



Ataques informáticos

Debilidades de seguridad comúnmente explotadas



Autor: Jorge Mieres
E-Mail: jorge.mieres.ef@gmail.com
www.evilfingers.com (enero de 2009)

White paper

Contenido

- 3. Introducción
- 4. ¿De qué estamos hablando?
- 5. Anatomía de un ataque informático
- 7. Aspectos de seguridad que compromete un ataque
- 8. Debilidades de seguridad comúnmente explotadas
 - 8. Ingeniería Social
 - 9. Factor Insiders
 - 10. Códigos maliciosos
 - 11. Contraseñas
 - 12. Configuraciones predeterminadas
 - 13. OSINT (Open Source Intelligence)
- 16. Palabras finales
- 17. Bibliografía



Introducción

A lo largo del tiempo, el avance de los medios tecnológicos y de comunicación ha provocado el surgimiento de nuevos vectores de ataques y de nuevas modalidades delictivas que han transformado a Internet y las tecnologías informáticas en aspectos sumamente hostiles para cualquier tipo de organización, y persona, que tenga equipos conectados a la World Wide Web.

A diferencia de lo que sucedía años atrás, donde personas con amplias habilidades en el campo informático disfrutaban investigando estos aspectos con el ánimo de incorporar mayor conocimiento; en la actualidad se ha desvirtuado completamente dando origen a nuevos personajes que utilizan los medios informáticos y el conocimiento sobre su funcionamiento como herramientas para delinquir y obtener algún beneficio económico.

Cada día se descubren nuevos puntos débiles y, por lo general, son pocos los responsables de IT que comprenden en su justa medida la importancia que tiene la seguridad y cómo pueden abordar el grave problema que existe detrás de vulnerabilidades que permiten a un atacante, violar la seguridad de un entorno y cometer delitos en función de los datos robados.

Bajo esta escenografía donde los principales actores son las organizaciones de cualquier magnitud y rubro, los sistemas de información, el dinero y delincuentes informáticos; se torna realmente necesario y fundamental idear estrategias de seguridad que permitan establecer barreras defensivas orientadas a mitigar efectivamente ataques tanto externos como internos.

Pero para lograr mitigar de manera eficaz el impacto provocado por los ataques informáticos, es de capital importancia conocer de qué manera atacan y cuáles son los puntos débiles de un sistema comúnmente explotados en los que se deben enfocar los esfuerzos de seguridad tendientes a la prevención de los mismos.

En consecuencia, el presente documento pretende ofrecer una rápida visión sobre las debilidades comúnmente explotadas por atacantes para traspasar los esquemas de seguridad en los sistemas informáticos, junto a posibles contramedidas bajo las cuales es posible ampararse para prevenir de manera efectiva los diferentes tipos de ataques que diariamente recibe un sistema.



¿De qué estamos hablando?

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

Para minimizar el impacto negativo provocado por ataques, existen procedimientos y mejores prácticas que facilitan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques.

Uno de los pasos más importantes en seguridad, es la educación. Comprender cuáles son las debilidades más comunes que pueden ser aprovechadas y cuáles son sus riesgos asociados, permitirá conocer de qué manera se ataca un sistema informático ayudando a identificar las debilidades y riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas.



Anatomía de un ataque informático

Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque.

La siguiente imagen¹ muestra las cinco etapas por las cuales suele pasar un ataque informático al momento de ser ejecutado:

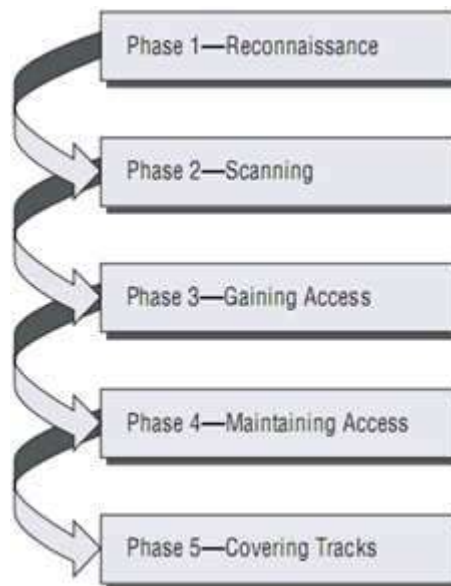


Figura 1. Fases comunes de un ataque informático

Fase 1: Reconnaissance (Reconocimiento). Esta etapa involucra la obtención de información (*Information Gathering*) con respecto a una potencial víctima que puede ser una persona u organización.

Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social, el *Dumpster Diving*, el *sniffing*.

Fase 2: Scanning (Exploración). En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.

Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el *network mappers*, *port mappers*, *network scanners*, *port scanners*, y *vulnerability scanners*.

¹ Official Certified Ethical Hacker Review Guide.

Fase 3: Gaining Access (Obtener acceso). En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema (*Flaw exploitation*) descubiertos durante las fases de reconocimiento y exploración.

Algunas de las técnicas que el atacante puede utilizar son ataques de *Buffer Overflow*, de *Denial of Service (DoS)*, *Distributed Denial of Service (DDoS)*, *Password filtering* y *Session hijacking*.

Fase 4: Maintaining Access (Mantener el acceso). Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos.

Fase 5: Covering Tracks (Borrar huellas). Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS).

*"Si utilizas al enemigo para derrotar al enemigo, serás poderoso en cualquier lugar a donde vayas."*²

² Sun Tzu, El arte de la guerra.



Aspectos de seguridad que compromete un ataque

La seguridad consta de tres elementos fundamentales que forman parte de los objetivos que intentan comprometer los atacantes. Estos elementos son la confidencialidad, la integridad y la disponibilidad de los recursos.

Bajo esta perspectiva, el atacante intentará explotar las vulnerabilidades de un sistema o de una red para encontrar una o más debilidades en alguno de los tres elementos de seguridad.

Para que, conceptualmente hablando, quede más claro de qué manera se compromete cada uno de estos elementos en alguna fase del ataque, tomemos como ejemplo los siguientes casos hipotéticos según el elemento que afecte.

Confidencialidad. Un atacante podría robar información sensible como contraseñas u otro tipo de datos que viajan en texto claro a través de redes confiables, atentando contra la confidencialidad al permitir que otra persona, que no es el destinatario, tenga acceso a los datos. Un ejemplo que compromete este elemento es el envenenamiento de la tabla ARP (*ARP Poisoning*).

Integridad. Mientras la información se transmite a través del protocolo de comunicación, un atacante podría interceptar el mensaje y realizar cambios en determinados bits del texto cifrado con la intención de alterar los datos del criptograma. Este tipo de ataques se denomina *Bit-Flipping* y son considerados ataques contra la integridad de la información.

El ataque no se lleva a cabo de manera directa contra el sistema de cifrado pero sí en contra de un mensaje o de una serie de mensajes cifrados. En el extremo, esto puede convertirse en un ataque de denegación de servicio contra todos los mensajes en un canal que utiliza cifrado.

Disponibilidad. En este caso, un atacante podría utilizar los recursos de la organización, como el ancho de banda de la conexión DSL para inundar de mensaje el sistema víctima y forzar la caída del mismo, negando así los recursos y servicios a los usuarios legítimos del sistema. Esto se conoce como *Denial of Service (DoS)* y atenta directamente contra la integridad de la información.



Debilidades de seguridad comúnmente explotadas

Afortunadamente, en la actualidad existe una gama muy amplia de herramientas de seguridad lo suficientemente eficaces que permiten obtener un adecuado nivel de seguridad ante intrusiones no autorizadas haciendo que la labor de los atacantes se transforme en un camino difícil de recorrer.

Ingeniería Social

Sin embargo, más allá de cualquiera de los esquemas de seguridad que una organización pudiera plantear, existen estrategias de ataque que se basan en el engaño y que están netamente orientadas a explotar las debilidades del factor humano: la **Ingeniería Social**. Los atacantes saben cómo utilizar estas metodologías y lo han incorporado como elemento fundamental para llevar a cabo cualquier tipo de ataque.

