.Seguridad

Cultura de prevención para TI

.Seguridad, Cultura de prevención TI I Número 12 I Diciembre'11 –Enero '12 I ISSN en trámite I Revista Bimestral

Hacktivismo y DDoS: Tendencias actuales de ataque

#12

En este número

Editorial

Principios Básicos de Seguridad en Bases de Datos

Hacking ético: mitos y realidades

La importancia de las pruebas de penetración (Parte 1)

¿Qué es y cómo funciona un ataques DDoS?

Hacktivismo: ¿delito o comunicación ciudadana?

Redes sociales, entre la ingeniería social y los riesgos a la privacidad

Editorial

Las tecnologías de la información han alcanzado límites hasta hace algunas décadas inimaginables. Su importancia social ha desbocado en escenarios que parecen, con el paso del tiempo, intensificarse. La creación de nuevos términos está a la orden del día.

Ahora, escuchamos hablar de *pentester*, *ataques de DDoS*, *grupos hacktivistas*, entre otros; todos ellos parte de una cultura en la que queramos o no estamos inmersos. La responsabilidad de jugar un papel activo y responsable al respecto depende de cada uno de nosotros.

Un ejemplo tangible lo encontramos en las redes sociales, esos espacios virtuales de los que nos hemos apoderado para distintos fines, y ahora son seriamente criticados por cuestiones relacionadas a la privacidad de los mismos usuarios, dejando hasta cierto grado libre de culpa a estos últimos.

Es tiempo de analizar, y asumir qué rol deseamos jugar en esta dinámica; de la cual parece no tenemos escapatoria alguna.

Bienvenido nuevamente a .Seguridad, una revista que invita a la reflexión.

Galvy Ilvey Cruz Valencia
Subdirección de Seguridad de la Información.

Principios Básicos de Seguridad en Bases de Datos

Por Msc. Johnny Villalobos Murillo*

1. La seguridad de las bases de datos

La gran mayoría de los datos sensibles del mundo están almacenados en sistemas gestores de bases de datos comerciales tales como Oracle, Microsoft SQL Server entre otros, y atacar una bases de datos es uno de los objetivos favoritos para los criminales.
Esto puede explicar por qué los ataques externos, tales como inyección de SQL, subieron 345% en 2009, "Esta tendencia es prueba adicional de que los agresores tienen éxito en hospedar páginas Web maliciosas, y de que las vulnerabilidades y explotación en relación a los navegadores Web están conformando un beneficio importante para ellos"[1]

Para empeorar las cosas, según un estudio publicado en febrero de 2009 The Independent Oracle Users Group (IOUG), casi la mitad de todos los usuarios de Oracle tienen al menos dos parches sin aplicar en sus manejadores de bases de datos [1].

Mientras que la atención generalmente se ha centrado en asegurar los perímetros de las redes por medio de, firewalls, IDS / IPS y antivirus, cada vez más las organizaciones se están enfocando en la seguridad de las bases de datos con datos críticos, protegiéndolos de intrusiones y cambios no autorizados.

En las siguientes secciones daremos las siete recomendaciones para proteger una base de datos en instalaciones tradicionales.

2. Principios básicos de seguridad de bases de datos

En esta sección daremos siete recomendaciones sobre seguridad en bases de datos, instaladas en servidores propios de la organización.

2.1 Identifique su sensibilidad

***No** se puede asegurar lo que no se conoce.*

Confeccione un buen catálogo de tablas o datos sensibles [2] de sus instancias de base de datos. Además, automatice el proceso de identificación, ya que estos datos y su correspondiente ubicación pueden estar en constante cambio debido a nuevas aplicaciones o cambios producto de fusiones y adquisiciones.

Desarrolle o adquiera herramientas de identificación, asegurando éstas contra el malware [3], colocado en su base de datos el resultado de los ataques de inyección SQL [4]; pues aparte de

---

* Consultor de Auditoría de Tecnologías de Información. Posee la licenciatura en Ingeniería en Computación e Informática, así como en Informática con énfasis en Sistemas de Información. Concluyó el Máster en Auditoría de Tecnologías de Información y otro más en Ciencias de la Computación. Imparte cátedra en la Facultad de Ciencias Exactas y Naturales, la Escuela Informática de la Universidad Nacional de Costa Rica, además se desempeña como Coordinador de la Cátedra de Bases de Datos. Es Profesor en la Facultad de Ciencias Económica y de Maestría en Auditoría de Tecnologías de Información de la Universidad de Costa Rica.

[1] El Reporte X-Force de IBM revela que el phishing y las amenazas relacionadas a documentos se incrementan [en] http://www.lawebdelprogramador.com/noticias/mostrar.php?id=2460

exponer información confidencial debido a vulnerabilidades, como la inyección SQL, también facilita a los atacantes incorporar otros ataques en el interior de la base de datos.

2.2 **Evaluación de la vulnerabilidad y la configuración**

Evalúe su configuración de bases de datos, para asegurarse que no tiene huecos de seguridad. Esto incluye la verificación de la forma en que se instaló la base de datos y su sistema operativo (por ejemplo, la comprobación privilegios de grupos de archivo -lectura, escritura y ejecución- de base de datos y bitácoras de transacciones).
Asimismo con archivos con parámetros de configuración y programas ejecutables.

Además, es necesario verificar que no se está ejecutando la base de datos con versiones que incluyen vulnerabilidades conocidas; así como impedir consultas SQL desde las aplicaciones o capa de usuarios. Para ello se pueden considerar (como administrador):

- Limitar el acceso a los procedimientos a ciertos usuarios.
- Delimitar el acceso a los datos para ciertos usuarios, procedimientos y/o datos.
- Declinar la coincidencia de horarios entre usuarios que coincidan.

2.3 Endurecimiento

Como resultado de una evaluación de la vulnerabilidad a menudo se dan una serie de recomendaciones específicas. Este es el primer paso en el endurecimiento de la base de datos. Otros elementos de endurecimiento implican la eliminación de todas las funciones y opciones que se no utilicen. Aplique una política estricta sobre que se puede y que no se puede hacer, pero asegúrese de desactivar lo que no necesita.

2.4 Audite

Una vez que haya creado una configuración y controles de endurecimiento, realice auto evaluaciones y seguimiento a las recomendaciones de auditoría para asegurar que no se desvíe de su objetivo (la seguridad).

Automatice el control de la configuración de tal forma que se registre cualquier cambio en la misma. Implemente alertas sobre cambios en la configuración. Cada vez que un cambio se realice, este podría afectar a la seguridad de la base de datos.

2.5 Monitoreo

Monitoreo en tiempo real de la actividad de base de datos es clave para limitar su exposición, aplique o adquiera agentes inteligentes [5] de monitoreo, detección de intrusiones y uso indebido.

Por ejemplo, alertas sobre patrones inusuales de acceso, que podrían indicar la presencia de un ataque de inyección SQL, cambios no autorizados a los datos, cambios en privilegios de las cuentas, y los cambios de configuración que se ejecutan a mediante de comandos de SQL.

Recuerde que el monitoreo usuarios privilegiados, es requisito para la gobernabilidad de datos y cumplimiento de regulaciones como SOX y regulaciones de privacidad. También,

ayuda a detectar intrusiones, ya que muchos de los ataques más comunes se hacen con privilegios de usuario de alto nivel.

El monitoreo dinámico es también un elemento esencial de la evaluación de vulnerabilidad, le permite ir más allá de evaluaciones estáticas o forenses. Un ejemplo clásico lo vemos cuando múltiples usuarios comparten credenciales con privilegios o un número excesivo de inicios de sesión de base de datos.

2.6 Pistas de Auditoría

Aplique pistas de auditoría y genere trazabilidad de las actividades que afectan la integridad de los datos, o la visualización los datos sensibles.

Recuerde que es un requisito de auditoría, y también es importante para las investigaciones forenses.

La mayoría de las organizaciones en la actualidad emplean alguna forma de manual de auditoría de transacciones o aplicaciones nativas de los sistemas gestores de bases de datos. Sin embargo, estas aplicaciones son a menudo desactivadas, debido a:

- su complejidad,
- altos costos operativos
- problemas de rendimiento,
- La falta de segregación de funciones y
- la necesidad mayor capacidad de almacenamiento.

Afortunadamente, se han desarrollado soluciones con un mínimo de impacto en el rendimiento y poco costo operativo, basado en tecnologías de agente inteligentes.

2.7 Autenticación, control de acceso, y Gestión de derechos

No todos los datos y no todos los usuarios son creados iguales. Usted debe autenticar a los usuarios, garantizar la rendición de cuentas por usuario, y administrar los privilegios para de limitar el acceso a los datos.

Implemente y revise periódicamente los informes sobre de derechos de usuarios, como parte de un proceso de formal de auditoría.

Utilice el cifrado [6] para hacer ilegibles los datos confidenciales, complique el trabajo a los atacantes, esto incluye el cifrado de los datos en tránsito, de modo que un atacante no puede escuchar en la capa de red y tener acceso a los datos cuando se envía al cliente de base de datos.

Referencias

[1] ISO/IEC 27001:2005 - Information technology -- Security techniques [en] http://www.iso.org/iso/catalogue_detail?Csnumber=42103

[2] ISO/IEC 17799:2005 - Information technology -- Security techniques [en] http://www.iso.org/iso/catalogue_detailcsnumber=39612

[3] Malware - Wikipedia, la enciclopedia libre [en] *es.wikipedia.org/wiki/Malware*

[4] Inyección de código SQL - MSDN – Microsoft [en] http://msdn.microsoft.com/es-es/library/ms161953.aspx

[5] Escolano F. "Inteligencia Artificial", Editorial Paraninfo, 2003

[6] Aguilera L "Seguridad Informática" 2010, Madrid, Editorial Editex, S.A.

- El Reporte X-Force de IBM revela que el phishing y las amenazas relacionadas a documentos se incrementan [en] http://www.lawebdelprogramador.com/noticias/mostrar.php?id=2460

- http://sox.sourceforge.net/

- Daniel Camargo Montero, Sistema de selección de personal inspirado en agentes inteligentes, [en] http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/camargo_m_d/

Hacking ético: mitos y realidades

Por Ing. Anaid Guevara Soriano[*]

En los últimos años, y con gran ímpetu, el llamado "hacking ético" ha despertado innumerables puntos de vista a favor y en contra. La combinación de dos palabras tan distantes, parece confundir a muchas personas, pues la palabra "ético" siempre nos refiere a algo "bueno", mientras que "hacking" indica lo contrario.

