GLOSARIO DE TERMINOS USADOS EN SEGURIDAD INFORMATICA

A B D E I K M N O P R S T V U W

A

Active-X

Como la mayor parte de sitios web son documentos estáticos con poca interactividad, Microsoft ha creado un lenguaje de programación, llamado ActiveX, para remediar la situación. Los controles ActiveX tienen por objetivo hacer que la navegación por internet sea comparable a la de un CD-Rom, y poder escuchar música, ver animaciones y video clips e interactuar con el programa

Administrador de lista

Un administrador de lista es una persona que administra una lista de distribución, añade y borra miembros, y se ocupa de los aspectos generales del mantenimiento de la lista. En ocasiones modera la discusión e interviene cuando se producen disputas o una flame war, guerra de llamas

ADSL

Abreviación de Asymmetric Digital Subscriber Line, el ADSL es un método de transmisión de datos a través de las líneas telefónicas de cobre tradicionales a velocidad alta. Los datos pueden ser descargados a velocidades de hasta 1.544 Megabits por segundo y cargados a velocidades de hasta 128 Kilobits por segundo. Esa es la razón por la cual se le denomina asimétrico. Esta tecnología es adecuada para el web, ya que es mucho mayor la cantidad de datos que se envían del servidor a un ordenador personal que lo contrario.

Agente

Un agente es un tipo de software programado para ir a Internet y realizar una función específica para el usuario. El tipo más común de agente son los programas llamados spiders y worms (arañas y gusanos), que transitan por el Internet, recolectando la información e catalogando su contenido, creando sus propias bases de datos del contenido encontrado. Se están desarrollando otros agentes, con funciones más complejas, que permitirán a los usuarios hacer cosas como buscar sitios de música en línea y comparar los precios de sus discos.

Ancho de banda

El ancho de banda es la máxima cantidad de datos que pueden pasar por un camino de comunicación en un momento dado, normalmente medido en segundos. Cuanto mayor sea el ancho de banda, más datos podrán circular por ella al segundo.

API (Application Program Interface).

Interface de programa de aplicación. Un conjunto de rutinas que un programa de aplicación utiliza para solicitar y efectuar servicios de nivel inferior ejecutados por el sistema operativo de un equipo. También, un conjunto de convención de llamada en programación que definen cómo se debe invocar un servicio a través de la aplicación.

ARCHIVOS PE (Portable Executable).

Este formato de archivos ejecutables de Windows, recibe el nombre de "portátil" porque puede ser compartido por todos los sistemas operativos de 32 bits. El mismo archivo puede ejecutarse en cualquier versión de Windows 95, 98, Me, NT, 2000 y XP. Todos los archivos de formato PE son ejecutables (las extensiones más conocidas son .EXE, .DLL, .OCX, .SCR y .CPL), pero no todos los ejecutables son portátiles.

atrás A B D E I K M N O P R S T V U W arriba

B

BINDER

Pequeño programa que simplemente une dos o más archivos en un solo ejecutable. También es conocido como Joiner, Juntador, Trojan-Dropper, Dropper, etc.

atrás A B D E I K M N O P R S T V U W arriba

D

DCC (Direct Client to Client)

Los archivos enviados entre usuarios participantes de un canal de chat (IRC) se transmiten por medio de una sesión denominada DCC (Direct Client to Client), que permite la transferencia directa de los mismos.

D.D.o.S (Distributed Denial of Service).

Ataques de negación de servicio distribuidos. En lugar de una sola computadora, se utilizan cientos o hasta miles de ellas, todas actuando al mismo tiempo contra una misma víctima, un servidor o cualquier computadora conectada a Internet, la que recibe una sucesión de solicitudes de servicio, con tal frecuencia y cantidad, que al no poder ser respondidas van disminuyendo paulatinamente su rendimiento, ocasionando casi siempre la caída del sistema, además de la saturación del ancho de banda asignado.

D.o.S - Un ataque de D.o.S (Denial of Service, o negación de servicio)

Hace que los servidores o cualquier computadora conectada a Internet, reciban una sucesión de solicitudes de servicio, con tal frecuencia y cantidad, que al no poder ser respondidas van disminuyendo paulatinamente su rendimiento, ocasionando casi siempre la caída del sistema, además de la saturación del ancho de banda asignado.

DROPPER (cuentagotas)

Es un archivo que cuando se ejecuta "gotea" o libera un virus. Un archivo "dropper" tiene la capacidad de crear un virus e infectar el sistema del usuario al ejecutarse. Cuando un "dropper" es escaneado por un antivirus, generalmente no se detectará un virus, porque el código viral no ha sido creado todavía. El virus se crea en el momento que se ejecuta el "dropper".

atrás A B D E I K M N O P R S T V U W arriba

E

EXPLOIT

Programa o método concreto que saca provecho de una falla o agujero de seguridad de una aplicación o sistema, generalmente para un uso malicioso de dicha vulnerabilidad.

atrás A B D E I K M N O P R S T V U W arriba

I

ICMP (Protocolo de mensajes de control de Internet)

Es una extensión del Protocolo de Internet (IP), y permite generar mensajes de error, paquetes de prueba y mensajes informativos relacionados con IP. Básicamente, se usa para comprobar la existencia de la máquina consultada.