Si bien esta técnica es utilizada en cualquier ámbito, en lo que a informática se refiere, consiste en la obtención de información sensible y/o confidencial de un usuario cercano a una sistema u organización explotando ciertas características que son propias del ser humano.

Sin lugar a dudas, las personas constituyen uno de los problemas más importantes de seguridad para cualquier organización porque a diferencia de los componentes tecnológicos, son el único elemento, dentro de un entorno seguro, con la capacidad de decidir “romper” las reglas establecidas en las políticas de seguridad de la información.

Ya sea por ignorancia, negligencia o coacción, pueden permitir a un atacante obtener acceso no autorizado, quien, de esta manera, podrá eludir los complejos esquemas y tecnologías de seguridad que se hayan implementado en la organización. Por ejemplo, en este sentido, la confianza y la divulgación de información son dos de las debilidades más explotadas para obtener datos relacionados a un sistema.

Como **contramedida**, la única manera de hacer frente a los métodos de Ingeniería Social es la educación. Absolutamente todas las personas que forman parte de la organización, desde la secretaria, los administradores de la red y la cúpula mayor, deben estar capacitados en cuanto a las debilidades y los métodos de engaño más empleados por los atacantes para que logren identificarlos y dar aviso de cualquier anomalía que se produzca en el equipo o en determinado ambiente.

Esto no significa que cada uno de los empleados deba realizar cursos de seguridad informática, sino que el proceso de capacitación debe formar parte de las Políticas de Seguridad de la Información y debe ser ejecutada a través de planes dinámicos de concientización.



Por otro lado, es muy común que el personal crea erróneamente que su posición dentro de la Institución u organización es de poca importancia y que por lo tanto no podrían ser objeto de ataque, pero contrariamente, son en realidad los objetivo preferidos por los atacantes; en consecuencia, la educación es una contramedida muy efectiva, pero es de suma importancia que las personas tomen real conciencia de que ellos son el blanco perfecto de la Ingeniería Social.

"Usted puede tener implementada la mejor tecnología, Firewalls, sistemas de detección de intrusos o complejos sistemas de autenticación biométricos... Pero lo único que se necesita es una llamada telefónica a un empleado desprevenido y acceden al sistema sin más. Tienen todo en sus manos"³

Factor Insiders

Cuando se habla sobre las personas que se dedican a atacar sistemas informáticos, se asume que se trata de alguien desconocido que realiza el ataque y maneja todo desde un lugar remoto llevándolo a cabo a altas horas de la noche. Aunque en algunos casos puede ser cierto, varios estudios han demostrado que la mayoría de las violaciones de seguridad son cometidos por el **Factor Insiders**, es decir, por los mismos empleados desde dentro de la Institución u Organización.

Una de las formas más eficaces que posee un atacante para romper los esquemas de seguridad, es desde el interior de la organización. Por ejemplo, el atacante podría conseguir un empleo en la organización que desea atacar y obtener el suficiente nivel de confianza en la organización para luego explotar los puntos de acceso. Del mismo modo, cualquier integrante puede convertirse en un empleado disgustado y decidir robar información y/o causar daños como una forma de venganza.

Cuando este tipo de actos es cometido con intenciones de obtener beneficios económicos a través de información corporativa, es denominado *Insiders Trading* (comercio de personal interno).

En cualquiera de los casos, muchas de las herramientas y medidas de seguridad que se implementen en el entorno informático no serán eficaces. Bajo esta perspectiva, es necesario acudir a estrategias de defensa internas y específicas para el control de posibles ataques ocasionados por el personal de la organización. Estas estrategias defensivas funcionarán como **contramedidas**.

Una de las mejores soluciones es realizar auditorias continuas que incluyan monitoreos a través de programas keyloggers que pueden ser por hardware o por software, mecanismos que impidan la instalación de programas por parte del personal, estricta configuración del principio de privilegios mínimos, deshabilitación de puertos USB y prohibición del uso de dispositivos de almacenamiento extraíbles para evitar la fuga de información y entrada de otras amenazas como malware, si las computadoras forman parte de un dominio es necesario establecer políticas rigurosas en el *Active Directory*, entre otras.

