

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 César Arango Serna

www.itforensic-la.com



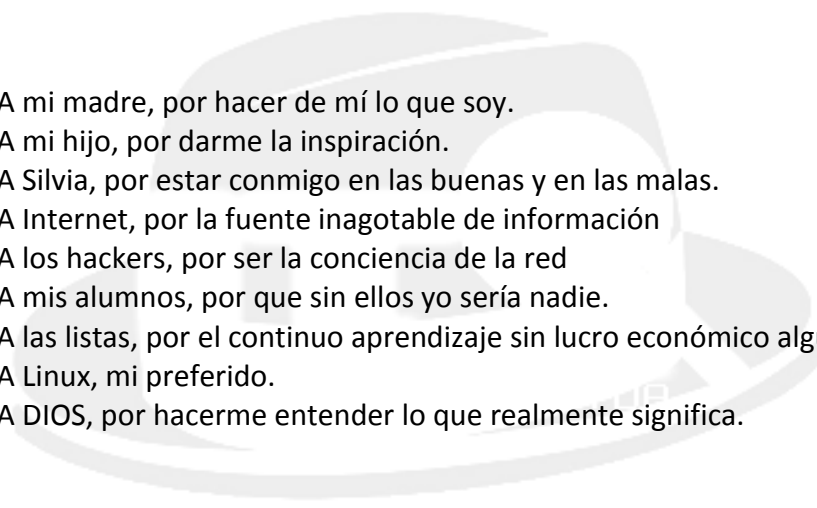
EL ATACANTE INFORMÁTICO

IT Forensic Ltda
<http://www.itforensic-la.com>

AUTOR: Ing. Jhon César Arango Serna

Enero de 2010.

AGRADECIMIENTOS



A mi madre, por hacer de mí 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

Revisado por: Ing. Ivan Humberto Gonzalez

CAPÍTULO 1

INTRODUCCIÓN

“La seguridad absoluta, tendría un costo infinito.”

Anónimo.

“Son muchas las técnicas y herramientas para atacar medios tele-informáticos
Sin embargo solo dos 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 cómputo.

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 él, 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 " bombeador 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 cibernética.

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.

MÉTODOS Y HERRAMIENTAS DE ATAQUES

El objetivo es describir cuáles 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.

¿QUÉ 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 él.

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 así 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 aprovechará esta circunstancia y no habrá una segunda vez.

ELEVACIÓN 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.

DENEGACIÓN 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 produce 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 hacen 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 ocultada. 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 Troya 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 buscará siempre la manera más fácil para comprometer a una máquina o a la red.

En algunos casos, El atacante puede acertar con sólo 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 término 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 SESIÓN

En algunos casos, es más fácil realizar un ataque como un usuario legítimo, 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 él.

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 él.

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 por qué 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 sólo verá 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 auditorías 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.l0phtcrack.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 éste 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 sólo 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 nómina. 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 INALÁMBRICAS.

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

OBSERVACIÓN DETRÁS 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 él.

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

MÁQUINAS 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.

CONEXIÓN 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 puede 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.

Para que entienda en que puede ser atacado su sistema, miremos las cosas más comunes que se pueden buscar 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 máquina 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 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.synnergy.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 CÓMO 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
MÉTODOS Y HERRAMIENTAS DE ATAQUES.....	7
¿QUÉ 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

Conociendo al Enemigo

EL ATACANTE INFORMÁTICO

Protocolos de Comunicación
Ambientes Operativos

DoS

Buffer Overflow

Exploits

Enumeración

CAPÍTULO 2

PROTOCOLOS
DE

COMUNICACIÓN

Rookits

Virus

Criptografía

Metodologías y Estándares



Jhon César Arango Serna

www.itforensic-la.com

CAPÍTULO 2

INTRODUCCIÓN

Una vez conocida los pasos utilizados por los atacantes informáticos, es necesario conocer en profundidad como funciona los diferentes protocolos de comunicación que intervienen en una conexión de red, este capítulo nos ayudará a entender los diferentes mecanismos que intervienen en una comunicación, la estructura de IPv4 e IPv6.

Sin duda al finalizar este tema, estará preparado para emprender el fascinante mundo de la Enumeración, tema que será tratado en el capítulo 4. No sólo entenderá lo que es una dirección IP si no que también entenderá su estructura y sus diferentes cálculos que ayudan de forma ágil a dimensionar el tamaño de una red basada en TCP/IP.

Modelo de Referencia OSI

En 1980 Organización Internacional para la Estandarización (ISO), con sede en Ginebra desarrollo un Modelo de Referencia para la Interconexión de los Sistemas Abiertos el cual le dio el nombre del modelo OSI. Este modelo separa las comunicaciones de red en siete niveles los cuales explican lo que sucede cuando un computador se desea comunicar con otro, cada computador utiliza una serie de protocolos para realizar las funciones asignadas a cada nivel. El conjunto de niveles forma lo que se conoce con el nombre de “pila de protocolos”.

En otras palabras, cuando dos computadores desean comunicarse entre sí, una serie de módulos de software operan sobre cada sistema para garantizar la comunicación. Un módulo se asegura de formatear apropiadamente los datos para la transmisión, otro se encarga de la retransmisión de los paquetes perdidos y así sucesivamente. Cada uno de estos módulos es lo que llamamos Capa o Nivel.

Las capas del modelo OSI se muestran a continuación:

CAPA	NOMBRE	DESCRIPCION
7	Aplicación	Servicios de Red a Aplicaciones
6	Presentación	Representación de los Datos (ASCII)
5	Sesión	Comunicación de Dispositivos de Red
4	Transporte	Conexión Extremo a Extremo y Fiabilidad de los Datos
3	Red	Determinación de ruta IP
2	Enlace a Datos	Dirección Física (Mac y LLC)
1	Física	Señal y Transmisión Binaria

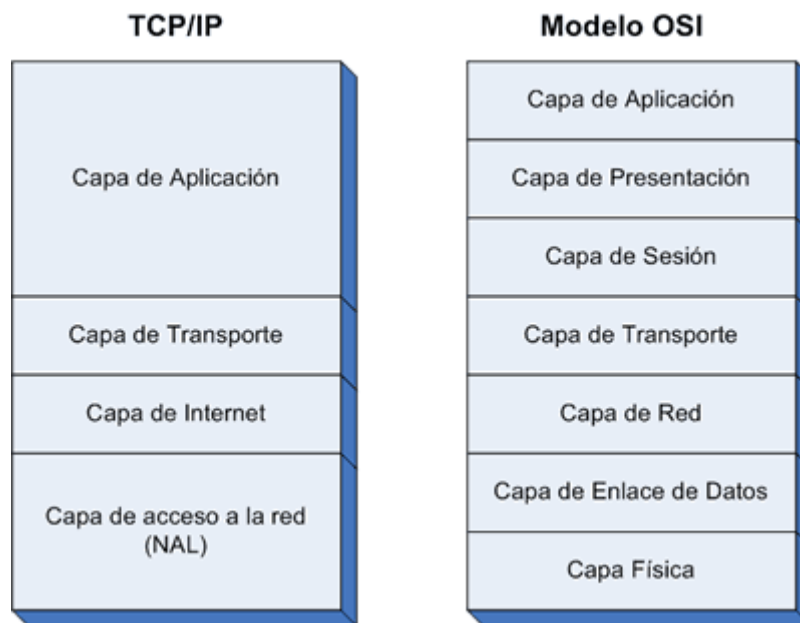
Modelo de Referencia TCP/IP

A mediados de los años sesenta el Departamento de Proyecto e Investigaciones Avanzadas para la Defensa de los EE.UU (ARPA o DARPA como se llamo más tarde) empezaron la investigación de para crear una red que enlazará los contratantes de ARPA. Los resultados no se hicieron esperar y a finales de los años 70 empezó a ver a luz lo que hoy conocemos con el nombre de TCP/IP. La RFC¹ 760, que describe el protocolo de Internet que se entregó al público el 1 de enero de 1980, sufro luego

¹ http://es.wikipedia.org/wiki/Request_For_Comments

modificaciones en los RFC 791, 793 y 768 los cuales integran el Protocolo de Control de Flujo (TCP) y el Protocolo de Datagramas de Usuario (UDP).

Los diseñadores de la familia de protocolos de TCP/IP eligieron un modelo más simple con menos niveles para mejorar el rendimiento y facilitar la implementación. Este modelo consta de 4 capas, a continuación se muestra el modelo TCP/IP comparado con el modelo OSI.



Para entender como atacan un sistema de cómputo a través de una red, necesitamos conocimientos del más popular de los protocolos, el TCP/IP ampliamente usado hoy en Internet. Este protocolo incluye varios componentes: el Protocolo de Control de Flujo (TCP), el Protocolo de Datagramas de Usuario (UDP), el Protocolo de Internet (IP) y Protocolo de Control de Mensajes de Internet (ICMP). Exploraremos ahora cada uno de estos protocolos.

Protocolo de Internet (IP)

La dirección IP es el identificador de cada host dentro de su red de redes. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser

distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos computadores con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos computadores con la misma dirección IP (privadas) siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comunique).

Las direcciones IP se clasifican en:

Direcciones IP públicas.

Son visibles en todo Internet. Un computador con una IP pública es accesible (visible) desde cualquier otro computador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.

Direcciones IP privadas (reservadas).

Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por enrutadores (routers). Se utilizan en las empresas para los puestos de trabajo. Los computadores con direcciones IP privadas pueden salir a Internet por medio de un router (o proxy) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a computadores con direcciones IP privadas.

A su vez, las direcciones IP pueden ser:

Direcciones IP estáticas (fijas).

Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas a través de un proveedor de servicios (ISP) o registrándolas directamente a través de <http://lacnic.net/sp/index.html>

Direcciones IP dinámicas.

Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un Módem, Router Adsl, Router inalámbrico, Etc. Los proveedores de

Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP (es muy improbable que todos se conecten a la vez).

Clases de Direcciones

Las direcciones IP versión 4 están formadas por 4 bytes (32 bits). Se suelen representar de la forma a.b.c.d donde cada una de estas letras es un número comprendido entre el 0 y el 255. Por ejemplo la dirección IP 201.228.3.147.

Las direcciones IP también se pueden representar en hexadecimal, desde la 00.00.00.00 hasta la FF.FF.FF.FF o en forma binaria, desde la 00000000.00000000.00000000.00000000 hasta la 11111111.11111111.11111111.11111111.

Utilizando la calculadora científica de un computador podemos realizar las siguientes conversiones:

Decimal	201.228.3.147
Hexadecimal	C9.E4.3.93
Binario	11001001.11100100.00000011.10010011

¿Cuántas direcciones IP existen? Si calculamos 2 elevado a 32 (232) obtenemos 4,294,967,296 direcciones distintas. Sin embargo, no todas las direcciones son válidas para asignarlas a hosts. Las direcciones IP no se encuentran aisladas en Internet, sino que pertenecen siempre a alguna red. Todas las máquinas conectadas a una misma red se caracterizan en que los primeros bits de sus direcciones son iguales. De esta forma, las direcciones se dividen conceptualmente en dos partes: la porción de red y la porción de host.

Dependiendo del número de hosts que se necesiten para cada red, las direcciones de Internet se han dividido en las clases primarias A, B y C. La clase D está formada por direcciones que identifican no a un host, sino a un grupo de ellos. Las direcciones de clase E no se pueden utilizar (están reservadas).

CLASE A

0	1	8	16	24	31
0	Red (7 bits)		Dirección local (24 bits)		

Su primer octeto en su forma binaria empieza por 0, por lo que una IP como: 00101001.11100010.01010101.10101010 se considera como una dirección de clase A.

En su forma decimal son todas aquellas que en su primer octeto están entre 0-127, si convertimos el ejemplo anterior tenemos: 41.226.85.170 lo que lo hace una IP de clase A.

CLASE B

0	1	2		15	16		31
10	Red (14 bits)				Dirección local (16 bits)		

Su primer octeto en su forma binaria empieza por 10, por lo que una IP como: 10101001.11100010.01010101.10101010 se considera como una dirección de clase B.

En su forma decimal son todas aquellas que en su primer octeto están entre 128-191, si convertimos el ejemplo anterior tenemos: 169.226.85.170 lo que lo hace una IP de clase B.

CLASE C

0	1	2	3		24	25		31
110	Red (21 bits)				Dirección local (8 bits)			

Su primer octeto en su forma binaria empieza por 110, por lo que una IP como: 11001001.11100010.01010101.10101010 se considera como una dirección de clase C.

En su forma decimal son todas aquellas que en su primer octeto están entre 192-223, si convertimos el ejemplo anterior tenemos: 201.226.85.170 lo que lo hace una IP de clase C.

CLASE D

Las direcciones de clase D son direcciones de IP de multidifusión los cuales se usan para enviar un único paquete de uno a muchos. Los 4 primeros bits se establecen al valor de 1110. los 28 restantes se usan para direcciones IP de multidifusión.

CLASE E

Las direcciones de clase E son direcciones experimentales, reservadas para usos futuros. Los primeros 5 bits se establecen al valor 11110.

Clase	Bits Red (m)	Número de redes (2^m)	Bits de Hosts (n)	Número de Host por red ($2^n - 2$)	Rango de direcciones de redes	Máscara de Subred
A	7	128	24	16.777.214	0.0.0.0 – 127.0.0.0	255.0.0.0
B	14	16.384	16	65.534	128.0.0.0 – 191.255.0.0	255.255.0.0
C	21	2.097.152	8	254	192.0.0.0 – 223.255.255.0	255.255.255.0
D		-		-	224.0.0.0 - 239.255.255.255	-
E		-		-	240.0.0.0 - 255.255.255.255	-

Difusión (broadcast) y multidifusión (multicast).

El término difusión (broadcast) se refiere a todos los hosts de una red; multidifusión (multicast) se refiere a varios hosts (aquellos que se hayan suscrito dentro de un mismo grupo). Siguiendo esta misma terminología, en ocasiones se utiliza el término unidifusión (unicast) para referirse a un único host.

Direcciones IP especiales y reservadas

No todas las direcciones comprendidas entre la 0.0.0.0 y la 223.255.255.255 son válidas para un host: algunas de ellas tienen significados especiales.

Difusión o broadcasting es el envío de un mensaje a todos los computadores que se encuentran en una red. La dirección de loopback (normalmente 127.0.0.1) se utiliza para comprobar que los protocolos TCP/IP están correctamente instalados en nuestro propio computador. Lo veremos más adelante, al estudiar el comando PING.

Las direcciones de redes siguientes se encuentran reservadas para su uso en redes privadas (intranets). Una dirección IP que pertenezca a una de estas redes se dice que es una dirección IP privada.

Clase	Rango de direcciones reservadas de redes
A	10.0.0.0
B	172.16.0.0 - 172.31.0.0
C	192.168.0.0 - 192.168.255.0

Por ejemplo, si estamos construyendo una red privada con un número de computadores no superior a 254 podemos utilizar una red reservada de clase C. Al primer computador le podemos asignar la dirección 192.168.23.1, al segundo 192.168.23.2 y así sucesivamente hasta la 192.168.23.254. Como estamos utilizando direcciones reservadas,

tenemos la garantía de que no habrá ninguna máquina conectada directamente a Internet con alguna de nuestras direcciones. De esta manera, no se producirán conflictos y desde cualquiera de nuestros computadores podremos acceder a la totalidad de los servidores de Internet (si utilizásemos en un computador de nuestra red una dirección de un servidor de Internet, nunca podríamos acceder a ese servidor).

Intranet.

Red privada que utiliza los protocolos TCP/IP. Puede tener salida a Internet o no. En el caso de tener salida a Internet, el direccionamiento IP permite que los hosts con direcciones IP privadas puedan salir a Internet pero impide el acceso a los hosts internos desde Internet. Dentro de una intranet se pueden configurar todos los servicios típicos de Internet (web, correo, mensajería instantánea, etc.) mediante la instalación de los correspondientes servidores. La idea es que las intranets son como "internets" en miniatura o lo que es lo mismo, Internet es una intranet pública gigantesca.

Extranet.

Unión de dos o más intranets. Esta unión puede realizarse mediante líneas dedicadas (RDSI, X.25, frame relay, ADSL, punto a punto, etc.) o a través de Internet.

Internet.

La mayor red pública de redes TCP/IP.

Máscara de subred

Una máscara de subred es aquella dirección que enmascarando nuestra dirección IP, nos indica si otra dirección IP pertenece a nuestra subred o no.

La siguiente tabla muestra las máscaras de subred correspondientes a cada clase:

Clase	Máscara de subred	Bits de Red
A	255.0.0.0	8
B	255.255.0.0	16
C	255.255.255.0	24

Si expresamos la máscara de subred de clase A en notación binaria, tenemos: 11111111.00000000.00000000.00000000

Los unos indican los bits de la dirección correspondientes a la red y los ceros, los correspondientes al host. Según la máscara anterior, el primer

byte (8 bits) es la red y los tres siguientes (24 bits), el host. Por ejemplo, la dirección de clase A 35.120.73.5 pertenece a la red 35.0.0.0.

Supongamos una subred con máscara 255.255.0.0, en la que tenemos un computador con dirección 148.120.33.110. Si expresamos esta dirección y la de la máscara de subred en binario, tenemos:

$$\begin{array}{rcl}
 148.120.33.110 & = & 10010100.01111000.00100001.01101110 \\
 255.255.0.0 & = & 11111111.11111111.00000000.00000000 \\
 \hline
 148.120.0.0 & = & 10010100.01111000.00000000.00000000 \\
 & & <-----\text{RED}-----><-----\text{HOST}----->
 \end{array}$$

Al hacer la operación AND entre la dirección IP y la Mascara (donde hay dos 1 en las mismas posiciones ponemos un 1 y en caso contrario, un 0) obtenemos la tercera que se considera la dirección de RED.

Si hacemos lo mismo con otro computador, por ejemplo el 148.120.33.89, obtenemos la misma dirección de subred. Esto significa que ambas máquinas se encuentran en la misma subred (la subred 148.120.0.0).

En cambio, si tomamos la 148.115.89.3, observamos que no pertenece a la misma subred que las anteriores.

$$\begin{array}{rcl}
 148.115.89.3 & = & 10010100.01110011.01011001.00000011 \\
 255.255.0.0 & = & 11111111.11111111.00000000.00000000 \\
 \hline
 148.115.0.0 & = & 10010100.01110011.00000000.00000000
 \end{array}$$

Para calcular la dirección de Broadcast o Difusión, hay que hacer la suma lógica en binario (OR) de la IP con el inverso (NOT) de su máscara, en otras palabras tomamos como una plantilla el numero de ceros que existe en la máscara, en nuestro ejemplo anterior son los 16 últimos bits.

$$\begin{array}{rcl}
 255.255.0.0 & = & 11111111.11111111.00000000.00000000 \\
 & & <-16 \text{ bits (16 Ceros)}->
 \end{array}$$

Con este valor de 16 bits, lo que hacemos en la dirección de red en su forma binaria es cambiar los últimos 16 dígitos a su base contraria, es decir lo que este en 0 sea 1 y viceversa.

$$\begin{array}{rcl}
 \text{Dr. de Red} & 148.115.0.0 & = 10010100.01110011.00000000.00000000 \\
 \text{Dr de Difus.} & 148.115.0.0 & = 10010100.01110011.11111111.11111111
 \end{array}$$

Para este caso podemos decir que la dirección de broadcast es forma decimal es: 148.115.255.255

En una red de redes TCP/IP no puede haber hosts aislados: todos pertenecen a alguna red y todos tienen una dirección IP y una máscara de subred (si no se especifica se toma la máscara que corresponda a su clase). Mediante esta máscara un computador sabe si otro computador se

encuentra en su misma subred o en otra distinta. Si pertenece a su misma subred, el mensaje se entregará directamente. En cambio, si los hosts están configurados en redes distintas, el mensaje se enviará a la puerta de salida o router de la red del host origen. Este router pasará el mensaje al siguiente de la cadena y así sucesivamente hasta que se alcance la red del host destino y se complete la entrega del mensaje.

Para cada clase de dirección IP corresponde mínimo una máscara obligatoria según los visto anteriormente, sin embargo es posible aumentar el número de bits en unos (1) de la máscara para realizar algo que se conoce con el termino de sub enmascaramiento. Esta técnica nació debido a que el direccionamiento IP versión 4 se está agotando, por tanto los proveedores de servicios de internet solo entregan un pequeño rango de IP publicas con las cuales la empresa debe sacar todas sus maquinas a internet utilizando técnicas de NAT.

Si retomamos el ejemplo anterior tenemos:

IP	148.115.89.3	=	10010100.01110011.01011001.00000011
Mas	255.255.0.0	=	11111111.11111111.00000000.00000000

Note que por su primer octeto (148) la dirección se considera de clase B y a su vez esta le corresponde una máscara obligatoria, la cual es 255.255.0.0.

El sub enmascaramiento consiste en cambiar a uno (1) los primeros bits de la porción de host (los ceros) de la máscara de subred. El numero de ceros que desee cambiar depende de el numero de subredes que quiera construir, si escoge 1 seria 2^1 lo que representaría 2 subredes, si escoge 2 seria 2^2 lo que representaría 4 subredes, si escoge 3 seria 2^3 lo que representaría 8 subredes y así sucesivamente. Sin importar la clase de dirección mínimo tiene que dejar dos ceros en la máscara cuando está haciendo sub enmascaramiento.

Supongamos que vamos a convertir 5 bits de la porción de host de la máscara del ejercicio anterior, lo cual nos daría una nueva mascara, una nueva dirección de red y una nueva dirección de broadcast:

Ip	148.115.89.3	=	10010100.01110011.01011001.00000011
Mas	255.255. 248 .0	=	11111111.11111111. 11111 000.00000000
D.red	148.115. 88 .0	=	10010100.01110011.01011000.00000000
D.bro	148.115. 95.255	=	10010100.01110011.01011 111.11111111

Con esta nueva mascara podemos deducir:

Se pueden tener 2^{16} posibles redes, por cada una se puede construir 2^5 subredes y cada una puede albergar 2^{11} posibles host.

PRACTICA DE LABORATORIO

- Dada la dirección y la máscara de red hallar:
- Dirección de la Red
- Primera dirección de la Red
- Dirección de Broadcast
- Última dirección de Red

Dirección IP : 129.5.208.17
Máscara de Red : 255.255.252.0

Para hallar la dirección de Red desarrollamos un AND entre la Dirección IP y la Máscara de Red en binario

IP : 10000001.00000101.11010000.00010001
Máscara : 11111111.11111111.11111100.00000000

10000001.00000101.11010000.00000000 *

Al convertir a Decimal: Dirección de Red: 129. 5. 208. 0
La primera dirección de red es la siguiente a la dirección de red:
Primera Dirección de Red: 129. 5. 208. 1

Para averiguar la dirección de Broadcast, pasamos la máscara a binario:
Máscara : 11111111.11111111.11111100.00000000

El posible número de Hosts es igual a $2^n - 2$, donde n es igual al número de ceros a la derecha de la máscara, en este caso $n=10$, luego el número posible de Hosts = $2^{10} - 2 = 1022$.

El número de posibles subredes es igual a $2^{16-n} = 2^{16-10} = 2^6 = 64$
Se pueden crear 64 subredes de 1022 Hosts cada una, para un total de Hosts de $1022 * 64 = 65408$

Luego convertimos el número de ceros en unos y unos en ceros, hasta n dígitos, tomando la AND de los últimos 16 dígitos de la dirección IP y los 16 dígitos de la máscara.

11010000.00010001 *
11010011.11111111, tenemos entonces así:
211 . 255

Luego: La dirección de Broadcast es 129. 5. 211. 255

La última dirección de red es una menos que la de Broadcast
La última dirección de Red es: 129. 5. 211 .254

Formato del datagrama IP

El datagrama IP es la unidad básica de transferencia de datos entre el origen y el destino. Viaja en el campo de datos de las tramas físicas (recuérdese la trama Ethernet) de las distintas redes que va atravesando.

Cada vez que un datagrama tiene que atravesar un router, el datagrama saldrá de la trama física de la red que abandona y se acomodará en el campo de datos de una trama física de la siguiente red. Este mecanismo permite que un mismo datagrama IP pueda atravesar redes distintas: enlaces punto a punto, redes ADSL, redes Ethernet, redes Token Ring, etc. El propio datagrama IP tiene también un campo de datos: será aquí donde viajen los paquetes de las capas superiores.

0										10										20										30		
0	1	2	3	4	5	6	7	8	9	0	1	2	3	3	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
VERS				Long En			Tipo de servicio										Longitud total															
Identificación															Bandrs			Desplazamiento de fragmento														
TTL							Protocolo										CRC cabecera															
Dirección IP origen																																
Dirección IP destino																																
Opciones IP (si las hay)																							Relleno									
Datos																																
...																																