Esta problemática se basa en el desconocimiento de la labor que realizan los expertos en seguridad de la información cuando aplican auditorías planeadas a los sistemas a través de diversas metodologías, mediante ellas, evalúan los puntos vulnerables a ataques informáticos en una organización.

Pero, ¿qué es el hacking ético?

El hacking ético es en sí una auditoría efectuada por profesionales de seguridad de la información, quienes reciben el nombre de "pentester". A la actividad que realizan se le conoce como "hacking ético" o "pruebas de penetración".

Las pruebas de penetración surgieron como respuesta a la presencia y realización de los primeros ataques informáticos a las organizaciones, los cuales trajeron graves consecuencias, como pérdidas monetarias y de reputación. Es aquí donde interviene el trabajo de un "hacker ético", ya que su labor es buscar vulnerabilidades en los sistemas de la organización para, posteriormente, poder mitigarlos y evitar fugas de información sensible.

Durante los últimos años, nuevas técnicas de intrusión que atentan contra la seguridad de la información se han sofisticado, por lo que organizaciones y empresas han implementado al hacking ético, aunque combatir la idea de que esta actividad es dañina, no ha sido tarea fácil.

El hacking ético, también es conocido como prueba de intrusión o pentest, se define esencialmente como el ``arte´´ de comprobar la existencia de vulnerabilidades de seguridad en una organización, para posteriormente a través de un informe, revelar aquellos fallos de seguridad encontrados, mitigarlos a la brevedad posible y evitar fugas de información y ataques informáticos.

Pese a su mala fama, no todos los hackers son delincuentes cibernéticos, algunos ayudan a las organizaciones a reforzar su seguridad. Por ello, para tratar de diferenciar a un grupo de otro, se introdujeron los términos crackers y hackers éticos. Los primeros identifican a aquéllos que realizan técnicas de intrusión con fines maliciosos y lucrativos; mientras que los segundos se refieren a quienes lo hacen con fines éticos y por el bien de la organización que lo solicite.

---

[*] Ingeniera en Computación por la UNAM. Se desempeña como académica en las facultades de Contaduría y Administración (FCA) e Ingeniería (UNAM). Es analista del laboratorio de Redes y Seguridad de la Facultad de Ingeniería. Colaboró en la SSI/UNAM-CERT como analista de vulnerabilidades. Actualmente cursa la Maestría en Administración de Nuevas Tecnologías de la FCA.

Otra conceptualización que reciben es la de "sombrero negro o Black Hat" y "sombrero blanco o White Hat".

Los hacker de sombrero negro, mejor conocidos como "Black Hat", tienen la cualidad de explotar vulnerabilidades en los sistemas con la finalidad de demostrarse que lo pudieron hacer burlando la seguridad del mismo. Ejemplo de ello lo tenemos en el caso acontecido en febrero del 2008, cuando la página web oficial de la Presidencia de la República fue afectada por un atacante que se hacía llamar "H4t3 M3"; logró dejar como recordatorio una imagen de lo más elocuente gracias a que esa página web tenía una vulnerabilidad.

La información fue revelada en el foro de la Comunidad Underground Latinoamericana, en dónde el joven hacker advirtió que podía modificar desde la agenda presidencial hasta las noticias, pero que no lo haría.

Por su parte, los hackers de sombrero blanco o "White Hat", también conocidos como hackers éticos, pentesters y expertos en seguridad; tienen la finalidad de realizar pruebas de intrusión en organizaciones que así lo pidan, para posteriormente rendirles un informe, en el que se detallan todos aquellos puntos vulnerables encontrados para que, posteriormente, la empresa los mitigue a la brevedad posible.

A continuación, se describe dicha clasificación en la siguiente ilustración:

Fig. 1 Clasificación de sujetos que realizan pruebas de intrusión
Fuente: Elaboración propia

Cuando en 1997, la cultura de la seguridad informática comenzó a tomar fuerza, se pensó que los hackers éticos podían ofrecer sus servicios a las empresas para ayudarlas a ser menos vulnerables, y en 2001 arrancaron en forma este tipo de asesorías.

Así los hackers blancos, ya sea trabajando individualmente, dentro de una empresa bien organizada o dentro de diversas consultoras, comenzaron a ofrecer sus servicios "para ayudar a las compañías a encontrar fallas y actuar en consecuencia", precisa Luis Guillermo Castañeda, consultor en seguridad.

Convencer a las compañías de contratar un hacker, por mucho que se llame ético, y conseguir el permiso para que ingrese y juegue con sus sistemas no ha sido fácil. "No puedes llegar y simplemente decir te ofrezco un hackeo ético, debes explicar muy bien qué es esto y cuáles son los objetivos", comenta Luis Alberto Cortés, consultor en seguridad y hackeo ético

Así, el término poco a poco se ha ido aceptando, ahora los hackers éticos empiezan a ser conocidos y buscan sus servicios. Por otra parte, grandes empresas de seguridad, como *Ernest & Young* o *PriceWaterhouse*, han empezado a ofrecer servicios de hackeo ético, lo cual ayuda a generar mayor confianza en este tipo de asesorías.

Así mismo, se ha desarrollado, alrededor de estas prácticas, una especie de código de honor y contratos especiales, que se firman entre los hackers éticos y las compañías usuarias, para mayor protección de estas últimas. En dicho contrato, se conviene que la empresa da permiso para realizar la intrusión, marca un lapso de duración, dispone las fechas para hacerlo y cómo se entregarán los resultados, generalmente un reporte, donde se enumeran las vulnerabilidades y fallas encontradas, así como las recomendaciones para mitigarlas.

Generalmente, esos contratos incluyen una cláusula de confidencialidad, donde se estipula que toda información encontrada a raíz de las pruebas de penetración, no podrá ser divulgada por el hacker a otra entidad que no sea la compañía que contrató sus servicios, ni tampoco podrá quedarse con una copia del reporte final generado para la empresa, esto con la finalidad de evitar sea revelado a terceros. De no cumplir con ello, se haría acreedor a una demanda.

¿Qué evalúa un hacker ético?

Los servicios que con mayor frecuencia ofrecen los hackers blancos (hackers éticos) a las empresas son las pruebas de penetración, con la intención de analizar si la compañía está preparada para soportar un ataque sofisticado perpetrado desde fuera, es decir por un hacker externo o por un atacante interno con conexión a la red.

Durante las pruebas de penetración, según enumera Victor Chapela, se analizan tanto la red interna, como Internet, aplicaciones expuestas, servidores, puertos y avenidas de acceso, además se hacen pruebas de contraseñas. Al mismo tiempo, se analiza la red inalámbrica, de ésta se revisa la configuración, se hace sniffing[2] de tráfico y contraseñas, intentando penetrar y romper el cifrado.

[2] Sniffing: Se trata de una técnica por la cual se puede "escuchar" todo lo que circula por una red. Esto que en principio es propio de una red interna o Intranet, también se puede dar en Internet.

Parte de la auditoría incluye también revisar módems, VPN, página web, incluso se hace ingeniería social, es decir se trabaja con el personal o con los asociados de la empresa para ver si se dejarían engañar para proporcionar contraseñas o acceso a la red.

De igual forma, se mide el nivel de respuesta a incidentes internos, también se busca emular si un empleado de bajos privilegios podría tener acceso a los estados financieros o a la nómina de la compañía. Se consideran además los valores de los activos, la criticidad de la vulnerabilidad y la probabilidad del ataque, su impacto, la forma de corregirlo y el esfuerzo requerido para esto.

Para evitar cualquier contratiempo o daño a la infraestructura, o continuidad de negocio del cliente, las pruebas siguen una metodología y manejan estándares, como el *Manual de la Metodología Abierta de Comprobación de la Seguridad* (OSSTMM, por sus siglas en inglés) o el *Proyecto Abierto de Seguridad de Aplicaciones Web* (OWASP).

Según el Mapa de Seguridad propuesto por el OSSTMM[3], las secciones a las cuales se aplican el hacking ético son las siguientes:

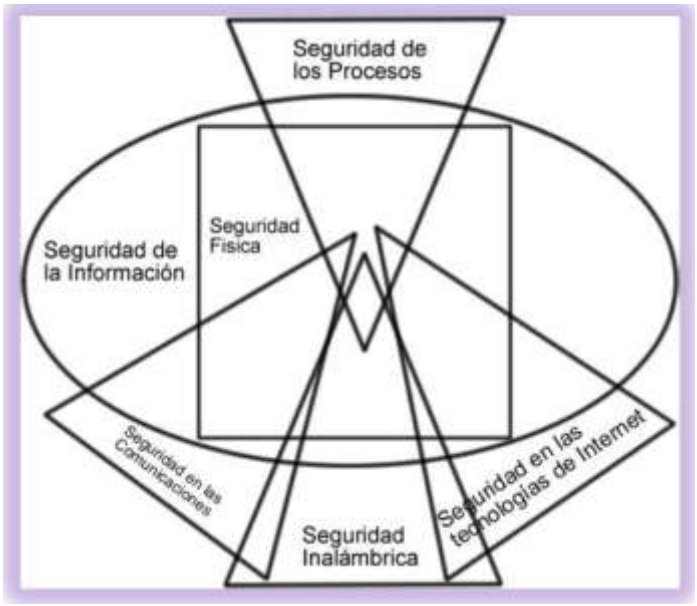


Fig. 2 Mapa de Seguridad
Fuente: Tomado del Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM 2.1 de ISECOM

A continuación, se describen brevemente dichas secciones.

a. Seguridad física

Alude a las pruebas de seguridad realizadas a un medio físico y no electrónico en la naturaleza. Comprende el elemento tangible de la seguridad donde la interacción requiere un esfuerzo físico o una transmisión de energía para que sea manipulado. A considerar:

- Revisión del perímetro,
- Revisión de monitoreo,

[3] HERZOG, Peter, *"OSSTMM 2.1 Manual de la Metodología Abierta de Testeo de Seguridad"*. ISECOM Institute for Security and Open Methodologies.

