

Conociendo al Enemigo

EL ATACANTE INFORMÁTICO

Protocolos de Comunicación

Ambientes Operativos

DoS

Buffer Overflow

Exploits

Enumeración

CAPÍTULO 1

CONOCIENDO

Rookits

AL

ENEMIGO

Virus

Criptografía

Metodologías y Estándares



Jhon Cesar Arango Serna

www.itforensic-la.com



EL ATACANTE INFORMÁTICO

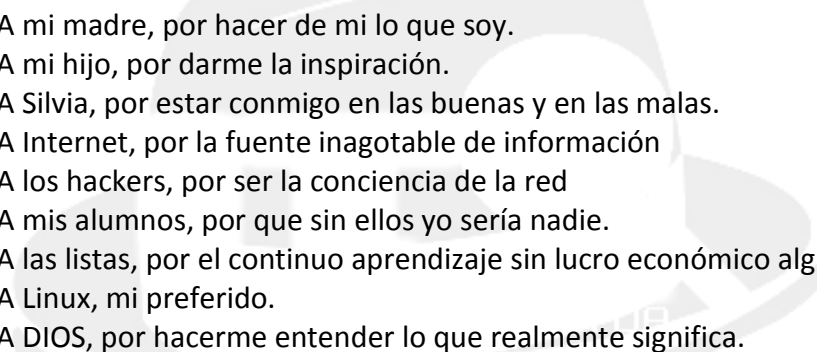
IT Forensic Ltda

<http://www.itforensic-la.com>

AUTOR: Ing Jhon Cesar Arango Serna

Enero de 2010.

AGRADECIMIENTOS



A mi madre, por hacer de mi lo que soy.
A mi hijo, por darme la inspiración.
A Silvia, por estar conmigo en las buenas y en las malas.
A Internet, por la fuente inagotable de información
A los hackers, por ser la conciencia de la red
A mis alumnos, por que sin ellos yo sería nadie.
A las listas, por el continuo aprendizaje sin lucro económico alguno.
A Linux, mi preferido.
A DIOS, por hacerme entender lo que realmente significa.

Este libro es para usted: el amigo experto, el novato o el inquieto, el profesor y el estudiante
Cualquier aporte, sugerencia, inquietud no dude en contactarme:
jca@itforensic-la.com

CAPITULO 1

INTRODUCCIÓN

“La seguridad absoluta, tendría un costo infinito.”

Anónimo.

“Son muchas las técnicas y herramientas para atacar medios tele informáticos
Sin embargo solo 2 herramientas lo protegen un ataque”

JCA

“PBSAT SJUNG BREÑM AVJEA CPÑFI BFNDJ PSETM OMBYI MPRUE QVEDF
BSPJS ARVÑA CSJAT VSAHV NANBI EDJDH ODPNF JBRNP IEDJD HOUFN
ESGEL BGEET VNATP LENÑE PFSDI EBDEU JEMQP POSRU EDSEE SFNLP
RUEÑP VETFS MBTLO HJCOD PNFJB RYTPL OTFCO ÑGIAD VANEP SETJE
NUFSI MPGRB TCOÑG IASFN EMCUE ÑEIoT IACFS SUWPL UÑUAD IBBRB
TTRJV NFBEo EÑMAV JEANP PLVJE ESFMC OÑTEJ PTENU JRAEJ OSFTI NGJNI
UBMEÑ UEMBT IMQPR TBÑTE RVECS FERFÑ EL”

J.J.B

“Los piratas ya no tienen un parche en su ojo ni un garfio en reemplazo de la mano. Tampoco existen los barcos ni los tesoros escondidos debajo del mar. Llegando al año 2010, sin importar la edad, el sexo, el credo o el color; los piratas se presentan con un cerebro desarrollado, curioso y con muy pocas armas: una simple computadora, una conexión a internet y muchas veces una línea telefónica. Hackers. Una palabra que suena en todas las personas que alguna vez se interesaron por la informática o leyeron algún diario. Proviene de "Hack", el sonido que hacían los técnicos de las empresas telefónicas al golpear los aparatos para que funcionen. Hoy es una palabra temida por empresarios, legisladores y autoridades que desean controlar a quienes se divierten descifrando claves para ingresar a lugares prohibidos y tener acceso a información indebida.”¹

¹ Fragmentos tomados del Libro Negro del Hacker

UNA CIBERSOCIEDAD A LA QUE DEBEMOS CONOCER

A raíz de la introducción de la informática en los hogares y los avances tecnológicos, a surgido toda una generación de personajes que difunden el miedo en la Red y/o cualquier sistema de computo.

Todos ellos son catalogados como "*piratas informáticos*" o "*piratas de la Red*" la nueva generación de "*rebeldes*" de la tecnología aportan, unos sabiduría y enseñanza que difunden, otros destrucción o delitos informáticos. Hay que saber bien quien es cada uno de ellos y catalogarlos según sus actos de rebeldía en la mayoría de los casos.

Hasta la fecha esta nueva Cibersociedad, ha sido dividida en una decena de grandes áreas fundamentales en las que reposan con fuerza, la filosofía de cada uno de ellos.

Todos y cada uno de los grupos aporta, en gran medida algo bueno en un mundo dominado por la tecnología, pero esto, no siempre sucede así. Algunos grupos ilícitos toman estas iniciativas como partida de sus actos rebeldes.

HACKERS

El primer eslabón de una sociedad " delictiva " según los medios de comunicación. Estos personajes son expertos en sistemas avanzados. En la actualidad se centran en los sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica para lograr comprender sistemas tan complejas como la comunicación móvil. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Les encanta entrar en computadores remotos, con el fin de decir aquello de " he estado aquí " o " fui yo " pero no modifican ni se llevan nada del computador atacado.

Un Hacker busca, primero el entendimiento del sistema tanto de Hardware como de Software y sobre todo descubrir el modo de codificación de las órdenes. En segundo lugar, busca el poder modificar esta información para usos propios y de investigación del funcionamiento total del sistema.

El perfil del Hacker no es el típico charlatán de los computadores que vive solo y para los computadores, aunque sí es cierto que pasa largas horas trabajando en el, ya que sin trabajo no hay resultados. Los conocimientos que adquiere el Hacker son difundidos por él, para que otros sepan cómo funciona realmente la tecnología.

Otros datos erróneos sobre la descripción del Hacker, es aquella que los presenta como personas desadaptadas a la sociedad, pues hoy en día la mayoría son estudiantes de informática. El Hacker puede ser adolescente o adulto, lo único que los caracteriza a todos por igual, son las ansias de conocimientos.

Los verdaderos Hackers aprenden y trabajan solos y nunca se forman a partir de las ideas de otros, aunque es cierto que las comparten, si estas son interesantes.

Este grupo es el más experto y menos ofensivo, ya que no pretenden serlo, poseen altos conocimientos de programación, lo que implica el conocimiento de la creación de Virus o Crack de un software o sistema informático.

Los buenos Hackers, no son nunca descubiertos y apenas aparecen en la prensa, a menos que sean descubiertos por una penetración en un sistema con seguridad extrema.

En otras palabras, un Hacker es una persona que tiene el conocimiento, habilidad y deseo de explorar completamente un sistema informático. El mero hecho de conseguir el acceso (adivinando la clave de acceso) no es suficiente para conseguir la denominación. Debe haber un deseo de liderar, explotar y usar el sistema después de haber accedido a él. Esta distinción parece lógica, ya que no todos los intrusos mantienen el interés una vez que han logrado acceder al sistema. En el submundo informático, las claves de acceso y las cuentas suelen intercambiarse y ponerse a disposición de la comunidad Internet. Por tanto, el hecho de conseguir el acceso puede considerarse como la parte "fácil", por lo que aquellos que utilizan y exploran los sistemas son los que tienen un mayor prestigio.

CRACKERS

Es el siguiente eslabón y por tanto el primero de una familia rebelde. Cracker es aquel experto fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas.

Un Crack es el proceso o la llave necesaria para legalizar un software sin límites de tiempo y sin pagar por ello un centavo.

Para los grandes fabricantes de sistemas y los medios de comunicación este grupo es el más peligroso de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica ahí, si no en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers.

En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet. El motivo de que estos Cracks

formen parte de la red es por ser estos difundidos de forma impune por otro grupo que será detallado más adelante.

Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware. Así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y parte de electrónica.

El Cracker diseña y fabrica programas de guerra y hardware para violar el software y las comunicaciones como el teléfono, el correo electrónico o el control de otros computadores remotos. Muchos Crackers " cuelgan " páginas Web por diversión o envían a la red su última creación de virus polimórfico.

LAMERS

Este grupo es el más numeroso que existe y son los que mayor presencia tienen en la red. Normalmente son individuos con ganas de hacer Hacking, pero que carecen de cualquier conocimiento. Habitualmente son individuos que apenas si saben lo que es un computador, pero el uso de este y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información de interés y que se puede encontrar en Internet. Normalmente la posibilidad de entrar en otro sistema remoto, le fascinan enormemente.

Es el grupo que más peligro refleja en la red ya que ponen en práctica todo el Software de Hacking que encuentran en Internet. Así es fácil ver como un Lamer prueba a diestra y siniestra un " bombardeador de correo electrónico " esto es, un programa que bombardea el correo electrónico ajeno con miles de mensajes repetidos hasta colapsar el sistema y después se ríe auto denominándose Hacker.

También emplean de forma habitual programas como los Sniffers (Programa que escucha el tráfico de una Red) para controlar la Red, interceptan las contraseñas de las cuentas del sistema y después envían varios mensajes, con dirección falsa amenazando el sistema, pero en realidad no pueden hacer nada mas que cometer el error de que poseen el control completo del disco duro, aun cuando el computador pretenda estar por fuera de una red.

Este tipo de personajes es quien emplea los Back Orifice, Netbus o virus con el fin de fastidiar y sin tener conocimientos de lo que está haciendo realmente. Son el último escalón de la nueva cibersociedad.

COPYHACKERS

Es una nueva raza solo conocida en el terreno del crackeo de Hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de telefonía celular. La principal motivación de estos nuevos personajes, es el dinero.

BUCANEROS

Son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros sólo buscan el comercio negro de los productos entregados por los Copyhackers. Los bucaneros sólo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos "Crackeados" pasan a denominarse "Piratas Informáticos " así puestas las cosas, el bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de Cracking a un nivel masivo.

PHREAKER

Este grupo es bien conocido en la Red por sus conocimientos en telefonía. Se convirtió en una actividad de uso común cuando se publicaron las aventuras de John Draper, en un artículo de la revista Esquire, en 1971. Se trata de una forma de evitar los mecanismos de facturación de las compañías telefónicas. Permite desde cualquier parte del mundo sin costo alguno. En muchos casos también evita, o al menos inhibe, la posibilidad de que se pueda trazar el camino de la llamada hasta su origen, evitando así la posibilidad de ser atrapado. Para la mayor parte de los miembros del submundo informático, esta es simplemente una herramienta para poder realizar llamadas de larga distancia sin tener que pagar enormes facturas. La cantidad de personas que se consideran Phreakers, contrariamente a lo que sucede con los Hackers, es relativamente pequeña. Pero aquellos que si se consideran Phreakers lo hacen para explorar el sistema telefónico. La mayoría de la gente, aunque usa el teléfono, sabe muy poco acerca de este grupo.

Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente.

