Diccionario de Términos en *Seguridad Informática*

Anti-spam:
Herramienta, software o aplicación informática que se encarga de eliminar el correo no deseado.

Anti-spyware:
Herramienta, software o aplicación informática que se encarga de eliminar aplicaciones espía.

Anti-virus:
Herramienta, software o aplicación encargada de identificar programas que son diseñados con intenciones mal intencionadas, destructivas o dañinas para el sistema operativo o los datos del usuario.

Aplicación (Informática):
La aplicación es un programa que poseé interfaz y métodos, que realizan, una o más tareas determinadas en un sistema informático, o con dispositivos para la computadora.

Ataque de Denegación de Servicio (DDoS):
Ataque dirigido y propagado por la red que inhabilita el acceso a recursos o servicios a usuarios autenticados en un sistema de modo que el destino queda inaccesible para los usuarios.

Boot:
Instrucciones de inicio de un sistema informático.

Bot:
Usuario automatizado que esta programado para ejercer ciertas tareas que requerirían a usuarios reales para ello.

Botnet:
Una botnet es un conjunto de ordenadores, denominados “zombie bots” (usuarios zombis automatizados), que están infectados con algunos tipos de programas que son controlados remotamente por un atacante y puede ser utilizado para realizar actividades maliciosas y mal intencionadas.

Ciberseguridad:
Es el área relacionada con la informática y la telemática que se enfoca en proteger infraestructuras informáticas con todo el hardware y el software del que se disponga.

Cracker:
Persona dedicada a romper la seguridad de un sistema informático sin autorización, por motivos de protesta, retribución económica o simplemente por desafiar la seguridad del sistema.

Crimeware:
Software malicioso utilizado para cometer delitos que engloba a los Troyanos, a los Virus, al Spyware y a las Botnets.

Cibercriminal:
Persona que usa sistemas informáticos para cometer sus delitos.

Diccionario de Términos en *Seguridad Informática*

Disco USB:
Dispositivo que se enchufa en “caliente” (mientras esta encendido el dispositivo que lo acepte), con el que poder leer y escribir en una memoria física no volátil.

Exploit:
Vulnerabilidad explotada por un programa para robar información o ejecutar código malicioso o mal intencionado que puede ser dañino para el hardware o el software atacado.

Firmware:
Es el conjunto de instrucciones de un programa que reside en la memoria ROM, flash o similar de un determinado hardware. Estas instrucciones fijan la lógica primaria que ejerce el control de los circuitos de algún dispositivo.

Hacker:
Persona con grandes conocimientos de informática que se dedica a detectar fallos en sistemas informáticos, reportar y/o entregar una solución en algunos casos, sean estos referentes a la seguridad o no.

Hardware:
Dispositivo o conjunto de ellos que ejercen determinadas tareas encargadas por un sistema operativo, firmware o software especifico para controlar estos dispositivos.

Herramientas:
Software, Aplicación o conjunto de aplicaciones destinadas para resolver algunas tareas en especificas entre los dispositivos conectados.

Malware:
Es una aplicación malintencionada que una vez instalada se encarga de robar información para cometer fraudes o robos de identidad.

Memoria:
En computación, es una sección designada a el almacenamiento y recuperación de datos e información.

Memoria RAM:
Memoria de acceso aleatorio, usada para leer y escribir información volátil (que no va a ser almacenada a largo plazo).

Memoria USB:
La Memoria USB (Universal Serial Bus) es un Dispositivo de Almacenamiento que utiliza memoria flash para leer y escribir. Es un tipo de memoria no volátil que conserva los datos una vez desconectado el dispositivo.

Navegador Web:
Un navegador Web es una aplicación de software que es usada para visitar sitios web. Ejemplos de estos son Firefox, Google Chrome, Microsoft Edge, Opera, Etc...

Diccionario de Términos en *Seguridad Informática*

Pharming:
El pharming es la captura de información confidencial a través de la re-dirección de tráfico a un sitio web falso.

Phising:
Técnica que se enfoca en copiar sitios Web con el fin de robar información sensible de los usuarios, cómo por ejemplo el nombre de usuario y su contraseña, números de tarjetas de crédito haciendo creer al usuario que esta en la página Web real cuando es una ficticia.

Políticas de seguridad:
Son una serie de sentencias formales (normas) que deben cumplir todas las personas que tengan acceso a cualquier información y tecnología de una organización.

Programa (informático):
Conjunto de métodos algorítmicos que pueden ejercer alguna tarea determinada.

Protocolo:
Conjunto de reglas de comunicación que rigen el intercambio de información entre dos equipos o sistemas conectados entre sí.

Ransomware:
Programa o aplicación que bloquea el acceso total al usuario y pide dinero a cambio para habilitar el acceso.

Seguridad informática:
Se encarga de proteger los activos de informáticos, entre los que se encuentran la información, infraestructura y usuarios.

Sistemas Zombis:
Computadores o servidores controlados remotamente que envían información a la fuente de origen que la solicita, sin notificarlo al usuario.

Software:
Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas gracias a su programación concurrente.

Spam:
Esto es correo electrónico con contenido idéntico enviado de forma masiva, también conocido como correo basura.

Spyware:
Software organizado por paquetes para realizar seguimiento de un usuario el cual envía información de los usuarios a la fuente original sin solicitar permisos al usuario atacado.

Diccionario de Términos en *Seguridad Informática*

SQL:
Structured query language o lenguaje de consulta de estructurado, es un lenguaje diseñado para manejar grandes volúmenes de datos. Es el lenguaje basado en el álgebra relacional que es utilizado en gestión de bases de datos y permite entre otras cosas hacer consultas, inserciones y modificaciones de esquemas.

Trackware:
Programa diseñado con el fin de rastrear las acciones que realiza el usuario mientras visita Internet, con el fin de crear anuncios y publicidad mejorados.

Troyano:
Puerta de entrada a una aplicación maliciosa. Se caracterizan por estar constituidas de dos partes, una que envía información sin consentimiento del usuario y la otra parte recibe lo que la aplicación maliciosa envía.

Virus:
Programa que se establece en el disco duro, replicando acciones, que sin permiso del usuario, afectan al sistema operativo.

Vulnerabilidad:
Es un fallo de programación, configuración o diseño. Permite de alguna manera a los atacantes alterar el comportamiento normal de un programa y realizar alguna acción maliciosa o malintencionada.

0 day exploit:
Es una vulnerabilidad o error del sistema del que no se sabia nada y empieza desde el día 0 en el que se encuentra la vulnerabilidad que podría darse en un sistema operativo, firmware o software, hasta el día en el que se soluciona.

Créditos del Documento

Fuentes Consultadas:
https://www.google.es/
https://es.wikipedia.org/wiki/Wikipedia:Portada
https://platzi.com/

Ampliación, Aportes y Mejoras Por:
Pol Flórez - https://www.dos-a-la-tres.com/