Seguridad informática: Vocabulario

(Basado en MENTOR)

A

AAA

Abreviatura de Autenticación, Autorización y Accounting, sistema en redes IP para controlar qué recursos informáticos tiene acceso el usuario y rastrear la actividad del usuario en la red.

- Autenticación es el proceso de identificación de un individuo, normalmente mediante un nombre de usuario y contraseña. Se basa en la idea de que cada individuo tendrá una información única que le identifique o que le distinga de otros.
- Autorización es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito. La cantidad de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido.
- Accounting es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluso la cantidad de tiempo que permanece conectado, los servicios a los que accede así como los datos transferidos durante la sesión. Los datos registrados durante este proceso se utilizan con fines estadísticos, de planeamiento de capacidad, billing, auditoría y cost allocation.

A menudo los servicios AAA requieren un servidor dedicado. RADIUS es un ejemplo de un servicio AAA.

Acceso Remoto

Utilidad para que un usuario acceda desde su propio PC a otro que esté ubicado remotamente y pueda operar sobre él.

Acreditación Voluntaria del Prestador de Servicios de Certificación(1)

Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se dicta, a petición del prestador al que le beneficie, por el organismo público encargado de su supervisión.

Active-X

Los denominados controles Active-X son componentes adicionales que se pueden incorporar a las páginas web, para dotar a éstas de mayores funcionalidades (animaciones, vídeo, navegación tridimensional, etc.). Escritos en un lenguaje de programación como Visual Basic, C o C++, que no es el propio de las páginas web (HTML) y podrían estar infectados con virus.

Ad Hoc

Una WLAN bajo topología "Ad Hoc" consiste en un grupo de equipos que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso. Las configuraciones "Ad Hoc" son comunicaciones de tipo punto-a-punto. Los equipos inalámbricos necesitan configurar el mismo canal y SSID en modo "Ad Hoc".

Adware

Variante “comercial” del spyware. Se trata de un pequeño trozo de código que tiene como finalidad recolectar datos a efectos de marketing. Es difícil distinguirlo del malware.

AES - Estándar de Cifrado Avanzado

También conocido como "Rijndael", algoritmo de encriptación simétrica de 128 bit desarrollado por los belgas Joan Daemen y Vincent Rijmen. En Octubre de 2000 era seleccionado por el Instituto Nacional de Estándares y Tecnología (NIST) norteamericano como estándar de cifrado reemplazando al hasta entonces estándar DES.

Consulte también: Rijndael: ¡Conózcalo de la manera más sencilla!

Agujero

Una vulnerabilidad en el diseño del software y/o hardware que permite engañar a las medidas de seguridad.

Alias

Nombre diferente por el cual se conoce un virus.

Algoritmo de Encriptación

Codificadores de bloques de bits sobre los que iteran determinadas operaciones tales como sustitución, transposición, suma/producto modular y transformaciones lineales. Cada algoritmo utiliza bloques de distintos tamaños. Ver DES, 3DES y Blowfish.

Amplificador

Produce un incremento significativo en el alcance de la señal de las WLAN. Consta de un receptor de bajo ruido pre-amplificado y un amplificador lineal de salida de radio frecuencia (RF).

Antena

Dispositivo generalmente metálico capaz de radiar y recibir ondas de radio que adapta la entrada/salida del receptor/transmisor del medio. Dependiendo de hacia qué punto emitan la señal podemos encontrarlas direccionales u omnidireccionable.

Appliance Server

Servidores (dedicados a Internet sharing, servicios FTP, e-mail, conexiones VPN, servicios de cortafuegos, de impresora y archivo y también operan como servidores web) que incorporan hardware y software en el mismo producto de modo que todas las aplicaciones se encuentran preinstaladas. El appliance está plug-in dentro de una red existente y puede comenzar a funcionar casi de inmediato con una mínima configuración y mantenimiento.

Análisis Heurístico

Se trata de una análisis adicional que solamente algunos programas anti-virus pueden realizar para detectar virus que hasta ese momento son desconocidos.

Analizador de Comportamiento

Un programa anti-virus emplea una técnica para comprobar si un archivo incorpora los comportamientos habituales de un virus. Un behavior blocker trabaja bajo un conjunto de reglas de funcionamiento que legitima programas bajo las reglas de comportamiento que siguen los virus. Además analiza y determina las tareas y comportamientos que han sido diseñadas para un archivo y averigua si el éste contiene algún virus.

Ancho de Banda

Este término define la cantidad de datos que puede ser enviada en un periodo de tiempo determinado a través de un circuito de comunicación dado.

Anti-Virus

Aplicación cuya finalidad es la detección y eliminación de virus, troyanos y gusanos informáticos.

Appender

Es un virus que inserta una copia de su código al final del archivo de la víctima.

Armouring

Mediante esta técnica el virus impide ser examinado. Para conocer más datos sobre cada uno de los virus, éstos son abiertos como archivos, utilizando programas especiales que permiten descubrir cada una de las líneas de su código. De un virus que utilice esta técnica no se podrá leer su código.

Ataque Activo

Ataque al sistema para insertar información falsa o corromper la ya existente.

Ataques a Passwords

Es un intento de obtener o descifrar una password legítima de usuario. Las medidas de seguridad contra estos ataques es muy limitada consistiendo en una política de passwords, que incluye una longitud mínima, palabras no reconocibles y cambios frecuentes.

Ataque de Diccionario

Método empleado para romper la seguridad de los sistemas basados en passwords (contraseñas) en la que el atacante intenta dar con la clave adecuada probando todas (o casi todas) las palabras posibles o recogidas en un diccionario idiomático. Generalmente no se introducen manualmente las posibles contraseñas sino que se emplean programas especiales que se encargan de ello.

Ataque de Fuerza Bruta

Método empleado para romper la seguridad vía contraseña probando todas las combinaciones posibles de palabras (distinto del ataque de diccionario que prueba palabras aisladas). Un ataque de fuerza bruta teóricamente no puede ser resistido por ningún sistema, siempre y cuando se disponga del tiempo suficiente y del equipo adecuado. Así, las claves lo suficientemente largas (y mejor aún si combinan caracteres alfanuméricos) ponen una limitación física, pero no lógica, al éxito de este tipo de ataque.

Auditoría

Análisis de las condiciones de una instalación informática por un auditor externo e independiente que realiza un dictamen sobre diferentes aspectos. Conjunto de procedimientos y técnicas para evaluar y controlar, total o parcialmente, un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente.

Autenticación

Proceso en el que se da fe de la veracidad y autenticidad de un producto, de unos datos o de un servicio, así como de la fiabilidad y legitimidad de la empresa que los ofrece.

Auto- Encriptación

Capacidad de algunos virus para esconderse de posibles programas anti-virus. Las soluciones anti-virus se encargan de encontrarlos buscando determinadas cadenas de caracteres (firma del virus), identificativas de cada uno de ellos. Para evitar este mecanismo de búsqueda, algunos virus consiguen codificar o cifrar estas cadenas de texto de forma diferente en cada nueva infección. Esto supone que en la nueva infección, el anti-virus no encontrará la cadena que busca para detectar a un virus en concreto, pues éste la habrá modificado. No obstante, existen otros mecanismo alternativos para detectarlos.

Autorización

Proceso por el que se acredita a un sujeto o entidad para realizar una acción determinada.

