Seguridad informática/Terminología

< Seguridad informática

Sumario

El por qué de esta sección

Términos

- Access Control List (ACL)
- Adware
- AES
- Almacén de Certificados
- Amenaza
- Anti-spam
- Antivirus
- Aplicaciones engañosas
- Ataque activo
- Ataque pasivo
- Ataques Web (CNA Computer Network Attack)
- Autenticación
- Backdoor (Puerta trasera)
- Back Hack
- Blowfish
- Bluejacking
- Bluesnarfing
- Botnet
- Canal de control y comando
- Carding
- Carga destructiva
- Certificado SSL Standard
- Certificado SSL Wildcard
- Cibercrimen
- Ciberterrorista
- Clickjacking (UI redress attack)
- Computación forense
- Confidencialidad
- Cookie Poisoning
- Cracker
- Crasher
- Crimeware
- Criptografía
- Criptograma
- Criptolibertario (cipherpunk)
- Criptología
- Cross-site scripting (XSS)
- Cruncher
- Cyber Pearl Harbor
- Deep Web/Dark Web
- Defacement
- DES (Data Encryption Standard)

Descarga inadvertida
Eavesdropping
ElGamal
Encriptación
Esteganografía
Exploit
Filtración de datos
Firewall
Firma Digital
Framework(Mecanismo)
Gusanos o mutex
Hash
Hijacking
Hoax o bulo
Honeypot (Trampa o tarro de miel)
HTTPS (Hyper Text Transfer Protocol Secure)
IMSI catcher
Infección
Ingeniería Social
Insider Attack
Integridad
Involuciones
Key Log
Llaves pública y privada = Public and private key
MacAddress
Malware
Man in the middle
Mule phisher
No repudiación
NSA
Onion routing
Phreakers
Piggybacking
PKI (Infraestructura de llave pública = Public Key Infrastructure)
Privacy-enhancing technologies
Protocolo Criptográfico
Proxy Server (Servidor Proxy)
Ransomware
Redes punto a punto (P2P)
Retrovirus
Reverse Proxy
RFID
Root Kit
RSA (Rivest, Shamir y Adleman)
Seguridad de Operaciones
Sistema de detección de intrusos
Sistema de prevención de intrusos
Sistemas afectados
Sniffer
Spambot
Spoofing (Falsificación)
Spyware
SSL (Secure Socket Layer)
Tactical Data (Datos tácticos)
TLS (Transport Layer Security)

Toolkit
Traffic Encryption Key (TEK)
Troyanos
Tunneling protocol
Variantes
Vector de ataque
Virus
VPN (Virtual Private Network -Red Virtual Privada-)
Vulnerabilidad (Vulnerability)
Warez

El por qué de esta sección

La creación de esta sección obedece a ayudarle a familiarizarse con algunos términos (en su mayoría anglicismos) que han surgido con el pasar del tiempo para referirse a los problemas de seguridad.

No se sienta extrañado, ya que la mayoría de estos términos por lo menos usted y yo los hemos escuchado alguna vez (como el caso de virus informáticos o spyware).

En esta sección usted se familiarizará con algunos de los términos utilizados en la seguridad informática.

Términos

Access Control List (ACL)

Son los privilegios y limitaciones de un objeto, para establecer qué tipo de usuarios tienen un determinado tipo de acceso al objeto.

Adware

La palabra Adware proviene del inglés ***Ad****vertistement Soft****ware*** traducido como "Sofware publicitario". A diferencia de otros malwares, el adware se centra en mostrar reiteradas veces y sin el consentimiento del usuario publicidades de todo tipo; si bien es más molesto que peligroso, los anuncios que contienen pueden efectuar descargas de otro malwares más dañinos como virus o gusanos. A veces, algunas empresas proponen versiones "Free" o gratuitas de sus productos pero con la disconformidad de venir con publicidad incluida pidiendo a cambio dinero para obtener versiones sin esta propaganda.

AES

Advanced Encryption Standard (AES). Es un algoritmo de criptografía simétrica, también conocido como Rijndael. Se transformó en un estándar el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica. Desarrollado por los criptólogos belgas, Joan Daemen y Vincent Rijmen, estudiantes de la *Katholieke Universiteit Leuven,* y enviado al proceso de selección AES bajo el nombre "Rijndael", para sustituir al algoritmo DES. Las claves AES son de 128, 192 o 256 bits.

