Glosario.

Amenaza: Circunstancia, suceso o persona con el potencial para dañar un sistema mediante la destrucción, la divulgación, la modificación de datos o la negación de servicios.

Apache: Programa que opera en la capa de aplicación del modelo OSI, el cual emplea el protocolo HTTP para servir documentos HTML. Es desarrollado por la organización Apache Software Foundation.

DBMS (DataBase Management System): Son sistemas gestores de bases de datos, que permiten el manejo adecuado de datos, con un esquema de almacenamiento ordenado que permite realizar consultas ordenadas y controladas. Utilizan el lenguaje SQL.

DoS (Denial of Service): Se trata de un ataque que tiene como consecuencia la no disponibilidad de un servicio a usuarios autorizados de este. Por lo general es provocado por el envío de peticiones masivas al servidor que provee el servicio, lo que propicia que el servidor sea incapaz de atender las peticiones de los usuarios.

Exploit: Proceso que se encarga de encontrar y explotar vulnerabilidades en un sistema.

Firewall: Es un sistema diseñado para impedir el acceso no autorizado o el acceso desde una red privada. Pueden implementarse firewalls en hardware, software o en ambos. Los firewalls se utilizan con frecuencia para impedir que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet. El firewall personal protege al equipo frente a ataques de Internet, contenidos Web peligrosos, análisis de puertos y otros comportamientos de naturaleza sospechosa.

FTP (File Transfer Protocol): Se trata de un protocolo que tiene como objetivo promover el intercambio de ficheros entre computadoras de manera remota de manera rápida y eficiente. Las especificaciones completas de este protocolo se encuentran descritas en el RFC 959.

HTML (HyperText Markup Languaje): Es un lenguaje de marcado de hipertexto, que se basa en el uso de etiquetas y que es interpretado por clientes HTTP (navegadores web). Estándar para las páginas de internet.

HTTP (HyperText Transfer Protocol): Es un protocolo de la capa de aplicación con la ligereza y la velocidad necesaria para sistemas de información hipermedia colaborativos y distributivos. HTTP ha estado en uso desde 1990 por el *World-Wide Web*. Las especificaciones del protocolo HTTP se encuentran descritas en el RFC 1945, dicha especificación describe las características que se encuentran implementadas en la mayor parte de clientes y servidores HTTP.

HTTPS(HyperText Transfer Protocol Secure): Es una versión segura del protocolo HTTP, la cual permite transacciones seguras a través de la red, como por ejemplo en operaciones bancarias.

IIS (Internet Infirmation Services): Es una aplicación desarrollada por Microsoft Coorporation, que es útil para proveer servicios de Correo y Web por medio de los protocolos SMTP, HTTP y FTP.

MySQL: Es un manejador de base de datos (véase DBMS) soportado desde 2008 por Sun Microsystems, es ampliamente conocido por su gran adaptación con los sistemas operativos de la familia Linux, con el servidor Web Apache y el lenguaje PHP, a lo que se conoce como LAMP (Linux, apache, MySQL, PHP), aunque también tiene una gran adaptación con Java.

Netcraft: Compañía que tiene el objetivo de proveer servicios de seguridad en Internet, incluyendo servicios anti-fraude y anti-phishing, pruebas de seguridad en aplicaciones, revisión de códigos pruebas automáticas de penetración en sistemas.

OWASP (Open Web Application Security Project): Es una comunidad libre y abierta centrada en la mejora de la seguridad del software de aplicación. Su misión es hacer visible la seguridad de las aplicaciones, de modo que las personas y organizaciones puedan tomar decisiones informadas sobre los verdaderos riesgos de seguridad en las aplicaciones. La OWASP Foundation es una organización sin fines de lucro.

Phishing: Es un ataque que suele comenzar con un mensaje de correo electrónico falseado, que en apariencia procede de una compañía reconocida y fiable. En tal mensaje se le engaña a un usuario para que revele información confidencial como contraseñas de tarjetas de crédito y de cuentas bancarias. En dichos mensajes de correo, se incluyen ligas en las que se guía al usuario a una réplica de un sitio de internet reconocido en donde el usuario engañado revela su información confidencial, la cual es utilizada para cometer fraudes.

PHP: Es un lenguaje de *scripting* de propósito general, que es especialmente orientado a la construcción de sitios web dinámicos.

SSH (Secure Shell): Es un protocolo para el inicio de sesión remoto y el uso de otros servicios de red de manera segura. Sus especificaciones completas se encuentran descritas en el RFC 4254.

SSL (Secure Socket Layer): Se trata de un protocolo que nos permite hacer uso de comunicaciones cifradas para la transmisión segura de datos. SSL fue desarrollado conjuntamente por Netscape Communications y RSA Data Security.

TLS (Transport Layer Security): El protocolo TLS permite a aplicaciones cliente/servidor comunicarse a través de un canal seguro, diseñado para prevenir la escucha, manipulación o falsificación de mensajes.

Vulnerabilidad: Una vulnerabilidad es un estado en un sistema informático que: permite a un atacante ejecutar comandos como otro usuario, permite a un atacante acceder a los datos en contra de las restricciones de acceso especificadas para esos datos, permite a un atacante hacerse pasar por otra entidad o permite a un atacante realizar una negación de servicio.
XSS (Cross-Site Scripting): Es una vulnerabilidad que permite a un atacante inyectar código (por lo regular de JavaScript o HTML) en una aplicación web, modificando el comportamiento habitual de la aplicación.