B

Background

Se dice que una aplicación funciona "en background" cuando está trabajando sin afectar a la actividad del usuario.

Biométrica

Ciencia que estudia las características biológicas del ser humano (el iris, la huella dactilar, la voz, etc.) para su aplicación a la seguridad informática como medio de identificación del usuario.

Blowfish

Blowfish es un codificador simétrico de bloques. Toma una clave de longitud variable, entre 32 y 448 bits.

Bluetooth

Estándar de comunicación inalámbrica que utiliza FHSS, capaz de transmitir a velocidades de 1 Mbps a una distancia de 10 metros entre aparatos (normalmente portátiles, impresoras, monitores, teclados, ratones, etc.) que implementen esta tecnología ya que su FHSS/Hopping Pattern es de 1600 veces por segundo, lo que asegura transmisiones altamente seguras. En cuanto a su implementación Bluetooth utiliza el término piconet.

Un piconet es un grupo de 2 u 8 aparatos que utilizan "Bluetooth" que comparten el mismo rango que es utilizado por un "Hopping Sequence", a su vez cada piconet contiene un aparato principal ("master") que es el encargado de coordinar el "Hopping Pattern" del piconet para que los demás aparatos ("slaves") sean capaces de recibir información.

Bridge

Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar

Bomba de e-mail

Son mensajes de correo electrónico excesivamente largos enviados a la cuenta de correo de un usuario con el propósito de provocar la caída del sistema o evitar que los mensajes verdaderos sean recibidos.

Bomba de Tiempo

Programa que se activa en una determinada fecha.

Bomba Lógica

Programa que se ejecuta cuando existen condiciones especificas para su activación. Los suelen utilizar muchos virus como mecanismo de activación.

Bots

Término utilizado en Internet y que se deriva de la palabra “robot”. Con él se denomina a pequeños trozos de software que tienen la finalidad de actuar de manera independiente en un computador, como un “robot” controlado remotamente.

Bugtraq

Lista de correo de divulgación completa, moderada para la discusión detallada y anuncio de vulnerabilidades en seguridad informática; qué son, cómo explotarlas y cómo solucionarlas.

Búsqueda Exhaustiva de Clave

Consiste en descubrir la clave empleada en un sistema de encriptación, probando todas las posibilidades.

C

Cadena

Una consecución de caracteres de texto, dígitos numéricos, signos de puntuación o espacios en blanco consecutivos. Alguna de las técnicas empleadas por los anti-virus para la detección de virus es buscar determinadas cadenas de texto (o código) que éstos incluyen de manera frecuente.

Centrino

Tecnología móvil desarrollada por Intel compuesta por un procesador Pentium M, chipset 855 y conectividad inalámbrica integrada.

CHAP - Challenge Handshake Authentication Protocol

Protocolo de autenticación para servidores PPP donde la contraseña no sólo se exige al empezar la conexión sino también durante la conexión, mucho más seguro que el PAP. Una vez efectuado el enlace, el servidor envía un mensaje de desafío al solicitante de la conexión, el cual responde con un valor hash que será comparado por el servidor con sus cálculos del valor hash esperado. Si el valor coincide, la autenticación prospera, de lo contrario, finaliza. En cualquier momento el servidor puede solicitar un mensaje de desafío. Debido a que los identificadores cambian frecuentemente y por que la autenticación puede ser solicitada en cualquier momento.

Cliente Inalámbrico

Todo dispositivo susceptible de integrarse en una red wireless como PDAs, portátiles, cámaras inalámbricas, impresoras, etc.

Certificado Digital

Es la certificación electrónica que emiten las Autoridades Certificadoras donde constan unos datos de verificación de firma a un signatario y confirma su identidad. Entre los datos figuran la fecha de emisión y la fecha de caducidad, la clave pública y la firma digital del emisor. Los Certificados Digitales siguen las estipulaciones del estándar X.509. Este documento sirve para vincular una clave pública a una entidad o persona

Consulte también: FIRMA DIGITAL Y CERTIFICADOS DIGITALES

Certificado Reconocido

Es el certificado que contiene la información descrita en el artículo 8 y es expedido por un prestador de servicios de certificación que cumple los requisitos numerados en el artículo 12.

Chequeador de Integridad

Es un programa que determina si otro programa ha sido alterado. Para que una infección de virus ocurra, el código ejecutable necesita haber sido alterado por un virus. Un chequeador de integridad investiga tales cambios y los marca como sospechosos.

Checksum Criptográfico

Checksum calculado mediante la utilización de un algoritmo con base criptográfica. Es imposible cambiar unos datos sin que el checksum criptográfico cambie. Ver también Checksummer.

CheckSummer

Herramienta que calcula un único número asociado a determinados archivos que habitualmente no cambian para protegerlos. CheckSummer recalculará periódicamente dicho número y si se detecta que ha cambiado, será un indicio de infección.

Clave de Encriptación

Serie de números utilizados por un algoritmo de encriptación para transformar plaintext (texto sin encriptar que se puede leer directamente) en datos ciphertext (encriptados o cifrados) y viceversa.

Clave de Registro

El registro (Registry) de Windows es un elemento en el que se guardan las especificaciones de configuración del PC mediante claves. Estas claves cambiarán de valor y/o se crearán cuando se instalen nuevos programas o se altere la configuración del sistema. Los virus pueden modificar estas claves para producir efectos dañinos.

Codificador por Bloques

Ciencia que estudia las características biológicas del ser humano (el iris, la huella dactilar, la voz, etc.) para su aplicación a la seguridad informática como medio de identificación del usuario.

Código Malicioso

Es un término genérico utilizado para describir el software malicioso tales como: virus, troyanos, etc.

COMPSEC

Abreviatura de COMPuter SECurity (Seguridad Informática).

Confidencialidad

Calidad de secreto, que no puede ser revelado a terceros o personas no autorizadas.

Control de Accesos

Se utiliza para restringir el acceso a determinadas áreas del PC, de la red, mainframes, Internet, ftp, web, etc. El permiso o la denegación de acceso puede realizarse en función de la dirección IP, el nombre de dominio, nombre de usuario y password, certificados del clientes, protocolos de seguridad de redes, etc.

Copia de Seguridad

Es una copia de todos los datos originales contenidos en redes y PC's que puede ser utilizada en caso de que éstos se destruyan por diversas causas.

Cortafuegos

Software y hardware de seguridad encargado de chequear y bloquear el tráfico de la red. Sistema que se coloca entre una red e Internet para asegurar que todas las comunicaciones se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, anti-virus, autenticación, etc.

Cracker

Persona que elimina las protecciones lógicas y físicas de los sistemas para acceder a los mismos sin autorización y generalmente con malas intenciones.

Criptoanálisis

Estudio de un sistema de encriptación con la intención de detectar cualquier punto débil dentro de su algoritmo clave.

Criptología

Ciencia que estudia el arte de crear y utilizar sistemas de encriptación.

Crosstalk

Ruido (interferencia) que fluye entre los cables de comunicación o dispositivos.

D

Datos de Carácter Personal

Cualquier información concerniente a personas físicas identificadas o identificables.

Datos de Creación de Firma Electrónica

Son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma (electrónica).

Datos de Verificación de Firma Electrónica

Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

Delito Informático

Delito cometido utilizando un PC; también se entiende por delito informático cualquier ataque contra un sistema de PC's.

