Tarea 02 Cuestionario CTF

Licenciatura en Software, Universidad Autónoma de Zacatecas

Seguridad en Redes y Sistemas de Software

Autor:

Jonathan Alexis Martínez Reyes

Profesor: Carlos Héctor Castañeda Ramírez

04/Febrero/2025

1.¿Qué son los concursos CTF (Capture The Flag)?
Es un concurso de competencia informática, objetivo es resolver diversos retos asociados a diferentes vulnerabilidades de hardware y/o software.

2. ¿Por qué son tan útiles los Capture The Flag?
Aprendizaje: ofrecen mejorar la capacidad de reconocer vulnerabilidades, comprender el análisis forense y dominar herramientas de seguridad.
Mantenerse Actualizado: Nos permite familiarizarnos con las ultimas tecnologías.
Accesibilidad y colaboración: Las plataformas de CTF gratuitas cuentan con una amplia comunidad donde podemos intercambiar ideas y experiencias de manera segura.

3. ¿Cuáles son los tipos de CTF?
Ingeniería inversa, Análisis forense, Criptografía, Web, OSINT y Explotación.

4. ¿Qué tipos de modalidades pueden tener?
Puntaje (Jeopardy), Juegos de Guerra (Ataque y defensa) y Mixtos.

5. ¿Qué es la ingeniería inversa en CTF?
La ingeniería inversa en el contexto de Capture the Flag (CTF) se refiere al proceso de analizar y descomponer aplicaciones y programas con el objetivo de entender su funcionamiento o identificar vulnerabilidades. Los participantes en CTF suelen utilizar técnicas de ingeniería inversa para resolver desafíos que implican la explotación de software o protocolos.

6. ¿Cual es la diferencia entre el modo de puntaje contra el de Ataque y defensa?
Puntaje: Es un modelo sencillo, hay pruebas, dan puntos al completarse y cuanto más puntos consiga tu equipo mejor. Los equipos no interactúan entre ellos, se suele usar en concursos con mucha gente, ya que es más sencillo de montar.
Ataque y Defensa: se usa en finales de eventos importantes donde hay pocos equipos y tienen que saber proteger su sistema además de atacar al del adversario. Un ejemplo lo encontramos en el DefCon, la conferencia más importante de ciberseguridad (junto con la BlackHat), entre cuyas actividades encontramos un CTF; las primeras fases son al estilo Jeopardy y las finales son estilo ataque y defensa.

7. ¿Qué categorías comprende un CTF Jeopardy?
1. Pwn (Explotación de vulnerabilidades)
2. Rev (Reversión de ingeniería)
3. Web (Seguridad en aplicaciones web)
4. Crypto (Criptografía)
5. Forensics (Análisis forense)
6. Misc (Diversos, que pueden incluir preguntas sobre otras áreas de la seguridad informática)

8. ¿De qué constan las categorías de Jeopardy?

PWN: Los participantes deben desarrollar exploits para tomar el control de un servicio vulnerable.

REV: Se centra en la ingeniería inversa de binarios. Los competidores deben analizar programas para entender su funcionamiento y extraer información o encontrar vulnerabilidades.

Web: Se refiere a la seguridad en aplicaciones web. Los retos pueden incluir la explotación de vulnerabilidades como SQL injection, XSS, CSRF, etc.

Crypto: Examina desafíos relacionados con criptografía. Los participantes deben desencriptar textos, romper algoritmos o resolver problemas matemáticos asociados a la criptografía.

Forensics: Involucra el análisis forense digital. Los competidores examinan imágenes de disco, registros, o sistemas para extraer información o entender lo ocurrido en un incidente.

Misc: Incluye retos de diversas temáticas que no encajan en las categorías anteriores. Pueden ser rompecabezas, preguntas de cultura general en seguridad o problemas de lógica.

9.¿Cuáles son las categorías con mayor dificultad de los Jeopardy y por qué?