Almacén de Certificados

Es un archivo o directorio donde se almacenan los certificados digitales. El estándar PKCS#7 establece lineamientos para los almacenes de certificados.

Amenaza

Cualquier evento que ponga en riesgo la seguridad o daños a un sistema

Anti-spam

Es una serie de técnicas y heramientas usadas para disminuir el spam (o correo no deseado), antes de que se convierta en una molesti para los usuarios.

Antivirus

Es un software de seguridad que protege a un equipo de virus, su funcionamiento de detección es normalmente en tiempo real y mediante análisis paulatinos del sistema, que al identificar algún archivo dañino lo pone en cuarentena. El antivirus es parte fundamental de una estrategia de seguridad.

Aplicaciones engañosas

Son programas que intentan obtener información confidencial de usuarios (cómo su nombre completo y número telefónico), con el fin de acceder a algún privilegio (como un supuesto acceso a un recurso).

Ataque activo

Son los ataques donde se altera información, o se toma el control de una cuenta.

Ataque pasivo

Son los ataques cuyo propósito es sólo la interceptación de la información.

Ataques Web (CNA Computer Network Attack)

Es cualquier ataque informático que se realiza desde el internet.

Autenticación

Es el proceso para acreditar o verificar que un usuario o mecanismo es quien afirma ser, cuando intenta acceder a un equipo o servicio en línea.

Backdoor (Puerta trasera)

Son o líneas de código implantadas en programas de sistemas operativos o en aplicaciones, de importancia o no, o vulnerabilidades conocidas de antemano en una cierta tecnología, que no son corregidas intencionalmente. Un backdoor tiene el propósito de poder romper la seguridad de un equipo o una red.

Back Hack

Back Hack es un concepto del cómputo forense. Es el proceso de identificar ataques a un sistema y, si es posible, identificar el origen de los ataques. Un cierto tipo de ataque deja un cierto tipo de rastros, y el Back hacking puede ser pensado como una especie de ingeniería inversa de los esfuerzos de hacking.

Blowfish

Es un algoritmo criptográfico simétrico, con una clave variable y una función Feistel para cifrar y descifrar la información. Tiene la particularidad de poder encriptar con tamaños de llaves grandes, como 1024 bits.

Bluejacking

Bluejacking permite a una persona enviar mensajes anónimos a dispositivos con bluetooth dentro de cierto radio.

Bluesnarfing

Bluesnarfing es la penetración de un dispositivo Bluetooth que se encuentra en modo detectable, logrando el control del dispositivo infectado.

Botnet

Un botnet es un conjunto de hosts infectados por bots, que son controlados por un tipo un malware, normalmente sin el conocimiento del usuario. Pueden gobernarse a partir de un canal de comando y control (C&C) o a través de una conexión peer-to-peer (P2P).

Canal de control y comando

Es el medio por el cual un atacante de malware se comunica y controla los equipos que infectó, típicamente mediante botnets.

Carding

Es un tipo de cibercrimen, dirigido al compromiso de tarjetas bancarias.

Carga destructiva

Es la actividad dañina de un malware o crimeware. Por ejemplo, el ransomware es un tipo de crimeware, cuya carga destructiva es la encriptación de archivos de datos de una computadora atacada, para extorsionar a los usuarios afectados.

Certificado SSL Standard

Un certificado SSL, en general, permite autenticar digitalmente la identidad de un servidor. Contiene, entre otros datos, la información de la empresa o persona propietaria, número de serie del certificado, fecha de expedición y fecha de expiración, información de la entidad que lo certifica (Certification Authority), así como detalles para lo que se va a utilizar. El certificado SSL Standard es el más utilizado y ampara un solo nombre de dominio, por ejemplo: dominio.com. Cuando un navegador lo reconoce, cambia automáticamente al protocolo HTTPS. Los detalles de cada certificado pueden consultarse en el ícono de candado que se encuentra junto al URL.

Certificado SSL Wildcard

Un Certificado SSL Wildcard es similar al standard, sin embargo, este tipo de certificados permite asegurar subdominios, es decir, que además de asegurar el nombre del dominio también lo hace para los subdominios asociados a el, por ejemplo: mail.dominio.com, ftp.dominio.com. Por lo general, este certificado es ilimitado para la cantidad de subdominios, ya que permite certificar utilizando comodines (de ahí su nombre), ejemplo: *.dominio.com

Cibercrimen

Son aquellos ataques computacionales tipificados como delitos por el código penal.