Denegación de Servicio (DoS)

O ataque DoS. Se trata de una ofensiva diseñada específicamente para impedir el funcionamiento normal de un sistema y por consiguiente impedir el acceso legal a los sistemas para usuarios autorizados.

DES

Algoritmo que codifica los textos haciendo bloques de datos de 64 bits y utilizando una clave de 56 bits. Existe otra modalidad más avanzada denominada 3DES que utiliza el algoritmo DES tres veces. Hay varios tipos de algoritmo 3DES en función del número de claves que utilicen y de la longitud de éstas.

Desbordamiento de Búfer

Error de software que se produce cuando se copia una cantidad más grande de datos sobre un área más pequeña sin interrumpir la operación sobre-escribiendo otras zonas de datos no previstas. En algunas ocasiones eso puede suponer la posibilidad de alterar el flujo del programa pudiendo hacer que este realice operaciones no previstas. Si el programa que tiene el error en cuestión tiene privilegios especiales se convierte

además en un fallo de seguridad. El código copiado especialmente preparado para obtener los privilegios del programa atacado se llama shellcode.

Desencriptar

Proceso de transformación de ciphertext - texto encriptado o cifrado - a plaintext. Es la acción inversa a encriptar.

Desinfección

Acción que realizan los programas anti-virus cuando, tras detectar un virus, lo eliminan del sistema y, en la medida de lo posible, recuperan o restauran la información infectada.

DHA

Llamado el “Asesino Silencioso”. Este ataque consiste en el envío masivo de emails a un dominio determinado con el fin de “cosechar” y recolectar direcciones válidas de emails, para ser incorporadas a las listas de spam. En Inglés: Directory Harvest Attack.

Dialback

Rasgo de seguridad que asegura que las personas sin autorización no conecten con módems a los que no deben tener acceso. Cuando se pide una conexión, el sistema verifica el nombre del usuario para validarlo, e inicia una rellamada al número asociado con ese nombre de usuario.

Dialer

Programa que permite cambiar el número de acceso telefónico automáticamente, de acuerdo a la situación geográfica del usuario. Estos códigos (que se descargan de sites a veces sin percatarnos) toman el control sólo de la conexión telefónica vía módem, desviando las llamadas normales que efectúas a través de tu proveedor hacia una número del tipo 908, 906, etc., números de tarifa especial y bastante cara por lo general. Últimamente se han detectado un aumento de incidentes relativos a "dialers porno" que permiten visualizar páginas pornográficas de forma gratuita pero que sin embargo se pagan cuando llega la escandalosa factura telefónica.

Dispositivo Móvil (DM)

Ya sea Tarjeta PCMCIA, USB, PCI (Slot de un PC de sobremesa), Centrino, que sustituyen a las tarjetas de red

Su función es la de recibir/enviar información desde la estación en que están instaladas (portátiles, PDAs, móviles, cámaras, impresoras,...).

DSSS - Espectro Amplio mediante Secuencia Directa

A diferencia de la técnica de transmisión de Espectro Amplio (Spread Spectrum) FHSS, DSSS no precisa enviar la información a través de varias frecuencias sino mediante transmisores; cada transmisor agrega bits adicionales a los paquetes de información y únicamente el receptor que conoce el algoritmo de estos bits adicionales es capaz de descifrar los datos .Es precisamente el uso de estos bits adicionales lo que permite a DSSS transmitir información a 10Mbps y una distancia máxima entre transmisores de 150 metros. Un estándar que utiliza DSSS es IEEE 802.11b.

Dispositivo de Creación de Firma Electrónica

Es un programa o un aparato informático que sirve para aplicar los datos de creación de firma (electrónica).

Dispositivo de Verificación de Firma Electrónica

Es un programa o un aparato informático que sirve para aplicar los datos de verificación de firma (electrónica).

Dispositivo Seguro de Creación de Firma Electrónica

Es un dispositivo de creación de firma que cumple los requisitos establecidos en el artículo 19.

Dongle

Hardware de seguridad que se debe conectar al sistema informático antes de que se ejecute una determinada aplicación; previene las copias ilegales de los programas informáticos.

Dropper

Usado como portador de virus, un dropper es un programa ejecutable que instala el virus en memoria, en el disco o en un archivo (aunque un dropper por sí mismo no tiene capacidades de infección ni de replicación).

E

EAP - Protocolo de Autenticación Extensible

Extensión del Protocolo punto a punto (PPP). Proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un sólo uso, autenticación por clave pública mediante tarjetas inteligentes, certificados y otros. Junto con los métodos de autenticación EAP de alto nivel, es un componente tecnológico crítico para las conexiones seguras a través de una red privada virtual (VPN), puesto que ofrece mayor seguridad frente a ataques físicos o de diccionario y de investigación de contraseñas, que otros métodos de autenticación, como CHAP.

Echelon

Sistema internacional de interceptación mediante satélites de las telecomunicaciones iniciado como proyecto en 1947 e implementado en 1960. Desde su nacimiento en plena Guerra Fría ha evolucionando con los tiempos incluyendo actualmente actividades de espionaje industrial. Su dirección está al cargo de la NSA (National Security Agency, Estados Unidos) y de la GCHQ (Government Communications Headquarters, Gran Bretaña) aunque también tiene estaciones de control en Australia, Canadá y Nueva Zelanda.

Encriptación

Proceso para transformar la información escrita en plaintext a ciphertext.

Encriptación Asimétrica

Encriptación que permite que la clave utilizada para encriptar sea diferente a la utilizada para desencriptar. El algoritmo de encriptación asimétrico más difundido es RSA.

Encriptación de Archivos

Transformación de los contenidos plaintext de un archivo (texto sin cifrar) a un formato ininteligible mediante algún sistema de encriptación.

En el Terreno

Clasificación utilizada por la organización Wildlist que recoge todos aquellos virus sobre los que más de una persona ha notificado alguna incidencia.

En el Zoo

Describe un virus que únicamente existe dentro de un entorno de investigación.

Engaño

No se trata de virus, sino de falsos mensajes de alarma (bromas o engaños) sobre virus que no existen. Estos se envían por correo electrónico con la intención de extender falsos rumores por Internet. Los mensajes no suelen estar fechados, con lo que se pretende que los mensajes siempre parezcan recientes. En ocasiones, los Hoax pretenden engañar a los usuarios mediante el uso de palabras técnicas. , mensajes que simulan a los reales, alertas de nuevos virus, anuncios de nuevas soluciones, cadena de correos a reenviar,..., etc. Por otra parte, suele ser frecuente la inclusión del nombre de ciertas agencias de prensa (CBS...) en el encabezamiento de estos mensajes. Con todo esto se pretende dar un aspecto verídico a los mensajes.

Escáner

Programa que busca virus en la memoria del PC o en los archivos.

Escáner bajo Demanda

Programa escáner antivirus que el usuario ejecuta manualmente cuando lo estima conveniente (Ver Resident Scanner y Heuristic Scanner).

Escáner Heurístico

Programa escáner antivirus que busca virus nuevos y desconocidos.

Escáner Residente

Programa escáner antivirus que está buscando virus recursivamente en background.

Estándar

Norma que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones, protocolos, etc.

