

Branch Name:	MCA
Program Code:	CS201
Course Title	Vulnerability Assessment and Penetration Testing (VAPT) Practical
Course Code	4CS2010310P
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	
-	-	4	2	-	-	25	25	50

LAB/ Practical:

Note: The practical list provided beneath is for reference only. The course teacher may Change/formulate it as per his/her methodology and requirement.

Sr. No	Practical Experiments
1	OSINT & Recon Gather public information on a simulated target: subdomains, WHOIS, metadata etc.
2	DNS Misconfiguration & Zone Transfer Testing Test DNS server misconfigurations, Enumerate DNS records, Perform DNS Zone Transfer.
3	Vulnerability Scan Run a web application scanner (e.g., OWASP ZAP), Nessus, OpenVAS on a vulnerable test site like DVWA.
4	Manual Vulnerability Analysis Validate automated scan results manually; identify false positives/negatives.
5	Clickjacking Exploitation Demonstrate UI redressing attack and demonstrate hidden button click.
6	Privilege Escalation Identify and exploit privilege escalation flaws in a Linux or Windows test environment.

7	Wireless Network Penetration Capture and crack WPA2 handshakes with tools like Aircrack-ng (in a controlled lab).
8	Web App Exploitation Exploit SQL injection or cross-site scripting on a deliberately vulnerable web app.
9	Post-Exploitation & Pivoting Move laterally within a virtual environment, set up a pivot to attack another subnet.
10	VAPT Reporting Compile findings from the above exercises into a professional-style pentest report, including remediation steps.

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 Out comes(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