ICQ ("I Seek You", Te busco)

Programa que ofrece un servicio de mensajería en línea a través de Internet, permitiendo hacer saber a otras personas conocidas, que uno está conectado (online). A través de él se pueden intercambiar mensajes y archivos, conversar (chat), establecer conexiones de voz y video, etc.

IMAP (Interactive Mail Access Protocol)

Este protocolo, propuesto por M. Crispin en 1994, supone una mejora de POP3. La principal ventaja es que IMAP permite, no sólo la manipulación de los mensajes en nuestro buzón, sino también la gestión de un conjunto de buzones, distribuidas como carpetas de información. Aunque su potencia y prestaciones son superiores a las de POP3, en la práctica los dos sistemas coexisten. Microsoft Exchange, por ejemplo, actúa como servidor tanto IMAP como POP3, y algunos clientes de correo, como Outlook Express, permiten escoger el protocolo a utilizar.

Ingeniería Social

Se le dice ingeniería social a la acción de engañar a un usuario para que sea él el que actúe, ejecutando un archivo o revelando datos secretos como una clave. Se utiliza la astucia para convencer a una persona a dar por si mismo información acerca de su sistema.

IP SPOOFING

La técnica denominada IP Spoofing permite que un atacante tome la identidad de un host "confiable" (cambiando su dirección IP por la dirección de dicho) y obtenga de este modo accesos no autorizados a otros sistemas. En numerosos sitios (bajo Unix o Linux), existe un archivo denominado .rhosts conteniendo una lista de nombres de hosts que se consideran de confianza. Si un atacante se hace pasar por una de esas direcciones, puede llegar a ejecutar comandos en forma remota o logearse en el mismo sin una contraseña.

IRC (Internet Relay Chat)

Un sistema de conversación multiusuario, donde la gente se reúne en ambientes virtuales llamados "canales", normalmente identificados con temas definidos de conversación, para poder charlar en grupo o en privado. IRC trabaja en arquitectura Cliente/Servidor. El usuario ejecuta un programa cliente (los más conocidos son mIRC y Pirch), el cual se conecta a través de la red (Internet por

ejemplo) con otro programa servidor. La misión del servidor es pasar los mensajes de usuario a usuario.

atrás A B D E I K M N O P R S T V U W arriba

K

Keylogger

Rutina que intercepta todas las pulsaciones realizadas en el teclado, y las guarda en un archivo para obtener datos sensibles como contraseñas, etc. Este archivo puede ser enviado por un troyano a un atacante.

atrás A B D E I K M N O P R S T V U W arriba

M

MAPI (Messaging Application Programming Interface)

Se trata de una interface de programación para aplicaciones que gestionen correo electrónico, servicios de mensajería,
trabajos en grupo, etc.

MUTEX

Un mutex es un objeto utilizado para controlar el acceso a recursos (cualquier tipo de programas y aplicaciones, etc.) y evitar que más de un proceso acceda al mismo tiempo al mismo recurso. Un caso concreto: si un mutex determinado (puede haber uno diferente para cada programa) está en memoria, el programa al que le corresponda ese mutex, asume que existe una sesión anterior de él mismo ejecutándose actualmente, negándose por lo tanto a hacerlo por segunda vez. Esto previene la múltiple carga del programa en memoria.

atrás A B D E I K M N O P R S T V U W arriba

N

Network File System (NFS),

Desarrollado por Sun Microsystems, es un protocolo que permite establecer sistemas de archivos distribuidos
entre múltiples máquinas. Aquellas que estén conectadas a través de NTFS pueden tener acceso a los directorios de cada una de las otras de forma transparente.

atrás A B D E I K M N O P R S T V U W arriba

O

Outgoing Connections

Conexiones salientes

atrás A B D E I K M N O P R S T V U W arriba

P

PING (Packet INternet Groper)

Comando usado para comprobar las conexiones a uno o más hosts remotos. Emplea paquetes ICMP de petición de eco y respuesta de eco para determinar si un sistema IP concreto de una red es funcional. Es útil para diagnosticar fallos IP de la red o del enrutador.

