SEGURIDAD EN REDES DE COMPUTADORAS

Ingeniería en Computación

UNIVERSIDAD AUTÓNOMA DE ZACATECAS

UNIDAD ACADÉMICA DE INGENIERÍA ELÉCTRICA

INGENIERÍA EN COMPUTACIÓN

Tarea 2

Cuestionario

Docente

Carlos Héctor Castañeda Ramírez

Alumna

Jessica Vanegas López

Grado

8° “B”

Zacatecas, Zacatecas 01/02/2023

1. **¿Por qué se captura una bandera (flag) en los concursos CTF?**

   Porque es como prueba de la solución del reto o la intrusión al sistema.

2. **¿Cuáles son las dos fases y cuánto tiempo toman los concursos CTF?**

   Fase de calificación en línea y fase final en presencial. Y un concurso CTF puede tomar unas pocas horas, un día completo o incluso varios días.

3. **¿Por qué las empresas suelen organizar los CTFs?**

   Porque reclutan talento y satisfacen la demanda de la fuerza laboral en ciberseguridad.

4. **¿Qué es Jeopardy?**

   Es un concurso CTF que comprende una serie de tareas o desafíos clasificados en categorías tales como: general skills, osint, web, forensic, crypto, reversing, pwning, misc.

5. **¿Cómo se llama el tipo de concurso que desarrolla a exploits para atacar los servicios vulnerables del oponente y obtener las banderas que dan los puntos de ataque?**

   Attack – Defense

6. **¿Cuáles son los temas que maneja la categoría de General Skills?**

   - Sistemas numéricos y conversión entre ellos.
   - Conceptos básicos de Linux.
   - Conceptos básicos de programación en diferentes lenguajes.
   - Conceptos básicos de redes e internet.
   - Conceptos básicos de ciberseguridad.

7. **¿Qué significa OSINT y para que usan la recolección y análisis de datos de fuentes abiertas?**

   Significa Open Source Intelligence y se usan para encontrar información

procesable que permita identificar plenamente a una persona o institución partiendo de un nombre, un correo, una imagen, una dirección IP, o cualquier dato disponible.

8. **¿Cuáles son las diferencias entre Web, Forensic, Cryptography y Reversing de las categorías CTF Jeopardy?**

Web	Forensic	Cryptography	Reversing
- Tiene vulnerabilidades específicas a los diferentes lenguajes de programación utilizados para crear los sitios web. - Incluyen retos asociados a problemas de configuración o implementación de los protocolos de internet o errores en la lógica de la aplicación.	- Recupera el rastro que queda en una computadora al usarla. - Encuentra datos que aparentemente se eliminan, no se almacenan o se registran de forma encubierta	- Maneja diferentes algoritmos de cifrado clásicos y modernos como cifrado por bloques y criptografía. - Funcionamiento de los algoritmos de cifrado y los cálculos matemáticos asociados. -	- Maneja programa compilado y aplicar ingeniería inversa para obtener un código legible generalmente en lenguaje ensamblador o una interpretación en lenguaje C.

9. **¿En qué consiste el CTF Binary Explotation (Pwning) y en que se programa?**

   En encontrar vulnerabilidades en un archivo binario (compilado), explotarla para obtener acceso a la línea de comando de un sistema remoto. Y se programa con exploit para automatizar la explotación, se lanza contra el servicio en un host remoto y tener acceso a la terminal.

10. **¿Cuáles son las principales fases que maneja CTF Attack-Defense?**

    - Reconocimiento.
    - Escaneo.
    - Ganar acceso.

- Mantener acceso.
- Borrar huellas.

11. **¿Cómo se llama la fase que busca obtener la mayor cantidad de información y recaba información sobre clientes?**

    Reconocimiento (Reconnaissance or Footprinting).

12. **¿Qué puede incluir el uso de escaneo y que puede extraer?**

    Puede incluir el uso de dialers, port scanners, network mapping, sweeping, vulnerability scanners, etc Y puede extraer máquinas activas, puertos, estado de puertos, detalles del SO, para posteriormente realizar el ataque.

13. **¿Qué asegura Gaing Access o Exploiting?**

    Un acceso exclusivo con un backdoor, rootkit o trojan.

14. **¿Cuál es la fase que trata de retener su propiedad sobre el sistema y puede subir, bajar o manipular datos?**

    Mantener acceso (maintaining access)

15. **¿Cuáles son las plataformas para resolver retos sencillos o Wargames?**

    - Overthewire – Bandit
    - Hack my vm - Venus

16. **Menciona las redes sociales del concurso al participar en un CTF.**

    - Busca un equipo.
    - Busca integrantes para el tuyo.
    - Interactúa con los demás.
    - Conoce a los integrantes de otros equipos en el CTF, pregunta y comparte tu experiencia.

17. **¿Por qué es importante documentar la solución de los retos y que herramienta se puede usar al participar en un CTF?**

Ayuda a tener una referencia para posteriores eventos. Y la herramienta que se puede usar es obsidian.

Zacatecas, Zacatecas 01/02/2023