Glosario

ACK (Acknowledgement)	Tipo de señal de respuesta enviada entre procesos o computadoras que se están comunicando para indicar que la información fue recibida completa y libre de errores.
Análisis forense	Metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir el cómo se penetró en un sistema, a la par que se valoran los daños ocasionados.
API (Application Program Interface)	Se refiere al conjunto de rutinas, protocolos y herramientas necesarias para construir aplicaciones de software.
ARP (Address Resolution Protocol)	Es un protocolo de nivel de red responsable de encontrar la dirección física correspondiente a una dirección IP determinada.
Backdoor	Es una aplicación que permite el acceso remoto a una computadora, evitando una autenticación normal y manteniéndose oculta del sistema.
Banner	Se llama *banner* a la información que transmite un servicio cuando se trabaja con él. Dicha información puede incluir el nombre del servicio, la versión, por mencionar algunas.
Banner grabbing	Técnica de enumeración que trata de usar la información del banner como referencia para conocer los servicios que corren en un equipo protegido por un firewall.
BIOS (Basic Input Output System)	Código de software que localiza y reconoce todos los dispositivos necesarios para carga el sistema operativo en la memoria RAM.
Bit	Es el acrónimo de Binary DigIT. Es la unidad mínima de información empleada en informática. Con él, podemos representar dos valores cualquiera, sea verdadero o falso o 1 y 0.
Broadcast	Es un modo de transmisión de información donde un dispositivo emisor envía información a una multitud de dispositivos receptores de manera simultánea, sin necesidad de repetir la misma información equipo por equipo.
Buffer	Se refiere al área de almacenamiento temporal, reservada para uso en las operaciones de entrada-salida dentro de la cual los datos son leídos o escritos.
Buffer overflow	También conocido como desbordamiento de *buffer*, se refiere a un error de software que se produce cuando se copia una cantidad de datos sobre un área que no es lo suficientemente grande para contenerlos sobre escribiendo otras zonas de memoria.
Byte	Unidad de información compuesta por 8 bits.
Cadena	Secuencia ordenada de longitud arbitraria de elementos que pertenecen a un cierto alfabeto.
Cliente	Se llama así al dispositivo electrónico que recibe servicios de otro dispositivo conocido como servidor.
Cluster	Conjunto contiguo de sectores que componen la unidad más pequeña de almacenamiento de un disco. Los archivos se almacenan en uno o varios clusters, dependiendo de su tamaño de asignación. Sin embargo, si el archivo es más pequeño que un clúster, éste lo ocupa completo.
CPU (Central Processing Unit)	Se llama así al componente central de la computadora donde se realizan las funciones lógicas y aritméticas básicas.
Cracking	Irrumpir en un sistema informático de manera ilegal, quebrantando su seguridad.

DHCP (Dynamic Host Configuration Protocol)	Protocolo de red que permite a los nodos en una red IP, obtener sus parámetros de configuración automáticamente. Trabaja bajo la capa de aplicación del modelo OSI y está definido en el RFC 2131.
DNS (Domain Name System)	Base de datos distribuida y jerárquica que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a un dirección numérica IP.
DoS (Denial of Service)	Se refiere a una ofensiva diseñada específicamente para impedir el funcionamiento normal de un sistema y por consiguiente, impedir el acceso legal a los sistemas a los usuarios autorizados.
ESSID (Extended Service Set IDentifier)	Véase *SSID*.
Exploit	Es un software que tiene como finalidad automatizar el aprovechamiento de un error, fallo o vulnerabilidad de un programa o hardware.
Fingerprinting	Es el proceso de determinar el sistema operativo instalado en un equipo objetivo.
Firewalking	Técnica creada en 1998 con el objetivo de conocer las políticas de filtrado de un firewall.
Firewall	Dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos con los que interactúa sobre una base de normas y otros criterios.
Flooding	Es la acción de enviar una cantidad muy grande de información a alguien o a algo para intentar que se sature.