Sin embargo es, en estos últimos tiempos, un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centrales es la parte primordial a tener en cuenta y/o emplean la informática para el procesamiento de datos.

NEWBIE

Es un novato o más particularmente es aquel que navega por Internet, tropieza con una página de Hacking y descubre que existe un área de descarga de buenos programas de Hackeo. Después se baja todo lo que puede y empieza a trabajar con los programas.

Al contrario que los Lamers, los Newbies aprenden el Hacking siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, sino que aprende.

SCRIPT KIDDIE

Denominados también “Skid kiddie”, son el último eslabón de los clanes de la red. Se trata de simples usuarios de Internet, sin conocimientos sobre Hack o Crack en su estado puro. En realidad son devotos de estos temas, pero no los comprenden. Simplemente son internautas que se limitan a recopilar información de la Red. En realidad se dedican a buscar programas de Hacking en la Red y después los ejecutan sin leer primero los archivos Readme o de ayuda de cada aplicación. Con esta acción, sueltan un virus, o fastidian ellos mismos su propio computador. Esta forma de actuar, es la de total desconocimiento del tema, lo que le lleva a probar y probar aplicaciones de Hacking. Podrían llamarse los “Pulsa botones o Clickquiadores” de la Red. Los Kiddies en realidad no son útiles en el progreso del Hacking.

METODOS Y HERRAMIENTAS DE ATAQUES

El objetivo es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática, (confidencialidad, integridad y disponibilidad de la información) de una organización o empresa y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar (y desde donde), es tan importante como saber con qué soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo.

Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

A esta altura del desarrollo de la "sociedad de la información" y de las tecnologías computacionales, los piratas informáticos ya no son novedad. Los hay prácticamente desde que surgieron las redes digitales, hace ya unos buenos años. Sin duda a medida que el acceso a las redes de comunicación electrónica se fue generalizando, también se fue multiplicando el número de quienes ingresan "ilegalmente" a ellas, con distintos fines. Los piratas de la era cibernética que se consideran como un Robin Hood moderno y reclaman un acceso libre e irrestricto a los medios de comunicación electrónicos.

Genios informáticos, sin importar la edad, se lanzan desafíos para quebrar tal o cual programa de seguridad, captar las claves de acceso a computadoras remotas y utilizar sus cuentas para viajar por el ciberespacio, ingresar a redes de datos, sistemas de reservas aéreas, bancos, o cualquier otra "cueva" más o menos peligrosa.

Como los administradores de todos los sistemas, disponen de herramientas para controlar que "todo vaya bien", si los procesos son los normales o si hay movimientos sospechosos, por ejemplo que un usuario esté recurriendo a vías de acceso para las cuales no está autorizado o que alguien intente ingresar repetidas veces con claves erróneas que esté probando. Todos los movimientos del sistema son registrados en archivos, que un buen administrador debería revisar diariamente.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas. Esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevo a la desaparición de aquellas organizaciones o empresas con altísimo grado de dependencia tecnológica (bancos, servicios automatizados, etc).

Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita conocimiento técnico básico para realizarlos. El aprendiz de intruso tiene acceso ahora a numerosos programas y scripts de numerosos "hacker" bulletin boards y web sites, donde además encuentra todas las instrucciones para ejecutar ataques con las herramientas disponibles.

Los métodos de ataque descritos a continuación están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras. Por ejemplo: después de crackear un password (contraseña), un intruso realiza un login como usuario legítimo para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente también, el atacante puede adquirir derechos a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema antes de huir.

¿QUE ES UN EXPLOIT ?

La forma más correcta de describir un Exploit, es decir que este es cualquier cosa que puede ser usada para comprometer una máquina. Una máquina comprometida puede incluir lo siguiente:

- Obtener Acceso
- Instalar una puerta trasera (Backdoor).
- Dejar la máquina fuera de línea.
- Escuchar la información que la máquina está transmitiendo.

Si deseamos una definición más formal, <http://www.dictionary.com> define un Exploit como un hueco de seguridad.

Ahora que se tiene una buena idea de lo que es un Exploit miraremos a continuación el proceso del atacante para aprovechar un Exploit sobre el sistema.

EL PROCESO DE LOS ATACANTES

Son muchos los caminos que un atacante utiliza para obtener acceso o Exploit sobre un sistema, algunos de los pasos básicos se muestran a continuación:

- Reconocimiento Pasivo.
- Reconocimiento Activo (Escaneo – Scanning).
- Explotando el Sistema (Exploiting).
 - Adquiriendo Accesos a través de:
 - Ataques al Sistema Operativo.
 - Ataques a las Aplicaciones.
 - Ataques por medio de pequeños programas (Scripts).
 - Ataques a la configuración del sistema.
 - Elevación de Privilegios.
 - Denegación de Servicios (Denial of Service).
- Subir programas.
- Descargar Datos.
- Conservar el Accesos usando:
 - Puertas Traseras (Backdoors).
 - Caballos de Troya (Trojan Horses).
- Cubriendo el Rastro.

RECONOCIMIENTO PASIVO

Para violar un sistema, un atacante debe tener cierta información de carácter general; si no, él no sabe qué atacara. Un ladrón profesional no roba casas aleatoriamente. La reunión pasiva de la información no es siempre útil por sí mismo, sino que es paso de progresión necesario, porque sabe que la información es necesaria de antemano para realizar otros pasos de progresión. En un caso, recopilaba la información para realizar una prueba de penetración autorizada para una compañía. En algunos casos, el reconocimiento pasivo puede proporcionar todo lo que un atacante necesita para acceder. Puede parecer que el reconocimiento pasivo no es tan útil, no se debe subestimar la cantidad de información que un atacante puede adquirir si se hace correctamente.

Uno de los más populares tipos de ataques pasivos es el Sniffing (Olfateando).

Esto implica el sentarse en un segmento de la red y el mirar y registrar todo el tráfico que pase por el.

Un buen ejemplo es un Sniffing Password (Olfateador de Contraseñas), es un programa que coloca el atacante en una estación de trabajo para registrar los paquetes de autenticaciones en sistemas Windows, Unix, Linux u otro. Una vez obtiene un buen numero de autenticaciones almacenadas en un archivo, el próximo

paso consiste en ejecutar sobre dicho registro un Password Cracker (decodificador de contraseñas) para obtener un archivo que contiene las contraseñas en texto plano.

Imagine ejecutar este programa entre las 7:00 Am y las 10:00 Am, cuantas contraseñas no descubriría.

Otro de los tipos de ataques pasivos es la “Information Gathering” (Recolección de Información). Un atacante recopila la información que ayudará a lanzar un ataque activo.

Por ejemplo imagine un atacante observar los casilleros de correos o escarbar en la basura dejada por una empresa, La mayor parte de las compañías utilizan en sus sobres los logos de las misma. Si el atacante observa un logo de la empresa Sun, puede darse a la idea que el objetivo utiliza un sistema operativo Solaris o por el contrario encuentra papelería con los logos de Microsoft , el atacante puede descartar automáticamente cualquier otro sistema operativo diferente a la serie Windows.

RECONOCIMIENTO ACTIVO

A este punto, un atacante tiene bastante información para intentar hacer un reconocimiento o una exploración contra un sitio. Después de que un ladrón sepa dónde se localiza una casa y si tiene una cerca, un perro, barras en los ventanas, etcétera, él puede realizar un reconocimiento activo. Esto consiste en ir hasta la casa e intentar ver a través de las puertas y ventanas.

A nivel de Hacking, el procedimiento es el mismo, El atacante prueba el sistema para encontrar información adicional. La siguiente lista son algunas de las cosas que el atacante puede descubrir:

- Computadores que son accesibles.
- Ubicación y reconocimiento de Switches (Segmentadores), Routers (Enrutadores), Firewalls (Cortafuegos) y Hubs.
- Sistemas Operativos que se corren sobre los equipos.
- Puertos que están abiertos.
- Servicios que están corriendo.
- Versiones de aplicaciones que están corriendo.

Por ejemplo, si el atacante descubre un servidor que está utilizando Windows 2003 Server Service Pack 1, El puede escanear todas las vulnerabilidades que existen para esta versión y así explotar el sistema (Exploit the System).

Otro ejemplo clásico, es el de detectar las direcciones IP de los Switches, Firewall y Routers. Después, se intenta determinar que marca y que versión de sistema

operativo tienen dichos dispositivos para luego investigar los posibles Exploit conocidos sobre dichos sistemas.

La meta de una compañía es el proteger su red y sus computadores para hacer difícil al atacante el acceso a sus recursos. Hoy en día, son muchas las empresas que tienen un mínimo de seguridad o que sencillamente no tienen absolutamente nada, por lo que el atacante usualmente obtiene fácil acceso con un bajo nivel de experiencia.

EXPLOTANDO EL SISTEMA

Mucha gente piensa que explotar el sistema es Obtener Acceso, pero actualmente se trabaja en dos áreas adicionales: La Elevación de Privilegios y la Denegación de Servicios. Los tres son útiles al atacante dependiendo del tipo de ataque que él desea lanzar.

Es importante observar que un atacante puede utilizar un sistema de una Red para atacar a otra Red. Piense en esto, sin importar si alguien está o no autorizado, puede utilizar los computadores de la Compañía A, para ingresar a los computadores de la Compañía B, cuando la Compañía B investiga, todo apunta a la Compañía A. Esto es lo que se llama el problema del Downstream Liability el cual puede tener implicaciones legales para una empresa si la persona que está a cargo de la seguridad informática no está actualizado en cuestiones de seguridad.

ADQUIRIENDO ACCESO

Esta es una de las maneras más populares de explotar un sistema. Son varias maneras que un atacante puede acceder a un sistema, pero en el nivel fundamental, él debe aprovecharse de un cierto aspecto de una entidad. Esa entidad es generalmente un sistema operativo o una aplicación; pero si estamos incluyendo vulnerabilidades físicas de la seguridad, podría ser una debilidad en la construcción del sistema como tal, esto puede proporcionar debilidades que puedan ser comprometidas. La clave es reducir al mínimo esas debilidades para proporcionar un ambiente seguro. Los siguientes son algunas maneras que un atacante puede acceder a un sistema:

- Ataques al Sistema Operativo.
- Ataques a las Aplicaciones.
- Ataques por medio de Pequeños Programas (Scripts).
- Ataques a la Configuración del Sistema.

ATAQUES AL SISTEMA OPERATIVO

Previamente se había comparado las puertas y ventanas de una casa con un sistema operativo. Las puertas y ventanas de un sistema operativo son los servicios que se están corriendo y los puertos que están abiertos. Entre mas puertos y servicios, mayores posibilidades de acceso. Basados en esto uno podría suponer que la instalación por defecto de un sistema operativo podría tener menos números servicios corriendo y puertos abiertos.

En realidad, la verdad es otra. La instalación por defecto de un sistema operativo, deja muchos servicios corriendo y puertos abiertos. La razón por la que la mayoría de los fabricantes hacen esto es simple, dinero. Quieren que un usuario de su producto; pueda instalar y configurar un sistema con la menos cantidad de esfuerzo y de apuro posible. También quiere evitar dar algún soporte telefónico al usuario lo cual incrementaría los costos sobre el fabricante. Menos llamadas, menos número del personal de soporte técnico, y más bajo sus costos. Menos llamadas, Menos es la frustración de que un usuario experimenta, así aumenta la satisfacción con el producto.