- Evaluación de controles de acceso,
- Revisión de respuestas de alarmas,
- Revisión de ubicación y
- Revisión de entorno

b. Seguridad en las comunicaciones

Comprende dos fases: Telecomunicaciones y las redes de datos. La primera fase alude a todas las redes de telecomunicación, sean digitales o analógicas, la otra, se refiere a todos los sistemas electrónicos y redes de datos donde la interacción se realiza a través de cables establecidos y cables de líneas de red.

c. Seguridad inalámbrica

Refiere a todas las comunicaciones electrónicas, señales y emanaciones que se producen del conocido espectro EM – Electromagnetic. Esto incluye ELSEC como comunicaciones electrónicas, SIGSEC como señales, y EMSEC que son emanaciones sin ataduras por los cables. Los módulos de verificación requeridos en el hacking ético para dicho rubro son:

- Verificación de radiación electromagnética (EMR),
- Verificación de redes inalámbricas 802.11, Verificación de redes bluetooth,
- Verificación de dispositivos de entrada inalámbricos,
- Verificación de dispositivos móviles inalámbricos,
- Verificación de comunicaciones sin cable,
- Verificación de dispositivos de vigilancia inalámbricos,
- Verificación de dispositivos de transacción inalámbricos,
- Verificación de RFID y
- Verificación de sistemas Infrarrojos.

d. Seguridad en las tecnologías de Internet

Se refiere a las pruebas de intrusión efectuadas a las aplicaciones web, tales pruebas son esencialmente el ``arte´´ de comprobar una aplicación en ejecución remota o local, sin saber el funcionamiento interno de la aplicación, para encontrar vulnerabilidades de seguridad[4]. Los módulos de verificación requeridos en el hacking ético para dicho rubro son:

- Logística de Controles,
- Sondeo de Red,
- Identificación de los servicios de sistemas,
- Búsqueda de información competitiva,
- Revisión de privacidad,
- Obtención de Documentos,
- Búsqueda y verificación de vulnerabilidades,
- Testeo de aplicaciones de internet,
- Enrutamiento,

[4] 6 OWASP Foundation. “Guía de pruebas OWASP versión 3.0”.

- Testeo de sistemas confiados,
- Testeo de control de acceso,
- Testeo de Sistema de Detección de Intruso IDS,
- Testeo de Medidas de Contingencia,
- Descifrado de contraseñas,
- Testeo de Negación de servicios y
- Evaluación de políticas de Seguridad.

e. Seguridad del resguardo de información

Aborda los medios empleados para el almacenamiento adecuado de la información, va ligado con los controles empleados para su seguridad.

f. Seguridad de los proceso

Representa un método para lograr acceso privilegiado a una organización y sus activos mediante la ayuda involuntaria del personal de la organización, en especial con la ayuda de aquellos que resguardan los puntos de accesos principales. Esto se hace por medios de comunicación tales como el teléfono, e-mail, chat, tablones de anuncios, etcétera, y se realiza de una manera fraudulenta con la finalidad de obtener una posición "privilegiada

En este rubro la aplicación del hacking ético se emplea por medio de la práctica de la ingeniería social, la cual es una técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten manipular a las personas para que voluntariamente realicen actos que normalmente no harían[5].

En conclusión, el hacking ético es una técnica aplicada a distintos escenarios, por lo que es importante hacerlo del conocimiento de la gente en beneficio de las organizaciones; así la relación entre detección y explotación de vulnerabilidades existentes podrá controlarse de la mejor manera posible.

Referencias:

- Harris, S. et. al. “Hacking ético. Traducción de: Gray hat hacking” (2005). Madrid: Anaya Multimedia.
- Picouto, F. et. al. “Hacking práctico” (2004). España: Anaya Multimedia.
- Daltabuit, E. et. al. “Seguridad de la información” (2007). Noriega, México: Limusa
- Aceituno, V. “Seguridad de la información: Expectativas, riesgos y técnicas de protección “(2006). México: Limusa.
- Rodríguez, L. A. “Seguridad de la información en sistemas de cómputo” (1995). México D.F: Ventura.
- E-WORLD: Arm yourself against black hats, Anonymous. Businessline. Chennai: Jul 12, 2010.
- DATA SECURITY AND ETHICAL HACKING: Points to Consider for Eliminating Avoidable Exposure, Ronald I Raether Jr. Business Law Today. Chicago: Sep/Oct 2008. Tomo 18, No. 1; Pág. 55
- Ethical hacking on rise, Bill Goodwin. Computer Weekly. Sutton: Jan 31, 2006. Pág. 8 (1 página)
- Ethical Hackers: Testing the Security Waters, Phillip Britt. Information Today. Medford: Sep 2005. Tomo 22, No. 8; Pág. 1 (2 páginas)

[5] MITNICK, Kevin, “Controlling the Human Element of Security. The Art Of Deception", Ed. John Wiley & Sons Australia, USA, 2002, 577 pp.

- IT takes a thief: Ethical hackers test your defenses Bill Coffin. Risk Management. New York: Jul 2003. Tomo 50, No. 7; Pág. 10).
- MITNICK, Kevin, “Controlling the Human Element of Security. The Art Of Deception", Ed. John Wiley & Sons Australia, USA, 2002, 577 pp.

La importancia de las pruebas de penetración (Parte I)

Por Ing. Erika Gladys De León Guerrero[*]

Las pruebas de penetración son de suma importancia para las instituciones, hoy en día con la inseguridad existente en muchas aplicaciones y sistemas es necesario contar con este tipo de pruebas que nos permite evaluar el nivel de seguridad de la infraestructura tecnológica.

Si bien este tipo de pruebas no es la panacea de la seguridad, desde hace varios años se ha comprobado que gracias a ellas se pueden descubrir una gran cantidad de huecos en los activos críticos de las organizaciones.

A pesar de que es necesario tener experiencia y gran conocimiento para realizar pruebas de penetración, este tipo de pruebas no es exclusivamente para grandes organizaciones con un conjunto de servidores que proporcionan distintos servicios y con segmentos de red de decenas o cientos de computadoras.

Se pueden ejecutar pruebas de penetración a equipos independientes e incluso a un equipo personal; es evidente que la profundidad con la que se realizan este tipo de pruebas no será la misma que la aplicada por un *pentester* profesional, pero llevar a cabo pruebas de penetración de este tipo permitirá encontrar los puntos vulnerables más visibles, facilitando la implantación de controles de seguridad y medidas preventivas para evitar intrusiones y comportamientos no esperados en el equipo evaluado.

En este articulo dividido en dos partes, se mostrará de manera general como realizar pruebas de penetración con herramientas automáticas y fáciles de usar, el objetivo no es crear *pentesters* expertos, se pretende ayudar al usuario que no tiene gran experiencia en seguridad a descubrir las vulnerabilidades en su infraestructura tecnológica casera así como a pequeñas organizaciones que deseen evaluar pocos activos críticos que posean.

Existen diversas metodologías que indican el camino a seguir para la evaluación de seguridad de un equipo algunas orientadas a herramientas otras a elementos a evaluar y otras a procedimientos generales, todas las metodologías incluyen un conjunto de etapas o fases de evaluación, a pesar de ser distintas se pueden englobar en las siguientes:

- Reconocimiento
- Escaneo
- Explotación
- Reporte

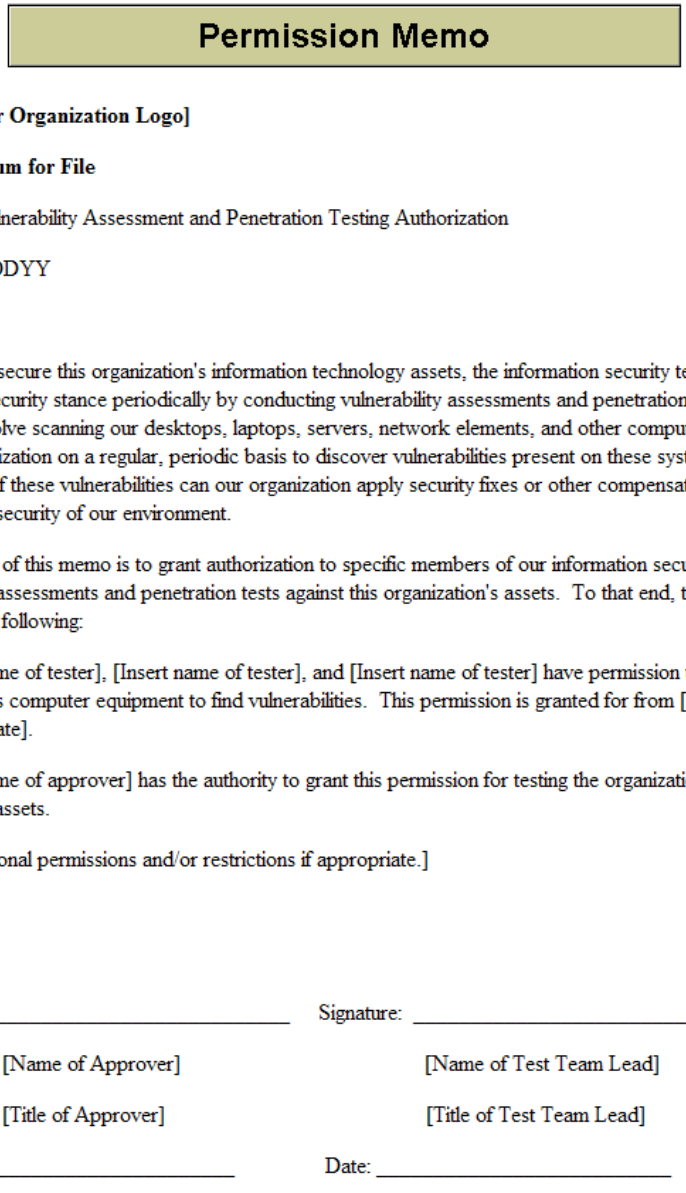
Existe una primera etapa independiente a las mencionadas anteriormente, es de gran importancia y no debe omitirse por ninguna razón, en esta etapa se establece la autorización por parte del solicitante de las pruebas de penetración esta acción es una de las que marcan la diferencia entre un pentester y un cracker. En algunas metodologías así como en cursos de

[*] Ingeniera en Computación por la UNAM. Colaboradora de la Subdirección de Seguridad de la Información (SSI/UNAM-CERT) en el Área de Auditoría y Nuevas Tecnologías, realizando pruebas de Penetración y Análisis de Vulnerabilidades, así como investigación sobre nuevas tecnologías de seguridad para la emisión de recomendaciones. Fue miembro del Plan de Becarios de Seguridad en Cómputo impartido por el UNAM-CERT a través de la Dirección General de Servicios y Cómputo Académico. Se encuentra desarrollando un sistema de prevención de intrusiones para Redes Inalámbricas.

capacitación para *pentesters* se menciona que no se puede lanzar ni un simple ping si no se cuenta con la autorización firmada por el solicitante, esta autorización es muy importante ya que será el respaldo legal ante cualquier problema existente en el proceso de evaluación. Este documento de autorización debe contener al menos los siguientes datos:

- Fecha y hora de inicio de las pruebas
- Fecha y hora de término de las pruebas
- Equipos a evaluar, especificando dirección IP
- Nombre del equipo o persona que realizará las pruebas
- Datos de contacto del equipo o persona que realizará las pruebas
- Nombre del solicitante de las pruebas
- Firma de conformidad del solicitante

Un ejemplo de autorización se puede obtener en la siguiente página:
http://www.counterhack.net/permission_memo.html



Permission Memo

[Insert Your Organization Logo]

Memorandum for File

Subject: Vulnerability Assessment and Penetration Testing Authorization

Date: MMDDYY

To properly secure this organization's information technology assets, the information security team is required to assess our security stance periodically by conducting vulnerability assessments and penetration testing. These activities involve scanning our desktops, laptops, servers, network elements, and other computer systems owned by this organization on a regular, periodic basis to discover vulnerabilities present on these systems. Only with knowledge of these vulnerabilities can our organization apply security fixes or other compensating controls to improve the security of our environment.

