Capture The Flag Masterclass

Instructor: Pranay from CyberBlockz

40 Hours | Telugu

Table of Contents

1. Introduction to CTFs

2. Types of CTF's

3. Services and utilization

4. CTF Lab Setup

5. CTF Solving Techniques

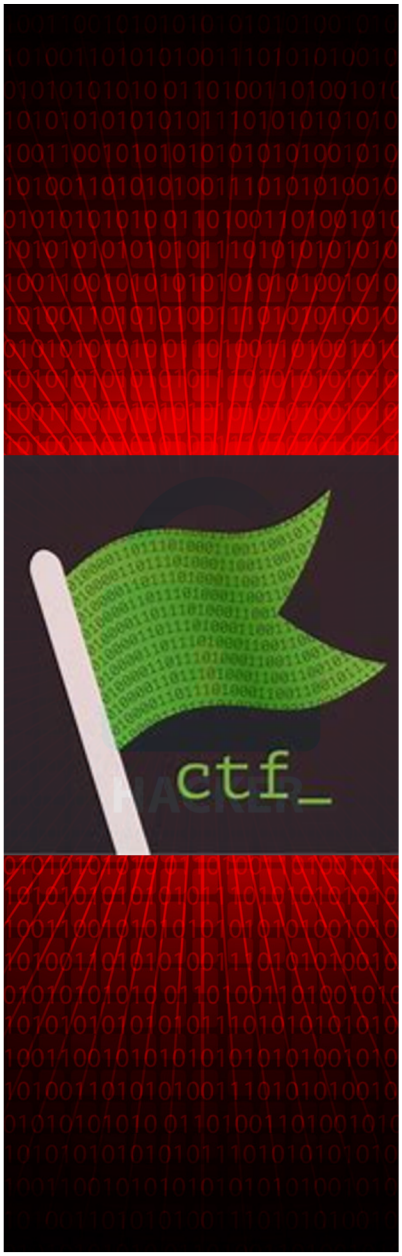
6. CTF Creation Techniques

7. How to Research to find Latest vulnerabilities

8. How to Earn via CTF's (freelancing)

9. Labs and Practical Assessments

10. Prerequisites



Introduction to CTF's Programs

- What is CTF?
- Types of CTFs: Jeopardy, Attack-Defense, Hybrid
- Overview of CTF platforms

Identifying Services and Utilization

1. Understanding Common Ports and Services
2. How to use those services in real time
3. Configuration files and commands
4. Automation scripts

CTF Lab Setup

1. Setting up Virtual Environments
2. Installation of new files and tools
3. Installation of Assessment Labs

CTF Solving Techniques

- Phases of Solving
- Initial Phase Hacking Techniques
- Understanding the OS level Structure
- Privilege Escalation
- Reverse Proxy Port forwarding Techniques

CTF Creation Techniques

- Choosing Operating System
- Basic Design for CTF's
- User level Configurations
- Checking Rabbit Holes
- Hosting it Real Time

How to Research to find Latest vulnerabilities

- Real-world case studies of bugs
- Platforms to find latest vulnerabilities

How to Earn via CTF's (freelancing)

- Platforms to Submit our CTF's
- Finding Clients to Sell our CTF's

Labs and Practical Assessments

- Hands-on practice with vulnerable applications.
- Capture the Flag (CTF) challenges.

Prerequisites

- Advance Networking Skills
- Knowledge of Kali Linux Operating System
- Top 10 Owasp Vulnerabilities
- Basic knowledge of cybersecurity tools

CONTACT US :

rajesh@cyberblockz.in

+91 8074557618

@cyberblockz_official

@cyberblockz

https://b3.cyberblockz.in