Test de penetración como apoyo a la evaluación de riesgos en seguridad de la información

Penetration test on the support of risk evaluation on information security

***Enrique Javier Santiago Chinchilla**

** Ingeniero de sistemas (Universidad Autónoma del Caribe), Egresado Sobresaliente, especialista en redes de computadoras, Universidad del norte, especialista en sistemas de telecomunicaciones, Máster en Telecomunicaciones de la universidad de Vigo (España), D.E.A en Ingeniería Telemática, Estudiante de doctorado en ingeniería telemática, Universidad de Vigo (España).*

RESUMEN

El propósito de este instrumento es presentar un punto de vista técnico asociado a la productividad corporativa y a las situaciones que propicia la dependencia de tecnología en las empresas del siglo XXI. Dando a conocer las técnicas utilizadas por los equipos de seguridad de la información para testear el grado de riesgo a que esta expuesto cualquier sistema informático en la actualidad.

Palabras clave: I+D, hacker, Cracker, 0-days, CISO, CEO,CIO, SQL, penetración.

ABSTRACT

The intention of this instrument is to present a technical point of view associated with the corporate productivity and with the situations that propitiates the dependence of technology in the companies of the 21st century. Announcing the technologies used by the teams of safety of the information for testear the level of risk to which this exposed any computer system at present.

Key words: I+D, hacker, Cracker, 0-days, CISO, CEO,CIO, SQL, penetration.

1. Introducción

No puede negarse que las unidades de I+D de muchas organizaciones mundiales lideres en tecnología han apoyado el crecimiento de las herramientas tecnológicas que hoy en día soportan el 99% de las operaciones corporativas y de negocios.

Todas las empresas comerciales del siglo XXI soportan sus operaciones contables en sistemas de información e integran su plataforma de comunicaciones con Internet. El 97% de las transacciones bancarias, operaciones bursátiles, administración de los procesos operacionales, operaciones en cuanto a fuerza de ventas e incluso muchos servicios médicos de la nueva era, están soportados por tecnología informática y de telecomunicaciones [6].

El uso de tecnología como apoyo a la operatividad de las organizaciones hace más competitivas a las empresas, ya que a través de esta se puede brindar productos y servicios de mejor calidad y en muchos casos la atención puede hacerse en tiempo real. Pero también hace dependientes a las unidades de negocios de las herramientas de apoyo tecnológico, de manera que la competitividad basada en TIC es proporcional a la dependencia de ellas.

Es innegable que este siglo ha sido catalogado como el siglo de la información [1], por eso precisamente los datos y la información misma se han convertido en el activo más importante de las empresas pertenecientes a la era de la revolución informática. Debido a esto la información y sus cualidades principales: disponibilidad, confidencialidad e integridad son vitales para las operaciones de cualquier negocio, incluso de la garantía de las mismas depende en gran porcentaje la competitividad y el crecimiento de las compañías, ya que si algún componente de negocios en línea no dispone del flujo de información correcto en el momento adecuado, la transacción no podría llevarse a cabo haciendo imposible realizar la operación comercial.

La interconectividad realmente se ha convertido en una herramienta irremplazable en el mundo de los negocios, tanto así que ha llegado a afirmarse que la empresa que no este "conectada" a la red de redes (Internet) está destinada a fracasar [9]. La situación de dependencia tecnológica es derivada de la Telemática que ha permitido la integración de las tecnologías de las telecomunicaciones con las soluciones informáticas, estas últimas cada vez más escalables y más fáciles de usar. Gracias a la Telemática muchos fabricantes y organizaciones líderes en tecnología han apuntado acertadamente a la fabulosa convergencia de servicios, la cual hoy en día permite que usted pague sus tarjetas de crédito a través de su teléfono móvil, que lea su correo electrónico a través de su televisor o que pueda consultar a su médico de cabecera desde su computadora de escritorio; no puede negarse que gracias a la tecnología hoy hacemos las tareas de la vida diaria de forma más fácil.

Pero no todo es color rosa, ya que la integración de plataformas de servicios, las nuevas arquitecturas orientadas a servicios y los nuevos desarrollo de software intuitivos; fácilmente acoplables e integrables entre sí, con requerimientos mínimos de interacción con el usuario apuntando siempre a la automatización de tareas; no sólo hacen fácil la vida al usuario convencional sino que también facilitan el acceso a los recursos tecnológicos y a la información misma a los vándalos informáticos conocidos como crackers y porque no "Hackers".

2. Metodología

El tipo de investigación utilizado en este proyecto es la "Investigación experimental", esta integrada por un conjunto de actividades metódicas y técnicas que se realizan para recabar en la evaluación de riesgos en seguridad de la información a través de un test de penetración.

