

Branch Name:	MCA
Program Code:	CS201
Course Title	Vulnerability Assessment and Penetration Testing (VAPT)
Course Code	4CS2010310T
Pre-requisite Course:	Basic knowledge of computer networks, operating systems (Windows/Linux), and programming/scripting is required. Students should also be familiar with web technologies, databases, and fundamental cybersecurity concepts (CIA triad).

Course Objective:

- To enable students to understand the fundamentals of cybersecurity and the role of Vulnerability Assessment and Penetration Testing (VAPT) in securing systems and networks.
- To develop the ability to identify, analyze, and exploit vulnerabilities using standard tools and methodologies.
- To provide hands-on knowledge of network, system, and web application security testing techniques.
- To introduce best practices for reporting, risk assessment, and remediation of security vulnerabilities.
- To prepare students for cybersecurity roles such as Penetration Tester, Security Analyst, Ethical Hacker, and VAPT Consultant.

Teaching and Examination Scheme:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture	Tutorial	Practical	Credit	Theory		Practical		Total
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
3	-	-	3	60	40	-	-	100

Course Contents:

Unit No	Topics	Total Hours	Weightage (%)
1	Introduction to VAPT Core Security Concepts: -Confidentiality, Integrity, Availability (CIA), - Ethical hacking vs. malicious hacking, - The role of VAPT in modern cybersecurity VAPT Methodologies & Standards: - Penetration Testing Execution Standard (PTES), - OWASP Testing Guide (focus on web applications), -NIST SP 800-115 (Technical Guide to Information Security Testing) Legal and Ethical Framework: - Computer Fraud and Abuse Act (general overview), - Scope definition and Rules of Engagement, -Understanding liabilities and disclaimers VAPT Phases: -Reconnaissance, - Scanning and Enumeration, - Vulnerability Assessment, - Exploitation, - Post-Exploitation and Reporting Setting Up a Testing Lab: - Virtual machines and isolated networks, - Kali Linux, Parrot OS, or similar distros, - Overview of essential VAPT tools (Nmap, Metasploit, Burp Suite, Nessus)	7	25

2	Reconnaissance & Scanning Open-Source Intelligence (OSINT): - Passive Recon: Using public data, social media, databases, - Searching for leaked credentials, metadata analysis Active Reconnaissance: - Port scanning with Nmap/Masscan, - Identifying live hosts and running services, - Banner grabbing and version detection Network Enumeration: - Techniques for mapping network topology, - Scanning protocols (SMB, SNMP, FTP, HTTP), - OS fingerprinting Service & Application Enumeration: - Enumerating web technologies (CMS, frameworks), - Finding hidden files, directories, or subdomains, - DNS enumeration, zone transfers Avoiding Detection: - Timing techniques to bypass Intrusion Detection Systems (IDS), - Rate-limiting, randomization, decoys, - Evasion strategies	8	25
3	Vulnerability Assessment Vulnerability Scanning Tools: - Nessus, OpenVAS, QualysGuard, - Web vulnerability scanners (Nikto, OWASP ZAP), -Evaluating scan results, handling false positives Vulnerability Classification: - OWASP Top 10 for web applications, - Common Vulnerabilities and Exposures (CVE), - Common Vulnerability Scoring System (CVSS) In-Depth Analysis: - Manual verification of automated findings, - Exploit databases (Exploit-DB, Rapid7), - Researching patches and known exploits Vulnerability Assessment Across Environments: - Web applications and APIs, - Network devices (routers, firewalls), Virtual machines and containerized deployments Prioritizing Remediation: - Risk-based approach to patching, - Business impact vs. exploit likelihood, - Coordinating with system owners and development teams	8	25
4	Penetration Testing Pen Test Methodology: -Planning and reconnaissance review, - Identifying high-value targets, - Scanning, enumeration, and vulnerability exploitation Exploitation Techniques: - Local and remote exploits, - Payloads, shells, reverse connections, - Utilizing Metasploit and custom scripts Network Penetration Testing: - Wireless attacks (WEP/WPA cracking, Rogue APs), - Man-in-the-Middle (MITM) attacks, ARP spoofing, - Pivoting within compromised networks Web Application Penetration Testing: - Injection attacks (SQLi, command injection), - Cross-Site Scripting (XSS), CSRF, - Session hijacking, broken authentication, SSRF Post-Exploitation & Lateral Movement: - Privilege escalation on Windows and Linux, - Persistence and covering tracks, - Data exfiltration techniques	9	25