ATAQUES A LAS APLICACIONES

Los ataques del nivel de la aplicación se aprovechan de la poca seguridad que encuentra hoy a nivel lógico del software. El ciclo de desarrollo de programación para muchas aplicaciones es demasiado corto sin tener en cuenta para nada su seguridad. Un problema importante con la mayoría del software que se esté desarrollando actualmente es que los programadores y los probadores están bajo plazos muy apretados para la versión final de un producto.

Debido a esto, la prueba no es tan completa como debería ser. Además, podemos agregar a esto, convirtiendo el problema mucho mayor desde que el software que se está desarrollando se le estén agregando funciones y componentes pequeños, la probabilidad de probar cada característica todavía sería pequeño. La seguridad no debe estar en agregar o parchar componentes. Para proporcionar un alto nivel de seguridad, la aplicación tiene que ser diseñada segura desde el principio.

ATAQUES POR MEDIO DE PEQUEÑOS PROGRAMAS (Scripts)

Especialmente en las versiones de UNIX, los pequeños programas conocidos también con el nombre de “*Scripts*”, son responsables de una gran cantidad de entradas y de problemas de seguridad. Cuando el sistema operativo o las aplicaciones están instalados en su PC, los fabricantes distribuyen archivos y los Scripts simples de modo que el propietario en el sistema pueda entender mejor cómo funciona o trabaja y puede utilizar los Scripts para desarrollar nuevas aplicaciones.

Desde un punto de vista, esto es extremadamente provechoso. ¿Para que inventar la rueda si usted puede utilizar algún otro Script y estructura sobre ella?. Al programar y desarrollar código fuente uno puede crear modelos que ayudan al tiempo de desarrollo enormemente.

Una de las áreas principales donde hay muchos Scripts de muestra está en el desarrollo del Web. Las versiones anteriores del Web Server de apache y algunos Browsers del Web vinieron con varias escrituras y la mayoría de ellas tenían vulnerabilidades.

También, se encuentran muchas muchos Scripts a través de Internet que permiten aun teniendo un conocimiento mínimo de programación, desarrollar aplicaciones en un período de tiempo relativamente corto. En estos casos, las aplicaciones trabajan, pero qué se esconde detrás de la aplicación?. Hay generalmente en muchas aplicaciones código muy extraño que lo único que hacen es crear una puerta trasera para los atacantes. Los ASP (Active Server Pages) son un ejemplo perfecto.

ATAQUES A LA CONFIGURACION DEL SISTEMA.

Son varios los casos, en que un sistema tiene muchos problemas de seguridad porque no fueron configurados correctamente. Son muchos los administradores que instalan un sistema con las opciones por defecto o por otra parte al tratar de instalar un nuevo programa modifica una serie de opciones hasta que logra que un producto trabaje. El problema con esto es que él nunca deshace lo que hizo o limpia el trabajo extraño realizado. Esta es una de las mayores razones del por qué cierto sistema son quebrantados y otros no.

Para maximizar la configuración correcta de una máquina, quite cualquier servicio innecesario o software. De esta manera, solo dejara en su sistema los componentes únicos y necesarios para su funcionamiento.

Son varios los ejemplos que se pueden extraer de este tema, uno de ellos es el no colocarle contraseña al setup de la maquina, existen muchos programas bajados de Internet que pueden generar un Diskette o Cd de arranque que permite descifrar las contraseñas de cualquier Sistema Windows o cualquier otro. El atacante solo debe apagar la maquina bruscamente y modificar la configuración del sistema (Setup) para que este arranque por la unidad deseada y así conocer las contraseñas del sistema. Otro ejemplo clásico es cuando se desea instalar un Servidor de Internet bajo Linux, sin importar la distribución son muchos los administradores inexpertos que instalan el Linux con las opciones que vienen por defecto, esto deja un gran número de puertos y servicios abiertos y disponibles para el atacante.

La configuración del sistema es una área que usted puede controlar puesto que usted es el que está configurando el sistema. Por lo tanto, cerciorase de sacar el tiempo necesario para planificar la instalación de un sistema. Recuerde, que si usted piensa que no tiene el tiempo suficiente para hacerlo la primera vez, un atacante aprovechara esta circunstancia y no habrá una segunda vez.

ELEVACION DE PRIVILEGIOS.

La última meta de un atacante es tener el “root” o el acceso del administrador en un sistema. En algunos casos, un atacante puede adquirir directamente el acceso de los servidores. En otros casos, un atacante tiene que tener un acceso con una cantidad mínima de privilegios y después elevarlos para tener acceso completo. Por ejemplo, un atacante pudo adquirir el acceso de un usuario normal y después utilizar este acceso para obtener información adicional. Después de que se haya obtenido la información adicional, el atacante utiliza este conocimiento para aumentar los privilegios al acceso como root o como el administrador. Este tipo de ataque, donde un atacante tiene indirectamente el acceso del root o del administrador a través de varios niveles del acceso, se llama elevación de privilegios.

DENEGACION DE SERVICIOS (DENIAL OF SERVICE)

Los dos tipos principales de ataques activos son Denegación del Servicio y Ruptura Interna.

Los ataques de denegación de servicios producen en un sistema el rechazo al acceso legítimo a un recurso. Estos pueden extenderse a bloquear usuarios que

ingresan a través de Web Site para impedir su ingreso a la red. Por ejemplo, si usted se comunica remotamente para ingresar a su compañía y trabajar día a día, un atacante puede realizar un ataque sobre el servidor con el fin de suspender el servicio de autenticación de usuarios, este tipo de ataque evita que usted realice el trabajo normalmente debido a que no podrá ingresar al sistema.

Desafortunadamente, estos ataques son bastante fáciles de realizarse en Internet porque no requieren ningún acceso anterior. Si usted está conectado con Internet, usted es vulnerable a un ataque de Denegación de Servicio. También, las herramientas que realizan estos tipos de ataques son fácilmente disponibles y fáciles de ejecutarse.

SUBIR PROGRAMAS.

Después de que un atacante haya accedido a un sistema, él realiza generalmente un cierto conjunto de acciones sobre el servidor. Son pocos los casos donde un atacante accede apenas por el motivo de acceder. Lo más común son las cargas o descargas de archivos o programas del sistema. Por qué un atacante perdería horas en acceder a un sistema si el no espera nada de él? Si un atacante está indagando para robar la información, después de que se tenga el acceso, la meta es descargar la información lo más secretamente posible y luego salir del sistema.

En la mayoría de los casos, el atacante cargará algunos programas al sistema. Estos programas se pueden utilizar para aumentar el privilegio sobre el acceso y así comprometer el sistema sobre el cual accede y convertirlo en una plataforma de trabajo.

¿Por qué un atacante va a utilizar su propia máquina para atacar a otra compañía, cuando él puede utilizar alguna otra máquina más rápida, haciendo más duro de rastrear el ataque?.

Para alterar o para adquirir información, un atacante debe quebrantar con éxito un sitio y recibir la información necesaria. Internet, sin embargo, agrega una nueva dimensión a esto. Como discutimos, en algunos casos, la razón única para quebrantar un sitio es la de utilizarlo de plataforma para realizar otros ataques. Algunas de las herramientas que son utilizadas por los atacantes requieren potencia de proceso significativo y una conexión con buen ancho de banda en Internet. Qué mejor manera de adquirir estos recursos que romper un sitio grande. Una ventaja agregada para el atacante es que es mucho más duro rastrear el ataque. Si un atacante está lanzando un ataque de la compañía A y él cubre su rastro y se viola la seguridad de la compañía B, la compañía B puede considerar solamente que la compañía A lo atacó.

DESCARGAR DATOS

Con algunos ataques, como espionaje corporativo, un atacante solo le interesa la información. Esta información puede ser datos de investigación y desarrollo de un nuevo producto, una lista de direcciones de clientes, o el futuro de una compañía. En todos estos casos, el atacante desea el acceso ilegal al sitio para luego hacer una transferencia de los datos a otra localización. Después que los datos sean descargados, el atacante puede realizar cualquier análisis sobre la información adquirida.

Es clave recordar con este tipo de ataque, es que si usted no detecta el atacante cuando él está descargando los datos, usted no tiene ninguna oportunidad de parar el ataque. Una vez se hayan descargado los datos, el resto del ataque se hace fuera de línea o conexión.

CONSERVANDO EL ACCESO

Después de que un intruso ingresa al sistema, el puede colocar una puerta trasera (Backdoor) para acceder fácilmente en el momento que desee. Si al atacante le cuesta mucho trabajo conseguir el acceso al sistema, por qué realizar nuevamente este trabajo para ingresar la próxima vez que se necesite? En la mayoría de los casos, un atacante ha tenido el acceso equivalente al “root” o administrador del sistema por lo que el puede hacer lo que desee con el, así que porqué no poner una puerta trasera? Pues se ha discutido, que la razón para mantener el acceso es utilizar esos computadores como plataforma para lanzar ataques contra otras compañías.

Una puerta trasera o Backdoor puede ser tan simple como agregar una nueva cuenta de usuario al sistema. Esto es sencillo, pero si la compañía verifica sus cuentas activas, tiene una alta probabilidad de detectarla. Sin embargo, si es un sistema con millares de cuentas, las probabilidades son tan pocas que nadie lo notaría.

Son muchas las empresas que tienen cuentas usuarios activas, pero son pocas la que eliminan las cuentas del personal que ya no laboran con la compañía. En este caso los atacantes se aprovechan de dichas cuentas utilizándolas como puertas traseras. Es preocupante saber que la mayoría de las compañías no hacen un seguimiento sobre las personas que tienen acceso a sus sistemas. Si los atacantes acceden y descubren cuentas que no son utilizadas pueden garantizar acceso durante mucho tiempo.

Un tipo más sofisticado de puerta trasera es el sobrescribir un archivo del sistema con una versión que tenga una característica oculta. Por ejemplo, un atacante puede sobrescribir al demonio de la conexión que procesa peticiones cuando la gente entra al sistema. Para la mayoría de los usuarios, trabaja correctamente, pero si usted proporciona cierta identificación de usuario, le permitirá automáticamente trabajar en el sistema con los privilegios del administrador. Estos programas

modificados que están instalados son conocidos normalmente como Caballos de Trola, porque tienen una característica oculta.

Un Caballo de Trola es un programa que tiene una característica abierta y secreta. Un ejemplo es cuando un usuario recibe un email que tenga supuestamente la foto suya o la foto de una modelo famosa desnuda en formato comprimido. Cuando él da doble clic sobre el archivo, abre un archivo que contiene unas imágenes. El usuario piensa que esto es divertido y se lo envía a todos sus amigos. Lo que la víctima no sabe es que dicho archivo también ejecuta un programa que agregue una cuenta al sistema de modo que un atacante pueda entrar en cualquier momento o que por el contrario se propaga a través de los contactos que posea el usuario.

Otra manera que tiene un atacante para crear una puerta trasera es instalar un programa servidor sobre cualquier maquina de un usuario. Si los atacantes se conectan con dicho programa, podrán tener acceso completo al sistema o aún a la red.

Es importante precisar que existen algunos casos donde un atacante no desea conservar el acceso para el uso posterior. La mayoría de estos casos implican una cierta forma de espionaje corporativo, donde un atacante accede para adquirir cierta información. En la mayoría de los casos del espionaje corporativo, un atacante sabe lo que desea y cuando lo consigue.

