

Ethical Hacking

1. Introduction to Ethical Hacking & Cybersecurity

- What is ethical hacking and its importance
 - Difference between ethical hackers & malicious hackers
 - Cybersecurity concepts, threat landscape
 - OSI/ TCP/IP models review and hacker mindset
-

2. Footprinting & Reconnaissance

- Passive and active information gathering
 - Tools: WHOIS, TheHarvester, OSINT techniques
 - Understanding target scope and rules of engagement
-

3. Scanning and Enumeration

- Network scanning approaches (TCP/UDP)
 - Tools: Nmap, Nessus, OpenVAS
 - Enumeration of services, shares, and users
-

4. Vulnerability Assessment Fundamentals

- What is vulnerability assessment vs penetration testing
 - OWASP Top 10, common CVEs
 - Automated scanners vs manual checks
-

5. Penetration Testing Methodologies

- PTES / OSSTMM / NIST frameworks
- Pen testing lifecycle: planning, discovery, attack, reporting
- Safe testing practices and non-destructive techniques

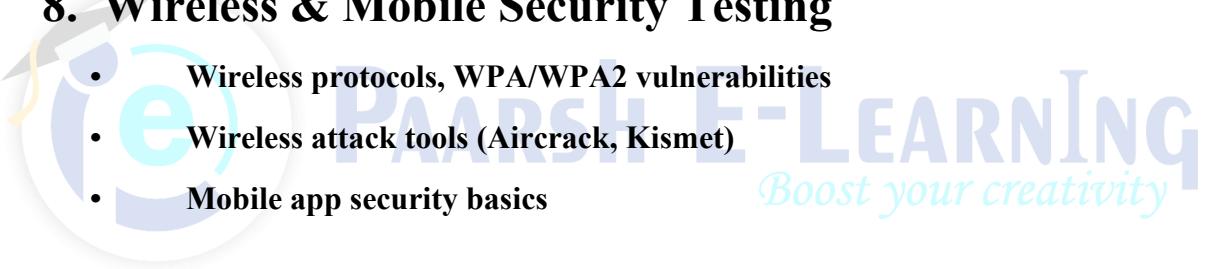
6. Network Penetration Testing

- Port scanning & service enumeration
 - Exploiting network vulnerabilities
 - Man-in-the-middle, ARP spoofing, DNS attacks
-

7. Web Application Penetration Testing

- SQL Injection, XSS, CSRF, security misconfigurations
 - Tools: Burp Suite, OWASP ZAP, sqlmap
 - Manual testing techniques and validation
-

8. Wireless & Mobile Security Testing

- 
- Wireless protocols, WPA/WPA2 vulnerabilities
 - Wireless attack tools (Aircrack, Kismet)
 - Mobile app security basics
-

9. Exploitation Techniques & Tools

- Metasploit Framework basics
 - Creating and using payloads
 - Exploitation of services and applications
-

10. Post-Exploitation & Privilege Escalation

- Maintaining access and establishing persistence
 - Privilege escalation on Windows and Linux
 - Clearing logs and covering tracks
-

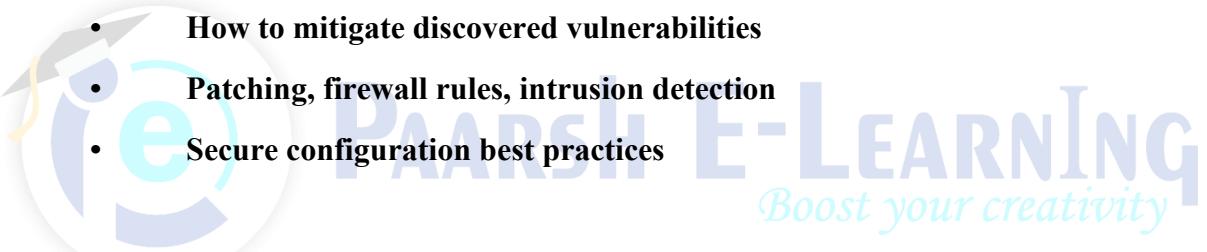
11. Reporting & Legal / Ethical Issues

- Writing professional penetration test reports
 - Executive summaries and risk ratings
 - Cyber laws, consent, and ethical boundaries
-

12. Security Tools Lab & Practical Sessions

- Hands-on labs with Kali Linux tools
 - Scenario-based VAPT exercises
 - Capture-the-Flag (CTF) style practice
-

13. Defensive Countermeasures & Security Hardening

- How to mitigate discovered vulnerabilities
 - Patching, firewall rules, intrusion detection
 - Secure configuration best practices
- 
- The logo for Paarsh E-Learning features a stylized 'P' and 'e' in blue and grey, followed by the text 'PAARSH E-LEARNING' in a large, bold, blue font. Below it, the tagline 'Boost your creativity' is written in a smaller, italicized blue font.

14. Capstone Project: Full VAPT Process

- End-to-end vulnerability assessment and penetration test
 - Report generation and presentation
 - Real-world case study application
-