VERS (Versión, 4 bits) Indica la versión del protocolo IP que se utilizó para crear el paquete. Actualmente se utiliza la versión 4 (IPv4) aunque ya está implementándose la versión, la 6 (IPv6).

Long En (Longitud del Encabezado, 4 bits) Longitud de la cabecera expresada en múltiplos de 32 bits. El valor mínimo es 5, correspondiente a 160 bits = 20 bytes.

Tipo de servicio. Los 8 bits de este campo se dividen a su vez en:

Prioridad (3 bits). Un valor de 0 indica baja prioridad y un valor de 7, prioridad máxima. Los siguientes tres bits indican cómo se prefiere que se transmita el mensaje, es decir, son sugerencias a los enrutadores que se encuentren a su paso los cuales pueden tenerlas en cuenta o no. Bit D (Delay). Solicita retardos cortos (enviar rápido). Bit T (Throughput). Solicita un alto rendimiento (enviar mucho en el menor tiempo posible). Bit R (Reliability). Solicita que se minimice la probabilidad de que el datagrama se pierda o resulte dañado (enviar bien). Los siguiente dos bits no tienen uso.

Longitud total (16 bits). Indica la longitud total del paquete expresada en bytes. Como el campo tiene 16 bits, la máxima longitud posible de un paquete será de 65, 535 bytes.

Identificación (16 bits). Número de secuencia que junto a la dirección origen, dirección destino y el protocolo utilizado identifica de manera única un paquete en toda la red. Si se trata de un paquete fragmentado, llevará la misma identificación que el resto de fragmentos.

Banderas o indicadores (3 bits). Sólo 2 bits de los 3 bits disponibles están actualmente utilizados. El bit de Más fragmentos (MF) indica que no es el último paquete. Y el bit de No fragmentar (NF) prohíbe la fragmentación del paquete. Si este bit está activado y en una determinada red se requiere fragmentar el datagrama, éste no se podrá transmitir y se descartará.

Desplazamiento de fragmentación (13 bits). Indica el lugar en el cual se insertará el fragmento actual dentro del paquete completo, medido en unidades de 64 bits. Por esta razón los campos de datos de todos los fragmentos menos el último tienen una longitud múltiplo de 64 bits. Si el paquete no está fragmentado, este campo tiene el valor de cero.

Tiempo de vida o TTL (8 bits). Número máximo de saltos que puede estar un paquete en la red de redes. Cada vez que el paquete atraviesa un router se resta 1 a este número. Cuando llegue a cero, el paquete se descarta y se devuelve un mensaje ICMP de tipo "tiempo excedido" para informar al origen de la incidencia.

Protocolo (8 bits). Indica el protocolo utilizado en el campo de datos: 1 para ICMP, 2 para IGMP, 6 para TCP y 17 para UDP.

CRC cabecera (16 bits). Contiene la suma de comprobación de errores sólo para la cabecera del paquete. La verificación de errores de los datos corresponde a las capas superiores.

Dirección origen (32 bits). Contiene la dirección IP del origen.

Dirección destino (32 bits). Contiene la dirección IP del destino.

Opciones IP. Este campo no es obligatorio y especifica las distintas opciones solicitadas por el usuario que envía los datos (generalmente para pruebas de red y depuración).

Relleno. Si las opciones IP (en caso de existir) no ocupan un múltiplo de 32 bits, se completa con bits adicionales hasta alcanzar el siguiente múltiplo de 32 bits (recuérdese que la longitud de la cabecera tiene que ser múltiplo de 32 bits).

Datos. Son los datos que se están transmitiendo

Protocolo ICMP

Debido a que el protocolo IP no es fiable, los datagramas pueden perderse o llegar defectuosos a su destino. El protocolo ICMP (Internet Control Message Protocol, protocolo de mensajes de control y error) se encarga de informar al origen si se ha producido algún error durante la entrega de su mensaje. Pero no sólo se encarga de notificar los errores, sino que también transporta distintos mensajes de control.

El protocolo ICMP únicamente informa de incidencias en la red pero no toma ninguna decisión. Esto será responsabilidad de las capas superiores. Los mensajes ICMP viajan en el campo de datos de un datagrama IP, como se puede apreciar en el siguiente esquema:

		Tipo	Datos ICMP	
		↓	↓	
	Encabezado del datagrama	Área de datos del datagrama IP		
	↓		↓	
Encabezado de la trama	Área de datos de la trama			Final de la trama

Debido a que el protocolo IP no es fiable puede darse el caso de que un mensaje ICMP se pierda o se dañe. Si esto llega a ocurrir no se creará un nuevo mensaje ICMP sino que el primero se descartará sin más.

Los mensajes ICMP comienzan con un campo de 8 bits que contiene el tipo de mensaje, según se muestra en la tabla siguiente. El resto de campos son distintos para cada tipo de mensaje ICMP².

Campo de tipo	Tipo de mensaje ICMP
0	Respuesta de eco (Echo Reply)
3	Destino inaccesible (Destination Unreachable)
4	Disminución del tráfico desde el origen (Source Quench)
5	Redireccionar (cambio de ruta) (Redirect)
8	Solicitud de eco (Echo)
11	Tiempo excedido para un datagrama (Time Exceeded)
12	Problema de Parámetros (Parameter Problem)
13	Solicitud de marca de tiempo (Timestamp)
14	Respuesta de marca de tiempo (Timestamp Reply)
15	Solicitud de información (obsoleto) (Information Request)
16	Respuesta de información (obsoleto) (Information Reply)
17	Solicitud de máscara (Addressmask)
18	Respuesta de máscara (Addressmask Reply)

² El formato y significado de cada mensaje ICMP está documentado en la RFC 792 (en inglés, en español).

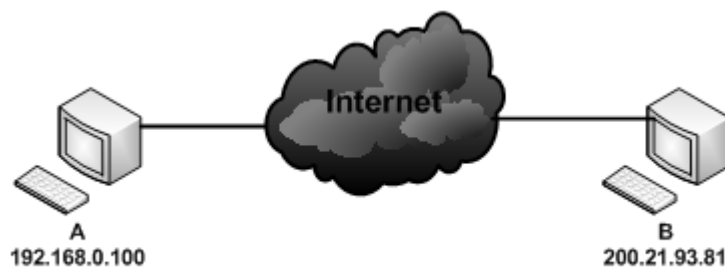
Los mensajes de solicitud y respuesta de eco, tipos 8 y 0 respectivamente, se utilizan para comprobar si existe comunicación entre 2 hosts a nivel de la capa de red. Estos mensajes comprueban que las capas física (cableado), acceso al medio (tarjetas de red) y red (configuración IP) están correctas. Sin embargo, no dicen nada de las capas de transporte y de aplicación las cuales podrían estar mal configuradas; por ejemplo, la recepción de mensajes de correo electrónico puede fallar aunque exista comunicación IP con el servidor de correo.

La orden PING envía mensajes de solicitud de eco a un host remoto e informa de las respuestas. Veamos su funcionamiento, en caso de no producirse incidencias en el camino.

A envía un mensaje ICMP de tipo 8 (Echo) a B

B recibe el mensaje y devuelve un mensaje ICMP de tipo 0 (Echo Reply) a A

A recibe el mensaje ICMP de B y muestra el resultado en pantalla



```
C:\Users\usuario>ping 200.21.94.81 -n 1
Haciendo ping a 200.21.94.81 con 32 bytes de datos:
Respuesta desde 200.21.94.81: bytes=32 tiempo=52ms TTL=244

Estadísticas de ping para 200.21.94.81:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 52ms, Máximo = 52ms, Media = 52ms
```

En la orden anterior hemos utilizado el parámetro "-n 1" para que el host A únicamente envíe 1 mensaje de solicitud de eco. Si no se especifica este parámetro se enviarían 4 mensajes (y se recibirían 4 respuestas).

Si el host de destino no existiese o no estuviera correctamente configurado recibiríamos un mensaje ICMP de tipo 11 (Time Exceeded).

```
C:\Users\usuario>ping 200.21.94.85 -n 1
Haciendo ping a 200.21.94.85 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 200.21.94.85:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
    (100% perdidos),
```

Si tratamos de acceder a un host de una red distinta a la nuestra y no existe un camino para llegar hasta él, es decir, los enrutadores no están correctamente configurados o estamos intentando acceder a una red aislada o inexistente, recibiríamos un mensaje ICMP de tipo 3 (Destination Unreachable).

Pero también puede suceder que el equipo al que se le está haciendo Ping tenga deshabilitado las respuestas eco por cuestiones de seguridad:

```
C:\Users\usuario>ping www.unicauca.edu.co -n 1
Haciendo ping a acuario.unicauca.edu.co [190.5.195.137] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 190.5.195.137:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
    (100% perdidos),
```

En este ejemplo vemos como el DNS resuelve la IP sin problemas, pero el Ping no responde. Para estos casos hay que utilizar otros mecanismos como por ejemplo la apertura de conexión a un puerto, como veremos más adelante.

El comando Ping es ampliamente utilizado para diagnosticar errores en la red, que van desde la interfaz local de red a condiciones de red o equipos de comunicación de datos.

Mensajes ICMP de tiempo excedido. Los datagramas IP tienen un campo TTL (tiempo de vida - TDV) que impide que un mensaje esté dando vueltas indefinidamente por la red de redes. El número contenido en este campo disminuye en una unidad cada vez que el datagrama atraviesa un router. Cuando el TTL de un datagrama llega a 0, éste se descarta y se envía un mensaje ICMP de tipo 11 (Time Exceeded) para informar al origen. Los mensajes ICMP de tipo 11 se pueden utilizar para hacer una traza del camino que siguen los datagramas hasta llegar a su destino. ¿Cómo? Enviando una secuencia de datagramas con TTL=1, TTL=2, TTL=3, TTL=4, etc... hasta alcanzar el host o superar el límite de saltos (30 si no se indica lo contrario). El primer datagrama caducará al atravesar el primer router y se devolverá un mensaje ICMP de tipo 11 informando al origen del router que descartó el datagrama. El segundo datagrama hará lo propio con el segundo router y así sucesivamente. Los mensajes ICMP recibidos permiten definir la traza.

Puertos

Un computador puede estar conectado con distintos servidores a la vez; por ejemplo, con un servidor de noticias y un servidor de correo. Para distinguir las distintas conexiones dentro de un mismo computador se utilizan los puertos. Un puerto es un número de 16 bits, por lo que existen 65536 puertos en cada computador. Las aplicaciones utilizan estos puertos para recibir y transmitir mensajes.

Los números de puerto de las aplicaciones cliente son asignados dinámicamente y generalmente son superiores al 1024. Cuando una aplicación cliente quiere comunicarse con un servidor, busca un número de puerto libre y lo utiliza.

En cambio, las aplicaciones servidoras utilizan unos números de puerto prefijados: son los llamados puertos well-known (bien conocidos). Estos puertos están definidos en la RFC 1700 y se pueden consultar en <http://www.ietf.org/rfc/rfc1700.txt>. A continuación se enumeran los puertos well-known más usuales:

Puerto	TCP o UDP	Nombre de protocolo o servicio	RFC
7	TCP/UDP	echo	792
20	TCP	Protocolo de transferencia de archivos (FTP)	959
21	TCP	Control de FTP	959
22	TCP	Shell segura (SSH)	-
23	TCP	Telnet	854
25	TCP	Protocolo simple de transferencia de correo (SMTP)	5321
53	TCP/UDP	Sistema de nombres de dominio (DNS)	1034
67	UDP	Servidor de protocolo de inicio (BootP, bootps)	951
68	UDP	Cliente de protocolo de inicio (bootpc)	951
69	UDP	Protocolo trivial de transferencia de archivos (TFTP)	1350
79	TCP	Finger	1288
80	TCP	Protocolo de transferencia de hipertexto (HTTP)	2616
88	TCP	Kerberos	4120
106	TCP	Servidor de contraseñas (Uso no registrado)	-
110	TCP	Protocolo de oficina de correos (POP3) Protocolo de oficina de correos de autenticación (APOP)	1939
111	TCP/UDP	Llamada a procedimiento remoto (RPC)	1057, 1831
113	TCP	Protocolo de identificación	1413
115	TCP	Programa seguro de transferencia de archivos (SFTP)	913
119	TCP	Protocolo de transferencia de noticias de red (NNTP)	3977
123	TCP/UDP	Network Time Protocol (NTP)	1305
137	UDP	Windows Internet Naming Service (WINS)	-

Puerto	TCP o UDP	Nombre de protocolo o servicio	RFC
138	UDP	Servicio de datagramas de NETBIOS	-
139	TCP	Bloque de mensaje de servidor (SMB)	-
143	TCP	Protocolo de acceso a mensajes de Internet (IMAP)	3501
161	UDP	Protocolo simple de administración de red (SNMP)	1157
192	UDP	-	-
311	TCP	Server Admin, Workgroup Manager, Server Monitor, Xsan Admin	-
389	TCP	Protocolo ligero de acceso a directorios (LDAP)	4511
427	TCP/UDP	Protocolo de ubicación de servicios (SLP)	2608
443	TCP	Capa de sockets seguros (SSL o "HTTPS")	-
445	TCP	Servidor de dominio SMB de Microsoft	-
497	TCP/UDP	Dantz Retrospect	-
500	UDP	ISAKMP/IKE	-
514	TCP	shell	-
514	UDP	Syslog	-
515	TCP	Impresora de línea (LPR), Protocolo LPD (Line Printer Daemon)	-
532	TCP	netnews	-
548	TCP	Protocolo de archivos de Apple (AFP) a través de TCP	-
554	TCP/UDP	Protocolo de secuencias en tiempo real (RTSP)	2326
587	TCP	Envío de mensajes para Mail (SMTP autenticado)	4409
600-1023	TCP/UDP	Servicios basados en RPC de Mac OS X	-
623	UDP	Lights-Out-Monitoring (LOM)	-
625	TCP	Directory Service Proxy (DSProxy) (Uso no registrado)	-
626	TCP	AppleShare Imap Admin (ASIA)	-
626	UDP	serialnumberd (Uso no registrado)	-
631	TCP	Protocolo de impresión de Internet (IPP)	2910
636	TCP	LDAP seguro	-
660	TCP	MacOS Server Admin	-
687	TCP	Agregar Server Admin a usos	-
749	TCP/UDP	Kerberos 5 admin/changepw	-
985	TCP	Puerto estático NetInfo	-
993	TCP	Mail IMAP SSL	-
995	TCP/UDP	Mail POP SSL	-
1085	TCP/UDP	WebObjects	-
1099 & 8043	TCP	RMI remoto y Acceso IIOP a JBOSS	-
1220	TCP	QT Server Admin	-
1649	TCP	IP Failover	-
1701	UDP	L2TP	-
1723	TCP	PPTP	-
2049	TCP/UDP	Sistema de archivos de red (NFS) (versión 3)	1094
2236	TCP	Macintosh Manager (Uso no registrado)	-

Puerto	TCP o UDP	Nombre de protocolo o servicio	RFC
2336	TCP	Directorios de inicio portátiles	
3004	TCP	iSync	-
3031	TCP/UDP	Eventos de Apple Remote	-
3283	TCP/UDP	Asistente de red	-
3306	TCP	MySQL	-
3632	TCP	Compilador distribuido	-
3659	TCP/UDP	Autenticación simple y capa de seguridad (SASL)	-
3689	TCP	Protocolo de acceso de audio digital (DAAP)	-
4111	TCP	XGrid	-
4500	UDP	IKE NAT Traversal	-
49152-65535	TCP	Xsan	-
5003	TCP	FileMaker: transporte y enlace de nombres	-
5009	TCP	(Uso no registrado)	-
5060	UDP	Protocolo de iniciación de sesión (SIP)	3261
5100	TCP	-	-
5190	TCP/UDP	America Online (AOL)	-
5222	TCP	Jabber (Uso no registrado)	-
5223	TCP	Servidor iChat SSL/XMPP	-
5269	TCP	Comunicación servidor a servidor de iChat	-
5297	TCP	-	-
5298	TCP/UDP	-	-
5353	UDP	DNS de difusión múltiple (MDNS)	-
5354	TCP	Respondedor DNS de difusión múltiple	-
5432	TCP	Base de datos de ARD 2.0	-
5678	UDP	Servidor SNATMAP	-
5897-5898	UDP	(Uso no registrado)	-
5900	TCP	Computación en red virtual (VNC) (Uso no registrado)	-
5988	TCP	WBEM HTTP	-
6970-9999	UDP	-	-
7070	TCP	RTSP (Uso no registrado) Protocolo de configuración de router automático (ARCP - Uso registrado)	-
7070	UDP	RTSP alternativo	-
7777	TCP	Proxy de transferencia de archivos del servidor iChat	-
8005	TCP	Apagado remoto Tomcat	-
8080	TCP	Puerto alternativo para Apache	-
8170	TCP	HTTPS (servicio o sitio web)	-
8175	TCP	Pcast Tunnel	-

Puerto	TCP o UDP	Nombre de protocolo o servicio	RFC
8000-8999	TCP	-	-
8821	TCP	Almacenado (almacena servidor para comunicarse con el servidor)	-
8891	TCP	Idsd (transferencias de datos)	-
9006 & 8080 & 8443	-	Puertos HTTP y HTTPS para Tomcat Standalone y JBOSS (J2EE)	-
16080	TCP	-	-
16384-16403	UDP	Protocolo de transferencia en tiempo real (RTP), Protocolo de control en tiempo real (RTCP)	-
24000-24999	TCP	-	-
42000-42999	TCP	-	-
50003	-	Servicio de servidor de FileMaker	-
50006	-	Servicio de aplicación auxiliar de FileMaker	-

Los puertos tienen una memoria intermedia (buffer) situada entre los programas de aplicación y la red. De tal forma que las aplicaciones transmiten la información a los puertos. Aquí se va almacenando hasta que pueda enviarse por la red. Una vez que pueda transmitirse, la información irá llegando al puerto destino donde se irá guardando hasta que la aplicación esté preparada para recibirla.

Los dos protocolos principales de la capa de transporte son UDP y TCP. El primero ofrece una transferencia de mensajes no fiable y no orientada a conexión y el segundo, una transferencia fiable y orientada a conexión.

Para conocer los puertos que puede utilizar su equipo puede editar los archivos “services”, estos se encuentra en el caso de Linux en el directorio /etc, para el caso de Windows los encuentra en el directorio c:\windows\system32\drivers.

Protocolo UDP

El protocolo UDP (User Datagram Protocol, protocolo de datagrama de usuario) proporciona una comunicación muy sencilla entre las aplicaciones de dos computadores. Al igual que el protocolo IP, UDP es: No orientado a conexión. No se establece una conexión previa con el otro extremo para transmitir un mensaje UDP. Los mensajes se envían sin más y éstos pueden duplicarse o llegar desordenados al destino. También involucra que puedan perderse o que lleguen dañados por los que se considera un protocolo No fiable

UDP utiliza el protocolo IP para transportar sus mensajes. Como vemos, no añade ninguna mejora en la calidad de la transferencia; aunque sí incorpora los puertos origen y destino en su formato de mensaje. Las aplicaciones (y no el protocolo UDP) deberán programarse teniendo en cuenta que la información puede no llegar de forma correcta.

		Encabezado UDP	Área de datos UDP	
		↓	↓	
	Encabezado del datagrama	Área de datos del datagrama IP		
	↓		↓	
Encabezado de la trama	Área de datos de la trama			Final de la trama

Formato del mensaje UDP

0										10										20										30	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	3	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Puerto UDP origen															Puerto UDP destino																
Longitud mensaje UDP															Suma verificación UDP																
Datos																															
...																															

Puerto UDP de origen (16 bits, opcional). Número de puerto de la máquina origen.

Puerto UDP de destino (16 bits). Número de puerto de la máquina destino.

Longitud del mensaje UDP (16 bits). Especifica la longitud medida en bytes del mensaje UDP incluyendo la cabecera. La longitud mínima es de 8 bytes.

Suma de verificación UDP (16 bits, opcional). Suma de comprobación de errores del mensaje. Para su cálculo se utiliza una pseudo-cabecera que también incluye las direcciones IP origen y destino. Para conocer estos datos, el protocolo UDP debe interactuar con el protocolo IP.

Datos. Aquí viajan los datos que se envían las aplicaciones. Los mismos datos que envía la aplicación origen son recibidos por la aplicación destino después de atravesar toda la Red de redes.

Protocolo TCP

El protocolo TCP (Transmission Control Protocol, protocolo de control de transmisión) está basado en IP, es Orientado a conexión. Por lo que es necesario establecer una conexión previa entre las dos máquinas antes de poder transmitir algún dato. A través de esta conexión los datos llegarán siempre a la aplicación destino de forma ordenada y sin duplicados. Finalmente, es necesario cerrar la conexión.

Se considera Fiable ya que la información que envía el emisor llega de forma correcta al destino. De esta forma, las aplicaciones que lo utilicen no tienen que preocuparse de la integridad de la información: dan por hecho que todo lo que reciben es correcto.

El flujo de datos entre una aplicación y otra viajan por un circuito virtual. Sabemos que los datagramas IP pueden seguir rutas distintas, dependiendo del estado de los enrutadores intermedios, para llegar a un mismo sitio. Esto significa que los datagramas IP que transportan los mensajes siguen rutas diferentes aunque el protocolo TCP logró la ilusión de que existe un único circuito por el que viajan todos los bytes uno detrás de otro (algo así como una tubería entre el origen y el destino). Para que esta comunicación pueda ser posible es necesario abrir previamente una conexión. Esta conexión garantiza que los todos los datos lleguen correctamente de forma ordenada y sin duplicados. La unidad de datos del protocolo es el byte, de tal forma que la aplicación origen envía bytes y la aplicación destino recibe estos bytes. Sin embargo, cada byte no se envía inmediatamente después de ser generado por la aplicación, sino que se espera a que haya una cierta cantidad de bytes, se agrupan en un segmento y se envía el segmento completo. Para ello son necesarias unas memorias intermedias o buffers. Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Si el segmento es muy grande será necesario fragmentar el datagrama, con la consiguiente pérdida de rendimiento; y si es muy pequeño, se estarán enviando más cabeceras que datos. Por consiguiente, es importante elegir el mayor tamaño de segmento posible que no provoque fragmentación.

El protocolo TCP envía un flujo de información no estructurado. Esto significa que los datos no tienen ningún formato, son únicamente los bytes que una aplicación envía a otra. Ambas aplicaciones deberán ponerse de acuerdo para comprender la información que se están enviando.

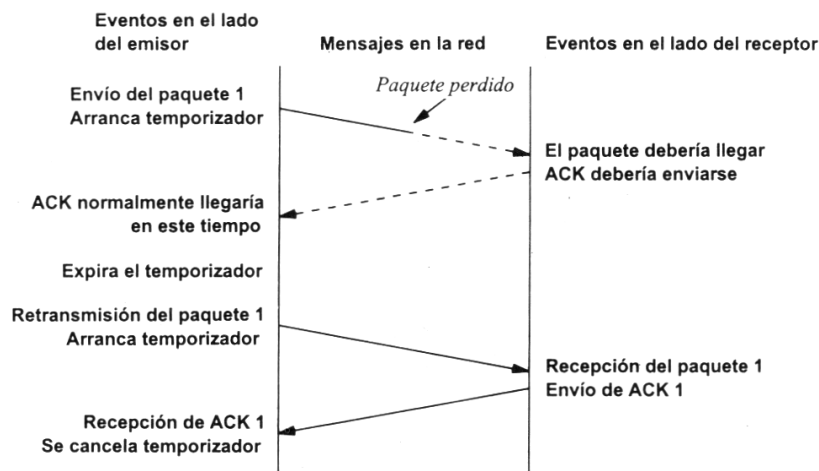
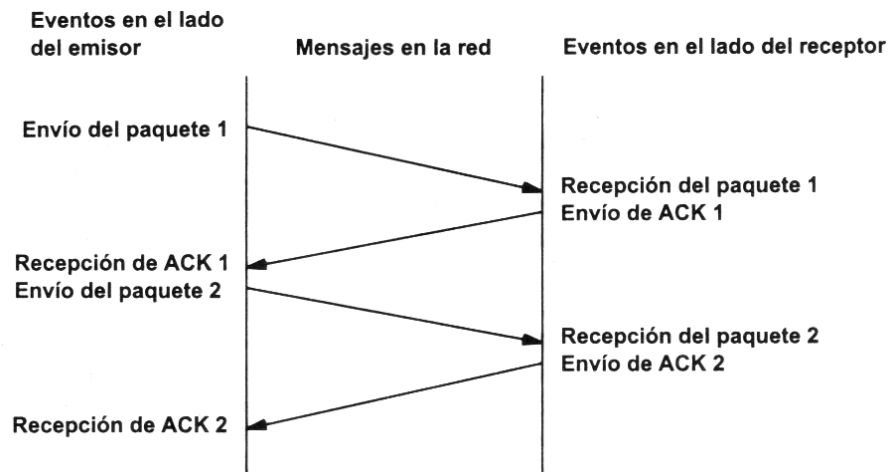
Cada vez que se abre una conexión, se crea un canal de comunicación bidireccional en el que ambas aplicaciones pueden enviar y recibir información, es decir, una conexión es full-dúplex.