La meta principal de conservar el acceso es mantener dicho acceso pero cubrir sus huellas de modo que siga siendo desapercibido

CUBRIENDO EL RASTRO

Después de que un atacante compromete la seguridad de una máquina y crea una puerta trasera, lo siguiente es cerciorarse de no ser descubierto. Por tanto el atacante debe cubrir sus huellas.

La más sencillo es limpiar los registros del sistema que se generan diariamente, estos archivos contienen un expediente que indican que personas ingresaron al sistema y cuando, así que si cualquier persona que visualice el contenido de los logs puede detectar fácilmente que persona no autorizada ingreso al sistema y determinar también el trabajo realizado sobre la maquina. Desde el punto de vista de un atacante, los logs del sistema son una mala cosa. Así que el cubre sus huellas, lo primero que hace es descubrir donde se encuentran los logs del sistema y luego limpia dentro de los archivos los registros que se relacionan con su ataque.

¿ Por qué un atacante no borra todo el contenido de los logs del sistema para asegurarse que no existirá ningún registro que lo comprometa? Hay dos desventajas importantes para realizar esta acción. Primero, los archivos de logs del sistema

vacíos levanta la sospecha inmediata de que algo es incorrecto. En segundo lugar, cuando un sistema operativo está bien instalado y administrado puede lanzar una advertencia al administrador de que uno o varios archivos logs del sistema fueron modificados en su tamaño o indicar que el archivo se borro. Una buena administración del sistema recomienda almacenar los logs del sistema en una maquina alterna o enviarlos directamente a un medio de impresión. De esta manera, las oportunidades de que alguien busque los logs del sistema y los limpie se reducen al mínimo.

Otra técnica común del atacante es suspender el registro sobre los logs del sistema tan pronto como el acceda al sistema. De esta manera, nadie sabrá lo que él ha hecho. Esto requiere maestría adicional, pero, es extremadamente eficaz. Cabe recordar, que si el registro se hace correctamente, incluso si un atacante suspende el registro sobre los logs del sistema, el sistema todavía registra el hecho de que el atacante ingreso al sistema, donde entró y otra información útil.

Si un atacante modifica o sobrescribe los archivos del sistema, su labor es cerciorarse de que los archivos modificados no levantan sospecha. La mayoría de los archivos tienen fechas de cuando fueron modificados por última vez y el tamaño del mismo. Existen programas que por medio de una bandera, detectan el cambio anormal sobre los archivos. Para omitir esto, un atacante puede entrar y engañar el sistema. Aunque se hayan modificado los archivos del sistema, el puede entrar y fijar nuevamente sus configuraciones anteriores lo hace mucho más duro de detectar.

Se recomienda que si usted va a ejecutar un programa para cerciorarse de que los archivos del sistema no fueron modificados, utilice un programa que calcule sumas de comprobación. Una suma de comprobación es un cálculo realizado en el archivo, y dos sumas de comprobación pueden solamente ser iguales si los archivos son idénticos. Esto significa que incluso si un atacante entra e intenta cubrir su rastro, la suma de comprobación debe ser diferente.

LOS TIPOS DE ATAQUES

Ahora démonos una idea de los tipos de ataques que están ocurriendo sobre Internet. Estos se clasifican a continuación:

- Ataques Activos
 - Denegación del Servicio
 - Quebrantar un Sitio
 - Obtener Información
 - Uso de los Recursos
 - Engaño
- Ataques Pasivos
 - Sniffing (Olfateo)
 - Contraseñas (Passwords)
 - Tráfico de la Red
 - Información de Interés
 - Obtener Información

Los Ataques Activos implican una acción deliberada de parte del atacante para acceder a la información. Un ejemplo es hacer Telnet sobre el puerto 25 para conocer la información sobre el servidor de correo que la empresa está manejando. El atacante está haciendo activamente algo contra un sitio para conseguir un acceso lo que significa que el esta también utilizando una conexión de red. Debido a esto, estos ataques son fáciles de detectar, si usted los busca adecuadamente. Sin embargo, por lo regular los ataques activos pasan desapercibidos porque las compañías no saben que es lo que están buscando y además al observar los registros del sistema no saben si la información es correcta o no. Muchas empresas centran sus esfuerzos en determinada área; desafortunadamente, es el área incorrecta o solamente una de muchas áreas que deben ser vigiladas.

Los Ataques Pasivos, por otra parte, se centran en la recopilación de información. Esto no quiere decir que los Ataques Activos no pueden recopilar información o que los Ataques Pasivos no se pueden utilizar para ganar un acceso, en la mayoría de los casos, los dos tipos de ataques se utilizan conjuntamente para comprometer un sistema. Desafortunadamente, los ataques pasivos implican una actividad que los hace más difíciles de descubrir.

CATEGORIA DE LOS EXPLOIT

Existen diversas categorías de exploit que un atacante puede utilizar para atacar una máquina, es imprescindible recordar que un atacante utiliza diversos tipos de ataque y buscara siempre la manera más fácil para comprometer a una maquina o a la red.

En algunos casos, El atacante puede acertar con solo lanzar el primer ataque. En otros casos, el atacante lanza diversos tipos de ataques hasta encontrar uno que sea exitoso. Como hemos indicado, hay varias categorías de Exploits siendo las más populares:

- Sobre Internet
- Sobre la LAN
- Localmente
- Fuera de Línea
- Hurto
- Engaño

La mayor parte del tiempo, un atacante utiliza varias de estas categorías para lanzar un ataque acertado.

SOBRE INTERNET

Este tipo de ataque es el más popular debido a que son muchas las noticias de los Hackers que irrumpieron en este medio. La mayoría de ellos adolescentes que trabajan a lo oscuro a las 2:00 Am, Sistemas comprometidos a través de una conexión telefónica.

La razón que tiene la gente para pensar que Internet es el medio principal para atacar una maquina son: Primero, Internet es tecnología de punta y Segundo, es la manera ideal para comprometer una máquina porque la mayoría de las compañías tienen conectividad con Internet. Hoy en día con toda seguridad cualquier empresa importante está conectada a Internet, lo que proporciona un método fácil para comprometer su seguridad.

Hay que tener en cuenta que aunque la mayoría de las compañías no están trabajando las 24 horas, sus conexiones de Internet y las máquinas están por encima de este horario. Esto proporciona un mecanismo fácil para los atacantes irrumpir en los sistemas mientras que los empleados están descansando o almorzando.

Los ataques Sobre Internet implican el comprometer una máquina usando el Internet como herramienta en un computador remoto. Los ataques más comunes sobre Internet son:

- Ataques Coordinados
- Secuestro de Sesión
- Spoofing
- Relaying (Re transmisión)
- Caballos de Troya o Virus

ATAQUES COORDINADOS

Puesto que Internet permite conectividad mundial, hace muy fácil para la gente de todo el mundo colaborar o participar en un ataque. Si usted puede conectarse con Internet, que virtualmente cualquier persona en el mundo puede hacer, usted puede comunicarse y trabajar con alguien como si él estuviera en la puerta siguiente o aún en el mismo cuarto.

Para que algunos ataques sean acertados, los hackers tienen que coordinar con otros usuarios y máquinas en una red. Ahora, no es el atacante contra la máquina víctima, si no el atacante y sus 50 amigos y a su vez estos amigos pueden agregar otros 50 si no tienen éxito. Recuerde que el atacante tiene a su disposición herramientas y atacantes en el mundo entero. Se debe tener en cuenta que encontrar a algunos cientos de atacantes que tenga computador no es una tarea dura.

Como si fuera poco, hemos utilizado el termino Amigos, pero no tienen que ser realmente amigos, porque en este tipo de ataque no se necesita saber en realidad quien está ayudando.

SECUESTRO DE SESION

En algunos casos, es más fácil realizar un ataque como un usuario legitimo, que buscar la manera de romper el sistema. Esta técnica básica se llama secuestro de sesión y funciona encontrando una sesión establecida y después asumiendo el control de dicha sesión. Una vez que entre un usuario, el atacante puede asumir el control de la sesión y permanecer conectado por varias horas sin contar que también puede colocar puertas traseras para el próximo ingreso.

Este método puede parecer fácil pero en realidad es muy complicado por varias razones. Una de las razones principales es que el atacante está asumiendo el control una sesión existente que debe personificar al usuario legítimo. Esto significa conseguir todo el tráfico que se encamina a su dirección IP para ser enrutado hacia el sistema de los delincuentes.

SPOOFING

Spoofing es un término que describe el acto de personificar o de asumir una identidad que no sea la propia. En el caso de los ataques de Internet, esta identidad puede ser una dirección de Correo Electrónico, una identificación de usuario, Dirección IP, etcétera.

Esto llega a ser importante cuando un atacante está atacando perfiles de confianza. En muchos sistemas, especialmente NT/UNIX, trabajan con perfiles de confianza. La lógica es que si una compañía tiene diez Servidores, es ineficaz que un usuario tenga que abrir una sesión en cada servidor con diversas contraseñas para realizar su trabajo. Una manera mejor sería tener la conexión individual a un servidor y hacer que los otros confíen en esta conexión. Con este método una máquina autentica a un usuario, las otras que poseen los perfiles de confianza confiarán automáticamente en ese usuario sin tener que re-autenticarlo. Desde el punto de vista funcional, esto ahorra mucho tiempo. Desde el punto de vista de seguridad, si no se configura correctamente, puede ser una pesadilla. El Spoofing se puede considerar más como un ataque pasivo que el secuestro de sesión. Con la sesión secuestrada, un atacante asume el control sobre una sesión existente y personifica activamente al usuario una vez el está por fuera de línea. Con Spoofing, un atacante se aprovecha de un lazo de confianza entre la gente y/o las máquinas y las engaña para que confíen en el.

RELAYING

En la mayoría de los casos, cuando un atacante irrumpe en una red o una máquina y lo utiliza de plataforma para lanzar varios ataques como “email spoofing”, no quisieran que el ataque fuera rastreado lo que crea un dilema interesante, puesto que el atacante realiza el ataque usando su computador y debe evitar que cualquier persona sepa que era el.

Hay varias maneras de hacer esto, pero la más popular es la Retransmisión (Relaying). La retransmisión es donde un atacante retransmite su tráfico a través de terceros, lo que hace parecer que los ataques provienen de un tercero. Esto crea un problema interesante para la víctima. Cómo debe proceder una empresa si nunca pueden identificar quien es el atacante verdadero? Ahora estamos comenzando a ver porqué el problema es tan grande y porqué los atacantes utilizan estas técnicas para ocultar su presencia.

Un tipo popular de retransmisión es la retransmisión del email. Esto implica estar conectando con otro individuo en su sistema email y usar su computador para enviar el email a otra persona o sistema.

CABALLOS DE TROYA O VIRUS

Los caballos de Troya pueden causar mucho daño debido a la filosofía que manejan: tienen una función abierta y secreta. La función abierta puede ser cualquier cosa que la víctima encontraría interesante. Un ejemplo perfecto es cuando se envía un correo con imágenes animadas que bailan. Los usuarios no pueden oponerse al impulso de abrir estas animaciones en sus propias máquinas y como si fuera poco si les divierte lo más seguro es que reenvían estos correos a sus amigos. Esto se convierte en un problema cuando traemos la función secreta. Se lanza la función secreta cuando se está ejecutando la función abierta, la mayoría de los usuarios no saben que está sucediendo internamente en su máquina. Piensan que están ejecutando un archivo entretenido, y en realidad están infectando su máquina y a las máquinas de sus amigos. Un uso común de los caballos de Troya es instalar Puertas Traseras de modo que un atacante puede conseguir fácilmente acceso en el sistema de la víctima.

