CERTIFIED JR. PENETRATION TESTER

Module 1: Introduction

- Introduction to Hacking
- Types Of Hackers
- Common Types of Attacks and Threats
- Ethical Hacking v/s Penetration Testing
- CIA Triad and Its Importance
- Ethical Hacking Life-Cycle

Module 2: Building Virtual Lab

- Introduction to Virtualization
- Installation of Kali Linux
- Installation of Metasploitable
- Installation of Windows 10

Module 3: Networking

- Introduction to Networking
- Types of Networks
- Introduction to Network Topologies & Components
- Introduction to IP Addresses & Ports
- Understanding TCP/IP, UDP Protocols
- Introduction to Client-Server Architecture
- OSI Model, Layers & Functions

Module 4: Linux Commands

- Introduction to Kali Linux
- Understanding File System Hierarchy
- Package Management Commands
- File & Directory Management Commands
- User & Group Management Commands
- Permission & Ownership Management Commands
- Understanding Passwd, Shadow files
- Security & Privilege Escalation Commands
- Process Management Commands

Module 5: Footprinting

- Introduction to Footprinting
- Types of Footprinting
- Understanding Domain Name Systems (DNS)
- Types of DNS Servers
- Passive Footprinting Techniques
- Active Footprinting Techniques

Module 6: Scanning

- Introduction to Network Scanning
- Types of Network Scanning Techniques
- Introduction to NMAP
- Host Discovery using NMAP
- Port Scanning using NMAP
- Banner Grabbing using Nmap
- Basics of Nmap Scripting Engine (NSE)
- Introduction to Nessus
- Scanning using Nessus

Module 7: Enumeration

- Introduction to Enumeration
- Difference between Enumeration & Scanning
- Types of Enumeration
- Banner Grabbing
- SNMP Enumeration
- SMTP Enumeration
- SMB Enumeration
- DNS Enumeration
- Netbios Enumeration

Module 8: Cryptography

- Introduction to Cryptography
- Key concepts in Cryptography
- Types of Encryption and Hashes
- Understanding Encryption, Hashing and Salting

Module 9: System Hacking

- Introduction to System Hacking
- Introduction to Password Cracking
- Types of Password Cracking
- Introduction to Metasploit-Framework
- Payload generation using MSF Venom and other tools
- Exploiting System Vulnerabilities using Metasploit Framework
- Gaining Access
- Stealing SAM Database
- Cracking Password
- Maintaining Access

Module 10: Malware Threats

- Introduction to Malware
- Types of Malware
- Malware Creation Toolkit
- Detection of Malware
- Malware Distribution Techniques
- Protection and Prevention Strategies

Module 11: Sniffing, Spoofing & Social Engineering

- Introduction to Sniffing
- Types of Sniffing
- Sniffing Techniques and Attacks
- Packet Sniffing using Wireshark
- Session Hijacking Attack
- Introduction to ARP Spoofing
- ARP Spoofing and ARP Poisoning Attack
- IP Spoofing Attacks
- MAC Spoofing Attack
- DNS Spoofing Attack
- Email Spoofing Attack
- Introduction to Social Engineering

- Types of Social Engineering Attacks
- Human-Based Social Engineering Attacks
- Computer-Based Social Engineering Attacks
- Phishing-Based Social Engineering Attacks

Module 12: DOS & DDOS Attack

- Introduction to Denial of Service Attack
- SYN Flood Attack
- ICMP Flood Attack
- Smurf Attack
- Slowloris Attack
- Detection and Prevention Techniques

