Procedimientos estandarizados de Testing de Seguridad en Redes

Santiago Pérez, Higinio Facchini, Carlos Taffernaberry, Gustavo Mercado, Luis Bisaro
{santiago.perez, higinio.facchini, carlos.taffe, gustavo.mercado, luis.bisaro}@gridtics.frm.utn.edu.ar
GRID TICs
(Grupo de Investigación y Desarrollo en TICs)
Facultad Regional Mendoza,
Universidad Tecnológica Nacional
Mendoza Argentina
0261-5244576

Resumen

La seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado. Y mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad. La confidencialidad es que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades. La integridad significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada. Y la disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; es el contrario de la negación de servicio. Generalmente tienen que existir los tres aspectos descritos para que haya seguridad. Las pruebas de seguridad o testing de seguridad son los procesos que permiten verificar o revelar la calidad de la seguridad. La línea de investigación se desarrolla a través de los siguientes objetivos: 1) Identificar y clasificar los aspectos o rubros de seguridad y vunerabilidad en la redes, 2) Identificar los procedimientos asociados, 3) Compilar y clasificar herramienta hardware y software de testing de seguridad, 4) Efectuar Caso de Estudio experimental de seguridad, 5) Elaborar procedimientos estandarizados de testing.

Palabras claves: testing, seguridad, procesos, redes

1 INTRODUCCIÓN

Cada vez es más habitual que las empresas contraten los servicios de seguridad de una compañía externa, especializada en la materia, y que le permita olvidarse de los aspectos técnicos y organizativos de la seguridad, para poder centrarse así en su línea de negocio correspondiente. Esta política es lo que se conoce como externalización, aplicado en este caso a la seguridad corporativa. La seguridad en sí misma no es ningún fin, sino una herramienta al servicio de los negocios de la empresa, y por lo tanto, los esfuerzos han sido orientados a proteger el patrimonio humano, tecnológico, y económico de la misma. El director de una gran firma probablemente no conozca las implementaciones de cortafuegos o del sistema distribuido de detección de intrusos, pero si esté interesado en la seguridad, después que un atacante haya podido acceder a información crítica de esa compañía.

¿Por qué va a querer una empresa determinada que personas ajenas a la misma gestionen su seguridad? Especialmente si estamos hablando de la protección de muchos activos de la compañía, y encomendando esa tarea tan crítica a un tercero. Existen diferentes motivos para llegar a externalizar nuestra seguridad. Permite a la empresa que lo contrata despreocuparse relativamente de su seguridad para centrarse en sus líneas de negocio. Además, al contratar a personal especializado en la seguridad se consigue un nivel mayor de protección, tanto por el factor humano que ha de tener gente con un alto nivel en diferentes materias de seguridad para poder ofrecer correctamente sus servicios, como técnico dado que dispondrá también de productos y sistemas más específicos.

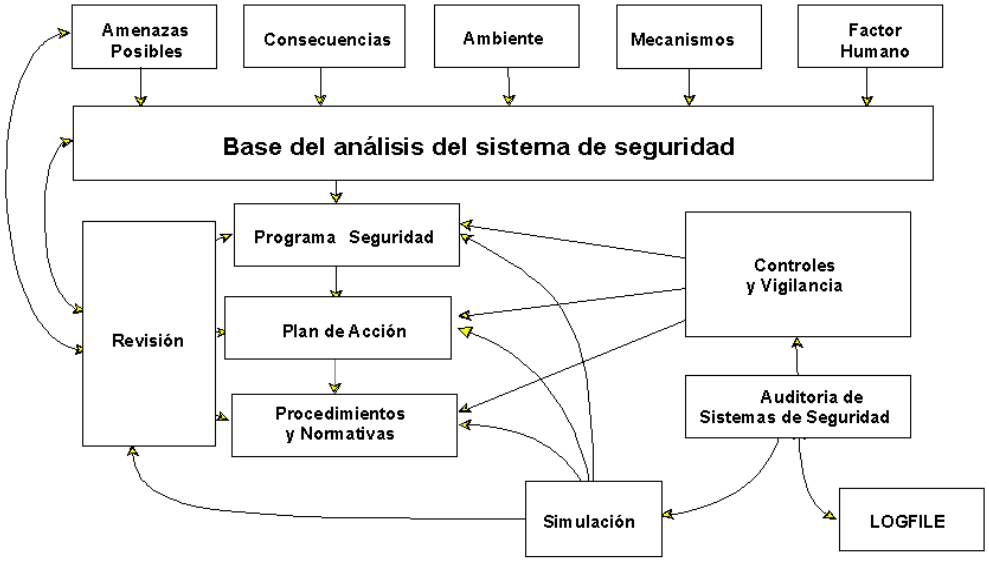
Cuanto más alejada de las nuevas tecnologías se encuentre la línea de negocio de una determinada empresa, más recomendable suele ser para la misma adoptar una solución de externalización. Es habitual que el nivel de externalización sea mayor conforme la empresa contratante se aleje del mundo de las nuevas tecnologías, contemplando un amplio abanico que abarca desde la gestión de elementos concretos de protección o auditorías y pruebas (testing) de penetración puntuales, hasta soluciones de externalización total. En cualquier caso, la empresa no debería despreocuparse totalmente de la gestión de la seguridad, recibiendo como poco un informe mensual que la mantenga al día de cualquier aspecto relevante que afecte a su seguridad.

