Universidad Tecnológica Fidel Velázquez
Ingeniería en Redes Inteligentes y Ciberseguridad - Hacking Ético

Resolver el siguiente ejercicio contestando únicamente en las hojas. Enviar un sólo archivo en formato PDF a través de la plataforma Google Classroom. Valor de la actividad: 10 puntos.

Nombre del estudiante	
Fecha de la actividad	
Calificación	

Práctica 2. Introducción al Hacking

Este cuestionario evalúa la comprensión de los conceptos fundamentales presentados en el Capítulo 1 del libro *Python Ethical Hacking From Scratch*.

1. (1 punto) ¿Cuál de los siguientes NO es un componente de la tríada de la CIA en ciberseguridad?
    A. Confidencialidad (Confidentiality)
    B. Integridad (Integrity)
    C. Autenticación (Authentication)
    D. Disponibilidad (Availability)
2. (1 punto) Un hacker que irrumpe en un sistema por diversión o para notificar al administrador sobre vulnerabilidades, a veces a cambio de una tarifa, se conoce como:
    A. Black hat hacker
    B. White hat hacker
    C. Script kiddie
    D. Gray hat hacker
3. (1 punto) Según la metodología de hacking descrita, ¿qué fase implica la recopilación de información sobre el objetivo sin interactuar directamente con él?
    A. Escaneo (Scanning)
    B. Reconocimiento pasivo (Passive reconnaissance)
    C. Mantenimiento del acceso (Maintaining access)
    D. Reconocimiento activo (Active reconnaissance)
4. (1 punto) ¿Qué tipo de ataque se caracteriza por engañar a alguien para que revele información confidencial, a menudo a través de correos electrónicos o sitios web falsos?
    A. Baiting
    B. Phishing
    C. System control
    D. Denial of Service (DoS)
5. (1 punto) ¿Cuál es el término para un hacker principiante que utiliza herramientas pre-construidas sin tener un conocimiento profundo de cómo funcionan?
    A. Hacktivista (Hacktivist)
    B. Espía corporativo (Corporate spy)
    C. Script kiddie
    D. Hacker de estado-nación (Nation-state hacker)

6. (1 punto) Explica con tus propias palabras los tres principios de la tríada de la CIA (Confidencialidad, Integridad y Disponibilidad) y proporciona un ejemplo de cómo un ataque podría violar cada uno de ellos.

7. (1 punto) Describe las diferencias clave en las motivaciones y objetivos entre un hacker de sombrero blanco (white hat), un hacker de sombrero negro (black hat) y un hacktivista.

8. (1 punto) Enumera y describe al menos cinco de las fases de la metodología de hacking mencionadas en el texto, desde la planificación inicial hasta la presentación de informes.

9. (1 punto) ¿Qué es la ingeniería social y por qué se considera a menudo el eslabón más débil en la seguridad de un sistema? Proporciona dos ejemplos de técnicas de ingeniería social descritas en el capítulo.

10. (1 punto) Según el libro, ¿cuál es la importancia de la legalidad en el hacking ético y qué se debe obtener siempre antes de realizar pruebas de penetración en un sistema?

Evaluación del desempeño

Pregunta:	1	2	3	4	5	6	7	8	9	10	Total
Puntos:	1	1	1	1	1	1	1	1	1	1	10
Calificación:											