Si usted tiene un computador o ha trabajado en la industria de los computadores, sabe bien que los virus no requieren de presentación. Los virus informáticos son como virus humanos, la meta es infectar tantos computadores como sea posible. Una vez que un computador se convierte en un portador puede infectar otras máquinas. El impacto de los virus puede extenderse de una simple molestia a la pérdida total de la información. Los Virus más populares son los que se transmiten a través del correo electrónico. Estos virus se introducen dentro de una conexión que se envía con un email. Cuando el usuario abre el correo, el Virus se ejecuta.

SOBRE LA LAN

Ahora demos un vistazo sobre los ataques que ocurren sobre una Red de Área Local (LAN), que son usualmente más perjudiciales debido a que la mayoría de las compañías no se preocupan por ello debido a que confían en que los accesos de sus sistemas son realizados por personal de confianza de la compañía (Empleados). Esto es peligroso por dos razones. Primero, una gran cantidad de ataques provienen del personal de confianza. En segundo lugar, los atacantes pueden acceder a la LAN por medio de una cuenta de un usuario legítimo y tener el acceso completo que un empleado normal tendría.

Los siguientes son algunos de los tipos más populares de ataques que ocurran sobre la LAN:

- Sniffing sobre el Tráfico.
- Broadcasts.
- Acceso a los Archivos.
- Control Remoto.
- Secuestro de Aplicaciones.
- Ataques a las redes inalámbricas.

SNIFFING SOBRE EL TRAFICO (Olfateando el trafico)

El Sniffing sobre el tráfico es un ataque pasivo que implica el observar todo el tráfico que ocurre en una red. Puesto que es un ataque pasivo, algunas personas lo pasan por alto debido a que este tipo de ataque no causa ningún daño a su red. Esta declaración no es del todo cierta. Sí los atacantes efectivamente no pueden causar ningún daño sobre la red, si pueden encontrar la información necesaria que haría mucho más fácil acceder en una fecha futura y causar el daño deseado. También, de un punto de vista corporativo del espionaje, alguien puede acceder a los archivos extremadamente importantes.

Una empresa normalmente utiliza dentro de su red corporativa Concentradores (Hubs) o Segmentadores (Swiches) para interconectar sus máquinas.

Un concentrador es una vieja tecnología y su trabajo radica en recibir un paquete del remitente y enviarlo a todas las máquinas conectados a el. El receptor recibirá el paquete y lo procesará, pero todas las otras máquinas en la red también la reciben. Normalmente, una máquina examina el paquete si determina que no es para el, lo descarta, pero debido a que cada máquina recibe el paquete se abusa del trafico de la red.

Un Switch determina qué máquinas están conectadas a cada uno de sus puertos y envían los paquetes únicamente al receptor. Esto es excelente no solo desde el punto de vista de la seguridad, sino también desde el punto de vista de ancho de banda, desde el punto de vista de seguridad es bueno, debido a que si una maquina esta capturando el trafico de la red solo vera los paquetes que se envían desde esa máquina o destinados para esa máquina.

Una manera posible de utilizar un Sniffer es ocultarlo en un programa de caballo de Troya. El usuario abriría este programa como por ejemplo un juego e instalar un sniffer en su ordenador, que enviaría todo el tráfico al atacante.

Cuando se hacen auditorias de seguridad, una de las cosas que hace es instalar un Sniffer para observar el impacto que tuvo en atacante dentro de la

empresa. Se sorprendería de las cosas que se pueden descubrir, como identificaciones de usuarios, contraseñas, archivos importantes, Etc.

Es importante precisar que incluso la utilización de los Swiches no garantiza que alguien pueda estar observando el tráfico de su red. Esto es más difícil porque requiere el acceso físico a los equipos de comunicación. La mayoría de los Swiches poseen un puerto que permiten conectar una consola y ver todo el tráfico que pasa por ellos (otra razón de la seguridad física).

Muchos dispositivos de comunicación permiten asignar una dirección IP, es importante saber que los dispositivos de comunicación como los switches vienen por defecto con contraseñas asignadas, las cuales se conocen por medio de Internet, por tanto asegúrese de cambiar dichas contraseñas.

Existen programas que permiten ubicar los equipos de comunicación de una compañía, así que un atacante puede perfectamente lanzar ataques sobre un switch que tenga un dirección lógica asignada.

Para que una tarjeta de la red (Nic) reciba todo el tráfico tiene que ser Switchhead de un modo diferente, de lo contrario se eliminaran los paquetes no destinados para la máquina. El modo promiscuo es el modo que permitirá que la tarjeta de red reciba todos los paquetes que se están enviando por el segmento de la red. Para cambiar a este modo, usted debe instalar un programa piloto para la tarjeta de la red. En Windows se hace a través del icono de red, que está situado en el panel de control.

Anti-Sniffer

Una de las preguntas que la mayoría de la gente hace es " cómo puedo decir si una máquina está en modo promiscuo? " Bien, si usted tiene acceso físico a la máquina usted podría mirar las configuraciones para la tarjeta de la red, pero sino, usted puede tener un programa como el AntiSniff de <http://www.10phtcrack.com/> que se ejecuta para determinar si una o un grupo de máquinas tienen su tarjeta de red en modo promiscuo. Según el website, " AntiSniff realiza 3 clases de pruebas: pruebas específicas del sistema operativo, pruebas del DNS, y pruebas del tiempo de espera de la red. "

Como este existen muchos programas, pero es importante dejar claridad que no es 100 por ciento exacto. De acuerdo con la información recolectada, hace una conjetura sobre los equipos encendidos si la tarjeta de interfaz de la red está observando tráfico, una máquina podría estar en modo promiscuo y no ser detectada.

BROADCASTS (Difusiones)

Todas las máquinas que están conectadas con el mismo segmento de la red (Lan) deben tener la misma identificación lógica de red. Es así como el TCP/IP trabaja. Cada dirección IP que se asigna a una máquina tiene una porción de red y una porción hosts. La porción red debe ser igual para las máquinas en la misma red y la porción del hosts debe ser única para cada máquina de la red.

Por ejemplo, si la dirección IP de una máquina es 25.10.5.50 y la máscara es 255.255.0.0., entonces el número 25.10 corresponde a la identificación de la red y el 5.50 es la identificación única de la máquina. Por lo tanto, cualquier otra máquina en este segmento de red debe comenzar con 25.10. Esto es similar a la dirección de una casa, note usted que en la calle donde vive todos tienen la misma dirección lo único que varía es el número de la casa.

Normalmente, los paquetes se envían a una sola dirección, pero hay ocasiones en que se desea enviar los paquetes a todas las direcciones en un segmento de la red. Una forma para hacer esto es enviar el paquete tantas veces como máquinas exista en el segmento. A excepción de segmentos muy pequeños, esto no es práctico. Para superar esto, hay una característica del TCP/IP llamado la dirección de Broadcast (Dirección de difusión), que enviará un paquete a cada máquina en el segmento de la red. La forma de fijar la dirección de broadcast es sencilla. Cada octeto en una dirección IP contiene 8 dígitos binarios, en el ejemplo anterior si convirtiéramos la porción del hosts todo en unos (1) conseguiríamos lo siguiente en binario: 11111111.11111111 que al pasarlo a decimal darían 255.255. Si combináramos esto con la porción de la red conseguiríamos 25.10.255.255, que representa la dirección de Broadcast para ese segmento de la red. Si un paquete se envía a esta dirección va a cada máquina que posea la misma dirección de red en ese segmento. Si hay solamente 10 máquinas, no es probablemente un gran reparto, pero si hay 60.000 máquinas? Eso podría generar mucho tráfico y causar problemas numerosos.

Este es realmente un tipo común de ataque donde un atacante envía un solo paquete a una dirección de broadcast con la meta de generar tanto tráfico que puede causar la negación de un servicio. Si la filtración apropiada no se aplica en el cortafuego (firewall) o Enrutadores, este ataque se podría realizar también vía Internet, pero esto se realiza sobre todo en un LAN.

ACCESO A LOS ARCHIVOS

En la mayoría de las compañías, las contraseñas son las primeras y solamente la línea de defensa contra un ataque. Sin embargo, la mayoría de las compañías no controlan adecuadamente sus accesos que limiten “quien puede tener acceso a que”, si accede un atacante (que lo hace generalmente con el login y

password de un usuario) el puede tener acceso a todos los archivos de la red.

Una de las cosas comunes que se escucha en la calle es “no tenemos archivos importantes y no sabemos si cualquier persona acceda a nuestro equipo”, otro posible comentario seria: “Yo solo trabajo desde mi casa y allí no tengo red”, ustedes se aterrarían de la forma simple de acceder maquinas remotas conectadas a Internet con solo escanear el puerto 139 y como si fuera poco la facilidad en las contraseñas que utiliza la gente hace más fácil el trabajo

En fin sin importar el método, ya sea con login y password o mediante recurso compartido un atacante puede observar la información importante de una persona o una empresa y utilizar esta información para el beneficio propio.

CONTROL REMOTO.

Para acceder a un sistema hay básicamente dos opciones: Puedo tener el acceso físico a la máquina, o puedo controlarla remotamente por medio de una red.

Controlar una máquina remotamente implica poder utilizar una máquina desde otra máquina por medio de la una red como si usted estuviera sentado en la máquina. Más adelante en este libro, cuando hablamos detalladamente sobre las puertas trasera y caballos de troya, usted verá ejemplos de los programas que permitirán que usted haga esto.

Un ejemplo conocido es el actual LogMein o Vnc Viewer, que una vez que esté instalado en una máquina le dejará tener acceso completo a la misma.

Si la filtración apropiada en un servidor o cortafuegos no se realiza adecuadamente se puede controlar remotamente una máquina a través de Internet, este es el caso de muchas compañías.

SECUESTRO DE APLICACIONES.

El secuestro de aplicación es similar al concepto de secuestro de sesión, que implica asumir el control de una aplicación y tener el acceso no autorizado. En muchos casos, si usted puede acceder a una aplicación, usted puede tener acceso a todos los datos creados por esa aplicación. En los casos de los procesadores de textos u hojas electrónicas puede ser que no sea de gran importancia, pero piense en aplicaciones corporativas más grandes como la facturación, cartera o nomina. Si un atacante puede acceder a un sistema de facturación, pueden adquirir muchos de información importante de la compañía.

Esta es un área en que muchas compañías fallan. Se preocupan por colocar un Cortafuegos conociendo sus amenazas en la red, pero no le prestan mucha atención a sus aplicaciones. Especialmente desde un punto de vista de la oficina corporativa o de negocio, las aplicaciones proporcionan un camino a la información más sensible de la empresa. Si usted no protege y no asegura correctamente estas aplicaciones, todos los cortafuegos del mundo no le ayudarán.

ATAQUES A LAS REDES INALAMBRICAS.

Técnica actualmente muy utilizada y consiste en obtener una conexión inalámbrica no autorizada para utilizar el ancho de banda de la organización para acceder a Internet, provocando una disminución del rendimiento en la red para sus usuarios legítimos.

