

## Ataques informáticos, debilidades y contramedidas

Jorge Mieres

[jamieres@gmail.com](mailto:jamieres@gmail.com)

Fecha Publicación: 17/01/2009

### Introducción

*A lo largo del tiempo, el avance de los medios tecnológicos y de comunicación han 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 realmente comprenden la importancia que tiene la seguridad y cómo pueden abordar el gran problema que existe detrás de las 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 más explotadas por los atacantes para traspasar los esquemas de seguridad en los sistemas informáticos junto a las posibles contramedidas bajo las cuales se puede amparar 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 en los activos de la organización.

Para evitar ser víctimas de cualquier tipo de ataques, existen procedimientos y mejores prácticas que facilitan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques informáticos minimizando el horizonte de la ventana de vulnerabilidades en la organización.

En primera instancia, es sumamente importante comprender cuáles son las debilidades del sistema que pueden ser aprovechadas por potenciales amenazas, y cuáles son los riesgos asociados ante los cuales se debe proteger la organización. El segundo paso, y uno de los más importantes en seguridad, es la educación. Conocer de qué manera se ataca un sistema informático permitirá identificar cuáles son las debilidades, las amenazas y los riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas.

### *Anatomía de un ataque informático*

Conocer las diferentes fases que conforman un ataque informático brinda la ventaja de poder pensar como los atacantes, al mismo tiempo se respetar su mentalidad y se aprende a jamás subestimarla. 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 imagen muestra las cinco facetas que suelen estar involucradas en un ataque:

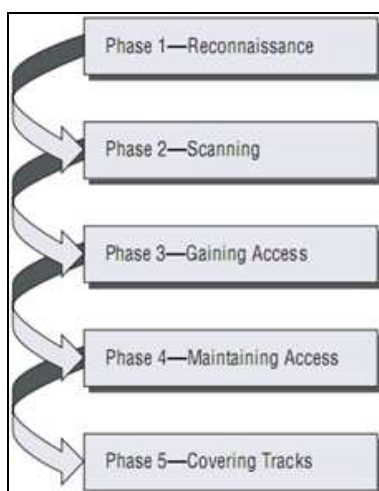


Figura 1. Fases comunes de un ataque informático <sup>1</sup>

<sup>1</sup> Official Certified Ethical Hacker.

**Fase 1: Reconnaissance (Reconocimiento).** Esta etapa involucra la recolección de información (*Information Gathering*) con respecto a una potencial víctima. Por lo general, la recolección se realiza buscando en Internet o buscando en Google los datos de una persona o de alguna organización. Algunas de las técnicas utilizadas en esta faceta 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 a atacar como direcciones IP, nombres de host, datos de autenticación, entre otros. Entre las herramientas que un atacante puede emplear durante la exploración se puede mencionar: *network mappers*, *port mappers*, *network scanners*, *port scanners*, y *vulnerability scanners*.

**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. Entre las técnicas que el atacante puede utilizar se encuentran el *Buffer Overflow*, *Denial of Service (DoS)*, *Distributed Denial of Service (DDoS)*, *Password filtering* y el *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. Por ejemplo, pueden recurrir a utilidades backdoors, rootkits y troyanos.

**Fase 5: Covering Tracks (Borrar huellas).** Una vez que el atacante ha sido capaz de 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, intentará 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.”<sup>2</sup>*

### **Aspectos de seguridad compromete un ataque**

La seguridad consta de tres elementos fundamentales que, en definitiva, constituyen los objetivos que intentan comprometer los atacantes: la confidencialidad, la integridad y la disponibilidad de los recursos (

Ver Boletín de Segu-Info Nro 97 “Fundamentos sobre Seguridad de la Información”: [www.segu-info.com.ar/boletin/](http://www.segu-info.com.ar/boletin/)

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.

---

<sup>2</sup> Sun Tzu, El arte de la guerra.

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

**Confidencialidad.** El robo de información sensible como las contraseñas u otro tipo de información que viajan en texto claro a través de redes confiables, atenta contra la confidencialidad, ya que permite a otra persona que no es el destinatario tenga acceso a los datos.

**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

Este tipo de ataque no es directamente contra el sistema de cifrado pero es 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 utilizan cifrado.

Ver Boletín de Segu-Info Nro 108 “Fundamentos sobre Criptografía”

[www.segu-info.com.ar/boletin/](http://www.segu-info.com.ar/boletin/)

**Disponibilidad.** 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)*.

Si bien un ataque de *Denial of Service* puede ser llevado a cabo a través de diferentes técnicas, siempre ataca contra la disponibilidad de los recursos de información.

