**Términos del glosario de la semana 4**

**Términos y definiciones del curso 5, semana 4**

**Agente de amenaza:** Persona o grupo de personas que representa una amenaza intencional para computadoras, aplicaciones o redes.

**Adware:** Tipo de software legítimo o malicioso que se utiliza para mostrar publicidad digital en las aplicaciones.

**Amenaza persistente avanzada (APT):** Situación en la que un agente de amenaza accede sin autorización a un sistema y permanece en él durante un periodo de tiempo prolongado.

**Amenaza:** Cualquier circunstancia o evento que pueda afectar negativamente a los activos.

**Angler phishing:** Tipo de ataque de suplantación de identidad en el que un agente de amenaza se hace pasar por representantes del servicio al cliente de una empresa en las redes sociales.

**Aplicación potencialmente no deseada (PUA):** Tipo de software que se incluye con programas legítimos y que puede mostrar anuncios, causar la ralentización del dispositivo o instalar otro software no deseado.

**Árbol de ataque:** Diagrama que muestra las amenazas a los activos y cómo se relacionan entre sí.

**Ataque de “agujero de agua” (watering hole)**: Tipo de ataque en el que un agente de amenaza compromete un sitio web visitado con frecuencia por un grupo específico de usuarios.

**Ataque de caza de ballenas (Whaling):** Tipo de ataque de suplantación de identidad dirigido específicamente a personal de alto rango de una organización.

**Ataque de inyección:** Ataque mediante el cual se introduce un código malicioso en una aplicación vulnerable.

**Ataque de secuencia de comandos en sitios cruzados, o entre sitios (XSS):** Tipo de ataque de inyección que consiste en insertar código en un sitio web o aplicación web vulnerables.

**Ataque de suplantación de identidad**: (Consultar **Phishing**).

**Ataque XSS almacenado:** Tipo de ataque en el que se inyecta un script o secuencia de código malicioso directamente en el servidor.

**Ataque XSS basado en DOM:** Tipo de ataque en el que se inyecta un código malicioso directamente en la página web que carga un navegador.

**Ataque XSS reflejado:** Tipo de ataque en el que se envía un script malicioso a un servidor que se activa durante la respuesta del mismo.

**Botnet:** Conjunto de computadoras infectadas por software malicioso (malware), que están bajo el control de un solo agente de amenaza, conocido como el “bot-herder”.

**Caballo de Troya (Troyano):** Software malicioso que parece un archivo o programa legítimo.

**Cebo (Baiting):** Táctica de ingeniería social que incita a las personas a comprometer su seguridad.

**Criptojacking:** Tipo de software malicioso que instala un programa para minar criptomonedas ilegalmente.

**Dropper:** Tipo de troyano que instala un programa o archivo malicioso en un equipo de destino.

**Exploits basados en la web:** Fragmento de software o secuencia de comandos que se aprovecha de un error o vulnerabilidad de codificación en una aplicación web.

**Gestión de identidad y acceso (IAM):** Conjunto de procesos y tecnologías que ayuda a las organizaciones a administrar las identidades digitales en su entorno**.**

**Gusano:** Software malicioso que se reproduce por sí mismo y se propaga a través de los sistemas y redes.

**Hacker:** Cualquier persona o grupo de personas que utiliza computadoras para obtener acceso no autorizado a los datos. Se diferencia entre hacker ético, que es quien tiene como objetivo mejorar la seguridad y prevenir posibles ataques, y no ético o malintencionado, que es aquel que busca comprometer la seguridad de un sistema informático o de una red, con fines delictivos.

**Ingeniería social:** Técnica de manipulación que busca engañar a las personas con el fin de que revelen información o realicen determinadas acciones.

**Inyección SQL:** Tipo de ataque que consiste en ejecutar consultas maliciosas, con el fin de manipular a una base de datos y acceder a la información.

**Kit de phishing:** Conjunto de herramientas de software, preparado para lanzar una campaña de phishing con facilidad.

**Malware sin archivos:** (Consultar **Software malicioso sin archivos**)**.**

**Malware:** (Consultar **Software malicioso**).

**Modelado de amenazas:** Proceso de identificación de activos, sus vulnerabilidades y su exposición a las amenazas, con el objetivo de planificar y optimizar las operaciones de seguridad de la red.

**Phishing (Suplantación de identidad):** Uso de comunicaciones digitales en las que se suplanta la identidad de una persona o empresa con el objetivo de engañar a otras personas para que revelen datos confidenciales o implementen un software malicioso.

**Proceso de simulación de ataques y análisis de amenazas (PASTA):** Metodología de modelado de amenazas de uso común en numerosas industrias

**Quid pro quo:** Tipo de cebo utilizado para engañar a una persona y hacerle creer que será recompensada si comparte un acceso, información o dinero.

**Ransomware:** (Consultar **Secuestro de datos**)**.**

**Rootkit:** Software malicioso que proporciona acceso administrativo remoto a una computadora.

**Saneamiento de entradas:** Programación que valida las entradas de usuarios y de otros programas.

**Scareware:** Software malicioso que emplea tácticas para asustar a los usuarios con el fin de que infecten su dispositivo.

**Secuestro de datos (Ransomware):** Ataque malicioso que consiste en cifrar los datos de una organización para exigir el pago de un rescate para restablecer el acceso a ellos.

**Sentencia preparada (Prepared Statement):** Técnica de codificación que ejecuta sentencias SQL antes de pasarlas a una base de datos.

**Sistema de detección de intrusiones (IDS):** Aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones.

**Smishing**:Tipo de ataque de suplantación de identidad (phishing) que utiliza mensajes de texto para engañar a los usuarios con el fin de obtener información confidencial.

**Software malicioso (Malware):** Programa diseñado para dañar dispositivos o redes.

**Software malicioso sin archivos (Malware sin archivos):** Tipo de software malicioso que utiliza programas legítimos que ya están instalados en una computadora para infectarla.

**Phishing localizado (Spear phishing):** Ataque de correo electrónico malicioso dirigido a una persona o grupo de personas específico que parece provenir de una fuente confiable

**Spyware:** Software malicioso que se usa para recabar y vender información sin el consentimiento de sus propietarios.

**SQL, Structured Query Language** (Lenguaje de consulta estructurado): Lenguaje de programación utilizado para crear, interactuar y solicitar información de una base de datos.

**Tailgating:** Táctica de ingeniería social en la que personas no autorizadas siguen a una persona autorizada hasta ingresar a una zona restringida.

**Vishing:** Tipo de estafa por suplantación de identidad en la que se busca obtener información sensible a través de una llamada telefónica.

Marcar como completo

Me gusta

No me gusta

Informar de un problema