The purpose of this memo is to grant authorization to specific members of our information security team to conduct vulnerability assessments and penetration tests against this organization's assets. To that end, the undersigned attests to the following:

1) [Insert name of tester], [Insert name of tester], and [Insert name of tester] have permission to scan the organization's computer equipment to find vulnerabilities. This permission is granted for from [insert start date] until [insert end date].

2) [Insert name of approver] has the authority to grant this permission for testing the organization's Information Technology assets.

[Insert additional permissions and/or restrictions if appropriate.]

Signature: _____ Signature: _____

[Name of Approver] [Name of Test Team Lead]

[Title of Approver] [Title of Test Team Lead]

Date: _____ Date: _____

Imagen 1. Ejemplo de Autorización

Reconocimiento

La primera etapa de las pruebas de penetración es el reconocimiento, esta etapa permite identificar la información públicamente accesible. Muchas veces en bases de datos publicadas en internet, en sitios web en caso de contar con ellos, en servidores ftp, hasta los perfiles de solicitud de personal pueden brindar mucha información valiosa para el *pentester*.

Como ejemplo se puede ver la siguiente imagen:

Imagen 2. Ejemplo de recopilación de información a través de ofertas de empleo

Es una oferta de trabajo en la que se proporcionan tres datos muy importantes:

- Plataformas NET
- Windows 2003 ó 2008
- SQL 2005 ó 2008

Si no se tiene información del equipo a evaluar, se irá recabando poco a poco con búsquedas públicas. De esta forma se puede detectar si se está divulgando más información de la que se debe, si se está publicando información confidencial o simplemente si se están brindando pistas a un cracker o individuo mal intencionado.

Una herramienta muy útil para esta tarea es whois, brinda información detallada sobre un sitio, los datos que se pueden recabar con whois son los siguientes:

- Fechas de registro del dominio
- Personas asociadas con el dominio
- Nombre del servidor
- Fecha de actualización del dominio
- Fecha de expiración del dominio
- Quien registró el dominio

La herramienta whois es proporcionada por diferentes organizaciones, una de ellas es InterNIC, permite la consulta de un dominio vía internet proporcionando una interfaz fácil de usar. Se encuentra disponible a través de http://www.internic.net/whois.html

Imagen 3. Whois

Por ejemplo, si se ejecuta whois a google.com el resultado es el siguiente:

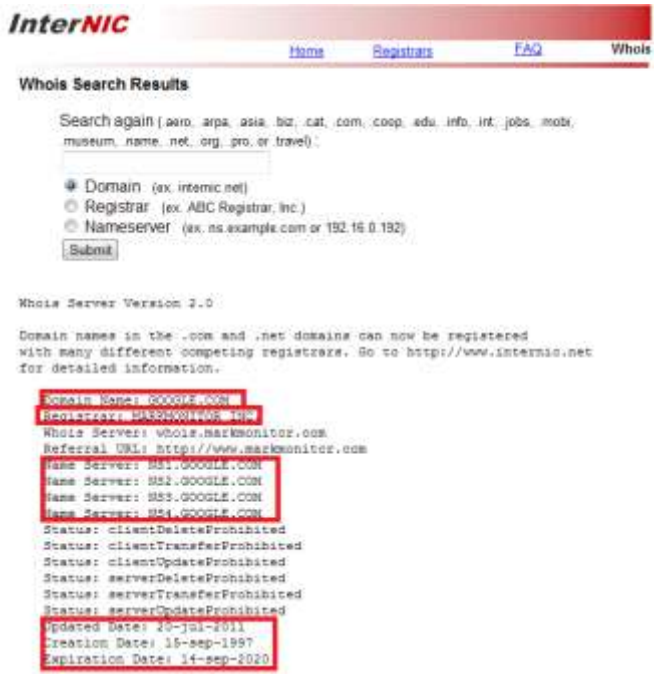


Imagen 4. Whois a google.com

Whois también se puede emplear por línea de comandos, tiene diferentes opciones que hacen muy flexible a esta herramienta.

Para ver las opciones y la explicación de cada una de ellas, se puede recurrir en un sistema Linux al siguiente comando:

$man whois

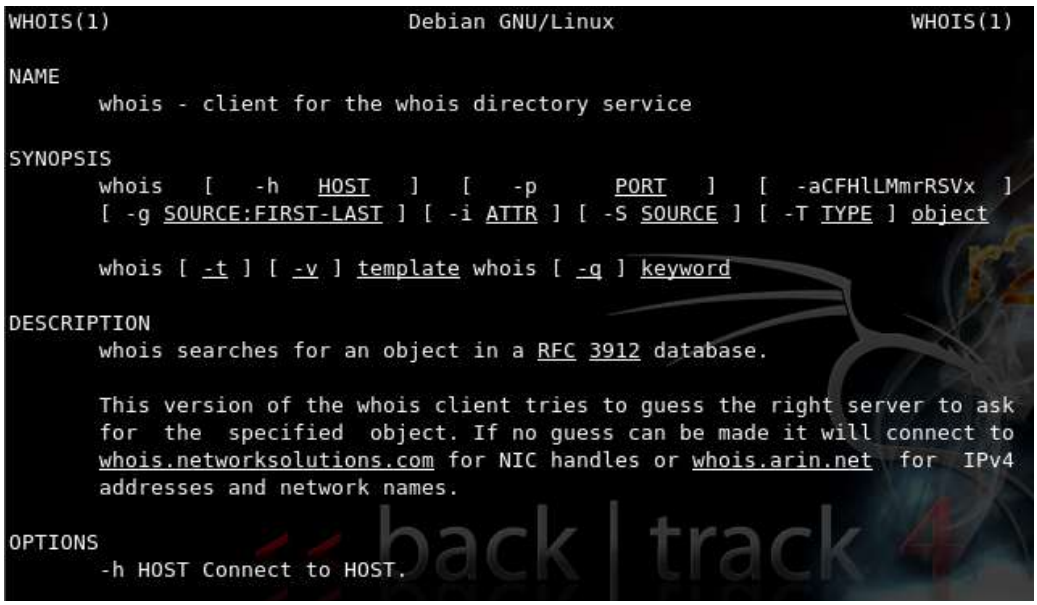


Imagen 5. Man whois en Linux

Otra herramienta muy útil para esta etapa es **Nslookup**, permite realizar consultas a los servidores DNS, la información que proporciona este comando es la siguiente:

- Dirección IP
- Nombre canónico

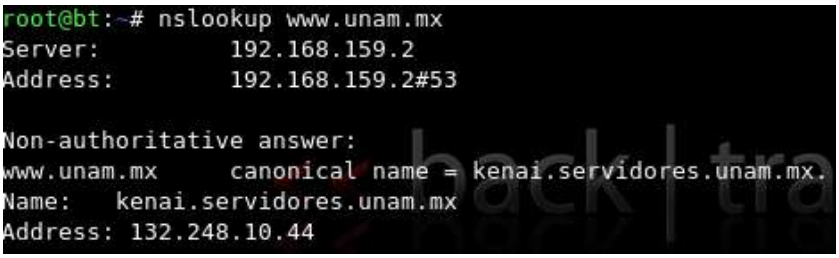


Imagen 6. Nslookup

Este comando cuenta con otras opciones, por ejemplo es posible consultar los registros que un servidor DNS ha cargado en su cache, y otras opciones que permitirían realizar un análisis más detallado, por el momento solo es necesaria la información por default que proporciona el comando.

Finalmente para esta etapa se recurrirá a búsquedas mediante motores de búsqueda públicos. Se requiere el envío de consultas adecuadas para encontrar información divulgada y útil tanto para un pentester como para un cracker.

Este artículo se enfoca al motor de búsqueda Google debido a su popularidad y calidad de resultados.

A continuación se listan un conjunto de directivas que permitirán generar búsquedas mas precisas y brindar mejores resultados.

***Site**:* permite la búsqueda en un solo sitio o dominio. Ejemplo, búsqueda de la cadena host en el sitio unam.mx se expresaría de la siguiente forma: site:unam.mx host
Link: Muestra las paginas que apuntan a un sitio web determinado.
Related: Muestra las paginas que tienen contenido similar y enlaces a la página de búsqueda.
Allintitle: Muestra las paginas que tienen todas las palabras especificadas en su titulo.

Existen muchas directivas que permiten generar resultados más específicos, aquí solo se mostraron pocos ejemplos para brindar el usuario la idea general.

Las redes sociales son una fuente importante de información ya que las personas revelan información muy útil y personal que podría dar pistas o un camino a seguir para el evaluador.

Como se pudo observar en esta etapa, la idea es recolectar información del equipo a evaluar, de la institución, etc. tal vez a partir de aquí se pueda generar un diccionario para realizar fuerza bruta a servicios vulnerables o se puedan obtener posibles nombres de usuarios a través de los nombres publicados, la idea es almacenar tanta información útil como sea posible.

Esta etapa es considerada pasiva ya que la información a la que se tiene acceso es pública y no se tiene contacto directo con el equipo a evaluar.

Escaneo

Esta fase es de gran importancia en el proceso de pruebas de penetración ya que permite identificar las "puertas" y vulnerabilidades por donde podría entrar un intruso.

Esta etapa se puede dividir en los siguientes aspectos:

- Barrido de Red (Network sweeping): Permite identificar los host presentes en la red.
- Seguimiento de red (Network tracing): Permite identificar la topología de la red.
- Escaneo de puertos (Port scanning): Identifica aperturas en los equipos.
- Toma de huellas dactilares del SO (OS fingerprinting): Permiten la identificación del sistema Operativo presente en el equipo.
- Versión de escaneo (Version scanning): Identifica los servicios presentes en cada puerto.
- Identificación de vulnerabilidades (Vulnerability scanning): Encuentra las vulnerabilidades presentes en el equipo.

