**TAREA 54: DICCIONARIO**

* **PENTERSTING:** Método de evaluar los sistemas de información y la red de una organización simulando un ataque para encontrar vulnerabilidades que permitirían a potenciales atacantes robar información o afectar los activos de la misma. Las medidas y controles de seguridad son analizados para encontrar debilidades, fallos técnicos y vulnerabilidades.

Estas pruebas se realizan utilizando técnicas y herramientas similares y en muchos casos las mismas que utilizan los atacantes, pero sin perjudicar a la organización ni realizar actividades ilícitas. Los test de intrusión realizados para otras partes deben ir precedidas de un acuerdo firmado donde se defina el alcance del mismo, así como las restricciones y/o limitaciones de las pruebas.

* **CIBERSEGURIDAD:** La seguridad informática, también conocida como ciberseguridad, es el área relacionada con la informática y la telematica que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de redes de las computadoras. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas, y leyes concebidas para minimizar los posibles riesgos a la infraestructura y/o a la propia información.
* **RANSOMWARE:** En castellano “secuestro de datos”, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.
* **PHISHING:** Es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar. Para realizar el engaño, habitualmente hace uso de la ingeniería social explotando los instintos sociales de la gente, como es de ayudar o ser eficiente. A veces también hace uso de procedimientos informáticos que aprovechan vulnerabilidades. Habitualmente el objetivo es robar información pero otras veces es instalar malware, sabotear sistemas, o robar dinero a través de fraudes.
* **SPYWARE:** Es un malware que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador. Un programa espía típico se autoinstala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de internet y mostrando anuncios relacionados. Sin embargo, a diferencia de otros virus, no se intenta replicar en otros ordenadores, por lo que funciona como parásito.
* **TROYANO:** Malware que presenta al usuario como un programa aparentemente legitimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo afectado. Los troyanos pueden realizar diferentes tareas, pero, en la mayoría de los casos, crean una puerta trasera que permite la administración remota a un usuario no autorizado.