VULNERABILIDADES DE SEGURIDAD EN LAS EMPRESAS

Julio César González Cervantes
UANL-FCFM
Universidad Autónoma de Nuevo León
Facultad de Ciencias Físico Matemáticas
San Nicolás de los Garza, Nuevo León, México

Resumen:
En este artículo se presenta el problema de la falta de conocimiento sobre el concepto del *hacking,* desde el punto de vista de las empresas, y sus posibilidades de solución; empezando por los inconvenientes en materia de seguridad y el riesgo que representan para todas ellas.

Palabras claves:
hacker, información, seguridad, empresas, ataques, prevención

Introducción

La estructura en que se manejan los datos, así como los protocolos de Internet son exactamente iguales desde que se crearon a partir de 1970; desde entonces solo se ha ido parchando para corregir los problemas de seguridad. Cualquier tipo de ataque, redunda en importantes pérdidas económicas para las empresas, además de crear una mala imagen ante los inversionistas y administrativos. Aquí existe el problema de que muchas empresas y compañías completas se encuentran en una gran disyuntiva de entre mantener abiertas y al alcance muchas aplicaciones para que los empleados puedan trabajar, y a la vez, evitar que la información sea modificada por la persona indicada sin sufrir ningún cambio.

En el siguiente artículo mencionaré diferentes términos y es importante una pequeña introducción a estos:

*Hacker: s*e refiere a una persona con la pasión por la resolución de problemas, por lo general con un amplio conocimiento técnico en su rama de especialización.

Cracker: se les conoce a las personas que buscan formas de penetrar en sistemas sin haber sido autorizados y que roban información para obtener un beneficio económico.

White Hat Hacker: son los *hackers* que se dedican a la protección de sistemas contra ataques dentro de sistemas empresariales y se conducen bajo un tipo de ética donde se dedican a proteger la información confidencial.

Black Hat Hacker: También conocidos como *Crackers* son los *hackers* que se dedican al robo de información para beneficio propio.

Actualmente, las empresas están expuestas a una gran cantidad de diferentes ataques externos e internos que pueden crear pérdidas muy grandes de información y afectar económicamente a la empresa; de allí la importancia de mantener la seguridad de los sistemas, puesto que las consecuencias de un ataque informático pueden poner en riesgo la integridad de la información. El problema principal no es siempre técnico, sino del conocimiento de todos los peligros potenciales en la transmisión de información confidencial y la falta de cultura sobre las distintas técnicas de *hacking* empresarial.

La información es uno de los pilares más trascendentales a la hora de la toma de decisiones en una entidad; de allí la importancia que tiene para estos entes la protección y prevención del manejo de información y datos.

Sabiendo esto como punto de partida, para una empresa no es tan sencillo como implementar medidas y protocolos de seguridad (ya sean antivirus, *firewalls*, etc.) sino que se inicia una carrera de conocimiento contra todos los posibles atacantes, ya que todos los días se descubren cientas de vulnerabilidades nuevas y técnicas que pueden volver muy sencillo obtener los datos de una empresa. Por eso, las empresas necesitan tener a personas únicamente enfocadas a realizar esta tarea.

Hacking empresarial

Los sistemas informáticos han creado otros patrones de delincuencia, así que como ingenieros de sistemas, técnicos, empresas, trabajadores de la misma y usuarios, tomemos conciencia y seriedad frente a los problemas que pueden llegar a afectar no solo nuestro empleo, sino a nuestra información en cualquier momento.

Técnicas de *hacking*

Tratar de enumerar todas las ramas en que se dividen los distintos ataques que se pueden hacer, es tan extenso como hablar de todas las ramas en que se dividen los sistemas informáticos; no obstante, mencionaré las más comunes y sencillas.

Ingeniería Social: Es un método basado en engaño y persuasión para obtener información importante o lograr que la víctima realice un determinado acto; como por ejemplo, hacer que la víctima ejecute un archivo que le llegó por correo electrónico.

Este método se puede llevar a cabo a través de canales tecnológicos (impersonal a través de Internet o teléfono) o bien, en persona: cara a cara.

