¿Qué Comprende Ethical Hacking?

Ricardo Fernando Jáuregui Lima
Universidad Mayor de San Andrés
Carrera de Informática
Análisis y Diseño de Sistemas de Información
in_quie_to@hotmail.com

RESUMEN

El presente artículo nos habla sobre los diferentes componentes y herramientas que comprende Ethical Hacking que significa hacker ético.
En el hacker ético existe una organización internacional conocida como EC-Countil dedicada al desarrollo de cursos y al otorgamiento de certificaciones en las áreas de Seguridad de la Información y Comercio Electrónico, ya que algunas personas opinan que la organización es la mejor el área de informática por tener un nivel bastante bueno y hacer que los certificados sean 100 % efectivos, son profesionales dotados de habilidades que sirven para encontrar debilidades en los sistemas utilizando las herramientas de un hacker malicioso como ser footprinting Y reconocimiento, exploración de redes y los famosos virus conocidos como los caballos de troya.

Palabras Clave

Footprinting, Ec-Council, backdoors, sniffers, perifericos.

1.-INTRODUCCION

Ethical hacking que significa la ética hacker es aplicada en las comunidades virtuales o de la ciber comunicación.
La certificación de este brinda un amplio conocimiento sobre las más actuales herramientas que nos permiten proteger un sistema de ataques y diversos entornos en el área de la seguridad informática. Los que hacen posible este tipo de tareas son conocidos como la organización Ec-Countil que son profesionales dotados de habilidades para encontrar debilidades o vulnerabilidades en los sistemas utilizando el mismo conocimiento y herramientas de un hacker malicioso.

2. ¿QUE MANEJA EL ETHICAL HACKING?

Como mencionamos anteriormente a los Ec-Council estos maestros de la información son los que más manejan los siguientes aspectos que mencionaremos a continuación:

- Footprinting y reconocimiento.
- Exploración de redes.
- Caballos de Troya y backdoors.
- Sniffer.

2.1. FOOTPRINTING Y RECONOCIMIENTO

La fase conocida como Footprinting en un proceso que consiste en la búsqueda y recolección de cualquier tipo de información de un objetivo que pueda ser capturada de forma pasiva, es decir, sin el uso de herramientas que realicen escaneos o ataques de reconocimiento de la plataforma objetivo. La información recolectada puede estar en el contexto público o privado pública.

Los usuarios malintencionados también realizan el reconocimiento como primer paso en un eficaz ataque.

2.2. EXPLORACION DE REDES

Estos hackers que exploran las redes son conocidos como:

- Hackers de sombrero blanco.
- Hackers de sombrero negro.

Los hackers de sombrero blanco son conocidos como los hackers de buenas intenciones.

Mientras que los hackers de sombrero negro son conocidos como los hackers de malas intenciones, o también como crackers según los de sombrero blanco como podemos observar en la figura 2.

Figura 2

Como los hackers hoy en día se encontraron uno al otro, los intercambios de información aumentaron dramáticamente.

2.3. CABALLOS DE TROYA Y BACKDOORS

No son virus como tales, pero pueden realizar acciones destructivas como algunos virus. Los más peligrosos constan de dos programas, un servidor y un cliente. El servidor es por ejemplo nuestro Ordenador (para hacernos una idea) y el cliente es el usuario que intenta "entrar" en nuestro Ordenador
De acuerdo con un estudio de la empresa responsable del software de seguridad Bit Defender desde enero hasta junio de 2009, *"El número de troyanos está creciendo, representando el 83% del* malware detectado como se muestra en la figura 2

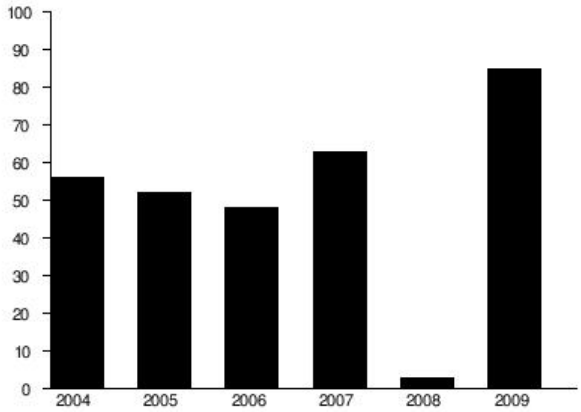

Figura 2

2.4. SNIFFER

Un sniffer es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador.

3. INGENIERIA SOCIAL

El término "**ingeniería social**" hace referencia al arte de manipular personas para eludir los sistemas de seguridad. Esta técnica consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo.

4. CONCLUSIÓN

Hoy en día la organización de los profesionales llamados Ec-countil son los que toman en cuenta estos aspectos ya que estos son lo que pueden tacar o defender un sistema ya que estos maestros del hacker informático son profesionales especializados en esta rama del hacker ético (Ethical Hacking).
"Hacker" es una persona que disfruta aprendiendo detalladamente de los sistemas de computación, y de cómo ampliar sus capacidades. A diferencia de la mayoría de usuarios de computadoras, quienes prefieren aprender solo lo más mínimo sobre estas.

El hacking ético se diferencia del hacking normal por el simple hecho que en el uno se pide permiso y en el otro no pues éticamente se da un aviso y se ejecuta el análisis y en algo no ético sencillamente se ingresa se ataca y no se dice nada.

5. REFERENCIAS

[1]**Titulo**: Que Comprende Ethical Hacking
Disponible en:
http://www.cttbolivia.org/CTT_Ethical_hacking.html

- [2]**Titulo**: Ethical Hacking

Disponible en:
https://es.wikipedia.org/wiki/%C3%89tica_hacker