Una vez se cuenta con una conexión a la red inalámbrica, podría ser utilizado por un atacante para llevar a cabo actividades delictivas en Internet (actividades que se estarían originando desde la propia red de la organización, por lo que ésta podría ser responsable de los daños y perjuicios ocasionados a terceros): atacar otras redes, distribuir contenido censurado, descarga de archivos protegidos por derechos de autor (como la música o las películas), robo de números de tarjetas de crédito, fraudes y amenazas contra otros usuarios.

En términos de ataques a la red corporativa se puede analizar el tráfico y sustraer información confidencial.- Para llevar a cabo este tipo de ataques, los intrusos puede utilizar programas especializados de "sniffers" para redes inalámbricas, programas especialmente diseñados para interceptar el tráfico transmitido vía radio en este tipo de redes. Entre los más conocidos se puede citar: NetStumbler, AiroPeek, Wireshark, Kismet, Ettercap y Dstumbler.

LOCALMENTE

Si un atacante puede tener el acceso local a un computador, servidor o a un componente de la red, puede causar la mayor parte de daño. Dependiendo del tamaño del componente, un tipo de daño que un atacante puede causar es hurto del equipo (Por ejemplo un computador portátil). En esta sección, nos centraremos en los ataques que requieren acceso local al computador sin hurtar el mismo. Los siguientes son los tipos de ataques locales:

- Observación detrás de Hombros.
- Terminales Abiertas
- Contraseñas Escritas
- Maquinas Desconectadas
- Conexión Local

OBSERVACION DETRAS DE HOMBROS

La observación detrás de hombros es probablemente uno de los tipos de ataques más básicos, extremadamente eficaz si usted tiene acceso físico a un recurso o a una persona con el acceso. Consiste en mirar detrás del hombro de una persona cuando él está digitando su contraseña, con el fin de conseguir su acceso. Si usted hace obvio que usted está mirando a alguien, seguramente esta persona no trabajará, pero si usted disimula observando al rededor tendrá más oportunidades de recolectar alguien que digite una contraseña.

Una de las tareas realizadas durante una auditoria de seguridad informática en una empresa es ver cómo es vulnerable la misma con la observación detrás de hombros. Para hacer esto usted tiene que generalmente observar cómo está comprometida la seguridad física, que es una tarea relativamente simple en la mayoría de las empresas.

Tenga en cuenta que aquí asumimos una posición de que nuestro enemigo es externo, pero muchas veces los enemigos son nuestros propios compañeros de trabajo y/o amigos.

Un ejemplo simple es intentar acceder entre las 8:00 AM y 9:00 AM, cuando los empleados de una empresa están entrando a trabajar. Si usted realiza esto en un día lluvioso, usted puede perfectamente utilizar una capa y un fólter o agenda para pasar desapercibido, usted puede rastrear fácilmente a alguien que este ingresando una contraseña con una probabilidad de 9/10. Además, la mayoría de las compañías tienen empleados que fuman y/o toman refrigerio en la mayoría de los casos, esas personas lo hacen en los pasillos, cafeterías o en las zonas verdes de la compañía, lo cual puede aprovechar un atacante para acceder fácilmente a los cubículos de trabajo.

Ahora que ya está dentro del edificio, simplemente observa a las personas que están digitando contraseñas. Esto es muy simple ya que existen personas que

utilizan su propio nombre como contraseña, existen otras que dejan que el computador les recuerde la contraseña y otros que su vocalizan su contraseña mientras la digitan, si usted es un buen lector de labios puede deducir lo que dice.

TERMINALES ABIERTAS

La mayoría de la gente entra a trabajar en la mañana y sale al finalizar el día. Desafortunadamente, cada persona no permanece todo el tiempo en su escritorio. Van a reuniones, almuerzo, al baño, entre otros; por lo tanto su computador se deja sin cuidado con la sesión a la red abierta. Alguien podría acceder al computador y buscar información importante para ser almacenada en un dispositivo USB o enviarla a través de correo electrónico. Si un atacante es realmente elegante, podría instalar una puerta trasera de modo que pudiera recuperar el acceso a la máquina remotamente o podría instalar un programa de capture los paquetes enviados o recibidos al equipo y entonces volver unos días después y extraer los resultados. Esta información proporcionaría contraseñas, datos importantes y una gran cantidad de información útil.

Puesto que hemos visto que tener el acceso físico a un recurso es bastante fácil, combinar eso con la amenaza de una terminal abierta proporciona una vulnerabilidad enorme a alguien quien la pueda utilizar para atacar una red.

Una forma de contrarrestar esto es culturizar a los empleados de una compañía que cierren sus sesiones cada vez que dejen solo su equipo a si sea por unos minutos. Debo precisar que este proceder debe estar en un documento donde residan las políticas de seguridad adoptadas por la empresa. Sin embargo, si no se le pone la seriedad del caso puede recibir maldiciones de los empleados al usted hacerle notar que no está cumpliendo con las políticas de seguridad, en estos casos es recomendable tener buenos lazos con el departamento de recursos humanos de modo que puedan tratar tales situaciones.

CONTRASEÑAS ESCRITAS

Con la observación detrás de hombros usted tiene que extraer la contraseña una vez el usuario la esta digitando, pero en algunos casos hay una manera más fácil de obtener esto. Un gran número de personas escriben su contraseña con el fin de no olvidarlas. Esto lo hacen generalmente cada vez que les asignan una contraseña nueva. Unos días después cuando la contraseña la recuerdan permanentemente se olvidan de destruir la evidencia de la misma.

La mayoría de la gente que hace esto mantiene su copia de la contraseña pegada al teclado, monitor o cualquier otro sitio fácil de buscar y cerca de su computador. Nada es más emocionante o frustrante para un atacante que el sentarse en un computador y visualizar inmediatamente la contraseña cerca de el.

No es recomendable que un usuario normal escriba su contraseña, pero no lo es incluso cuando un administrador de red lo hace. En normal ver a una gran cantidad de administradores anotar sus contraseñas. La razón es triple. Primero, los administradores tienen que recordar generalmente varias contraseñas para los diferentes sistemas en los cuales trabajan. Cuantas más contraseñas tiene, más difícil es recordarlas. En segundo lugar, los administradores utilizan periódicamente estas contraseñas. Cuanto menos utiliza una contraseña, más difícil es recordar. Tercero, Si usted no ha utilizado una contraseña en dos semanas y de pronto se cae la red y

usted monta el respaldo del sistema, no es el momento de olvidarse de una contraseña. La mayoría de los administradores anotan sus contraseñas no solamente para asegurarse de que las recordarán, también lo hacen para garantizar su trabajo. Pues aunque usted no lo crea es una de las maneras más rápida de perder un trabajo el no levantar un sistema por que usted no recuerda la contraseña de ella.

Una buena práctica es que en los meses de cambio de año Diciembre – Enero, son muchas las personas que cambian su agenda de apuntes y la agenda vieja la mandan a la basura. Se aterroraría que muchos atacantes utilizando técnicas de Trashing (Escarbar en basureros) encuentran como una buena fuente de información de contraseñas, las agendas encontradas en los basureros

MAQUINAS DESCONECTADAS

Los computadores y los componentes de comunicación de una empresa deben de ir conectados a tomas eléctricos, dichos tomas deben estar protegidos y fuera del acceso de personas no autorizadas. Si alguien desconecta accidentalmente o adrede una máquina, ellos pueden causar la negación de un servicio contra un computador.

Si un servidor está apagado, la gente no puede tenerle acceso. Piense en el impacto si, el viernes, alguien desconecta accidentalmente el web server o mail server, nadie da aviso hasta la mañana de lunes, dejando el sitio inaccesible por todo el fin de semana.

CONEXION LOCAL

La última meta de la mayoría de los atacantes es acceder a una máquina. El acceso remoto es bueno, pero el acceso local es incluso mejor. Se configuran algunos sistemas para solamente poder realizarse ciertas funciones localmente.

También, teniendo el acceso local, un atacante conserva más fácilmente transferencia directa las grandes cantidades de datos. Si no, instalan un dispositivo de almacenamiento secundario, un atacante puede instalar rápidamente y fácilmente una unidad almacenamiento USB que permitiría copiar de manera automática grandes cantidades de datos. Restringir el acceso local y observar los logs del sistema es una manera de controlar este tipo de ataque.

Computadores Portátiles

Los atacantes roban información sensible comúnmente a través de computadores portátiles. Piense en esto: Las computadoras portátiles actuales contienen por lo menos difícilmente discos duros de 250-gigabyte, si son no más grandes, que pueden contener grandes cantidades de información. Los portátiles en forma de rectángulos y fáciles de transportar pueden ser objetivos de los ladrones de datos. Es normal ver hoy en día personas de una compañía determinada que, cuando viajan, copian el contenido del servidor a su computador portátil. Esto permite a cualquiera y a todos los documentos posibles estar en su disposición, no obstante de un punto de vista de la seguridad, descargar todos sus ficheros sobre una computadora portátil es una pesadilla de la seguridad.

Además de los datos que están en una computadora portátil, las computadoras portátiles contienen generalmente información de acceso remoto y contraseñas. La mayoría de la gente hace que las computadoras portátiles sean utilizadas para conectarse remotamente con su empresa o Internet. En estos casos, cuando el atacante da doble click sobre los iconos de acceso remoto, se conecta inmediatamente a la red, porque la contraseña se guarda en el portátil.

FUERA DE LÍNEA

La mayoría de los ataques que ocurren en una red son detectables siempre y cuando la compañía este atenta, pero existen ciertos tipos de ataques que no son detectables fácilmente, no hay ninguna manera de saber que se está realizando el ataque real.

Uno de esos casos, son los ataques por fuera de línea (fuera de la red), en que el atacante utiliza la red para adquirir cierta información y luego utiliza esa información para planear un ataque. Los siguientes son los tipos generales de ataques fuera de línea:

- Descargas de Archivos de Contraseñas
- Descargas de Textos Encriptados
- Copiar Grandes Cantidades de Datos

DESCARGA DE ARCHIVOS DE CONTRASEÑAS

Más adelante trataremos a fondo la forma de quebrantar las contraseñas. Aquí solo nos centraremos en adquirir el archivo de contraseñas y no en la forma de conseguirlo. Cuando un atacante desea ingresar de diferentes formas a un sistema, la manera más fácil de hacer esto es descargar o capturar una copia del archivo cifrado de las contraseñas y luego descifrarlas fuera de línea ósea por fuera de la red.

Dependiendo del sistema operativo y de la configuración, hay varias maneras en que alguien puede adquirir un archivo de contraseñas. El truco está en que el atacante debe ser persistente y creativo, hasta encontrar una eventual manera de conseguir el archivo de contraseñas. La mayoría de las compañías tienen una política muy liberal con las contraseñas que asigna o cambia, se pueden encontrar contraseñas que nunca expiran o otras que expiran cada seis meses. Esto significa que si un atacante se demora un mes para descifrar una contraseña le quedan 3,4 o 5 meses para disfrutarla antes de que el usuario la cambie nuevamente. Incluso si un atacante consigue solamente una semana de acceso a la red, le dará bastante tiempo a instalar puertas traseras de modo que él pueda conseguir nuevamente accesos en el futuro sin requerir contraseña.