³ Kevin Mitnick, The Art of Intrusión.



"...si piensas que la tecnología puede resolver todos los problemas de seguridad, entonces no entiendes el problema y no entiendes la tecnología"⁴

Códigos maliciosos

Los **códigos maliciosos**, o **malware**, constituyen también una de las principales amenazas de seguridad para cualquier Institución u Organizaciones y aunque parezca un tema trivial, suele ser motivo de importantes pérdidas económicas.

Esta amenaza se refiere a programas que causan algún tipo de daño o anomalía en el sistema informático. Dentro de esta categoría se incluyen los programas troyanos, gusanos, virus informáticos, spyware, backdoors, rootkits, keyloggers, entre otros.

Actualmente, casi el 80% de los ataques informáticos llevados a cabo por códigos maliciosos, se realizan a través de programas troyanos.⁵ Este tipo de malware ingresa a un sistema de manera completamente subrepticia activando una carga dañina, denominada *payload*, que despliega las instrucciones maliciosas.

La carga dañina que incorporan los troyanos puede ser cualquier cosa, desde instrucciones diseñadas para destruir algún sector del disco rígido, por lo general la MBR, eliminar archivos, registrar las pulsaciones que se escriben a través del teclado, monitorear el tráfico de la red, entre tantas otras actividades.

Los atacantes suelen utilizar troyanos de manera combinada junto a otros tipos de códigos maliciosos. Por ejemplo, cuando han ganado acceso a través del troyano, implantan en el sistema otros códigos maliciosos como rootkits que permite esconder las huellas que el atacante va dejando en el equipo (*Covering Tracks*), y backdoors para volver a ingresar al sistema cuantas veces considere necesario; todo, de manera remota y sin que, en la mayoría de los casos, los administradores de la red adviertan su actividad.

Si bien cualquier persona con conocimientos básicos de computación puede crear un troyano y combinar su *payload* con programas benignos a través de aplicaciones automatizadas y diseñados para esto, los troyanos poseen un requisito particular que debe ser cumplido para que logren el éxito: necesitan la intervención del factor humano, en otras palabras, tienen que ser ejecutados por el usuario.

Es por ello que estas amenazas se diseminan por medio de diferentes tecnologías como dispositivos USB, mensajería instantánea, redes P2P, e-mail, etcétera; a través de alguna metodología de engaño (Ingeniería Social), aparentando ser programas inofensivos bajo coberturas como protectores de pantalla, tarjetas virtuales, juegos en flash, diferentes tipos de archivos, simulando ser herramientas de seguridad, entre tantos otros.

Con respecto a los ataques internos, ya comentado en **Factor Insiders**, suele ser común la ejecución de malware por parte de los empleados, instalar programas *keyloggers* o realizar

⁴ Bruce Schneier, *Secrets & Lies*.

⁵ Informe sobre malware en América Latina, Laboratorio ESET Latinoamérica.



ataques *ARP Poisoning*, con el ánimo de capturar información privada como datos de autenticación.

Las **contramedidas** tendientes a prevenir ataques a través de este tipo de amenazas, radican principalmente en la implementación de programas antivirus que operen bajo mecanismos de detección avanzados como la heurística, que también permitan monitorear, controlar y administrar de manera centralizada cada uno de los nodos involucrados en la red, junto a planes de educación orientados a crear conciencia en el personal sobre los riesgos de seguridad que representa el malware.

*"Pero, vamos, pasa a otro tema y canta la estratagema del caballo de madera que fabricó Epeo con la ayuda de Atenea; la emboscada que en otro tiempo condujo el divino Odiseo hasta la Acrópolis, llenándola de los hombres que destruyeron Ilíon."*⁶

Contraseñas

Otro de los factores comúnmente explotados por los atacantes son las **contraseñas**. Si bien en la actualidad existen sistemas de autenticación complejos, las contraseñas siguen, y seguirán, siendo una de las medidas de protección más utilizadas en cualquier tipo de sistema informático.

