

Diez formas en que los atacantes violan la seguridad

Autor: James Michael Steward, Global Knowledge Instructor

http://images.globalknowledge.com/wwwimages/whitepaperpdf/WP_Steward_Hackers.pdf

Traducción para Segu-Info: Jorge A. Mieres

Revisión: Raul Batista y Lic. Cristian Borghello, CISSP

Fecha Publicación: 13 de septiembre de 2008

Introducción

Hacking, cracking y delitos informáticos son temas latentes en la actualidad y seguirán siéndolo en un futuro previsible. Sin embargo, hay pasos que se pueden dar para reducir el nivel de amenazas en las organizaciones.

El primer paso consiste en entender cuáles son los riesgos, las amenazas y las vulnerabilidades que existen actualmente en tu entorno. El segundo paso es aprender tanto como sea posible sobre los problemas para poder articular una respuesta sólida. El tercer paso radica en desplegar inteligentemente las contramedidas y salvaguardas para construir una protección en torno a los activos más críticos.

Este documento examina los diez métodos que comúnmente son utilizados por los atacantes para violar los esquemas de seguridad.

1. Robo de contraseñas

Los expertos en seguridad han discutido los problemas con las contraseñas de seguridad por años. Pero parece que son pocos los que han escuchado y tomado acciones para resolver esos problemas. Si en su entorno tecnológico los controles de autenticación usan sólo contraseñas, esto es un riesgo mayor ante ataques de hacking e intrusiones comparado con los que utilizan algún esquema de autenticación de factor múltiple.

El problema radica en la siempre creciente capacidad que poseen las computadoras para procesar grandes cantidades de información en un corto plazo. Una contraseña no es más que una cadena de caracteres, por lo general, caracteres del teclado que una persona puede recordar y escribir en una terminal de la computadora cada vez que lo requiera.

Desafortunadamente, las contraseñas que también son complejas de recordar por una persona, pueden ser fácilmente descubiertas por una herramienta de cracking en un periodo terriblemente corto de tiempo. Ataques por diccionario, ataques por fuerza bruta y ataque híbridos son los distintos métodos utilizados para adivinar o romper contraseñas.

La única protección real contra dichas amenazas es crear una contraseña muy larga o utilizar un esquema de autenticación por múltiples factores. Por desgracia, requerir siempre contraseñas más largas causa un retroceso de seguridad debido al factor humano. Simplemente, la gente no se encuentra preparada para recordar numerosas y largas cadenas de caracteres caóticos.

Pero incluso, con contraseñas razonablemente largas que las personas puedan recordar (entre 12 y 16 caracteres), todavía hay otros problemas a los cuales se enfrentan los sistemas de autenticación sólo por contraseñas. Estos incluyen:

- Personas que utilizan la misma contraseña en varias cuentas, especialmente cuando algunas de esas cuentas están en sitios públicos de Internet con poca o ninguna seguridad.
- Personas que escriben y almacenan sus contraseñas en lugares muy evidentes. Escribir las contraseñas es a menudo fomentado por la necesidad de cambiarlas con frecuencia.
- La continua utilización de protocolos inseguros que transfieren las contraseñas en texto plano como los utilizados al navegar por la web, en correos electrónicos, chat, transferencia de archivos, etc.
- La amenaza de los capturadores de teclado (keyloggers) de software y hardware.
- El problema de obtener contraseñas mirando por detrás del hombro (shoulder surfing) y video vigilancia (video surveillance).

Robo de contraseñas, cracking de contraseñas, incluso, adivinar contraseñas, siguen siendo graves amenazas en entornos TI. La mejor protección contra estas amenazas es desplegar sistemas de autenticación múltiple y capacitar al personal en cuanto a los hábitos de crear contraseñas seguras.

2. Troyanos

Los troyanos son amenazas continuas para todas las formas de comunicación TI. Básicamente, un troyano es programa malicioso que subrepticamente activa una carga dañina (payload) e ingresa dentro de un host. Quizás usted haya escuchado sobre alguno de los troyanos más famosos como El Back Orifice, NeuBus o SubSeven.

Pero la amenaza real de los troyanos no es su carga dañina acerca de lo cual se conoce, sino sobre la que no se conoce. Un troyano puede ser creado o diseñado por cualquier persona con conocimientos básicos de computación, y cualquier carga dañina puede ser combinada con cualquier programa benigno para crear un troyano.