La parte de barrido de host se da solamente cuando se trata de una red completa donde existen varios equipos a evaluar. El mismo caso para el seguimiento de red, se ejecuta cuando se tiene toda una red a evaluar.

Se verificarán los puertos abiertos así como su correspondiente servicio ejecutado y la versión del servicio.

Existen distintas herramientas para llevar a cabo esta tarea, una de ellas es nmap, una herramienta muy flexible y de gran ayuda al *pentester*. Para obtener puertos abiertos, servicios y versiones se puede ejecutar el siguiente comando:

`nmap -T4 -A 127.0.0.1`

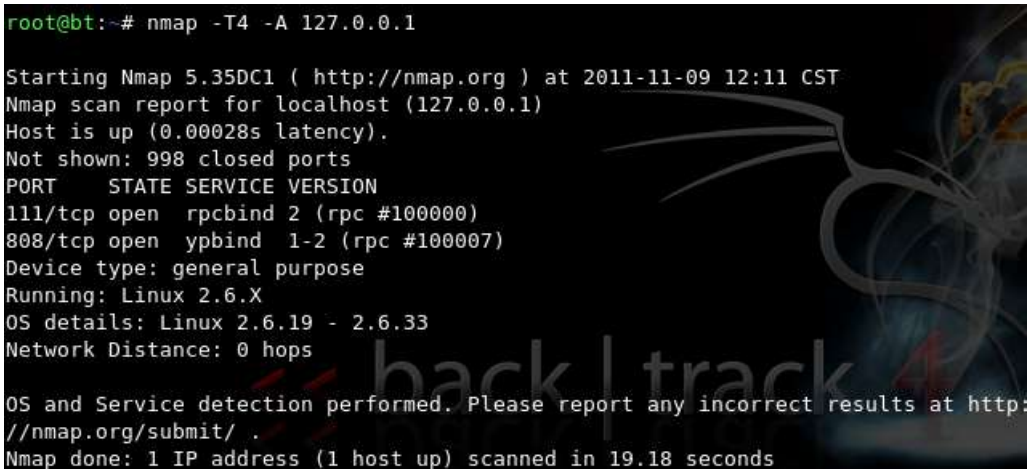


Imagen 7. Nmap

Una vez que se conocen las versiones y puertos abiertos, lo que resta es investigación sobre cada punto para detección de vulnerabilidades. Generalmente las versiones no actualizadas pueden tener vulnerabilidades. Este punto será detallado en la segunda parte del artículo.

Hasta aquí la primera parte de este artículo. En la siguiente parte se realizará escaneo de vulnerabilidades, explotación y reporte de los hallazgos encontrados.

Referencias:

- http://nmap.org/
- http://www.internic.net/whois.html
- http://www.kloth.net/services/nslookup.php
- www.google.com

¿Qué es y cómo funciona un ataques DDoS?

Por: Alejandro Reyes Plata

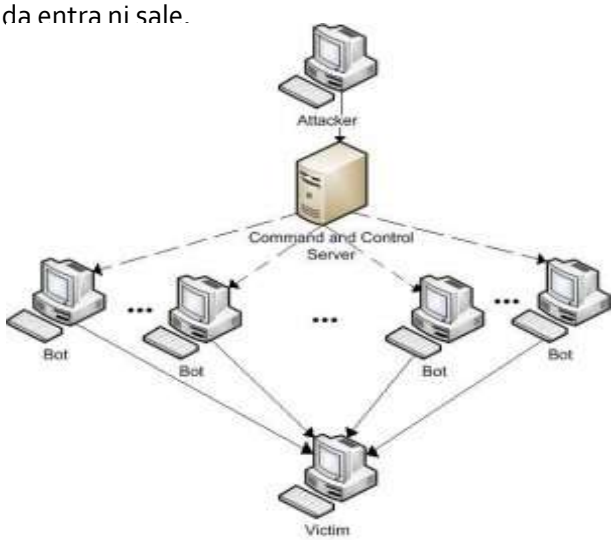
¿Qué es un ataque de DDoS?

En términos coloquiales un ataque de Denegación de Servicio Distribuido (*Distributed Denial of Service*) se puede explicar de la siguiente forma:

Éstos ataques se pueden explicar de diversas formas, por ejemplo imaginen un estadio de futbol que albergará la final del campeonato mundial, el estadio cuenta con diversas puertas para que los aficionados ingresen al estadio, 1 hora antes de inicio del juego la gente ingresa de forma ordenada al estadio a un ritmo lento pero constante, las personas ubicadas en las puertas encargadas de revisar la fiabilidad de los boletos están muy cansadas pero no se detienen en su labor, de pronto, faltando 5 minutos para el inicio del juego, una gran cantidad de personas con boletos falsos, arriban al estadio al mismo tiempo, los encargados de revisar los boletos no se dan abasto en atender a tanta gente, las personas que cuentan con su boleto auténtico no pueden entrar al estadio.

Los responsables de restringir el acceso al estadio se ven imposibilitados para diferenciar los boletos auténticos de los falsos y además están exhaustos, la carga de trabajo es excesiva. Se les explica que llevará más tiempo de lo previsto para ingresar, pues se tienen que revisar a detalle cada uno de los boletos, ante este anuncio las personas que no tienen boleto auténtico intentan ingresar al mismo tiempo de forma desorganizada y por la fuerza, por varios minutos los accesos se ven saturados, muy pocas personas logran ingresar, y por el contrario miles de personas se pierden el gran partido aun cuando tenían boleto auténtico. ¿Qué sucedió? pues ocurrió una Denegación de Servicio Distribuido de acceso al Estadio.

Un sitio Web es como una puerta de acceso, sólo puede dar servicio a un número limitado de personas al mismo tiempo, por tanto si recibe más solicitudes de las que puede atender, el servicio se bloquea, nada entra ni sale.



Esquema de un ataque DDoS

¿Cómo se hace un DDoS?

Para que el ataque sea realmente efectivo se debe contar con muchas maquinas que envíen peticiones a la página Web. Existen personas que se dedican a infectar equipos y crear grandes redes de equipos "zombie" (botnets) y posteriormente rentarlas. El precio de renta depende de distintos factores como el tamaño de la botnet (número de equipos infectados), el tipo de ataque, su duración, etc. Según un estudio realizado por eweekeurope en el 2010, rentar una botnet para efectuar un ataque de DDoS por 24 horas puede oscilar entre los 50 y varios miles de Dólares. De esta forma no es necesario tener conocimientos para realizar un ataque de DDoS sino una cartera con al menos 50 Dólares.

Bots (Zombie)

En la siguiente imagen se muestra una interface de un sitio Web que renta botnets, el precio depende del número de equipos infectados y cuántos de ellos están en línea.

Information	
Total logz in database:	1346862
Time of first install:	12:02:27 25.05.2009
Total bots:	12049
Total active bots in 24 hours:	5548

Botnets: Any >>

Installs (12044)	Reset
IN	3507
--	2002
BR	1395
US	736
MX	523
EG	223
TR	220
CO	212
FR	162
PE	158
AR	151
NL	134
AU	129
CR	122
MA	116
VE	113
VN	108
ES	101
CL	91
CA	88
BE	82
JP	77

Online bots (530)	Reset
--	90
BR	88
US	60
IN	45
MX	27
EG	15
TR	15
MA	13
FR	11
CA	11
AU	10
AR	9
NL	8
HO	8
BG	7
GB	7
ES	7
TN	6
CO	6
PE	6
CL	5
PL	5

Número de equipos infectados por país.

En el párrafo anterior se mencionaba que existen diversos tipos de ataques de DDoS, a continuación se explicaran los más comunes.

Tipos más comunes de ataques DDoS

Syn Flood (inundación de paquetes Syn): El más común de todos, este ataque se basa en la esencia del protocolo de conexión TCP, el cual requiere una conexión de tres pasos, si el paso final nunca llega se queda una conexión abierta en el servidor por un lapso de tiempo, es decir si una persona estira sus manos para saludar a dos personas diferentes y estas lo dejan con la mano estirada por 1 minuto, nadie más podrá saludar a ésta persona hasta que ella decida terminar el saludo.

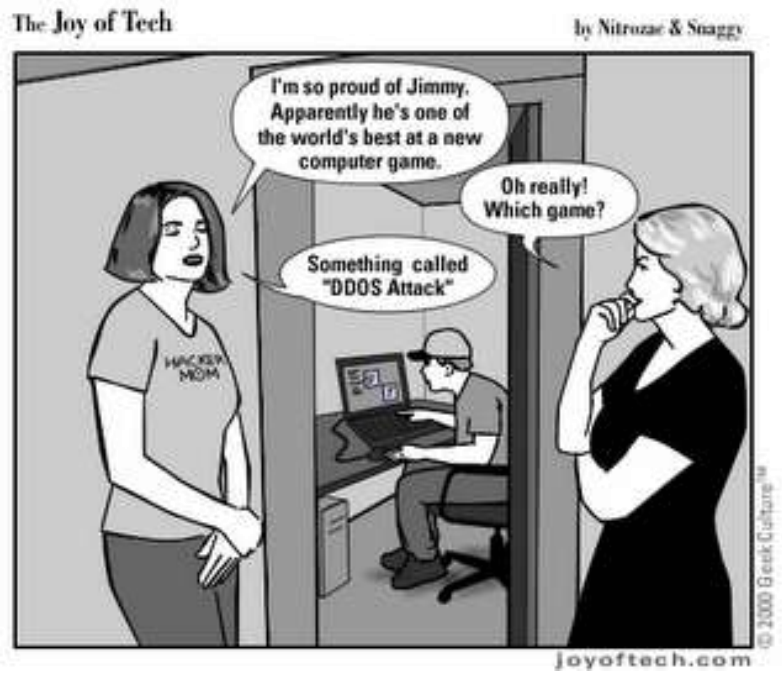
Connection Flood (inundación de conexión): Explota la dificultad del servidor para atender un gran número de peticiones al mismo tiempo, si un atacante realiza 10,000 peticiones al servidor este estará ocupado por un período de tiempo, conforme caduquen las conexiones el atacante vuelve a establecer más conexiones impidiendo así que los clientes utilicen el servicio.

