9



Universidad autónoma   
De Zacatecas

Unidad académica de ingeniería eléctrica

Programa de ingeniería en computación

Gilberto Huerta Reynoso

Instructor: Carlos Héctor Castañeda Ramírez

Zacateas, Zacatecas a 31 de enero del 2023

Seguridad en Redes de  
Computadoras

Concursos CTF

1. **¿Qué son los concursos CTF?**

Un concurso CTF o Capture The Flag, es un tipo especial de concurso de competencia informática cuyo objetivo es resolver diversos retos asociados a diferentes vulnerabilidades de hardware o software.

1. **¿Por qué los concursos CTF?**

En la academia, una herramienta didáctica muy eficaz para aumentar el interés de los estudiantes en la ciberseguridad y generar competencias para el mundo laboral.

1. **¿Cuáles son los tipos de concursos CTF?**

Existen básicamente dos tipos de concursos CTF:

Jeopardy

Attack - Defense

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

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

El equipo puede ganar algunos puntos por cada tarea resuelta.

Las tareas complicadas generalmente dan más puntos.

La siguiente tarea en cadena, solo puede ser abierta hasta que alguien del equipo resuelva la tarea previa.

Una vez que el tiempo del juego termina se suman los puntos y se muestra al equipo ganador del CTF.

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

• En concurso CTF tipo attack-defense, cada equipo tiene uno o varios

hosts con servicios vulnerables.

• Se conecta a los equipos en un mismo entorno en red e inicia el

concurso.

• El equipo desarrolla exploits para atacar los servicios vulnerables del

oponente y obtener las banderas que dan los puntos de ataque.

• El equipo corrige las vulnerabilidades en sus propios servicios para

evitar ser atacados y obtener las banderas que dan los los puntos de

defensa.

• Se debe balancear el tiempo entre estas dos actividades de forma

estratégica para obtener más puntos antes del fin del concurso.

• Suele usarse la metodología de ethical hacking o también llamada

pentesting, para abordar los retos en este tipo de concursos.

-------------------------------------------------------------------------------------------------------------------

1. **¿Qué es el Social Engineering?**

Intenta manipular a las personas para que realicen acciones, cometan errores de seguridad o divulguen información confidencial.

Se aprovecha de la disponibilidad de las personas de ayudar, y también se explotan sus debilidades como vanidad, miedo, codicia.

Se pretender ser otra persona: una autoridad, un empleado, solicitando información de forma inusual o desesperada.

Puede falsificarse gafetes para acceder a espacios restringidos o entrar detrás de alguien que tiene ese acceso.

Ponerse tras el teclado para mirar cuando se teclean contraseña, hasta escuchar conversaciones privadas sin autorización.

1. **¿Qué es el Phising?**

Correos electrónicos malicioso disfrazados como confiables o legítimos.

Engaña al usuario para que comparta información personal, o haga clic en algún enlace que instala malware, o captura credenciales de acceso.

En algunos casos viene con faltas de ortografía, malas redacciones o traducciones, además de que el dominio del correo del remitente es algo sospechoso, o al poner el puntero sobre el enlace en el cuerpo del correo, no coincide con lo que dice el texto.

Puede ser muy difícil de detectar, puede ser en apariencia muy formal y parecerse al de tu banco, empresa de trabajo, tiende de conveniencia, que te pide actualizar tus datos y te envía a un sitio web falso para robar tus datos.

Puede ser dirigido a empleados específicos de una empresa (spear phisig).

1. **¿Qué es el Zero-day Exploit?**

Se explota una vulnerabilidad recien descubierta o no reportada.

No existe aún un parche de seguridad o actualización que la mitigue por parte del fabricante o desarrollador.

Existe un mercado negro de venta de Zero-day exploits, lo que incremente el riesgo. Suelen ofrecerse en paquete como un software como servicio (software as a service) donde creador recibe parte del beneficio una vez efectuado el ataque, ya sea por la venta o por comisión del pago de rescate en el caso de ransomware.

1. **¿Qué es Denial of Service Attack (DoS)?**

Inunda los sistemas, redes o servidores con tráfico masivo, lo que hace que el sistema no pueda cumplir con las solicitudes legítimas.

Puede agotar los recursos de un sistema como memoria, espacio en disco duro.

Se pueden utilizar varios dispositivos infectados para lanzar un ataque en el sistema objetivo, generando una de denegación de servicio distribuida (DDoS).

Contenerlo puede ser difícil dado que se falsifican las direcciones IP de origen (IP Spoofing) y puede requerir equipamiento especial, o contramedidas a nivel proveedor de servicios.

1. **¿A qué se refiera el Man in the midle?**

Ponerse en medio de la comunicación entre dos partes.

Mediante la escucha y captura de paquetes enviados por la red, se puede tener acceso a datos confidenciales, o incluso modificar la respuesta al usuario.

Si los datos no viajan cifrados (texto plano) son fácilmente interceptados.

En algunos casos es posible interceptar datos cifrados y aplicar técnicas de cracking para obtener contraseñas en texto plano (wifi cracking).

1. **¿Qué es el Password cracking?**

Se prueban diversas contraseñas posibles hasta adivinar la correcta (guessing).

Se prueban combinaciones numéricas o alfabéticas como contraseñas.

Se prueban palabras en un diccionario como contraseñas.

Se prueban combinaciones de palabras de diccionario con frases al inicio o al final de estas palabras.

Finalmente, como último recurso, se van combinando todos los caracteres posibles en todas las posiciones.

1. **¿A qué se refiere el Covert Hardware?**

El atacante puede utilizar diferentes dispositivos de hardware que le faciliten la

infiltración encubierta en las redes y sistemas.

1. **¿Qué es un Hacker?**

Personas con amplios conocimientos de informática, exploran diversas técnicas para sobrepasar los controles de seguridad y explotar las vulnerabilidades en redes y sistemas. Desarrollan nuevas técnicas de ataque por la emoción del desafío o para presumir en la comunidad de hackers.

1. **¿Cuáles son los Black Hat Hackers?**

Operan en el anonimato, motivados por el beneficio personal o económico, la venganza, el acecho o el activismo político.

1. **¿Cuáles son los White Hat Hackers?**

Operan bajo permiso expreso del dueño de la red o sistema, y al cual le reportan sus los hallazgos como entregable del contrato, también llamados, hackers éticos o analistas de seguridad.

1. **¿Qué hacen los Terrorist groups?**

Llevan a cabo ataques cibernéticos para destruir, infiltrarse o explotar la infraestructura crítica para amenazar la seguridad nacional, comprometer el equipo militar, perturbar la economía y causar bajas masivas.

En algunos casos patrocinados por gobiernos con fines de inteligencia / ciber

guerra. A veces llamados también grupos APT (Advanced Persistent Threat).

1. **¿Qué son los Malicious Insiders?**

Son personas con información privilegiada, pueden incluir empleados, proveedores externos, contratistas u otros socios comerciales.

Tienen acceso legítimo a los activos de la empresa, pero hacen un mal uso para robar o destruir información con fines de lucro personal o financiero.

Atacan por venganza al no ser promocionados, o infiltrados a propósito para filtrar secretos comerciales. Son más difíciles de detectar que los atacantes externos, dado que la organización confía en ellos.