Ciberterrorista

Es una categoría de cibercrimen, donde el programa tiene el propósito fundamental de lanzar un ataque de terror, por ejemplo, atacando una infraestructura pública.

Clickjacking (UI redress attack)

Es un tipo de aplicación engañosa, que utiliza los clicks de un usuario, donde se ejecutan capas ocultas de código en una página o descarga aparentemente válida.

Computación forense

Es la disciplina de seguridad computacional responsable de documentar la evidencia de que en cierto equipo de cómputo se cometió un cibercrimen.

Confidencialidad

Es la garantía de que la información sólo debe ser conocida por quienes tengan derecho a ella. Es uno de los requerimientos de la seguridad informática.

Cookie Poisoning

El envenenamiento de Cookies es la modificación no autorizada de los datos de una cookie, como parte de algún ataque.

Cracker

El cracker es la persona que logra evadir o romper la seguridad de un software u otro artefacto tecnológico, bien sea para obtener ganancias, o simplemente por desafío intelectual o boicot.

Crasher

Es la persona que realiza un ataque con el propósito de suspender la ejecución de un sistema, normalmente como un boicot contra una organización.

Crimeware

Es un software diseñado para facilitar la comisión de algún tipo de cibercrimen.

Criptografía

Se encarga de las técnicas de cifrado, con el objetivo de modificar mensajes para hacerlos ocultos. Toda criptografía involucra una clave, un algoritmo y un texto en claro, y produce un criptograma, o parte de un criptograma para recuperar el texto en claro. Existen dos tipos de criptografía: Simétrica: se encripta y desencripta con la misma llave. Asimétrica: se encripta con una llave y desencripta con otra llave.

Criptograma

Es una archivo encriptado.

Criptolibertario (cipherpunk)

Es un tipo de hacktivista que parte de la premisa de que los gobiernos y corporaciones violan sistemáticamente la privacidad de las personas, y en consecuencia busca que todos los paquetes del internet viajen encriptados con criptografía robusta.

Criptología

Es la Ciencia que se encarga de proporcionar seguridad a la información por medio del ocultamiento de los datos. Se compone de la criptografía, el criptoanálisis, la criptocomputación y las criptomatemáticas.

Cross-site scripting (XSS)

Vulnerabilidad de seguridad de aplicaciones web, en el cual se permite inyectar código malicioso, bien sea en JScript, VBScript o PHP.

Cruncher

Es un tipo de hacktivista que dona ciclos de reloj de sus equipos de cómputo, cuando dichos equipos están desocupados, para participar en proyectos científicos, por ejemplo, para realizar diseño de drogas asistido por computadora para enfermedades raras o ignoradas. Los cruncher se agrupan fundamentalmente alrededor de la plataforma BOINC (Berkeley Open Infrastructure for Network Computing).

Cyber Pearl Harbor

Cyber Pearl Harbor es un escenario hipotético de un ataque cibernético que amenace la infraestructura de TI de los Estados Unidos, posiblemente en el contexto de una guerra o de un ataque terrorista.

Deep Web/Dark Web

La deep weeb/dark web (la web oscura), se compone de sitios que no son accesibles por los navegadores usados en Internet, y que en su mayoría tampoco son identificados por buscadores como google. El uso de la deep web desde entornos inseguros (con sistemas operativos inseguros, con aplicaciones provistas de puertas traseras, o con passwords vulnerables), hace factible el ataque o la persecución de usuarios de la deep web. La deep web es una red diseñada para garantizar el anonimato, accesible desde el navegador Tor y con sus propios recursos de búsqueda (como Hidden Wiki). En la deep web coexisten dos grandes tipos de usuarios: por un lado los luchadores sociales, el periodismo independiente y hackers (el servidor de wikileaks está en la deep web), y por otro lado la deep web se presta para el crimen organizado, el mercado negro, la trata de personas y la pornografía infantil.

Defacement

Defacement es la forma de vandalismo en que los **defacers** marcan un sitio web. Hay sitios donde los defacers exhiben sus logros.