ICMP Flood (inundación ICMP): Éste ataque también es conocido como "Ping-Pong", imaginen una conversación por MSN donde ustedes son los encargados de hablar y contestarle siempre a las personas que lo solicitan, entonces reciben un mensaje que dice: ¿estás? y ustedes responden: Sí, y les vuelven a decir ¿estás? y responden: Sí y así continúan por varios minutos, de pronto empiezan a recibir cientos de mensajes del mismo tipo, entonces ustedes empiezan a cerrar las ventanas del chat y estas se vuelven a abrir. Lo que pasa es que realmente la conexión se lleva a cabo pero se desperdicia el recurso. Lo mismo pasa con los servidores, se satura la línea con conexiones correctas pero todas ellas de tipo "basura", las cuales impiden que las conexiones de clientes verdaderos se concreten.

UDP Flood (inundación UDP): se utiliza el protocolo de conexión UDP para enviar una gran cantidad de paquetes al servidor utilizando muchas conexiones al mismo tiempo, ocasionando que los recursos (Memoria RAM, Procesador) del servidor sean insuficientes para manipular y procesar tal cantidad de información, en consecuencia el sistema se bloquea.

Evitar que un ataque de DDoS ocurra es como querer evitar que un soldado de infantería salga a la guerra y nadie le dispare. Lo que sí podemos hacer es ponerle un casco y un chaleco antibalas para mitigar el riesgo de que muera si es alcanzado por una bala. De forma general la estrategia de defensa consiste en identificar las direcciones IP (balas) causantes de ataque y bloquearlas (chaleco antibalas), utilizar otros servidores como balanceadores de carga distribuyendo así el trabajo del servidor crítico y por último colocar una versión ligera de la página del sitio atacado lo que permitirá reducir el tiempo de respuesta y minimizar la carga de procesamiento del servidor.

Para finalizar, ¡una imagen de reflexión!



Glosario:

Botnets: Conjunto de computadoras infectadas por un malware que permite que un servidor (*Command & Control*) las manipule remotamente para realizar trabajos de forma distribuida.

UDP: Por sus siglas en inglés "*User Datagram Protocol*" un protocolo no orientado a conexión, se utiliza sobre todo cuando la velocidad es un factor importante en la transmisión de la información.

TCP: Por sus siglas en inglés "*Transmission Control Protocol*" es un protocolo orientado a conexión, el protocolo asegura que los datos serán entregados a su destino sin errores lo que lo hace más lento a diferencia del protocolo UDP.

ICMP: Por sus siglas en inglés "*Protocolo de Mensajes de Control de Internet*" su función básica es el control y notificación de errores del Protocolo de Internet IP.

Referencias:

http://www.jmu.edu/computing/security/info/archived/ddos.shtml
http://cremc.ponce.inter.edu/360/revista360/tecnologia/Los%20Botnets%20R%20Toro.pdf
http://www.eecis.udel.edu/~sunshine/publications/ccr.pdf
http://www.eweekeurope.es/noticias/¿cuanto-cuesta-alquilar-una-botnet-8924
http://blog.damballa.com/?p=330
http://antivirus.about.com/od/whatisavirus/a/ddosattacks.htm
http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml
http://www.masadelante.com/faqs/udp
http://www.networksorcery.com/enp/protocol/icmp.htm

Hacktivismo: ¿delito o comunicación ciudadana?

Por L.C.C. Galvy Ilvey Cruz Valencia[*]

La comunicación se entiende como el acto de relación entre dos o más sujetos, mediante el cual se persigue evoca un fin común.

Para poder hacerlo, no sólo se trata el compartir un concepto o fin común, sino compartir experiencias similares que evoquen lo que sea que se tenga en común.

Como disciplina de las ciencias sociales, se aboca a estudiar los fenómenos que la sociedad experimenta para comunicar una idea, un evento, un pensamiento, la información de un grupo de personas o incluso datos personales y las repercusiones que pudieran tener.

Hoy, a través de distintos medios de comunicación, se habla de sociedad de la información, en la que los individuos parecen interrelacionarse en el ambiente web, para poner todas estas cosas en común mediante las redes sociales, correo electrónico, redes empresariales, información en la nube, etcétera.

Al considerar este panorama, en el que los conceptos tecnología, información y comunicación parecen formar un campo semántico, parece imperante que el concepto seguridad también lo sea, ya que la idea de que un nuevo y diferente paradigma de la comunicación ha impactado a la información con estas tecnologías produciendo resultados desconcertantes para el área de la seguridad de la información, es cada vez más palpable.

Analicemos.

Primero, es necesario entender que al referirme a un paradigma de la comunicación lo hago a "una forma de dar cuenta de que las características de esta sociedad de la información afectan a todos los ámbitos de la vida social, construyendo de esa manera una serie de acuerdos, certezas, valores, en definitiva formas de ser y hacer"[6].

Aparentemente, el paradigma señala que el individuo de esta sociedad de la información a medida que tiene acceso a una diversificación de tecnologías, le es más fácil apoderarse y cumplir con una tarea mediática que lo pondrá en el centro del acontecer cotidiano; y más aún beneficios que antes no conocía como la inmediatez, el anonimato y la masificación.

Lo anterior hace preciso mencionar algunos de los hechos que han marcado la evolución de la sociedad de la información, para después ir directo a explicar cómo esas características intervienen en la seguridad de la información.

---

[*] Licenciado en Ciencias de la Comunicación por la Facultad de Ciencias Políticas y Sociales. Se ha desempeñado como difusor de tecnologías de la información y la comunicación. Actualmente, es editor de la revista .Seguridad y otros contenidos de la Subdirección de Seguridad de la Información/UNAM-CERT.

[6] Rodrigo Prieto, en su libro *Casi todos en línea, retazos de una sociedad en red*, p. 19

Antecedentes

Algunos eventos sucedidos a principios del siglo XX, bien podrían ser los antecedentes claros del punto actual en el que nos encontramos, y el cual quisiera evaluar en esta ocasión.

Brevemente los señalo:

1) El nacimiento, en 1908, del término "medios de comunicación"; en el que Charles Horton Colley, agremió a la prensa, radiotelegrafía, radiotelefonía, carreteras y vías de ferrocarril, al considerar que la emisión y/o transportación de los mensajes acercaban a los emisores con sus receptores.

2) La Primer Guerra Mundial proporciona la perspectiva del poder que la propaganda podía tener sobre la opinión pública, al utilizar distintos medios para enviar a los ciudadanos estímulos hábilmente dirigidos que, según creían, serían entendidos y respondidos a un mismo nivel por cada una de ellos.

3) Con la posición que la comunicación se acompaña únicamente del estímulo-respuesta, se da por sentado que la respuesta positiva de las mayorías resulta capital para la funcionalidad de un sistema social dado.

4) La aparición de tecnologías digitales resulta en el planteamiento de la teoría matemática de la comunicación, en el que se aprecia que los individuos pueden sostener procesos comunicacionales a través de la circulación de mensajes entre máquinas por medio de canales electrónicos.

Relaciones sociales a través de los medios digitales

Los antecedentes anteriores dan pista del terreno hacia el que me quiero aproximar, como punto crucial de este análisis del paradigma.

Si consideramos que la relación social es el proceso mediante el cual los individuos son capaces de tener cosas en común, sin importar si son o no contrarios; y que la acción social es el desarrollo de una idea compartida por los individuos por la acción de otro u otros; entonces alcanzaremos a discernir que tanto la relación social como la acción social afectan los modos de percepción que resultan en modos diferentes de comprender la realidad.

Este fenómeno se agudiza cuando se trata de relaciones y acciones sociales desarrolladas a través de las tecnologías, pues uno de los puntos que más se afectan es el de la identidad.

La identidad a través de estos medios electrónicos se confecciona y adapta a formas como las siguientes:

1) Dilución de la posición espacial y tiempo. "Los participantes actúan aquí e intervienen allá".

2) Adquisición de más de una identidad, por lo que pueden intervenir en diversos y muchos *allás*. Por ejemplo la creación de Avatares.

3) Dirección de correo electrónico y de página web (también cuenta el proveedor). El nombre de dominios en Internet (DNS) permiten ser buscados e identificados por los "otros".

4) Cuentas de redes sociales que se tienen que gestionar y organizar (también cuenta el proveedor).

En conjunto, se puede decir que la identidad creada a través de este tipo de recursos tecnológicos no responde a un único nombre, sino a la multiplicidad de los que se pueden crear. Esta pluralidad hace que los usuarios se pueden atrever a realizar múltiples tareas en la red, unas que por supuesto pueden ser bien intencionadas y otras que no.

Nos vamos acercando a lo que pretendo dilucidar: ¿cómo estas transformaciones están modificando los procesos de comunicación de los individuos a través de la creación de una nueva forma de identidad enfocada a *telemovimientos sociales*?

Un hecho, que a pesar de las consideraciones anteriores queda, es el tema de la individualidad y la agrupación. Aquí, los individuos, por intereses varios, se asocian libremente entre sí, a pesar de las fronteras, las diferencias de horarios y las formas de gobierno, logrando incluso trascender de las redes y saltar a la realidad física.

A este punto, llegamos al análisis medular que da razón a lo que vengo elucidando. Durante los últimos meses, la sociedad internacional ha sido testigo de diferentes movimientos encausados por usuarios de redes sociales, quienes en el ímpetu de compartir con sus pares, han logrado derrocar a gobiernos autoritarios, alentar la constitución de grupos hacktivistas, ejecutar ataques a organizaciones estatales o privadas, en fin, una serie de eventos que no dejan duda a que la manera de comunicarnos ha cambiado.

Los movimientos ciberculturistas y hacktivistas

La cibercultura y la cultura hacker parecen estar transformando la comunicación más allá de lo que los medios de comunicación digital o tradicional lo han hecho. Varios aspectos han cambiado.

La aparición de una cibercultura libertaria por Internet ha añadido y añade un ingrediente cultural controvertido a las formas tradicionales de expresión. Los carteles, los magnetófonos, los pregoneros y la comunicación de boca en boca van paulatinamente cediendo al nuevo orden: la construcción de espacios virtuales para la acción y las relaciones sociales.

La cultura hacking, al parecer no tan reciente como parece, también va haciendo lo propio. El enfoque tiene sus variantes, ya que el comienzo de ésta se enfoca en romper las protecciones de copiado o las reglas impuestas por el mundo informático.

Como parte de un espíritu muy post-setentas, el 8 de enero de 1986, se publicó un Manifiesto Hacker, en el que detallan 6 principios "éticos" que describirían la naturaleza de sus actos, y cuál sería su lucha:

Principio 1. Los accesos a los equipos deberían ser ilimitados y totales, a fin de que la humanidad pueda aprender cuáles son las tendencias por las que se dirige el mundo.

Principio 2. La información deberá ser libre y gratuita.

Principio 3. Desconfiar de cualquier autoridad y pugnar por la descentralización.