Fiabilidad

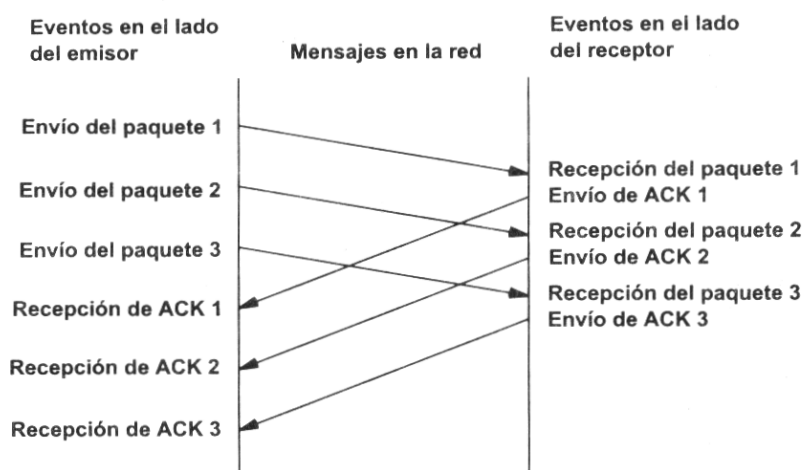
¿Cómo es posible enviar información fiable basándose en un protocolo no fiable? Es decir, si los datagramas que transportan los segmentos TCP se pueden perder, ¿cómo pueden llegar los datos de las aplicaciones de forma correcta al destino?

La respuesta a esta pregunta es sencilla: cada vez que llega un mensaje se devuelve una confirmación (acknowledgement) para que el emisor sepa que ha llegado correctamente. Si no le llega esta confirmación pasado un cierto tiempo, el emisor reenvía el mensaje.

Veamos a continuación la manera más sencilla (aunque ineficiente) de proporcionar una comunicación fiable. El emisor envía un dato, arranca su temporizador y espera su confirmación (ACK). Si recibe su ACK antes de agotar el temporizador, envía el siguiente dato. Si se agota el temporizador antes de recibir el ACK, reenvía el mensaje. Los siguientes esquemas representan este comportamiento:



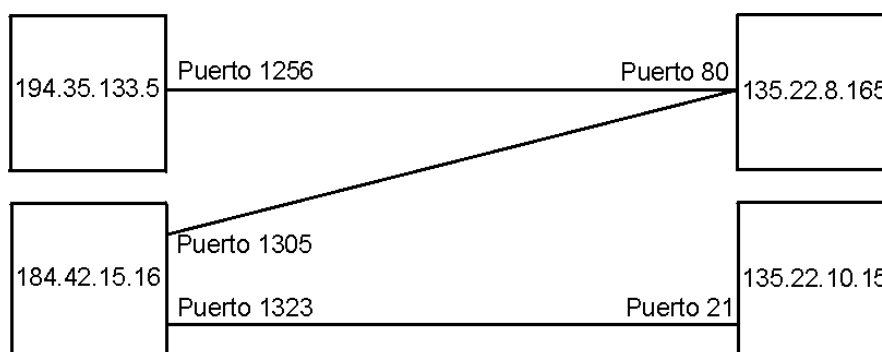
Este esquema es perfectamente válido aunque muy ineficiente debido a que sólo se utiliza un sentido de la comunicación a la vez y el canal está desaprovechado la mayor parte del tiempo. Para solucionar este problema se utiliza un protocolo de ventana deslizante, que se resume en el siguiente esquema. Los mensajes y las confirmaciones van numerados y el emisor puede enviar más de un mensaje antes de haber recibido todas las confirmaciones anteriores.



Conexiones

Una conexión son dos pares dirección IP y Puerto. No puede haber dos conexiones iguales en un mismo instante en toda la Red. Aunque bien es posible que un mismo computador tenga dos conexiones distintas y simultáneas utilizando un mismo puerto. El protocolo TCP utiliza el concepto de conexión para identificar las transmisiones. En el siguiente ejemplo se han creado tres conexiones. Las dos primeras son al mismo servidor Web (puerto 80) y la tercera a un servidor de FTP (puerto 21).

PC 1	PC 2
194.35.133.5:1256	135.22.8.165:80
184.42.15.16:1305	135.22.8.165:80
184.42.15.16:1323	135.22.10.15:21



Reservado (6 bits). Bits reservados para un posible uso futuro.

Bits de código o indicadores (6 bits). Los bits de código determinan el propósito y contenido del segmento. A continuación se explica el significado de cada uno de estos bits (mostrados de izquierda a derecha) si está a 1.

- URG. El campo Puntero de urgencia contiene información válida.
- ACK. El campo Número de acuse de recibo contiene información válida, es decir, el segmento actual lleva un ACK. Observemos que un mismo segmento puede transportar los datos de un sentido y las confirmaciones del otro sentido de la comunicación.
- PSH. La aplicación ha solicitado una operación push (enviar los datos existentes en la memoria temporal sin esperar a completar el segmento).
- RST. Interrupción de la conexión actual.
- SYN. Sincronización de los números de secuencia. Se utiliza al crear una conexión para indicar al otro extremo cual va a ser el primer número de secuencia con el que va a comenzar a transmitir (veremos que no tiene porqué ser el cero).
- FIN. Indica al otro extremo que la aplicación ya no tiene más datos para enviar. Se utiliza para solicitar el cierre de la conexión actual.

Ventana (16 bits). Número de bytes que el emisor del segmento está dispuesto a aceptar por parte del destino.

Suma de verificación (24 bits). Suma de comprobación de errores del segmento actual. Para su cálculo se utiliza una pseudo-cabecera que también incluye las direcciones IP origen y destino.

Puntero de urgencia (8 bits). Se utiliza cuando se están enviando datos urgentes que tienen preferencia sobre todos los demás e indica el siguiente byte del campo Datos que sigue a los datos urgentes. Esto le permite al destino identificar donde terminan los datos urgentes. Nótese que un mismo segmento puede contener tanto datos urgentes (al principio) como normales (después de los urgentes).

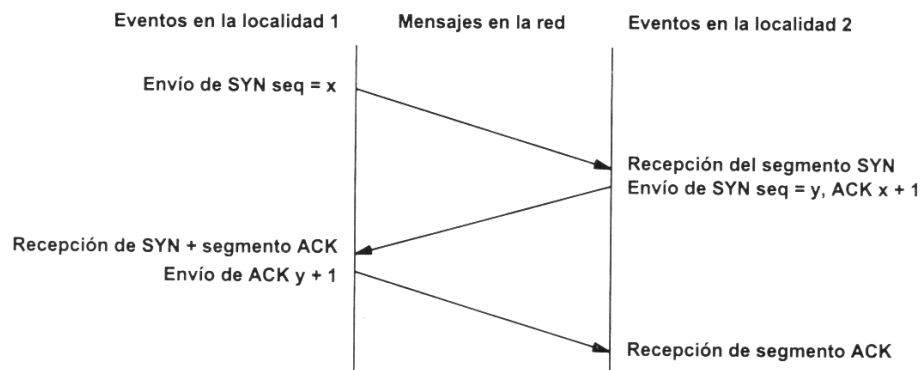
Opciones (variable). Si está presente únicamente se define una opción: el tamaño máximo de segmento que será aceptado.

Relleno. Se utiliza para que la longitud de la cabecera sea múltiplo de 32 bits.

Datos. Información que envía la aplicación.

Establecimiento de una conexión

Antes de transmitir cualquier información utilizando el protocolo TCP es necesario abrir una conexión. Un extremo hace una apertura pasiva y el otro, una apertura activa. El mecanismo utilizado para establecer una conexión consta de tres vías.



La máquina que quiere iniciar la conexión hace una apertura activa enviando al otro extremo un mensaje que tenga el bit SYN activado. Le informa además del primer número de secuencia que utilizará para enviar sus mensajes.

La máquina receptora (un servidor generalmente) recibe el segmento con el bit SYN activado y devuelve la correspondiente confirmación. Si desea abrir la conexión, activa el bit SYN del segmento e informa de su primer número de secuencia. Deja abierta la conexión por su extremo.

La primera máquina recibe el segmento y envía su confirmación. A partir de este momento puede enviar datos al otro extremo. Abre la conexión por su extremo.

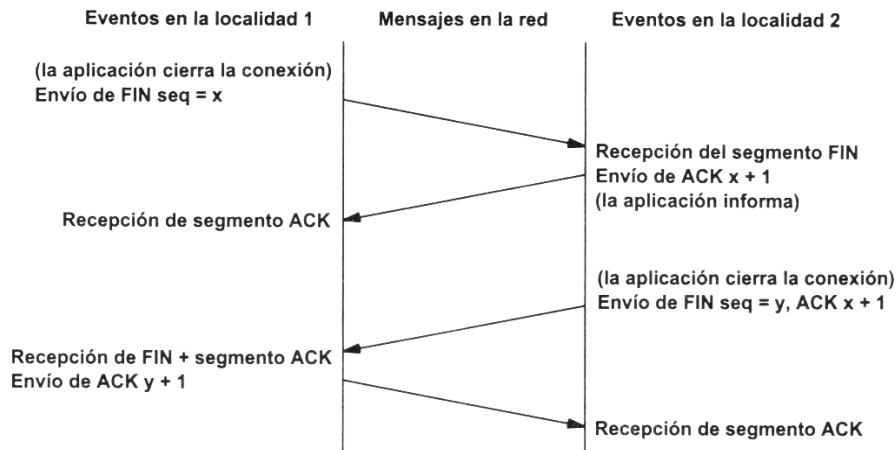
La máquina receptora recibe la confirmación y entiende que el otro extremo ha abierto ya su conexión. A partir de este momento puede enviar ella también datos. La conexión ha quedado abierta en los dos sentidos.

Observamos que son necesarios 3 segmentos para que ambas máquinas abran sus conexiones y sepan que la otra también está preparada.

Números de secuencia - Se utilizan números de secuencia distintos para cada sentido de la comunicación. Como hemos visto el primer número para cada sentido se acuerda al establecer la comunicación. Cada extremo se inventa un número aleatorio y envía éste como inicio de secuencia. Observamos que los números de secuencia no comienzan entonces en el cero. ¿Por qué se procede así? Uno de los motivos es para evitar conflictos: supongamos que la conexión en un computador se interrumpe nada más empezar y se crea una nueva. Si ambas han empezado en el cero es posible que el receptor entienda que la segunda conexión es una continuación de la primera (si utilizan los mismos puertos).

Cierre de una conexión

Cuando una aplicación ya no tiene más datos que transferir, el procedimiento normal es cerrar la conexión utilizando una variación del mecanismo de 3 vías explicado anteriormente.



El mecanismo de cierre es algo más complicado que el de establecimiento de conexión debido a que las conexiones son full-duplex y es necesario cerrar cada uno de los dos sentidos de forma independiente.

La máquina que ya no tiene más datos que transferir, envía un segmento con el bit FIN activado y cierra el sentido de envío. Sin embargo, el sentido de recepción de la conexión sigue todavía abierto.

La máquina receptora recibe el segmento con el bit FIN activado y devuelve la correspondiente confirmación. Pero no cierra inmediatamente el otro sentido de la conexión sino que informa a la aplicación de la petición de cierre. Aquí se produce un lapso de tiempo hasta que la aplicación decide cerrar el otro sentido de la conexión.

La primera máquina recibe el segmento ACK.

Cuando la máquina receptora toma la decisión de cerrar el otro sentido de la comunicación, envía un segmento con el bit FIN activado y cierra la conexión.

La primera máquina recibe el segmento FIN y envía el correspondiente ACK. Observemos que aunque haya cerrado su sentido de la conexión sigue devolviendo las confirmaciones.

La máquina receptora recibe el segmento ACK.

IPv6 (Protocolo de Internet versión 6)

Surge ante la necesidad de crear un protocolo para la nueva generación de Internet que brinde solución o mejora a los problemas que IPv4 (Protocolo utilizado actualmente) posee y que no fueron tomados en cuenta en el momento de su creación a principios de los años 70. (Escasez de direcciones, ineficiente ruteo y falta de seguridad).

Uno de los grandes inconvenientes de la implementación de IPv6, consiste en la transición de redes soportadas en IPv4 a redes que soporten IPv6. Tunneling o túneles surge como mecanismo básico de transición al IPv6 con la menor interrupción posible. La idea básica de tunneling consiste en encapsular paquetes IPv6 dentro de headers IPv4 siendo transportados a través de infraestructura de ruteo IPv4. Una vez implementadas redes IPv6 se debe instalar y configurar servicios de red como DHCPv6, DNSv6 y HTTPv6.

Motivos de Ipv6

El motivo básico por el que surge, en el seno del IETF (Internet Engineering Task Force), es la necesidad de crear un nuevo protocolo, ante la falta de direcciones. Ipv4 tiene un espacio de direcciones de 32 bits, es decir, 2³² (4.294.967.296); en cambio, Ipv6 nos ofrece un espacio de 2¹²⁸:

(340.282.366.920.938.463.463.374.607.431.768.211.456).

Sin embargo, Ipv4 tiene otros problemas o dificultades que Ipv6 solucione o mejore. Los creadores de Ipv4, a principio de los años 70, no predijeron en ningún momento, el gran éxito que este protocolo iba a tener en muy poco tiempo, en una gran multitud de campos, no solo científicos y de educación, sino también en innumerables facetas de la vida cotidiana. Ipv4 presenta varios problemas:

- Escaso direccionamiento, junto al hecho de una importante falta de coordinación, durante la década de los 80, en la delegación de direcciones, sin ningún tipo de optimización, dejando incluso grandes espacios discontinuos.
- Gran dimensión de las tablas de enrutamiento en el troncal de Internet, que la hace ineficiente, y perjudica enormemente los tiempos de respuesta.
- Imposibilidad práctica de muchas aplicaciones que quedan relegadas a su uso en intranet ya que muchos protocolos no soportan atravesar dispositivos NAT
- (solución temporal a la escasez de direcciones IP).
- No es escalable.

El crecimiento de Internet esperado en los próximos años es enorme, aparte del aumento de internautas a nivel mundial, tenemos el imparable crecimiento de aplicaciones que necesitan direcciones IP publicas únicas, globales, validas para conexiones extremo a extremo, y por tanto Enrutadores, Videoconferencia, Voz sobre IP, seguridad, e incluso juegos. También dispositivos de la red y los innumerables dispositivos que se van creando, o los ya existentes que se le dan nuevas o mejoradas aplicaciones, mediante su conexión a la red.

Algunos ejemplos:

- Teléfonos IP
- Radio y Televisión basados en tecnologías IP.
- Sistemas de seguridad, tele vigilancia y control.
- Refrigeradores que evalúan nuestros hábitos de consumo y nos permiten incluso navegar por un supermercado virtual y llenar nuestro carro según nuestras necesidades.
- Despertadores que conocen nuestros tiempos de desplazamiento habituales y nos pueden informar del estado del tiempo, trafico etc... mediante servicios de la red.
- Nuevas tecnologías emergentes, como Bluetooth, WAP, redes inalámbricas, redes domesticas, etc... hacen más patente esta necesidad de crecimiento, al menos, en los que al número de direcciones se refiere.
- En general, casi cualquier dispositivo tanto doméstico como industrial, integrado en la gran red, pero también dispositivos de control médico, marcapasos, etc.

Características principales de Ipv6:

- Mayor espacio de direcciones.
- “Plug and Play”: autoconfiguración.
- Seguridad intrínseca en el núcleo del protocolo (IPsec).
- Calidad de servicio (QoS) y clase de servicio (CoS).
- Multicast: envío de un mismo paquete a un grupo de receptores.
- Anycast: envío de un paquete a un receptor dentro de un grupo.
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los Router alineados a 64 bits.
- Posibilidad de paquetes con carga útil de más de 65.535 bytes.
- Enrutado más eficiente en el troncal de la red debido a una jerarquía de direccionamiento basada en la agregación.
- Características de movilidad.
- Escalabilidad.

Especificaciones básicas de Ipv6

Datagrama



La longitud de esta cabecera es de 32 bytes, el doble que en el caso de Ipv4, pero con muchas ventajas, al haberse eliminado campos redundantes. Además, la longitud fija de la cabecera, implica una mayor facilidad para su procesado en routers y conmutadores, incluso mediante hardware, lo que implica unas mayores prestaciones. Los campos están alineados a 64 bits, lo que permite que las nuevas generaciones de procesadores y microcontroladores, de 64 bits, puedan procesar mucho más eficazmente la cabecera Ipv6.

La MTU (Unidad Máxima de Transmisión), debe ser como mínimo, de 1.280 bytes, aunque se recomiendan tamaños mayores a 1.500 bytes. Los nodos descubren el valor MTU a través de la inspección de la ruta. Se prevé así una optimización de los paquetes y del número de cabeceras, dado el continuo crecimiento de los anchos de banda disponibles, así como del incremento del propio tráfico.

Dado que Ipv6 no realiza verificación de errores de la cabecera, en tráfico UDP, se requiere el empleo de su propio mecanismo de checksum⁴.

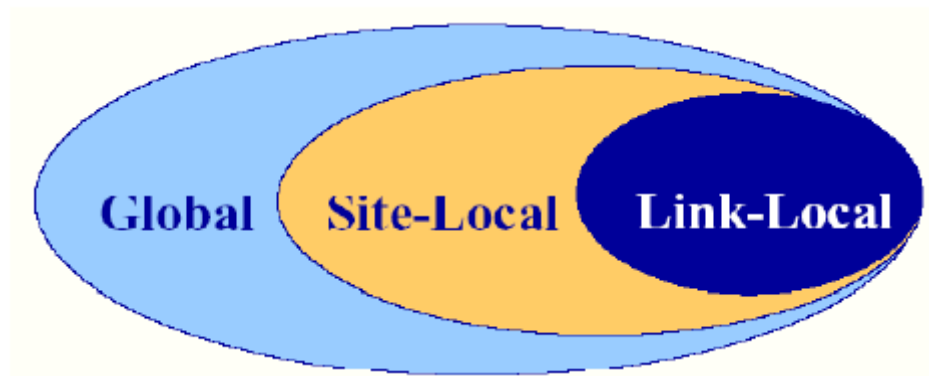
4 RFC 2460, Internet Protocol Version 6(IPv6) Specification (Disponible en Internet www.ietf.org/rfc/rfc2460.txt)

Direcciones IPv6

Las direcciones IPv6 son identificadores de 128 bits que se asignan a interfaces lógicas, una interfaz puede tener muchas direcciones. Las direcciones tienen ámbitos de acción local link, site local y global.

La representación de las direcciones Ipv6 se realiza mediante 8 grupos de 16 bits en valor hexadecimal separados por ":" ejemplo:

FEDC:BA98:76FA:3210:BA14:417A:FECD



Estas direcciones se clasifican en 3 tipos⁵:

Unicast: Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado solo a la interfaz identificada con dicha dirección. (es el equivalente a las actuales direcciones Ipv4). Puede ser usada en un ámbito global como dirección pública de Internet y también como dirección local en una red local, para esto se han definido dos tipos de direcciones unicast de uso local: local de enlace (Link Local) y local de sitio (Site Local).

Las direcciones locales de enlace han sido diseñadas para direccionar un único enlace para propósitos de auto configuración (mediante identificadores de interfaz), descubrimiento del vecindario, o situaciones en las que no hay routers. Por tanto, los enrutadores no pueden retransmitir ningún paquete con direcciones fuente o destino que sean locales de enlace (su ámbito está limitado a la red local). Sus primeros 10 bits [1111111010], seguido de 54 bits[0000...] y por último 64 bit del identificador de interfaz. Por tanto se trata de direcciones:

FE80::<ID de interfaz>/10.

⁵ The TCP/IP Guide A comprehensive, Illustrated Internet Protocols Reference, Capitulo 25 IPv6 addressing, Charles M. Kozierok, Octubre del 2005. (disponible en internetnostarch.com/download/tcpip_ch25.pdf)

Las direcciones locales de sitio permiten direccional dentro de un “sitio” local u organización, sin necesidad de un prefijo global. Se configuran mediante un identificador de subred, de 16 bits. Los enrutadores no deben de retransmitir fuera del sitio ningún paquete cuya dirección fuente o destino sea “local de sitio” (su ámbito esta limitado a la red local o de la organización). Sus primeros 10 bits [1111111011] seguidos de 38 bits[000...] seguidos de 16 bits [ID de subred] y por ultimo 64 bits del identificador de interfaz. Por tanto se trata de direcciones:
FEC0::<ID subred>:<ID de interfaz>/10.

Anycast: Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección anycast es entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la mas próxima, de acuerdo a las medidas de distancia del protocolo de enrutamiento).

Multicast: Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es hacer broadcast. Los primeros 8 bits [11111111], los siguientes 4 bits [000T], los siguientes 4 bits [ámbito] y por ultimo 112 bits [identificador de grupo]. El bit T significa, si su valor es 0, una dirección multicast permanente, asignada únicamente por la autoridad de numeración global de Internet. En caso contrario, si su valor es 1, significa que se trata de una dirección multicast temporal.

El “identificador de grupo” identifica el grupo concreto al que nos referimos dentro de un determinado ámbito. Los bits “ámbito” tienen los siguientes significados:

0	Reservado
1	Ambito Local de Nodo
2	Ambito Local de Enlace
3	No asignado
4	No asignado
5	Ambito Local de Sitio
6	No asignado
7	No asignado
8	Ambito Local de Organización
9	No asignado
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Ambito Global
F	Reservado

Direcciones especiales.

Ipv6 maneja ciertas direcciones especiales como:

- Dirección de loopback (::1).
- Dirección no especificada (::)
- Dirección túneles dinámicos/automáticos de Ipv6 sobre Ipv4 (::<dirección Ipv4>).

La representación de los prefijos Ipv6 se realiza así: dirección Ipv6/longitud del prefijo(valor decimal que indica cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo). Ejemplo: 12ab::cd30:0:0:0/60

Todos los nodos, en el proceso de identificación, al unirse a la red, deben de reconocer como mínimo, las siguientes direcciones:

- Direcciones locales de enlace para cada interfaz.
- Direcciones unicast asignadas.
- Dirección de loopback.
- Direcciones multicast de todos los nodos.
- Direcciones multicast solicitadas para cada dirección unicast o anycast asignadas.
- Direcciones multicast de todos los grupos a los que dicho host pertenece.
- En el caso de los routers también se tienen que reconocer:
- La dirección anycast del router de la subnet, para las interfaces en las que esta configurado para actuar como router.
- Todas las direcciones anycast con las que el router ha sido configurado.
- Las direcciones multicast de todos los routers.
- Las direcciones multicast de todos los grupos a los que el router pertenece.

Mecanismos de Transición⁶

Para coexistir con una infraestructura Ipv4 y proveer una eventual transición a una infraestructura Ipv6, son usados los siguientes mecanismos: Ipv4 e Ipv6 al tiempo y túneles Ipv6 sobre Ipv4.

IPv4 e IPv6 al tiempo

Durante el tiempo que una infraestructura de red hace su transición de IPv4, a IPv4/IPv6, y finalmente a una red IPv6 pura, los host deben tener la posibilidad de alcanzar sus destinos ya sea utilizando IPv4 o IPv6. Esto es gracias a que los host puedan soportar ambos protocolos IPv4 e IPv6.

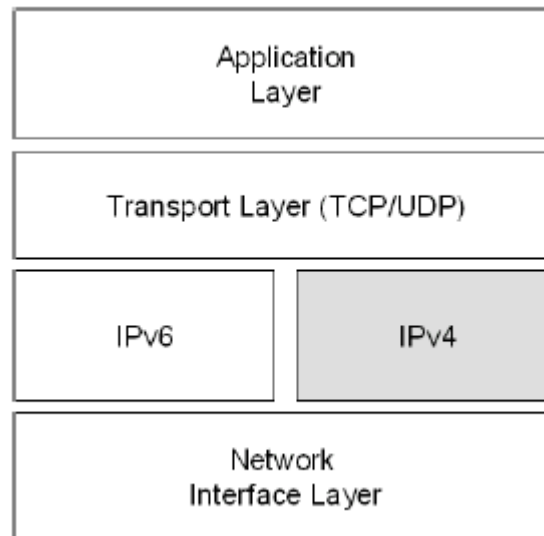
⁶ IPv6 Transition Technologies, Microsoft Corporation, enero del 2007 (disponible en internet www.microsoft.com/downloads)

Para que esto sea posible los host deben tener las siguientes arquitecturas:

- Arquitectura de doble capa IP
- Arquitectura de doble pila.

