Universidad Autónoma de Zacatecas

"Francisco García Salinas"

Unidad Académica de Ingeniería Eléctrica

Ingeniería en Computación

Materia: Fundamentos de seguridad de la información

Docente: Carlos Héctor Castañeda Ramírez

Tarea 2
Cuestionario sobre Concursos CTF

Alumno:

Amaya Hernández Jhohana María

8° B

Zacatecas, México, 07 de febrero de 2024

1. ¿Qué significa CTF?
   Capture the Flag.
2. ¿Cuál es el objetivo de los concursos CTF?
   Es resolver diversos retos asociados a distintas vulnerabilidades de hardware o software.
3. ¿Cuáles son las fases que suelen tener estos concursos?
   Fase de clasificación en línea y una fase final presencial.
4. Tipo de concurso CTF que comprende una serie de tareas o desafíos clasificados en distintas categorías:
   Jeopardy
5. Tipo de concurso en el cual cada equipo tiene uno o varios hosts con entornos vulnerables:
   Attack-Defense
6. ¿Por qué se debe de balancear el tiempo entre atacar y defender en un CTF Attack-Defense?
   Para obtener más puntos antes de que termine el concurso.
7. Menciona las categorías que comprende un CTF Jeopardy:
   Generals skills, OSINT, Web, Forensic, Crypto, Reversing, Pwning, Misc.
8. Categoría de un concurso CTF Jeopardy que comprende conocimientos generales de las ciencias computacionales:
   General Skills
9. Da una breve explicación de la categoría OSINT:
   Tiene que ver con la recolección y análisis de datos obtenidos de fuentes abiertas (disponibles públicamente), para encontrar información procesable que permita identificar plenamente a una persona o institución.
10. Menciona algunos temas a entender en la categoría Forensic:
    - Steganography
    - File Formats
    - Metadata
    - Packet Analysis
    - Disk Imaging
    - Memory Dump.
11. ¿Cuál es el objetivo de realizar problemas en la categoría de criptografía?
    Entender los principios del funcionamiento de algoritmos cifrados y los cálculos matemáticos asociados.
12. ¿Qué fases comprende un CTF Attack-Defense?
    a. Reconocimiento
    b. Escaneo
    c. Ganar acceso
    d. Mantener acceso
    e. Borrar huellas
13. ¿Qué metodología sigue los CTF Attack-Defense?
    Metodología de hacking ético o metodología de pruebas de penetración.
14. Es la fase donde el atacante trata de retener su propiedad sobre el sistema:
    Mantener acceso.

15. En qué fase de un CTF Attack-Defense el atacante puede extraer información tal como: máquinas activas, puertos, estado de puertos, detalles del SO, para posteriormente realizar el ataque:
    En el escaneo.