Existen numerosas formas de crearlos con herramientas precisamente diseñadas para ello. Por lo tanto, el verdadero problema de estas amenazas es lo desconocido. La carga maliciosa de un troyano puede ser cualquier cosa, incluyendo programas que destruyen el disco rígido, corrompen archivos, registran las pulsaciones que se escriben a través del teclado, monitorear el tráfico de la red, a través de la web, falsificar correos electrónicos, permitir el acceso y control remoto del equipo, transferir archivos e información a terceros, lanzar ataques contra otros objetivos, implantar servidores proxys, servicios para compartir archivos y muchas cosas más. Estas cargas dañinas pueden ser obtenidas de Internet o pueden ser código escrito por el hacker.

En consecuencia, el payload (carga dañina) puede ser embebida en cualquier programa benigno para crear un troyano.

Los anfitriones usuales incluyen: juegos, protectores de pantalla, tarjetas virtuales, herramientas de administración, formatos de archivos, e incluso documentos.

Todo lo que necesita el ataque de un troyano para ser exitoso, es que un usuario lo ejecute en su computadora. Una vez que lo logra, automáticamente se activa su carga maliciosa, generalmente, sin síntomas de actividades no deseadas.

Un troyano podría ser enviado a la víctima a través del correo electrónico como archivo adjunto, podría ser descargado desde un sitio web, o podría ser colocado en un dispositivo extraíble como una tarjeta de memoria, un CD, un DVD, un PenDriver USB, un disquete, etcétera.

En cualquiera de los casos, las protecciones son herramientas automatizadas de detección de códigos maliciosos como las modernas protecciones antivirus, otras formas de protección específicas de escaneo de malware y la educación de los usuarios.

3. Explotación de configuraciones predeterminadas

Nada hace que atacar un objetivo dentro de una red sea tan fácil como cuando esos objetivos se encuentran con los valores por defecto establecidos por el vendedor o fabricante del mismo. Muchas herramientas de ataque y códigos exploit asumen que los objetivos se encuentran con las configuraciones por defecto. Por lo tanto, uno de las más eficaces precauciones de seguridad, y que muchas veces pasada por alto, es simplemente cambiar las configuraciones por defecto.

Para ver el verdadero alcance de este problema, todo lo que necesita hacer es buscar en Internet sitios web a través de las palabras claves “contraseñas por defecto” (“default passwords”). Hay muchos sitios que catalogan todos los nombres de usuarios por defecto, las contraseñas, los códigos de acceso, las configuraciones y convenciones de nombres de todos los programas y dispositivos de TI que se venden. Es su responsabilidad conocer acerca de las opciones por defecto de los productos que instale Ud. y hacer todo lo que se encuentre a su alcance para modificar los valores predeterminados por alternativas no obvias.

Pero no se trata solamente de que se preocupe por las cuentas y contraseñas por defecto, también hay instalaciones con opciones predeterminadas como nombres de rutas, nombres de carpetas, componentes, servicios, configuraciones y otros ajustes.

Todas y cada una de las opciones personalizables deben ser consideradas para personalizar. Trate de evitar la instalación de sistemas operativos en las unidades y carpetas por defecto establecidas por el fabricante. Tampoco instalar aplicaciones en la ubicación “estándar”, ni acepte los nombres de carpeta establecidos por el asistente de instalación o scripts.

Cuanto más personalice sus instalaciones y configuraciones, su sistema será más incompatible con las herramientas de ataques automatizadas y los scripts de explotación.

4. Ataques Hombre en el Medio (Man-in-the-Middle)

Cada persona que están leyendo este documento ha sido objeto de numerosos ataques Man-in-the-Middle. Un ataque MITM se produce cuando un atacante es capaz de engañar al usuario en el establecimiento de un enlace comunicacional con un servidor o servicio a través de una entidad ilegal. La entidad ilegal es el sistema controlado por el delincuente informático.

Este ha sido creado para interceptar la comunicación entre el usuario y el servidor sin dejar que el usuario se percate de que un ataque se ha llevado a cabo. Un ataque MITM funciona engañando de alguna manera al usuario, a su equipo, o a alguna parte de la red para redireccionar tráfico legítimo hacia el sistema de engaño ilegítimo.