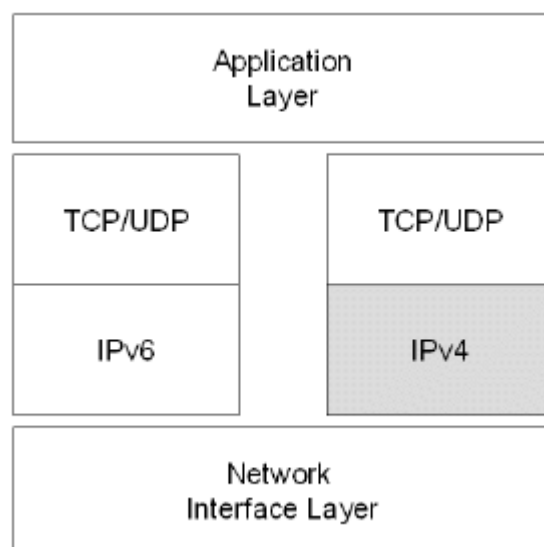
Arquitectura de doble capa IP

Una arquitectura de doble capa IP contiene ambos protocolos IPv4 e IPv6 con una única implementación de protocolos de la capa de transporte como TCP y UDP.



Arquitectura de doble pila.

Una arquitectura de doble pila contiene ambos protocolos IPv4 e IPv6 en pilas de protocolos separados que contiene implementaciones separadas de la capa de transporte como TCP y UDP.



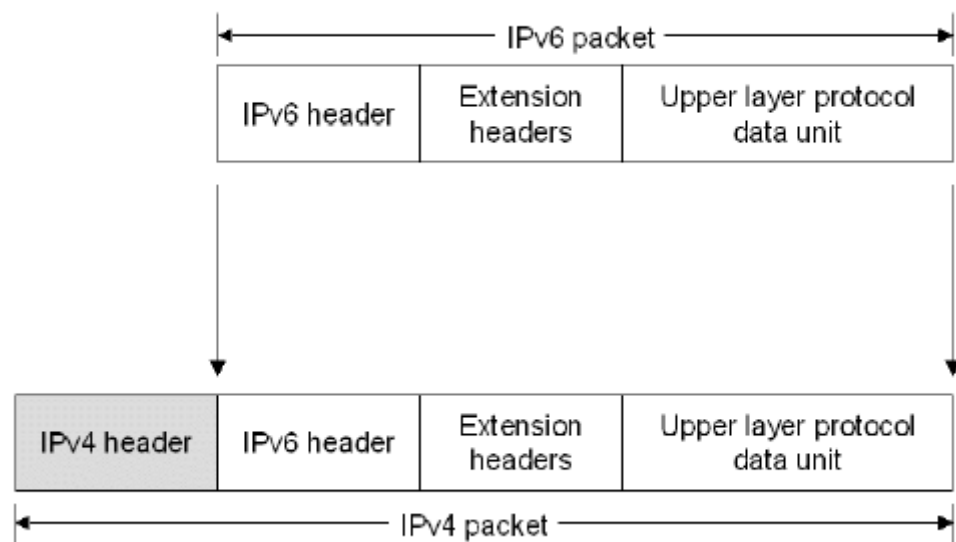
IPv6 sobre IPv4 Tunneling

IPv6 sobre IPv4 tunneling es la encapsulación de paquetes IPv6 en un encabezado IPv4, para permitir que los paquetes IPv6 puedan ser enviados a través de un paquete IPv4.

Características del paquete IPv4:

El campo del protocolo IPv4 se identificara con 41 para indicar que es encapsulado con un paquete IPv6.

Los campos fuente y destino contiene las direcciones IPv4 de los puntos finales del túnel. Los puntos finales del túnel pueden ser configurados como parte de la interface del túnel o se generan automáticamente de la dirección de siguiente salto que coincida con la ruta de destino y la interface del túnel.

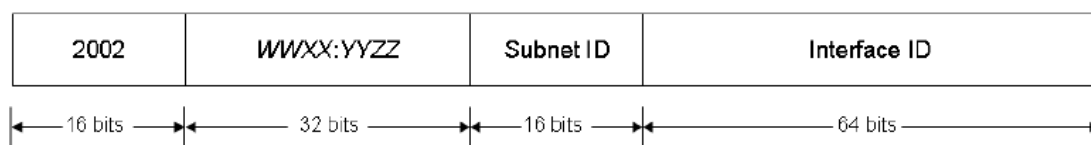


6to4 (RFC 3056)

6to4 es un asignador de direcciones y una tecnología automática de túneles (router-a-router, host-a-router, y router-a-host). Provee conectividad unicast entre sitios y hosts IPv6 a través de una red IPv4.

6to4 toma toda la red IPv4 como un solo enlace.

6to4 utiliza un prefijo global 2002:WWXX:YYZZ::/48, en el cual WWXX:YYZZ es la representación hexadecimal de la dirección IPv4 (w.x.y.z) asignada a el sitio o a el host.



Host 6to4: no requiere ninguna configuración manual, crea direcciones 6to4 usando un estándar de auto configuración de direcciones. Los hosts 6to4 no ejecutan túneles IPv6 sobre IPv4. Usa las siguientes rutas:

1. una ruta de enlace para el prefijo de la subred de la interfaz LAN. En nuestro ejemplo será 2002:9D3C:1:1::/64 .
2. una ruta por defecto que usa la interfaz LAN y tiene la dirección del siguiente salto de un router 6to4, esta ruta permite que los host 6to4 puedan ver otros host 6to4 u otros sitios en la red IPv6. en nuestro ejemplo sera ::/0.

Router 6to4: son enrutadores IPv6/IPv4 que usan una interface de túnel 6to4 para reenviar trafico de direcciones 6to4 entre hosts 6to4 dentro de un sitio y a otros enrutadores 6to4, estos enrutadores requieren una configuración adicional. Usa las siguientes rutas:

1. una ruta de enlace para el prefijo de la subred de la interfaz LAN. Esta ruta permite que el router 6to4 pueda enviar tráfico desde y hacia hosts 6to4 en la subred. En nuestro ejemplo será 2002:9D3C:1:1::/64 .
2. una ruta de enlace para el prefijo de la dirección 6to4 (2002::/16) que use la interface de túnel 6to4. esta ruta permite que el router 6to4 pueda crear un túnel router-a-router para alcanzar otros 6to4 routers.
3. una ruta que use la interfaz de túnel 6to4 y tenga el siguiente salto de dirección 6to4. esta ruta permite que el enrutador 6to4 envíe tráfico IPv6 a destinos IPv6 en la red IPv6. ::/0.⁷

⁷ RFC 3056, Connection of IPv6 Domains via IPv4 Clouds (disponible en Internet www.ietf.org/html/rfc2460)

ARP

El protocolo ARP es un protocolo estándar específico de las redes. Su status es electivo. El protocolo de resolución de direcciones es responsable de convertir las direcciones de protocolo de alto nivel(direcciones IP) a direcciones de red físicas. Consideremos algunos aspectos generales acerca de Ethernet.

ARP se emplea en redes IEEE 802 además de en las viejas redes DIX Ethernet para mapear direcciones IP a dirección hardware. Para hacer esto, ha de estar estrechamente relacionado con el manejador de dispositivo de red. De hecho, las especificaciones de ARP en RFC 826 sólo describen su funcionalidad, no su implementación, que depende en gran medida del manejador de dispositivo para el tipo de red correspondiente, que suele estar codificado en el microcódigo del adaptador.

Si una aplicación desea enviar datos a una determinada dirección IP de destino, el mecanismo de encaminamiento IP determina primero la dirección IP del siguiente salto del paquete (que puede ser el propio host de destino o un "router") y el dispositivo hardware al que se debería enviar. Si se trata de una red 802.3/4/5, deberá consultarse el módulo ARP para mapear el par <tipo de protocolo, dirección de destino> a una dirección física.

El módulo ARP intenta hallar la dirección en su caché. Si encuentra el par buscado, devuelve la correspondiente dirección física de 48 bits al llamador (el manejador de dispositivo). Si no lo encuentra, descarta el paquete (se asume que al ser un protocolo de alto nivel volverá a transmitirlo) y genera un broadcast de red para una solicitud ARP.

ARP y subredes

El protocolo ARP es el mismo aunque haya subredes. Recordar que cada datagrama IP pasa primero por el algoritmo de encaminamiento IP. Este algoritmo selecciona el manejador de dispositivo que debería enviar el paquete. Sólo entonces se consulta al módulo ARP asociado con ese manejador.

ARP se utiliza en 4 casos referentes a la comunicación entre 2 hosts:

- Cuando 2 hosts están en la misma red y uno quiere enviar un paquete a otro.
- Cuando 2 host están sobre redes diferentes y deben usar un gateway/router para alcanzar otro host.
- Cuando un router necesita enviar un paquete a un host a través de otro router.
- Cuando un router necesita enviar un paquete a un host de la misma red.

Tablas ARP

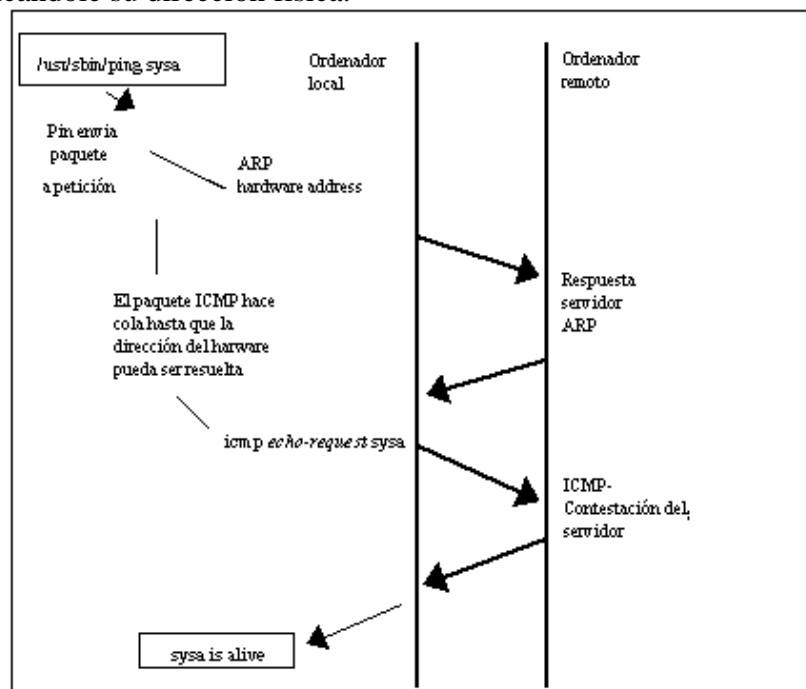
La filosofía es la misma que tendríamos para localizar al señor X entre 150 personas: preguntar por su nombre a todo el mundo, y el señor X nos responderá. Así, cuando a A le llegue un mensaje con dirección origen IP y no tenga esa dirección en su tabla ARP, enviará su frame ARP a la dirección broadcast (física), con la IP de la que quiere conocer su dirección física. Entonces, el equipo cuya dirección IP coincida con la preguntada, responderá a A enviándole su dirección física. En este momento A ya puede agregar la entrada de esa IP a su tabla ARP. Las entradas de la tabla se borran cada cierto tiempo, ya que las direcciones físicas de la red pueden cambiar (Ej: si se estropea una tarjeta de red y hay que sustituirla)

Funcionamiento I

Si A quiere enviar un frame a la dirección IP de B (misma red), mirará su tabla ARP para poner en la frame la dirección destino física correspondiente a la IP de B. De esta forma, cuando les llegue a todos el frame, no tendrán que deshacer el frame para comprobar si el mensaje es para ellos, sino que se hace con la dirección física.

Funcionamiento II

Si A quiere enviar un mensaje a C (un nodo que no este en la misma red), el mensaje deberá salir de la red. Así, A envía el frame a la dirección física del router de salida. Esta dirección física la obtendrá a partir de la IP del router, utilizando la tabla ARP. Si esta entrada no esta en la tabla, mandará un mensaje ARP a esa IP (llegará a todos), para que le conteste indicándole su dirección física.



Una vez en el router, éste consultará su tabla de encaminamiento, obteniendo el próximo nodo (salto) para llegar al destino, y saca el mensaje por el interfaz correspondiente. Esto se repite por todos los nodos, hasta llegar al último router, que es el que comparte el medio con el host destino. Aquí el proceso cambia: el interfaz del router tendrá que averiguar la dirección física de la IP destino que le ha llegado. Lo hace mirando su tabla ARP o preguntando a todos.

Comprobación de las tablas ARP

En ciertas ocasiones, es útil poder ver o alterar el contenido de las tablas ARP del núcleo, por ejemplo, cuando se sospecha que una dirección IP duplicada es la causa de algún problema intermitente en la red. La herramienta arp se hizo para situaciones como ésta. Sus opciones son:

- Arp [-v] [-t tipohw] -a [hostname]
- Arp [-v] [-t tipohw] -s [hostname] dirección hardware
- Arp [-v] -d máquina [hostname]

Todos los argumentos hostname pueden ser nombres simbólicos, o direcciones IP en notación de cuaterna.

El primer comando muestra el registro de la tabla correspondiente a la dirección IP o máquina especificada, o si no se pasa ninguna, se mostrarán todos los registros. Por ejemplo, al invocar arp en vlager obtendríamos:

```
C:\Users\usuario>arp -a

Interfaz: 192.168.1.135 --- 0xb
Dirección de Internet      Dirección física      Tipo
192.168.1.126              00-1b-77-9d-47-96    dinámico
192.168.1.254              00-1e-58-19-02-72    dinámico
192.168.1.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático

Interfaz: 192.168.117.1 --- 0x16
Dirección de Internet      Dirección física      Tipo
192.168.117.255            ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático

Interfaz: 192.168.92.1 --- 0x18
Dirección de Internet      Dirección física      Tipo
192.168.92.255             ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
```

Se puede limitar el listado a un tipo de hardware especificado usando la opción: -t. La opción -s se usa para añadir permanentemente la dirección

Ethernet de la máquina especificada a las tablas ARP. La dirección de hardware son seis bytes en hexadecimal separados por dos puntos o por guiones dependiendo del sistema operativo. Se puede incluso definir las direcciones de hardware para otros tipos de hardware, usando la opción: `-t`.

Por alguna razón, las peticiones ARP para máquinas remotas fallan algunas veces, por ejemplo cuando el controlador ARP no funciona, o cuando alguna otra máquina se identifica erróneamente como si ella misma tuviera esa dirección IP. Este problema requiere que se añada manualmente una dirección IP en la tabla ARP. También es una forma (muy drástica) de protegerse a sí mismo de otras máquinas de su Ethernet que tratan de hacerse pasar por otras.

El uso de `arp` con el modificador `-d` borra todas las entradas ARP referentes a la máquina dada. Este modificador puede ser usado para forzar a la interfaz a intentar obtener la dirección Ethernet correspondiente a la dirección IP en cuestión. Esto es útil cuando un sistema mal configurado ha emitido una información ARP errónea (por supuesto, se debe reconfigurar la máquina estropeada primero).

La opción `-s` también puede usarse para implementar un proxy ARP. Esta es una técnica especial, en la que una máquina, llamémosla gate, actúa como una pasarela a otra máquina llamada `fnord` simulando que las dos direcciones hacen referencia a la misma máquina, en este caso gate. Esto se consigue incluyendo una entrada ARP para `fnord` que apunte a su propia interfaz Ethernet. Cuando una máquina envíe una petición ARP para `fnord`, gate devolverá una respuesta con su propia dirección Ethernet. La máquina que hizo la petición enviará entonces todos los datagramas a gate, que se los pasará a `fnord`.

Estos tips pueden ser necesarios cuando usted quiera acceder a `fnord` desde una máquina DOS con una implementación errónea de TCP, que no entienda el enrutado demasiado bien. Cuando use proxy ARP, éste le aparecerá a la máquina DOS como si `fnord` estuviera en la subred local, así que no tiene que saber cómo enrutar a través de una pasarela.

Otra aplicación útil del proxy ARP es cuando una de las máquinas actúe como una pasarela para otra máquina sólo temporalmente, por ejemplo a través de un enlace telefónico.

Laboratorio Práctico

Recomiendo seguir este tutorial paso a paso para entender los términos aquí explicados

<http://seguridadyredes.nireblog.com/post/2009/11/05/wireshark-windump-analisis-capturas-traffic-red-interpretacion-datagrama-ip-actualizacion>

BIBLIOGRAFÍA

- TANENBAUM, Andrew S. Redes de Computadores: Prentice-Hall.
- STALLING, William. Comunicaciones y Redes de Computadores: Prentice-Hall.
- UYLESS, Black. Tecnologías Emergentes para Redes de Computadores. : Prentice Hall
- DERFLER. Frank, Descubre Redes LAN y WAN. Prentice Hall.
- HALSELL. Fred, Comunicaciones de Datos, Redes de Computadores y Sistemas Abiertos.: Addison Wesley
- GIBBS, Mark. Redes para Todos. : Prentice-Hall.
- SHELDON. Tom, Enciclopedia de Redes Serie LAN Times.: McGraw-Hill.
- LEE, Davies. Windows 2000 TCP/IP Protocolos y servicios. : McGraw-Hill.
- RODRÍGUEZ, Jorge E. Introducción a las redes de área local. : McGraw-Hill.
- TIM, Parker. Aprendiendo TCP/IP en 14 días. : Prentice Hall.

Internet:

www.cisco.com
www.3com.com
www.nortell.com
www.lucent.com
www.hispasec.com
www.cibercursos.net
www.red.com.mx
www.noticias.com
www.eltiempo.com
www.dragonjar.org

TABLA DE CONTENIDO

INTRODUCCIÓN.....	1
PROTOCOLOS TCP/IP.....	2
MODELO DE REFERENCIA OSI.....	2
MODELO DE REFERENCIA TCP/IP	2
<i>Protocolo de Internet (IP)</i>	3
Direcciones IP públicas.	4
Direcciones IP privadas (reservadas).	4
Direcciones IP estáticas (fijas).	4
Direcciones IP dinámicas.	4
Clases de Direcciones.....	5
Difusión (broadcast) y multidifusión (multicast).	7
Direcciones IP especiales y reservadas	7
Intranet.....	8
Extranet.....	8
Internet.....	8
Máscara de subred	8
Formato del datagrama IP	12
Protocolo ICMP.....	14
Puertos	17
Protocolo UDP.....	20
Protocolo TCP	22
<i>IPv6 (Protocolo de Internet versión 6)</i>	29
Motivos de Ipv6.....	29
Características principales de Ipv6:	30
Especificaciones básicas de Ipv6.....	31
Direcciones IPv6	32
Mecanismos de Transición	34
<i>ARP</i>	38
ARP y subredes	38
Tablas ARP.....	39
<i>Laboratorio Práctico</i>	41
BIBLIOGRAFÍA	42

Conociendo al Enemigo

EL ATACANTE INFORMÁTICO

Protocolos de Comunicación

Ambientes Operativos

DoS

Buffer Overflow

Exploits

Enumeración

CAPÍTULO 3

Rookits

AMBIENTES
OPERATIVOS

Virus

Criptografía

Metodologías y Estándares



Jhon César Arango Serna

www.itforensic-la.com

CAPÍTULO 3

AMBIENTES OPERATIVOS

LINUX/UNIX

Para entender la numerosa función de los ataques, usted debe tener una comprensión básica del sistema operativo LINUX, debido a su popularidad es una plataforma ideal para servidores y como un sistema operativo para lanzar ataques. Este capítulo presenta una apreciación global del sistema operativo de LINUX y describe conceptos subyacentes que se exigen entender los diversos ataques explicados a lo largo del libro.

UNIX es una bestia bonita pero extraña, introducido hace más de 30 años como un proyecto de investigación a AT&T, el sistema operativo de UNIX se usa ampliamente a lo largo del mundo en los servidores y sistemas de estación de trabajo.

Mucho del Internet se construyó con UNIX, en recientes años, el proyecto de código abierto de LINUX (como OpenBSD, GNU/Linux, y otros) ha ayudado a llevar LINUX al escritorio (desktop) e incluso a los dispositivos móviles, LINUX es muy poderoso. Son miles las personas que han trabajado en LINUX en vías de su desarrollo durante los últimos años, han perfeccionado rutinas y han creado numerosas herramientas.

Muchos sistemas LINUX tienen gran fiabilidad, alto rendimiento y rasgos de seguridad fuertes. Dado a los aportes de una comunidad global que utilizan este sistema como una herramienta de investigación. Gracias a Esto y a su relación íntima con el Internet, papel crítico del software libre y los movimientos de código abiertos, los administradores del sistema pueden encontrar una variedad de herramientas libremente disponible en Internet y pueden hacer preguntas a una comunidad grande y relativamente amistosa de LINUX a través de listas de correo grupos de noticias.

Pero LINUX es también una bestia extraña, por dos razones en particular. Primero: No hay un solo sistema operativo llamado LINUX. En cambio, LINUX es una familia de sistemas operativos puesta al día por muchos distribuidores que compiten entre ellos, cada uno con metas y visiones diferentes. Varias variantes populares de LINUX/UNIX incluyen:

- Solaris de Sun Microsystems.
- HP-UX (11iv3) by Hewlett Packard.
- IRIX de Sgi (Su nuevo nombre es Silicon Graphics).
- AIX de IBM.
- SCO, de Santa Cruz Operation.

- BSD de BSDi.
- FreeBSD una versión freeware de BSD.
- OpenBSD, otra versión gratis de BSD el cual se ha catalogado como el systema operativo más seguro.
- Linux, una fuente abierta de UNIX creada por Linux Torvalds, disponible para descarga libre y distribuida comercialmente por una variedad de vendedores en la que se incluye: Ubuntu, OpenSuse, Fedora, Centos, Mandriva, Debian, Linux Mint, Slackware, Gentoo y FreeBsd, entre otras.
- SunOS, el sistema operativo más viejo de Sun Microsystems.

ESCOGIENDO UNA DISTRIBUCIÓN DE LINUX¹



Un paso crucial a la hora de construir un servidor Linux seguro, está en la selección de la distribución que beneficiara las necesidades perfiladas en su política de seguridad.

Esta decisión determina el éxito de mantener un servidor de Linux seguro. Pero qué hace una distribución exactamente "Segura"? A continuación encontrará un juego de criterios que debe considerar antes de tomar esta decisión:

- ¿Tiene el distribuidor un mecanismo muy conocido para informar de las vulnerabilidades de seguridad encontradas en su distribución?
- ¿El distribuidor hace públicas las advertencias de seguridad que indica a los usuarios de vulnerabilidades encontrado en su distribución?
- ¿Qué tan a menudo resuelve los problemas de seguridad se resueltos encontrados?
- ¿El distribuidor posee un sitio especializado Web o FTP donde reside la información de seguridad (parches, actualizaciones de seguridad, etc.)?

¹ <http://tuvia.com/wp-content/uploads/2009/10/distros.jpg>

- ¿Qué tan a menudo el distribuidor arroja las versiones revisadas de la distribución en uso? Es probable que el horario en que se permiten las descargas sea tan lento que prolongue la exposición de vulnerabilidades conocidas.
- ¿Ofrece el distribuidor un método fácil de usar para instalar y poner al día paquetes del software?
- ¿El vendedor abre el código fuente de sus productos a la comunidad global para mejorar seguridad de Linux y/o las herramientas?
- ¿Desde cuando existe el Distribuidor?
- ¿Las versiones anteriores han sido bien soportadas y seguras?

Como con cualquier otra opción de software de Linux no hay ningún ganador, pero usted puede tomar la decisión más educada teniendo en cuenta las preguntas anteriores.

A continuación miraremos algunas distribuciones de Linux examinando un poco sus rasgos de seguridad.



Para muchos el nombre de Red Hat equivale a Linux, ya que Probablemente se trata de la compañía de linux más popular del mundo. Fundada en 1995 por Bob Young y Marc Ewing, red Hat Inc solo ha mostrado beneficios recientemente gracias a otros servicios en lugar de la distribución en sí. Aun y así, Red Hat es la primera elección para muchos profesionales y parece que seguirá siendo un peso pesado durante mucho tiempo. Ha podido consagrar recursos considerables al rastrear, diseminar y la resolver fallas de seguridad en los paquetes que distribuye. A la fecha se puede considerar como el vendedor de Linux más exitoso.