DES (Data Encryption Standard)

Es un algoritmo criptográfico simétrico, para cifrar y descifrar información, desarrollado a partir del algoritmo Lucifer de IBM, con bloques de 8 bytes y clave de 64 bits. Ya no es seguro. Evolucionó en el algoritmo triple DES (o DES-EDE).

Descarga inadvertida

Es uno de los mecanismos de propagación del malware, consistente en lograr la descarga de un malware sin intervención del usuario.

Eavesdropping

Término usado para identificar a la práctica de interceptar, registrar y almacenar comunicaciones ajenas, para procesarlas, escucharlas o leerlas. La práctica masiva del eavesdropping es realizada por agencias de inteligencia de múltiples gobiernos. Es un ataque gubernamental al derecho de privacidad de las personas. Las principales formas de combatir este ataque es lograr que todas las comunicaciones viajen encriptadas con criptografía robusta, que las personas usen entornos de hardware y software libres de backdoors, y que los usuarios utilicen passwords que resistan ataques.

ElGamal

Es un algoritmo asimétrico basado en el problema del algoritmo discreto, que es utilizado para trabajar con firmas digitales.

Encriptación

Es un mecanismo de seguridad para codificar cierta información, en la cual sólo aquellos usuarios que tiene un acceso o una clave, pueden descifrar o utilizar los datos.

Esteganografía

Es una técnica que se utiliza para ocultar información secreta en archivos de extensiones ampliamente usadas, como .jpg o .pdf, sin que se perciba su existencia, y permitiendo que el archivo se pueda abrir normalmente. Su principal uso es ocultar criptogramas.

Exploit

Traducido al español como "Explotar" o "Aprovechar", es un programa informático, o incluso sólo un fragmento ejecutable, que se utiliza a partir de una vulnerabilidad de seguridad de un sistema, para conseguir que éste tenga un comportamiento no deseado.

Filtración de datos

Es la difusión pública de información comprometida en un ataque.

Firewall

Es un sistema que proporciona seguridad de red, mediante el filtrado del tráfico entrante a una red o saliente de la misma. Por ejemplo, es común que el badware envía información desde una máquina infectada. El firewall intercepta ese envío de información y le pregunta al usuario si está de acuerdo.

Firma Digital

Es una técnica para validar el origen de una información. Por ejemplo, con algunos algoritmos asimétricos, el origen del mensaje lo firma utilizando su llave privada, y el destinatario del mensaje puede validar dicha firma utilizando la llave pública del origen.

Framework(Mecanismo)

Conjunto de patrones que soluciona una problemática. Cabe mencionar que un patrón es una buena solución a un problema, por ende un anti-patrón son las malas soluciones. El framework más usado en seguridad involucra criptografía simétrica y asimétrica, firma digital y certificados digitales, tecnologías que se usan para garantizar las problemáticas de la autenticación, confidencialidad, integridad y no repudiación.

Gusanos o mutex

A diferencia de los virus, estos son aplicaciones que se copian a la **PC** y ralentizan (hacen más lento) su funcionamiento. Los gusanos pueden bloquear aplicaciones, o buscar más víctimas. La infección de un gusano puede provenir de un correo electrónico tipo "**spam**", o se pueden descargar de un sitio web.

Los gusanos tienen la característica de poder autoreplicarse en un mismo ordenador, por ejemplo, aquellos que se copian en cada carpeta, y se abren con cada carpeta. Algunos no desean eso y generan una regla que indica que solo una copia por equipo se debe ejecutar, que es un **MUTEX** lo cual les da también este nombre.

Hash

Es una función para transformar un dato en un entero de longitud fija, en seguridad se utiliza para comprobar la integridad de la información. Algunos algoritmos hash utilizados en seguridad son el SHA-1, el SHA-2 y el MD5.

Hijacking

El hijacking es una metodología ilegal para apoderarse de una posesión digital. Incluye robo de información, de dominios de internet, de conexiones de red y de sesiones de terminal, entre otras.

Hoax o bulo

Bulo es chisme, engaño, mentira, Hoax también. Son correos electrónicos que dicen "Reenvía esto! un virus genéticamente modificado infecta máquinas!!!!" o el clásico "A partir del verano del <inserte año> el messenger será de pago a menos de que <inserte algo que hay que hacer en una pagina>!!!"

