SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

101.1.0. Seguridad Informática
Hacking ético 1

JOSÉ PABLO HERNÁNDEZ

INTRODUCCIÓN HACKING ÉTICO

- **El hacking ético es la acción que realiza un individuo que utiliza los conocimientos de informática y seguridad para detectar fallos y vulnerabilidades de seguridad en los sistemas, siempre con el objetivo de informar de éstas a las organizaciones y que puedan tomar medidas al respecto.**

- **Los hackers éticos suelen realizar pruebas o tests denominados "tests de penetración". El objetivo de estos test es poder burlar las vallas de seguridad que tiene la red de la organización que contrató sus servicios, siempre con la única intención de demostrar las vulnerabilidades.**

INTRODUCCIÓN HACKING ÉTICO

BENEFICIOS DEL HACKING ÉTICO PARA LAS EMPRESAS

Hoy en día la protección de los sistemas informáticos y las redes es fundamental para cualquier empresa.

Con su labor, el hacker ético aporta una serie de beneficios fundamentales como:

- Mejora la ciberseguridad detectando las vulnerabilidades y proponiendo soluciones.
- Evita que los equipos queden inutilizados reforzando los protocolos de seguridad
- Previene el espionaje industrial y salvaguarda la integridad de la información de los clientes
- Conciencia sobre el valor de la ciberseguridad para impulsar las mejoras de los procesos internos.

¿POR QUÉ ÉTICO?

Para emular la metodología de ataque de un intruso informático y no serlo, tiene que haber ética de por medio, más allá de todas las condiciones, términos y activos que haya alrededor del caso.

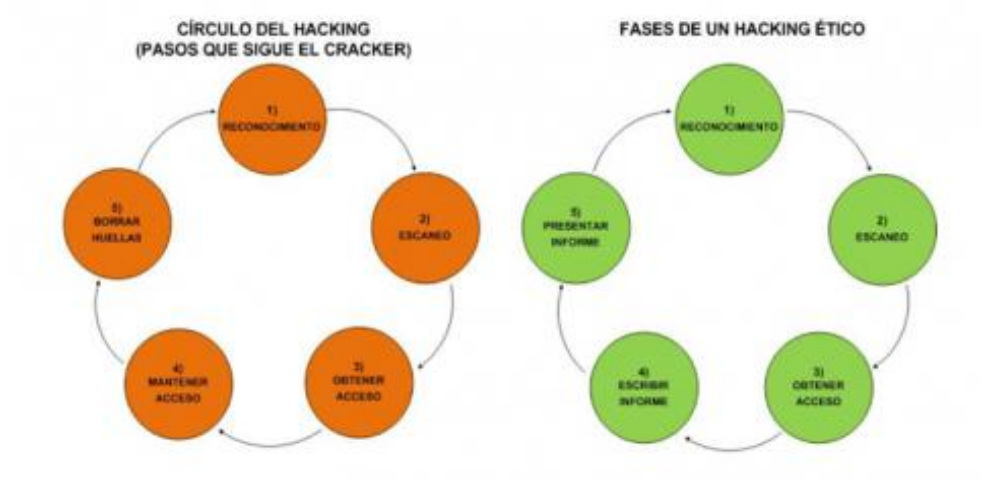
La ética implica que el trabajo y la intervención del profesional en seguridad informática o de la información no comprometen de ningún modo los activos de la organización, que son los valiosos datos con los que ella cuenta.

¿POR QUÉ ÉTICO?

Conductas mínimas que éste debe cumplir:

- Hacer su trabajo de la mejor manera posible.
- Dar el mejor reporte.
- Acordar un precio justo.
- Respetar el secreto.
- No hablar mal ni inculpar a un administrador o equipo de programadores.
- No aceptar sobornos.
- No manipular o alterar resultados o análisis.
- Delegar tareas específicas en alguien más capacitado.
- No prometer algo imposible de cumplir.
- Ser responsable en su rol y función.
- Manejar los recursos de modo eficiente.