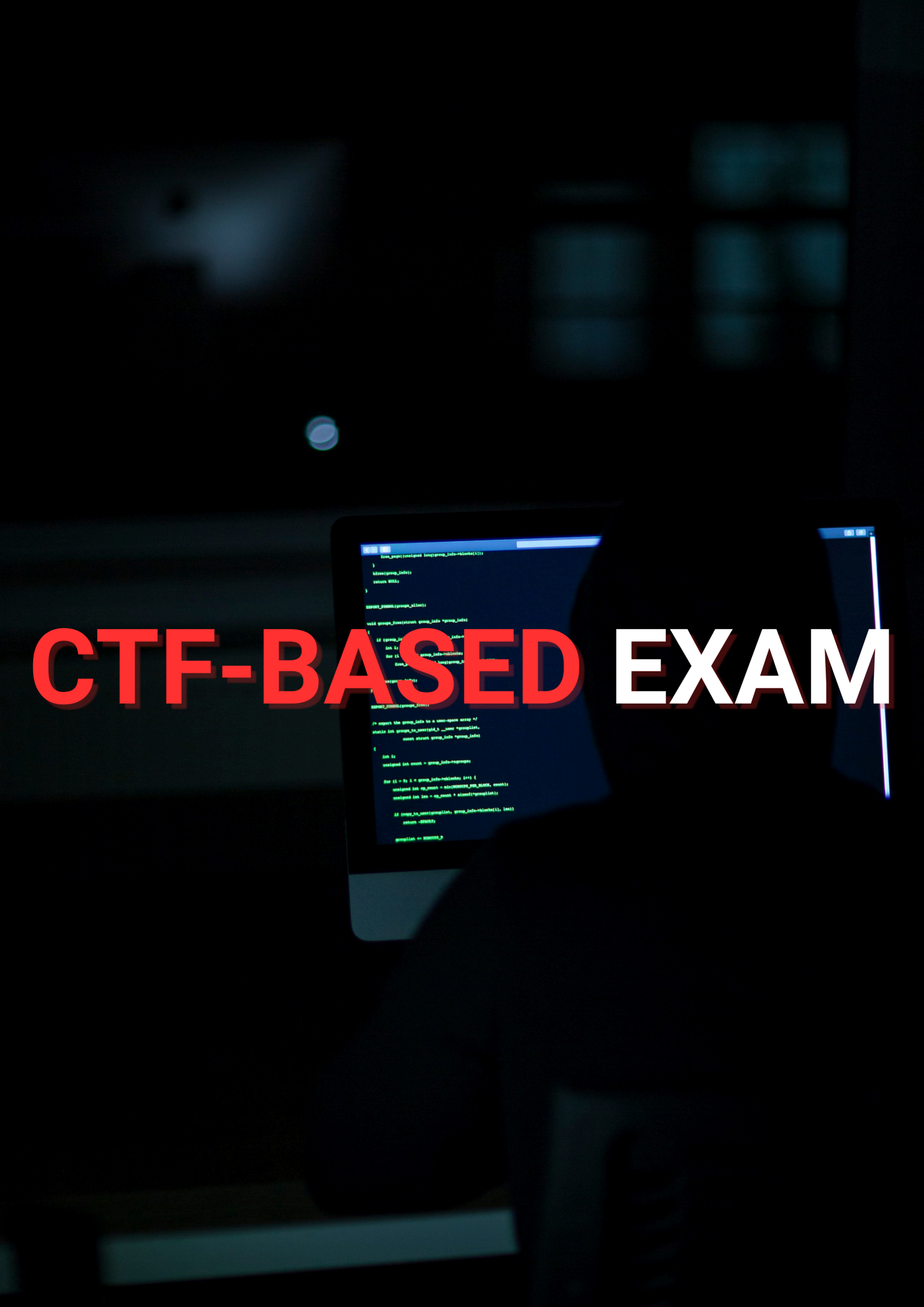
Module 13: Wireless Hacking

- Introduction to Wireless Hacking
- Fundamentals of Wireless Security
- Understanding Wireless Encryption Standar (WEP, WPA, WPA2 & WPA3)
- Wireless Network Discovery and Reconnaissance
- Packet Sniffing and Traffic Analysis
- WEP/WPA/WPA2 Cracking Techniques
- Deauthentication and Disconnection Attack
- Rogue Access Point Attack
- Man-In-The Middle Attack

Module 14: Web Application Pentesting

- Introduction to Web Application Security
- Understanding Web Application Components (Client, Server, Database)
- OWASP Top 10 Introduction
- Setting Up Lab
- Common Web Application Vulnerabilities
    - Injection Attacks
    - Cross-Site Scripting (XSS)
    - Broken Authentication and Session Management
    - Security Misconfigurations

    - Sensitive Data Exposure
    - Insecure Direct Object Reference (IDOR)
- Reconnaissance and Information Gathering
- Introduction to Burpsuite
- Post Exploitation and Privilege Escalation
- Report Writing


CTF-BASED EXAM

At the end of this course, you'll face a hands-on, real-world challenge in the form of a Capture The Flag (CTF) exam. This practical assessment tests everything you've learned—reconnaissance, exploitation, privilege escalation, and more. Solve live scenarios on a custom vulnerable machine and prove your skills to earn your certification.

CONNECT WITH US