### ***Debilidades de seguridad comúnmente explotadas***

En la actualidad, existen diferentes implementaciones de seguridad como *firewalls*, *IDS*, *IPS*, *honeynets*, programas antimalware, entre otros, cuyos mecanismos suelen ser muy efectivos contra gran parte de intentos de intrusiones no autorizadas, haciendo un tanto más difícil la tarea del atacante.

### **Ingeniería Social**

Sin embargo, más allá de cualquiera de los esquemas de seguridad planteados, existen estrategias a las cuales recurren los atacantes basadas en el engaño, 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.

Ver Boletín de Segu-Info Nro 30 “Uso de la Ingeniería Social”

[www.segu-info.com.ar/boletin/](http://www.segu-info.com.ar/boletin/)

Ver Cruzada Antifraude de Segu-Info: [www.segu-info.com.ar/cruzada/](http://www.segu-info.com.ar/cruzada/)

Ver Segu-Info “Tipos de ataques”: [www.segu-info.com.ar/ataques/](http://www.segu-info.com.ar/ataques/)

Si bien esta técnica es utilizada en cualquier ámbito, en lo que a informática se refiere, la Ingeniería Social consiste en la obtención de información sensible y/o confidencial de los usuarios que forman parte de un sistema informático.

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 es 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.

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”<sup>3</sup>*

### 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

---

<sup>3</sup> Kevin Mitnick, The Art of Intrusión.

cometidos por el **Factor Insiders**, es decir, por los mismos empleados desde dentro de la Institución u Organización.

Ver Segu-Info "Insiders"

<http://www.segu-info.com.ar/amenazashumanas/amenazashumanas.htm>.

Una de las formas más eficaces que posee un atacante para romper los esquemas de seguridad, es como empleado. 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.

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 auditorías 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.

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

### 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.

Ver Segu-Info: [www.segu-info.com.ar/virus/](http://www.segu-info.com.ar/virus/)

Actualmente, casi el 80% de los ataques informáticos llevados a cabo por códigos maliciosos, se realizan a través de programas troyanos <sup>5</sup>. Los troyanos ingresan a un sistema de manera completamente subrepticia

<sup>4</sup> Bruce Schneier, *Secrets & Lies*.

<sup>5</sup> Informe sobre malware en América Latina, Laboratorio ESET Latinoamérica.

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 (keylogger), monitorear el tráfico de la red (sniffing), entre tantas otras actividades.

Los atacantes suelen utilizar troyanos de manera combinada junto a otros tipos de *malware*. 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 como **Factor Insider**, suele ser común la ejecución de códigos maliciosos como troyanos por parte de los empleados, emplear keylogger o realizar ataques *ARP Poisoning*, entre tantos otros, con el ánimo de capturar información privada como contraseñas de acceso.

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 representan estas amenazas.

*“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 Ilión.”* <sup>6</sup>

---

<sup>6</sup> La Odisea de Homero. Canto VIII, 490.



## 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 computacional.

Ver Artículo de Segu-Info Nro 2 “¿Por qué nuestras passwords?”

[www.segu-info.com.ar/articulos/](http://www.segu-info.com.ar/articulos/)

En consecuencia, constituyen uno de los blancos más buscados por atacantes informáticos porque conforman el componente principal utilizado en procesos de autenticación simple (usuario y contraseña), donde cada usuario posee un identificador, que es el nombre de usuario, y una contraseña asociada a ese identificador, que permite identificar frente al sistema la identidad del usuario en el proceso de autenticación.

En este tipo de proceso, llamado de factor simple, la seguridad del esquema de autenticación planteado radica inevitablemente en mantener la contraseña en secreto, siendo potencialmente vulnerable a técnicas de Ingeniería Social cuando los propietarios de la contraseña no poseen un adecuado nivel de capacitación que permita mitigar 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 ataques híbridos, por fuerza bruta y/o por diccionarios en un plazo sumamente corto, el problema es realmente importante.