En consecuencia, constituyen uno de los blancos más buscados por atacantes informáticos porque conforman el componente principal utilizado en procesos de autenticación simple (usuario/contraseña) donde cada usuario posee un identificador (nombre de usuario) y una contraseña asociada a ese identificador que, en conjunto, permiten identificarse frente al sistema.

En este tipo de proceso, llamado de factor simple, la seguridad del esquema de autenticación radica inevitablemente en la fortaleza de la contraseña y en mantenerla en completo secreto, siendo potencialmente vulnerable a técnicas de Ingeniería Social cuando los propietarios de la contraseña no poseen un adecuado nivel de capacitación que permita prevenir este tipo de ataques.

Si el entorno informático se basa únicamente en la protección mediante sistemas de autenticación simple, la posibilidad de ser víctimas de ataques de *cracking* o intrusiones no autorizadas se potencia. Sumado esto a que existen herramientas automatizadas diseñadas para "romper" las contraseñas a través de diferentes técnicas como ataques por fuerza bruta, por diccionarios o híbridos en un plazo sumamente corto, el problema se multiplica aún más.

Sobre la base de lo anteriormente explicado, se puede suponer que la solución ante este problema es la creación de contraseñas mucho más largas (lo cual no significa que sean robustas). Sin embargo, esta estrategia sigue siendo poco efectiva, simplemente, porque el personal no se encuentra preparado para recordar largas cadenas de caracteres y terminan

⁶ La Odisea de Homero. Canto VIII, 490.



escribiéndolas en lugares visibles o sitios accesibles por cualquier otra persona, incluso, ante personas que no pertenecen a determinada área de acceso restringido.

Si bien es cierto que una contraseña que supere los diez caracteres y que las personas puedan recordar, es mucho más efectiva que una contraseña de cuatro caracteres, aún así, existen otros problemas que suelen ser aprovechados por los atacantes. A continuación se expone algunos de ellos:

- La utilización de la misma contraseña en varias cuentas y otros servicios.
- Acceder a recursos que necesitan autenticación desde lugares públicos donde los atacantes pueden haber implantado programas o dispositivos físicos como *keyloggers* que capturen la información.
- Utilización de protocolos de comunicación inseguros que transmiten la información en texto claro como el correo electrónico, navegación web, chat, etcétera.
- Técnicas como *surveillance* (videoconferencia) o *shoulder surfing* (mirar por detrás del hombro), entre otras tantas, que permiten evadir los controles de seguridad.

Como **contramedida** destinada a fortalecer este aspecto de la seguridad, es posible implementar mecanismos de autenticación más robustos como “autenticación fuerte de doble factor”, donde no sólo se necesita contar con algo que se conoce (la contraseña) sino que también es necesario contar con algo que se tiene, como por ejemplo una llave electrónica USB o una tarjeta que almacene certificados digitales para que a través de ellos se pueda validar o no el acceso de los usuarios a los recursos de la organización.

"De nada sirve utilizar contraseñas fuertes si luego son olvidadas o compartidas, ya que con ello se compromete la seguridad de todo el mecanismo de autenticación."

Configuraciones predeterminadas

Las **configuraciones por defecto**, tanto en los sistemas operativos, las aplicaciones y los dispositivos implementados en el ambiente informático, conforman otra de las debilidades que comúnmente son poco atendidas por pensar erróneamente que se tratan de factores triviales que no se encuentran presentes en la lista de los atacantes.

Sin embargo, las configuraciones predeterminadas hacen del ataque una tarea sencilla para quien lo ejecuta ya que es muy común que las vulnerabilidades de un equipo sean explotadas a través de códigos *exploit* donde el escenario que asume dicho código se basa en que el objetivo se encuentra configurado con los parámetros por defecto.

Muchas aplicaciones automatizadas están diseñadas para aprovechar estas vulnerabilidades teniendo en cuenta las configuraciones predeterminadas, incluso, existen sitios web que almacenan bases de datos con información relacionada a los nombres de usuario y sus contraseñas asociadas, códigos de acceso, configuraciones, entre otras, de los valores por defecto de sistemas operativos, aplicaciones y dispositivos físicos. Sólo basta con escribir en un buscador las palabras claves “*default passwords*” (contraseña por defecto) para ver la infinidad de recursos disponibles que ofrecen este tipo de información.