En primera instancia se define el marco teórico relacionado con el tema y posteriormente ejecutar el test de penetración que será analizado por especialistas

3. Marco Teórico

3.1 Efectos de la dependencia tecnológica.

El problema de la dependencia tecnológica no apunta al uso de estas herramientas, sino al grado de riesgo que asume la compañía asociado a la vulnerabilidad de los productos que soportan sus operaciones.

Mientras más vulnerables sean los productos que soportan las operaciones de negocios corporativos, mayor será el grado de riesgo que asume la compañía que haga uso de esos. Obviamente cualquier compromiso de seguridad Informática, significativo de algún componente tecnológico de la infraestructura de la compañía, será reflejado en el proceso que este soporta.

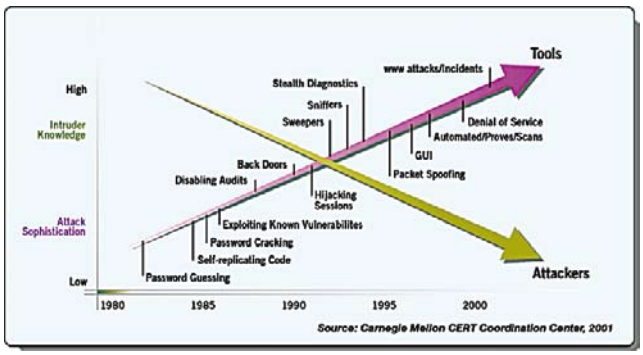
Tanto para hacker como Crackers, años atrás la característica común apuntaba al dominio de un gran conocimiento sobre tecnología aunque el diferencial entre ellos sigue siendo el beneficio propio o de un tercero y el reto mismo respectivamente.

La época en que pocos dominaban el conocimiento tecnológico y computacional debido a la dificultad en la construcción y operación de unos pocos sistemas conectados ha sido sucedida por la era del conocimiento público de los nuevos sistemas "intuitivos" denominados de fácil uso, en la que cualquier persona prácticamente de cualquier edad con dominio básico del acceso a Internet y con el uso de algunas herramientas de software puede realmente convertirse en una gran amenaza para la compañía, ya que con sólo haber descargado la suite de Hacking correcta (que hoy día disparan ataques con un click a un blanco alcanzable vía Internet - sólo por citar un ejemplo) podría comprometer seriamente los sistemas de cualquier empresa en cualquier escala.

En la actualidad, debido a la evolución vertiginosa de las tecnologías de procesamiento, almacenamiento, transmisión y transporte, así como la aparición de nuevas técnicas de ingeniería de software y de programación, que facilitan el desarrollo de programas informáticos; los grupos de hackers y Crakers desarrollan y publican en la red, herramientas automatizadas que reducen el tiempo en la ejecución de ataques informáticos y que permiten que estos puedan ser perpetrados por usuarios con poca experticia tecnológica, con la misma efectividad de cualquier experto.

En la grafica siguiente puede apreciarse que el grado de conocimientos requeridos para realizar ataques que comprometan fuertemente a las compañías soportadas en tecnología, es mínimo gracias al uso de herramientas especializadas fácilmente descargables desde la red.

Figura 1. Nivel de conocimientos Atacante



Incluso el uso de herramientas de administración y gestión de red son de gran ayuda para que cualquier atacante logre su cometido contra un blanco específico o porque no contra un blanco seleccionado al azar con el fin de probar los conocimientos de hacking del delincuente en formación [2].

Teniendo claro lo anterior, el concepto de seguridad de la información ha tomado gran fuerza en el mundo, incluso a partir de la norma británica BS 17799 que promueve las mejores prácticas en seguridad de la información, la misma ISO ha incluido a la 27001 y 27002 como parte de su normativa.

Un gran porcentaje de compañías en el mundo ha integrado como parte de su unidad de administración de tecnologías a un equipo especializado en seguridad de la información o por lo menos esta realizando una autoevaluación de sus operaciones y de la infraestructura que las apoya con el fin de apuntar a las mejores prácticas y por qué no, a una certificación [7].

Generalmente los procesos de evaluación previos a la implementación de un sistema de gestión de seguridad de la información, apuntan a la evaluación de vulnerabilidades del sistema y en muchos casos a la realización de test de penetración con el fin de validar la posibilidad que existe sobre la plataforma en evaluación de que se pueda aprovechar alguna vulnerabilidad existente para comprometer seriamente algún activo importante para la compañía.

Realmente el objeto de las tareas antes descritas más algunas no mencionadas en detalle no es más que implementar las mejores prácticas, los controles técnicos y administrativos para dejar la plataforma "0-days" o plataforma sin "Bugs" conocidos [4]. Realmente se apunta a que el grado de riesgo sea el mínimo aunque nunca se puede llevar a cero (0), ya que ningún control por robusto que sea se considera totalmente infalible.