¿Qué áreas de la seguridad conviene externalizar? Evidentemente, no existe una respuesta universal a esta pregunta. Existen áreas que por su delicadez o criticidad no conviene casi nunca dejar en manos de terceros, como es el caso de la realización y verificación de backups. No obstante, elementos importantes, pero no críticos como las pruebas de penetración, de visibilidad o las auditorías de vulnerabilidades, habitualmente se suelen externalizar, ya que incluso existen empresas de seguridad especializadas en este tipo de acciones. Otro ejemplo de área a externalizar puede ser la gestión de los cortafuegos corporativos. En definitiva, no se puede dar un listado donde se indiquen por orden las prioridades de externalización, ya que es algo que depende completamente de cada compañía y entorno. Normalmente es el personal de la propia compañía, asesorado por consultores de seguridad y por abogados, quien decida qué y de qué forma gestionar en externalización.

2 DIAGRAMA DE UN SISTEMA DE SEGURIDAD

Tal como puede visualizarse, en el gráfico están plasmados todos los elementos que intervienen para el estudio de una política de seguridad. Se comienza realizando una evaluación del factor humano interviniente - teniendo en cuenta que éste es el punto más vulnerable en toda la cadena de seguridad -, de los mecanismos con que se cuentan para llevar a cabo los procesos necesarios (mecanismos técnicos, físicos ó lógicos). Y luego, del medio ambiente en que se desempeña el sistema, las consecuencias que puede traer aparejado defectos en la seguridad (pérdidas físicas, pérdidas económicas, en la imagen de la organización, etc.), y cuáles son las amenazas posibles.

Una vez evaluado todo lo anterior, se origina un programa de seguridad, que involucra los pasos a tomar para poder asegurar el umbral de seguridad que se desea. Luego, continúa el plan de acción, que es cómo se va a llevar a cabo el programa de seguridad. Finalmente, se redactan los procedimientos y normas que permiten llegar a buen destino.
Con el propósito de asegurar el cumplimiento de todo lo anterior, se realizan los controles y la vigilancia que aseguran el fiel cumplimiento de los tres puntos antepuestos. Para asegurar un marco efectivo, se realizan auditorías a los controles y a los archivos logísticos que se generen en los procesos implementados.
Con el objeto de confirmar el buen funcionamiento de lo creado, se procede a simular eventos que atenten contra la seguridad del sistema. Como el proceso de seguridad es un proceso dinámico, es necesario realizar revisiones al programa de seguridad, al plan de acción y a los procedimientos y normas. Estas revisiones, tendrán efecto sobre los puntos tratados en el primer párrafo y, de esta manera, el proceso se vuelve a repetir.
Es claro que el establecimiento de políticas de seguridad es un proceso dinámico sobre el que hay que estar actuando permanentemente, de manera tal que no quede desactualizado; que, cuando se le descubran debilidades, éstas deben subsanarse y, finalmente, que su práctica por los integrantes de la organización no caiga en desuso.



3 ALGUNOS TIPOS DE ATAQUES Y VULNERABILIDADES

Hay numerosos ejemplos de ataques y vulnerabilidades respecto a redes que se citan en distintas bibliografías. A continuación citamos algunas de ellas, como pueden ser:

Denegación de Servicio (Denial of service)

Es un tipo de ataque cuya meta fundamental es la de negar el acceso del atacado a un recurso determinado o a sus propios recursos.
Algunos ejemplos de este tipo de ataque son:

- tentativas de inundar una red con tráfico espúreo, evitando de esta manera el tráfico legítimo de datos en la misma;
- tentativas de evitar que una determinada persona tenga acceso a un servicio;
- tentativas de interrumpir un servicio específico a un sistema o a un usuario;

Averiguación de contraseñas (Cracking de passwords)

es un proceso informático que consiste en descifrar la contraseña de determinadas aplicaciones elegidas por el usuario. Se busca codificar los códigos de cifrado en todos los ámbitos de la informática. Se trata del rompimiento o desciframeinto de claves (passwords).

