, de forma transparente al usuario y a las aplicaciones que lo usan. Actualmente es el estándar de comunicación segura en los navegadores más importantes como Netscape Navigator e Internet Explorer.

d) Tcp wrappers: su función radica en que autentica las redes, es decir, reconoce que la Ip de una red en realidad pertenece a dicha red. Esto se debe a que alguien que sabe la aceptación de una Ip para ingresar a un sistema, puede poner en una red inventada esa Ip –a esto se le llama spoofing– y así ingresar a cierto sistema.

e) Parches (patch): es conveniente su colocación en el sistema, ya que diariamente surgen nuevos ataques a través de agujeros no protegidos por el sistema y al poner estos parches se pueden contrarrestar las posibles incursiones de los atacantes informáticos además de que éstos permiten actualizar y mejorar la operatividad del sistema.

f) Portsentry: es un programa que cuenta con un archivo de los puertos más vulnerables del sistema, también se pueden agregar a esa lista otros que no se consideran pertinentes para la seguridad del sistema, esta herramienta identifica si alguien quiere entrar por alguno de esos puertos impidiéndole la entrada.

g) Sniffers: tal vez sea una de las herramientas más completas para la revisión de una red ya que además de poder ver en forma clara conexiones no encriptadas, también permite verificar varios servicios como el correo por su puerto 25, la web por su puerto 80 y todos los servicios que se desean revisar en cada momento.

h) Tripwire: es un monitor de la integridad de los archivos, esta herramienta rastrea cambios en los permisos de los archivos y ligas, tamaños en archivos, tamaños en directorios y cambios en los identificadores de grupos (groupid) y usuarios (userid).

i) Nmap: existe para el escaneo de puertos, éste permite a los administradores de sistemas el escaneo de grandes redes para determinar qué servidores se encuentran activos y qué servicios ofrecen.

j) PEM (Privacy Enhaced Mail): da soporte a la criptografía, autenticación e integridad de mensajes de correo electrónico ya que permite cifrar de manera automática los mensajes antes de enviarlos. PEM realiza las siguientes funciones:
   - Especifica los formatos de mensajes para pedir y revocar certificados.

- Especifica la jerarquía de las autoridades certificadoras (AC).

- Especifica la jerarquía de los algoritmos de criptografía.

k) IDS (Intrusion Detection System): sistema para detectar intrusiones al sistema[18], existen varios tipos:

- HIDS o HostIDS (Host Intrusion Detection System): protege contra un único servidor, una computadora o un host. Observa una gran cantidad de eventos, analizando actividades con una gran precisión, determinando de esta manera qué procesos y usuarios se involucran en una determinada acción, también recaba información del sistema como archivos, logs, recursos, para su posterior análisis en busca de posibles incidencias. Todo ello en modo local, dentro del propio sistema. Cabe mencionar que éstos fueron los primeros IDS en ser desarrollados por la industria de la seguridad informática.

- NIDS o NetIDS (Network Intrusion Detection System): protege un sistema basado en la red ya que actúan sobre ésta capturando y analizando paquetes de red. Luego analiza los paquetes capturados buscando patrones que suponen algún tipo de ataque –como la entrada al sistema o la denegación del servicio–. Un NIDS es capaz de monitorear muchas máquinas mientras los anteriores sólo monitorean el equipo donde están instalados, por ello, cuando se ubican correctamente pueden analizar grandes redes y su impacto en el tráfico suele ser pequeño. Actúan mediante la utilización de un dispositivo de red configurado en modo promiscuo (analizan y observan todos los paquetes que circulan por un segmento de red aunque éstos no vayan dirigidos a un determinado equipo). Cabe destacar que analiza el tráfico de red, normalmente, en tiempo real y no sólo trabaja a nivel TCP/IP, sino que también lo puede hacer a nivel de aplicación.

- SIV (System integrity verifiers): monitorea los archivos del sistema para detectar cuándo un intruso intenta alterarlos o intenta abrir una puerta trasera. También puede detectar cuándo un usuario normal adquiere privilegios de administrador.

- LFM (Log file monitors): monitorea archivos marcados que se generan por los servicios de la red, de manera similar a los NIDS, estos sistemas buscan algún patrón que sugiere el ataque de un intruso.

[18] Un intruso es alguien que trata de destruir el sistema desde dentro o darle un mal uso. Por darle un mal uso se entiende desde robar información confidencial hasta usar un correo para enviar correo spam.