3.2 Ejecución del Test de penetración

Un test de penetración es el arte de ejecutar hacking ético donde un grupo de especialistas en seguridad de la información verifican y documentan la seguridad o los controles de protección de una plataforma tecnológica con las mismas técnicas de un hacker/cracker con el fin de lograr comprometer a algún activo alcanzable por algún punto de la superficie de ataque de un sistema [1].

Básicamente el test de penetración a diferencia de la Evaluación de Vulnerabilidades consiste en la ejecución de una penetración (o intento) real sobre un sistema en evaluación con el fin de identificar sus vulnerabilidades y de probar hasta donde puede penetrarse en ese sistema con el aprovechamiento de las debilidades identificadas.

Los test de penetración generalmente son ejecutados por personal especializado en seguridad de la información (ethical hackers) en modo outsourcing y siempre deben ejecutarse previo permiso firmado por una autoridad de la compañía en evaluación, en muchos casos por el CISO, CEO o CIO.

El test de penetración se hace generalmente desde dos frentes y asumiendo dos roles diferentes: el de un agente externo a la compañía y el de un empleado con acceso a los recursos internos de la plataforma.

4. Resultados

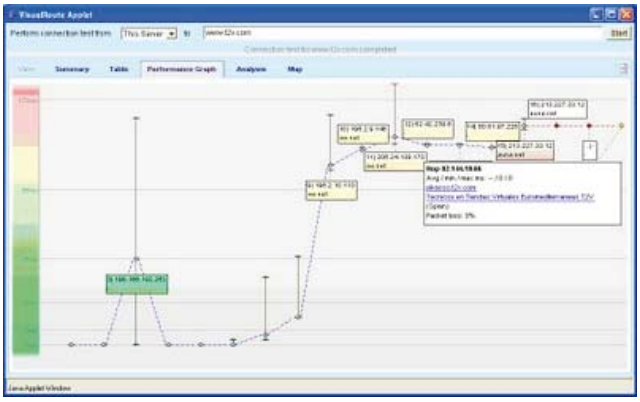
Estas pruebas se conocen como test de caja negra y de caja blanca, ambas se ejecutan en 9 pasos:

Figura 2. Pasos del test de penetración

Footprinting(Rastreo): en este se determina el blanco, por ejemplo:

- Registros DNS.
- Ámbitos/Rangos de IP.
- Información pública.
- Información de Contacto, etc.

Figura 3. Traza de un objetivo



Scanning (Escaneo): aquí se determinan los blancos abiertos y alcanzables, por ejemplo:

- Puertos asociados a servicios.
- Redes Inalámbricas.
- Arreglos de Modems.
- Servidores de VPN, etc.

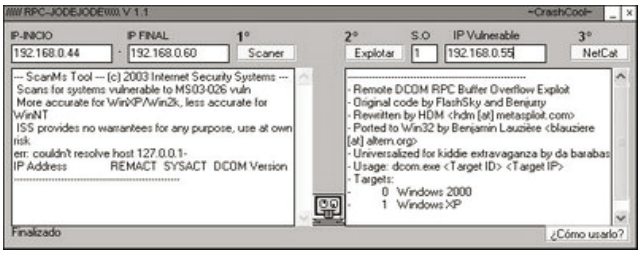
Enumeration(Enumeración): aquí se determinan los servicios que estan disponibles, por ejemplo:

- Servidores Web.
- Sistemas.
- Routers.

- Firewalls.
- Servidors de AAA.

Penetration(Penetración): aquí se seleccionan los exploits apropiados y se penetra el objetivo, por ejemplo:
- Inyección de SQL.
- Ejecución de desbordamiento de Buffer.
- Ataques por fuerza bruta (passwords), etc.

Figura 4. Ejecución exploit RPC



Escalation (Escala de privilegios): en este punto se realiza la escala de privilegios con el fin de obtener permisos superiores sobre el sistema comprometido para poder así tener acceso a la mayor cantidad de recursos posibles o a uno en específico, por ejemplo:
- Obtención de credenciales de root o admin.
- Inyección de dll's.
- Exploits locales.
- Cambios en la configuración.
- Planificación de tareas, etc.

Getting Interactive (Tener interactividad y tomar el control): aquí se pretende obtener una Shell remota de la victima, por ejemplo:
- Abrir o instalar un servidor de inicio de sesión remota.
- Hacer uso de Remote Desktop protocol.
- Hacer Uso de VNC, Netcat, etc.

Expanding Influence (Comprometer otros sistemas): en este punto se pretende moverse desde la máquina comprometida hacia otros nodos de la plataforma de red, por ejemplo:
- Llegar al filesystem del servidor de bases de datos.
- Llegar hasta una impresora o hasta un equipo activo (switch p.e), etc.

Cleaning Up(Limpieza): aquí se pretende asegurar las puertas traseras usadas y eliminar la evidencia que facilite la detección de la penetración, tales como rootkits, remoción y edición de logs y eliminación de registros de control de conexiones, etc.