Los paquetes no son los más actuales, una vez se anuncia una nueva versión beta, las versiones de los paquetes se mantienen, excepto para actualizaciones de seguridad. Como resultado se obtiene una distribución bien probada y estable. El programa de betas y las facilidades para enviar fallos están abiertos al público y hay un gran espíritu en las listas de correo.

Su manejador de paquetes (RPM) permite la actualización constante sobre los programas donde se halla encontrado y resuelto problemas de seguridad. Esto se recomienda hacerlo una vez cada mes, siempre y cuando la actualización no sea crítica en cuyo caso debe hacerse inmediatamente. Todo esto con el fin de garantizar la seguridad de su sistema y el de estar corriendo siempre la versión reciente.

Actualmente Red Hat ha dividido el negocio en dos áreas distintas, por una parte promociona el proyecto Fedora para usuarios finales, el cual saca tres versiones al año, manteniendo los paquetes de Red Hat para usuarios corporativos, que se mantienen más tiempo, y garantizan su estabilidad.

Red Hat Linux se ha convertido en la distribución linux dominante en servidores en todo el mundo.. Otra de las razones del éxito de Red Hat es la gran variedad de servicios populares que ofrece la compañía. Los paquetes de software son fácilmente actualizables usando la Red Hat Network, un repositorio oficial de software e información. Una larga lista de servicios de soporte son accesibles en la compañía y, aunque no siempre baratos, tienes virtualmente asegurado un excelente soporte de personal altamente cualificado. La compañía ha desarrollado incluso un programa de certificación para popularizar su distribución, el RHCE (Certificado de Ingeniería de Red Hat), academias y centros examinadores están disponibles en el casi todas partes del mundo.



Debian GNU/Linux inició su andadura de la mano de Ian Murdock en 1993. Debian es un proyecto totalmente no-comercial; posiblemente el más puro de los ideales que iniciaron el movimiento del software libre. Cientos de desarrolladores voluntarios de alrededor del mundo contribuyen al proyecto, que es bien dirigido y estricto, asegurando la calidad de una distribución conocida como Debian. En cualquier momento del proceso de desarrollo existen tres ramas en el directorio principal: "estable", "en pruebas" e "inestable" (también conocida como "sid").

Cuando aparece una nueva versión de un paquete, se sitúa en la rama inestable para las primeras pruebas, si las pasa, el paquete se mueve a la rama de pruebas, donde se realiza un riguroso proceso de pruebas que dura muchos meses. Esta rama solo es declarada estable tras una muy intensa fase de pruebas.

Como resultado de esto, la distribución es posiblemente la más estable y confiable, aunque no la más actualizada. Mientras que la rama estable es perfecta para servidores con funciones críticas, muchos usuarios prefieren usar las ramas de pruebas o inestable, más actualizadas, en sus computadores personales. Debian es también famosa por su reputación de ser difícil de instalar, a menos que el usuario tenga un profundo conocimiento del hardware de la computadora. Compensando este fallo está "apt-get" un instalador de paquetes Debian.



SuSE es otra compañía orientada a los escritorios, aunque variedad de otros productos para empresas están disponibles. La distribución ha recibido buenas críticas por su instalador y la herramienta de configuración YaST, desarrollada por los desarrolladores de la propia SuSE. La documentación que viene con las versiones comerciales, ha sido repetidas veces evaluada como la más completa, útil y usable con diferencia a la de sus competidores. SuSE Linux 7.3 recibió el premio "Producto del año 2001" que entrega el Linux Journal. La distribución tiene un gran porcentaje de mercado en Europa y América del norte, pero no se vende en Asia y otras partes del mundo.

El desarrollo de SuSE se realiza completamente a puerta cerrada, y no se lanzan betas públicas para probar. Siguen la política de no permitir descargar el software hasta tiempo después de que salgan a la venta las versiones comerciales. A pesar de todo, SuSE no entrega imágenes ISO de fácil instalación de su distribución, usando el software empaquetado para la gran mayoría de su base de usuarios.

Novell ha comprado a esta compañía, y esta haciendo inversiones importantes en mantener y desarrollar esta distribución, a nivel corporativo, pero sin olvidarse del usuario final (Compra de Ximan, y la reciente liberación del instalador YaST bajo licencia GPL), y ha seguido la misma estrategia que Redhat, dejando SuSE para SOHO (Small Office, home, en español, pequeñas oficinas y usuarios domésticos), y creando una distribución para entornos empresariales (Novell Linux Desktop para escritorio, basada en gnome, y Novell Open Enterprise Server, para servidores).

ARQUITECTURA

SISTEMAS DE ARCHIVOS

Aunque los discos duros pueden ser muy chicos, aún así contienen millones de bits, y por lo tanto necesitan organizarse para poder ubicar la información. Éste es el propósito del sistema de archivos.

El sistema de archivos nativo de Linux es el EXT2. Ahora proliferan otros sistemas de archivos con journalising (si se arranca sin haber cerrado el sistema, no necesitan hacer un chequeo sino que recuperan automáticamente su último estado), los más conocidos son EXT3, EXT4, ReiserFS, Entre Otros

EXT2 (SECOND EXTENDED FILESYSTEM)

El sistema de ficheros EXT2 fue desarrollado originalmente por Remy Card quien es un programador y desarrollador de origen Francés el cual ha aportado mucha de su investigación al proyecto GNU/Linux. Particularmente Remy Card desarrolló el sistema de ficheros ext2 para los sistemas operativos RedHat, Fedora y Debian, Este sistema de ficheros tiene un tipo de tabla FAT de tamaño fijo, donde se almacenan los inodos.

Los inodos son una versión muy mejorada de FAT, donde un puntero inodo almacena información del archivo (ruta o path, tamaño, ubicación física). En cuanto a la ubicación, es una referencia a un sector del disco donde están todos y cada una de las referencias a los bloques del archivo fragmentado. Estos bloques son de tamaño especificable cuando se crea el sistema de archivos, desde los 512 bytes hasta los 4 kB, lo cual asegura un buen aprovechamiento del espacio libre con archivos pequeños. Los límites son un máximo de 2 TB de archivo, y de 4 TB de partición.

EXT3 (THIRD EXTENDED FILESYSTEM)

La principal diferencia de EXT2 con EXT3 es que EXT3 dispone de un registro por diario o mayormente conocido como “journaling”. Así mismo EXT3 puede ser montado y usado como un sistema de archivos EXT2. Otra diferencia importante es que EXT3 utiliza un árbol binario balanceado (árbol AVL) e incorpora el asignador de bloques de disco.

Aunque su velocidad y escalabilidad es menor que sus competidores, como JFS, ReiserFS o XFS, tiene la ventaja de permitir actualizar de EXT2 a EXT3 sin perder los datos almacenados ni formatear el disco y un menor consumo de CPU.

El sistema de archivo EXT3 agrega a EXT2 lo siguiente:

- Registro por diario.
- Índices en árbol para directorios que ocupan múltiples bloques.
- Crecimiento en línea.

EXT4 (FOURTH EXTENDED FILESYSTEM)

Ext4 es un sistema de archivos con bitácora (en inglés: Journaling) que fue concebida como una mejora compatible de ext3. Ext4 fue publicado como estable el 25 de diciembre de 2008 en la versión 2.6.28 del núcleo Linux y desde entonces se encuentra disponible para el uso en sistemas de producción.

El sistema de archivos ext4 es una notable mejora sobre ext3 mucho mas de la que fue ext3 sobre ext2. La mayor mejora del sistema de archivos ext3 sobre ext2 fue añadir el soporte de journaling (bitácoras). En cambio ext4 modifica importantes estructuras de datos del sistema de archivo tales como aquellas destinadas a almacenar los archivos de datos. El resultado es un sistema de archivos con un mejorado diseño, mejores características, rendimiento y confiabilidad.

Características principales

- Soporte de volúmenes de hasta 1 exabyte (260 bytes) y archivos con tamaño hasta 16 terabytes.
- Capacidad de reservar un área contigua para un archivo denominada "extents", la cual puede reducir y hasta eliminar completamente la fragmentación de archivos.
- Menor uso del CPU.
- Mejoras en la velocidad de lectura y escritura.

Actualmente, el ext4 es compatible con su anterior versión, el ext3, esto quiere decir que se puede montar como una partición ext3. También se pueden montar las particiones ext3 como ext4, aunque, si la partición ext4 usa extent (una de las mayores mejoras), la compatibilidad con la versión anterior, y por lo tanto, montar la partición como ext3, no es posible. La opción extent no es usada por defecto.

HPFS (HIGH PERFORMANCE FILE SYSTEM)

Fue creado específicamente para el sistema operativo OS/2 para mejorar las limitaciones del sistema de archivos FAT. Fue escrito por Gordon Letwin y otros empleados de Microsoft, y agregado a OS/2 versión 1.2, en esa época OS/2 era todavía un desarrollo conjunto entre Microsoft e IBM.

Se caracteriza por permitir nombres largos, metadatos e información de seguridad, así como de autocomprobación e información estructural. Otra de sus características es que, aunque poseía tabla de archivos como FAT, ésta se encontraba posicionada físicamente en el centro de la partición, de tal manera que redundaba en menores tiempos de acceso a la hora de leerla o

escribirla.

REISERFS

ReiserFS es un sistema de archivos de propósito general, diseñado e implementado por un equipo de la empresa Namesys, liderado por Hans Reiser. Actualmente es soportado por Linux y existen planes de futuro para incluirlo en otros sistemas operativos. También es soportado bajo windows de forma no oficial, aunque por el momento de manera inestable y rudimentaria. A partir de la versión 2.4.1 del núcleo de Linux, ReiserFS se convirtió en el primer sistema de ficheros con journal en ser incluido en el núcleo estándar. También es el sistema de archivos por defecto en varias distribuciones, como SuSE (excepto en openSuSE 10.2 que su formato por defecto es ext3), Xandros, Yoper, Linspire, Kurumin Linux, FTOSX, Libranet y Knoppix.

Con la excepción de actualizaciones de seguridad y parches críticos, Namesys ha cesado el desarrollo de ReiserFS (también llamado reiser3) para centrarse en Reiser4, el sucesor de este sistema de archivos.

ReiserFS ofrece funcionalidades que pocas veces se han visto en otros sistemas de archivos:

- Journaling. Esta es la mejora a la que se ha dado más publicidad, ya que previene el riesgo de corrupción del sistema de archivos.
- Reparticionamiento con el sistema de ficheros montado y desmontado. Podemos aumentar el tamaño del sistema de ficheros mientras lo tenemos montado y desmontado (online y offline). Para disminuirlo, únicamente se permite estando offline (desmontado). Namesys nos proporciona las herramientas para estas operaciones, e incluso, podemos usarlas bajo un gestor de volúmenes lógicos como LVM o EVMS.
- Tail packing, un esquema para reducir la fragmentación interna comparado con EXT2 y EXT3 en el uso de archivos menores de 4k, ReiserFS es normalmente más rápido en un factor de 10–15. Esto proporciona una elevada ganancia en las news, como por ejemplo Usenet, caches para servicios HTTP, agentes de correo y otras aplicaciones en las que el tiempo de acceso a ficheros pequeños debe ser lo más rápida posible.

Algunas de las desventajas de ReiserFS son:

- Los usuarios que usen como sistema de ficheros ext2, deben formatear sus discos, aunque no así los que usen ext3.
- ReiserFS en versiones del kernel anteriores a la 2.4.10 se considera inestable y no se recomienda su uso, especialmente en conjunción con NFS
- Algunas operaciones sobre archivos no son síncronas bajo ReiserFS, lo que pueden causar comportamientos extraños en aplicaciones fuertemente basadas en locks de archivos.
- No se conoce una forma de desfragmentar un sistema de archivos ReiserFS, aparte de un volcado completo y su restauración.
- Tempranas implementaciones de ReiserFS (anteriores a la incluida en el kernel 2.6.2), eran susceptibles de problemas de escrituras fuera de orden, lo que provocaba que archivos siendo escritos durante una caída del sistema, ganaran un pico de bytes extras de basura en el siguiente montado del sistema de archivos. La implementación actual de journaling, es correcta en este aspecto, manteniendo el journaling ordenado, del estilo de ext3.

ZFS (ZETTABYTE FILE SYSTEM)

Es un sistema de ficheros desarrollado por Sun Microsystems para su sistema operativo Solaris. El significado original era “Zettabyte File System”, pero ahora es un acrónimo recursivo.

El anuncio oficial de ZFS se produjo en septiembre del 2004. El código fuente del producto final se integró en la rama principal de desarrollo de Solaris el 31 de octubre del 2005 y fue lanzado el 16 de noviembre de 2005 como parte del build 27 de OpenSolaris.

ZFS fue diseñado e implementado por un equipo de Sun liderado por Jeff Bonwick. ZFS destaca por su gran capacidad, integración de los conceptos anteriormente separados de sistema de ficheros y administrador de volúmenes en un solo producto, nueva estructura sobre el disco, sistemas de archivos ligeros, y una administración de espacios de almacenamiento sencilla.

XFS

XFS es un sistema de archivos de 64 bits con journaling de alto rendimiento creado por SGI (antiguamente Silicon Graphics Inc.) para su implementación de UNIX llamada IRIX. En mayo del 2000, SGI liberó XFS bajo una licencia de código abierto.

XFS se incorporó a Linux a partir de la versión 2.4.25, cuando Marcelo Tosatti (responsable de la rama 2.4) lo consideró lo suficientemente estable para incorporarlo en la rama principal de desarrollo del kernel. Los programas de instalación de las distribuciones de SuSE, Gentoo, Mandriva, Slackware, Fedora Core, Ubuntu y Debian ofrecen XFS como un sistema de archivos más. En FreeBSD el soporte para solo lectura de XFS se añadió a partir de Diciembre de 2005 y en Junio de 2006 un soporte experimental de escritura fue incorporado a FreeBSD7.0CURRENT.

SWAP

La swap es un espacio reservado en tu disco duro para poder usarse como una extensión de memoria virtual de tu sistema. Es una técnica utilizada desde hace mucho tiempo, para hacer creer a los programas que existe más memoria RAM de la que en realidad existe. Es el propio sistema operativo el que se encarga de pasar datos a la swap cuando necesita más espacio libre en la RAM y viceversa.

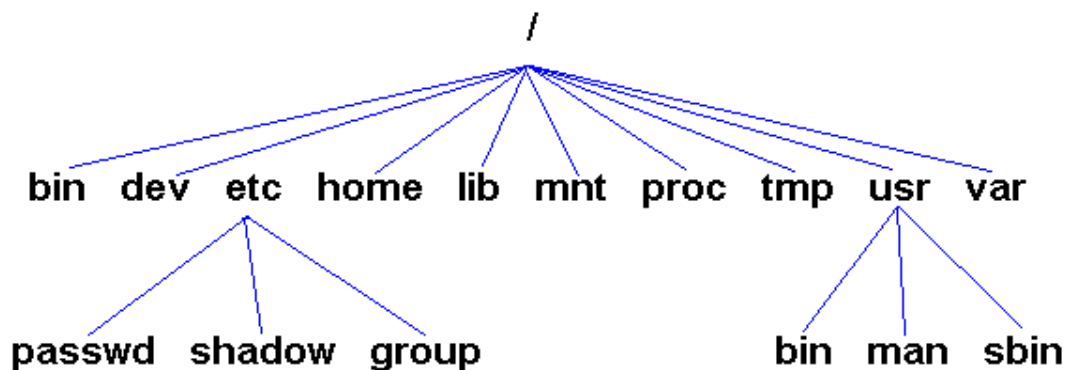
En Linux, la memoria total disponible por el sistema está formada por la cantidad de memoria RAM instalada + la swap disponible.

El acceso a la swap (disco duro) es más lento que el acceso a la memoria RAM, por lo que si nuestro ordenador está muy cargado de trabajo y hace un uso intensivo de la swap, la velocidad del sistema disminuirá. Un uso muy intensivo y continuado de la swap es un indicativo de que necesitamos más memoria en nuestro sistema para que funcione desahogado con el uso que le estamos dando.

En linux generalmente se usa como minimo una partición dedicada a swap (aunque también se puede tener un fichero swap).

ESTRUCTURA DEL SISTEMA DE ARCHIVOS

Todo alrededor de LINUX o de UNIX, se basa en la estructura del Sistema de Archivos (File System) ya que todos se trata como un archivo: Los procesos, los dispositivos y los archivos como tal. Explorar el sistema de archivos de LINUX es como viajar a través de una ciudad, con diversos directorios actuando como las calles para conducirlo a los edificios, que son archivos individuales. Aunque son muchas las versiones de LINUX/UNIX el siguiente esquema representa la estructura general de estas versiones:



El primer nivel es conocido como el directorio “Raíz” (Root), simplemente porque a partir de esta ubicación se encuentran el resto de los directorios que están bajo ella. El directorio raíz convenientemente es nombrado "/". (Se llega con el comando `cd /`). A partir de este directorio se visualizan otros directorios que contienen la información del sistema que incluye configuración del sistema, ejecutables del sistema, datos del usuario entre otros. La siguiente tabla muestra el significado de cada uno de estos directorios:

DIRECTORIO	PROPÓSITO
/	Es el directorio Raíz.
/bin y/o /sbin)	Contiene ejecutables críticos necesarios para el arranque del sistema.
/dev	Contiene todos los dispositivos del sistema (terminales, unidades de disco, modem, etc.)
/etc	Contiene los archivos de configuración del sistema, incluyendo grupos y usuarios.
/home	Aquí se localiza el directorio de los usuarios.
/lib	Aquí reside las librerías compartidas de los programas.
/mnt y/o /media	Es el punto donde se almacena temporalmente otro sistema de archivos exportado, como Usb, CD Rom, discos esclavos, Etc.
/proc	Imágenes de los procesos que actualmente se estan corriendo en el sistema.
/tmp	Archivos, temporales que son eliminados cada vez que se enciende el equipo.
/usr	Una variedad de archivos críticos, incluye: utilidades estándar del sistema (/usr/bin), manuales (/usr/man), encabezados de programas de C (/usr/include) y ejecutables de administración (/usr/sbin).

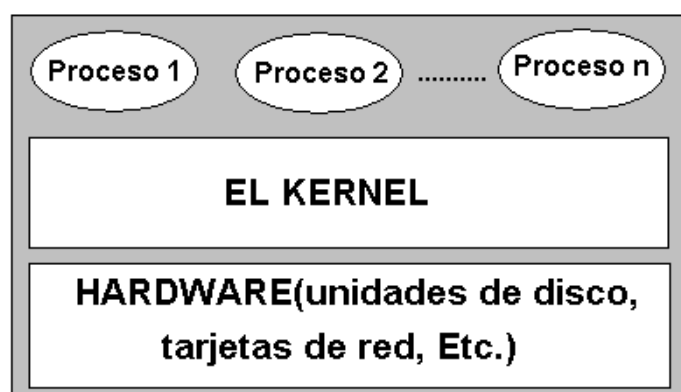
/var	Directorio donde se almacena los log's del sistema, para luego ser usados en cuestiones de administración. Incluye: registro de las acciones sobre el sistema, paginas web visitadas, correos enviados, entre otras.
------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

EL KERNEL Y LOS PROCESOS

Los sistemas de UNIX y/o LINUX tienden a tener una arquitectura modular, con un corazón central y varios programas alrededor de dicho corazón. En una máquina de UNIX/LINUX, el programa especial en el corazón del sistema se llama, “Kernel”. El Kernel es el corazón y cerebro del sistema y controla las funciones críticas del sistema, como las interacciones con el hardware y la administración de los recursos de los diferentes usuarios. Cuando un programa corre, necesita acceder a componentes de hardware como discos, cintas o interfaces de red, el Kernel proporciona las funciones necesarias para acceder a este hardware. Cuando un programa se ejecuta en un sistema UNIX/LINUX, el Kernel lanza un proceso para ejecutar dicho programa. Un proceso contiene el código ejecutable del programa que se esta corriendo y la memoria que le fue asociada. Programas de usuario, herramientas administrativas, y incluso algunos servicios (como servidores Web o servidores de Correo) son procesos en la máquina.

Un sistema UNIX/LINUX tiene a menudo centenares o incluso miles de procesos activos en cualquier momento dado. Sin embargo, en la unidad central de proceso (CPU) sólo un proceso puede correr en cualquier momento dado. El Kernel hace malabares en la CPU entre todos los procesos activos fijando cuando debe de correr cada uno para que el procesador del sistema pueda compartirse entre los procesos.

Adicionalmente, el kernel asigna cuidadosamente y maneja la memoria usada por los procesos. Cada proceso tiene su propio set de memoria limitada, y el Kernel impide a un proceso acceder a la memoria usada por otro proceso. Con esta capacidad de protección de memoria, un proceso renegado que intente leer o borrar la memoria de otro proceso será detenido por el kernel.



Muchos procesos en un sistema UNIX/LINUX corren sin que el usuario se de cuenta de su existencia, pero son procesos que manejan la información crítica del servidor, como un spool de paginas a ser enviadas a la impresora, la búsqueda efectiva de paginas Web, capacidades de asignación dinámica de direcciones de red. Éstos procesos, que prestan un servicio a los usuarios y que normalmente se inician automáticamente una vez de enciende el sistema son conocidos como demonios “daemons”. Se les da este nombre basados en la función que ellos realizan, se reconocen por tener una “d” al final del nombre el proceso. Por ejemplo, httpd es un demonio para el servidor Web que permite a los clientes visualizar paginas Web, demonios por el estilo están sshd, ftpd, xinitd, entre otros.

PONIENDO EN MARCHA PROCESOS AUTOMÁTICAMENTE

Todos los procesos que corren en un sistema de UNIX/LINUX, desde el poderoso servidor Web hasta el humilde generador de caracteres, tienen que ser activados por el kernel o algún otro proceso que active su funcionamiento. Durante el encendido del sistema, el Kernel activa un demonio llamado “init”, que es el padre de otros procesos que corren sobre la máquina.

El trabajo de “init” es terminar la carga completa del sistema, ejecutando una variedad de procesos que lo complementan. Dependiendo de las versiones de Unix o de Linux varia la ubicación de estos Scripts que se pueden encontrar en la siguiente ruta: /etc/init.d y /etc/rc.d .

el “init” también empieza una serie de procesos asociado a los servicios de red. Estos activan demonios los cuales escuchan sobre que puerto entra el trafico, y actúan recíprocamente con los usuarios. Algunos de los servicios de red más comunes iniciados por demonios a través del “init” incluyen:

Httpd:	Un servidor Web, manejando HTTP o demandas de HTTPS.
Sendmail:	Una aplicación común de UNIX/LINUX de un servidor de correo electrónico.
NFS:	Sistemas de Archivos de Red, originalmente creado por Sun Microsystems, usado para compartir archivos entre los sistemas UNIX.

Cuando el “init” empieza a trabajar conectado a una red, el proceso asociado con el servicio escucha al trafico de la red entrante. Por ejemplo, la mayoría los servidores de Web escuchan en el puerto TCP 80, mientras los servidores de correo electrónico escuchan por el puerto TCP 25.

Algunos servicios de red, como Web, correo y el compartir archivos, normalmente tienen mucho tráfico entrante, para lo cual necesitan estar constantemente listos para manipular la demanda que ello implica, este tipo de procesos son cobijados por el “init”.

Otros servicios, como Ftp, no son de acceso frecuente, solo esperan a ser solicitados por algún cliente de la red. Este tipo de procesos son llamados Demonios de Internet o initd, que tiene como fin esperar las solicitudes de servicios que son pedidos frecuentemente.

Dependiendo de las distribuciones de Linux, usted podrá encontrar un archivo de configuración llamado inetd.conf, el cual contiene todos los demonios de Internet que debe tener en cuenta en caso de una solicitud o puede encontrar un archivo llamado xinetd.conf el cual incluye un directorio llamado xinetd.d, donde se crea un archivo por cada servicio que se desee habilitar.

Inetd es activado por el demonio de init durante el encendido del sistema. Una vez activado, el inetd consulta su archivo de configuración, localizado en el directorio de /etc el cual es llamado inetd.conf o xinetd.conf. Este archivo de configuración dice al inetd que tráfico debe escuchar de acuerdo a ciertos servicios. Los puertos TCP y UDP para estos servicios son definidos en el archivo /etc/services el cual simplemente contiene un nombre de servicio, número del puerto, y indicación si un servicio es TCP (Orientado a Conexión) o UDP (No orientado a Conexión).