Honeypot (Trampa o tarro de miel)

Es una técnica que forma parte de múltiples ataques. Consiste en ofrecer algo que se piensa es irresistible para el objetivo del ataque, con el propósito de ganar su confianza o penetrar la seguridad.

HTTPS (Hyper Text Transfer Protocol Secure)

Es la versión segura del protocolo HTTP, que sirve para el envío y recepción de información a través de Internet. El protocolo HTTPS utiliza el puerto 443 mientras que HTTP usa el 80. La información en HTTPS viaja encriptada, pasando a través de un túnel seguro con conexión SSL/TLS desde el emisor hasta el receptor y viceversa, evitando que pueda ser leída por terceros.

IMSI catcher

Son grandes instalaciones, mimetizadas como torres de telefonía celular, para realizar eavesdropping de gran escala.

Infección

Este término hace referencia al equivalente biológico de la palabra infección. Sucede cuando un malware se ejecuta libremente en la computadora por primera vez, sin importar de que tipo de malware sea.

Ingeniería Social

Se refiere a una manera de engañar y/o manipular a las personas y su comportamiento, con la finalidad de obtener información sobre su acceso/credenciales/contraseñas.Se puede llegar a influir tanto en una persona, que se puede lograr que actúen de alguna manera en específico o divulguen cierta información privada.

Insider Attack

Evento donde un individuo miembro de una organización lanza un ataque contra esa organización. Pueden ser ataques devastadores. Por ejemplo, el whistleblower Edward Snowden, agente de la NSA, lanzó un poderosísimo ataque contra dicha organización. Otro ejemplo fue Mark Felt (*Deep Throat*), subdirector adjunto del FBI, quien proporcionó documentos a periodistas del Washington Post, detonando el escándalo Watergate y la renuncia de Nixon.

Integridad

Es la garantía de que la información no ha sido alterada sin autorización. Es uno de los requerimientos de la seguridad informática.

Involuciones

Son transformaciones reversibles por medio de las cuales se realiza la criptografía simétrica. Son o sustituciones (reemplazar un carácter o un conjunto de bits por otros), o transposiciones (cambiar el orden de caracteres o de conjuntos de bits).

Key Log

"Registro de teclas", son programas que registran todo lo que uno teclea, la información obtenida se puede guardar o enviar inmediatamente, suponen un peligro al poder registrar contraseñas, direcciones de correo electrónico y páginas.

Llaves pública y privada = Public and private key

Cada par de llaves criptográficas pública y privada están relacionadas entre sí. La información encriptada con la llave pública solo puede ser desencriptada por la llave privada, creando así un par de llaves únicas que permiten de forma segura el intercambio de información. El secreto de esta criptografía se basa en que la llave privada sólo la debe conocer su propietario.

MacAddress

Es una número de 48 bits, que funciona como identificador único de un dispositivo o tarjeta de red.

Malware

Es la contracción de dos palabras:***Mal****icious Soft****ware*** (traducido al español como software malicioso). Se utiliza para referirse a todo software que cause daños a los usuarios, como pérdida de datos, robo de contraseñas, etcétera. Es un término más abarcativo que virus.

Man in the middle

Se refiere a cualquier interceptación de información, bien sea con fines de*eavesdropping* o para realizar un ataque activo.

Mule phisher

Es un participante del ciberdelito del phishing, quien permite que se realice un depósito a una cuenta bancaria a su nombre, retira la mayor parte del depósito (menos su comisión), y transfiere la cantidad retirada a alguna cuenta no rastreable (normalmente en bitcoins). Suelen ser los participantes de este ciberdelito que son detenidos y encarcelados.

No repudiación

Garantiza la imposibilidad de que alguna de las partes involucradas en una comunicación o transacción niegue haber enviado o recibido un mensaje u originado o haber sido el destinatario de una acción. La no repudiación permite el comercio electrónico. Es uno de los requerimientos de la seguridad informática.

NSA

La National Security Agency, es la organización de seguridad nacional del gobierno de los Estados Unidos. Es un hecho que la NSA intercepta gran parte de las comunicaciones del planeta. Otros organismos de seguridad nacional de otros gobiernos también interceptan comunicaciones, pero sus capacidades no se comparan con las de la NSA. La NSA trabaja conjuntamente con las

organizaciones de seguridad nacional de Gran Bretaña, Canadá, Australia y Nueva Zelanda en el espionaje a las comunicaciones del planeta.