Un ataque MITM puede ser tan sencillo como un ataque de phishing por e-mail cuando un correo electrónico aparentemente legítimo es enviado a un usuario con un enlace URL que apunte hacia el sistema de engaño ilegítimo en lugar de ser direccionado al sitio verdadero. El sistema falso tiene un aspecto similar a la interfaz del sitio real que engaña al usuario para que acceda al mismo proveyendo sus credenciales de acceso.

Las credenciales de acceso son duplicadas y luego reenviadas al verdadero servidor. Esta acción abre un vínculo con el servidor real, permitiéndole al usuario interactuar con sus recursos sin el conocimiento de que sus comunicaciones han sido desviadas a través de un sistema malicioso de escucha espía y posiblemente alterando el tráfico.

Los ataques MITM pueden ser realizados utilizando métodos mas complicados como la duplicación de direcciones MAC (Media Access Control - Control de Acceso al Medio), envenenamiento ARP (Address Resolution Protocol - Protocolo de Resolución de Direcciones), envenenamiento de la tabla del router, falsas tablas de enrutamiento, envenenamiento de consultas DNS (Domain Name Server - Servidor de Nombres de Dominio), Secuestro de DNS (DNS Hijacking), Servidores DNS ilegítimos, alteración de archivos HOSTS (pharming local), envenenamiento de la caché local DNS y redireccionamiento proxy. Y sin mencionar la ofuscación de URL, la codificación o manipulación que a menudo se utilizan para ocultar el enlace malicioso.

Para protegerse contra los ataques MITM, es necesario evitar hacer clic en los enlaces encontrados en los mensajes de correo electrónico. Además, siempre verifique que los enlaces de los sitios Web pertenezcan a dominios de confianza o mantienen un cifrado SSL. También, puede utilizar un sistema IDS (Sistema de detección de intrusión) para monitorear el tráfico de la red, así como los DNS y alteraciones del sistema local.

5. Ataques Wireless

Las redes inalámbricas tienen el atractivo de estar libres de cables - la capacidad de ser móviles dentro de la oficina manteniendo la conectividad de la red. Las redes wireless son baratas para desplegar y fácil de instalar.

Por desgracia, el verdadero costo de las redes inalámbricas no se percibe hasta que se considera la seguridad. A menudo es el caso de que el tiempo,

esfuerzo y gastos necesarios para garantizar las redes inalámbricas es mucho más que el despliegue de una red cableada tradicional.

Interferencia, Ataques de Denegación de Servicio (DoS), hijacking, man-in-the middle, eavesdropping, sniffing y muchos ataques más se simplifican para los atacantes cuando se encuentran presentes redes inalámbricas. Sin siquiera mencionar la cuestión de que una red inalámbrica segura (802.11a o 802.11g) por lo general, soportará debajo de los 14 Mbps de rendimiento y luego sólo bajo las distancias y condiciones de transmisión casi ideales. Compare esto con que el estándar mínimo de 100 Mbps para una red cableada, y la economía ya no tiene sentido.

Sin embargo, incluso si su organización oficialmente no autoriza y despliega una red inalámbrica, aun así podría tener vulnerabilidades de red inalámbricas. Muchas organizaciones han descubierto que los trabajadores la han utilizado para desplegar en secreto su propia red inalámbrica.

Ellos pueden hacer esto trayendo su propio punto de acceso inalámbrico (WAP), conectando el cable de red de su escritorio en el WAP y luego volviendo a conectar su equipo a uno de los puertos del router o switch de la WAP.

Esto conserva la conexión de su escritorio a la red y añade conectividad inalámbrica. Con mucha frecuencia, cuando una WAP no aprobada es desplegada, se hace con poca o ninguna seguridad habilitada. De este modo, una WAP de U\$S 50 puede fácilmente abrir una gigantesca brecha de seguridad en una multimillonaria red cableada asegurada.

Para combatir puntos de acceso inalámbricos no autorizados, se debe realizar una inspección regular del sitio. Esto puede ser realizado con una computadora portátil inalámbrica utilizando un detector de redes inalámbricas como NetStumbler o con un dispositivo portátil dedicado.