Cuando el tráfico llega a la máquina destino solicitando un servicio específico que esta identificado en /etc/inetd.conf o /etc/xinetd.conf, el inetd activa el programa asociado con el servicio. El proceso del servicio solicitado manipula el tráfico y se detiene una vez finaliza la solicitud. Inetd continúa esperando más tráfico para ese servicio y otros.

Se activan numerosos servicios normalmente usando inetd entre los cuales se incluyen:

Echo:	Un servicio para replicar los caracteres enviados por la red.
Chargen:	Un servicio que genera una lista repetida de caracteres.
Ftpd:	El demonio para la transferencia de archivos.

Para hacer que inetd escuche cierto servicio en particular, se debe especificar en el archivo de configuración /etc/inetd.conf o en el directorio de /etc/xinetd.d para el caso de /etc/xinetd.conf. A continuación se explica las características que debe tener estos servicios en los casos xinetd.conf ya que actualmente es el más utilizado:

Xinetd.conf

Este archivo en algunas distribuciones de Linux, reemplazo al inetd.conf y se caracteriza por su potencia en opciones y servicios. A diferencia de inetd.conf este archivo normalmente tiene un directorio asociado donde se crea un archivo por cada servicio que se desee habitar. El siguiente es un ejemplo de xinetd.conf (recuerde que las líneas que empiezan por #, no se toman en cuenta):

```
#
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

defaults
{
    instances                = 60
    log_type                  = SYSLOG authpriv
    log_on_success            = HOST PID
    log_on_failure            = HOST
    only_from                 = 128.138.193.0 128.138.204.0
    cps                       = 25 30
}

includedir /etc/xinetd.d

# fin de archivo
```

Note que la instrucción includedir hace un llamado al directorio /etc/xinetd.d que es donde residen los archivos que contiene los servicios a ser habilitados. Miremos el siguiente ejemplo, suponga que al listar el contenido de dicho directorio (ls) visualizara el nombre de 2 archivos: ftp y telnet; el contenido de cada archivo respectivamente podría ser:

```
# Archivo ftp
service ftp
{
    socket_type              = stream
    wait                     = no
    nice                     = 10
    user                     = root
    server                   = /usr/etc/in.ftpd
    server_args              = -l
    instances                = 4
    log_on_success            += DURATION HOST USERID
    access_times              = 2:00-9:00 12:00-24:00
}

# Archivo telnet
service telnet
{
    socket_type              = stream
```

wait	= no
nice	= 10
user	= root
server	= /usr/etc/in.telnetd
rlimit_as	= 8M
disabled	= no
}	

Sin importar si es inetd.conf o xinetd.conf, son varios los campos que describen la forma es que se comporta dicho servicio. A continuación se explicará los campos principales:

Id: Este atributo se usa para identificar un servicio. Es útil porque existen servicios que pueden usar protocolos diferentes y pueden necesitar parámetros diferentes en el archivo de configuración. Por defecto, el id del servicio es igual que el nombre de servicio, para xinetd el id del servicio es el mismo nombre de archivo ubicado en xinetd.d.

Socket_type: Los posibles valores para este atributo son:

stream	Servicios basados en Stream.
dgram	Servicios basados en datagramas.
Raw	Servicio que requiere acceso directo a IP.
seqpacket	Servicio que requiere transmisión secuencial del datagrama en forma segura.

Protocolo: Se determina el protocolo que es empleado por el servicio. El protocolo debe existir en /etc/protocols. Si este atributo no se define, el protocolo predefinido empleado por el servicio se usará.

Wait: Normalmente los servicios “dgram” necesitan este parámetro activo, mientras que los servicios “stream” no lo requieren, sin embargo hay algunas excepciones. Con este parámetro activo (wait o yes) inetd o xinetd espera a que el programa servidor libere el socket de red antes de empezar a escuchar más solicitudes de conexión en ese socket. Con el parámetro inactivo (nowait o no), inetd o xinetd continua escuchando más solicitudes de conexión tan pronto como ha lanzado el programa servidor.

User:	determina el usuario que ejecutara el proceso en el servidor. El nombre del usuario debe existir en /etc/passwd. Este atributo es de gran cuidado ya que muchos servicios se ejecutan como "root" o administrador.
Instances:	determina el número de servicios que pueden ser simultáneamente activos (el valor por defecto es ningún límite).
Nice:	Determina la prioridad del servicio.
Server_args:	Determina los argumentos pasados al servicio.
only_from:	Determina para quienes está disponible el servicio. Su valor es una lista de direcciones IP que pueden especificarse en cualquier combinación ya sea numerico de 4 octetos (172.28.17.0), en forma de factor (172.28.), nombre de una red definida en /etc/networks, un nombre de un host o una direccion Ip y su máscara en forma reducida (172.28.16.0/32).
Disable:	Este es un valor lógico que puede ser "yes" o "no". Uno de estos parámetros producirá que el servicio este o no disponible.
No_access:	Determina para quienes no está disponible el servicio. Su valor puede especificarse de la misma manera como el valor del atributo de only_from.
Access_time:	determina los intervalos de tiempo cuando el servicio estará disponible. Un intervalo tiene el formato: hora:minutos-hora:minuto . Horas pueden ir de 0 a 23 y minutos de 0 a 59.

Más allá del init y inetd, otra manera de empezar procesos automáticamente es a través del demonio del cron. Cron es un demonio que puede ejecutar procesos en un horario específico. Los administradores frecuentemente acostumbran mediante cron a fijar procesos automáticos regulares para aliviar el trabajo de administración del sistema.

Por ejemplo si usted desea ejecutar un programa que examina el sistema para escanear los archivos en busca de virus todas las noches a medianoche o a las 3:00 Am cada 2 días, esto lo podrá realizar a través de un cron. Cron lee uno o más archivos de configuración, conocidos como crontabs, para determinar qué ejecutará y cuándo. Estos archivos del crontab se almacenan dependiendo de las versiones de UNIX/LINUX normalmente en /usr/lib/crontab y /etc/crontab.

Así como administradores del sistema acostumbran a usar este demonio para facilitar su trabajo sin requerir de su presencia, los atacantes también emplean el cron para lograr su trabajo de explotar el sistema. Un atacante con acceso a una máquina de la víctima podría editar los archivos del crontab para correr varios comandos sobre la víctima. Comandos que pueden incluir la negación de un servicio el cierre de un programa en un momento crítico, una puerta trasera (backdoor) a cierta hora para garantizar el acceso remoto a la máquina, o cualquier otro tipo de ataque cronometrado contra el sistema.

A pesar de que init, inetd o cron son procesos que corren automáticamente sobre la máquina. También se pueden ejecutar o terminar de manera manual por usuarios y administradores. Siempre que usted ejecuta un programa en una máquina de UNIX/LINUX bajo la ventana de terminal a través de la línea de comando, un proceso empieza a trabajar el programa. Cuando un usuario ejecuta un programa, el proceso resultante corre normalmente con los permisos del usuario que activó el programa.

Un ejemplo se puede indicar con el servicio de Web server, que corre con el demonio httpd, si se deseara detener este servicio se ejecutaría el siguiente comando:

```
# /etc/init.d/httpd stop
```

Otra forma de ejecutar este comando seria

```
# service httpd stop
```

Para iniciarlo nuevamente, se teclea:

```
# /etc/init.d/httpd start
```

Otra forma de ejecutar este comando seria

```
# service httpd start
```

A parte de los demonios, los procesos aplican también a los comandos como ls, dir, who, finger, Etc. Cuando un usuario ejecuta un comando al mismo tiempo se está ejecutando un proceso, dicho comando se busca en una variedad de directorios que están pre-asignados dependiendo del usuario. La búsqueda se hace en el directorio propio del usuario "." y luego en el "camino de búsqueda" para ese usuario. El camino de búsqueda del usuario es una variable que contiene todos los directorios en que buscare por defecto, Para entender mejor esto teclee el siguiente comando:

```
$ echo $PATH
```

Usted podría obtener una respuesta como:

```
/usr/bin:/usr/local/bin:/usr/bin/X11:/usr/X11R6/bin:/home/jca/bin
```

Esto significa que cuando usted ejecute un comando, primero lo buscare en /usr/bin en caso tal de que no lo encuentre seguirá con /usr/local/bin, o si no /usr/bin/X11 o /usr/X11R6/bin y finalmente en /home/jca/bin.

Es muy peligroso tener el directorio actual, ".", en el camino de búsqueda. Para entender por qué, considera lo que pasa cuando usted teclea un orden normal, como ls para listar el contenido del directorio actual, pero usted tiene "." en su camino de búsqueda. Lo que significa que usted podrá crear un script con el nombre de "ls" bajo dicho directorio que ejecute algo diferente al comando original. Los atacantes les encanta ver "." En el camino de búsqueda ya que pueden depositar troyanos con los mismos nombres de comandos que saben que un usuario normalmente ejecutara y la verdad es que el programa engaña al usuario extrayéndole la contraseña, le niega un servicio, y así sucesivamente.

INTERACTUANDO CON LOS PROCESOS

El kernel asigna a cada proceso que corre sobre la máquina, una única identificación de de proceso llamado Id o Pid que es un número entero que hace referencia al proceso.

Los usuarios pueden correr el comando "ps" para desplegar una lista de los procesos que actualmente se ejecutan. La orden "ps" también puede usarse para mostrar los pids, nombres de programas, utilización de CPU, y otros aspectos de cada programa que se esté ejecutando.

A continuación veremos un ejemplo de los procesos que corren sobre una instalación típica de Linux, mostrada con el comando ps -aux:

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	1.7	0.0	1368	476	?	S	20:24	0:03	init
root	8	0.0	0.0	0	0	?	SW	20:24	0:00	[mdrecoveryd]
root	651	0.0	0.1	1428	560	?	S	20:25	0:00	syslogd -m 0
rpc	676	0.0	0.1	1512	552	?	S	20:25	0:00	portmap
rpcuser	704	0.0	0.1	1556	712	?	S	20:25	0:00	xinetd
root	832	0.0	0.0	1360	480	?	S	20:25	0:00	/usr/sbin/apmd -p
root	886	0.0	0.2	2620	1228	?	S	20:25	0:00	/usr/sbin/sshd
root	960	0.0	0.3	4600	1812	?	S	20:25	0:00	sendmail: accepti
root	997	0.0	0.1	1536	616	?	S	20:25	0:00	cron
xfs	1051	0.3	0.6	4856	3552	?	S	20:25	0:00	xfs -droppriv -da
root	1069	0.0	0.1	1380	552	?	S	20:25	0:00	anacron
daemon	1087	0.0	0.1	1404	524	?	S	20:25	0:00	/usr/sbin/atd
root	1096	0.0	0.0	1344	400	tty1	S	20:25	0:00	/sbin/mingetty tt
root	1097	0.0	0.0	1344	400	tty2	S	20:25	0:00	/sbin/mingetty tt
root	1289	0.0	0.6	7188	3184	?	S	20:26	0:00	magicdev --sm-cli
root	1291	2.0	2.2	28896	11532	?	S	20:26	0:01	nautilus start-he
root	1323	0.0	0.2	2508	1340	pts/0	S	20:26	0:00	bash
root	1459	0.0	0.1	2736	776	pts/0	R	20:27	0:00	ps -aux

Tenga en cuenta que en este ejemplo, se eliminaron algunas líneas para hacerlo más fácil leer. En la anterior lista usted puede ver los procesos init, crond, y xinetd corriendo en el sistema. Adicionalmente, se muestra el shell del usuario que ha ingresado en el sistema (un programa llamado bash) y como puede ver también se muestra el proceso que generó esta lista: ps.

Una manera de actuar recíprocamente con procesos es enviarles un signo (signal). Un signo es un mensaje especial que interrumpe un proceso. Uno de los signos más comunes es el "TÉRMIN" (Abreviación de Terminate) que indica al kernel para detener cierto proceso que se este ejecutando. Otro de los signos frecuentemente usados es el (HUP) que causará que muchos procesos (especialmente el inetd o xinetd) releen sus archivos de configuración. Un usuario puede ejecutar el comando "kill" para enviar un signo a un proceso específico refiriéndose al ID del proceso. Similarmente, el comando "killall" se usa para enviar un signo a un proceso refiriéndose a su nombre. Los comandos "kill" y "killall" no se usan necesariamente para matar, detener o terminar procesos. Por ejemplo, suponga que el Administrador del sistema o un atacante altera la configuración de xinetd, y crea o deshabilita un servicio en el directorio /etc/xinetd.d/. Para lograr que el sistema asuma los cambios, debe obligar a xinetd a releer sus archivos de configuración. Por tanto la persona interesada podría ejecutar la siguiente orden para terminar un proceso:

```
# kill -HUP 919
```

O, alternativamente, el administrador podría usar el comando "killall" para referirse al nombre del proceso. Note que la orden "killall" no mata todos los procesos. Apenas envía un signo a un proceso, con el nombre entrado por el usuario o administrador:

```
# killall -HUP xinetd
```

Ahora que tenemos una leve comprensión de procesos, pongamos nuestra atención a otros conceptos fundamentales de UNIX: cuentas y grupos.

CUENTAS Y GRUPOS

Debido a que Unix o Linux es un sistema multiusuario, para poder ingresar al sistema se requiere de una cuenta de usuario, teniendo en cuenta que cada proceso activo corre con los permisos de una cuenta dada. Igualmente cada cuenta pertenece a un grupo.

Por tanto para usted poder ingresar a un sistema, es obligación el poseer una cuenta.

Analicemos cómo están configuradas las cuentas en un sistema de UNIX/LINUX.

Los actuales sistemas Unix o Linux guardan información acerca de los usuarios en dos archivos, `/etc/passwd` y `/etc/shadow`; las versiones viejas solo era el archivo `/etc/passwd`. Estos archivos son usados por el programa “login” para validar los usuarios que ingresan al sistema y preparar el entorno de trabajo inicial.

Todos los usuarios de un sistema Unix o Linux pueden leer el archivo `/etc/passwd`, por que tiene permiso de lecturas para todo tipo de usuario. Sin embargo, solamente el usuario “root” (Administrador) puede leer el archivo `/etc/shadow`, que contiene las contraseñas cifradas.

El archivo `/etc/passwd`

Existe una línea en `/etc/passwd` por cada usuario y para ciertos nombres de presentación utilizados por el sistema. Cada una de estas líneas contiene una secuencia de campos, separados por dos puntos. El siguiente ejemplo muestra un archivo `/etc/passwd` de una instalación por defecto de sistema Linux:

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
mailnull:x:47:47:/:/var/spool/mqueue:/dev/null
rpm:x:37:37:/:/var/lib/rpm:/bin/bash
ntp:x:38:38:/:etc/ntp:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
gdm:x:42:42:/:/var/gdm:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/bin/false
ident:x:98:98:pident user:/:/sbin/nologin
radvd:x:75:75:radvd user:/:/bin/false
pcap:x:77:77:/:var/arpwatch:/sbin/nologin
jca:x:500:500:Jhon Cesar Arango:/home/jca:/bin/bash
```

El primer campo de una línea en el archivo `/etc/passwd` contiene el nombre de presentación del usuario.

El segundo campo contiene la letra x. (En las versiones anteriores este campo contenía una contraseña cifrada, de lo que se derivaba una

debilidad en la seguridad. La utilización de una x siempre proporciona un cierto grado de protección, pero sigue siendo una debilidad, ya que un intruso podría identificarla. En las Versiones recientes la contraseña cifrada está en /etc/shadow.).

Los campos tercero y cuarto son el ID de usuario e ID de grupo, respectivamente.

En el quinto campo se colocan comentarios. Generalmente este campo contiene el nombre del usuario y con frecuencia también contiene su número de despacho y el número de teléfono.

El sexto campo es el directorio propio, es decir, el valor inicial de la variable HOME.

El campo final designa al programa que el sistema ejecuta automáticamente cuando el usuario abre una sesión. Éste se denomina shell de presentación del usuario. El shell estándar, sh (bash), es el programa de inicio por defecto. Así, si el campo último está vacío, sh será el programa de inicio del usuario.

La información referente al nombre de presentación root está incluida en la primera línea del archivo /etc/passwd. El ID de usuario de root es 0, su directorio propio es el directorio raíz, representado por /, y el programa inicial que el sistema ejecuta para root es el shell estándar, sh, ya que el último campo está vacío.

Como se puede ver, en el ejemplo anterior, el archivo /etc/passwd contiene nombres de presentación usados por el sistema para su funcionamiento y para administración del sistema. Entre ellos se incluyen los siguientes ID de presentación: daemon, bin, adm, halt, Entre otros. También se incluyen nombres de presentación utilizados para la conexión en red, como uucp usado para la operación de la red de área local. El programa de inicio para cada uno de estos nombres de presentación puede encontrarse en el último campo de la línea asociada en el archivo /etc/passwd.

El archivo /etc/shadow

Existe una línea en /etc/shadow por cada línea del archivo /etc/passwd. El archivo /etc/shadow contiene información acerca de la contraseña de un usuario y datos referentes al envejecimiento de la contraseña. Por ejemplo, el archivo asociado al ejemplo anterior es el siguiente:

```

root:$1$ÓolB1ô1X$/Q171zopIt.yoqyAcF7jE/:11922:0:99999:7:::
bin:*:11922:0:99999:7:::
daemon:*:11922:0:99999:7:::
adm:*:11922:0:99999:7:::
lp:*:11922:0:99999:7:::
sync:*:11922:0:99999:7:::
shutdown:*:11922:0:99999:7:::
halt:*:11922:0:99999:7:::
mail:*:11922:0:99999:7:::
news:*:11922:0:99999:7:::
uucp:*:11922:0:99999:7:::
operator:*:11922:0:99999:7:::
games:*:11922:0:99999:7:::
gopher:*:11922:0:99999:7:::
ftp:*:11922:0:99999:7:::
nobody:*:11922:0:99999:7:::
vcsa:!!:11922:0:99999:7:::
mailnull:!!:11922:0:99999:7:::
rpm:!!:11922:0:99999:7:::
ntp:!!:11922:0:99999:7:::
rpc:!!:11922:0:99999:7:::
xfs:!!:11922:0:99999:7:::
gdm:!!:11922:0:99999:7:::
rpcuser:!!:11922:0:99999:7:::
nfsnobody:!!:11922:0:99999:7:::
nscd:!!:11922:0:99999:7:::
ident:!!:11922:0:99999:7:::
radvd:!!:11922:0:99999:7:::
pcap:!!:11922:0:99999:7:::
jca:$1$yâp6èÉPÛ$jXMnsdZ0iaIIiTezZDfQe0:11922:0:99999:7:::

```

El primer campo de la línea contiene el nombre de presentación. Para usuarios con contraseñas.

El segundo campo contiene la contraseña cifrada para ese nombre de presentación. Este campo puede tener NP (No Password) cuando no existe contraseña para ese nombre de presentación y * para los nombres de presentación propios del sistema. Ninguna de estas cadenas (NP, y *) pueden ser nunca la versión cifrada de una contraseña válida, por lo que es imposible presentarse con uno de estos nombres al sistema, ya que cualquier respuesta dada a la petición «Password:» dejará de producir una coincidencia con los contenidos de este campo. De este modo estos nombres de presentación están efectivamente bloqueados.

El tercer campo indica el número de días entre el 1 de enero de 1970 y el día en que la contraseña fue modificada la última vez.

El cuarto campo indica el número mínimo de días requerido entre cambios de la contraseña. Un usuario no puede cambiar su contraseña de nuevo hasta que transcurra ese número de días.

El quinto campo indica el número máximo de días que una contraseña es válida. Transcurrido ese número de días, el usuario se ve forzado a cambiar la contraseña.

El sexto campo indica el número de días antes de la expiración de una contraseña que el usuario es avisado. Se enviará un mensaje de aviso a un usuario cuando éste se presente para notificarle que su contraseña está a punto de expirar dentro de esos días.

El séptimo campo indica el número de días de inactividad permitido a este usuario. Si ese número de días transcurre sin que el usuario se presente, su línea de presentación se bloquea.

El octavo campo indica la fecha absoluta (especificada mediante el número de días desde el 1 de enero de 1970; por ejemplo, 9800 es el 3 de mayo de 1996) a partir de la cual el nombre de presentación ya no puede ser utilizado.

El noveno campo es una opción que actualmente no es utilizada, pero que puede serlo en el futuro.

En las versiones anteriores de Unix y de Linux, el archivo `/etc/passwd` contenía las contraseñas cifradas para los usuarios en el segundo campo de cada línea. Puesto que los usuarios ordinarios pueden leer este archivo, un usuario autorizado, o un intruso que hubiera tenido acceso a un nombre de presentación, podría también ganar acceso a otros nombres de login. Para hacer esto, el usuario, o el intruso, ejecuta un programa (como `john the ripper`²) para cifrar palabras desde un diccionario de palabras o cadenas comunes formadas a partir de nombres, utilizando el algoritmo del sistema UNIX/LINUX para cifrar contraseñas (que no se mantiene en secreto), y compara los resultados con las contraseñas cifradas en el sistema. Si encuentra una coincidencia, el intruso tiene acceso a los archivos de un usuario. Esta vulnerabilidad ha sido reducida colocando una `x` en el segundo campo del archivo `/etc/passwd` y usando el archivo `/etc/shadow`.

CONTROL DE PRIVILEGIOS

En Linux O Unix , el acceso de los usuarios a los distintos archivos y directorios se limita mediante la concesión de permisos. Hay tres tipos básicos de permisos:

- De lectura: permite a los usuarios leer el archivo especificado.
- De escritura: permite a los usuarios modificar el archivo especificado.
- De ejecución: permite a los usuarios ejecutar el archivo especificado.

Cuando se asignan estos permisos, Linux o Unix guarda un registro de los mismos que posteriormente aparece reflejado en las listas de archivos.

² Enlace de John the ripper

El estado de los permisos de cada uno de los archivos se expresa mediante marcas. Las marcas de permiso son:

- r : acceso de lectura.
- w : acceso de escritura.
- x : acceso de ejecución.

El comando “ls -l” o “dir -l” para linux, muestra el contenido de un directorio, esta lista puede contener directorios o archivos, observemos el ejemplo siguiente:

-rw-----	1	root	root	10200	oct	1	21:18	boot.log
-rw-----	1	root	root	960	oct	1	21:20	cron
drwxr-xr-x	2	lp	root	4096	sep	2	22:43	cups
-rw-r--r-x	1	root	root	6762	oct	1	21:16	dmesg
drwxr-xr-x	2	root	root	4096	feb	26	2002	fax
drwxr-xr-x	2	root	root	4096	ago	23	22:54	gdm
-rw-r--r--	1	root	root	59445	oct	1	21:16	ksyms.0
-rw-r--r--	1	root	root	59445	sep	15	19:55	ksyms.1
-rw-r--r--	1	root	root	59445	sep	2	22:39	ksyms.2
-rw-r--r--	1	root	root	19136220	oct	1	21:18	lastlog
-rw-----	1	root	root	554	oct	1	21:18	maillog
-rw-----	1	root	root	47573	oct	1	21:19	messages
-rw-r--r--	1	root	root	16539	sep	2	22:46	rpmpkgs
drwxr-xr-x	2	root	root	4096	oct	1	21:20	sa
-rw-----	1	root	root	450	oct	1	21:18	secure
-rw-----	1	root	root	0	sep	2	22:46	spooler
drwxr-xr-x	2	root	root	4096	abr	8	08:07	vbox
-rw-rw-r--	1	root	utmp	31104	oct	1	21:18	wtmp

Observe que la primera columna de la anterior lista contiene 10 campos, los cuales se muestran a continuación:



Existen tres clases de permisos para los archivos y directorios que se corresponden con las tres clases de usuario: el propietario (o usuario) del archivo o directorio, el grupo al que pertenece el propietario y los otros usuarios del sistema. El primer campo indica el tipo de archivo (si es un archivo, un directorio u otro), los tres siguientes campos hacen referencia a los permisos del propietario; las tres siguientes a los miembros del grupo del propietario y las tres últimas a los otros usuarios.

Note que en el ejemplo anterior, la salida correspondiente al denominado “dmesg”, indica: El primer campo indica que es un archivo, los tres siguientes rw-, muestran que el propietario del archivo puede leerlo (r) y

escribirlo (w). El segundo grupo de tres caracteres, r--, indican que los miembros del grupo pueden leer el archivo, pero no pueden escribirlo, ni ejecutarlo. Los tres últimos caracteres, r-x, muestran que todos los demás pueden leer y ejecutar el archivo, pero no escribirlo.

El sistema octal

En el sistema octal, los números representan permisos. La siguiente tabla, resume el esquema octal y lo que representa cada número.

r	w	x	Equivalente Octal
0	0	0	0
0	0	1	1
0	1	0	2
0	1	1	3
1	0	0	4
1	0	1	5
1	1	0	6
1	1	1	7

Si se utilizan valores octales puros, hay que añadirlos juntos, lo que deriva un número final que expresa todos los permisos concedidos. Pero para facilitar las cosas, es posible reducir rápidamente los permisos del propietario, de los grupos y de otros usuarios a un número de tres dígitos utilizando estos valores:

- 0 = Sin permisos.
- 1 = Ejecución.
- 2 = Escritura.
- 3 = Escritura y ejecución (actualmente no se utiliza mucho).
- 4 = Lectura.
- 5 = Lectura y ejecución.
- 6 = Lectura y escritura.
- 7 = Todo el conjunto: lectura, escritura y ejecución.

Por ejemplo, suponga que quiere darle al archivo “dmesg” permisos de lectura y ejecución al usuario, lectura al grupo y ningún permiso a los demás. El comando “chmod” permite cambiar estos permisos y facilita su utilización si usted conoce el equivalente octal, así por ejemplo; si ejecutamos el comando:

```
# chmod 340 dmesg
```

Notará que los permisos del archivo, cambiaron al ejemplo anteriormente mencionado.

En seguridad este comando es bastante utilizado para colocar permisos a archivos que deseamos que ciertos usuarios ejecuten mas no que modifiquen, se podría asignar fácilmente a un archivo o directorio el permiso 751 que indica:

- El propietario puede leerlo, escribirlo y ejecutarlo (7).
- El grupo puede leerlo y ejecutarlo (5).
- El mundo (usuarios externos) sólo pueden ejecutarlo (1).

PROGRAMAS SUID Y SGID

Existen dos bits adicionales de permiso asociados a un archivo: los bits SUID y SGID. SUID representa el identificador del usuario y SGID representa el identificador del grupo. Cuando se ejecutan programas con permisos, éstos se comportan como si pertenecieran a identificadores de usuarios distintos. Cuando se ejecuta un programa SUID, su identificador de usuario efectivo es el mismo que el del usuario propietario del programa en el sistema de archivos, independientemente de quién esté ejecutando realmente el programa. SGID es similar, salvo que cambia el identificador de grupo.

Veamos el siguiente ejemplo, a veces usuarios o procesos tienen una razón legítima por acceder a un archivo que ellos no tienen permisos. Considere lo que pasa cuando un usuario desea cambiar su contraseña. El usuario tiene que entrar a modificar los archivos `etc/passwd` y `etc/shadow`.

Sin embargo, estos archivos solo son de propiedad del “root” y solo pueden ser modificados por él, entonces ¿Cómo puede cambiar un usuario normal su contraseña sin tener que importunar a los administradores del sistema cada vez que necesite temporalmente las propiedades del administrador?

La respuesta la da otra capacidad de los sistemas LINUX/UNIX llamado SetUID (“Set User ID”). Con esta capacidad, un programa particular puede configurarse para siempre se ejecute con los permisos de su dueño, y no con los permisos del usuario que lanzó el programa. Recuerde, normalmente cuando un usuario empieza un proceso, el proceso corre con los permisos del usuario.

Por tanto, en nuestro ejemplo anterior, el usuario correrá un programa de SetUID especial llamado “passwd” para cambiar una contraseña. El programa del passwd está configurado por defecto para ejecutarse como “root”. Es decir, sin tener en cuenta quién ejecuta este comando, corre con permisos del “root”. Lo que nos permite decir, que este tipo de programas convierten temporalmente a usuarios normales en administradores.

Así, si deseamos hacer que el comando “dmesg” lo pueda ejecutar cualquier usuario con las propiedades del dueño original se podría teclear:

```
# chmod 4741 dmesg
```

Aunque la función SUID/SGID puede ser de gran utilidad, también compromete la seguridad del sistema. Los programadores normalmente hacen todo lo posible por garantizar cierta seguridad en sus programas

SUID. Los problemas de seguridad de los programas surgen cuando el programa ejecuta una línea de comandos, la cual puede activar un shell o ejecutar un archivo que los usuarios pueden modificar para que contenga sus propios comandos.

A pesar de que algunos programas SUID son necesarios, es mejor reducirlos al mínimo. Esto se logra explorando regularmente los sistemas de archivos a través del comando find. (Ejecutar el comando “man find” para entender los parámetros del siguiente ejemplo)

```
# find / -user root -perm 4000 -print
```

RELACIÓN DE CONFIANZA EN MÁQUINAS LINUX/UNIX

Anteriormente las máquinas en Linux podrían ser configurados de forma de que un equipo confiara en otro. Estas relaciones de confianza se realizaban a través de las opciones de algo llamado los “Los Comandos R” y mediante el archivo “/etc/hosts.equiv”.

Los comandos R incluyen normalmente un grupo de comandos que se derivan de los sistemas BSD. Estos comandos son: “rlogin” para el inicio de sesión remoto; “rsh” y “rexec” para la ejecución remota de comandos de shell; y “rcp”, para la copia de archivos remotos.

Las herramientas que proporcionan Telnet y los comandos R son adecuadas, pero tiene una serie de problemas que se pueden solucionar con un programa que puede aportar una solución: SSH.

Tanto Telnet como los comandos R están lejos de ser seguros. El mecanismo de autenticación de rhosts, basado en la confianza y que usan los comandos R, es especialmente peligroso: confía en las direcciones IP del origen para identificar a los usuarios, por lo que puede ser interceptado con facilidad. El uso de tcpd o de xinetd para detectar los intentos de falsificación y las conexiones rechazadas eliminan parte del riesgo de este método, pero no son infalibles.

Telnet no está tan mal en cuanto a que pide siempre la contraseña antes de conceder el acceso, pero sufre de otra debilidad que también comparten los comandos R: debido a que las contraseñas, como todos los demás datos, se envían como texto plano a través de la red, son muy susceptibles a los ataques mediante el rastreo de paquetes (“Sniffing”).

Telnet y Rlogin tienen también una serie de problemas desde el punto de vista del usuario. La copia remota de archivos no es ni mucho menos apropiada. Puede que se considere a FTP como el mecanismo de transferencia de archivos, pero es muy poco manejable y muy difícil de pasar a scripts. Rcp es fácil de usar, pero no funcionará en absoluto hasta que el usuario autorice la equivalencia en el ámbito de cuentas entre las máquinas.

SSH, Secure Shell Service, Servicio de shell seguro

El servicio Secure Shell, SSH, intenta solucionar estos problemas de manera excelente. Entre todas las desventajas, destaca el uso de un potente cifrado para los datos transmitidos, con lo que ni las contraseñas ni otros datos pueden ser robados ni siquiera por atacantes que escuchen los datos que se están transmitiendo. El uso del cifrado impide también los ataques en los que el intruso entra en una conexión existente y cambia los datos en las dos direcciones. Los ataques de esta índole pueden usarse para añadir comandos a las sesiones, incluso en los casos en que la sesión haya sido autenticada mediante una segura contraseña de un solo uso. SSH usa otras técnicas criptográficas para efectuar una potente autenticación de los hosts y de los clientes. Esto significa que se puede tener un alto grado de confidencialidad a la que sólo los usuarios autorizados tienen permiso para conectarse. SSH se preocupa también por la facilidad de uso y tiene soporte completo para ejecutar aplicaciones X11 a través del canal autenticado y cifrado.

Cuando un cliente se conecta a un servidor SSH, verifica que el servidor sea realmente la máquina a la que se quería conectar. El cliente y el servidor intercambian claves de cifrado (de modo que impide a los espías que se aprendan las claves). El servidor autentifica entonces al cliente, usando el mecanismo de rhosts, la autenticación tradicional basada en la contraseña, o bien (de manera más segura) la autenticación RSA. Una vez que el cliente ha sido autenticado, el servidor lanza una shell o ejecuta un comando, a petición del cliente.

El método de autenticación usado por SSH se basa en criptografía o cifrado de clave pública, también conocida como criptografía asimétrica. La criptografía de clave pública cuenta con la existencia de un par asimétrico de claves: una clave pública y una clave privada. Las dos claves están relacionadas, pero no es posible deducir la clave privada desde la pública sin tener que hacer una búsqueda tanteando por todo el espacio de claves. La clave pública se usa para el cifrado y la clave privada para el descifrado. La clave privada debe mantenerse secreta, pero la pública puede ser emitida libremente por canales de comunicación insegura. Un agente remoto puede usar la clave pública para cifrar un flujo de datos que debería ser privado; sólo un agente con la clave privada correcta será capaz de leer los datos cifrados.

SSH usa también la autenticación para verificar la identidad del cliente y de los hosts de los servidores. Esto elimina todos los ataques basados en la suplantación de identidades de host mediante el falseamiento del DNS, del encaminamiento o de la dirección IP.

SERVICIOS COMUNES DE UNIX/LINUX

Cuando se instala un sistema operativo como Linux o Unix, normalmente hay un conjunto de servicios que se instalan por defecto; esto es bueno para los proveedores del sistema operativo ya que se evitan el soporte que acarrea una instalación, pero es muy peligroso porque muchos de estos servicios no se requieren en un servidor y son usados por los atacantes como puntos de vulnerabilidad sobre una red.

Podemos ver los diferentes servicios que un sistema Unix o Linux ofrece como potenciales puertas de entrada al mismo, o al menos como fuentes de ataques que ni siquiera tienen porque proporcionar acceso a la máquina (como las negaciones de servicio). De esta forma, si cada servicio ofrecido es un posible problema para nuestra seguridad, parece claro que lo ideal sería no ofrecer ninguno, poseer una máquina completamente aislada del resto; evidentemente, esto no suele ser posible hoy en día en la mayor parte de los sistemas. Por tanto, ya que es necesaria la conectividad entre equipos, hemos de ofrecer los mínimos servicios necesarios para que todo funcione correctamente; esto choca frontalmente con las políticas de la mayoría de fabricantes de sistemas Unix/Linux, que por defecto mantienen la mayoría de servicios abiertos al instalar un equipo nuevo: es responsabilidad del administrador preocuparse de cerrar los que no sean estrictamente necesarios.

Típicos ejemplos de servicios que suele ser necesario ofrecer son sendmail o ftp; en estos casos es necesaria una correcta configuración para que solo sea posible acceder a ellos desde ciertas máquinas, a través de xinetd.d. También es una buena idea sustituir estos servicios por equivalentes cifrados, como la familia de aplicaciones ssh, y concienciar a los usuarios para que utilicen estos equivalentes: hemos de recordar siempre (y recordar a los usuarios) que cualquier conexión en texto claro entre dos sistemas puede ser fácilmente capturada por cualquier persona situada en una máquina intermedia lo cual coloca en juego la seguridad de sistema y de la red completa. Tenga en cuenta que aparte de puertas de entrada, los servicios ofrecidos también son muy susceptibles de ataques de negación de servicio (DoS).

Para determinar la seguridad de un sistema usted podría desactivar o remover todos los servicios que su red no utilizara. Para determinar qué servicios son o no de importancia, usted debe tener claro el propósito de su servidor o equipo y así determinar los servicios mínimos necesarios, los servicios más comunes en una instalación por defecto son:

- Bluetooth
- Cron
- Cups
- Haldaemon
- Iptables
- Rsyslog
- Sendmail
- Sshd

XWindow

El entorno XWindow proporciona herramientas increíblemente potentes, pero que si no son correctamente configuradas pueden convertirse en peligrosas. Este sistema está formado por una serie de piezas que trabajan conjuntamente para ofrecer al usuario final un interfaz grafica:

La más importante de ellas, sobre todo desde el punto de vista de la seguridad es el servidor X. Este programa generalmente se ejecuta en la terminal de usuario, y tiene como función principal ofrecer unas primitivas básicas de dibujo (trazado de rectas, relleno de áreas. . .) sobre la pantalla; además gestiona eventos de teclado y ratón.

Las aplicaciones X son programas de usuario que lanzan llamadas contra un servidor X, mientras que el servidor se ejecuta habitualmente en la terminal desde donde conecta el usuario las aplicaciones se pueden lanzar desde el mismo equipo o también desde una máquina más potente, de forma que aprovechamos la capacidad de procesamiento de ese equipo.

El gestor de ventanas es un caso particular de aplicación, ya que se encarga de ofrecer un entorno de trabajo más amigable al usuario que está trabajando en la terminal: dibujo de marcos, menús, cerrado de ventanas.

Laboratorio Práctico

Con el fin de ambientarnos con el sistema operativo Linux Recomendando seguir los laboratorios de la comunidad drangonjar³ en la instalación y uso de backtrack⁴

<http://labs.dragonjar.org/video-tutorial-backtrack-booteo-interfaz-grafica-y-directorios>

Gracias a nuestros amigos DragonJar y 4v4t4r por el aporte.

³ <http://www.dragonjar.org>

⁴ <http://www.backtrack-linux.org/>

AMBIENTE OPERATIVO WINDOWS NT/XP/200X/VISTA/7

Como las máquinas LINUX, las plataformas de WINDOWS NT, XP, 200X, VISTA Y WINDOWS 7 son blancos populares de atacantes. Solo consultar algunas fuentes de estadísticas de vulnerabilidades como la del FBI o la del grupo X-Force, veremos que los sistemas operativos mas atacados son aquellos basados en Windows. Adicionalmente, si usted <http://www.microsoft.com/security/about/sir.aspx#MTCSC>, encontrara que la casa Microsoft se ha preocupado por mantener al día sus sistemas operativos.

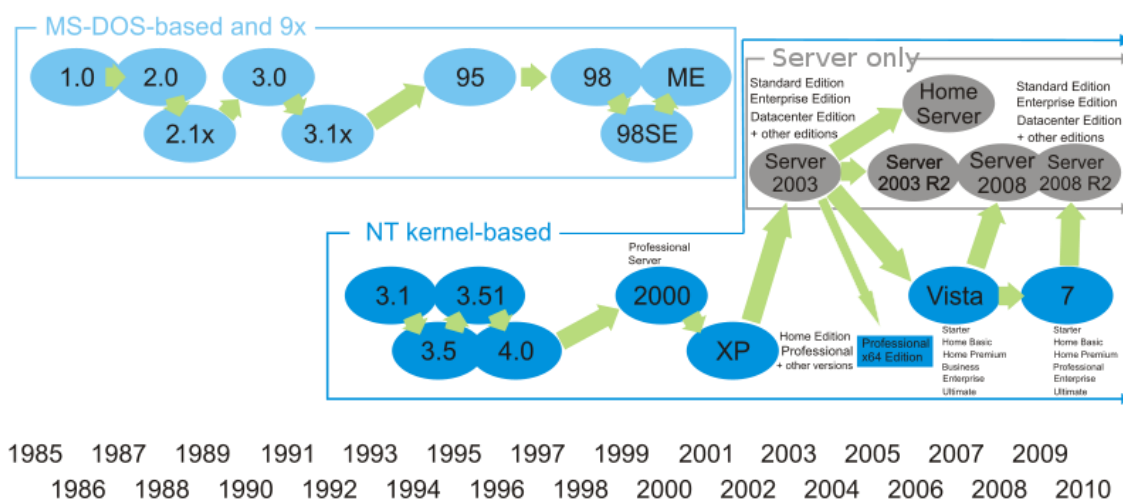
En este capítulo, echaremos una mirada a los sistemas operativos de WINDOWS NT, XP, 200X, VISTA y 7 conociendo su estructura para así analizar los mecanismos de seguridad específicos que ellos ofrecen. Veremos una breve historia de WINDOWS NT y centraremos nuestra atención a los conceptos de fundamentales, varios componentes de la arquitectura y opciones de seguridad de WINDOWS NT. Adicionalmente, examinaremos a Windows 2000 (qué realmente es WINDOWS NT 5.0) para determinar los cambios ocurridos y su impacto en la seguridad.

Este capítulo proporciona una breve apreciación global de la seguridad de WINDOWS NT y 2000 para que se pueda entender los ataques básicos descritos a lo largo del libro.

UNA BREVE HISTORIA EN EL TIEMPO⁵

Microsoft Windows

family tree



WINDOWS NT evoluciono a través de dos sistemas operativos previos: OS/2 y LAN MANAGER. Para adaptarse a la compatibilidad de estos productos, WINDOWS NT uso muchos de sus mecanismos para la conexión a red, con la

⁵ http://es.wikipedia.org/wiki/Microsoft_Windows

diferencia de una interfaz de usuario funcional y amigable. Esto aumento los esfuerzos de mercado lo cual coloco a WINDOWS NT en la cima de los mapas de ventas de sistemas operativos comerciales.

El "NT" en WINDOWS NT significa "Nueva Tecnología", también es conveniente considerar que existen diferentes compañías detrás de las versiones de UNIX, mientras que la empresa Microsoft es la única detrás de la serie WINDOWS.

Microsoft libero al mercado la versión de WINDOWS NT 3.1, luego 3.5, 3.51, 4.0, Windows Vista, Windows 2000 Server, Windows 2003 Server, Windows 2008 Server y Windows 7.

Windows 2008 Server

Windows 2008 Server es un sistema operativo multiproceso que soporta tanto redes basadas en servidores como redes punto a punto. Las características principales de este nuevo sistema operativo de red radica en la manera en que se gestiona el sistema hasta el punto de que se puede llegar a controlar el hardware de forma más efectiva, se puede controlar mucho mejor de forma remota y cambiar de forma radical la política de seguridad. Entre las mejoras que se incluyen, están:

- Nuevo proceso de reparación de sistemas NTFS: proceso en segundo plano que repara los archivos dañados.
- Creación de sesiones de usuario en paralelo: reduce tiempos de espera en los Terminal Services y en la creación de sesiones de usuario a gran escala.
- Cierre limpio de Servicios.
- Sistema de archivos SMB2: de 30 a 40 veces más rápido el acceso a los servidores multimedia.
- Address Space Load Randomization (ASLR): protección contra malware en la carga de controladores en memoria.
- Windows Hardware Error Architecture (WHEA): protocolo mejorado y estandarizado de reporte de errores.
- Virtualización de Windows Server: mejoras en el rendimiento de la virtualización.
- PowerShell: inclusión de una consola mejorada con soporte GUI para administración.
- Server Core: el núcleo del sistema se ha renovado con muchas y nuevas mejoras.

La mayoría de las ediciones de Windows Server 2008 están disponibles en x86-64 (64 bits) y x86 (32 bits). Windows Server 2008 para sistemas basados en Itanium soporta procesadores IA-64. La versión IA-64 se ha optimizado para escenarios con altas cargas de trabajo como servidores de bases de datos y aplicaciones de línea de negocios (LOB). Por ende no está optimizado para su uso como servidor de archivos o servidor de medios. Microsoft ha anunciado que Windows Server 2008 será el último sistema operativo para servidores disponible en 32 bits. Las ediciones se enumeran a continuación:

- Windows Server 2008 Standard Edition (x86 y x86-64)
- Windows Server 2008 R2 Todas las Ediciones (Solo 64Bit)
- Windows Server 2008 Enterprise Edition (x86 y x86-64)
- Windows Server 2008 Datacenter Edition (x86 y x86-64)
- Windows HPC Server 2008 (reemplaza Windows Compute Cluster Server 2003)
- Windows Web Server 2008 (x86 y x86-64)
- Windows Storage Server 2008 (x86 y x86-64)
- Windows Small Business Server 2008 (Nombre clave "Cougar") (x86-64) para pequeñas empresas
- Windows Essential Business Server 2008 (Nombre clave "Centro") (x86-64) para empresas de tamaño medio3
- Windows Server 2008 para sistemas basados en Itanium
- Windows Server 2008 Foundation Server

Windows 7

Windows 7 es la versión más reciente de Microsoft Windows, línea de sistemas operativos producida por Microsoft Corporation. Esta versión está diseñada para uso en PC, incluyendo equipos de escritorio en hogares y oficinas, equipos portátiles, "tablet PC", "netbooks" y equipos "media center".

A diferencia del gran salto arquitectónico y de características que sufrió su antecesor Windows Vista con respecto a Windows XP, Windows 7 fue concebido como una actualización incremental y focalizada de Vista y su núcleo NT 6.0, lo que permitió el mantener cierto grado de compatibilidad con aplicaciones y hardware en los que éste ya era compatible. Sin embargo, entre las metas de desarrollo para Windows 7 se dio importancia en mejorar su interfaz para volverla más accesible al usuario e incluir nuevas características que permitieran hacer tareas de una manera más fácil y rápida, al mismo tiempo en que se realizarían esfuerzos para lograr un sistema más ligero, estable y rápido.

Existen seis ediciones de Windows 7, construidas una sobre otra de manera incremental, aunque solamente se centrarán en comercializar tres de ellas para el común de los usuarios: las ediciones Home Premium, Professional y Ultimate. A estas tres, se suman las versiones Home Basic y Starter, además de la versión Enterprise, que está destinada a grupos empresariales que cuenten con licenciamiento "Open" o "Select" de Microsoft.

Starter: Es la versión de Windows 7 con menos funcionalidades de todas. Posee una versión incompleta de la interfaz Aero que no incluye los efectos de transparencia Glass, Flip 3D o las vistas previas de las ventanas en la barra de inicio y que además no permite cambiar el fondo de escritorio. Está dirigida a PC de hardware limitado —como netbooks—, siendo licenciada únicamente para integradores y fabricantes OEM. Incluye una serie de restricciones en opciones de personalización, además de ser la única edición de Windows 7 sin disponibilidad de versión para hardware de 64 bits.

Home Basic: Versión con más funciones de conectividad y personalización, aunque su interfaz seguirá siendo incompleta como en la edición Starter. Sólo estará disponible para integradores y fabricantes OEM en países en vías de desarrollo y mercados emergentes.

Home Premium: Además de lo anterior, se incluye Windows Media Center, el tema Aero completo y soporte para múltiples códecs de formatos de archivos multimedia. Disponible en canales de venta minoristas como librerías, tiendas y almacenes de cadena.

Professional: Equivalente a Vista "Business", pero ahora incluirá todas las funciones de la versión Home Premium más "Protección de datos" con "Copia de seguridad avanzada", red administrada con soporte para dominios, impresión en red localizada mediante Location Aware Printing y cifrado de archivos. También disponible en canales de venta al público.

Enterprise: Añade sobre la edición Professional de Windows 7, características de seguridad y protección de datos como BitLocker en discos duros externos e internos, Applocker, Direct Access, BranchCache, soporte a imágenes virtualizadas de discos duros (en formato VHD) y el paquete de opción multilinguaje. Únicamente se vende por volumen bajo contrato empresarial Microsoft software Assurance. También es la única que da derecho a la suscripción del paquete de optimización de escritorio MDOP.

Ultimate: Esta edición es igual a la versión Enterprise pero sin las restricciones de licenciamiento por volumen, permitiéndose su compra en canales de venta al público general, aunque Microsoft ha declarado que en lugar de publicitarse en medios comunes, será ofrecida en promociones ocasionales de fabricantes y vendedores.

Ediciones N: Las ediciones N están disponibles para actualizaciones y nuevas compras de Windows 7 Premium, Professional y Ultimate. Las características son las mismas que sus versiones equivalentes, pero no incluyen Windows Media Player. El precio también es el mismo, ya que Windows Media Player puede descargarse gratuitamente desde la página de Microsoft.

WINDOWS XP PROFESIONAL

Integra los puntos fuertes de Windows 2000 Profesional (como seguridad basada en estándares, la capacidad de administración y confiabilidad), características comerciales de Windows 98 y Windows Me (Plug and Play, interfaz de usuario sencilla y servicios de soporte). Entre sus características están:

Basado en el nuevo motor de Windows, integra la base de códigos de Windows NT y Windows 2000, que presenta una arquitectura informática de 32 bits y un modelo de memoria totalmente protegido.

Escenarios de reinicio reducidos drásticamente, elimina la mayoría de los escenarios que obligan a los usuarios finales a reiniciar los equipos en Windows NT 4.0 y Windows 95/98/Me.

Protección de códigos mejorada, la estructura de los datos importantes del núcleo son de solo lectura, por lo que los controladores y las aplicaciones no pueden corromperlas. Todos los códigos de controladores de dispositivos son de solo lectura y con protección de página.

Directivas de restricción de software mejoradas, proporciona a los administradores un mecanismo impulsado por directivas para identificar el software que se encuentra en ejecución en su entorno y controlar su capacidad de ejecución. Se utiliza en la prevención de virus y caballos de Troya y el bloqueo de software.

Sistema de cifrado de archivos con soporte para varios usuarios, cifra todos los archivos con una clave generada aleatoriamente. Los procesos de cifrado y descifrado son transparentes para el usuario. En Windows XP Profesional permite que varios usuarios tengan acceso a un documento cifrado.

Seguridad IP, ayuda a proteger los datos transmitidos a través de la red, IPSec es una parte importante de las redes virtuales privadas (VPN), que permiten a las organizaciones transmitir datos de forma segura por Internet.

Archivos y carpetas sin conexión, los usuarios pueden especificar los archivos y las carpetas de la red que necesitarán cuando se desconecten. Las carpetas sin conexión se pueden cifrar para brindar el más alto nivel de seguridad.

Consola de recuperación, proporciona una consola de línea de comandos para iniciar y detener servicios, dar formato a unidades, leer y escribir datos en una unidad local y realizar tareas administrativas.

Directiva de grupo, simplifica la administración de los usuarios, al permitir a los administradores organizarlos en unidades lógicas, como departamentos o ubicaciones, y asignar la misma configuración, incluidas las opciones de seguridad, aspecto y administración a todos los empleados del grupo.

CONCEPTOS FUNDAMENTALES DE SERVIDORES WINDOWS Y SISTEMAS WINDOWS 7

DIRECTORIO ACTIVO

El directorio activo es un servicio de directorio. El término servicio de directorio se refiere a dos cosas – un directorio donde la información sobre usuarios y recursos está almacenada, y un servicio o servicios que dejan acceder y manipular estos recursos. El directorio activo es una manera de manejar todos los elementos de una red, incluido computadoras, grupos, usuarios, dominios, políticas de seguridad, y cualquier tipo de objetos definidos para el usuario. Además de esto, provee de funciones adicionales más allá de estas herramientas y servicios.

El directorio activo está construido alrededor de la tecnología DNS y LDAP – DNS porque es el estándar en Internet y es bastante familiar, LDAP porque la mayoría de fabricantes lo soportan. Los clientes de directorio activo usan DNS y LDAP para localizar y acceder a cualquier tipo de recurso de la red. Al ser protocolos de plataforma independiente, Los computadores Unix, Linux y Macintosh pueden tener acceso a los recursos de igual modo que los clientes de Windows.

La consola MMC (*Microsoft Management Console*) se usa para implementar y gestionar el directorio activo. Las metas de directorio activo tienen dos acercamientos importantes:

- Los usuarios deben poder acceder a recursos por todo el dominio usando un único acceso o login a la red.
- Los administradores deben poder centralizar la gestión de usuarios y recursos.

La estructura de directorio activo tiene una forma jerárquica donde se localizan los objetos. Estos objetos caen en tres tipos de categorías:

- Recursos, como por ejemplo impresoras.
- Servicios, como correo, Web, FTP, etc.
- Usuarios, los cuales incluyen cuentas para conectarse, grupos de trabajo, etc.

Un objeto es únicamente identificado por su nombre y tiene un serie de atributos definidos por un esquema, que también determina la clase de objeto que se pueden almacenar en el directorio. Los atributos son las características y la información que el objeto contiene.

Cada atributo del objeto puede ser usado en diferentes clases de objetos dentro del esquema del objeto. Dicho esquema existe para que se pueda hacer modificaciones o extensiones cuando sea necesario. Hay que tener

cuidado al cambiar estos atributos una vez que estén creados, ya que podemos cambiar la estructura ya creada del directorio activo, por lo que hay que hacerlo de un modo planeado.

El dominio se observa desde un número de niveles. En la parte más alta tenemos el bosque – la colección de todos los objetos, sus atributos y reglas en el directorio activo. Los dominios se identifican por su nombre de estructura DNS. Un dominio tiene un sólo nombre DNS.

Los objetos dentro de un dominio pueden estar agrupados en contenedores llamados unidades organizativas (OU). Estas unidades dan al dominio una jerarquía, facilita la administración y proporciona una imagen de la compañía en términos organizativos y geográficos.

Estas unidades organizativas pueden contener a su vez otras unidades organizativas. Normalmente, se suelen aplicar las políticas de grupo a nivel de OU, aunque también pueden ser aplicados a dominios. Se suelen dar poderes de administrador a estos OU y todo lo que contienen por debajo, aunque también se pueden delegar funciones de administrador a objetos individuales o atributos.

El directorio activo también soporta la creación de sitios, los cuales son grupos físicos más que lógicos, definidos por una o más subredes. Estos sitios son independientes del dominio y a estructura OU, y son comunes por todo el bosque. Se utilizan para controlar el tráfico de red generado por replicación, y también para referir a los clientes al controlador de dominio más cercano.

RECURSOS COMPARTIDOS

Desde una perspectiva de usuario, los recursos compartidos son una de las principales funciones de los sistemas Windows. Un recurso compartido es una conexión (normalmente remota) a un dispositivo de la red, como por ejemplo un disco duro o una impresora. Los usuarios pueden acceder a los recursos a través del Explorador de Windows o haciendo Doble Clic en el icono del Entorno de red en el escritorio, sin embargo es bueno conocer otra alternativa que se hace a través de la ventana de comandos mediante la instrucción “net use”, la cual tiene la siguiente sintaxis:

C:\> Net use \\ [Dirección IP o Nombre de Hosts] \ [Nombre del Recurso] – [Nombre de Usuario] : [Contraseña]

Una vez conectado a un recurso, los usuarios pueden acceder los objetos (Ejemplo, archivos, directorios o carpetas y demás), dependiendo, claro, de los permisos particulares que se aplican a estos objetos.

SERVICES PACKS Y ADVERTENCIAS CRÍTICAS (HOT FIXES)

Cuando se descubren vulnerabilidades, cada fabricante del sistema operativo libera actualizaciones y arreglos para cada producto del mismo; Microsoft no esta exento de esta regla. Los arreglos y actualizaciones para WINDOWS 200X/XP/VISTA/7 se clasifican en dos tipos: Service Pack y Advertencias Criticas (Hot Fixes).

Los Services Packs son, en efecto, un grupo de Advertencias Criticas integrados en un solo paquete de instalación, mientras que una Advertencia Crítica sólo se dirige a un problema específico como una falla en la programación que permite a un atacante romper los sistemas remotamente. Estos se pueden descargar de Internet permanentemente o se delega la función para que se haga de manera automática a través de la utilidad de Windows Update. Las Advertencias Críticas están incorporadas en los Services Packs, pero no de forma inmediata. Normalmente, los Service Packs son lanzados cuando ha pasado un tiempo razonable después del Service Pack anterior (Ejemplo, seis meses a un año).

La gran parte de administradores de sistemas, no se preocupan por estas actualizaciones por lo que un atacante podría perfectamente ensayar sus scripts para alterar o denegar el acceso a los sistemas.

CONTROL DE CUENTAS DE USUARIO

El Control de Cuentas de Usuario (UAC por sus siglas en ingles) es una tecnología e infraestructura de seguridad que Microsoft introdujo con Windows Vista. Su objetivo es mejorar la seguridad de Windows al impedir que aplicaciones maliciosas hagan cambios no autorizados en el ordenador.

Como Windows no puede diferenciar entre un usuario haciendo click sobre un botón y un programa haciendo click sobre un botón, la UAC fue implementada inicialmente para siempre advertir al usuario via una ventana de dialogo mostrada en un Escritorio Seguro (Secure Desktop), similar a la pantalla de inicio de sesión, sobre cualquier cambio en la configuración del sistema.

Windows 7, sin embargo, ahora incluye la posibilidad de configurar UAC para ocultar estos – molestos a veces – avisos cuando los usuarios cambien configuraciones de Windows. Mientras que este modo aun asegura que las aplicaciones normales no puedan sobre escribir completamente alguna llave del registro, Microsoft ha permitido que los usuarios cambien cualquier configuración de Windows sin ningún aviso advirtiendo de aquello. Sí, incluso se puede cambiar la configuración de UAC – desactivar – de tal modo que Windows no advierta nunca al usuario de estos cambios que se están llevando a cabo en el sistema.

ARQUITECTURA

La arquitectura de Windows 200X/XP/7 está dividida en dos modos, Modo del Usuario y Modo del Kernel. A continuación explicaremos el trabajo de cada uno de estos modos.

MODO USUARIO

Esta capa está compuesta de subsistemas que pasan los requerimientos de Entrada y Salida (E/S) al controlador del kernel mediante los servicios de sistema de E/S. Una aplicación siempre se ejecutará en este modo, el cual actúa como un intermediario entre las aplicaciones y los componentes del modo kernel. Este modo se divide además en el subsistema de entorno y el subsistema integral. Las aplicaciones escritas para varios sistemas operativos pueden ejecutarse sobre Windows 200X/XP/7 usando los Subsistemas de Entorno. La Interfaz de Programación de Aplicación (Application Programming Interface, API) pasa los llamados hechos por la aplicación, los cuales después de ser recibidos por el subsistema de entorno, son pasados a los componentes de ejecución del modo kernel. Los subsistemas de entorno están limitados a una dirección ya asignada y no tienen contacto directo con el hardware o los controladores de dispositivos. Comparados con el Modo Kernel, poseen una baja prioridad de ejecución y utilizan espacio del disco duro como memoria virtual cada vez que el sistema necesita memoria. El subsistema integral ejecuta varias funciones, entre las cuales se encuentran la seguridad, los servicios de la estación de trabajo y los servicios del servidor.

Este modo contiene también el Subsistema de Seguridad, también conocido como la “Autoridad de Seguridad Local (LSA)”, tiene un papel crítico en la seguridad de WINDOWS 200X/XP/7. Este subsistema de Modo de Usuario determina si los esfuerzos del inicio de sección son válidos. Cuando un usuario entra su Nombre de Usuario y la Contraseña durante el proceso de inicio de sección, el Subsistema de Seguridad envía estos datos para facilitar el llamado al Manejador de Cuentas Seguras o SAM. El SAM tiene una base de datos que se identifica con su nombre “Base de Datos SAM”. Normalmente, en esta base de datos está compuesta por dos parámetros para cada usuario, uno (llamado LM contraseña de representación) que contiene una representación de la contraseña del usuario para los propósitos de compatibilidad dirigida hacia los productos menos sofisticados de la casa Microsoft, como LanMan y Windows para Trabajo en Grupo.

El otro parámetro en la base de datos de SAM se llama los "Windows hash – (Picadillo de Windows)" y contiene la contraseña cifrada la cual es necesaria para la compatibilidad con los sistemas Windows 200X/XP/7. Este archivo podrá ser encontrado en la siguiente ruta: \WINDOWS\SYSTEM32\CONFIG, y tiene el siguiente esquema:

```
jca:1011:3466C2B0487FE39A417EAF50CFAC29C3:80030E356D15FB1942772DCFD7DD3234:::  
alfredof:1000:89D42A44E77140AAAAD3B435B51404EE:C5663434F963BE79C8FD99F535E7AAD  
8:::  
william:1012:DBC5E5CBA8028091B79AE2610DD89D4C:6B6E0FB2ED246885B98586C73B5BFB  
77:::  
silvia:1001:1C3A2B6D939A1021AAD3B435B51404EE:E24106942BF38BCF57A6A4B29016EFF6:::
```

Observe que cada línea consiste de un juego de entradas: el nombre de cuenta, un número único de identificación conocido como el ID relativo, la contraseña de representación LM, el Windows Hash, y varios campos opcionales. Cada uno de estos campos está separado por dos puntos.

Las contraseñas de representación LM y los Windows hash para cada cuenta, se genera básicamente de dos formas diferentes. En WINDOWS, la longitud de la contraseña es máxima de 14 caracteres. Efectivamente, un usuario puede teclear más de 14 caracteres para una contraseña, pero el sistema arrastrara algunos caracteres para solo tomar en cuenta una contraseña real de 14 caracteres.

La representación de LM se genera ajustando la longitud de la contraseña a exactamente 14 caracteres, o anulando los caracteres de exceso o insertando caracteres en blanco. Entonces, la cadena resultante está dividida en dos partes iguales: Un carácter de paridad (necesario para la Norma de Encriptación de Datos [DES]) que se agrega a cada parte, y cada parte se usa como una llave para el encriptación de DES de un número hexadecimal. La representación LM es increíblemente débil, un atacante puede perfectamente tomar cada parte de la clave (7 caracteres de los 14 de la contraseña) para formar la representación LM a partir de suposiciones.

Los Windows hash son mucho más fuertes, pero no imposibles de descifrar. Al igual que LM la longitud de la contraseña se ajusta a 14 caracteres exactamente. El algoritmo de encriptación MD-4 (MD-5) usa tres permutaciones sobre la contraseña original para dar como resultado una contraseña derivada o picadillo de la contraseña (Windows hash).

Hay una notable falla en el algoritmo que produce los Windows hash, y es el de no poseer un numero grande de permutaciones lo que hace que se puedan realizar ataques a base de diccionario sobre la base datos SAM

MODO KERNEL

Aunque ambos modos tienen seguridad incorporada, el Modo Kernel, reservado para la funcionalidad del sistema operativo (incluso el acceso a la memoria y hardware) es el más seguro de los dos. Este contiene unos subsistemas como son el Manejador de Entrada y Salida, El manejador de Objetos, el Monitor de Seguridad, el Manejador de Procesos, Las Llamadas de los Procedimientos Locales, el Manejador de la Memoria Virtual, y el subsistema de los controladores de la Interface Gráfica.

De todos estos subsistemas, el Monitor de Seguridad es el más importante obviamente desde nuestro punto de vista. Se encarga de verificar, aprobar o rechazar cada esfuerzo por acceder al Modo kernel, el monitor de seguridad sirve como un tipo de "guardián" del modo kernel, pero este también desempeña una función paralela para el usuario inicial y programas basados en objetos como son los archivos y directorios. Verifica que los usuarios y programas tengan los permisos apropiados antes de permitir el acceso a los objetos. Finalmente, define como audita el sistema para traducir la captura en tiempo real de los eventos ocurridos en la máquina (Even Log).

Mucha funcionalidad de sistemas operativos WINDOWS (incluyendo el Monitor de Seguridad) es basada en el Manejador de Objetos, el cual es un subsistema crítico que maneja la información sobre los objetos dentro del sistema. Los objetos incluyen archivos, directorios, dispositivos como impresoras, usb, DVD entre otros. El manejador de objetos asigna un Identificador de Objeto (OID) a cada uno cuando se crea por primera vez. Este OID perdura por el tiempo de vida del objeto y se usa para referirse a él. Siempre que un objeto se elimine (por ejemplo, cuando un usuario arrastra el icono de un archivo a la papelera de reciclaje, y luego vacía la papelera), el manejador de objetos anula el OID asignado para dicho archivo.

Finalmente, el Modo Kernel también incluye la Capa de Abstracción de Hardware (HAL). Una ventaja del HAL es que un DVD de WINDOWS puede ser instalado en diferentes plataformas de hardware.

En resumen podemos decir que el Modo Kernel está compuesto por todos los controladores y dispositivos de hardware, los cuales son los bloques de construcción de Windows 200X/XP/7.

CUENTAS Y GRUPOS

Las cuentas y los grupos son los puntos centrales en la seguridad de cada sistema operativo, incluyendo a WINDOWS 200X/XP/7. Cuentas con accesos inapropiados y grupos con privilegios inapropiados, pueden facilitar acceso ilimitado a los atacantes.

A continuación exploraremos las consideraciones de seguridad relacionados con los grupos y las cuentas de usuario.

LAS CUENTAS

En WINDOWS 200X/XP/7 hay dos tipos de cuentas: las cuentas predeterminadas y las cuentas creadas por los administradores.

Las Cuentas Predeterminadas

En los sistemas WINDOWS, se crean dos cuentas automáticamente cuando el PDC se instala y ellas son el Administrador y el Invitado. La cuenta Administrador tiene el nivel más alto de privilegios que se puedan considerar, es como la cuenta “root” de UNIX/LINUX. Es posible usar la función de Copia con WINDOWS GUI para crear cuentas adicionales con los privilegios del administrador, o alternativamente, crear completamente nuevas cuentas que son incluidas en el Administrador del Dominio para lograr el mismo efecto.

Una propiedad interesante de la cuenta Administrador es que, por defecto, no puede bloquearse no importa cuántos intentos fallidos en contraseñas supuestas o mal digitadas se utilicen. Adicionalmente, esta cuenta nunca podrá eliminarse, y sólo puede desactivar desde otra cuenta no deshabilitada con propiedades de Administrador. Crear más de una cuenta administradora es esencial; ya que la cuenta administradora por defecto, puede recibir ataques de fuerza bruta para suponer la contraseña y crear una cuenta sin privilegios y una cuenta administradora por cada Administrador es una buena práctica de seguridad que permite responsabilizar a cada individuo por las acciones hechas con propiedades de Administrador, en este caso cada administrador usaría su cuenta sin privilegios para el acceso normal al sistema; cuando requiera realizar acciones de administración solo cerraría su sección y pasaría a la cuenta administradora.

La segunda cuenta predetermina en el sistema es la cuenta Invitado. Si se habilita esta cuenta, es un blanco fácil para los atacantes informáticos. Afortunadamente, por defecto esta cuenta está deshabilitada. Como la cuenta del Administrador, la cuenta de Invitado no puede eliminarse. Por las razones de seguridad, es conveniente mantener desactivada dicha cuenta.

Otras Cuentas

Las cuentas adicionales, como cuentas del usuario o cuentas para servicios específicos o aplicaciones, pueden ser creadas por administradores por necesidad. Muchas aplicaciones también crean cuentas durante la instalación. Mientras la cuenta Administrador y la cuenta Invitado tienen muchas restricciones, cualquier cuenta adicional puede desactivarse o puede eliminarse sin estas restricciones.

Estrategias Usadas En Sitios Seguros Sobre Las Cuentas

A simple vista las medidas expuestas a continuación pueden parecer demasiado simples, pero la realidad es que complica aún más el trabajo de un atacante a la hora de irrumpir en nuestro servidor. Una primera estrategia es el renombramiento de la cuenta del “Administrador” creado por defecto por el sistema y asignarle otro nombre como por ejemplo un nombre de usuario ficticio, esto hará que dicha cuenta sea menos visible para un atacante (claro, que un atacante experimentado puede determinar el nombre de una cuenta administradora rápidamente a través de un programa de fácil acceso llamado escáner de vulnerabilidades). También, si el nombre de la cuenta del Administrador se cambia, es una buena idea cambiar la descripción de dicha cuenta.

Una segunda estrategia es crear una cuenta sin privilegios llamada “Administrador” para actuar como una cuenta señuelo. Los atacantes pueden perseguir esta cuenta que tiene una contraseña de difícil suposición y cuyos privilegios de acceso son sumamente limitados. Con esta cuenta señuelo es posible examinar los datos de seguridad ubicados en los log del sistema para determinar si alguien ha intentado atacar la cuenta del Administrador.

GRUPOS

En la mayoría de las versiones de WINDOWS 200X/XP/7, se usan los grupos para controlar el acceso y privilegios de un conjunto de usuarios. La razón de ser de esto, es para cada usuario que ingrese al sistema se genera un esquema el cual controla su acceso y sus privilegios, estos esquemas colocan el sistema demasiado lento y pesado cuando tiene una gran cantidad de usuarios, por lo que la solución es asignar un esquema a un grupo de usuarios.

Los sistemas WINDOWS tienen dos tipos de grupos, grupos globales y locales. Los grupos globales permiten el acceso potencialmente a cualquier recurso en cualquier servidor dentro de un dominio. Los grupos locales permiten solamente el acceso en el servidor o puesto de trabajo en que fueron creados.

Los Grupos Por Defecto

Son varios los grupos que se crean por defecto cuando el PDC se instala. Algunos de éstos son grupos locales mientras otros son globales. Estos grupos (la mayoría tiene un nombre auto explicativo, salvo el grupo de Replicadores controla la función de soluciones a tolerancia a fallos) se muestra en el siguiente cuadro:

GRUPOS LOCALES	GRUPOS GLOBALES
Administradores	Administradores de Dominio
Usuarios Avanzados	Usuario de Dominio
Duplicadores	
Invitados	
Operadores de Copias	
Usuarios	

Más allá de estos grupos predefinidos, hay también grupos especiales pensados para controlar ciertos tipos de funcionalidades del sistema.

CONTROL DE PRIVILEGIOS

En Windows 200X/XP/7, la capacidad de acceder y manipular las diferentes utilidades del sistema en forma colectiva, es conocida como “privilegios”. Los privilegios está compuesta de dos áreas: los derechos y las habilidades. Los derechos son las cosas que los usuarios pueden hacer para agregar o revocar cuentas de usuarios y grupos (con algunas restricciones). Las habilidades por otro lado, no pueden agregarse o revocarse; son las capacidades incorporadas de varios grupos que no pueden alterarse. Los grupos definidos previamente vienen con un nivel particular de derechos y habilidades.

Hasta donde pueden llegar los privilegios de los usuarios logueados, los privilegios del Administrador son el nivel más alto de cualquier sección en WINDOWS 200X/XP/7, actuando un poco como la cuenta del “root” UNIX/LINUX.

BIBLIOGRAFÍA

LINUX

- SANCHEZ PRIETO, Sebastián; GARCIA POBLACION, Oscar. Linux Guía Practica.
- CARAZO GIL, Francisco Javier. Ubuntu Linux. Instalación y configuración básica en equipos y servidores.
- MCCARTY, Bill. SELinux.
- TURNBULL, James. LIEVERDINK, Peter. MATOTEK, Dennis; GONZÁLEZ CRUZ, Sergio Luis. Administración de Sistemas Linux.
- ADELSTEIN, Tom; LUBANOVIC, Bill. Administración de Sistemas Linux.

WINDOWS

- DOMÍNGUEZ ALCONCHEL, José. Microsoft Windows7: Guía de Información.
- RAYA CABRERA, José Luis; MARTÍNEZ RUIZ, Miguel Ángel; RAYA GONZÁLEZ, Laura. Aprenda Microsoft Windows Server 2003.
- RAYA CABRERA, José Luis; RAYA GONZÁLEZ, Laura; MARTÍNEZ RUIZ, Miguel Ángel. Domine Microsoft Windows Server 2008.
- PÉREZ, César. Guía de campo de Microsoft Windows XP (SP2).
- PARDO NIEBLA, Miguel. Windows XP Professional
- CRAIG, Zacker. Planning and Maintaining a MS Windows Server 2003 Network
- CHARTE, Francisco. Windows 7. Registro y Configuración.
- STANEK, William R. (1966-); CABRERIZO PASCUAL, María. Windows 7. Guía de Configuración.
- TEMPRADO MORALES, José Carlos. Windows Server 2008. Registro y Configuración.
- MARTOS RUBIO, Ana. Windows XP.

ENLACES

www.microsoft.com/es/es/default.aspx
www.fedoraproject.org/es/
www.debian.org/index.es.html
www.ubuntu.com
www.opensuse.org/es/
www.redhat.com/
www.kubuntu.org/
www.mandriva.com/
www.gentoo.org/
www.oracle.com/us/products/servers-storage/solaris/index.html
www.dragongar.org

TABLA DE CONTENIDO

AMBIENTES OPERATIVOS.....	1
<i>LINUX/UNIX</i>	<i>1</i>
<i>ESCOGIENDO UNA DISTRIBUCIÓN DE LINUX</i>	<i>2</i>
<i>ARQUITECTURA</i>	<i>5</i>
SISTEMAS DE ARCHIVOS	5
ESTRUCTURA DEL SISTEMA DE ARCHIVOS	10
EL KERNEL Y LOS PROCESOS	12
PONIENDO EN MARCHA PROCESOS AUTOMÁTICAMENTE	13
INTERACTUANDO CON LOS PROCESOS	19
CUENTAS Y GRUPOS	20
CONTROL DE PRIVILEGIOS	24
PROGRAMAS SUID Y SGID	27
RELACIÓN DE CONFIANZA EN MÁQUINAS LINUX/UNIX	28
SERVICIOS COMUNES DE UNIX/LINUX	30
<i>Laboratorio Práctico</i>	<i>31</i>
<i>AMBIENTE OPERATIVO WINDOWS NT/XP/200X/VISTA/7</i>	<i>32</i>
<i>UNA BREVE HISTORIA EN EL TIEMPO</i>	<i>32</i>
<i>Windows 2008 Server</i>	<i>33</i>
<i>Windows 7</i>	<i>34</i>
<i>WINDOWS XP PROFESIONAL.....</i>	<i>35</i>
<i>CONCEPTOS FUNDAMENTALES DE SERVIDORES WINDOWS Y SISTEMAS</i>	
<i>WINDOWS 7</i>	<i>37</i>
DIRECTORIO ACTIVO	37
RECURSOS COMPARTIDOS	38
SERVICES PACKS Y ADVERTENCIAS CRÍTICAS (HOT FIXES).....	39
CONTROL DE CUENTAS DE USUARIO	39
ARQUITECTURA	40
CUENTAS Y GRUPOS	42
CONTROL DE PRIVILEGIOS	45
BIBLIOGRAFÍA	46