Onion routing

Es un sistema de comunicación que tiene como objetivo realizar una conexión sin perder la privacidad de ésta, ni de sus involucrados. Es una tecnología de la deep web.

Phreakers

Individuos que utilizan ilegalmente las redes de telefonía para hacer llamadas o usar servicios telefónicos de manera gratuita.

Piggybacking

Es la conexión no autorizada a una red inalámbrica.

PKI (Infraestructura de llave pública = Public Key Infrastructure)

Se trata de una tecnología principalmente utilizada en empresas y aplicaciones de comercio electrónico/e-business, que permite crear un ambiente seguro y confiable para el intercambio de información y comercio electrónico entre redes no seguras, como Internet. Combina software, criptografía y políticas de seguridad que permiten autenticar la identidad de los usuarios a través de un par de llaves criptográficas: una pública y otra privada.

Privacy-enhancing technologies

Es un término estandarizado con el que se refiere a métodos específicos que regularizan la información conforme a las leyes de la protección de información.

Protocolo Criptográfico

Es una secuencia de pasos donde se utiliza uno o más algoritmos criptográficos, para asegurar los requisitos de seguridad y llevar a cabo el intercambio de datos cumpliendo, por ejemplo, con la confidencialidad, integridad, o no repudiación.

Proxy Server (Servidor Proxy)

Es una aplicación que funciona como un representante de un cliente con otro servidor, de manera que los servidores externos sólo negocian con el servidor proxy, y no con la computadora del cliente. Esto introduce una capa de seguridad y de ocultamiento de la identidad del cliente.

Ransomware

Es una categoría del cibercrimen que encripta los archivos con datos de un equipo (normalmente con criptografía AES de 128 bits), extorsionando al usuario para que pague un rescate (normalmente realizando un depósito a una cuenta de bitcoin). Si el usuario no paga el rescate en un tiempo perenterio, los datos son destruidos definitivamente. Y si el usuario paga el rescate puede recibir (o no) la llave con la que puede desencriptar sus archivos personales.

Redes punto a punto (P2P)

Es una red donde los participantes comparten información sin necesidad de concentrar esa información en servidores. Sin embargo, también están expuestas a virus, spyware, troyanos, etcétera.

Retrovirus

Es un tipo de virus que detectan los antivirus e intentan ocultarse de ellos.

Reverse Proxy

Es una aplicación instalada en el servidor web, que funciona como una capa de seguridad para detener algunos ataques, en particular DoS.

RFID

De las siglas Radio Frequency IDentification, (identificación por radiofrecuencia), es una tecnología de etiquetado donde se trasmiten frecuencias de radio desde un lector RFID a una etiqueta RFID, con el fin de identificar objetos. Hay varias diferencias de las etiquetas de código de barras con las etiquetas RFID: mientras que los códigos de barras tienen el mismo código para un sólo tipo de producto, una etiqueta RFID tiene un código único para cada etiqueta, otra diferencia es que las etiquetas RFID pueden ser leídas de forma remota, una tercera diferencia es que una etiqueta RFID puede estar empotrada en otro material, y pasar desapercibida. Hay muchos tipos de etiquetas RFID. Algunas pueden ser desactivadas, mientras que otras no ofrecen esa opción. Desde la perspectiva de la seguridad, la tecnología RFID involucra un riesgo, ya que una etiqueta RFID activa puede ser usada como parte de un ataque.

Root Kit

Se trata de programas que ocultan todo proceso que un *cracker* considere como vital para mantenerse oculto (por eso algunos lo denominan en español *Encubridores* ya que evitan que se detecten los malwares). Actúan ya sea en **Linux** o **Windows**. También es un programa que permite un acceso privilegiado a un sistema de manera continua. Los root kit no son sencillos de eliminar

RSA (Rivest, Shamir y Adleman)

Es el algoritmo asimétrico más utilizado. Su funcionamiento se basa en el producto de dos números primos grandes.

Seguridad de Operaciones

Procesos y controles que tienen como fin garantizar prácticas seguras en los usuarios de una organización.

Sistema de detección de intrusos

Servicio que monitorea y analiza los eventos del sistema, con el fin de encontrar y proporcionar en el momento, advertencias de intentos de acceso a los recursos del sistema de manera no autorizada.