Formulario	Se llama formulario a una plantilla o página que cuenta con espacios en vacíos con el fin de que sean rellenados por un usuario.
Frame	También conocido como trama, es un bloque de datos de una transmisión.
FTP (File Transfer Protocol)	Protocolo de red para la transferencia de archivos entre computadoras conectadas a una red TCP. Se sitúa en la capa de aplicación del modelo OSI. Está descrito en el RFC 959.
Función	Se le conoce así a un subprograma que forma parte de un programa principal que permite resolver una tarea específica.
Gateway	También conocido como puerta de enlace, es un dispositivo activo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al usado en la red destino.
Hacker	Un especialista con grandes habilidades computacionales, que busca obtener acceso no autorizado a sistemas sin ninguna intención maliciosa.
Hash	Se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, entre otras.
Heap	Estructura de datos del tipo árbol que contiene información perteneciente a un conjunto ordenado. Eta región queda disponible para las solicitudes de memoria dinámica al S.O. Su crecimiento va ligado a la disminución de la pila y viceversa.
Heap overflow	Error de software similar al *buffer overflow* que afecta al *heap,* permitiendo un acceso no autorizado a parte de la memoria.
Hipertexto	Es el nombre que recibe el texto que en la pantalla de un

	dispositivo electrónico conduce a otro texto relacionado. La forma más habitual de hipertexto en documentos es la de hipervínculos.
Hipervínculo	Elemento de un documento electrónico que hace referencia a otro recurso, por ejemplo, otro documento o punto específico del mismo.
Host	Término utilizado para referirse a las computadoras que, conectadas a una red, proveen y/o utilizan servicios a/de ella.
Hostname	Denominación otorgada por el administrador a una computadora.
HTML (HyperText Markup Languaje)	Se refiere al lenguaje de marcado predominante para la construcción de páginas web.
HTTP (HyperText Transfer Protocol)	Protocolo de comunicación que utiliza la WWW y que permite la interacción entre los servidores y el navegador. Trabaja en la capa de aplicación del modelo OSI y se encuentra definido bajo una serie de RFC's, siendo el más importante el 2616.
ICMP (Internet Control Message Protocol)	Es un sub protocolo de control y notificación del Internet Protocol (IP) usado para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible. Se encuentra definido en el RFC 792.
IDS (Intrusion Detection System)	Aplicación utilizada para detectar accesos no autorizados a un equipo o red determinados. Normalmente, esta herramienta se integra conjuntamente un firewall.
Interfaz	Punto de interconexión entre dos entidades, sistemas, equipos, conceptos, por ejemplo.
IP (Internet Protocol)	Protocolo de comunicación no orientada a conexión, funciona bajo la capa 3 del modelo OSI. Se encuentra descrito por el RFC 791.
IRC (Internet Relay Chat)	Protocolo de comunicación en tiempo real basado en texto. Se diferencia de la mensajería instantánea en que los usuarios no deben acceder a establecer la comunicación de antemano. Se encuentra definido por el RFC 1459.
Kernel	También llamado núcleo, es el responsable de facilitar el acceso seguro al hardware de la computadora a los distintos programas dentro de un sistema operativo.
keylogger	Tipo de software que se encarga de registrar las pulsaciones que se realizan en el teclado para posteriormente guardarla en un archivo. Generalmente, se usa con fines maliciosos.
LiveCD, LiveUSB	Es un sistema operativo almacenado en un medio extraíble (CD y USB, respectivamente) que puede ejecutarse desde éste sin necesidad de ser instalado. Utiliza memoria RAM como disco duro virtual y el propio medio como sistema de archivos.
Log	Término anglosajón equivalente a la palabra bitácora, se trata de un archivo que registra movimientos y actividades de un programa determinado (*log file*).
Malware	Del inglés malicious software, también conocido como *badware,* término general utilizado para definir una variedad de software malicioso, entre ellos virus informáticos, software espía, troyanos y amenazas similares.
