# Certified Ethical Hacker (CEH)  Intermediate Level Syllabus

## Module 1: Introduction to Ethical Hacking

- Ethical Hacking vs. Malicious Hacking
- Cybersecurity Terminologies & Concepts
- Phases of Ethical Hacking
- Legal & Ethical Considerations

## Module 2: Networking Refreshers

- Basics of Networking (IP, MAC, DNS, DHCP)
- TCP/IP Model & OSI Model
- Common Protocols (HTTP, HTTPS, FTP, SSH, SMTP, SNMP)
- NAT, VPNs & Proxy Servers

## Module 3: Windows Fundamentals

- Windows OS Architecture
- Windows Filesystem & Registry
- Windows User & Group Management
- Command Prompt & PowerShell Basics

## Module 4: Linux Fundamentals

- Linux Filesystem & Directory Structure
- Common Linux Commands
- User & Permission Management
- Package Management (APT, YUM)

## Module 5: Active Directory Introduction

- What is Active Directory (AD)?
- AD Components: Domains, Trees, Forests
- User Authentication & Group Policies
- AD Security Basics & Common Threats

## Module 6: Footprinting & Reconnaissance

- OSINT (Open-Source Intelligence) Techniques
- Active vs. Passive Reconnaissance
- Whois, Netcraft, Shodan & Google Dorking

- DNS Footprinting & Social Media Recon

### Module 7: Scanning & Enumeration

- Network Scanning with Nmap & Masscan
- Port Scanning Techniques (TCP, UDP, SYN, ACK)
- Enumerating Users, Shares & Services
- SNMP, LDAP, SMB & NetBIOS Enumeration

### Module 8: Vulnerability Analysis

- Common Vulnerability Types (CVE, CWE)
- Automated Scanning with Nessus, OpenVAS
- Manual Vulnerability Analysis Techniques
- ExploitDB & Public Exploit Repositories

### Module 9: System Hacking & Privilege Escalation

- Password Cracking (Hashcat, John the Ripper)
- Exploiting Windows & Linux Systems
- Privilege Escalation Techniques
- Covering Tracks & Maintaining Access

### Module 10: Malware Threats & Reverse Engineering

- Types of Malware (Viruses, Worms, Trojans, Ransomware)
- Malware Obfuscation & Evasion
- Sandboxing & Behavioral Analysis
- Reverse Engineering Basics

### Module 11: Sniffing & Traffic Analysis

- Packet Sniffing with Wireshark & Tcpdump
- MITM (Man-in-the-Middle) Attacks
- ARP Spoofing & DNS Poisoning
- Detecting & Preventing Sniffing Attacks

### Module 12: Web Application Security

- OWASP Top 10 Vulnerabilities
- SQL Injection, XSS, CSRF Attacks
- Web Server & API Exploitation
- Secure Coding Practices

## Module 13: Wireless Network Security

- Wi-Fi Encryption Standards (WEP, WPA, WPA2, WPA3)
- Cracking Wireless Networks with Aircrack-ng
- Rogue Access Points & Evil Twin Attacks
- Hardening Wireless Security

## Module 14: Social Engineering & Phishing Attacks

- Types of Social Engineering Attacks
- Phishing Techniques & Red Teaming
- Credential Harvesting & Impersonation Attacks
- Defending Against Social Engineering

## Module 15: Exploiting Enterprise Services (Updated with Basics)

- Introduction to Enterprise Networks (AD, DNS, DHCP, VPNs)
- Active Directory Basics  Users, Groups, Policies
- SMB, LDAP, Kerberos Overview
- Attacking & Exploiting SMB, LDAP, RDP
- Lateral Movement Techniques (Pass-the-Hash, Pass-the-Ticket)
- Defensive Measures for Enterprise Networks

## Module 16: Firewall & IDS/IPS Security

- What is a Firewall? Types & Working
- Bypassing Firewalls & IDS/IPS
- Configuring and Hardening Firewalls
- Intrusion Detection & Prevention Systems

## Module 17: Cloud Security & Hacking

- Cloud Computing Basics (AWS, Azure, GCP)
- Cloud Storage Exploitation
- Container Security (Docker, Kubernetes)
- Cloud Misconfigurations & Exploitation

## Module 18: Digital Forensics & Incident Response (DFIR) (Updated with Basics)

- Introduction to Digital Forensics & Incident Response
- Understanding Digital Evidence (Types & Collection Methods)
- Memory, Disk, and Network Forensics Basics
- Windows & Linux Log Analysis for Beginners

- Analyzing Log Files & Indicators of Compromise (IoCs)
- SIEM & Threat Intelligence Overview

## Module 19: Denial of Service (DoS & DDoS) Attacks

- DoS vs. DDoS: Attack Vectors & Tools
- Amplification & Reflection Attacks
- Botnets & IoT-based DDoS Attacks
- Mitigation & Defense Strategies

## Module 20: Ethical Hacking Challenges & Certifications

- Capture The Flag (CTF) Platforms (TryHackMe, HackTheBox)
- Preparing for CEH, OSCP, and Other Certifications
- Bug Bounty Platforms & Responsible Disclosure
- Career Roadmap for Ethical Hackers