

FACULTY OF COMPUTER APPLICATIONS

Programme	Master of Computer Applications	Branch/Spec.	Computer Application
Semester	II	Version	1.0.0.0
Effective from Academic Year	2026-27	Effective for the batch Admitted in	July 2026
Subject Code	P12A5EHV	Subject Name	Ethical Hacking & Vulnerability Assessment

Teaching scheme						Examination scheme (Marks)			
(Per week)	Lecture (DT)		Practical (Lab.)		Total		CIA	SEE	Total
	L	TU	P	TW					
Credit	2	0	2	0	4	Theory	40	60	100
Hours	2	0	4	0	6	Practical	20	30	50

Objective:

To develop knowledge of ethical hacking, reconnaissance, vulnerability assessment, penetration-testing methodologies, and network, wireless, and web application security and enable them report security vulnerabilities using recognized methodologies and tools in authorized environments.

Pre-requisites:

Require the basic knowledge of computer networks, operating systems, Linux, web technologies, databases, programming fundamentals, and cybersecurity concepts. Familiarity with TCP/IP, HTTP/HTTPS, virtualization, and basic network-security concepts is desirable.

Course Outcomes:

Name of CO	Description
CO1	Explain ethical hacking principles, legal and ethical requirements, penetration-testing methodologies, and security assessment processes.
CO2	Perform systematic reconnaissance, scanning, enumeration, and vulnerability assessment using appropriate security tools.
CO3	Analyze common vulnerabilities in networks, operating systems, wireless systems, and web applications in controlled environments.
CO4	Apply VAPT methodologies to prioritize vulnerabilities and prepare professional penetration-testing reports with remediation recommendations.

Mapping of CO and PO

Cos	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	2	3	2	2	1	-	3	2
CO2	2	3	2	3	1	-	3	2

CO3	2	3	3	3	1	-	3	3	
CO4	2	3	3	3	2	1	3	3	
Content:									
Unit	SECTION – I								Hrs
1	Foundations of Ethical Hacking and Penetration Testing Introduction to cyber security , information security and ethical hacking.CIA triad, threat, vulnerability, exploit and risk concepts. Types of hackers and threat actors, hacking phases and penetration-testing lifecycle, legal and ethical framework, Information Technology Act 2000 and relevant cyber laws, authorization, scope, rules of engagement, contracts and responsible disclosure, penetration-testing methodologies, Penetration Testing Execution Standard (PTES), OWASP Testing Guide, black-box, white-box and grey-box testing.vulnerability assessment versus penetration testing,								07
2	Reconnaissance, Scanning, Enumeration and Vulnerability Assessment Passive reconnaissance, OSINT fundamentals, WHOIS, DNS enumeration, search-engine intelligence, Shodan and Censys concepts, active reconnaissance, host discovery, ping sweep and traceroute, port scanning, TCP and UDP scanning, Nmap, service and operating-system fingerprinting, banner grabbing, Nmap Scripting Engine, SMB, NetBIOS, SNMP, LDAP and NFS enumeration, vulnerability-scanning fundamentals, Nessus, OpenVAS and Qualys, authenticated and unauthenticated scanning, vulnerability validation, CVE, CVSS-based vulnerability scoring, false positives and false negatives, vulnerability prioritization, vulnerability management lifecycle, remediation strategies, and security hardening.								08
SECTION – II									
3	Network, Wireless, System and Web Application Security Password and credential security, password hashing, dictionary and brute-force attacks, credential stuffing, John the Ripper and Hashcat concepts, malware and malicious-code fundamentals, network attacks including ARP spoofing, man-in-the-middle attacks, DNS spoofing, session hijacking and network sniffing, Wireshark-based traffic analysis, Metasploit Framework architecture, controlled exploitation, privilege-escalation concepts in Windows and Linux, wireless security, WEP, WPA, WPA2 and WPA3, rogue access points, Evil Twin, Bluetooth and IoT attack surfaces, web application architecture, HTTP/HTTPS security, Burp Suite and OWASP ZAP, OWASP Top 10, SQL injection, command injection, XSS, CSRF, SSRF, broken access control, authentication and session-management weaknesses, insecure deserialization, security misconfiguration, API security, REST/GraphQL security testing and business-logic vulnerabilities.								08
4	VAPT, Risk Assessment, Reporting and Emerging Security Areas Vulnerability assessment and penetration-testing methodology comparison, CVSS-based risk prioritization, exploitation and post-exploitation concepts, maintaining access, pivoting and lateral movement in controlled environments, social engineering fundamentals including								07

	phishing and pretexting, physical security-testing concepts, cloud and mobile application penetration-testing overview, vulnerability verification, evidence collection, executive and technical reporting, risk ratings, remediation roadmap, professional communication with stakeholders, responsible disclosure, bug-bounty ecosystems, security-testing certifications including CEH, OSCP and CompTIA PenTest+, case-study analysis, and complete VAPT assessment methodology.	
Practical Content:		
List of programs specified by the subject teacher based on above mentioned topics		
Text/Reference Books:		
1	☐ Patrick Engebretson, The Basics of Hacking and Penetration Testing , Syngress. ☐ EC-Council, Certified Ethical Hacker (CEH) v12 Courseware , EC-Council. ☐ Dafydd Stuttard and Marcus Pinto, The Web Application Hacker’s Handbook , Wiley.	
2	☐ Georgia Weidman, Penetration Testing: A Hands-On Introduction to Hacking , No Starch Press. ☐ Michael Sikorski and Andrew Honig, Practical Malware Analysis , No Starch Press. ☐ OWASP Foundation, OWASP Web Security Testing Guide . ☐ NIST, SP 800-115: Technical Guide to Information Security Testing and Assessment . ☐ Penetration Testing Execution Standard (PTES) .	
Web References / MOOC / Certification Course		
1	Google Cybersecurity Professional Certificate Coursera	
2	https://learn.saylor.org/mod/page/view.php?id=29506	
3	https://labex.io/free-labs/cybersecurity	
Question Paper Scheme:		
	University Examination Duration: 3 Hours Note for Examiner: - (I) Questions 1 and 4 are compulsory with no options. (II) Internal options should be given in questions 2, 3, 5 and 6. SECTION – I Q.1 –8 Marks Q.2 –11 Marks Q.3 –11 Marks SECTION - II Q.4 –8 Marks Q.5 –11 Marks Q.6 –11 Marks	