Multicast	O multidifusión, se refiere al envío de la información en una red a múltiples destinos simultáneamente. En oposición al *multicast,* se encuentra el envío de un punto a otro denominado *unicast.*

NetBIOS(Network Basic Input Output System)	Es una API que complementa la BIOS de DOS al agregar funciones especiales para redes locales.
***NTFS* (New Technology File System**	Sistema de archivos de Windows NT incluido en las versions de Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista y Windows 7. NTFS permite definir el tamaño del cluster a partir de 512 bytes de forma independiente al tamaño de su partición.
OSI (Open System Interconnection)	Es el modelo de red descriptivo creado por la International Standarization Organization (ISO) en 1984 con el objetivo de convertirlo en estándar internacional de arquitectura de redes de computadoras.
Paquete	Cantidad mínima de datos que se transmiten en una red o entre dispositivos. Su longitud varía según el protocolo que los construya.
Pentesting	Es la acción que un hacker ético lleva a cabo para buscar vulnerabilidades potenciales en una infraestructura de red.
Phising	Término informático que denomina un tipo de delito encontrado dentro del ámbito de las estafas cibernéticas caracterizado por obtener información confidencial de forma fraudulenta suplantando a una entidad, generalmente bancaria.
Pila	Véase *buffer*.
Plug-in	Pequeños programas que se agregan a otro ya existente para ofrecer una nueva función, por ejemplo, parches para el navegador que permiten escuchar música o ver videos.
Pop-up	Mensaje que se despliega automáticamente en la pantalla sin antes ser solicitado expresamente por el usuario. Un *pop-up* puede ser una página completa o pequeñas ventanas.
Proceso	Se conoce así a un programa en ejecución.
Protocolo	Conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red.
Proxy	Servidor conectado normalmente al servidor WEB que almacena en caché la información recibida por los usuarios, así, si un usuario accede a través del proxy a un sitio anteriormente visitado, recibirá la información del servidor proxy y no del sitio real.
Puerto	Forma genérica de denominar a una interfaz a través de la cual los diferentes tipos de datos se pueden enviar y recibir. Dicha interfaz puede ser de tipo físico o lógico, a nivel de software, en cuyo caso se puede utilizar el término puerto lógico.
RAM (Random Acces Memory)	Se refiere al área de almacenamiento temporal de una computadora desde donde el procesador recibe instrucciones.
Root	En sistemas operativos del tipo Unix, *root* es el nombre convencional de la cuenta de usuario que posee todos los derechos en cualquier modo. Es también conocido como superusuario.
Router	Dispositivo que opera en la capa 3 del modelo OSI, para la interconexión de redes informáticas, que permite asegurar el enrutamiento de paquetes o las rutas que deben tomar los mismos.
Servidor	Se llama así a un dispositivo electrónico que, formando parte de una red, provee servicios a otros dispositivos a los que se les denomina clientes.

Sintaxis	Conjunto de reglas que definen las secuencias correctos de los elementos de un lenguaje de programación.
Sniffer	Programa que monitoriza los paquetes de datos que circulan a través de una red. Tienen diversos usos como la detección de fallos de una red, o la interceptación de mensajes electrónicos, el robo de contraseñas por mencionar algunos.
Spam	Se denomina *spam* o correo basura, a todo tipo de comunicación no solicitada, realizada vía electrónica. De este modo, es *spam* cualquier mensaje no solicitado que tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa.
Spoofing	Se refiere al uso de técnicas de suplantación de identidad, generalmente con fines maliciosos o de investigación. Existen varios tipos: i. IP spoofing, que consiste en sustituir una dirección IP. ii. ARP spoofing, que se refiere a la suplantación de identidad mediante la falsificación de la tabla ARP. iii. DNS spoofing, suplantación de identidad por nombre de dominio. iv. Web spoofing, suplantación de una página web real. v. Mail spoofing, suplantación de la cuenta de correo electrónico de alguien.