6. Haciendo la tarea

No quiero decir que los atacantes penetran en su red consiguiendo su trabajo desde la escuela, pero es posible que le sorprenda lo mucho que aprenden en la escuela sobre cómo comprometer la seguridad. Los atacantes, sobre todo los atacantes externos, aprenden a superar las barreras de seguridad investigando su organización. Este proceso puede ser llamado de reconocimiento (reconnaissance), descubrimiento (discovery) o footprinting. En última instancia, esto es producto de una investigación intensiva, enfocada en obtener toda la información disponible sobre su organización de recursos públicos y no tan públicos.

Si ha realizado algún estudio o lectura sobre tácticas de guerra, usted es consciente de que el arma más importante que puede tener a su disposición es la información. Los atacantes lo saben y dedican mucho tiempo y esfuerzo a adquirir un completo arsenal. Lo que a menudo es desconcertante es cuánto su organización contribuye libremente al acopio del arsenal de armas de los atacantes.

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. Aquí sólo se encuentran algunos de los

ejemplos más comunes de la información que un atacante puede obtener sobre su organización, por lo general, en cuestión de minutos:

Los nombres de sus altos ejecutivos y de cualquier empleado llamativo pueden ser obtenidos examinando sus comunicados de prensa.

La dirección de la empresa, números telefónicos y números de fax desde el registro de nombres de dominio.

El proveedor de servicio a Internet a través de DNS lookup y traceroute.

La dirección de la casa de los empleados, sus números telefónicos, currículum vitae de los empleados, los miembros de su familia, antecedentes penales y mucho más buscando sus nombres en varios sitios de investigación gratuitos y pagos.

Los sistemas operativos, los principales programas utilizados, los lenguajes de programación, plataformas especiales, fabricantes de los dispositivos de red utilizados y mucho más desde los anuncios en sitios de empleos.

Debilidades físicas, puntos de ventaja, señales activas, formas de entrada, coberturas para los caminos de acceso y más a través de imágenes satelitales de su empresa y las direcciones de los empleados.

Nombres de usuario, direcciones de correo electrónico, números de teléfono, estructura de archivos, nombres de archivos, tipos de sistemas operativos, la plataforma del servidor web, lenguajes de script, entornos de aplicaciones web y más con escaners de sitios web.

Documentos confidenciales accidentalmente enviados a un sitio web como archivo.org o Google Hacking.

Fallos de los productos, problemas con el personal, publicaciones internas, políticas de la empresa y muchos más desde blogs, comentarios, críticas de la empresa y servicios de inteligencia competitiva.

Como puede ver, no hay fin a la información que un atacante puede obtener desde fuentes públicas abiertas. Esta lista de ejemplos es sólo un comienzo. Cada dato obtenido por el atacante, puede llevar al descubrimiento de más información. A menudo, un atacante gastará más del 90% de su tiempo en actividades de reconocimiento y obtención de información. Cuanto más aprende el atacante sobre el objetivo, más fácil será el posterior ataque.

En cuanto a la defensa, que en última instancia está pérdida, principalmente porque ya es demasiado tarde. Una vez que la información se encuentra en Internet, siempre estará allí disponible. Evidentemente, puede limpiar cualquier recurso de información que se encuentre bajo su control directo. Incluso, puede ponerse en contacto con quienes poseen su información y solicitar que cambien su información.

Algunos sistemas de información en línea como los registros de dominios (pagos), ofrecen privacidad y seguridad en los servicios (por una cuota por supuesto). También se puede controlar o limitar la salida de información en el futuro siendo más discreto en los anuncios, los detalles de productos, comunicados de prensa, etc.

Sin embargo, esa es la información que se encuentra en Internet que no puede ser modificada o eliminada la que continuará erosionando su seguridad. La única forma de manejar la información fuera de control es modificar su entorno a fin de que ya no sea correcta o relevante. Piense en esto como un nuevo camino para apartarse de los valores por defecto o por lo menos de los conocidos con anterioridad..

7. Investigación y monitoreo de vulnerabilidades

Los atacantes tienen acceso a la investigación de las mismas vulnerabilidades que usted. Son capaces de leer los sitios Web, foros, blogs y otros servicios de información pública sobre problemas conocidos, publicaciones y vulnerabilidades en los dispositivos y programas. Cuanto más puede descubrir el atacante acerca de los posibles puntos de ataque, lo más probable es que puede descubrir una debilidad que todavía no ha sido solventada, protegida, o incluso descubierta.