Reporting(Generación de reportes): en este punto se realizan los reportes de toda la actividad ejecutada y de los hallazgos al igual que los activos que pudo comprometerse en la tarea. Este informe se socializa al personal de la compañía en evaluación.

5. Conclusiones

Las empresas del siglo XXI están en el proceso de concientización de la importancia en la inversión en el área de seguridad de la información debido a que muchas tienen claro que la información es el activo más importante de su negocio y que el uso de tecnologías así como facilita la eficiencia de los procesos, incrementa la productividad y apoya la competitividad y el crecimiento de la compañía, también la hace dependiente de su plataforma y vulnerable a ataques contra la confidencialidad, integridad y confidencialidad y que el compromiso de algunas de estas cualidades de la información corporativa a través de un ataque podrían representar pérdidas millonarias para la unidad de negocios.

El alto gradode riesgo que hoy es común denominador de muchas empresas se debe al pensamiento sistémico funcional de los desarrolladores de tecnologías de software y hardware que no consideran a la seguridad de la información como eje transversal de la construcción de sus productos.

De igual manera el poco conocimiento que poseen los ingenieros de software y de comunicaciones de nuestra región sobre seguridad informática, más el esfuerzo adicional que se requiere para desarrollar proyectos que tengan como transversalidad la seguridad de la información generan como resultado productos inseguros, con debilidades informáticas fácilmente explotables por individuos con habilidades técnicas importantes.

A esto le sumamos el uso de la internet, el tendiente crecimiento de la misma y la facilidad con que podemos interconectarnos en la actualidad a la que apuntan las redes de Próxima generación han facilitado la propagación del software malicioso en todos los extremos de nuestro planeta que día a día comprometen la seguridad de la información de las empresas y de las personas conectadas.

La migración de las redes de conmutación de Circuitos de la plataforma de red celular hacia una red de conmutación de paquetes hacen de la misma no sólo una gran ayuda para los usuarios móviles que requieren acceso a la red IP más grande del mundo sino que a la vez se ha vuelto parte de la autopista usada por miles de crackers para apoderarse de la información de generamos, procesamos y consultamos a través de nuestros teléfonos móviles.

Por ende todos los componentes de negocios y cada una de las piezas tecnológicas que soportan a estos procesos deben intrínsecamente garantizar la seguridad de la información que se gestiona como insumo de toda unidad de negocios.

Concientizados de que las amenazas informáticas son una realidad, muchas empresas de tecnología han formado expertos en el área de seguridad de la información abriendo un nuevo campo para el ingeniero de sistemas y electrónico a la ves que se apoya a las empresas en la disminución del grado de riesgo asociado a un ataque informático, implementando los controles necesarios sobre la plataforma TIC de la compañía previa ejecución de algunas actividades de valoración del estado de la seguridad de la información entre las que se incluyen la evaluación de vulnerabilidades y el test de penetración, siendo este último una de la mejores maneras de testear e identificar el compromiso real que conllevaría la penetración del sistema por parte de un intruso con fines maliciosos al tiempo que se evalúa la efectividad de los controles previamente implementados.

Referencias

[1] Stuart McClure,SM, Hackers, Secretos y soluciones para seguridad de redes , Osborne-McGrawHill, 2001

[2] Phil Williams, Casey Dunlevy, Tim Shimeall, 2008 Intelligence Analysis for Internet Security [internet] disponible desde www.cert.org/archive/html/Analysis10a.html [acceso 12 Junio 2008]

[3] Preventing and Detecting Insider Attacks Using IDS,(2007) [Internet], disponible desde: http://www.securityfocus.com/infocus/1558 [acceso 2 marzo 2008]

[4]Sans/FBI,(2008) The Twenty Most Critical vulnerabilities [Internet],disponible desde: http://www.sans.org [acceso 12 septiembre 2008]

[5] Klaus-Peter Kossakowski, Julia Allen and others, Carnegie Mellon, Responding to Intrusions [Internet] disponible desde: http://www.sei.cmu.edu/pub/documents/ [acceso 23 Febrero 2008]

[6] The Froehlich/Kent Encyclopedia of Telecommunications vol. 15. Marcel Dekker, New York, 1997, pp. 231-255.

[7]Information Securing (2007), [Internet] disponible desde: http://www.sonic.net/sales/rooftop/faq.shtml [acceso 23 Febrero 2008]

[8]Enciclopedia Libre Universal en Español (2008), [Internet] disponible desde: http://enciclopedia.us.es/index.php/Era_de_la_información.[acceso 16 Febrero 2008]

[9]Artículo del Diario El Pais /Madrid españa(2008), [Internet] disponible desde: http://www.elpais.com/articulo/internet/empresa[acceso 11 Mayo 2008].