DESCARGAS DE TEXTOS ENCRIPTADOS

Puesto que cada contraseña es un texto cifrado, descargar archivos de contraseñas es un subconjunto de descargas de texto cifrado. Hoy en día la gente esta asegurando un secreto por lo que a un archivo o texto le aplica unas claves para cifrar o descifrar el mensaje. En la mayoría de los casos, el algoritmo del cifrado es de conocimiento público. Por ejemplo, en Internet se explica y es muy conocido el algoritmo que UNIX y los sistemas operativos de Microsoft utilizan asegurar sus contraseñas, puesto que los atacantes conocen del algoritmo pero no la clave, ellos podrían completar un ciclo técnico con cada combinación posible para encontrar eventualmente la clave.

Esto es conocido como “Ataque por Fuerza Bruta” y es el más interesante sobre estos tipos de ataques porque es siempre el más acertado. Podría tomar 400 años, pero será acertado.

Puesto que todo cifrado se puede eventualmente romper, la meta de ser el primero en hacerlo lo hace mucho más difícil. Como usted puede imaginarse, cuanto más grande es el clave, más tiempo tomara en descifrala, si usted solamente tiene 4 caracteres para la clave, se puede completar un ciclo en poco tiempo para obtener la posible combinación. Por otra parte, si usted tuviera un clave de 2 millones de caracteres duraría una eternidad.

Pues bien el consejo es utilizar claves lo suficientemente largas que no se encuentren en un diccionario, para que en el momento en que alguien le aplique el ataque de fuerza bruta, desista en unas semanas o en unos meses.

Ahora tenga en cuenta, un atacante podría tomar un archivo y en su computador personal correrle un ataque de fuerza bruta que tome aproximadamente 5 años en descifrar una clave. Imagine ahora contar con 500 computadores (Cluster) realizando un ataque de fuerza bruta sobre el mismo archivo, el tiempo reduciría sustancialmente.

COPIAR GRANDES CANTIDADES DE DATOS

Con este tipo de ataque, alguien copia grandes cantidades de datos a una unidad de Tape Backup, Zip Drive o medio de almacenamiento USB en corto tiempo para luego ser analizada en su casa con calma, en busca de información importante. Si se conoce que un administrador almuerza entre 12:00 m y las 2:00 PM cada día, podría conectar un dispositivo de almacenamiento externo (si es que el computador ya no cuenta con uno) y copiar alrededor de 100 Megas a 2GB de datos.

Para que arriesgarse a ser descubierto analizando datos en el computador de la oficina si lo pude hacer desde su casa.

PROCEDIMIENTO QUE USAN LOS ATACANTES PARA COMPROMETER UN SISTEMA

Ahora que hemos echado una ojeada detallada a las varias categorías de exploits, miraremos en qué puede ser aplicada. Además de los tipos de exploits, es importante que entienda que se puede atacar, usted necesita conocer las debilidades de su sistema para poder protegerse de ellas. Si usted no sabe en que es débil su sistema tenga la seguridad que posiblemente está pasando por alto una vulnerabilidad que el atacante puede utilizar para comprometer su sistema. La principal razón de la seguridad de una red es el de tomar en cuenta todas las vulnerabilidades y no centrar nuestro esfuerzo en una sola de ellas o en una área equivocada.

Ahora que entiende en que puede ser atacado su sistema, miremos las cosas más comunes que se pueden atacar en una red:

- Puertos
- Servicios
- Software de Terceros
- Sistemas Operativos
- Contraseñas
- Ingeniería Social
- Puertas Traseras (Back doors)
- Caballos de Troya (Trojan horses)
- Rookits
- Canales Indirectos

En qué puedo ser atacado? En cualquier cosa y en todo. Si un atacante es creativo. El puede encontrar una manera de entrar a un sistema. Trataremos las cosas más comunes, los exploits de un atacante y cómo él consigue entrar en su sistema.

PUERTOS

Si un ladrón fuera a irrumpir a una casa, él entraría generalmente a través de una Ventana o de una Puerta, porque es la forma más fácil. Los puertos son las puertas y ventanas de un sistema operativo. Hay miles de puertos que puedan estar abiertos en un sistema. Actualmente el rango de los puertos varía de 1 a 65.535 para TCP y 1 a 65.535 para los UDP, de los cuales los primeros 1024 son reservados para el sistema. Cuantos más puertos abiertos hay en una maquina más puntos de vulnerabilidad existen en el sistema. Para obtener una lista de todos los puertos y los protocolos asignados a cada uno, pueden observar en RFC1700. RFC puede ser descargado de varios sitios incluyendo <http://www.rfc-editor.org/> . Algunos de los puertos más comunes son:

21 FTP
23 TELNET
25 SMTP
53 DNS
79 FINGER
80 HTTP
110 POP
137-139 NETBIOS

Técnicamente los puertos de entrada / salida en un computador son los canales por los que son transferidos los datos entre un dispositivo y el procesador.

Se recomienda que usted ejecute un escaneador de puertos en su sistema (Nmap es un buen ejemplo), con el fin de conocer que puertos están abiertos y cuáles son los puntos de vulnerabilidad.

SERVICIOS

Los servicios son los programas que se están ejecutando en una máquina para realizar una función específica. Los servicios llegan a ser peligrosos cuando se están ejecutando como administrador o como root y recuerde que el root o administrador puede hacer cualquier cosa. Si un servicio se está ejecutando como root, cualquier comando que ejecute, se ejecutará como administrador. Esto quiere decir que si soy un usuario normal y deseo ejecutar un proceso como root, debo atacar un servicio que se esté ejecutando como root para luego tomar el control.

Así mismo como los puertos, cuantos más servicios estén ejecutando, más son los puntos de vulnerabilidad que tiene un sistema. Sin embargo, cada administrador puede limitar el número de servicios, solo se debe dejar aquellos que son prioritarios en un sistema.

La manera de observar los servicios que se están ejecutando en un sistema es fácil, por ejemplo en Windows 200x server, la opción servicios me muestra los servicios habilitados y deshabilitados. En Unix/Linux lo hace el comando “ps -fea”, sin embargo, puede también editar los archivos “services” que se encuentran en los directorios de configuración de cualquier sistema operativo.

SOFTWARE DE TERCEROS

Debido a que somos buenos profesionales en seguridad informática, antes de comprar un software realizado por una tercera persona, obtenemos primero el código de fuente, lo revisamos, y nos cercioramos de que no tiene puerta trasera alguna. Entonces, instalamos confiadamente nuestro software. Por supuesto, nadie hace esto, ponemos nuestra confianza oculta en los vendedores de software asegurando que su producto trabaja según lo anunciado.

La historia ha mostrado que esta confianza es peligrosa, pero no tenemos ninguna opción. Ha habido casos donde los virus fueron embutidos dentro de software o el software tenía puertas traseras que fueron puestas por el vendedor. Piense en las muchas características ocultas en varios sistemas operativos. Éstas características se les llama huevos de Pascua, y si usted busca en Internet, podrá encontrar una gran cantidad ellos. Visite el sitio <http://www.eeggs.com> allí encontrará un listado grande de estos programas.

Nota: Si no puede ver las paginas indicadas es posible que su proveedor de internet las tenga filtradas, por lo que se sugiere cargarlas a través de evasores de proxys como: <http://proxify.com/> o <http://www.vtunnel.com/>²

Si un sistema operativo puede ser comercializado con estas características ocultas, qué otras puertas traseras se encontraría en ella que aun no han sido descubiertas?

² Mayor información de evasores de proxys, visite: http://proxy.org/proxies_sorted.shtml

La gente publica los huevos de Pascua por diversión, pero si un revelador pusiera una puerta trasera de un sistema operativo que podría comprometer la información del disco duro, usted cree que lo publicaría? Probablemente no. Recuerde, usted solo necesita una conexión a la red, para que su sistema este comprometido ante un atacante.

Otro tema a considerar son las prácticas empresariales que hacen las Universidades en convenio con la empresa pública o privada, muchas empresas por cuestiones de economía utilizan estudiantes que a cambio de una práctica para obtener su titulo profesional, ponen en sus manos el desarrollo de un software productivo para la organización.

Si bien muchos de estos productos han sido exitosos por la creatividad de los mismos estudiantes, son también muchos los que se han convertido en la pasarela de entrada para los atacantes. Surgen dos buenas preguntas:

- ¿Cuántos de estos desarrolladores han recibido formación por parte de la Universidad en temas de calidad de software y seguridad informática?

Y lo más importante:

- ¿Cuántas empresas utilizan metodologías de testeos de software para medir la calidad y seguridad de los productos desarrollados al interior de la empresa?

SISTEMAS OPERATIVOS

Previamente en “Ataques al Sistema Operativo”, comparamos un sistema operativo a una casa, las puertas y las ventanas de un sistema operativo son los servicios que se está ejecutando y puertos que tiene abierto. Entre más servicios y puertos tenga, más puntos de vulnerabilidad posee un sistema. De acuerdo con esto, es importante recordar que una instalación por defecto de un sistema operativo no es recomendable debido a que se instala gran cantidad de puertos y de servicios.

De la perspectiva de un fabricante de software, tiene sentido incluir todos los servicios y puertos ya que con esto evitan gasto de soporte. De una perspectiva del consumidor, no tiene sentido, ya que el valor por defecto, no es seguro. La mayoría de las empresas una vez instalan un sistema operativo piensan que su trabajo está hecho y no tienen en cuenta los parches y actualizaciones del mismo. Esto deja a la compañía con los sistemas operativos desactualizados, que tienen una gran cantidad de vulnerabilidades.

CONTRASEÑAS (PASSWORDS)

La mayoría de las empresa no creen que en sus contraseñas esta soportada gran parte de la seguridad de su sistema pero también se debe tener en cuenta que tampoco es la única línea de defensa.

Las contraseñas son también una manera común de conseguir acceso a un sistema porque los empleados tienen generalmente contraseñas muy débiles, es decir, contraseñas que se pueden encontrar en diccionario, contraseñas que nunca caducan, contraseñas alusivas al nombre del propietario, etc. Como si fuera poco, existen lugares en que las contraseñas nunca son cambiadas y las cuentas viejas nunca son borradas del sistema. Todas estas características conducen al hecho de que las

contraseñas son una manera muy fácil para que un atacante encuentre una abertura sobre una compañía.

INGENIERIA SOCIAL

Una de las últimas categorías de los exploits es el engaño o la mentira. La mayoría de los ataques no se pueden realizar, si no hay de por medio cierto elemento de engaño implicado. Algunas redes están abiertas de par en par pero, en la mayoría de los casos, usted tiene que utilizar una técnica llamada ingeniería social para adquirir la información adicional. La ingeniería social es básicamente cuando usted convence a la gente para que le suministre información que no darían normalmente, y usted hace esto fingiendo ser alguna otra persona.

La clave a recordar con la ingeniería social es que hay una pequeña línea que separa el confiar en alguien o no confiar en nadie. Así puede suceder, que si alguien llama solicitando información, dárselas es probablemente demasiado aventurado. Por otra parte, si usted no se la da; podría perder su empleo.

Actualmente una forma de utilizar la ingeniería social son las aplicaciones ROGUE que simulan ser programas de seguridad, causando miedo en el usuario para tentarlos a que adquieran el falso producto como un falso antivirus o técnicas como el PHISHING la cual se basa en la obtención de información sensible y confidencial del usuario, sobre todo de índole financiera. La clonación de páginas web y el pharming local son las técnicas más utilizadas en ataques de phishing.

Por tanto usted podría utilizar un recurso y es confirmar antes de entregar información valiosa.