Para combatir la investigación de vulnerabilidad por parte del atacante, tiene que estar tan atento como el atacante. Es necesario buscar los problemas con el fin de protegerse de ellos con la misma intensidad con la que el atacante busca problemas para explotar. Esto significa mantenerse informado en los grupos de discusión y sitios web de todos y cada uno de los fabricantes cuyos productos utiliza la organización.

Además, es necesario visitar los sitios web de terceros para obtener más información sobre las cuestiones relacionadas a las fallas que los fabricantes no hacen públicos o que aún no tienen soluciones sencillas. Esto incluye lugares como securityfocus.com, US CERT, hackerstorm.com y hackerwatch.org.

8. Sea paciente y persistente

Atacar la red de una compañía no es una tarea que típicamente que alguien puede realizar de manera completa en un periodo corto de tiempo. Por lo general, los atacantes investigan sus objetivos durante semanas o meses antes de comenzar sus primeras interacciones lógicas contra su objetivo con herramientas de exploración, banner-grabbing y rastreo de los servicios públicos. Y aún así, sus actividades iniciales son sondeos sutiles para verificar los datos que juntaron a través de su intensiva investigación "autónoma".

Una vez que los atacantes han creado un perfil de la organización, comienzan entonces a seleccionar un punto de ataque determinado, diseñar el ataque, probar el ataque, mejorarlo, programarlo y por último, ejecutarlo.

En la mayoría de los casos, el objetivo del atacante no es golpear la red de manera que usted pueda detectar sus actividades. Contrariamente, el atacante tiene como meta acceder al sistema de manera sutil para que nadie se percate de que un acceso no autorizado está ocurriendo. Los ataques más devastadores son los que pasan desapercibidos durante largos periodos de tiempo mientras el atacante mantiene un amplio control sobre el ambiente.

Una invasión puede permanecer no detectada casi indefinidamente si es ejecutado por un hacker que es paciente y persistente. La intrusión más exitosa es

a menudo la que se realiza de a pasos pequeños uno a la vez y en períodos de tiempo significativos entre cada paso, por lo menos hasta el punto de la violación.

Una vez que el atacante ha logrado entrar, rápidamente deposita herramientas que ocultan su presencia y les brindan un mayor grado de control sobre el objetivo. Ya implantada estas herramientas, se ocultan y se activan, para que luego puedan acceder al sistema y salir de ellos cuando quieran.

Del mismo modo, la protección contra la intrusión de los atacantes también es una tarea e la que hay que tener paciencia y persistencia. Se debe ser capaz de ver, incluso, el detalle de las actividades más pequeñas de la red con procesos de auditoría estandarizados, así como un sistema automático de IDS/IPS.

Nunca permita que cualquier anomalía quede sin investigar. Se debe tener sentido común y seguir las mejores prácticas recomendadas por los profesionales de seguridad, y mantenerse actualizado sobre los parches, actualizaciones y mejoras de los sistemas. Sin embargo, hay que ser consciente que la seguridad no es un objetivo que puede obtenido en su totalidad. No existe un entorno perfectamente seguro.

Cada mecanismo de seguridad se puede ser engañado, superado, deshabilitado, eludido, explotado o inutilizado. A menudo un atacante tiene éxito porque suele ser más persistente que el profesional de seguridad que intenta proteger un entorno.

En última instancia, es una carrera de armamentos para ver quien parpadea o quién se queda atrás primero. Con suficiente tiempo, herramientas adecuadas, suficiente experiencia y habilidad, recolección de información y persistencia, un atacante puede encontrar una forma de violar cualquier sistema de seguridad.

9. Juegos de confianza

La buena noticia sobre la piratería informática de hoy es que muchos mecanismos de seguridad son muy eficaces contra la mayoría de los intentos de hacking. Firewalls, IDS, IPSes y programas antimalware han hecho de las intrusiones y del hacking una tarea difícil.

Sin embargo, la mala noticia es que muchos atacantes han ampliado sus estrategias a fin de incluir metodologías de engaño más eficaces (Ingeniería Social): los atacantes van en busca del eslabón más débil de la seguridad en cualquier organización: las personas.