Pwn, Rev, y Crypto: La dificultad en estas categorías se deriva de la combinación de conocimientos técnicos profundamente especializados, la necesidad de habilidades prácticas en la resolución de problemas y la capacidad de aplicar conceptos teóricos a situaciones del mundo real.

10. ¿Qué fases comprende un CTF Attack-Defense?

1. Reconocimiento.
2. Escaneo.
3. Ganar Acceso.
4. Mantener Accesos.
5. Borrar Huellas.

11. ¿Cómo practicar para un CTF?

Estudiar y practicar.

Recursos de aprendizaje: hay libros, cursos y tutoriales en línea sobre temas específicos de ciberseguridad como explotación, criptografía, análisis forense, etc.

Documentación y blogs: Existen blogs de expertos en seguridad, como OWASP para aplicaciones web, o Exploit-DB para aprender sobre vulnerabilidades.

12. ¿Qué habilidades desarrolla un participante en los CTF?

Los CTF ayudan a mejorar habilidades como el pensamiento lógico, la resolución de problemas, el análisis forense, la ingeniería inversa, la criptografía, la seguridad en aplicaciones web, la explotación de vulnerabilidades y la administración de sistemas.

13. ¿Qué es un CTF basado en OSINT y en qué consiste?

Un CTF basado en OSINT (Open Source Intelligence) implica la recolección y análisis de información pública disponible en la web para resolver desafíos. Puede incluir la búsqueda de datos en redes sociales, bases de datos públicas, metadatos en archivos o imágenes y otras fuentes abiertas.

14. ¿Cuáles son los errores comunes de los principiantes en los CTF?
Algunos errores comunes incluyen no leer bien la descripción de los retos, no tomar notas de los intentos y soluciones, enfocarse demasiado tiempo en un solo desafío, no usar las herramientas adecuadas y no pedir ayuda o buscar referencias.

15. ¿Qué significa "enumeración" en el contexto de un CTF?
La enumeración es el proceso de obtener información sobre un sistema o aplicación para identificar posibles vulnerabilidades. En un CTF, esto puede incluir la identificación de servicios y puertos abiertos, la búsqueda de directorios ocultos en una web o la extracción de metadatos en archivos.

17.¿Cómo se puede participar en un CTF?
Participa en CTFs en línea: Inscríbete en plataformas como Hack The Box, TryHackMe, CTFtime y pwnable.kr. Estas plataformas ofrecen retos en diversas categorías.

18. ¿Qué se recomienda antes de participar en un CTF?
Elige un concurso CTF: Elige el concurso CTF que más rete tu intelecto, Beginner, Intermediate, Elite, Siempre habrá concurso CTF adecuado a tu nivel de conocimiento
Juega en equipo: Integrarte a un equipo en tu escuela o Inicia un equipo con otros que compartan tu pasión por la ciberseguridad.
Usa las redes sociales del concurso: Busca un equipo, Busca integrantes para el tuyo e interactúa con los demás, Conoce a los integrantes de otros equipos en el CTF, pregunta y comparte tu experiencia.
Instala las herramientas: Identifica las herramientas utilizadas para la solución de retos en cada categoría del concurso y procura instalarlas antes del concurso., Puedes hacerlo en tu distribución de Linux habitual o instalar una máquina virtual
que contenga las herramientas más comunes.

19. ¿Qué se recomienda hacer durante el concurso CTF?
Lee las reglas del juego antes de iniciar.
• Revisa el formato de la bandera: flagMX{}
• No publiques las soluciones o banderas.
• Busca retos similares en CTFs pasados o revisa tus propias notas.
• Toma notas de los aspectos esenciales del reto según avances en la solución: Te evitará que pruebes varias veces la misma solución y servirán para crear la documentación (writeup)
• Prueba un reto diferente si te atascas mucho tiempo.
• Pide una pista.

20. ¿Qué se recomienda después de participar en un CTF?
Documentar (writeup) la solución del reto te ayuda a tener una referencia para posteriores eventos, descripción del reto, procedimiento de solución, herramientas utilizadas, referencias consultadas y otras formas de solucionar el reto.