Bombardeo de correos electrónicos (e-mail bombing)

Consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando la casilla de correo del destinatario. El spamming, que es una variante del anterior, se refiere a enviar el email a centenares o millares de usuarios e, inclusive, a listas de interés. El Spamming puede resultar aún más perjudicial si los destinatarios contestan el mail manualmente o por un autorespondedor, haciendo que todos reciban la respuesta.

El e-mail bombing/spamming se puede combinar con el e-mail spoofing que altera la identidad de la cuenta que envía el mail -, logrando que sea más difícil determinar quién envía realmente el mail.

Problemas de seguridad en el FTP El comando PORT

En los últimos años, se ha incrementado el debate en torno a los problemas relacionados con el comando PORT del protocolo del FTP. Estos problemas se basan el uso erróneo de dicho comando.

TFTP

El Trivial File Transport Protocol (TFTP) es un mecanismo sencillo de transferencia de archivos basado en UDP. Este protocolo no tiene autenticación, constituyendo un potencial problema de seguridad.

TELNET

TELNET provee acceso de terminal a un sistema. Generalmente, el demonio de telnet llama al programa login para autenticar al usuario e iniciar la sesión. El mismo provee un nombre de cuenta y una password para el login.

Su mayor problema es de seguridad, ya que todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajan por la red como *texto plano* (cadenas de texto sin cifrar). Esto facilita que cualquiera que espíe el tráfico de la red pueda obtener los nombres de usuario y contraseñas, y así acceder él también a todas esas máquinas.

4 HERRAMIENTAS DE CONTROL Y SEGUIMIENTO DE ACCESO

En este apartado enumeramos algunas herramientas que permiten tener una información - mediante archivos de trazas o logísticos - de todos los intentos de conexión que se han producido sobre nuestro sistema o sobre otro que nosotros hayamos señalado, así como intentos de ataque de forma sistemática a puertos tanto de TCP como de UDP.

Este tipo de herramientas nos permite tener un control sobre todos los paquetes que entran por la interfaz de red de la máquina: IP (TCP, UDP) e ICMP, o analizando paquetes a nivel de aplicaciones (TELNET, FTP, SMTP, LOGIN, SHELL, etc.). Pueden ser utilizadas junto con otras que nos permitan definir desde qué máquinas permitimos ciertas conexiones y cuales se prohíben. Algunas no necesitan estar instaladas en la máquina que se quiere controlar, ya que se puede poner en una máquina cuya interfaz de red funcione en modo promiscuo, permitiendo seleccionar la dirección IP o máquina que queremos auditar. O pueden tener un doble uso. Es decir, nos permiten protegernos ante posibles ataques, pero también podrían ser utilizadas para intentar comprometer los sistemas. Por eso es importante que el uso de estas herramientas esté restringido - en la manera que se pueda - para que no todo el mundo esté utilizándolas de forma aleatoria y nos oculten realmente un ataque.

Algunos ejemplos que permiten este tipo de operatividad son:

tcp-wrappers

Es un software de domino público desarrollado por Wietse Venema (Universidad de Eindhoven, Holanda). Su función principal es: proteger a los sistemas de conexiones no deseadas a determinados servicios de red, permitiendo a su vez ejecutar determinados comandos ante determinadas acciones de forma automática.

Netlog
Este software de dominio público diseñado por la Universidad de Texas, es una herramienta que genera trazas referentes a servicios basados en IP (TCP, UDP) e ICMP, así como tráfico en la red (los programas pueden ejecutarse en modo promiscuo) que pudiera ser "sospechoso" y que indicara un posible ataque a una máquina (por la naturaleza de ese tráfico).

argus
Es una herramienta de dominio público que permite auditar el tráfico IP que se produce en nuestra red, mostrándonos todas las conexiones del tipo indicado que descubre. Este programa se ejecuta como un demonio, escucha directamente la interfaz de red de la máquina y su salida es mandada bien a un archivo de trazas o a otra máquina para allí ser leída. En la captura de paquetes IP se le puede especificar condiciones de filtrado como protocolos específicos, nombres de máquinas, etc.

tcpdump
Es un software de dominio público que imprime las cabeceras de los paquetes que pasan por una interfaz de red, al ejecutarlo en modo promiscuo. Tanto en la captura como en la visualización de la información, es posible aplicar filtros por protocolo (TCP, UDP, IP, ARP, RARP...), puertos, direcciones fuente, direcciones destino, direcciones de red, así como realizar filtros con operadores (=, <, >, !=, and, not, ...). En la última versión, es posible ver también los paquetes de datos.