Ethernet

Arquitectura de red de área local desarrollada en 1976 por Xerox Corp. en cooperación con DEC e Intelque. Emplea una topología lineal (bus) o de estrella, o lo que es lo mismo, los datos pasan en todo momento por todos los puntos de conexión (a 10 Mbps) utilizando el método de acceso por detección de portadora con detección de colisiones (CSMA/CD). Una nueva versión denominada 100Base-T (o Fast Ethernet) soporta velocidades de 100 Mbps. Y la más reciente, Gigabit Ethernet soporta 1 Gb por segundo.

Excepciones

Una alternativa a la búsqueda de cadenas es la búsqueda de excepciones. Cuando un virus utiliza una determinada cadena para realizar una infección pero en la siguiente emplea otra distinta, es difícil detectarlo mediante la búsqueda de cadenas. En ese caso, lo que el programa anti-virus puede chequear es el cambio en las cadenas (excepciones).

Explotar

Método de utilizar un bug o fallo para penetrar en un sistema.

F

Fallo

O error en un programa. Cuando uno de ellos tiene errores, se dice que tiene Bugs. Como los virus son programas, también pueden contener bugs. Esto implicaría que, si el virus debe realizar determinadas acciones, podría no realizarlas, o no hacerlo bajo las condiciones que su programador ha establecido inicialmente.

Falso Negativo

Evento que se da como inexistente cuando realmente si existe, por ejemplo, decir que un sistema está limpio de virus cuando realmente está infectado.

Falso Positivo

Evento que se da como existente cuando realmente no existe, por ejemplo, decir que un sistema está infectado de virus cuando realmente está limpio.

FAST - Flexible Authentication Secure Tunneling

Protocolo de seguridad WLAN del tipo EAP. Desarrollado por Cisco y presentado a la IETF como borrador a principios de 2004. Impide los denominados ataques de diccionario por fuerza bruta enviando una autenticación de contraseña entre el cliente WLAN y el punto de acceso inalámbrico a través de un túnel cifrado seguro. Elimina la necesidad de instalar servidores separados para tratar los certificados digitales empleados en otro sistema de seguridad WLAN (como el PEAP).

FHSS - Espectro Amplio mediante Saltos de Frecuencia

Primer desarrollo de la técnica de transmisión del Espectro Amplio (Spread Spectrum) que, al igual que Ethernet, divide los datos en paquetes de información pero que, por motivos de seguridad, para dificultar su interceptación por terceros, los envía a través de varias frecuencias (Hopping Pattern) seleccionadas al azar y que no se superponen entre sí. Para llevar a cabo la transmisión además es necesario que tanto el aparato emisor como el receptor coordinen este "Hopping Pattern". El estándar IEEE 802.11 utiliza FHSS, aunque hoy en día la tecnología que sobresale utilizando FHSS es Bluetooth.

Fichero

Todo conjunto organizado de datos de carácter personal, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso.

Filtering

Proceso mediante el cual un puente o conmutador Ethernet lee el contenido del paquete y descubre que éste no necesita volver a ser enviado, por lo que lo desprecia. La velocidad de filtrado es la velocidad a la que un dispositivo puede recibir paquetes y desecharlos sin ninguna pérdida de paquetes entrantes o demoras en su procesado.

Filtros Anti-Spam

Son herramientas para filtrar el spam o correo basura no solicitado en los programas de correo.

Firma Electrónica o Firma Digital

El conjunto de datos, en forma electrónica, anexos a otros datos del mismo tipo o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge y que impide la apropiación o daño de su contenido por parte de terceros. Se obtiene cifrando la huella digital de un mensaje con la clave privada del remitente. Garantiza la identidad del firmante y que el texto no se modificó.

Consulte también: FIRMA DIGITAL Y CERTIFICADOS DIGITALES

Firma Electrónica Avanzada

Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

Firmware

Software (programas o datos) escritos en la memoria de sólo lectura (ROM). El firmware es un combinación de software y hardware. ROMs, PROMs e EPROMs que tienen datos o programas grabados dentro son firmware.

Framing

División de datos para su transmisión en grupos de bits a los que se les añade una cabecera y un código de verificación para formar una trama.

FTP - Protocolo de Transferencia de Archivos

Protocolo de transferencia de archivos que permite a los usuarios de gestores de correo la captura de documentos, archivos, programas y otros datos contenidos en carpetas existentes en cualquier lugar de Internet sin tener que proporcionar nombre de usuario y contraseña. Solamente se puede acceder a los archivos públicos situados en el sistema remoto al que se accede.

G

Galleta

Rastro que el servidor de un sitio web deja en nuestro PC cuando lo visitamos por primera vez; cada vez que volvemos a dicho sitio, la señal se actualiza, dando información al servidor de nuestro paso por la página. Con estas señales, los servidores pueden saber por dónde navegamos, cuáles son nuestros intereses, etc.

Gateway

Dispositivo que funciona como puerta de enlace entre Internet y redes inalámbricas.

GPS - Sistema de Posicionamiento Global

Sistema de navegación por satélite con cobertura global y continua que ofrece de forma rápida y temporalmente bastante precisa una posición geográfica de un elemento. El primer satélite para esta técnica de seguimiento se lanzó en 1978, pero sin embargo el sistema no estuvo operativo hasta 1992 y fue desarrollado por las fuerzas aéreas de los EE.UU.

Gestión de Claves

Proceso para generar, transportar, almacenar y destruir claves de encriptación de modo seguro.

Gusanos de Internet Relay Chat

Infectan solamente a usuarios del software MIRC para acceder a los canales IRC (Internet Relay Chat). El gusano se aprovecha de cualquier desperfecto en el diseño de seguridad del software mIRC PARA sobre-escribir el archivo Script omitido (Script.ini) cuando los archivos son transferidos utilizando el protocolo DCC.

H

HASH

Un valor hash, también conocido como "message digest", es un número generado a partir de una cadena de texto. El hash es sustancialmente más pequeño que el texto en sí, y es generado por una fórmula de tal forma que sea poco probable que algún otro texto produzca el mismo valor. Los hashes juegan un papel crucial en la seguridad donde se emplean para asegurar que los mensajes transmitidos no han sido manipulados. El emisor genera un hash del mensaje, lo encripta y lo envía con el propio mensaje. El receptor luego decodifica ambos, produce otro hash del mensaje recibido y compara los dos hashes, si coinciden, existe una probabilidad muy elevada de que el mensaje recibido no haya sufrido cambios desde su origen.

Hacking Tools

Herramientas que usan los principiantes para asaltar ordenadores.

Honeypot

(tarros de miel en castellano). Un servidor diseñado para ser atacado y que actúa como señuelo para hackers los cuales piensan que se conectan a un verdadero sistema informático y actúan sobre él, permitiendo así a su propietario monitorizar la actividad del "pirata" con distintos fines: estudiar su comportamiento, fijar los puntos débiles de su red, etc.

Consulte también: ¿QUE SON LOS HONEYPOTS?

Hot Spot (Punto Caliente)

Punto de Acceso generalmente localizado en lugares con gran tráfico de público (estaciones, aeropuertos, hoteles, etc.) que proporciona servicios de red inalámbrico de banda ancha a visitantes móviles.

I

IEEE - Instituto de Ingenieros Eléctricos y Electrónicos

Formado a fecha de julio de 2003 por 377.000 miembros en 150 países. Cuenta con 900 estándares activos y 700 en desarrollo (http://www.ieee.org).