SQL (Structured Query Languaje)	Es un lenguaje del tipo declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ésta. Una de sus características es el manejo del álgebra y cálculo relacional, lo que permite efectuar consultas con el fin de recuperar información específica de forma sencilla, o realizar cambios sobre ella.
SSH (Secure SHell)	Dícese del protocolo que facilita las comunicaciones seguras entre dos equipos usando una arquitectura cliente/servidor. Trabaja bajo la capa de aplicación del modelo OSI. Se encuentra referido por el RFC 4251.
SSID (Service Set IDentifier)	Es un código incluido en todos los paquetes de red inalámbrica para identificarlos por parte de una red. A menudo, al SSID se le conoce como nombre de la red. Existen algunas variantes del SSID. Las redes ad-hoc que consisten en máquinas cliente sin punto de acceso, utilizan el BSSID (Basic Service Set Identifier); mientras que en las redes en infraestructura que incorporan un punto de acceso, se utiliza el ESSID (La E significa extendido).
Switch	Dispositivo que opera en la capa 2 del modelo OSI, para la interconexión de redes informáticas, que permite interconectar dos o más segmentos de red, pasando datos de un segmento a otro de acuerdo a la dirección MAC de destino.
TCP (Transmissión Control Protocol)	TCP es un protocolo de comunicación orientado a conexión perteneciente a la capa 4 del modelo OSI. Está descrito en el RFC 793.
Telnet (Telecommunication NETwork)	Protocolo de comunicación entre computadoras del tipo cliente-servidor que permite acceder mediante una red a otra máquina con el fin de controlarla remotamente. Actualmente en desuso por su carencia de cifrado en su comunicación. Trabaja bajo la capa de aplicación del modelo OSI y está referenciado por el RFC 854.

Three-Way Hand-Shake.	Proceso propio del protocolo TCP que ocurre entre un cliente y un servidor cuando se inicia una conexión TCP, esta se realiza en tres pasos: i. El sistema cliente envía un paquete con la bandera SYN al sistema destino. ii. El equipo destino responde con un paquete con las banderas SYN-ACK confirmando la recepción del paquete SYN inicial. iii. Para finalizar, el cliente reconoce la recepción del SYN enviado durante el segundo paso mediante el envío de un paquete ACK. En este momento queda establecida la conexión y la transferencia de datos puede iniciar.
Timestamp	Es una secuencia de caracteres que denotan la hora y fecha en la cual ocurrió un evento. Son típicamente usados para el seguimiento de eventos, siendo cada uno de ellos un log marcado.
Trama	Véase Paquete.
Tunneling	Técnica consistente en encapsular un protocolo de red dentro de otro creando lo que se conoce como un túnel dentro de una red de computadoras. El uso de este técnica puede perseguir diferentes objetivos, como por ejemplo la comunicación *multicast*, redirección de tráfico o el violar las políticas de seguridad de una red.
UDP (User Datagram Protocol)	Es un protocolo mínimo perteneciente al nivel de transporte del modelo OSI documentado en el RFC 768. Generalmente es usado junto a protocolos tales como DHCP y DNS.
Unicast	Se refiere a la comunicación establecida entre un solo emisor y un solo receptor.
WEP(Wired Equivalent Privacy)	Es el sistema de cifrado incluido en el protocolo IEEE 802.11 para redes Wireless. Está basado en el algoritmo RC4, que utiliza claves de 64 bits o de 128 bits.
Windows Task Manager	Utilidad que provee información acerca de programas y procesos que se encuentran corriendo en la computadora, entre otras cosas.
WPA (Wifi Protect Access)	Mecanismo de control de acceso a una red inalámbrica, pensando en la idea de eliminar las debilidades de WEP.
WWW (World Wide Web)	WWW o Web es el servicio de información distribuido, basado en hipertexto, cuya información puede ser de cualquier formato (texto, gráfico, audio, imagen fija o en movimiento) y fácilmente accesible a los usuarios mediante navegadores Web. Fue creado como tal en 1990 por Tim Berners-Lee y Robert Cailliau.