Course Outline — Ethical Hacking & Penetration Testing

Unit 1: Introduction to Ethical Hacking

- Overview of cyber security and ethical hacking principles.
- Understanding threat actors, attack vectors, and the cyber security landscape.
- Legal and ethical considerations in penetration testing.

Unit 2: Reconnaissance and Foot printing

- Passive vs. active information gathering.
- Identifying targets, domain information, and network mapping.
- Tools: Nmap, Maltego, Whois, and OSINT frameworks.

Unit 3: Scanning and Enumeration

- Identifying open ports and running services.
- Banner grabbing and vulnerability detection.
- Network and system enumeration with automated scanners.

Unit 4: Vulnerability Assessment

- Using vulnerability scanners (Nessus, OpenVAS).
- Manual vulnerability verification and prioritization.
- Risk rating and reporting vulnerabilities.

Unit 5: Exploitation and Privilege Escalation

- Exploiting discovered vulnerabilities in lab environments.
- Privilege escalation techniques on Windows and Linux systems.
- Maintaining access and simulating attacker behavior safely.

Unit 6: Post-Exploitation and Reporting

- Lateral movement and persistence mechanisms.
- Data extraction and cleanup processes.
- Writing professional penetration test reports and presenting findings.

Unit 7: Defensive Countermeasures

- Detecting and mitigating attacks.
- Blue Team perspectives and incident response basics.
- Integrating offensive insights into defensive strategy.

Expected Learning Outcomes

- Conduct professional penetration tests ethically and safely.
- Identify and exploit vulnerabilities using industry tools.
- Communicate findings effectively through structured reports.
- Understand legal frameworks and compliance requirements.
- Prepare for certifications such as CEH, OSCP, or CPT.