Las personas han sido siempre el mayor problema de seguridad porque son el único elemento dentro del ambiente asegurado de las organizaciones que tienen la capacidad de decidir romper las reglas. Las personas pueden ser coaccionadas, engañadas, o forzadas a la violación de algún aspecto del sistema de seguridad con el fin de conceder un acceso al atacante.

El antiguo problemas de gente explotando a otras personas aprovechándose de la naturaleza humana hoy han regresado como un medio utilizado para eludir modernos esquemas y tecnologías de seguridad. La protección contra la ingeniería social es principalmente la educación. La capacitación del personal sobre lo que deben buscar y que debe informar toda anomalía o intención extraña pueden ser contramedidas eficaces.

Pero esto sólo es válido si cada persona dentro de la organización comprende que es el objetivo de la Ingeniería Social. De hecho, mientras más crea una persona que su posición en la empresa es de tan poca importancia que no sería un objetivo que valga la pena, más será en realidad el objetivo preferido del atacante.

10. Desde el interior

Con demasiada frecuencia cuando se discute sobre los atacantes, se supone que se trata de una persona desconocida del exterior. Sin embargo, varios estudios han demostrado que la mayoría de violaciones de seguridad son cometidos por los mismos empleados.

Así, una de las formas más eficaces para que un atacante viole la seguridad es a siendo un empleado. Esto se puede leer de dos maneras diferentes.

En primer lugar, el atacante puede conseguir un trabajo en la empresa objetivo y luego explotar el acceso una vez que ganó confianza dentro de la organización. En segundo lugar, un empleado existente de la organización puede convertirse en un empleado disgustado y optar por causar daños a la empresa como una forma de venganza o retribución.

En cualquiera de los casos, cuando alguna persona de la organización decide atacar la red de la empresa, muchas de las defensas de seguridad implementadas contra atacantes y accesos no autorizados a menudo son ineficaces. Por el contrario, se deben desplegar defensas internas específicas para la gestión de las amenazas internas.

Esto podría incluir el monitoreo a través de teclado, estricta configuración del principio de privilegios mínimos, prevenir que los usuarios instalen programas, no permitir el uso de dispositivos extraíbles, deshabilitar todos los puertos USB, realizar auditorías exhaustivas, implementación de IDS/IPS, filtrado y monitoreo de Internet.

Conclusión

Hay muchas maneras y caminos posibles que un atacante puede tomar para obtener acceso a un entorno aparentemente seguro. Es responsabilidad de todos y cada una de las personas que forman parte de una organización apoyar los esfuerzos de seguridad y observar los eventos anormales.

Tenemos que garantizar la máxima seguridad en los entornos tecnológicos hasta donde dan nuestras capacidades y presupuestos, mientras vigilamos cualquier inevitable intento de violación. En esta continua carrera armada, se requiere atención, es necesario ser persistente y el conocimiento es un valor incalculable.

Más información

Aprenda más sobre cómo se puede mejorar la productividad, la eficiencia y obtener una aguda ventaja competitiva.

Revise los siguientes cursos de Global Knowledge:

- Essentials of Network Security
- Certified Ethical Hacker (CEH)
- Foundstone Essentials of Hacking
- Foundstone Ultimate Hacking
- Foundstone Ultimate Hacking: Expert

Sobre el autor

James Michael Stewart ha trabajado con computadoras y tecnologías por más de 20 años. Como instructor en Global Knowledge ha transmitido sus conocimientos en los cursos de CEH y CHFI. También se ha enfocado en certificaciones de Windows 2003/XP/2003 y seguridad en el aula. Además, Michael ha escrito numerosos libros sobre seguridad, certificaciones y asuntos de administración. Es instructor en Interop y posee las siguientes certificaciones: CISSP, ISSAP, SSCP, MCT, CEI, CEH, CHFI, TICSa, CIW SA, Security+, MCSE+ Security Windows 2000, MCSA Windows Sever 2003, MCDST, MCSE NT & W2K, MCP+I, Network+ y iNet+.

Versión original del artículo en:

http://images.globalknowledge.com/wwwimages/whitepaperpdf/WP_Steward_Hackers.pdf