**Cuestionario sobre Concursos CTF (Capture The Flag)**

**Docente: Carlos Castañeda Ramírez**

**Alumno: Rogelio Reveles Villegas**

**24 de Agosto de 2023**



1. **¿Qué es un concurso CTF(Capture The Flag)?**

Un concurso CTF es un tipo especial de concurso de competencia Informática que consiste en resolver retos asociados a vulnerabilidades de hardware y software y al final se debe capturar una bandera(flag) como prueba de haber solucionado el reto o intrusión. Se efectúan en un ambiente controlado y de manera ética.

1. **¿Por qué son importantes los concursos CTF?**

Son una herramienta didáctica para aumentar el interés en la ciberseguridad y generar personas competentes para el mundo laboral. Permiten que se desarrollen habilidades en ciberseguridad de una manera divertida y atractiva.

1. **¿Por quiénes son organizados estos concursos?**

Las empresas son las encargadas de organizar este tipo de actividades para reclutar talento y satisfacer la demanda de la fuerza laboral en ciberseguridad.

1. **Liste los tipos de concursos CTF:**

* Jeopardy
* Attack-Defense

1. **¿En qué consiste un concurso tipo Jeopardy?**

Este tipo de concurso comprende una serie de actividades o desafíos clasificados en categorías tales como:

* General Skills
* Osint
* Web
* Forensic
* Crypto
* Reversing
* Pwning
* Misc

El equipo gana puntos por desafío superado y las tareas tienen una complejidad diferente y otorgan diferente cantidad de puntos, las tareas están encadenadas, lo que implica que se debe resolver una tarea para poder resolver otra, al final de que se termine el tiempo se suman los puntos y se muestra al ganador.

1. **¿En qué consiste un concurso tipo Attack-Defense?**

En este tipo de concursos los participantes se dividen en 2 equipos y cada equipo tiene uno o varios host con servicios vulnerables.

Ambos equipos se conectan en el mismo entorno de red y deben desarrollar exploits para atacar los servicios vulnerables del oponente y obtener los puntos de ataque.

Los equipos deben corregir sus vulnerabilidades para evitar ser atacados y obtener las banderas que dan puntos de defensa.

La clave es balancear el tiempo entre ambas actividades y obtener más puntos. Por lo general se usa el Pentesting para los retos de este tipo de concursos.

1. **Liste por lo menos 5 categorías de los concursos tipo Jeopardy:**

* General Skills
* Web
* Cryptography (Crypto)
* Reversing
* Binary Exploitation (Pwning)

1. **En qué consiste la categoría OSINT?**

Se centra en la recolección y análisis de datos de fuentes abiertas para encontrar información procesable que permita identificar plenamente a una persona o institución utilizando información como el nombre, e-mail, una imagen o cualquier dato disponible.

1. **Explique la categoría Forensic:**

Se centra en la recuperación del rastro que queda en una computadora al usarla.

encuentra los datos que aparentemente se eliminan o registran de forma encubierta.

1. **¿Cómo funciona el Reversing?**

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

En algunos casos incluye revertir un cifrado o codificación hecho en algún lenguaje de alto nivel examinando el código y entendiendo su lógica.

1. **¿En qué consiste la categoría Pwning?**

Consiste en encontrar vulnerabilidades en un archivo binario (compilado), explotarlo para obtener acceso a la línea de comando de un sistema de manera remota. Se debe comprender la lógica del archivo binario desensamblado para modificar su función o evadir las medidas de seguridad. Se deberá programar un exploit para automatizar la explotación.

1. **Liste las fases de un concurso Attack-Defense:**

* Reconocimiento
* Escaneo
* Obtención del Acceso
* Mantener el Acceso
* Borrar el rastro

1. **Describa la fase de Footprinting:**

La fase de de Footprinting (Reconocimiento) consiste en que el atacante busca obtener la mayor cantidad de información como sea posible acerca del objetivo, pueden ser puntos de retorno si se descubre una entrada fácil y se tiene gran cantidad de información sobre el objetivo, se debe recabar cualquier tipo de información que le pertenezca al objetivo.

1. **Describa la fase de Scanning:**

Fase de pre-ataque cuando se escanea la red en busca de información específica en base a la información obtenida en el Reconocimiento. El escaneo incluye puertos, network mapping, vulnerability scanners y otras herramientas o formas y se obtiene información del equipo para después realizar el ataque.

1. **¿Qué se hace durante la fase de Exploiting?**

Se explotan las vulnerabilidades encontradas y se intenta retener el sistema accedido y se asegura de que solamente él pueda acceder al sistema, puede manipular los datos, aplicaciones y configuraciones del sistema y puede utilizar el sistema para ejecutar otros ataques.

1. **¿Qué hace el hacker para mantener el acceso en un sistema hackeado?**

Asegura el acceso exclusivo al sistema mediante la instalación de Backdoors, rootkits y Trojanos.

1. **Covering Tracks en qué consiste?**

El atacante trata de esconder sus actividades maliciosas trata de permanecer desapercibido, borra evidencia que podría llevar a su persecución, sobre escribe los registros del sistema para evitar sospechas y hace el que el trabajo del analista forense sea más difícil.

1. **Liste lo necesario para practicar un concurso CTF:**

* Empezar por entender los fundamentos de linux y ciberseguridad a través de páginas con retos sencillos.
* Elegir un CTF con retos disponibles (PicoCTF)
* Elegir un CTF en tiempo real (CFT Time)

1. **Liste qué se necesita antes de entrar a un concurso CTF:**

* Elegir un concurso CTF
* Jugar en equipo
* Usar las redes sociales del concurso
* Instalar las herramientas necesarias

1. **Liste que se debe hacer durante el concurso CTF:**

* Leer las reglas del concurso
* Revisar y conocer el formato del bandera del concurso
* No publicar las soluciones
* Buscar retos similares en concursos previos o revisar notas
* Anotar los aspectos esenciales de cada reto según se avance en cada uno
* Intentar un reto diferente si se tienen problemas
* Intenta pedir una pista más no la respuesta en sí

1. **Liste que se debe hacer después del concurso:**

* Documenta la solución de los retos que resolviste
* Haz un post-mortem
* Revisa que ha funcionado y que ha fallado
* Busca las soluciones a los retos que no pudiste resolver
* Piensa qué habilidades necesitas para próximos concursos y desarrollalas
* Cuida tu salud mental
* Divertirse y aprender