Herramientas de Protección

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

Conocidas las vulnerabilidades y los ataques a los que está expuesto un sistema es necesario saber de que recursos disponemos para protegerlo. Muchas de las vulnerabilidades de un sistema son el resultado de la implementación incorrecta de tecnologías y la falta de planeamiento de las mismas.

En el presente capítulo, luego de lo expuesto y vistas la gran cantidad de herramientas con las que cuenta el intruso para vulnerar nuestro sistema, es el turno de mencionar en resumen, implementaciones en la búsqueda de mantener el sistema seguro, las cuales iremos ampliando en sucesivas entregas.

Introducción

Los protocolos de comunicación utilizados carecen (en su mayoría) de seguridad o esta ha sido implementada en forma de "*parche*" tiempo después de su creación.

- Existen agujeros de seguridad en los sistemas operativos.
- Existen agujeros de seguridad en las aplicaciones.
- Existen errores en las configuraciones de los sistemas.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un Sistema Informático.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. *Los Insiders* (operadores, programadores, Data entry) utilizaban sus permisos para alterar archivos o registros. *Los Outsiders* ingresaban a la red simplemente averiguando una password válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "*agujeros*" en el diseño, configuración y operación de los sistemas.

Ninguna de las técnicas expuestas a continuación representarán el 100% de la seguridad deseada, aunque muchas parezcan la panacea, será la suma de algunas de ellas las que convertirán un sistema interconectado en confiable.

Vulnerar Para Proteger

Los intrusos utilizan diversas técnicas para quebrar los sistemas de seguridad de una red, buscando los puntos débiles del sistema para poder colarse en ella. El trabajo de los *Administradores y Testers* 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.

Un *test* está totalmente relacionado con el tipo de información que se maneja en cada organización. Por consiguiente, según la información que deba ser protegida, se determinan la estructura y las herramientas de seguridad; no a la inversa.

Firewalls

Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad.

Un *Firewall* es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

Access Control Lists (ACL)

Las *Listas de Control de Accesos* proveen de un nivel de seguridad adicional a los clásicos provistos por los Sistemas Operativos. Estas listas permiten definir permisos a usuarios y grupos concretos. Por ejemplo, pueden definirse sobre un *Proxy* una lista de todos los usuarios (o grupos de ellos) a quien se le permite el acceso a Internet, FTP, etc. También podrán definirse otras características como limitaciones de anchos de banda y horarios.

Wrappers

Un *Wrapper* es un programa que controla el acceso a un segundo programa. El *Wrapper* literalmente cubre la identidad de este segundo programa, obteniendo con esto un más alto nivel de seguridad. Los *Wrappers* son usados dentro de la seguridad en sistemas *UNIXs*. Estos programas nacieron por la necesidad de modificar el comportamiento del sistema operativo sin tener que modificar su funcionamiento.

Los *Wrappers* son ampliamente utilizados y han llegado a formar parte de las herramientas de seguridad por las siguientes razones:

- Debido a que la seguridad lógica está concentrada en un solo programa, los *Wrappers* son fáciles y simples de validar.
- Debido a que el programa protegido se mantiene como una entidad separada, éste puede ser actualizado sin necesidad de cambiar el *Wrapper.*
- Debido a que los *Wrappers* llaman al programa protegido mediante llamadas estándar al sistema, se puede usar un solo *Wrapper* para controlar el acceso a diversos programas que se necesiten proteger.

Continúa en página 204

Continúa en página 200

• Permite un control de accesos exhaustivo de los servicios de comunicaciones, además de buena capacidad de Logs y auditorías de peticiones a dichos servicios, ya sean autorizados o no.

El paquete *Wrapper* más ampliamente utilizado es el *TCP Wrappers*, el cual es un conjunto de utilidades de distribución libre.

Consiste en un programa que es ejecutado cuando llega una petición a un puerto específico. Este, una vez comprobada la dirección de origen de la petición, la verifica contra las reglas almacenadas, y en función de ellas, decide o no dar paso al servicio. Adicionalmente, registra estas actividades del sistema, su petición y su resolución.

Con lo mencionado hasta aquí, puede pensarse que los *Wrappers* son *Firewalls* ya que muchos de los servicios brindados son los mismos o causan los mismos efectos. Usando *Wrappers*, se puede controlar el acceso a cada máquina y a los servicios accedidos. Así, estos controles son el complemento perfecto de un *Firewall* y la instalación de uno no está supeditada a la del otro.