Por lo tanto, una de las **contramedidas** más eficaces para mitigar y prevenir problemas de seguridad en este aspecto, y que muchas veces se omite, es simplemente cambiar los valores por defecto. En este sentido, es importante no sacrificar la disponibilidad de los recursos por ganar seguridad. Se debe encontrar un equilibrio justo entre usabilidad y seguridad.

La práctica de fortalecer el ambiente informático configurando de manera segura la tecnología para contrarrestar los vectores de ataque se denomina *hardening*. En este aspecto, la responsabilidad de realizar todo lo que se encuentre a su alcance para modificar los valores predeterminados recae en quienes se encargan de la administración de los equipos.

Es importante que durante el proceso de *hardening* también se verifiquen otros aspectos como las opciones que se configuran de manera predeterminada al instalar sistemas operativos y demás recursos, como los nombres de rutas, nombres de carpetas, componentes, servicios, configuraciones y otros ajustes necesarios, o innecesarios, que brinden un adecuado nivel de protección.

"Nada hace que atacar un objetivo dentro de una red sea tan fácil como cuando los objetivos se encuentran con los valores por defecto establecidos por el fabricante del dispositivo." ⁷

OSINT (Open Source Intelligence)

Los atacantes, sobre todo los atacantes externos, aprenden constantemente técnicas de ataque que le permiten penetrar los esquemas de seguridad por más complejos que sean. En consecuencia, la pregunta que inmediatamente viene a colación es ¿cómo lo logran?, y aunque la respuesta pudiera parecer un tanto compleja, resulta más sencilla de lo que se imagina. La respuesta es investigación.

Una de las primeras facetas de un ataque informático, consiste en la recolección de información a través de diferentes técnicas como *reconnaissance*, *discovery*, *footprinting* o *Google Hacking*; y precisamente, **Open Source Intelligence** (Inteligencia de fuentes abiertas) se refiere a la obtención de información desde fuentes públicas y abiertas.

La información recolectada por el atacante, no es más que la consecuencia de una detallada investigación sobre el objetivo, enfocada a obtener toda la información pública disponible sobre la organización desde recursos públicos. En este aspecto, un atacante gastará más del 70% de su tiempo en actividades de reconocimiento y obtención de información por que cuanto más aprende el atacante sobre el objetivo, más fácil será llevar a cabo con éxito el ataque.

Lo realmente preocupante es la falta de conciencia en este sentido, ya que no caben dudas de que la información es el bien más importante para cualquier tipo de organización. En la mayoría de los casos, las empresas brindan una enorme cantidad de datos que hacen de la

⁷ Ten ways hackers breach security. Global Knowledge.



tarea de recolectar información una cuestión tan sencilla como la lectura de este artículo.

Generalmente, los atacantes hacen inteligencia sobre sus objetivos durante varios meses antes de comenzar las primeras interacciones lógicas contra el objetivo a través de diferentes herramientas y técnicas como el *scanning*, *banner grabbing* (captura de titulares) y rastreo de los servicios públicos. Aún así, estas actividades son sólo sondeos sutiles que buscan verificar los datos obtenidos.

Los responsables de las organizaciones se sorprenderían al ver el enorme caudal de información que se puede encontrar en Internet sobre, no sólo las actividades propias de la organización, sino que también, información sobre las actividades de los empleados y su familia.

A través del siguiente listado se refleja algunos ejemplos concretos sobre el tipo y sensibilidad de la información que un atacante podría obtener haciendo OSINT:

- Los nombres de sus altos jefes/ejecutivos y de cualquier empleado pueden ser obtenidos desde comunicados de prensa.
- La dirección de la empresa, números telefónicos y números de fax desde diferentes registros públicos o directamente desde el sitio web.
- Qué, o cuáles, empresas proveen el servicio de Internet (ISP) a través de técnicas sencillas como *DNS lookup* y *traceroute*.
- La dirección del domicilio del personal, sus números telefónicos, currículum vitae, datos de los familiares, puestos en los que desempeña funciones, antecedentes penales y mucho más buscando sus nombres en diferentes sitios.
- Los sistemas operativos que se utilizan en la organización, los principales programas utilizados, los lenguajes de programación, plataformas especiales, fabricantes de los dispositivos de networking, estructura de archivos, nombres de archivos, la plataforma del servidor web y mucho más.
- Debilidades físicas, accesspoint, señales activas, endpoint, imágenes satelitales, entre otras.
- Documentos confidenciales accidentalmente, o intencionalmente, enviados a cuentas personales de personas que no en la actualidad no guardan relación alguna con la organización, más allá del paso por la misma.
- Vulnerabilidades en los productos utilizados, problemas con el personal, publicaciones internas, declaraciones, políticas de la institución.
- Comentarios en blogs, críticas, jurisprudencia y servicios de inteligencia competitiva.

Como se puede apreciar, no hay límite a la información que un atacante puede obtener desde fuentes públicas abiertas donde, además, cada dato obtenido puede llevar al descubrimiento de más información.

En cuanto a las medidas preventivas que se pueden implementar, existe un punto de partida delimitado por la información que ya se encuentra en Internet y aquella que se publicará a futuro en fuentes públicas.

En el primero de los casos, una vez que la información se encuentra en Internet siempre está allí disponible sin poder ser modificada o eliminada, por consiguiente, continuará erosionando sobre la seguridad de la entidad. De todas formas, siempre queda la posibilidad



de limpiar cualquier recurso de información que se encuentre bajo su control directo, poniéndose en contacto con quienes poseen la información y solicitar que la cambien.

Con respecto a la información que se publicará, antes de hacerlo se debe ejecutar contramedidas efectivas que contemplen la protección de cierto tipo de información. Esto se logra a través de políticas de seguridad rigurosas tendientes a controlar o limitar la información que en el futuro sale al mundo exterior de la organización, siendo discreto en los anuncios, en detalles sobre proyectos y productos, comunicados de prensa, etcétera.

“La mayoría de las organizaciones son hemorragias de datos; las empresas dan libremente demasiada información que puede ser utilizada en su contra a través de diversos tipos de ataques lógicos y físicos.”⁸

⁸ Ten ways hackers breach security. Global Knowledge.



Palabras finales

Es sumamente necesario actuar de manera proactiva frente a los posibles ataques que puede sufrir la organización. Esto se logra buscando los problemas con la misma dedicación con la que los atacantes buscan vulnerabilidades a explotar.

Se debe tener en cuenta que una vez que el atacante ha obtenido acceso al sistema, lo primero que hará es implantar herramientas que permitan ocultar sus rastros (rootkits) e ingresar al equipo cada vez que lo necesite sin importar desde donde acceda (backdoors) logrando obtener un mayor grado de control sobre el objetivo. Además, una intrusión no autorizada puede ser no detectada casi indefinidamente si es llevado a cabo por un atacante con mucha paciencia.

Existen múltiples puntos de acceso y caminos que el atacante puede seguir para obtener información y acceso a un entorno que se considera seguro. Por lo tanto, no obviar ninguna de las cuestiones relacionadas al ambiente informático por mínimas que parezcan, y seguir las mejores prácticas recomendadas por los profesionales de seguridad es un buen consejo a tener en cuenta.

Recuerde siempre que el enemigo es la ignorancia y que el desconocimiento siempre favorece a los atacantes.



Bibliografía

- Informe sobre malware en América Latina, Laboratorio ESET Latinoamérica, 2008.
<http://www.eset-la.com/threat-center/1732-informe-malware-america-latina>
- Ten ways hackers breach security. Global Knowledge. 2008
<http://images.globalknowledge.com>
- Bruce Schneier, Secrets & Lies. Digital Security in a Networked World. John Wiley & Sons, 2000.
- Kevin Mitnick, The Art of Intrusión. John Wiley & Sons, 2005.
- La Odisea de Homero.
- Official Certified Ethical Hacker, Sybex. 2007.
- Sun Tzu, El arte de la guerra. Versión de Samuel Griffith. Editorial Taschen Benedikt. 2006.