FASES DEL HAKING ÉTICO



- Reconocimiento
- Escaneo
- Obtener acceso (explotación)
- Mantener acceso (redactar informe)
- Limpieza de huellas (presentar informe)

RECONOCIMIENTO

Fases en el pre-ataque (obtención de información):

- **Trashing**
- **Footprinting (OSINT)**

Obtención de los perfiles de seguridad de una organización haciendo uso de una metodología (footprinting).

El resultado del footprinting es un perfil único de la organización en cuanto a sus redes(Internet / Intranet / Extranet / Wireless) y sistemas.

RECONOCIMIENTO. TRASHING.

El trashing o dumpster diving es una técnica de obtener información privada, que consiste en revisar la basura de la persona u organización a investigar.

Es empleada principalmente por crackers (también conocidos como hackers de sombrero negro) y periodistas, aunque también para investigación privada.

La información obtenida puede variar desde nombres de usuario y claves, información personal y otras formas de información sensible.

RECONOCIMIENTO. FOOTPRINTING

El Footprinting comienza por la determinación del target, para luego averiguar información específica utilizando métodos no intrusivos.

Una herramienta fundamental son las búsquedas online, utilizando Google u otro buscador. Es importante conocer en profundidad las características avanzadas de búsqueda (site:, intitle:, allinurl:, etc.)

RECONOCIMIENTO. FOOTPRINTING

De manera general puede ser dividida en siete pasos.

Detectar la información inicial

Ubicación del rango de red

Trashed, Footprinting

Comprobación de equipos activos

Descubrimiento de puertos abiertos y puntos de acceso

Detección del sistema operativo

Descubrimiento de servicios en los puertos

Mapeo de red

RECONOCIMIENTO. FOOTPRINTING

Algunas fuentes comunes de información incluyen el uso de:

- Domain name lookup
- Whois

Nslookup

La mayor parte de la información puede obtenerse libremente y de manera legal.

Es muy importante comprender el sistema de resolución de nombres de dominio (DNS) para lograr una profunda comprensión de esta etapa y del funcionamiento de Internet.

RECONOCIMIENTO. FOOTPRINTING

Inteligencia competitiva:

Implica la averiguación de información sobre la competencia (productos, tecnologías, marketing, etc.)

Existen diversas herramientas que pueden ser utilizadas para esto.

La inteligencia competitiva incluye diversos temas como puede ser:

- Recopilación de datos
- Análisis de datos
- Verificación de información
- Seguridad de la información

Existen muchas empresas privadas que ofrecen el servicio de inteligencia competitiva

RECONOCIMIENTO. FOOTPRINTING

Buscando en Internet la dirección de correo electrónico o el nombre de una persona podemos encontrar en las listas de correo, foros, etc. información sobre la empresa donde trabaja.

Otra fuente de información útil son las redes sociales y los sitios de empleos.

CONCEPTO DE OSINT

Del inglés “Open Source Intelligence” hace referencia a la “inteligencia de fuentes abiertas”.

Es un procedimiento de obtención de información de fuentes abiertas, es decir, accesible a todo el mundo:

- Medios de comunicación: revistas, periódicos, radio, etc.
- Información pública de fuentes gubernamentales.
- Foros, redes sociales, blogs, wikis, etc.
- Conferencias, simposios, «papers», bibliotecas online, etc.

CONCEPTO DE OSINT

Algunos ejemplos de la utilización de OSINT son los siguientes:

- Conocer la reputación online de un usuario o empresa.
- Realizar estudios sociológicos, psicológicos, lingüísticos, etc.
- Auditoría de empresas y diferentes organismos con el fin de evaluar el nivel de privacidad y seguridad.
- Evaluar tendencias de mercados.
- Identificación y prevención de posibles amenazas en el ámbito militar o de la seguridad nacional.
- Como aspecto negativo, es utilizado por cibercriminales para lanzar ataques APT (Advanced Persistent Threat o tipos sofisticados de ciberamenazas) y «Spear Phishing» (estafa de correo electrónico o comunicaciones dirigida a personas, organizaciones o empresas específicas).

https://www.incibe-cert.es/blog/osint-la-informacion-es-poder