POP3 (Post Office Protocol 3)

Es la tercera versión del protocolo de oficinas de correos en Internet. Permite que los mensajes de correo electrónico sean enviados a un servidor sin que el destinatario esté en ese momento conectado a Internet. El mensaje es almacenado por el servidor (POP3), en el buzón del destinatario, el cuál debe estar registrado como usuario. Cuando este usuario desea leer su correo, sólo debe conectarse a Internet, acceder a su servidor POP3, y si su contraseña es válida, a los contenidos de su casilla.

atrás A B D E I K M N O P R S T V U W arriba

R

RPC (Remote Produce Call)

Desarrollado por Sun Microsystems y utilizado en muchos sistemas Unix, es una interfaz de programación que permite el desarrollo de aplicaciones distribuidas. Mediante un conjunto de funciones, este protocolo permite que los programas llamen a subrutinas que se ejecutan en un sistema remoto, incluyendo códigos de retorno y variables predefinidas para soportar el procesamiendo distribuido.

atrás A B D E I K M N O P R S T V U W arriba

S

SMTP (Simple Mail Transport Protocol)

Protocolo simple de transferencia de correo. Es el protocolo más utilizado en Internet para el envío de correo electrónico. Es el estándar de Internet para el intercambio de correo electrónico. Hace posible que un usuario pueda enviar un e-mail a otros usuarios de la red. A nivel de comunicaciones, SMTP necesita de un canal fiable para llevar a cabo los envíos, por lo que utiliza conexiones TCP.

Sniffer

Rutina o programa que monitorea y analiza el tráfico de una red para detectar problemas o cuellos de botella. Su objetivo es mantener la eficiencia del tráfico de datos. Pero también puede ser usado ilegítimamente para capturar datos en una red.

SNMP (Simple Network Management Protocol)

Es un protocolo de gestión y análisis para interconexión de redes heterogéneas, capaz de proporcionar mensajes de estado y avisar de los problemas detectados.

SPOOFING

"Spoofing" es la falsificación de la dirección IP de origen en los paquetes enviados.

SSL (Secure Socket Layer)

Es un protocolo que utiliza criptografía para cifrar los datos que se intercambian con un servidor seguro. Proporciona privacidad para datos y mensajes, y permite autenticar los datos enviados. Básicamente se utiliza para transmitir información personal o
relacionada con tarjetas de crédito de los usuarios a través de Internet. Las direcciones de páginas Web que utilizan conexiones SSL, comienzan con 'https:' en lugar del estándar 'http:'.

atrás A B D E I K M N O P R S T V U W arriba

T

Telnet

Permite a un programa cliente acceder a los recursos de otro servidor previa autentificación, facilitando nombre de usuario y contraseña. Proporciona una interfaz que permite ejecutar cualquier acción en la máquina remota a la que se está accediendo, tal y como si estuvieramos sentados físicamente delante del servidor.

TFTP (Trivial File Transfer Protocol)

Es un protocolo de transferencia de archivos muy sencillo y sin mecanismos de seguridad. Es similar a FTP, pero en vez de TCP, utiliza UDP como protocolo de transporte.

atrás A B D E I K M N O P R S T V U W arriba

U

UUENCODE

Este es otro protocolo de especificación de codificación de contenidos en mensajes SMTP. Antes de que apareciese MIME, la técnica de UUencode permitía incluir contenidos no textuales en los mensajes mediante la codificación en origen de los citados contenidos binarios transformándolos en caracteres ASCII de 6 bits que se adjuntaban al mensaje. Los contenidos eran interpretados por el emisor y el receptor SMTP como si de texto se tratase y decodificados en destino para recuperar los archivos binarios. Aunque, como es obvio, esta técnica está claramente superada por MIME, aún son abundantes los entornos de correo en los que se utiliza.

atrás A B D E I K M N O P R S T V U W arriba

V

VIRUS PARÁSITO (Parasitic virus)

Se les llama parásitos a los virus que requieren de un portador (o host) para propagarse. Se adjunta a otro programa y se activa cuando ese programa es ejecutado. En el caso de este virus de macro, esta acción se produce porque el virus utiliza como host un
módulo ya existente (Document_Close), y se activa cuando este módulo es ejecutado (por defecto al cerrar un documento).

VIRUS POLIMÓRFICO (Polymorphic).

Este tipo de virus, generalmente encriptado, cambia su código en forma aleatoria, agregando en algunos casos información basura a su código, con la idea de confundir a los antivirus, al obtener un aspecto diferente en cada archivo infectado.

atrás A B D E I K M N O P R S T V U W arriba

W

WSH (Windows Scripting Host).

Es un interprete de Java Script y de Visual Basic Script, que puede ayudar a automatizar varias tareas dentro de Windows, pero también puede ser explotado por virus en dichos lenguajes. Está instalado por defecto en Windows 98 y posteriores

atrás A B D E I K M N O P R S T V U W arriba

http://www26.brinkster.com/itsi/glosario/glosario.htm 28/02/2003