



## GLOSARIO DE TÉRMINOS

### A

**AAA:** Acrónimo de Autenticación, Autorización y Administración Siglas que se aplican en las herramientas de seguridad.

**Ataque Informático:** Es un método por el cual un individuo, mediante un sistema informático intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera)

**Ataque de denegación de servicio:** es un ataque a una red o a un sistema, que causa que un servicio o recurso sea inaccesible.

### B

**Backbone:** Es la infraestructura de la transmisión de datos en una red o un conjunto de ellas en Internet.

**Base de datos:** Almacén de datos relacionados con diferentes modos de organización.

**Bytecode:** Código intermedio entre el código fuente y el código máquina. Suele tratarse como un fichero binario que contiene un programa ejecutable similar a un módulo objeto.

**Backdoor:** (Español Puerta trasera) es una secuencia especial dentro del código de programación mediante la cual el programador puede acceder o escapar de un programa en caso de emergencia o contingencia en algún problema.

## C

**Caballo de Troya o Troyano:** Software malicioso que parece realizar ciertas acciones pero realizan otras tales como los virus de computadoras. Este tipo de malware es usado para la instalación de puertas traseras en sistemas que luego pueden ser utilizadas por el autor del malware u otros usuarios maliciosos para tener acceso al sistema infectado. Luego de la infección estas computadoras se convierten en zombis que pueden ser completamente controladas por el atacante.

**Código fuente:** Texto escrito en un lenguaje de programación específico y que puede ser leído por un programador. Debe traducirse a lenguaje máquina para que pueda ser ejecutado por la computadora o a bytecode para que pueda ser ejecutado por un intérprete.

**Código malicioso:** término que hace referencia a cualquier conjunto de códigos, especialmente sentencias de programación, que tiene un fin malicioso

**Conmutador:** es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 del modelo OSI. Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes, pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

**Contraseña:** Conjunto finito de caracteres limitados que forman una palabra secreta que sirve a uno o más usuarios para acceder a un determinado recurso.

## D

**Datagrama:** es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el DTE receptor, de manera independiente a los fragmentos restantes.

**Defacement:** Es la modificación de una página web sin autorización del dueño de la misma. La mayoría de las veces logran “defacear” un sitio consiguiendo acceso

mediante alguna vulnerabilidad que el programador haya dejado en el mismo. También por contraseñas (“passwords”) débiles, problemas en el FTP, etcetera.

**Dirección MAC:** es un identificador hexadecimal de 48 bits que se corresponde de forma única con una tarjeta o interfaz de red.

## G

**GUSANO:** Es un programa de computadora que se auto-replica. Usa la red para enviar copias de el mismo a otras computadoras y lo puede hacer sin la intervención del usuario.

## H

**Hardening:** Es una técnica compuesta por un conjunto de actividades llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de este.

## I

**Intruso (Cracker):** Experto en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. usan su conocimiento con fines maliciosos, antimorales o incluso bélicos, como intrusión de redes, acceso ilegal a sistemas gubernamentales, robo de información, distribuir material ilegal o moralmente inaceptable, piratería, fabricación de virus, herramientas de Crackeo y elementos de posible terrorismo como la distribución de manuales para fabricar elementos explosivos caseros o la clásica tortura china.

## M

**Malware:** (del inglés *malicious software*, también llamado badware, software malicioso o software malintencionado) es un software que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el conocimiento de su dueño, con finalidades muy

diversas, ya que en esta categoría encontramos desde un troyano, virus, rootkit a un spyware.

**Maquina virtual:** **Aplicación** que interpreta y ejecuta programas escritos en el **lenguaje de programación Java**. Específicamente puede interpretar el **bytecode** generado al **compilar** en Java.

**Memoria de acceso aleatorio (RAM):** Tipo de **memoria** donde la **computadora** guarda información para que pueda ser procesada más rápidamente. En la memoria RAM se almacena toda información que está siendo usada en el momento.

**Memoria de solo lectura (ROM):** Tipo de memorias añadidas desde fábrica, que no puede ser modificada ni tampoco se pierde su información al apagar el equipo (como sí pasa en las memorias **RAM**).

**Memoria Flash:** Tipo de memoria no volátil que suele ser usadas en celulares, cámaras digitales, **PDAs**, reproductores portátiles, discos rígidos (**disco rígido híbrido**), etc. Pueden borrarse y reescribirse.

**Memoria no volátil (NVRAM):** Tipo de **memoria** que puede retener información **almacenada** incluso cuando no recibe electricidad.

**Multidifusión:** es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión **nodo** por **nodo**.

**Multiplataforma:** es un término usado para referirse a los **programas**, **sistemas operativos**, **lenguajes de programación**, u otra clase de software, que puedan funcionar en diversas **plataformas**

O

**Objeto:** representación detallada y particular de algo de la realidad. Todo objeto tiene un identidad o nombre, estado (características definidas generalmente en variables) y comportamiento (sus funciones o procedimientos).

## P

**Protocolo:** es el lenguaje (conjunto de reglas formales) que permite comunicar **nodos (computadoras)** entre sí. Al encontrar un lenguaje común no existen problemas de compatibilidad entre ellas.

## R

**Rootkit:** Es una herramienta, o un grupo de ellas que tiene como finalidad esconderse a sí misma y esconder otros programas, procesos, archivos, directorios, claves de registro, y puertos que permiten al intruso mantener el acceso a un sistema para remotamente comandar acciones o extraer información sensible, a menudo con fines maliciosos o destructivos. Existen rootkits para una amplia variedad de sistemas operativos, como Linux, Solaris o Microsoft Windows.

**Red:** es una **interconexión** de **computadoras** para compartir información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico (alambrado) o inalámbrico.

## S

**Spyware:** Es un software que se instala furtivamente en una computadora para recopilar información sobre las actividades realizadas en ella.