Enhacke Ethical Hacking Certification

MODULO 1 - INTRODUCCION

enHacke
Su aliado en Seguridad Informática y de la Información

CIBERSEGURIDAD Y PENTESTING

Ciberseguridad

- Métodos, mecanismos y estrategias para proteger la infraestructura TI y sus datos.
- Consecuencia de:
  - Evolución de la tecnología
  - Aumento en complejidad de redes y aplicaciones
  - Ataques más complejos con menos conocimientos

Pentesting

- Métodos, técnicas y procedimientos utilizados para comprobar el estado de seguridad implementado por una organización.
- Serie de acciones que buscan simular un ataque real por un hacker malicioso que tiene como objetivo perjudicar de alguna manera a la organización.
- El objetivo final del pentesting es el aseguramiento.

IMPACTO DE UN CIBERATAQUE

TERMINOS ESENCIALES - Principios

- Confidencialidad
- Integridad
- Disponibilidad
- Amenaza
- Vulnerabilidad
- Riesgo
- Impacto
- Riesgo = vulnerabilidad * amenaza
- Riesgo = vulnerabilidad * amenaza * impacto

DEFINICION DE HACKER

- “apasionado de la investigación, persona curiosa que busca comprender como trabajan las cosas y como hacerlas funcionar de maneras inesperadas”
- “Persona con grandes habilidades en el manejo de sistemas informáticos, que usa sus conocimientos para descubrir fallos de seguridad y protegerlos de posibles ciberataques”
- Un hacker puede ser como cualquier persona, buena y/o mala.

TIPOS DE HACKERS

SUB-CATEGORIAS

- Hacktivistas
- Ciberterrorista
- Defacer
- Spammer

Blackhat

- Carder
- Dropper
- Skimmer

Banking

- Newbie
- Script kiddie
- Lammer

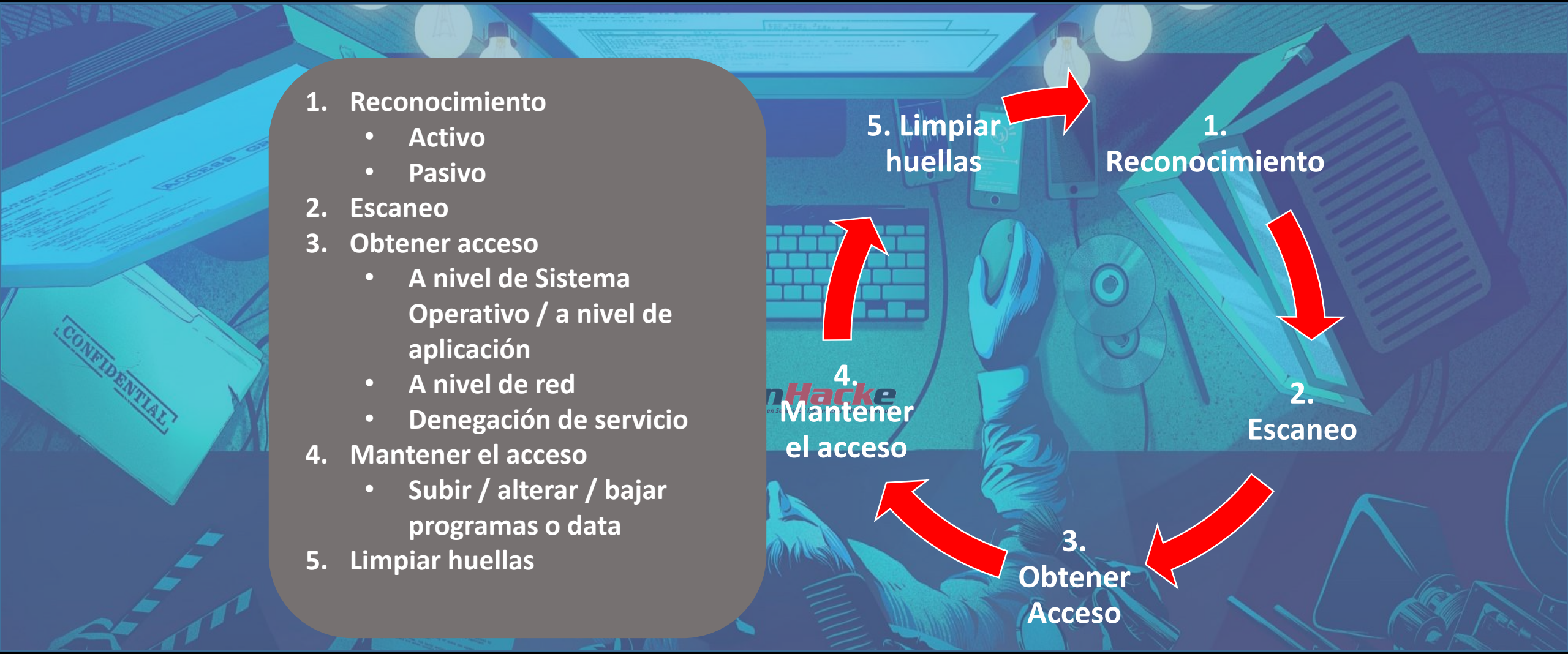
Principiantes

Tipos de Ataques

- Existen diferentes maneras en las cuales un hacker puede acceder al sistema.
- El hacker debe ser capaz de explotar una debilidad o vulnerabilidad del sistema.
- Algunas formas de categorizar ataques:
  - Por sistema operativo
    - Windows / Linux / Android
  - Por capa en la pila OSI
    - Ataques a nivel de aplicación.
    - Ataques a nivel de red
    - Ataques a nivel físico
  - Por alcance
    - Ataques locales
    - Ataques remotos
  - Por complejidad
    - Manuales
    - Automatizados

Lo que hace un hacker malicioso

1. Reconocimiento
   - Activo
   - Pasivo
2. Escaneo
3. Obtener acceso
   - A nivel de Sistema Operativo / a nivel de aplicación
   - A nivel de red
   - Denegación de servicio
4. Mantener el acceso
   - Subir / alterar / bajar programas o data
5. Limpiar huellas



TIPOS DE ETHICAL HACKING / PENTESTING

BLACKBOX

- Sin conocimientos de la infraestructura a ser analizada

GREYBOX

- Información parcial sobre los objetivos

WHITEBOX

- Información completa sobre los objetivos y la infraestructura a atacar

Ataques en tiempo real

- http://www.digitalattackmap.com
- https://cybermap.kaspersky.com/
- http://map.norsecorp.com/
- http://www.fireeye.com/cyber-map/threat-map.html

Enhacke Ethical Hacking Certification

FIN MODULO 1 - INTRODUCCION

enHacke
Su aliado en Seguridad Informática y de la Información