IETF - The Internet Engineering Task Force

Grupo principal auto-organizado comprometido en el desarrollo de nuevas especificaciones estándares para Internet (http://www.ietf.org).

Infraestructura

Topología de una red inalámbrica que consta de dos elementos básicos: estaciones cliente wireless y puntos de acceso.

IPsec - IP Security

Conjunto de protocolos desarrollado por el IETF para soportar intercambio seguros de paquetes a nivel IP donde el emisor y receptor deben compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtuales (VPNs), soporta dos modos de encriptación: Transporte y Túnel. El primero sólo encripta la parte relativa a los de datos (payload) de cada paquete, pero deja la cabecera intacta. Por su parte, el modo Túnel, más seguro, encripta todo.

Infección

Acción que realiza un virus al introducirse en un sistema, empleando cualquier método, para poder ejecutar sus acciones dañinas y su carga destructiva, o bien simplemente al haber conseguido acceder al mismo.

Integridad de Archivos

Técnicas utilizadas para conseguir archivos de backup correctos de modo que se pueda recurrir a ellos en caso de tener que recuperar datos críticos después de que los datos originales se contaminen debido a una acción accidental o provocada (por ejemplo, un virus).

ISO 17999

Estándar para la gestión de la seguridad de la información

Consulte también: ISO 17799: La gestión de la seguridad

L

LAN - Red de Área Local

Red informática que cubre que área relativamente pequeña (generalmente un edificio o grupo de edificios). La mayoría conecta puestos de trabajo (workstations) y PCs. Cada nodo (ordenador individual) tiene su propia CPU y programas pero también puede acceder a los datos y dispositivos de otros nodos así como comunicarse con éstos (e-mail)... Sus características son: Topología en anillo o lineal, Arquitectura punto a punto o cliente/servidor, Conexión por fibra óptica, cable coaxial o entrelazado, ondas de radio.

Lammers

Mirones, aficionados a hackers que suelen ser muy peligrosos porque no controlan la información que son capaces de manejar.

LDAP - Protocolo de Acceso Ligero a Directorio

Protocolo para el acceso a directorios jerárquicos de información. Basado en el estándar X.500, pero significativamente más simple por lo que también se le denomina x.500-lite, se diferencia de éste porque soporta TCP/IP, necesario para cualquier tipo de acceso a Internet. Aunque no está ampliamente extendido, debería poderse implementar en la práctica mayoría de aplicaciones que se ejecutan virtualmente sobre plataformas informáticas para obtener información de directorios tales como direcciones de correo y llaves públicas. Ya que es un protocolo abierto, no afecta el tipo de servidor en el que se aloje el directorio.

LEAP - Lightweight Extensible Authentication Protocol

Protocolo del tipo EAP patentado por Cisco basado en nombre de usuario y contraseña que se envía sin protección. Esta metodología descuida la protección de las credenciales durante la fase de autenticación del usuario con el servidor.

M

MAC - Dirección de Control de Acceso a Medios

Dirección hardware de 6 bytes (48 bits) única que identifica únicamente cada nodo (tarjeta) de una red y se representa en notación hexademinal. En redes IEEE 802, la capa Data Link Control (DLC) del Modelo de Referencia OSI se divide en dos sub-capas: Logical Link Control (LLC) y Media Access Control (MAC), la cual se conecta directamente con el medio de red. Consecuentemente, cada tipo de medio de red diferente requiere una capa MAC diferente. En redes que no siguen los estándares IEEE 802 pero sí el modelo OSI , la dirección del nodo se denomina Data Link control (DLC) address.

Mbps (Megabits por segundo)

Unidad de medida de la capacidad de transmisión por una línea de telecomunicación. Cada megabit está formado por 1.048.576 bits.

MD5

Algoritmo de encriptación de 128-bits del tipo EAP creado en 1991 por el profesor Ronald Rivest para RSA Data Security, Inc. empleado para crear firmas digitales. Emplea funciones hash unidireccionales, es decir, que toma un mensaje y lo convierte en una cadena fija de dígitos. Cuando se utiliza una función hash de una dirección, se puede comparar un valor hash frente a otro que esté decodificado con una llave pública para verificar la integridad del mensaje. Basado en Nombre de Usuario y Contraseña, EL PRIMERO SE ENVÍA sin protección. Sólo autentica el cliente frente al servidor, no el servidor frente al cliente.

MHz (Megahercio)

Unidad empleada para medir la "velocidad bruta" de los microprocesadores equivalente a un millón de hertzios.

MS-CHAP - Protocolo de Autenticación por Desafío Mutuo

Protocolo de autenticación utilizado por el acceso remoto de Microsoft y conexiones de red y de acceso telefónico. Con CHAP los clientes de acceso remoto pueden enviar de forma segura sus credenciales de autenticación a un servidor de acceso remoto. Microsoft ha creado una variante de CHAP específica de Windows denominada MS-CHAP. Challenge Handshake Authentication Protocol se llama también CHAP.

N

NCSC - Centro Nacional de Seguridad Informática

Institución de EEUU responsable de fomentar el desarrollo de sistemas informáticos seguros y de su implantación en las oficinas del gobierno para la clasificación de la información.

O

802.11

- 802.11 -- Familia de estándares desarrollados por la IEEE para tecnologías de red inalámbricas (wireless). Permite la conexión de dispositivos móviles (lap-top, PDA, teléfonos celulares a una red cableada, por medio de un Punto de Acceso (Access Point). La conexión se realiza a través de ondas de Radio Frecuencia. Originalmente ofrecía una velocidad de transmisión de 1 o 2 Mbps en la banda de frecuencia de 2.4 GHz. Se le conoce popularmente como WIFI. Tiene un área de cobertura aproximada de 100 ms.

- 802.11a -- Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 54 Mbps en una banda de 5 GHz. Utiliza la tecnología OFDM (Orthogonal Frecuency División Multiplexing. Esta banda de 5GHz no se pudo utilizar en muchos países, al comienzo, por estar asignada a las fuerzas y organismos de seguridad.

- 802.11b Estándar de conexión wireless que suministra una velocidad de transmisión de 11 Mbps en una banda de 2.4 GHz. Utiliza la tecnología DSSS (Direct Sequencing Spread). La mayoría de los equipos utilizados en la actualidad son de esta tecnología. Fue ratificado en 1999. No es compatible con el 802.11a pues funciona en otra banda de frecuencia.

- 802.11e -- Estándar en elaboración desde Junio de 2003, destinado a mejorar la calidad de servicio en Wi-Fi (QoS – Quality of Service). Es de suma importancia para la transmisión de voz y video.

- 802.11g -- Estándar de conexión wireless que suministra una velocidad de transmisión de 54 Mbps en una banda de frecuencia de 2.4 GHz. Se basa en la tecnología OFDM, al igual que el estándar 802.11a. Fue ratificado en Junio de 2003. Una de sus ventajas es la compatibilidad con el estándar 802.11b.

- 802.11i -- Estándar de seguridad para redes wifi aprobado a mediados de 2004. En el se define al protocolo de encriptación WPA2 basado en el algoritmo AES.

- 802.11n -- Estándar en elaboración desde Enero 2004. Tiene como objetivo conseguir mayores velocidades de transmisión para Wi-Fi. Estas serán superiores a 100 Mbps. Hay 2 propuestas distintas. En 2006 se aprobará una de las dos. La de TGn Sync o la WWiSE.