- Deception system: contiene pseudo-servicios cuya meta es emular los agujeros ya conocidos para poder atrapar a los intrusos.

l) PGP (Pretty Good Privacy): es una aplicación ampliamente utilizada en todo el mundo, sobre todo por usuarios particulares, ya que se trata de un programa de cifrado de datos que incluye múltiples funciones de seguridad adicionales y de gestión de claves, permite intercambiar archivos y mensajes con seguridad y comodidad. Está basado en un conjunto de comandos muy sencillos y en la criptografía de clave pública. PGP puede utilizarse para firmar un mensaje, como un certificado de autenticidad y para enviar archivos a través de correo electrónico codificados en formato ASCII, esto proporciona servicios de autenticación y confidencialidad, tanto para el correo electrónico como para el almacenamiento de archivos.

m) Kerberos: es un protocolo de seguridad para realizar servicios de autenticación en la red, usa la criptografía basada en claves secretas para proporcionar la seguridad de las contraseñas en la red, por consiguiente, el cifrado de contraseñas con kerberos ayuda a evitar que los usuarios no autorizados intercepten contraseñas en la red, esto representa un método de seguridad del sistema. Es un proceso en el que diferentes elementos colaboran para conseguir identificar a un cliente que solicita un servicio ante un servidor que lo ofrece; asegura que las contraseñas nunca se envíen de manera clara a través de la red. Un uso correcto de kerberos erradica la amenaza de analizadores de paquetes que interceptan contraseñas en la red. Cada usuario tiene una clave y cada servidor también, por lo tanto, se tiene una base de datos que las contiene a todas. En el caso de ser de un usuario, su clave se deriva de su contraseña y está cifrada, mientras que en el caso del servidor, la clave se genera aleatoriamente. Los servicios de red que requieren autenticación y los usuarios que requieren estos servicios, se deben registrar con kerberos. Como éste conoce todas las claves privadas, puede crear mensajes que convencen a un servidor de que un usuario es realmente quien dice ser y viceversa.

n) Windows Privacy Tools (Herramientas de privacidad para Windows): es una colección de aplicaciones multilingües para facilitar el cifrado de contenidos –como el correo electrónico–, la firma digital y la gestión de claves. Se basa en GnuPG, que es compatible con aplicaciones que soportan OpenPGP (como PGP) y además es gratis para uso comercial y personal, bajo la licencia GPL.

o) Firewall: software que se instala en una computadora la cual es el intermediario entre la red local (correspondiente a la organización) y la red externa que por lo general es Internet, aunque también pueden existir firewalls entre diferentes redes dentro de una organización si así se desea.

Los firewalls funcionan con las dos siguientes filosofías:

- Dejar pasar a todas las redes exceptuando a las que no se desea.
- Negar el acceso a todas las redes y sólo permitir a las que se desea.

La selección de la filosofía también depende directamente de las necesidades identificadas y de las políticas que al respecto (control de acceso) se hayan escrito.

En la máquina donde se instale el firewall sólo debe existir ese software activo y no usarla para otras aplicaciones, ya que el firewall sólo es el puente de comunicación entre las redes local y externa y no debe haber otro trabajo realizándose ni ninguna otra información guardada, ya que en caso de que llegara a ser accedida por alguna persona no autorizada, sólo podría dañar al firewall, el cual no contiene información importante de la organización y podría reponerse de inmediato tapando el agujero por donde se infiltró el perpetrador.

p) Honeypots: es un recurso de cómputo diseñado para capturar todo el tráfico y actividad del sistema, cuenta con servicios de red comunes en conjunción con mecanismos de captura de tráfico de red, casi todos están diseñados para registrar y monitorear intrusos. Son diferentes de los sistemas regulares de una red, ya que éstos cuentan con mecanismos de registro y control de servicios. El objetivo es que los honeypots aparenten ser sistemas normales de producción, los cuales se encuentran proporcionando algún servicio, aunque en realidad son sistemas emulando a una cantidad de servicios y vulnerabilidades. Su propósito es capturar las actividades de los intrusos sin que ellos tengan conocimiento de que están siendo monitoreados y registrados. Esto no implica que un honeypot tenga el propósito de capturar intrusos. Los honeypots pueden ayudar a una organización a mejorar sus mecanismos de seguridad ya que pueden mostrar de manera fácil la cantidad de amenazas que circulan por Internet, además pueden ayudar a contrarrestar algunos ataques o bien a alimentar a otros mecanismos de protección como lo son los IDS o firewalls, al proporcionar información sobre distintas amenazas de seguridad en cómputo.

Existen muchas herramientas más, pero es recomendable sólo poner las que permitan llevar un mejor control del sistema y no saturarlo con herramientas que no se revisen o no sean útiles para ciertos fines. Después de este listado de herramientas, es necesario mapear para cada política escrita, la herramienta que permitirá hacerla cumplir, de otra manera desde aquí se puede estar dejando algún hueco de seguridad y crearle alguna vulnerabilidad al sistema.

Como se ha podido observar, existe una gran serie de herramientas que se pueden emplear para implantar el esquema de seguridad desarrollado, y aun cuando éstas no son todas ni las únicas que existen, sí son una amplia gama de posibilidades a estudiar y elegir aquellas que sean necesarias para el entorno