Esta técnica es por mucho la más sencilla de llevar a cabo y la más eficiente, ya que no involucra ninguna especialización en sistemas informáticos; básicamente, es poder obtener información confidencial directamente de las personas que laboran dentro de una empresa mediante diferentes técnicas de presión social. De acuerdo con el *hacker* Kevin Mitnick en su libro "El arte de la decepción", este tipo de ataques se realiza aprovechándose del contacto social en el que vivimos, partiendo de 3 reglas básicas:

1. Todos los seres humanos quieren ayudar.
2. El primer movimiento es siempre de confianza hacia el otro.
3. No nos gusta decir no.

4. A todos nos gusta que nos alaben.

5. Todos tenemos algo de ingenuos.

Además de estos postulados, la técnica de ingeniería social fue ampliada por el Dr. Robert Cialdini así como por sus libros sobre persuasión, entre muchas otras técnicas psicológicas, para manejar a las personas dependiendo de su personalidad.

Por más increíble que parezca, esta es la técnica más sencilla y efectiva para hacerse de información confidencial dentro de las empresas y es de la que menos se protegen. Como más claro ejemplo, podemos encontrar al *hacker* Kevin Mitnick, quien tuvo acceso a North American Air Defense Command siendo menor de edad y además robó información importante del Security Pacific Bank.

La forma de estar seguro de esto es la concientización del personal sobre la información confidencial y la creación de *HoneyPots* tanto en los sistemas aplicativos, bases de datos e incluso archiveros, esto significa crear información falsa y dejarla como muy importante; así, en caso de que alguien se haga del acceso, se lleve información equivocada.

***Scanning* y *sniffing*:** El *Scanning* consiste en el escaneo de IPs dentro de una red, se realiza mediante herramientas que realiza pings a un rango de IPs proporcionadas por el atacante; después de los equipos encontrados, se procede a conocer el sistema operativo así como su versión, además de los puertos abiertos y que aplicaciones tiene instaladas para poder encontrar una vulnerabilidad específica así como saber dónde están los servidores que manejan la información importante.

Con el *Sniffing* se permite saber y analizar toda la información que se mueve dentro de una red; para hacer esto se utilizan analizadores de protocolos.

Las aplicaciones que sirven para usar el *Sniffing* dentro de una red, decifran la información que se transmite y se almacena para un posterior estudio; entre toda la información se encuentran: contraseñas, mensajes de correo electrónico, datos bancarios y otros datos confidenciales del usuario.

Es muy difícil lograr evitar efectivamente que se utilice esta técnica, solo se logra con ciertos routers empresariales muy especializados; lo más recomendado es que toda la información viaje de manera encriptada dentro de la red y nunca poner informacion confidencial en paginas que no tengan el protocolo HTTPS. Los clientes de mensajería y correo electrónico son muy propensos a ser intervenidos y mantener los accesos a la red muy vigilados, evitando el protocolo de redes inalámbricas WEP y siempre usando redes WAP con encriptación de 128 bits y evitar lo más posible conectar dispositivos moviles a una red WAP segura, ya que estos también son una vulnerabilidad dentro del ambiente.

Respecto a la técnica de *Sniffing* la forma más eficiente de usarse es mediante una técnica llamada *Man in the middle*, esta técnica consiste en mediante el uso de algunas herramientas intervenir la informacion que se maneja dentro de una red, realizando un ataque a las tablas ARP (Address Resolution Protocol). Estas tablas son las que se encargan de la vinculación entre una mac address y una IP de los equipos de los que se requiere obtener la información.

Primero, el atacante con el uso de herramientas, obtiene la *mac address* y la IP del equipo a atacar; luego, genera una tarjeta de red virtual con estos mismos datos y trata de engañar a la otra máquina o al *router* haciéndose pasar por la víctima y la información que recibe la reenvía a la víctima para pasar inadvertido.

Hijacking: El *Hijacking* consiste en el robo de una sesión dentro de una página *web* y también es un derivado de la técnica de *Man in the middle*.

Básicamente mediante un software de *sniffing* el atacante intercepta los paquetes entre la víctima y el servidor y al tener los datos de las *cookies* y las sesiones, se adelanta a la víctima y se adelanta al usuario autorizado.

La única manera de evitar esto es siempre autentificarse en sitios que sean HTTPS sin dejar a un lado el *firewall* y el *antispyware*.

Aportes

Las técnicas de *hacking* empresarial son el conjunto de procedimientos utilizados por una persona que posee una gran cantidad de conocimientos técnicos en por lo menos: redes, sistemas operativos, bases de datos y programación.