- 802.16 -- Estándar de transmisión wireless conocido como WIMAX (Worldwide Interoperability for Microwave Access). Es compatible con WIFI. Se originó en Abril de 2002 con la finalidad de cubrir inalámbricamente distancias de hasta 50 Km. La tecnología permite alcanzar velocidades de transmisión de hasta 70 Mbits en una banda de frecuencias entre 10 GHz y 66 GHz. La interoperatividad es certificada por el WIMAX FORUM (www.wimaxforum.org).

- 802.16d -- Estándar de transmisión wireless (WIMAX*) que suministra una velocidad de entre 300 K y 2 Mbps en una banda de frecuencia de 2GHz a 11GHz. Ratificado a finales de 2004. Se utiliza para el cubrimiento de la “primer milla”.

  WIMAX: Técnica de modulación FDM (empleada por el 802.11a y el 802.11g) para transmitir grandes cantidades de datos digitales a través de ondas de radio. OFDM divide la señal de radio en múltiples subseñales más pequeñas que luego serán transmitidas de manera simultánea en diferentes frecuencias al receptor. OFDM reduce la cantidad de ruido (crosstalk) en las transmisiones de señal.

- 802.1x -- Estándar de seguridad para redes inalámbricas y cableadas. Se apoya en el protocolo EAP y establece la necesidad de autenticar y autorizar a cada usuario que se conecte a una red.

OFDM - Orthogonal Frequency Division Multiplexing

Técnica de modulación FDM (empleada por el 802.11a wi-fi) para transmitir grandes cantidades de datos digitales a través de ondas de radio. OFDM divide la señal de radio en múltiples subseñales más pequeñas que luego serán transmitidas de manera simultánea en diferentes frecuencias al receptor. OFDM reduce la cantidad de ruido (crosstalk) en las transmisiones de señal.

P

PAP - Protocolo de Autenticación de Claves

El método más básico de autenticación, en el cual el nombre de usuario y la contraseña (clave) se transmiten a través de una red y se compara con una tabla de parejas nombre-clave, la no coincidencia provocará la desconexión. Típicamente, las contraseñas almacenadas en la tabla se encuentran encriptadas. El principal defecto de PAP es que tanto el nombre de usuario como la clave se transmiten sin codificar, a diferencia de sistema CHAP.

Payload

Efectos destructivos, nocivos o molestos que cualquier virus puede producir cuando ya ha tenido lugar su infección, además de los efectos secundarios de dicha infección (cambios en la configuración del sistema, reenvío de e-mail, ejecución del virus en el arranque del sistema o de Windows,...).

PEAP - Protected Extensible Authentication Protocol

Protocolo del tipo EAP desarrollado conjuntamente por Microsoft, RSA Security y Cisco para la transmisión datos autenticados, incluso claves, sobre redes inalámbricas 802.11. Autentica clientes de red wi-fi empleando sólo certificados del lado servidor creando un túnel SSL/TLS encriptado entre el cliente y el servidor de autenticación. El túnel luego protege el resto de intercambios de autenticación de usuario.

Phishing

Técnica en auge que consiste en atraer mediante engaños a un usuario hacia un sitio web fraudulento donde se le insta a introducir datos privados, generalmente números de tarjetas de crédito, nombres y passwords de las cuentas, números de seguridad social, etc. Uno de los métodos más comunes para hacer llegar a la "víctima" a la página falsa es a través de un e-mail que aparenta provenir de un emisor de confianza (banco, entidad financiera u otro) en el que se introduce un enlace a una web en la que el "phiser" ha reemplazado en la barra de dirección del navegador la verdadera URL para que parezca una legal.

Una de las consecuencias más peligrosas de este fraude es que la barra "falsa" queda en memoria aún después de salir de la misma pudiendo hacer un seguimiento de todos los sitios que visitamos posteriormente y también el atacante puede observar todo lo que se envía y recibe a través del navegador hasta que éste sea cerrado.

Una manera para el usuario de descubrir el engaño es que no se muestra la imagen del candado en la parte inferior del navegador que indica que la navegación es segura.

PIN - Personal Identifier Number

Número generalmente de 4 dígitos que actúa como contraseña de acceso para el uso de una diversidad de servicios: cajeros automáticos, conexión de teléfono móvil, etc..

Pirata Informático

Persona que accede a un sistema informático sin autorización para "cotillear", ver su funcionamiento interno y explotar vulnerabilidades. Este término se suele utilizar indistintamente con el término cracker (intruso), pero supuestamente hacker no implica necesariamente malas intenciones, mientras que cracker sí.

PKI - Infraestructura de Clave Pública

Sistema de certificados digitales, Autoridades Certificadores y otras entidades de registro que verifican y autentican la validez de cada una de las partes implicadas en una transacción vía Internet. Los estándares de PKI siguen evolucionando, aunque se estén implementando de forma generalizada como elemento necesario del comercio electrónico. La infraestructura de claves públicas se llama también PKI.

Polimorfismo

Característica que presentan algunos virus consistente en que su código no siga un patrón fijo de caracteres de modo que es muy difícil detectarlo.

Prestador de Servicios de Certificación

Es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

Procedimiento de Disociación

Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

Producto de Firma Electrónica

Es un programa o aparato informático o sus componentes específicos, destinados a ser utilizados para la prestación de servicios de firma electrónica por el prestador de servicios de certificación o para la creación o verificación de firma electrónica.

Protección contra copiado

Método para impedir hacer copias de programas de software. Es una forma de evitar el robo de aplicaciones informáticas.

Protección de datos

Conjunto de técnicas utilizadas para preservar la confidencialidad, la integridad y la disponibilidad de la información.

Protocolo

Estándar establecido. En lo referente a conectividad de redes, el empleo de un protocolo se realiza para direccionar y asegurar la entrega de paquetes a través de la red.

Puerta Trasera

No se trata de un virus, sino de una herramienta de administración remota. Si es instalada por un hacker tiene la capacidad de dar a un atacante privilegios como administrador. Puede incluso buscar passwords y datos confidenciales y enviarlos vía mail a un área remota.

Consulte también: PUERTAS TRASERAS O "BACKDOORS

Punto de Acceso (PA)

Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

R

RADIUS - Remote Authentication Dial-In User Service

Sistema de autenticación y accounting empleado por la mayoría de proveedores de servicios de Internet (ISPs) si bien no se trata de un estándar oficial. Cuando el usuario realiza una conexión a su ISP debe introducir su nombre de usuario y contraseña, información que pasa a un servidor RADIUS que chequeará que la información es correcta y autorizará el acceso al sistema del ISP si es así.

RAS - Servidor de Acceso Remoto

Servidor dedicado a la gestión de usuarios que no están en una red pero necesitan acceder remotamente a ésta. Permite a los usuarios, una vez autenticados, obtener acceso a los archivos y servicios de impresora de una LAN desde una localización remota.

Router

Dispositivo que transmite paquetes de datos a lo largo de una red. Un router está conectado al menos a dos redes, generalmente dos LANs o WANs o una LAN y la red de un ISP. Los routers emplean cabeceras y tablas de comparación para determinar el mejor camino para enviar los paquetes a su destino, y emplean protocolos como el ICMP para comunicarse con otros y configurar la mejor ruta entre varios hosts.

