CYBERIUM

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

VAPT

INTRODUCTION

The Vulnerability Assessment and Penetration Testing (VAPT) Course is designed to provide participants with a comprehensive understanding of cybersecurity testing techniques used to identify, assess, and exploit vulnerabilities in networks, applications, and systems. With increasing cyber threats and data breaches, organizations require skilled security professionals who can proactively assess their IT infrastructure and protect against potential attacks. This course equips learners with the theoretical knowledge and hands-on skills needed to perform penetration testing, security assessments, and ethical hacking using industry-standard tools and methodologies.

The course follows a structured approach, covering the fundamentals of ethical hacking, vulnerability scanning, penetration testing frameworks, web and network security testing, and report writing. Participants will gain hands-on experience using popular security tools like Kali Linux, Metasploit, Burp Suite, Nmap, Wireshark, and more. By the end of the course, learners will be able to identify security weaknesses, exploit vulnerabilities, and provide remediation strategies to enhance an organization's security posture.

COURSE OBJECTIVES

By completing this course, participants will be able to:

- Understand ethical hacking concepts, methodologies, and legal considerations.
- Conduct vulnerability assessments to identify security weaknesses in networks and applications.
- Perform penetration testing using industry-standard tools and techniques.
- Exploit common vulnerabilities such as SQL injection, cross-site scripting (XSS), buffer overflow, and privilege escalation.
- Assess the security of web applications, networks, wireless systems, and cloud environments.
- Generate comprehensive security reports with risk assessments and mitigation recommendations.
- Prepare for certifications like CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional), and eJPT (eLearnSecurity Junior Penetration Tester).

VAPT COURSE SYLLABUS

Module 01- Introduction to VAPT

1. **Understanding Vulnerability Assessment and Penetration Testing**
2. **Differences between Vulnerability Assessment and Penetration Testing**
3. **Ethical hacking methodologies and legal considerations**
4. **Importance of cybersecurity in modern organizations**

Module 02- Setting Up the Lab Environment

1. **Introduction to Kali Linux**
2. **Installing and configuring Virtual Machines (VMs)**
3. **Setting up Metasploitable 2, OWASP-BWA, and vulnerable applications**
4. **Using penetration testing tools and frameworks**

Module 03- Information Gathering and Reconnaissance

1. **Passive vs. Active Reconnaissance**
2. **OSINT Framework**
3. **Host Discovery**
4. **Using WHOIS, Shodan, and Google Dorking**
5. **DNS Lookup, Wappalyzer and Wayback Machine**
6. **Email Footprinting**

Module 04- Scanning and Enumeration

1. **Network scanning with Nmap and Zenmap**
2. **Host Discovery using Nmap**
3. **Port Scanning**
4. **Vulnerability Scanning using Nmap**
5. **Enumerating services**
6. **FTP, SMB, SSH, RDP, Telnet, SMTP, VNC and MySQL Enumeration**
7. **Service Credential Brute Forcing using Hydra**

Module 05- Vulnerability Assessment

1. **Introduction to vulnerability scanning**
2. **Vulnerability Analysis Life Cycle**
3. **Understanding terms such as CVE, CVSS, and NVD**
4. **Automated vs. Manual vulnerability assessment**
5. **Using Nessus, Burp Suite Professional and Nikto**
6. **Interpreting scan results and risk analysis**
7. **Generating Report**

Module 06- Penetration Testing Methodologies

1. **Planning and executing penetration tests**
2. **Black Box, White Box, and Gray Box Testing**
3. **Understanding OWASP Top 10 vulnerabilities**
4. **Reporting and documenting findings**

Module 07- Network Penetration Testing

1. **Identifying open ports and services**
2. **Exploiting misconfigurations and weak credentials**
3. **Conducting attacks such as Man-in-the-Middle (MITM), Brute Force attacks**
4. **Conducting Exploitation and Post Exploitation**
5. **Performing Privilege Escalation on Windows and Linux machines**
6. **Conducting Credential Looting**
7. **Pivoting in Networks**

Module 08- Web Application Penetration Testing

1. **Understanding OWASP Top 10 Web Vulnerabilities**
2. **SQL Injection, Cross-Site Scripting (XSS) and Command Injection attacks**
3. **Directory Traversal, File Upload and API vulnerabilities**
4. **Broken Access Control, SSRF, CSRF and Information Disclosure**
5. **Exploiting authentication and session management flaws**
6. **Burp Suite for manual web application testing**

Module 09- Exploitation and Privilege Escalation

1. **Exploiting vulnerabilities with Metasploit Framework**
2. **Windows and Linux privilege escalation techniques**
3. **Post-exploitation techniques and maintaining access**
4. **Covering tracks and avoiding detection**

Module 10- Social Engineering and Phishing Attacks

1. **Understanding social engineering techniques**
2. **Creating phishing campaigns using SET (Social Engineering Toolkit)**
3. **Spear phishing, credential harvesting, and email spoofing**
4. **Countermeasures and security awareness training**

Module 11- Writing Penetration Testing Reports

1. **Documenting findings and risk assessment**
2. **Writing professional security assessment reports**
3. **Recommendations and mitigation strategies**
4. **Presenting findings to stakeholders**