
# UNIVERSIDAD AUTÓNOMA DE ZACATECAS

## UNIDAD ACADÉMICA DE INGENIERÍA ELÉCTRICA

## PROGRAMA DE INGENIERÍA EN COMPUTACIÓN

# SEGURIDAD EN REDES DE COMPUTADORAS

### CONCURSOS CTF

GILBERTO HUERTA REYNOSO
INSTRUCTOR: CARLOS HÉCTOR CASTAÑEDA RAMÍREZ
Zacatecas, Zacatecas a 31 de enero del 2023

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.

2. **¿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.

3. **¿Cuáles son los tipos de concursos CTF?**
   Existen básicamente dos tipos de concursos CTF:
   Jeopardy
   Attack - Defense

4. **¿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.

5. **¿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 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.

6. **¿Qué categorías comprende un CTF Jeopardy?**
   Un concurso CTF del tipo Jeopardy comprende generalmente las siguientes categorías:
   - General Skills
   - OSINT
   - Web
   - Forensic
   - Cryptography (Crypto)

- Reversing
- Binary Explotation (Pwning)
- Misc

7. **¿En qué consiste el CTF Jeopardy General Skills?**
   Comprende conocimientos generales de ciencias computacionales.
   Algunos temas a entender:
   - 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.

   Estos retos aparecen en concursos para principiantes en la idea de fomentar las habilidades básicas que se deben tener para poder jugar otros CTFs de mayor complejidad.

8. **¿En qué consiste el CTF Jeopardy OSINT (Open Source Intelligence)?**
   Tiene que ver con la recolección y análisis de datos obtenidos de fuentes abiertas (disponibles públicamente), para encontrar información procesable que permita identificar plenamente a una persona o institución.
   Se parte de un nombre, un correo, una imagen, una dirección IP, o cualquier dato disponible.
   Algunos temas a aprender:
   - google dorks, google hacking database
   - sites: shodan.io, cert.sh, censys, fofa.info, zoomeye,org, osintframework.com
   - dnsdumpster.com, ipinfo.io, archive.org
   - tools: recon-ng, maltego

9. **¿En qué consiste el CTF Jeopardy Web?**
   Tienen que ver con vulnerabilidades específicas a los diferentes lenguajes de programación utilizados para crear los sitios web que todo desarrollador debe considerar.
   También se incluyen retos asociados a problemas de configuración o implementación de los protocolos de internet o errores en la lógica de la aplicación.
   Algunos temas a entender:
   - http protocol, request and response codes
   - Injection: sql ,no sql, command, xml
   - Cross Site Scripting (XSS)
   - Cross Site Request forgery (CSRF)
   - Insecure Deserialization
   - Server Side Template Injection (SSTI)
   - Http Request Smuggling,
   - Authentication: Oaut, jwt
   - Authorization: insecure direct object reference (IDOR)
   - OWASP – Top 10 vulnerabilities

10. **¿En qué consiste el CTF Jeopardy Forensic?**

    Trata sobre recuperar el rastro que queda en una computadora al usarla.

    Se trata de encontrar los datos que aparentemente se eliminan, no se almacenan o se registran de forma encubierta.

    Algunos temas a entender:

    - Steganography
    - File Formats
    - Metadata
    - Packet Analysis
    - Disk Imaging
    - Memory Dump

11. **¿En qué consiste el CTF Jeopardy Reversing?**

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

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

    Algunos temas a entender:

    - The C Programming Language
    - Assembly Language: x86, x64
    - Registers, Memory and Addressing, Instructions
    - Stack, Calling Conventions, Buffers
    - Machine Code
    - Dissaseblers
    - Decompilers

12. **¿En qué consiste el CTF Jeopardy Binary Explotation (Pwning)?**

    Consiste en encontrar vulnerabilidades en un archivo binario (compilado), explotarla para obtener acceso a la línea de comando de un sistema remoto.

    Pasa por entender la lógica del archivo binario desensamblado para modificar su función o evadir medidas de seguridad.

    Se programa un exploit para automatizar la explotación, se lanza contra el servicio en un host remoto y tener acceso a la terminal.

    Algunos temas a entender:

    - Registers, Stack, Buffers, Calling Conventions
    - Global Offset Table
    - Return Oriented Programming (ROP)
    - Binary Security
    - The Heap and Heap Exploitation
    - Format String Vulnerability

13. **¿Qué fases comprende un CTF Attack-Defense?**

    En un concurso CTF tipo attack-defense se sigue una metodología de hacking ético o también conocida como metodología de pruebas de penetración, para detectar y explotar las vulnerabilidades existentes en el host o la red, contempla las siguientes fases:

    1. Reconocimiento.
    2. Escaneo.
    3. Ganar acceso.
    4. Mantener acceso.
    5. Borrar huellas.

14. **Define la fase 1 (Reconocimiento) que comprende un CTF Attack-Defense**

    El atacante busca obtener la mayor cantidad de información como sea posible acerca del objetivo en evaluación previo al lanzamiento de un ataque.

    Podría ser un punto de regreso si se descubre una entrada fácil y se tiene gran cantidad de información sobre el objetivo.

    Puede incluir recabar información sobre clientes, empleados, operaciones, redes y sistemas de la organización objetivo.

15. **Define la fase 2 (Escaneo) que comprende un CTF Attack-Defense**

    Es la fase de pre ataque cuando el hacker escanea la red en busca de información específica en base a la información obtenida durante el reconocimiento.

    El escaneo puede incluir el uso de dialers, port scanners, network mapping, sweeping, vulnerability scanners, etc.

    El atacante puede extraer información tal como: máquinas activas, puertos, estado de puertos, detalles del SO, para posteriormente realizar el ataque.

16. **Define la fase 3 (Ganar acceso) que comprende un CTF Attack-Defense**

    Se explotan las vulnerabilidades encontradas.

    El atacante trata de retener su propiedad sobre el sistema.

    Harán difícil a otros poder acceder al mismo, asegurando un acceso exclusivo con un backdoor, rootkit o trojan.

    Pueden subir, bajar o manipular datos, aplicaciones, configuraciones en el sistema que posee.

    Usará el sistema para lanzar otros ataques.

17. **Define la fase 4 (Mantener el acceso) que comprende un CTF Attack-Defense**

    Es la fase donde el atacante trata de retener su propiedad sobre el sistema.

    Trata de asegurar un acceso exclusivo al sistema mediante la instalación de Backdoors, Rootkits o Trojans.

    Pueden subir, bajar o manipular datos, aplicaciones, configuraciones en el sistema bajo su control.

    Usa el sistema comprometido para lanzar otros ataques.

18. **Define la fase 5 (Cubrir huellas) que comprende un CTF Attack-Defense**

    El atacante trata de esconder sus actividades maliciosas.
    Trata de permanecer desapercibido y no capturado.
    Borra evidencia que podría llevar a su persecución.
    Sobrescribe los registros del sistema para evitar sospechas.
    Hace el trabajo del analista forense más difícil.