Roaming

En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Punto de Acceso a otra sin interrumpir el servicio o pérdida de conectividad

S

Sector de Arranque

Todo disco tiene un sector de arranque que el PC lee cuando se enciende. Este sector contiene todos los códigos necesarios para cargar los archivos de sistema DOS.

Sector de Partición

Todo disco duro o disquete tiene un sector de partición que es leído después de que se ha arrancado el PC. Contiene datos sobre el disco tales como el número de sectores de cada partición y la ubicación de las particiones.

Sectores Defectuosos

Aquellos que, tras formatear el disco duro en MS-DOS, se revelan inutilizables. Algunos virus tienen la capacidad de renombrar sectores útiles como "defectuosos" para almacenar en ellos su código, de modo que el usuario y el sistema operativo no accedan a él y garantizando así la infección del PC.

Servidor de Autenticación

Servidores que gestionan las bases de datos de todos los usuarios de una red y sus respectivas contraseñas para acceder a determinados recursos. Permiten o deniegan el acceso en función de los derechos atribuidos.

Shellcode

En términos underground, shellcode son una serie de órdenes de ensamblador que, beneficiándose de fallos informáticos, que ejecutan un código después de sobrescribir la dirección de retorno (ret) de un programa o función mediante un desbordamiento (overflow) u otro método válido. Si el atacante consigue insertar su shellcode sobre el ret, cuando se produzca el desbordamiento y el salto, se ejecutará sus órdenes.

Signatario

Persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

Sistema de Encriptación

Colección completa de algoritmos que tienen su propia denominación en función de las claves que utilizan para encriptar. (Ver Blowfish y DES).

Sobrepasamiento

Técnica diseñada para impedir que las aplicaciones anti-virus trabajen correctamente.

Spyware

Pequeñas aplicaciones cuyo fin es el de obtener información, sin que el usuario se de cuenta, de tipo comercial. Generalmente se encuentran dentro de aplicaciones gratuitas en Internet.

Stealth

Característica que tienen los virus para pasar inadvertidos ante el usuario al que infectan.

Tarjeta Inteligente

Pequeño dispositivo electrónico del tamaño de una tarjeta de crédito que contiene memoria digital y posiblemente un circuito integrado, llamándose entonces Integrated Circuit Cards (ICCs). Sus usos son variados: para almacenar historiales médicos, como monedero digital, para generar IDs (similar a un Token). Para utilizarla, y bien capturar los datos en ella almacenada o bien añadirlos, es necesario un pequeño lector especial para estos dispositivos.

Consulte también: SMART CARDS: TARJETAS DE SEGURIDAD POLIVALENTES

Sniffers

Programa y/o dispositivo que monitoriza la circulación de datos a través de una red. Los sniffers pueden emplearse tanto con funciones legítimas de gestión de red como para el robo de información. Los sniffers no autorizados pueden ser extremadamente peligrosos para la seguridad de una red ya que virtualmente es casi imposible detectarlos y pueden ser emplazados en cualquier lugar, convirtiéndolos en un arma indispensable de muchos piratas informáticos. Algunas herramientas sniffers conocidas son: WepCrack, Airsnort o NetStumbler, entre otras...

SPAM

También conocido como junk-mail o correo basura, consiste en la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados que, si bien en muchos casos tienen meramente un fin publicitario, lo que pueden provocar es un aumento de ancho de banda en la red.

Spoofing

Técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada; desde su equipo, un atacante simula la identidad de otra máquina de la red (que previamente ha obtenido por diversos métodos) para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado. Otros ataques de falseamiento conocidos son:

- DNS Spoofing: En este caso se falsea una dirección IP ante una consulta de resolución de nombre (DNS) o viceversa, resolver con un nombre falso una cierta dirección IP.
- ARP Spoofing: Hace referencia a la construcción de tramas de solicitud y respuesta ARP falseadas, de forma que un determinado equipo de una red local envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo.
- Web Spoofing: El pirata puede visualizar y modificar una página web (incluso conexiones seguras SSL) solicitada por la víctima.
- E.mail Spoofing: Falsifica la cabecera de un e-mail para que parezca que proviene de un remitente legítimo. El principal protocolo de envío de e-mails, SMTP, no incluye opciones de autenticación, si bien existe una extensión (RFC 2554) que permite a un cliente SMTP negociar un nivel de seguridad con el servidor de correo.

Consulte también: Los ataques spoofing. Estrategia general para combatirlos

SSID

Identificador de red inalámbrica, similar al nombre de la red pero a nivel WI-FI.

SSL - Secure Sockets Layer

Aprobado como estándar por el Internet Engineering Task Force (IETF), es un protocolo desarrollado por Netscape para la transmisión privada de documentos vía Internet cliente/servidor. Trabaja empleando una llave privada de encriptación de datos que es transferida a través de la conexión SSL. Los navegadores Netscape y Explorer soportan SSL, y muchas páginas web emplean el protocolo para obtener información confidencial del usuario, como números de tarjeta de crédito, etc.. Por convención, las URLs que precisen una conexión SSL comienzan con https, en lugar de http.

T

Tarjeta de Red Inalámbrica

Tarjeta típica de red (con conectividad para LAN) pero diseñada y optimizada para entornos inalámbricos. Dependiendo de a quien vaya destinada existen diversos modelos: CompactFlash, PCI, PCMCIA, USB

Texto Codificado

Se dice que un texto está escrito en ciphertext cuando es necesario decodificarlo para poder leerlo. (Ver plaintext).

Texto Simple

Se dice que un texto está escrito en plaintext cuando puede ser leído sin tener que realizar ninguna operación, es decir, no está codificado. (Ver ciphertext).

TKIP - Protocolo de Integridad de Clave Temporal

Cifra las llaves utilizando un algoritmo hash y, mediante una herramienta de chequeo de integridad, asegura que las llaves no han sido manipuladas.

TLS - Transport Layer Security

Protocolo del tipo EAP que garantiza la privacidad y la seguridad de datos entre aplicaciones cliente/servidor que se comunican vía Internet. Trabaja en dos niveles: El protocolo de registro TLS - situado en el nivel superior de un protocolo de transporte seguro como TCP asegura que la conexión es privada empleado encriptación simétrica de datos y asegura que la conexión es fiable. También se utiliza para la encapsulación de protocolos de nivel superior, tales como el TLS handshake Protocol. Y, el protocolo de handshake TLS - permite la autenticación entre el servidor y el cliente y la negociación de un algoritmo de encriptación y claves criptográficas antes de que el protocolo de la aplicación transmita o reciba cualquier dato. TLS es un protocolo independiente que permite que protocolos de niveles superiores se sitúen por encima de él de manera transparente. Basado en SSL de Netscape 3.0, TLS supercede y es una extensión de SSL, si bien no son interoperables.

Token

En lenguaje de programación un elemento simple de un elemento de programación. Por ejemplo un token podría ser una palabra clave, un operador una marca de puntuación.

En redes, un token es un serie especial de bits que viajan a través de una red token-ring y a los cuales tiene acceso cualquier equipo perteneciente a esa red. El token actúa como un ticket, permitiendo a su propietario enviar un mensaje a través de la red. Existe sólo un token para cada red de modo que no sea posible que dos equipos intenten transmitir mensajes al mismo tiempo.