Detección de Intrusos en Tiempo Real

La integridad de un sistema se puede corromper de varias formas y la forma de evitar esto es con la instalación de *Sistemas de Detección de Intrusos en Tiempo Real*, quienes:

• Inspeccionan el tráfico de la red buscando posibles ataques.

• Controlan el registro de los servidores para detectar acciones sospechosas *(tanto de intrusos como de usuarios autorizados).*

• Mantienen una base de datos con el estado exacto de cada uno de los archivos *(Integrity Check)* del sistema para detectar la modificación de los mismos.

• Controlan el ingreso de cada nuevo archivo al sistema para detectar *Troyanos* o semejantes.

• Controlan el núcleo del Sistema Operativo para detectar posibles infiltraciones en él, con el fin de controlar los recursos y acciones del mismo.

• Avisan al administrador de cualquiera de las acciones mencionadas.

Cada una de estas herramientas permiten mantener alejados a la gran mayoría de los intrusos normales. Algunos pocos, con suficientes conocimientos, experiencia y paciencia serán capaces de utilizar métodos sofisticados como para voltear el perímetro de seguridad (interna + externa) y serán estos los casos que deban estudiarse para integrar a la política de seguridad existente mayor seguridad.

Call Back

Este procedimiento es utilizado para verificar la autenticidad de una llamada vía modem. El usuario llama, se autentifica contra el sistema, se desconecta y luego el servidor se conecta al número que en teoría pertenece al usuario.

La ventaja reside en que si un intruso desea hacerse pasar por el usuario, la llamada se devolverá al usuario legal y no al del intruso, siendo este desconectado. Como precaución adicional, el usuario deberá verificar que la llamada - retorno proceda del número a donde llamó previamente.

Sistemas Anti-Sniffers

Esta técnica consiste en detectar *Sniffers* en el sistema. Generalmente estos programas se basan en verificar el estado de la placa de red, para detectar el modo en el cual está actuando (recordar que un Sniffer la coloca en Modo Promiscuo) y el tráfico de datos en ella.

Gestión de Claves "Seguras"

Si se utiliza una clave de 8 caracteres de longitud, con los 96 caracteres posibles, puede tardarse 2.288 años en descifrarla (analizando 100.000 palabras por segundo). Partiendo de la premisa en que no se disponen de esa cantidad de años para analizarlas por fuerza bruta, se deberá comenzar a probar con las claves más posibles, comúnmente llamadas *Claves Débiles.*

Criptología

La palabra Criptografía proviene etimológicamente del griego *Kruiptoz* (Kriptos- Oculto) y *Grajein* (Grafo - Escritura) y significa "*arte de escribir con clave secreta o de un modo enigmático*".

Aportando luz a la definición cabe aclarar que la Criptografía hace años que dejó de ser un arte para convertirse en una técnica (o conjunto de ellas) que tratan sobre la protección (ocultamiento ante personas no autorizadas) de la información. Entre las disciplinas que engloba cabe destacar la Teoría de la Información, la Matemática Discreta, la Teoría de los Grandes Números y la Complejidad Algorítmica.

Es decir que la Criptografía es la ciencia que consiste en transformar un mensaje inteligible en otro que no lo es (mediante claves que sólo el emisor y el destinatario conocen), para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado sea capaz de entenderlo.

Inversión

Los costos de las diferentes herramientas de protección se están haciendo accesibles, en general, incluso para las organizaciones más pequeñas. Esto hace que la implementación de mecanismos de seguridad se de prácticamente en todos los niveles: empresas grandes, medianas, chicas y usuarios finales. Todos pueden acceder a las herramientas que necesitan y los costos (la inversión que cada uno debe realizar) va de acuerdo con el tamaño y potencialidades de la herramienta.

Pero no es sólo una cuestión de costos, los constantes cambios de la tecnología hacen que para mantener un nivel parejo de seguridad, se deba actualizar permanentemente las herramientas con las que se cuenta. Como los intrusos mejoran sus armas y metodologías de penetración de forma incesante, el recambio y la revisión constantes en los mecanismos de seguridad se convierten en imprescindibles. Y éste es un verdadero punto crítico.

Según *Testers*, "*esto es tan importante como el tipo de elementos que se usen*". Sin duda, éstos deben ser las que mejor se adapten al tipo de organización. Pero tan importante como eso es el hecho de conocer exactamente cómo funcionan y qué se puede hacer con ellos. "*Es prioritario saber los riesgos que una nueva tecnología trae aparejados*".

Fuente: www.segu-info.com.ar