UNIVERSIDAD AUTÓNOMA DE ZACATECAS

PROGRAMA ACADÉMICO DE INGENIERÍA DE SOFTWARE

MAYELA SARRIA SALAZAR

MATERIA: SEGURIDAD EN REDES Y SISTEMAS DE SOFTWARE

MAESTRO: CARLOS CASTAÑEDA

FECHA: 09/09/2025 Matricula: 37184124

Actividad 2

1. ¿Qué significa la sigla CTF y qué es?

CTF significa "Capture The Flag" y es una competencia de ciberseguridad en la que los participantes resuelven retos técnicos para obtener banderas como prueba de solución.

2. ¿Quiénes suelen participar en este tipo de concursos?

Típicamente participan entusiastas, estudiantes y profesionales interesados en ciberseguridad.

3. ¿Por qué las empresas utilizan los concursos CTF?

Las empresas los usan para detectar talento y cubrir la alta demanda en seguridad informática.

4. ¿Cuáles son los dos tipos principales de concursos CTF?

Los dos tipos principales son Jeopardy y Attack-Defense.

5. ¿Qué caracteriza a un concurso CTF de tipo Jeopardy?

Los participantes resuelven retos organizados por categorías, cada uno con un puntaje, y el equipo con más puntos al final gana.

6. ¿Qué se necesita para tener éxito en un CTF de tipo Attack-Defense?

Se requiere un balance entre ofensiva y defensiva, ya que los equipos deben atacar los servicios vulnerables de otros para ganar puntos y, al mismo tiempo, defender y parchear sus propios servicios.

7. Menciona al menos tres de las categorías comunes en un CTF de tipo Jeopardy.

Las categorías comunes incluyen General Skills, OSINT, Web, Forensic, Cryptography (Crypto), Reversing, Binary Explotation (Pwning) y Misc.

8. ¿A qué se refiere la categoría OSINT?

Se refiere a la recolección y análisis de datos de fuentes abiertas públicamente para encontrar información procesable sobre una persona o institución.

9. En la categoría Web, ¿qué tipo de vulnerabilidades se abordan?

Se abordan vulnerabilidades de inyección (SQL, no-SQL), Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF) y errores de autenticación y autorización, entre otros.

10. ¿Cuál es el objetivo de la categoría Forensic (Forense)?

Su objetivo es recuperar rastros que quedan en una computadora, como datos que han sido eliminados o están ocultos, para encontrar información.

11. ¿Qué se hace en la categoría Reversing (Ingeniería Inversa)?

Consiste en tomar un programa compilado y aplicar ingeniería inversa para obtener un código legible, generalmente en lenguaje ensamblador o C.

12. ¿Cuál es el propósito de la categoría Binary Exploitation (Pwning)?

Consiste en encontrar vulnerabilidades en un archivo binario y explotarlas para obtener acceso a la línea de comando de un sistema remoto.

13. ¿Qué es la primera fase de un CTF de tipo Attack-Defense?

La primera fase es el Reconocimiento, donde el atacante busca obtener la mayor cantidad de información posible sobre el objetivo.

14. ¿Qué se hace en la fase de Escaneo?

Se escanea la red para buscar información específica basada en lo obtenido en la fase de reconocimiento, como máquinas activas, puertos y detalles del sistema operativo.

15. ¿Qué ocurre en la fase de "Ganar Acceso"?

Se explotan las vulnerabilidades encontradas y el atacante trata de asegurar su control sobre el sistema.

16. ¿Qué hace un atacante en la fase de "Borrar Huellas"?

El atacante trata de esconder sus actividades maliciosas, borrando la evidencia que podría llevar a su persecución.

17. ¿Qué plataforma se recomienda para empezar a practicar si eres principiante?

Se recomienda empezar por plataformas con retos resueltos, como Overthewire y Hack My VM.

18. ¿Qué es un writeup y por qué es importante documentarlo?

Un writeup es la documentación de la solución de un reto. Es importante porque sirve como referencia para futuros eventos, permitiendo reutilizar técnicas y fragmentos de código.

19. ¿Cuál es la principal recomendación para cuidar la salud mental durante un concurso?

La principal recomendación es divertirse y aprender.

20. Según el documento, ¿cuál es el objetivo principal de los CTFs más allá de competir?

El objetivo principal es aprender, colaborar y disfrutar.