En sistemas de seguridad, un pequeño dispositivo del tamaño de una tarjeta de crédito que muestra un código ID que cambia constantemente (cada x minutos). El usuario primero introduce una clave y luego la tarjeta muestra un ID que puede ser utilizado para acceder a la red. Un mecanismo similar de generación de IDs son las smart card.

Tratamiento de Datos

Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Troyano

Programa informático cuya ejecución tiene unos efectos imprevistos y, generalmente, insospechados para el usuario infectado. No se les puede denominar virus porque no se replican.

TTLS - Tuneless Transport Layer Security

Protocolo de seguridad para redes inalámbricas del tipo EAP propiedad de la multinacional norteamericana Funk Software. Se trata de una extensión de EAP-TLS, protocolo utilizado por Windows XP en sistemas inalámbricos que proporciona los servicios de autenticación entre los usuarios y el servidor de la red basados en certificados. EAP-TTLS sólo requiere certificados al servidor, lo que subsana una desventaja importante respecto a EAP-TLS, cuya gestión es mucho más tediosa y pesada. Con EAP-TTLS se elimina la necesidad de configurar certificados para cada cliente de la red inalámbrica. Además, EAP-TTLS autentica al cliente en el sistema con las credenciales ya existentes basadas en password, y encripta credenciales y password para garantizar la protección de la comunicación inalámbrica.

V

Variante de un Virus

Se conoce como variante de un virus ya existente a otro virus básicamente igual al primero pero con algún pequeño cambio en su programación.

Virus

Programa que está diseñado para copiarse a sí mismo sin conocimiento del usuario y con la intención de infectar el sistema operativo y/o aplicaciones, cuyos efectos pueden variar dependiendo de cada virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante emails a terceros, etc.

(Ver File virus, boot and partition sector virus, companion virus, overwriting virus, multipartite virus, macro virus).

Virus de Archivo

Virus que infecta los archivos ejecutables de los programas. Al abrir un programa infectado, primero se ejecuta el virus y luego se abre la aplicación. Cuando se ejecuta el virus se copia a sí mismo en otros archivos o en otro disco.

Virus de Compañía

Virus que crea un archivo para esconderse cuyo nombre es igual al de otro de extensión .EXE de algún programa legítimo y con extensión .COM. MS-DOS siempre lee primero los archivos con la extensión .COM, antes que los de extensión .EXE.

Virus de Ingeniería Social

Este término es utilizado frecuentemente para describir los trucos utilizados por los virus de correo masivo para atraer a los receptores de los mensajes con archivos adjuntos infectados para ejecutarlos o visualizarlos.

Virus de Macro

Virus que infecta las macros de Word y Excel, principalmente, de modo que cuando se abre un archivo que tenga una macro infectada, infectará el sistema.

Virus de Sector de Arranque y de Partición

Los virus de esta categoría infectan el sector de arranque y sector de partición. La mayoría de los PCs están configurados para intentar arrancar de la unidad a: antes que del disco duro, por lo que si se ha introducido un disquete infectado en la disquetera en el momento de arrancar, el PC se infectará.

Virus de Script

Estos virus son escritos en lenguajes de programación script, tales como Visual Basic Script o JavaScript.

Virus de Sobre-escritura

Virus que sobrescribe cada archivo que infecta: el programa maligno copia su propio código sobre el archivo de modo que los programas dejan de funcionar. Aunque la desinfección es viable, no es posible recuperar la información de los archivos infectados.

Virus Multipartito

Virus que utiliza una combinación de técnicas para expandirse infectando archivos ejecutables, de sector boot y de partición.

Virus Residente en Memoria

Virus que permanece en memoria después de que ha sido ejecutado e infecta otros objetos bajo determinadas circunstancias.

VLAN - Red de Área Local Virtual

Tipo de red que aparentemente parece ser una pequeña red de área local (LAN) cuando en realidad es una construcción lógica que permite la conectividad con diferentes paquetes de software. Sus usuarios pueden ser locales o estar distribuidos en diversos lugares

VPN - Red Privada Virtual

Red privada que se configura dentro de una red pública. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Por ejemplo, los datos se

pueden transmitir de forma segura entre dos sucursales a través de Internet o cifrarse entre un servidor y un cliente en una Red de área local (LAN).

W

WAN - Red de Área Amplia

Tipo de red compuesta por dos o más redes de área local (LANs) conectas entre si vía teléfono (generalmente digital).

Wapi

Estándar chino de seguridad para redes Wi-Fi. Se basa en un algoritmo simétrico de encriptación. Las autoridades chinas propugnan su obligatoriedad. En inglés: Wireless Authentication and Privacy Infrastructure Protocol.

WPA - Protocolo de Aplicación Inalámbrica

Protocolo de aplicación de tecnología inalámbrica que posibilita el acceso a páginas web especialmente diseñadas para este lenguaje y está disponible en versiones 1.1 y 2.0.

WPA2 - Protocolo de Aplicación Inalámbrica

Protocolo de seguridad para redes wifi, definido en el estándar 802.11i. Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar a todos los Puntos de Acceso de última generación.

Warchalking

Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico. Tiene sus antecedentes durante la Gran Depresión del 30 en los Estados Unidos, los desocupados dibujaban símbolos en los edificios para marcar los lugares donde podían conseguir comida.

Wardriving

Técnica difundida donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar en coche puntos wireless. Existen otras modalidades dependiendo de cómo se realice el rastreo: a pie, bicicleta, patines, etc.

Warspamming

Acceso no autorizado a una red inalámbrica y uso ilegítimo de la misma para enviar correo masivo (spam) o realizar otro tipo de acciones que comprometan el correcto uso de un sistema.

La Alianza Wi-Fi

Alianza sin ánimo de lucro formada por diversos fabricantes de redes inalámbricas en agosto de 1999 para certificar la interoperabilidad de productos WLAN basados en la especificación 802.11 así como la promoción del estándar WLAN en todos los segmentos del mercado (http:/www.weca.net).

WEP - Wired Equivalent Privacy

Protocolo para la transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits!, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado, aunque requiere tiempo.

Wi-Fi

Abreviatura de Wireless Fidelity. Es el nombre “comercial” con que se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica. En lenguaje popular: Redes wifi.

WIMAX - Worldwide Interoperability for Microwave Access

Grupo no lucrativo formado en abril de 2003 iniciativa de Intel/Nokia/Fujitsu/entre otras que certifica la interoperabilidad de los productos con tecnología inalámbrica (http://www.wimaxforum.org).

WLAN - Red de Área Local Inalámbrica

También conocida como red wireless. Permite a los usuarios comunicarse con una red local o a Internet sin estar físicamente conectado. Opera a través de ondas y sin necesidad de una toma de red (cable) o de teléfono.

WPA - Acceso Wi-Fi Protegido

Estándar Wi-Fi, aprobado en abril de 2003, desarrollado para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP, pero la tecnología incluye dos mejoras con respecto a este último: emplea el protocolo de integridad de claves TKIP y la autenticación de usuarios se realiza mediante el protocolo EAP.

WWWD - The WorldWide Wardrive

Evento internacional que durante una semana reúne a expertos de todo el mundo que buscan y catalogan nodos inalámbricos en sus ámbitos geográficos (http://www.worldwidewardrive.org/).