5	Reporting & Remediation Documentation & Reporting: - Structuring a professional penetration test report, - Technical findings vs. executive summaries, - Communicating risk to stakeholders Remediation Strategies: - Patch management processes, - Secure configuration and hardening guidelines, - Web Application Firewalls (WAF), Intrusion Prevention Systems (IPS) Verification & Retesting: - Confirming patches and mitigations, - Continuous monitoring and vulnerability management, - DevSecOps: Integrating security testing into the CI/CD pipeline Incident Response Integration: - Aligning pen test findings with incident response plans, -Forensic analysis of penetration test scenarios, - Building robust detection and response capabilities Career Path & Certification: - Recognized penetration testing certifications (OSCP, CEH, eCPPT), - Ethical responsibilities and ongoing skill development, - Future trends in penetration testing (AI-based detection, automated scanning)	7	25
---	---	---	----

Text Books:

1. Penetration Testing: A Hands-On Introduction to Hacking
2. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws
3. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy
4. Penetration Testing Fundamentals: A Hands-On Guide to Pen Testing

References Books:

1. Metasploit: The Penetration Tester's Guide
2. Hacking: The Art of Exploitation
3. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning
4. Kali Linux Revealed: Mastering the Penetration Testing Distribution
5. OWASP Testing Guide
6. Black Hat Python: Python Programming for Hackers and Pentesters
7. Advanced Penetration Testing: Hacking the World's Most Secure Networks
8. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy

List of Open Source Software/learning website:

- www.kali.org
- www.nmap.org
- www.metasploit.com
- www.zaproxy.org
- www.wireshark.org
- www.owasp.org
- www.tryhackme.com
- www.hackthebox.com
- www.portswigger.net/web-security

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Description	Bloom's Taxonomy Level
CLO1	Understand fundamental cybersecurity concepts, VAPT methodologies, and security standards used in vulnerability assessment and penetration testing.	1 Remembering, 2 Understanding
CLO2	Apply reconnaissance, scanning, and enumeration techniques to identify potential vulnerabilities in systems and networks.	2 Understanding, 3 Applying
CLO3	Analyze vulnerabilities using various tools and frameworks, and evaluate risks based on severity and impact.	3 Applying, 4 Analyze, 5 Evaluate
CLO4	Perform penetration testing by exploiting vulnerabilities in network and web applications using appropriate tools and techniques.	3 Applying, 4 Analyze, 5 Evaluate
CLO5	Develop professional reports and recommend remediation strategies to mitigate identified security risks.	3 Applying, 6 Create
CLO6	Identify legal, ethical, and compliance issues in VAPT and apply responsible practices during security testing.	2 Understanding, 4 Analyze

Mapping of CLOs with POs & PSOs

Course Learning Outcomes	Program Outcomes(POs)												Program Specific Outcomes (PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CLO1	H	M			L	-	-	-	-	-	-	-	M	L
CLO2	-	H	M	H	H	-	-	-	-	-	-	-	H	H
CLO3	-	M	H	H	H	-	-	-	-	L		-	H	H
CLO4	L	-	H	H	H	M	-	-	M	-	-	-	H	H
CLO5	-	-	M	M	M	H	-	-	-	H	L	-	M	H
CLO6	L	L	-	-	-	-	M	H	M	-	-	-	M	M

H: High, M: Medium, L: Low