Vulnerar para proteger

Osvaldo Callegari
Analista de Sistemas
ocalle@ar.inter.net

Los intrusos utilizan diversas técnicas para quebrar los sistemas de seguridad de una red, buscando los puntos débiles del sistema. El trabajo de los Administradores no difiere mucho de esto. En lo que sí se diferencia es en los objetivos: mientras que un intruso penetra en las redes para distintos fines (daño, robo, etc.) un administrador lo hace para poder mejorar los sistemas de seguridad.

Al conjunto de técnicas que se utilizan para evaluar y probar la seguridad de una red se lo conoce como Penetration Testing, uno de los recursos más poderosos con los que se cuenta hoy para generar barreras cada vez más eficaces.

Administración de la Seguridad

Al conjunto de técnicas que se utilizan para evaluar y probar la seguridad de una red se lo conoce como Penetration Testing, uno de los recursos más poderosos con los que se cuenta hoy para generar barreras cada vez más eficaces.

Es posible dividir las tareas de administración de seguridad en tres grandes grupos:

• **Autenticación:** se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.

• **Autorización:** es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.

• **Auditoría:** se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este grupo el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su "*voluntad de hacer algo*" que permita detener un posible ataque antes de que éste suceda (proactividad). A continuación se citan algunos de los métodos de protección más comúnmente empleados.

1. Sistemas de detección de intrusos: son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados. Pueden considerarse como monitores.

2. Sistemas orientados a conexión de red: monitorizan las conexiones que se intentan establecer en una red o equipo en particular, siendo capaces de efectuar una acción sobre la base de métricas como origen y destino de la conexión, servicio solicitado, permisos, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador. En esta categoría están los cortafuegos *(Firewalls)* y los Wrappers.

3. Sistemas de análisis de vulnerabilidades: analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La "*desventaja*" de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por aquellas que buscan acceso no autorizado al sistema.

4. Sistemas de protección a la integridad de información: sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como *Message Digest* (MD5) o *Secure Hash Algorithm* (SHA), o bien sistemas que utilizan varios de ellos como PGP, *Tripwire* y *DozeCrypt*.

5. Sistemas de protección a la privacidad de la información: herramientas que utilizan criptografía para asegurar que la información solo sea visible para quien tiene autorización. Su aplicación se realiza principalmente en las comunicaciones entre dos entidades. Dentro de este tipo de herramientas se pueden citar a *Pretty Good Privacy* (PGP), *Secure Sockets Layer* (SSL) y los *Certificados Digitales*.

Resumiendo, un modelo de seguridad debe estar formado por múltiples componentes o capas que pueden ser incorporadas de manera progresiva al modelo global de seguridad en la organización, logrando así el método más efectivo para disuadir el uso no autorizado de sistemas y servicios de red. Estas capas son:

1. Política de seguridad.
2. Auditoría.
3. Sistemas de seguridad a nivel de Router-Firewall.
4. Sistemas de detección de intrusos.
5. Plan de respuesta a incidentes.
6. Penetration Test.

Penetration Test, Ethical Hacking o Prueba de Vulnerabilidad

El *Penetration Test* es un conjunto de metodologías y técnicas, para realizar una evaluación integral de las debilidades de los sistemas informáticos. Consiste en un modelo que reproduce intentos de acceso a cualquier entorno informático, de un intruso potencial des-

Continúa en página 202

Continúa en página 198

de los diferentes puntos de entrada que existan, tanto internos como remotos.

El objetivo general del *Penetration Test* es acceder a los equipos informáticos de la organización tratada e intentar obtener los privilegios del administrador del sistema, logrando así realizar cualquier tarea sobre dichos equipos. También se podrá definir otros objetivos secundarios que permitan realizar pruebas puntuales sobre algunos ámbitos particulares de la empresa.

El *Penetration Test* se compone de dos grandes fases de testeo:

1. Test Externo: el objetivo es acceder en forma remota a los equipos de la organización y posicionarse como administrador del sistema. Se realizan desde fuera del *Firewall* y consisten en penetrar la *Zona Desmilitarizada* para luego acceder a la red interna.

2. Test Interno: este tipo de testeo trata de demostrar cual es el nivel de seguridad interno. Se deberá establecer que puede hacer un *Insider* (operadores, programadores) y hasta donde será capaz de penetrar en el sistema siendo un usuario con privilegios bajos.

Penetration Test

Estos test se componen de un elevado número de pruebas, entre las que se puede nombrar:

Test Externo:

- Pruebas de usuarios y la "*fuerza*" de sus passwords.
- Captura de tráfico.
- Detección de conexiones externas y sus rangos de direcciones.
- Detección de protocolos utilizados.
- Canning de puertos TCP, UDP e ICMP.
- Intentos de acceso vía accesos remotos, módems, Internet, etc.
- Análisis de la seguridad de las conexiones con proveedores, trabajadores remotos o entidades externas a la organización.
- Pruebas de vulnerabilidades existentes y conocidas en el momento de realización del Test.
- Prueba de ataques de Denegación de Servicio.

Test Interno:

- Análisis de protocolos internos y sus vulnerabilidades.
- Autenticación de usuarios.
- Verificación de permisos y recursos compartidos.
- Test de los servidores principales (WWW, DNS, FTP, SMTP, etc.)
- Test de vulnerabilidad sobre las aplicaciones propietarias.
- Nivel de detección de la intrusión de los sistemas.
- Análisis de la seguridad de las estaciones de trabajo.
- Seguridad de la red.
- Verificación de reglas de acceso.
- Ataques de Denegación de Servicio

HoneyPots-HoneyNets

Estas "*Trampas de Red*" son sistemas que se activan con la finalidad específica de que los *honeynets* expertos en seguridad puedan observar en secreto la actividad de los Hackers.

Consisten en activar un servidor y llenarlo de archivos tentadores, hacer que sea difícil, pero no imposible penetrarlo y sentarse a esperar que aparezcan los intrusos. Los *Honeynets* dan a los Hackers un gran espacio para recorrer. Presentan obstáculos que poseen el nivel de complejidad suficiente para atraerlos, pero sin irse al extremo para no desalentarlos. Ellos juegan con los archivos y conversan animadamente entre ellos, mientras el personal de seguridad observa con deleite cada movimiento que hacen.

Esta última frase se está presentando a menudo en el tema de la investigación y vigilancia electrónica. Este es el caso del *ex-director del proyecto Honeynet J. D. Glaser*, quien renunció a su puesto después de aclarar que está convencido de que "*la vigilancia electrónica no es correcta, aunque se utilice en aras de la investigación, un Honeynet es parecido a entrampar los derechos de otros, aunque sean los derechos de un delincuente.*" ☒

Fuente: www.segu-info.com.ar