PUERTAS TRASERAS (*Backdoors*)

Las backdoors o puertas traseras son programas que permiten el acceso y control de un ordenador de forma remota. Suelen instalarse mediante troyanos y abren en el ordenador comprometido una serie de puertos que permiten al delincuente informático conectarse y utilizarlo como si estuviese frente al ordenador.

CABALLOS DE TROYA

Una manera común en que un atacante accede a una máquina en una red alejada está en el uso de un programa de Caballo de Troya. Recuerde que un Caballo de Troya es un programa que tiene dos características: una abierta y una secreta. Un troyano realiza una acción deseada por el usuario, pero en realidad lleva a cabo una actividad maliciosa en su ordenador. Su principal cometido suele ser conseguir que el usuario ejecute un programa que instale otro tipo de malware, como backdoors, keyloggers, rootkits, etc. No se consideran en la misma categoría que los virus informáticos puesto que no pueden propagarse de forma autónoma y requieren de la intervención del usuario para activarse.

ROOTKITS

Los rootkits son conjuntos de programas que permiten al delincuente tomar el control del sistema con todos los privilegios. Su forma de actuar suele consistir en reemplazar componentes legítimos del sistema por versiones modificadas de los mismos. Esto les hace casi indetectables por los sistemas de control del sistema operativo (como el sistema de Restauración del Sistema de Windows) y provoca que el usuario tenga una falsa sensación de seguridad. Una vez se ha instalado el rootkit en el sistema, este puede llevar a cabo infinidad de acciones: buscar información confidencial en el sistema, como números de tarjetas de crédito, certificados digitales o archivos con usuarios y contraseñas, instalar keyloggers que registren la actividad del usuario y la envíen al delincuente, o instalar backdoors que permitan al delincuente tomar el control del sistema y utilizarlo para lanzar otros ataques sin comprometerle a él directamente.

CANALES INDIRECTOS

Este tipo de ataque no es de los más populares. Un canal Indirecto recopila la información de fuentes externas y de acontecimientos circundantes para deducir la información principal importante. En este caso, la información indirecta puede ser tan valiosa como la información directa por ejemplo, digamos que el gobierno está concediendo un contrato para un proyecto muy importante y no desea revelar quién ganó el contrato, pero un atacante sabe que existe cinco finalistas. En las semanas siguientes, él puede leer el periódico, o notar que una compañía recibe una gran cantidad de envíos o encuentra un aviso solicitando nuevos cargos por parte de X empresa, el atacante puede deducir claramente quién ganó el contrato. Otro ejemplo, si uno atacante observa las cajas que entra a una compañía o observa su basura puede encontrar documentación o cajas con el logo de Windows 2008, lo que le permite deducir cual es el sistema operativo utilizado por la empresa.

Con los canales indirectos, no hay abertura en seguridad porque el atacante está utilizando la información externa desechada por la compañía.

METAS A ALCANZAR POR LOS ATACANTES

Existen muchos tipos de Exploits y de variantes que es a veces difícil catalogarlos todos. Es conveniente mirar los componentes de la base de la seguridad de la red y del computador para ver cómo los Exploits entran en este juego. Las siguientes son las tres metas de la seguridad de la información:

- Autenticidad:** Se debe garantizar que la identidad del emisor este directamente relacionada con el documento.
- Integridad:** Se debe eliminar la posibilidad de alteraciones al documento.
- Disponibilidad:** Se debe garantizar que la información estará disponible en todo momento.

Es importante precisar que cuando la mayoría de la gente piensa en seguridad, ella piensa solamente en secreto, no integridad y la disponibilidad.

Para entender mejor los Exploits, miremos abreviadamente cada uno de estas áreas de la seguridad.

SECRETO

Cómo hace usted para controlar el acceso a la información importante y permitir el ingreso solamente a las personas autorizadas?

Los ataques normales contra el Secreto son como las de un ladrón de tarjeta de crédito a través de Internet, que irrumpe en las bases de datos para obtener los secretos vitales de una compañía, pero las amenazas contra la Autenticidad a veces no son tan normales. los errores de los empleado que arrojan a la basura documentación con información vital o los administradores de red que tienen un respaldo del sistema que trae todos los permisos posibles es lo que compromete la seguridad del sistema.

Algunas maneras de protegerse de las vulnerabilidades de la información en lo referente al secreto es examinar los permisos de acceso cuidadosamente y educar a sus empleados en los buenos principios de la seguridad (Políticas de Seguridad), cerciorándose de que solamente la gente que necesita realmente el acceso tiene acceso, y que sus empleados están enterados de las debilidades posibles que se manejan al mantener una información confidencial por tanto tiempo guardada con la misma clave de autorización de Acceso.

En varios casos, el hurto da lugar a un ataque contra el secreto o a una pérdida de autenticidad. A veces, si un delincuente roba el Disco Duro o una memoria USB, esta intrusión es más que un ataque contra la disponibilidad. Sin embargo, el hurto de medios magnéticos o los documentos, da lugar a un ataque contra el secreto. Esto es verdad porque los usuarios desautorizados ahora tienen acceso a datos de la compañía.

INTEGRIDAD

La integridad se trata de prevenir, de detectar, o de no permitir la modificación incorrecta de datos. Algunas veces, se combina la integridad con el secreto para cambiar la información, porque para esto usted generalmente necesita el acceso a los datos.

Los ataques contra integridad implican a una persona desautorizada que hace modificaciones a la información y/o a los datos. Es difícil defenderse contra los ataques a la integridad porque se notan solamente después de ocurrido y comprometido el sistema. La mayoría de las compañías no entienden que los ataques contra integridad son una amenaza grande, pero esperanzadamente los ejemplos anteriores ayudarán a cambiar sus mentes.

DISPONIBILIDAD

Con ataques del secreto y de la integridad, un atacante necesita tener un cierto acceso a una red corporativa. Un ataque de la disponibilidad, sin embargo, se puede realizar contra cualquier sistema que esté conectado a Internet. Esta es la razón por la cual este tipo de ataques son tan difíciles contrarrestar.

Hoy en día uno de los factores exitosos de una compañía es el estar conectado en el mundo de Internet, Intranet y extranet para realizar su trabajo. Es decir los datos, información, servidores, redes, etcétera deben estar disponibles para los usuarios autorizados cuando y donde los necesiten.

RESUMEN

Ya conoce los tipos de ataques que pueden hacer contra usted para comenzar a construir las defensas apropiadas.

Muchas compañías piensan que son seguras porque invierten mucho dinero en seguridad. Desafortunadamente, una gran cantidad de compañías aplican la seguridad en las áreas incorrectas.

Si este capítulo amplió la visión de la seguridad de la información tenga en cuenta que este peso no puede caer en el administrador de la red, son muchas las empresas que delegan esta función al administrador de la red sin tener en cuenta que la seguridad implica tiempo de investigación constante tiempo que el administrador de la red normalmente no tiene. La seguridad debe estar en manos del Oficial de Seguridad o en manos de terceros expertos en el tema.

BIBLIOGRAFÍA

Anonymous. *Maximum Security: a hacker's guide to protecting your Internet site and network*. McMillan Computer Publishing, 1997.

O_r Arkin. Network Scanning Techniques, Noviembre 1999. PubliCom Communications Solutions.

Sue Berg et al. Glossary of Computer Security Terms. Technical Report NCSC-TG-004, National Computer Security Center, Octubre 1988.

Steven M. Bellovin. Security problems in the tcp/ip Protocol Suite. *Computer Communications Review*, 19(2):32{48, Abril 1989.

Steven M. Bellovin. RFC1498: Defending against sequence number attacks, Mayo 1996

CERT. CERT Advisory CA{99{02. Trojan Horses. Technical report, Computer Emergency Response Team, Marzo 1999.

Fred Cohen. Simulating Cyber Attack Defenses and Consequences, <http://all.net/journal/ntb/simulate/simulate.html> , Mayo 1999.

Intrusion Detection System Consortium. Intrusion Detection Systems buyer's guide. Technical report, ICSA.NET, 1999.

Je_ Crume. *Inside Internet Security: What hackers don't want you to know*. Addison Wesley, 2000.

Dethy. Examining portscan methods { Analysing Audible Techniques, January 2001. <http://www.synnrgy.net/downloads/papers/portscan.txt>

Robert David Graham. Network Intrusion Detection Systems FAQ v. 0.8.3, Marzo 2000. <http://www.robertgraham.com/pubs/network-intrusion-detection.html>.

Leslie Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770{772, Noviembre 1981

Ed Skoudis. Counter hack, 2002, Prentice Hall.

Eric Cole. Hackers Beware, 2002, Sans Institute.

Stuart McClure, Joel Scambray, George Kurtz. Hackers 3, 2002, Mc Graw Hill.

Stephen Northcutt, Judy Novak. Detección de Intrusos. 2001, Prentice Hall.

The Honeynet Project. Know Your Enemy. 2002, The Honeynet Project.

John Chirillo. Hack Attack Revealed. 2001, Wiley. Sybex. Security Complete. 2001.

TABLA DE CONTENIDO

| | |
|---|-----------|
| INTRODUCCIÓN | 1 |
| CONOCIENDO AL ENEMIGO Y COMO TRABAJA | 2 |
| UNA CIBERSOCIEDAD A LA QUE DEBEMOS CONOCER | 2 |
| HACKERS | 2 |
| CRACKERS | 3 |
| LAMERS | 4 |
| COPYHACKERS | 5 |
| BUCANEROS | 5 |
| PHREAKER..... | 5 |
| NEWBIE | 6 |
| SCRIPT KIDDIE | 6 |
| METODOS Y HERRAMIENTAS DE ATAQUES..... | 7 |
| ¿QUE ES UN EXPLOIT ? | 8 |
| EL PROCESO DE LOS ATACANTES..... | 9 |
| RECONOCIMIENTO PASIVO..... | 9 |
| RECONOCIMIENTO ACTIVO | 10 |
| EXPLOTANDO EL SISTEMA | 11 |
| SUBIR PROGRAMAS..... | 15 |
| DESCARGAR DATOS..... | 16 |
| CONSERVANDO EL ACCESO | 16 |
| CUBRIENDO EL RASTRO | 17 |
| LOS TIPOS DE ATAQUES..... | 19 |
| CATEGORIA DE LOS EXPLOIT | 20 |
| SOBRE INTERNET | 20 |
| SOBRE LA LAN..... | 23 |
| LOCALMENTE..... | 29 |
| FUERA DE LÍNEA | 32 |
| PROCEDIMIENTO QUE USAN LOS ATACANTES PARA COMPROMETER UN | |
| SISTEMA | 35 |
| PUERTOS..... | 35 |
| SERVICIOS..... | 36 |
| SOFTWARE DE TERCEROS | 36 |
| SISTEMAS OPERATIVOS..... | 37 |
| CONTRASEÑAS (PASSWORDS) | 37 |
| INGENIERIA SOCIAL..... | 38 |
| PUERTAS TRASERAS (Backdoors) | 38 |
| CABALLOS DE TROYA | 38 |
| ROOTKITS | 39 |
| CANALES INDIRECTOS | 39 |
| METAS A ALCANZAR POR LOS ATACANTES..... | 40 |
| SECRETO | 40 |
| INTEGRIDAD..... | 41 |
| DISPONIBILIDAD | 41 |
| RESUMEN..... | 42 |
| BIBLIOGRAFÍA..... | 43 |