Ethical Hacking

Ing. Julio Javier Iglesias Pérez

MCP | MCTS | MCSA: Security | MCSE: Security | MCITP: Enterprise Administrator | MCSA: Windows 8, Server 2008, Server 2012 | MCSE: Private Cloud | MCT | MCC | ITIL | ISFS | CEH | ISO 27001 Lead Implementer
MVP Enterprise Security


1. Introducción
Julio Javier Iglesias Pérez
C|EH Julio Iglesias Pérez

Introducción a la Seguridad Informática

- **Seguridad Informática:** Conjunto de medidas de prevención, detección y corrección orientadas a proteger la confidencialidad, integridad y disponibilidad de los recursos informáticos.

Terminologías

- **Amenaza:** Acción o evento que puede comprometer la seguridad. Es una potencial violación a la seguridad.
- **Vulnerabilidad:** Existencia de debilidad, diseño o implementación de un error que puede desencadenar un evento comprometedor indeseado e inesperado en los sistemas de información.
- **Blanco de evaluación:** Sistema, producto o componente que es identificado/sometido y que requiere de evaluación de seguridad.
- **Ataque:** Es un asalto a la seguridad del sistema y que es derivado de una amenaza inteligente. Un ataque es cualquier acción que viole la seguridad.
- **Explotación (exploit):** Es un método definido que viola la seguridad de un sistema de información a través de una vulnerabilidad.
- **Día cero:** Una amenaza informática que trata de explotar las vulnerabilidades de aplicaciones informáticas que son desconocidos para los demás o no revelada por el desarrollador de software.

Elementos de Seguridad

La seguridad se basa en:

- **Confidencialidad.-** Es la ocultación de información o de recursos.
- **Autenticación.-** Es la identificación y la garantía del origen de la información
- **Integridad.-** Es la fiabilidad de los datos o recursos en términos de prevención de cambios inadecuados y no autorizados
- **Disponibilidad.-** Es la capacidad de utilizar: la información o recursos deseados.

El triángulo de Seguridad, funcionalidad y fácil uso

Hacktivismo

Se refiere a la idea de realizar hacking con o por una causa.

Se compone de los hackers con una agenda social o política.

Tiene por objeto enviar un mensaje a través de su actividad hacker y la obtención de visión para su causa o para ellos mismos.

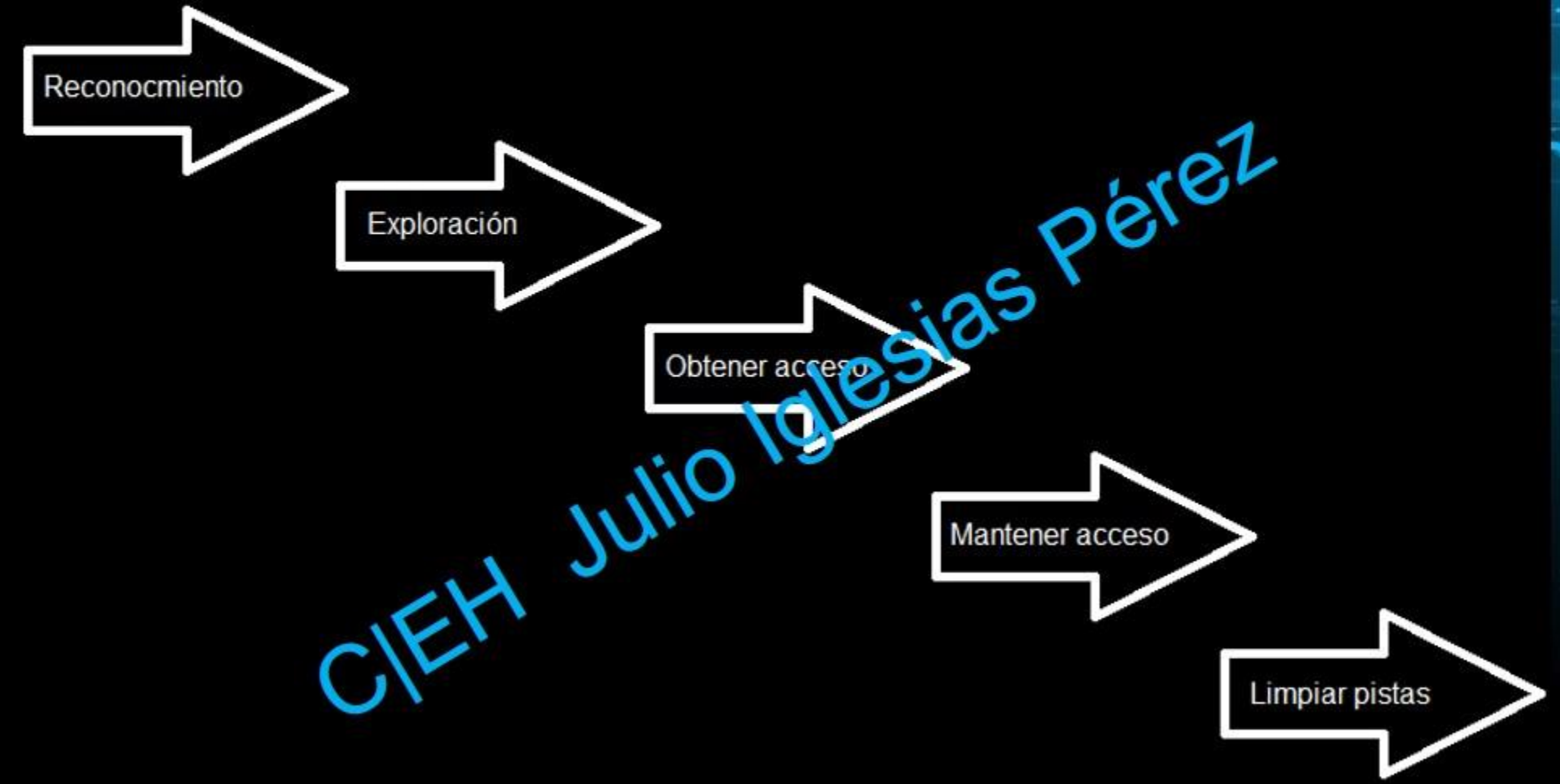
Los blancos comunes incluyen agencias gubernamentales, o cualquier otra entidad que es percibida como mala o equívoca por estos grupos o individuos.