Las técnicas de *cracking* se dividen en cuatro grupos principales: monitoreo, validación, denegación de servicio y modificación; cada una con una forma de ataque diferente y una forma de prevención.

El grupo de monitoreo se compone por: escaneo de puertos, enumeración y *Sniffing*.

La validación se compone de ataques de fuerza bruta, *spoofing, Hijacking* e ingeniería social.

En el grupo de denegación de servicio, las técnicas

que se utilizan son: *Jamming* (interferencia de servicio), *Syn flooding* y además *IP Flood*.

Por último, en la parte de modificación está el borrado de huellas o *Zapping*.

En los dos primeros grupos es donde se centran todas las bases para cualquier ataque informático.

Análisis de riego

Frente a la gran cantidad de áreas de oportunidad que existen referentes a la seguridad de la información dentro de las empresas, se han desarrollado muchos estándares abiertos enfocados en la protección de datos, que son los más utilizados por las empresas de auditoría para validar la seguridad de los servidores y el manejo de la información.

Debido a la gran complejidad, cantidad de variables e importancia de la información, es importante que los análisis de riesgo se realicen por un especialista en seguridad informática ya que, si bien existen muchos estándares, procedimientos, guías y *software* para realizar este tipo de estudios, hay que tener claro que cada empresa es diferente y son muchas las variables que pueden existir y siempre cabe la posibilidad de pérdida de continuidad en los procesos de la misma.

El estándar de auditoría de aplicaciones *web* más conocido se llama OWASP (Open Web Application Security Project)

Conclusiones

El objetivo de escribir este artículo es dar a conocer las técnicas de trabajo que manejan los *hackers Black Hat,* que se dedican al robo de información, conociendo las técnicas que se utilizan normalmente; nos sirve para conocer las formas de defensa y protección dentro de una empresa, sin tener que crear más burocracia en los sistemas informáticos. Además nos sirve para crear una concientización en las personas para crear una cultura de seguridad de la información y para tener una idea de la importancia de personas enfocadas a la seguridad dentro de nuestras empresas.

Ahora está en manos de los directivos de las organizaciones el aprender que mientras más tecnología se utiliza para gestionar los servicios de la misma, también hay que aprender a tomar las mejores decisiones para proteger al máximo la información confidencial de la empresa y los mecanismos de protección contra robo de información y fraudes.

Recomendaciones

Si este artículo fue de tu interés y además trabajas/ estudias en cualquier rama de la carreras informáticas, es importante que te adentres a investigar y profundizar en los alcances de estas técnicas y cómo evitarlas, ya que gran parte del éxito que han tenido los *crackers* es en que en general, las empresas en verdad no creen que puedan ser atacadas por personas externas; por lo que tiene que existir una cultura de seguridad de la información.

Con respecto a las cuestiones técnicas, además de conocer las diferentes técnicas de ataques que se pueden recibir, también hay que conocer las herramientas de detección y prevención de estos ataques además de saber a profundidad cómo funcionan los *passwords* cifrados, *firewalls* y *proxis*, para así poder hacer frente a los intrusos que intentan perjudicar a la empresa.

También existen muchas aplicaciones de libre descarga así como distribuciones de Linux que incluyen un compilado de las más populares, como lo es *BackTrack Linux* o *GameOver Linux*; este último más recomendado por incluir tutoriales además de instrucciones de cómo crear una máquina virtual para hacer las pruebas de penetración al sistema.

Referencias

[1] Mitnick, K. Takedown: *The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw. - By the Man Who Did It.* ISBN – 0786889136. 2006.

[2] Mitnick, K. *The Art of Deception: Controlling the Human Element of Security.* ISBN - 076454280X. 2003.

[3] Mitnick, K. No Tech Hacking: *A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing.* ISBN – 1597492159. 2006.

[4] *GameOver Linux*. SourceForge. 2013. http://sourceforge.net/p/null-gameover/wiki/Home/

[5] *Backtrack.* http://www.backtrack-linux.org/downloads/

Datos del autor:
Ing. Julio Cesár González Cervantes

Dirección del autor o de los autores: Lázaro Cárdenas #1212 colonia Las Puentes 14vo Sector, San Nicolás de los Garza C.P. 66460 .

Email: admin@dba.mx