Principio 4. Los hackers deberán ser juzgados de acuerdo a sus obras, y no según el criterio de quienes juzgan fácticamente como la posición, edad, nacionalidad o títulos.

Principio 5. Libertad para crear arte y estética en una computadora.

Principio 6. Las computadoras se crearon para cambiar la vida.

Para ellos, lo imperante de liberar información, responde a una necesidad práctica de compartir el conocimiento para mejorar las capacidades de las computadoras. Hoy, en un mundo donde la mayoría de la información es tratada a través de las computadoras, la necesidad es la misma.

Uno de los casos más célebres, es como sabemos el de John Draper, alías "Capitán Crunch", quien es reconocido por ser uno de los pioneros en hackear la industria de las telecomunicaciones. Su inventó consistió en la llamada "caja azul".

Desde entonces, la cultura hacktivista, quizá por el perfil de preparación y conocimientos, ha sido más activa que la construcción de la cibercultura, a la cual las poblaciones del orbe se han ido integrado paulatinamente, unas más rápido que otras, haciendo de este modo que parte de sus reglas sean una parte reglamentaria de Internet.

La cultura hacktivista se asume como parte de la construcción y el desarrollo de lo que es Internet para hacer circular la información; está impregnada de diversas prácticas: una de las más lógicas es la labor periodística.

Un caso fue Indymedia, que nació en 1999 para cubrir las expresiones de rechazo a la reunión de FMI y de la OMC en Seattle, fue uno de los precursores: esta red de colectivos, basada en el principio de la publicación abierta y el "periodismo ciudadano", en el que los grandes medios de comunicación social, no puedan intervenir para maquillar el descontento de los ciudadanos.

Un hecho reciente fue el caso WikiLeaks, el cual todavía tiene cierto impacto a nivel internacional en los medios de comunicación, ya que WikiLeaks reinventó en la opinión pública el significado de la "fuga de información" con protección de fuentes, una entrega ad-hoc transparente y compartida, cumpliendo con lo establecido por los primeros hackers.

Tras lo sucedido con WikiLeaks, apareció Anonymous, una comunidad internauta anónima que pregona el derecho a la libertad de expresión en Internet. Su principal forma de acción ha sido realizar ataques DDoS contra aquellos sitios que se opongan a los valores que defiende el movimiento. En esta situación se han visto afectados PayPal, MasterCard, entre otros, por haber decidido interrumpir los servicios destinados a WikiLeaks.

Como vemos, los hechos van cambiando. El hacking ya no es sólo un hecho exclusivo de aquellos genios. La llegada de diversas industrias del entretenimiento en línea, y las nuevas barreras sobre los contenidos puestos en línea, implica que todo el mundo esté hoy por hoy pendiente sobre lo que ocurre en Internet.

Esta atención se ve reflejada en la cultura de masas; así, lo que sucede en este medio de comunicación da contenidos a los otros medios como el cine, la televisión y la prensa.

Por mencionar algunas películas Matrix, Tron, Millenium y Red Social. Esta última consagrada a recapitular la vida del creador de Facebook.

Esta red social, después de todo, es un remanente derivado de la cultura hacking, nació de una asociación hacker; y su fundador la creó para poder colectar los datos de las chicas más guapas de su campus, aún así Mark retuvo dos de los principios de la cultura de los hackers:

- No jugar con los datos de otros.
- Favorecer el acceso a la información pública, proteger el derecho a la información privada.

Perspectivas a futuro

Como se ha revisado, la cultura de masas cambia. Los movimientos sociales tienen nueva táctica militante. Sin embargo, como en el pasado, los ciudadanos siguen, y muy probablemente seguirán, apoderándose *subterráneamente* de los medios para expresar sus diferencias o empatías.

Teniendo en cuenta esta cualidad social, se pueden plantear algunas de estas tendencias en el futuro del paradigma:

- Los movimiento sociales encuentran en la Web un camino amplio y dinámico para alentar "un nuevo orden de administración del poder"; tal y como la opinión pública pudo corroborar durante el llamado "Despertar de Oriente", en el que pueblos de esa región del mundo, lograron coordinarse a través de las redes sociales para derrocar o incentivar uan reforma a la política estatal.
- Los ciudadanos, usuarios o no usuarios de las tecnologías, iremos incorporando a nuestro imaginario colectivo los términos definitorios de esta "ciber corriente del pensamiento", tales como hacktivismo, DDoS, entre otros, hasta llegar a ser genéricos. Lo mismo ocurrirá con los grupos hacktivistas como los mencionados Anonymous, LulSec, etcétera.

- México y otras naciones latinoamericanas comenzarán a incluirse en este cambio social. El antecedente más cercano lo tuvimos con el EZLN (iniciado en 1994), que de una u otra manera, logro poner a México en los temas globales, a tal punto que personas de otras naciones estudiaran o participaran en él.

- Muchos aspectos sociales serán transformados profundamente:

- Educativos. La educación intensificará sus programas a distancia. Las aulas y profesores virtuales serán cada vez más comunes, generando espacios nuevos, que por supuesto representarán un espacio de interacción comunicacional que requerirá seguridad.

- Psicológicos. La adquisición de identidad, estereotipo y arquetipos entre grupos sociales, podrán generar alianzas estratégicas de colaboración, e incluso, no hay que descartar, conflictos en los que se podrán gestar otros tipos de movimientos sociales.

- Económicos. Las intrusiones a distintos sitios, sean gubernamentales o empresariales, generan impactos económicos, en los que no hay que dudarlo, en el corto plazo la Economía tendrá que realizar una propuesta seria al respecto.

- E incluso, las relaciones personales. Amor, conocer amigos, incluso ciber-sexo, son temas de moda; sin embargo, el boom de tecnologías móviles representan otro ingrediente extra en la transformación de comunicar e informar a nuestros semejantes.

Conclusión

El comportamiento hacktivista, aunque es difícil de ubicar su inicio, ha cambiado profundamente el arte de la técnica militante, logrando una perspectiva diferente de interacción en el que la comunicación y la seguridad de la información deben comenzar a entenderse a fin de lograr un acto social positivo.

Referencias

- **OWNI**, *Piratage: Du hactivisme au Hacking de Masse*, [en línea] http://owni.fr/2011/03/31/piratge-du-hacktivisme-au-hacking-de-masse/, 13 de noviembre de 2011.
- **LesInRocks**, *Petite histoire du Web militantisme et de l'hacktivisme*, [en línea] http://www.lesinrocks.com/medias/numerique-article/t/44428/date/2010-04-16/article/petite-histoire-du-web-militantisme-et-de-lhacktivisme/
- **Nathalie Magna**, *Art, Hack, Hacktivisme, culture jamming, médias tactiques,* [en línea] http://www.editions-hyx.com/site/media/download/extrait/magnan-hyx-artplus.pdf
- **Neblina Orrico**, *Mouvements sociaux sur Internet : le Mouvement des Sans*
- *Terre et l'Armée Zapatist,* [en línea] http://www.autresbresils.net/IMG/pdf/MSTEZLNb.pdf
- **Javier, Echeverría Ezponda**, *Los Señores del aire: Telépolis y el Tercer Entorno,* Barcelona. Ediciones Destino, 1999, 492 p.
- **Rodrigo Prieto, et. al.,** *Casi todos en línea, retazos de una sociedad en red,* Madrid, Editorial Voz de Papel, 2006, 282 pp.

Redes sociales, entre la ingeniería social y los riesgos a la privacidad

Ing. Jeffrey Steve Borbón Sanabria[*]

Un primer vistazo

En nuestro día a día, cada vez es más común el uso de las redes sociales. Hoy, ya no resulta extraño escuchar términos como Facebook, Twitter, e incluso Linkedin y FourSquare. La penetración de las redes de datos a partir del uso de dispositivos móviles, como teléfonos celulares, smarthphones, tablets, entre otros medios, ha facilitado el uso de este tipo de aplicaciones, portales y herramientas, transformándolas en parte de la vida diaria.

Sin embargo, como dice el adagio popular "no todo lo que brilla es oro", ya que en meses recientes, este tipo de aplicaciones y portales han enfrentado una gran cantidad de críticas por el manejo que tienen con la privacidad de la información publicada por sus usuarios, los controles de seguridad dentro de las aplicaciones y servicios prestados, así como con el manejo de la información una vez que el usuario ha cerrado su cuenta, o ha dejado de usar por un largo tiempo la herramienta.

Para ejemplificar este punto, se puede mencionar la situación acontecida con la red social Facebook y el buscador Google, el cual sin autorización comenzó desde hace unos días a indexar [1] (buscar y mostrar en sus resultados de búsqueda) los comentarios de muro que los usuarios realizan.

De la privacidad

Diseñadas para seducir, y provocar que compartamos grandes cantidades de información personal, las redes sociales se han transformado en parteaguas de la privacidad en línea. Comúnmente, los usuarios son acusados de estar desinformados de los problemas relacionados, dejando el debate abierto.

Es cierto, actualmente no existe un marco de trabajo ni instancias regulatorias que guíen por completo lo que debemos o no publicar. La necesidad de tener certidumbre sobre la propiedad de lo que publicamos, es una de las tareas pendientes de las redes sociales.

Los riesgos a la privacidad parecen estar por todas partes; por ejemplo, al intervenir una comunicación, el robo de identidad, el phishing, fuga de información, entre otras. Esta consideración hace necesario que los usuarios estemos cada vez más conscientes de los cambios que los desarrolladores de estas tecnologías implementan, para así aprovecharlos, y no estar expuestos.

De no hacerlo, corremos el peligro que estos cambios dejen abierta la oportunidad de hurgar en la privacidad. En primera instancia, es importante comentar que, en la mayoría de los casos, son los propios usuarios quienes revelan deliberadamente información privada a través de estas tecnologías, el correo electrónico y foros públicos.

---

[*] Ingeniero de sistemas egresado de la Universidad Distrital Francisco José de Caldas. Actualmente estudiante de máster de seguridad Informática de la Universidad Oberta de Catalunya. Ha realizado varios diplomados y cursos especializados (Sistemas operativos, Bases de datos, Telecomunicaciones, Desarrollo Web y Seguridad Informática). Se ha desempeñado como oficial de seguridad, hacker ético, administrador de sistemas, servidores y comunicaciones en varias organizaciones del mercado financiero, empresas desarrolladoras de software y ONGs. Certificado como CISSP - Certified Ethical Hacker - Auditor Interno 27001 - Itil Foundations V3.