Sistema de prevención de intrusos

Son sistemas que nos ayudan con la supervisión de actividades, tanto en sistemas, como en redes. Estos sistemas monitorean en tiempo real los comportamientos de los usuarios, buscando patrones de actividades que sean sintomáticos de un ataque en proceso, para alertar a los responsables de la operación de los sistemas, y proceder, una vez confirmado el ataque, a tomar acciones para documentarlo, abortarlo y revertirlo.

Sistemas afectados

Se refiere a la lista de sistemas operativos o aplicaciones, que tienen una determinada vulnerabilidad.

Sniffer

Es la interceptación y análisis de paquetes de una red. Una solución al problema del sniffing es que los paquetes viajen encriptados, con lo que la única información que se puede obtener de ellos es su origen y destino.

Spambot

Es un botnet usado para enviar spam. El programa intenta hacerse pasar por una persona real, para enviar correos, ligas, o solicitudes engañosas.

Spoofing (Falsificación)

Ataque informático que suplanta la identidad de alguna entidad computacional, alterando los datos de una comunicación, como la dirección IP o la mac address.

Spyware

Al igual que malware es una contracción de dos palabras, en este caso de ***Spy Software***, (traducido como Software espía); y como su nombre lo indica, a diferencia de otros malwares, su función principal, más que causar daños a la información de un equipo, se centra en enviar información privada del usuario al creador del spyware.

SSL (Secure Socket Layer)

Desarrollado en 1995 por Netscape Corporation, es una tecnología estándar de seguridad global que permite establecer conexiones encriptadas de forma segura para el intercambio de información entre servidores y clientes en Internet o una Intranet. Clientes y servidores pueden autenticarse mutuamente usando Certificados SSL, utilizando pares de llaves públicas y privadas. En Abril de 2017 la última versión era SSL 3.0.

Tactical Data (Datos tácticos)

Información que se debe de mantener protegida por un período limitado de tiempo.

TLS (Transport Layer Security)

Es el sucesor de SSL, pero se utiliza mayormente en correo electrónico, utilizando algoritmos de encriptación mas fuertes. En Abril de 2017, la versión más reciente era SSL 1.2.

Toolkit

Programas de software que ayudan a los hackers, crackers o cibercriminales a crear y propagar códigos maliciosos. También pueden utilizarse para lanzar ataques web, enviar spam y crear sitios de phishing.

Traffic Encryption Key (TEK)

Es una llave simétrica utilizada para encriptar el tráfico de una red. Se cambia frecuentemente.

Troyanos

Un "Troyano" o "Caballo de Troya" es un malware que se instala en un sistema bajo la apariencia de un programa valioso para el usuario que lo descargó. El programa puede hacer lo encomendado -o no-, pero adicionalmente realiza una infección en el entorno donde se ejecutó. Los troyanos toman su nombre del hecho mitológico en el que los espartanos dan a la ciudad de Troya como regalo un gran "caballo de madera". el cual contenía en su interior guerreros espartanos preparados para atacar

Tunneling protocol

Es un protocolo de redes utilizado en VPNs, para facilitar la encriptación de los paquetes de la red.

Variantes

Son nuevas cepas de malware que toman códigos de otros programas conocidos. Casi siempre se identifican con una letra, seguido del apellido del malware. por ejemplo, P33.Downadup.C.

Vector de ataque

Es la descripción pormenorizada de los pasos que explotan una vulnerabilidad para consumar un ataque exitoso.

Virus

Son **"Archivos vitales del sistema bajo acoso"**, y toman su nombre de una analogía con los virus biológicos, ya que se insertan en archivos válidos, y se replican cuando el archivo se ejecuta o se abra. Sus instrucciones son claras: busca otro de tu tipo y cópiame en su contenido. Algunos virus no sólo se replican, sino que pueden dañar la información o el funcionamiento de un equipo.

VPN (Virtual Private Network -Red Virtual Privada-)

Es una arquitectura de red P2P, que facilita una cierta confidencialidad y la transmisión de paquetes encriptados.

Vulnerabilidad (Vulnerability)

Una debilidad o falla de un sistema.

Warez

Es quien toma un crack (de un software o de un archivo multimedia) y lo hace público.
