¿Qué es la seguridad ofensiva en la ciberseguridad?

La **seguridad ofensiva** o "**pentesting**" es la acción de realizar simulaciones de ataques de hacking o ciberataques a los sistemas informáticos, redes, aplicaciones, etc. , con la intención de encontrar y explotar vulnerabilidades y de esa forma lograr acceder al sistema, red o aplicación en concreto.

Hay que tener en cuenta que la seguridad ofensiva se hace en entornos controlados o bajo contrato en situaciones de la vida real.

El objetivo principal de la seguridad ofensiva es ayudar a mejorar la seguridad informática identificando y explotando vulnerabilidades en los sistemas para que posteriormente sean reportadas y corregidas.

Made by Astaroz

Técnicas de la seguridad ofensiva en el hacking ético

1. Pentesting:

Como hemos visto anteriormente, el **pentesting** es la acción de hacer simulaciones de hacking en sistemas, redes, dispositivos y aplicaciones para evaluar la seguridad de éstos.

2. Ingenieria social:

Esta técnica se basa en engañar y manipular a usuarios para tener acceso a sus dispositivos y sistemas informáticos. Para conseguirlo el atacante se suele hacer pasar por una entidad importante (banco, gobierno, etc.) o también puede hacerse pasar por un compañero, jefe, o encargado importante en un entorno empresarial o de trabajo.

Made by Astaroz

3. Explotación de vulnerabilidades:

Esta técnica se basa en buscar, identificar y explotar vulnerabilidades o puntos débiles de un sistema informático, red informática o de un sistema/entorno informático en general. El objetivo de esto es explotar vulnerabilidades para ganar acceso al sistema víctima.

4. Desarrollo de exploits:

Un exploit es un software o fragmento de código que tiene la función de explotar una vulnerabilidad para conseguir acceso al sistema víctima, normalmente el código que tienen es código malicioso.

5. Auditorias empresariales:

De forma resumida, una auditoría en el mundo de la ciberseguridad es un proceso en el que se evalúa la seguridad de una empresa frente a ciberataques, se investiga cómo está montada la estructura informática de la empresa, detectar y reportar vulnerabilidades en las redes o equipos físicos de la empresa y como último paso, se notifica y reporta a la empresa sobre todas las vulnerabilidades y puntos débiles encontrados en sus sistemas y redes para que sean corregidos.