La privacidad se vuelve un tópico clave. Los usuarios experimentan una confrontación entre el uso y los riesgos, de ser titular de una red social. Algunos son lo suficientemente audaces para percibir los cambios realizados en redes sociales; pero otros no.

A estos últimos quisiera dedicar el siguiente contenido, la reflexión de que la vida privada de cada una de las personas debe representar una noción central que haga comprender las encrucijadas a las que nos podemos enfrentar al ser asiduos a estas tecnologías.

Hasta hace algunos años, los usuarios aún veíamos con cierta lejanía el uso de las redes sociales; hoy, las usamos con naturalidad para tener comunicación "cercana" con amigos, familiares, conocidos y, aunque peligroso, con desconocidos también.

Pero, ¿qué hay con la información que publico, comparto y avalo? En primera instancia, hay que reconocer y ser conscientes de que todo lo que "pongamos en línea", tenderá e alguna u otra forma, a hacerse del dominio público, y es esta parte de sensibilidad la que más debemos de desarrollar para mantener bajo control la integridad de nuestra privacidad.

La privacidad no debe asumirse como algo acabado, ni tampoco caer en el supuesto de que siempre estará en riesgo. El sentido común y una postura responsable acerca de lo que publicamos, serán de gran ayuda.

¿Qué debemos entender por privacidad?

La privacidad es un conjunto de prácticas que dividen las cosas públicas y privadas. En este sentido, partamos del punto de vista en que la privacidad y la confidencialidad forman parte imperativa de la actividad computacional. Así, los problemas que los circundan sistemáticamente se vuelven un conflicto para la seguridad de la información, en muchos de los casos van más allá de las ciencias de la computación.

A primera vista, estos problemas no tendrían tanta incidencia con un tema tan delicado como las consecuencias de ataques de ingeniería social, o tal vez un poco más peligroso como puede ser el tema de secuestro, extorsión e incluso "matoneo" o "bullying" a niños y jóvenes.

Entendiendo la ingeniería social

Una verdad absoluta, en términos de seguridad de la información, es decir que el eslabón más débil de la cadena es el usuario, el ser humano. Esto se traduce en que resulta más sencillo atacar a una persona y obtener información o una acción de ésta, que lograr vulnerar un sistema de información que se encuentra asegurado, blindado y protegido ante posibles atacantes. Esto nos lleva a la definición de la ingeniería social:

"Arte o ciencia de manipular a las personas para que realicen acciones que pueden ser o no del interés del objetivo" Chris Hadnagy [2]

"Acto de manipular personas y desarrollar acciones o divulgar información" Wikipedia [3]

En pocas palabras se puede hablar de la ingeniería social como una especie de hacking humano.

Ahora bien, así como en el hacking se deben realizar tareas de obtención de información (Information Gathering) de un posible objetivo, de igual forma la obtención de información es la base de los ataques de ingeniería social, con la diferencia que normalmente el objetivo del ataque será una persona, un humano y para ello es necesario cavar en todos los medios posibles que contengan posible información del blanco, es aquí donde aparece Internet y las redes sociales.

Desde la perspectiva de un ingeniero social, cualquier información acerca de la persona que se tiene como objetivo, puede aportar a formar un perfil o esquema de gustos, lugares que

frecuenta, actividades que realiza, lugar y actividades del trabajo, entre otros datos. Es por ello que sin lugar a dudas, las redes sociales pueden proveer mucha información que puede ser de utilidad. A continuación, vamos a observar en una corta tabla que abarca algunos datos que se pueden llegar a obtener a través de estos sistemas de información:

Red Social/Plataforma	Información obtenida	Utilidad
Facebook/G+/Hi5/Badoo/…	• Estados de ánimo • Lugares visitados • Fotografías • Intereses • Familiares • Relaciones • Etc.	Estas redes proveen mucha información en general de la persona y sus contactos.
Twitter/Tuenti/BBM/…	• Estados de ánimo • Lugares visitados • Fotografías • Intereses	Establecer un listado de actividades, perfil psicológico, lugares visitados, información consultada y gustos de la persona.
MySpace/Grooveshark/LastFM/…	2. Música escuchada 3. Gustos musicales	Establecer un perfil de preferencias y gustos musicales.
Linkedin/…	3. Estado laboral 4. Conocimientos 5. Asignación Salarial 6. Estudios en proceso	Identificar perfil laboral de la persona, trabajo actual, pasados, estudios, conocimientos, intereses de trabajo, etc.
Foursquare/…	• Lugares visitados • Gustos gastronómicos	Permite geoposicionar a las personas e identificar qué lugares suelen frecuentar o posibles movilizaciones a través de viajes.
Flickr/Picasa/…	• Lugares visitados • Gustos particulares • Entorno en que se desarrolla el individuo	Establecer un listado de actividades, perfil psicológico, lugares visitados y gustos de la persona.

Ahora bien, sabiendo que información se suele tener publicada por estos sistemas y teniendo en cuenta que esta información puede ser indexada en motores de búsqueda con o sin autorización expresa del usuario, es necesario validar que tanto se está compartiendo, para ello veamos cómo protegerse.

Entonces… ¿Cómo puedo protegerme?

El panorama que se puede percibir a través de noticias como estás (Navegación segura en Facebook [4] y Cookie espía en Facebook [5]) genera preocupación acerca de los alcances que pueden tener para nuestras vidas el compartir tanta información. Aquí quiero acuñar una frase muy empleada a nivel de seguridad: "Si está en internet ya es público".

Afortunadamente es posible cambiar esta situación a partir de un cambio en la cultura del uso de estos medios de comunicación, a continuación se presenta un listado de consejos para aplicar y protegernos de posibles ataques de ingeniería social usados para delinquir y afectar nuestra integridad y la de nuestras familias:

- Establezca los controles de privacidad a través de redes sociales permitiendo el acceso a información sólo a amigos y/o familiares.
- No publique información personal tal como dirección de residencia, teléfonos, lugares de trabajo, ocultando así información que puede ser empleada para establecer contacto y así realizar ataques o engaños contra usted y familiares o amigos cercanos.
- Evite realizar publicación de lugares que frecuenta o asiste.
- Evite publicar cambios de estado sentimental o problemas de este tipo, la información de este tipo puede ser empleada para establecer contacto ofreciendo ayuda o consejo y así ganar la confianza de la posible víctima.
- Evite seguir enlaces o notificaciones vía correo electrónico o mensajes de texto respecto a información personal o del perfil en redes sociales, puede ser un engaño para secuestrar las cuentas de usuario y la información en las redes almacenada.
- Dentro de las redes sociales evite dar clic a cualquier enlace, pueden enviarlo a sitios o descargar aplicaciones con código malicioso que pueden obtener información acerca de usted y quienes usen el equipo.

En los siguientes recursos podrá encontrar algunas guías o tutoriales que ilustran como aplicar estos controles o cambios en la seguridad de la información para sus cuentas de usuario en redes sociales:

- Configurando privacidad en Facebook [6]
- Configurando privacidad en Twitter [7]
- Configurando privacidad en Linkedin [8]
- Configurando privacidad en FourSquare [9]

Para finalizar unas frases que valen la pena analizar para ver como estamos en cuanto al aseguramiento de la información que publicamos en la red:

3. Cuando viaja, usted no publica en la puerta de su hogar un aviso que dice: "No molestar, estoy de viaje"; sin embargo, en las redes sociales sí publica información, fotografías y nociones de que se encuentra en otro lugar de viaje, lo que equivaldría a lo mismo. Esta noticia [9] ilustra lo aquí mencionado anteriormente.
4. Cuando se enfrenta a problemas sentimentales o familiares, no sale a la calle portando un cartel que diga: "Tengo problemas familiares"; sin embargo sí los hace públicos por redes sociales.

Revisado lo anterior, es momento de hacernos una pregunta ¿Qué tanto estoy publicando y qué tipo de información publico en la red?

Como usuarios debemos estar mejor informados sobre todo lo relacionado a redes sociales, articular de manera efectiva la configuración de privacidad, dejando lo que necesitamos, y eliminando lo que no.

Información complementaria:

- "Guía de seguridad en redes sociales" - http://www.eset-la.com/pdf/documento_redes_sociales_baja.pdf
- "Solo dos de nueve redes sociales protegen por defecto el perfil del usuario" - http://www.abc.es/20110930/medios-redes/abci-redes-sociales-privacidad-201109301611.html
- "Seguridad y redes sociales, la perspectiva del usuario" - http://blog.segu-info.com.ar/2011/09/seguridad-y-redes-sociales-la.html#axzz1ceX77KTO

Referencias

[1] Google Indexes Facebook Comments on Website – Digital Inspiration - http://www.labnol.org/internet/google-indexes-facebook-comments/20295/
[2] Social Engineering: The Art of Human Hacking – Chris Hadnagy - Wiley; 1 edition (December 21, 2010)
[3] Social Engineering: http://en.wikipedia.org/wiki/Social_engineering_%28security%29
[4] Opción frustrada de navegación segura en Facebook – Subdirección de seguridad de la información Unam (México) - http://www.seguridad.unam.mx/noticias/?noti=4337
[5] Regresa cookie espía de Facebook - Subdirección de seguridad de la información Unam (México) - http://www.seguridad.unam.mx/noticias/?noti=4903
[6] Guía de seguridad en Facebook – Inteco (España) http://www.inteco.es/file/nVpd_oWQOoblBIiD4wnTxQ
[7] Guía de seguridad en Twitter – Inteco (España) http://www.inteco.es/file/oGJXYRVkJXnLSDCfeJCkbA
[8] Guía de seguridad en Twitter – Inteco (España) http://www.inteco.es/file/nVpd_oWQOoZRK6aoe7iZKg
[9] Slides sobre seguridad en FourSquare – Alicantevor http://www.slideshare.net/Alicantevor/accin-24-seguridad-en-foursquare
[10] Delincuentes usan Facebook y Twitter para captar víctimas - http://www.seguridad.unam.mx/noticias/?noti=4881

Créditos

.Seguridad, Cultura de prevención para TI

Galvy Ilvey Cruz Valencia
Edición

Johnny Villalobos Murillo
Anaid Guevara Soriano
Alejandro Reyes Plata
Erika Gladys De León Guerrero
Galvy Ilvey Cruz Valencia
Jeffrey Steve Borbón Sanabria
Colaboraciones

Ing. Rubén Aquino Luna
Subdirector de Seguridad de la Información
UNAM-CERT

Luis Edgar García Chávez
Israel Andrade Canales
Iván Mauricio Alvarado Limones
Angie Aguilar Domínguez
Revisión de Contenidos

Iván Yossi Santa María González
Diseño y Desarrollo Web