Se puede suponer entonces que una buena solución ante este problema, es la creación de contraseñas mucho más largas (lo cual no significa que sean robustas); sin embargo, sigue siendo poco efectivo, simplemente, porque el personal no se encuentra preparado para recordar largas cadenas de caracteres y terminan 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 cuya cantidad de caracteres se encuentre entre 12-18, y que las personas puedan recordar, es mucho más efectiva que una contraseña de 6 caracteres, aún así, existen otros problemas que suelen ser aprovechados por los atacantes entre los cuales se encuentran:

- La utilización de la misma contraseña en varias cuentas y otros servicios;
- el acceso a recursos que necesitan autenticación desde lugares públicos donde los atacantes pueden haber implantado programas o dispositivos físicos que capturen la información;
- el uso de protocolos inseguros al navegar por la web, al utilizar el correo electrónico, en sesiones de chat, etcétera, que transmiten la información en texto plano;



- técnicas que evaden los controles de seguridad como video surveillance (videovigilancia) y shoulder surfing (mirar por detrás del hombro), entre otras tantas.

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 almacena certificados digitales para que a través de ellos se pueda validar o no el acceso de los usuarios.

*“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, estas configuraciones predeterminadas hacen del ataque una tarea sencilla ya que es muy común explotar las vulnerabilidades de un equipo a través de código *exploit* donde el escenario que asume dicho código se basa en que el objetivo se encuentra con las configuraciones por defecto.

Asimismo, muchas aplicaciones automatizadas están diseñadas para aprovechar estas vulnerabilidades teniendo en cuenta las configuraciones predeterminadas, incluso, existen sitios web que llevan una base de 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.

Para ver la verdadera magnitud de este problema, sólo basta con escribir en un buscador las palabras claves “*default passwords*” (contraseña por defecto) para ver la infinidad de recursos disponibles en torno a lo expresado.

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 las configuraciones 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*. Conocer las opciones por defecto de los productos y hacer todo lo que se encuentre al alcance para modificar los valores

predeterminados por alternativas no obvias es responsabilidad de quienes se encargan de la administración de los equipos.

Pero hacer *hardening* no se trata sólo de preocuparse por las contraseñas por defecto, también es importante verificar las opciones predeterminadas que se configuran por defecto 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.

Cuanto más fortalecida se encuentren las instalaciones, los sistemas, aplicaciones y dispositivos, serán más incompatible a herramientas de ataque automatizadas y la explotación de scripts.

*“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.”*<sup>7</sup>

### **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 consecuencia de una detallada investigación sobre el objetivo enfocada a obtener toda la información pública disponible sobre la Institución/organización desde recursos públicos; y en este aspecto, un atacante gastará más del 90% de su tiempo en actividades de reconocimiento y obtención de información porque cuanto más aprende el atacante sobre el objetivo, más fácil será llevar a cabo con éxito el ataque.

En este sentido, lo realmente preocupante es cuánto colaboran los entes en la obtención de este tipo de información por parte de atacante, sobre todo, cuando ya no caben dudas de que la información es el bien más importante para cualquier tipo de organización. La realidad es que, en la mayoría de los casos, las empresas brindan demasiada información que hacen que recolectar información, para el atacante, sea 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 blanco a través de herramientas y técnicas, como se mencionó

---

<sup>7</sup> Ten ways hackers breach security. Global Knowledge.

líneas arriba, de exploración, *banner grabbing* (captura de titulares) y rastreo de los servicios públicos; y 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 de la organización, sino que también, información sobre sus actividades y familia.

Algunos de los ejemplos de información que se puede recolectar a través de fuentes abiertas, se reflejan en el siguiente listado:

Los nombres de sus altos jefes/ejecutivos y de cualquier empleado pueden ser obtenidos desde comunicados de prensa.

La dirección de la empresa/institución, 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 varios 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 puede prevenir poner al alcance desde fuentes públicas. Lamentablemente esto es así por que 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.

En consecuencia, como **contramedida** efectiva, se debe idear políticas 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.”<sup>8</sup>*

### **Palabras finales**

Como podemos apreciar, cuanto más pueda descubrir el atacante acerca de los potenciales puntos de ataque en el blanco, más probabilidades va a tener de descubrir alguna debilidad que quizás todavía no ha sido solucionada o incluso descubierta.

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

Tenga en cuenta que una vez que el atacante ha logrado 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.

Teniendo en cuenta situaciones donde muchas organizaciones e Instituciones del Estado suelen ser muy pobres en cuanto al manejo de los riesgos asociados al ámbito informático debido a que, por lo general, el departamento de sistemas no cuenta con Políticas de Seguridad claras, no cuenta con los recursos necesarios que permitan implementar estrategias de seguridad efectivas o personal suficiente y capacitado en materia de seguridad o, lo más grave, no cuenta con un área de sistemas.

---

<sup>8</sup> Ten ways hackers breach security. Global Knowledge.

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.

Siempre recuerde 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.