



MERSENNE CYBERCOUNSELLORS LLP

Course Syllabus: Penetration Testing with Labs

Course Overview:

This 6-week hands-on course provides participants with in-depth knowledge and practical experience in penetration testing. Learners will engage in simulated penetration testing environments, practicing real-world scenarios, vulnerability exploitation, and security assessments using industry-standard tools.

Course Details:

- **Duration:** 6 Weeks
 - **Fee:** ₹15,000
 - **Mode:** Online/Offline (as applicable)
 - **Prerequisites:** Basic networking and cybersecurity knowledge recommended
 - **Certification:** Upon successful completion, participants will receive a certification from Mersenne Cybercounsellors LLP
-

Week 1: Introduction to Penetration Testing

- Ethical Hacking vs. Penetration Testing
- Understanding the Cyber Kill Chain and MITRE ATT&CK Framework
- Legal and Ethical Considerations in Penetration Testing
- Lab Setup: Kali Linux, Virtual Machines, and Testing Environments

Week 2: Reconnaissance and Information Gathering

- Active vs. Passive Reconnaissance Techniques
- OSINT (Open-Source Intelligence) and Social Engineering
- Network Scanning and Enumeration (Nmap, Netcat)
- Hands-on Lab: Identifying Open Ports and Services

Week 3: Exploitation and Vulnerability Assessment

- Understanding Common Vulnerabilities (OWASP Top 10, CVE)
- Web Application Penetration Testing (SQL Injection, XSS, CSRF)
- Exploiting Network Vulnerabilities with Metasploit
- Hands-on Lab: Identifying and Exploiting System Weaknesses

Week 4: Privilege Escalation and Post-Exploitation



MERSENNE CYBERCOUNSELLORS LLP

- Windows and Linux Privilege Escalation Techniques
- Maintaining Access: Backdoors, Persistence, and Rootkits
- Data Exfiltration and Lateral Movement
- Hands-on Lab: Gaining and Elevating Privileges

Week 5: Wireless, Cloud, and Mobile Penetration Testing

- Wireless Network Attacks: WPA Cracking, Rogue APs
- Cloud Security Testing: AWS, Azure, Google Cloud
- Mobile Application Penetration Testing (Android, iOS)
- Hands-on Lab: Attacking Wireless and Cloud Infrastructures

Week 6: Reporting, Mitigation, and Final Assessment

- Penetration Testing Report Writing and Documentation
- Security Hardening and Patch Management
- Red Team vs. Blue Team Exercises
- **Final Lab Assessment:** Conducting a Full Penetration Test

Assessment & Certification:

- Weekly hands-on labs and exercises
- Final penetration testing assessment
- Certification of Completion from Mersenne Cybercounsellors LLP

Target Audience:

- Cybersecurity professionals and ethical hackers
- IT security analysts and penetration testers
- Students and enthusiasts looking to gain hands-on experience

Learning Outcomes:

- Understand and apply penetration testing methodologies
- Identify and exploit security vulnerabilities in various environments
- Use industry-standard tools such as Metasploit, Nmap, and Burp Suite
- Generate professional penetration testing reports

For inquiries and enrollment,
contact us at : **7499076330**

email at : info.cybercounsellors@gmail.com