El hecho es que sin importar la intención, obtener acceso sin autorización es un crimen.

Clasificación de los Hackers

- **Sombreros negros (Black hats):** Individuos con habilidades tecnológicas extraordinarias, recurriendo a actividades maliciosas o destructivas. También conocidos como crackers.
- **Sombreros blancos (White hats):** Individuos profesando las habilidades hacker y utilizándolas para propósitos defensivos. También conocidos como analistas de seguridad.
- **Sombreros grises (Gray hats):** Individuos propósitos ofensivos y defensivos según la ocasión.
- **Hackers suicidas (Suicide hackers):** Individuos que pretenden derrocar una infraestructura importante por "una causa" y no les importa enfrentar 30 años de cárcel por sus acciones.

Fases de Hacking



Fase 1: Reconocimiento

La fase de reconocimiento, es la fase preparatoria donde un atacante busca la manera de obtener la mayor cantidad de información posible acerca de un blanco de evaluación antes de realizar un ataque

Fase 2: Exploración

La exploración se refiere a la fase de pre-ataque cuando el hacker explora la red para información específica en la base de la información adquirida durante la fase de reconocimiento

Fase 3: Obtener acceso

La obtención de acceso se refiere a la fase de penetración. El hacker explota la vulnerabilidad en el sistema.

La explotación puede ocurrir en la red LAN, en Internet, engaño o robo. Por ejemplo desbordamiento del búfer, negación de servicio, secuestro de sesión y ruptura de contraseña.

Fase 4: Mantener acceso

El mantenimiento del acceso se refiere a la fase cuando el hacker intenta retener su propiedad en el sistema. El hacker ha comprometido el sistema. Los hackers pueden asegurarse el acceso exclusivo al sistema reforzándolo (previniendo el acceso a otros hackers) mediante backdoors, rootkits o troyanos.

Los hackers pueden cargar, descargar, manipular información, aplicaciones y configuraciones propias del sistema.

Fase 5: Limpiar pistas

Esta fase se refiere a las actividades que el hacker hace para ocultar sus fechorías. Las razones incluyen la necesidad de prolongar su estadía, continuar utilizando los recursos, removiendo evidencia del hacking, o impedir acciones legales.

Los ejemplos incluyen esteganografía, tunneling y alteración de archivos de registro (logs).

Tipos de ataques

1. Ataques al Sistema Operativo.
2. Ataques al nivel de aplicación.
3. Ataques al código Shrink Wrap.
4. Ataques a la configuración incorrecta.

1. Ataques al Sistema Operativo

La naturaleza de los Sistemas Operativos hoy en día es compleja. Estos pueden correr servicios, puertos y modos de acceso y requerir un ajuste extensivo para ser bloqueados y bajados.

La instalación por defecto de muchos S.O. tiene un número extenso de servicios corriendo y puertos abiertos. Aplicar parches y revisiones no es una tarea fácil en esto días con tanta complejidad en las redes. Los atacantes buscan vulnerabilidades en los S.O. y las explotan para obtener acceso a la red del sistema.

2. Ataques al nivel de aplicación

Los desarrolladores de software están bajo presión para llevar los productos a tiempo. La programación extrema está en subida en la metodología de ingeniería de software. Las aplicaciones vienen con muchas funcionalidades y características. El tiempo no es suficiente para realizar un estudio completo antes de lanzar los productos. La seguridad es aplicada a último momento y es introducida en forma de un componente complementario.

La pobre o no existencia de revisión en las aplicaciones conlleva a los ataques de desbordamiento de búfer.

Nota.- Desbordamiento de búfer es un error de software que se produce cuando se copia una cantidad de datos sobre un área que no es lo suficientemente grande para contenerlos.

3. Ataques al código Shrink Wrap

Cuando se instala un S.O. aplicaciones, vienen con toneladas de scripts o guiones para hacer la vida del administrador más simple.

El problema es que estos scripts no tienen un "ajuste fino" o carecen de personalización.

Esto dará lugar a código defectuoso o ataques al código Shrink Wrap.

4. Ataques a la configuración incorrecta

Los sistemas que deben ser bastante seguros son hackeados porque no fueron configurados de manera correcta. Los sistemas son complejos y el administrador no tiene las habilidades o recursos necesarios para corregir el problema.

El administrador creará una configuración simple que funcione.

Para maximizar las posibilidades de configuración correcta de un equipo, se debe remover los servicios o software innecesarios.

Recordar esta regla: “Si un hacker quiere ingresar en un sistema, el/ella lo hará y no hay nada que se pueda hacer para impedirlo.
Lo único que se puede hacer es complicarle el acceso.”


¡Muchas Gracias!
C|EH Julio Iglesias Perez