SATAN (Security Administrator Tool for Analyzing Networks)
Es un software de dominio público creado por Dan Farmer que chequea máquinas conectadas en red y genera información sobre el tipo de máquina, qué servicios da cada máquina y avisa de algunos fallos de seguridad que tengan dichas máquinas. Una de las ventajas de SATAN frente a otros paquetes, es que utiliza una interfaz WEB, va creando una base de datos de todas las máquinas chequeadas y las va relacionando entre ellas (de forma que si encuentra una máquina insegura, y chequea otra máquina que está relacionada con ésta, automáticamente esta segunda quedará marcada también como insegura). Además, tiene la posibilidad de poder chequear las máquinas con tres niveles ("light", normal y "heavy"). Una vez realizado el chequeo de la máquina se genera una salida en formato html, y en el caso de encontrar fallos, da una pequeña explicación sobre el fallo en concreto. Cuando existe algún documento sobre ese fallo recogido en el CERT (advisory) tiene un enlace a ese documento, para que sobre la marcha pueda ser consultado.

ISS (Internet Security Scanner)
Es una herramienta de la cual existe versión de dominio público que chequea una serie de servicios para comprobar el nivel de seguridad que tiene esa máquina. ISS es capaz de chequear una dirección IP o un rango de direcciones IP (en este caso se indican dos direcciones IP e ISS chequeará todas las máquinas dentro de ese rango). El programa viene acompañado de dos utilidades que son ypx y strobe. La primera, nos permite la transferencia de mapas NIS a través de la red y la segunda, chequea y describe todos los puertos TCP que tiene la máquina que chequeamos. Como podemos ver, con la primera herramienta es posible la transferencia de los archivos de "password" en aquellas máquinas que hayan sido configuradas como servidores de NIS. ISS se puede ejecutar con varias opciones y la salida se deja en un archivo.

Courtney
Este software de dominio público sirve para identificar la máquina origen que intenta realizar ataques mediante herramientas de tipo SATAN. El programa es un script perl que trabaja conjuntamente con tcpdump. Courtney recibe entradas desde tcpdump y controla la presencia de peticiones a nuevos servicios del stack TCP/IP (las herramientas de este tipo realizan ataques, chequeando de forma ordenada todos los puertos TCP y UDP que tiene el sistema, para poder ver qué servicios tiene instalados dicha máquina). Si se detecta que se está produciendo un continuo chequeo de estos puertos en un breve intervalo de tiempo, Courtney da un aviso. Este aviso se manda vía syslog. Courtney puede generar dos tipos de alarmas dependiendo del ataque que se esté produciendo (normal o "heavy"). Esta herramienta necesita el intérprete de PERL y el tcpdump.

Gabriel

Software desarrollado por "Los Altos Technologies Inc" que permite detector "ataques" como los generados por SATAN. Gabriel identifica el posible ataque y de forma inmediata lo notifica al administrador o responsable de seguridad. La notificación se puede realizar de varias formas (e-mail, cu, archivo de trazas). Este programa está formado por un cliente y un servidor. El cliente se instala en cualquier máquina de la red, recoge la información que se está produciendo y la envía al servidor vía syslog. Estos clientes además envían de forma regular información al servidor para indicarle que están en funcionamiento.

nocol (Network Operations Center On-Line)

Es un conjunto de programas de monitoreo de sistemas y redes. El software es un conjunto de agentes que recogen información y escriben la salida en un formato que se puede, luego, procesar. Cada dato procesado recibe el nombre de evento y cada evento tiene asociado una gravedad. Existen cuatro niveles de gravedad: CRITICAL, ERROR, WARNING, INFO. Cada uno de estos niveles es controlado de forma independiente por cada agente. Existe un conjunto de herramientas que nos permite ver toda la información generada por los agentes y que puede ser filtrada dependiendo de la gravedad del evento.

5 CONCLUSION

En este documento, se han relacionado los temas de diagrama de seguridad, vulnerabilidad, testing y procesos normalizados de seguridad en redes. El volumen de los trabajos y literatura sobre seguridad de redes es creciente.

En la investigación se pretende proponer procedimientos normalizados de testing para la cuantificación de las vulnerabilidades, y su reparación y/o mantenimiento, en la seguridad de redes.

6 REFERENCIAS

Auditoría, Evaluación, Test de Seguridad – Metodología abierta - ¿OSSTMM…? Alejandro Corletti Estrada – Universidad Politécnica de Madrid, noviembre de 2005

http://www.abast.es/integrityit/test_intrusion.shtml

Instituto para la Seguridad y las Metodologías Abiertas. – www.isecom.org.

Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional – Oficina Nacional de Tecnologías de Información – SGP – www.sgp.gob.ar

Una guía metodológica para el cálculo de retorno de inversión en seguridad informática –Nicolas Sanchez Acevedo y Juan Segura Castañeda – Facultad de Ingeniería de Pontificia Universidad Javeriana – Bogotá – Junio de 2006

http://www.osstmm.org

http://www.inteco.es

http:// http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf

http:// http://www.baxware.com/auditoria-test-intrusion.htm