COURSE TITLE	**VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)**
COURSE CODE	**01CC0702**
COURSE CREDITS	**4**

Objective:

1. Students will understand core security concepts including CIA triad, ethical hacking vs. malicious hacking, and the role of VAPT in modern cybersecurity.
2. Students will learn VAPT methodologies and standards including PTES, OWASP Testing Guide, and NIST SP 800-115 along with legal and ethical frameworks.
3. Students will develop proficiency in reconnaissance and scanning techniques using OSINT, Nmap, Masscan, and enumeration tools for mapping targets.
4. Students will perform vulnerability assessments using tools like Nessus, OpenVAS, and OWASP ZAP, and classify vulnerabilities using CVE and CVSS.
5. Students will conduct penetration testing including exploitation, post-exploitation, privilege escalation, wireless attacks, and web application attacks.
6. Students will create professional penetration test reports, implement remediation strategies, and integrate security testing into DevSecOps CI/CD pipelines.

Course Outcomes: After completion of this course, student will be able to:

1. Understanding of VAPT Fundamentals and core security concepts.
2. Understand VAPT methodologies, standards, and legal/ethical frameworks.
3. Apply reconnaissance, scanning, and vulnerability assessment tools and techniques effectively.
4. Analyze and conduct penetration tests on networks, wireless systems, and web applications.
5. Create professional penetration test reports with remediation strategies and DevSecOps integration.

Pre-requisite of course: Basic Programming Knowledge, Fundamentals of Operating Systems (Linux and Windows), Basic Understanding of Web Technologies (HTTP, HTML)

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
3	0	2	50	30	20	25	25

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
1	**Introduction to VAPT** Core Security Concepts (CIA Triad), Ethical hacking vs. malicious hacking, Role of VAPT in cybersecurity,, VAPT Methodologies & Standards (PTES, OWASP Testing Guide, NIST SP 800-115),, Legal and Ethical Framework (CFAA, Scope, Rules of Engagement),, VAPT Phases (Reconnaissance, Scanning, Vulnerability Assessment, Exploitation, Post-Exploitation, Reporting), Setting Up a Testing Lab (Kali Linux, Parrot OS, Nmap, Metasploit, Burp Suite, Nessus).	9
2	**Reconnaissance & Scanning** Open-Source Intelligence (OSINT) and Passive Recon, Active Reconnaissance (Port scanning with Nmap/Masscan),, Banner grabbing and version detection, Network Enumeration (SMB, SNMP, FTP, HTTP),, Service & Application Enumeration (CMS, frameworks, subdomains),, DNS enumeration and zone transfers, OS fingerprinting,, Avoiding Detection (IDS evasion, timing, decoys).	8
3	**Vulnerability Assessment** Vulnerability Scanning Tools (Nessus, OpenVAS, QualysGuard, Nikto, OWASP ZAP), Vulnerability Classification (OWASP Top 10, CVE, CVSS), Manual verification of automated findings, Exploit databases (Exploit-DB, Rapid7), Vulnerability Assessment across environments (Web apps, APIs, Network devices, VMs, Containers), Risk-based approach to prioritizing remediation,, Business impact vs. exploit likelihood, Coordinating with system owners and development teams.	12
4	**Penetration Testing** Pen Test Methodology (Planning, Reconnaissance review, High-value targets),, Exploitation Techniques (Local/remote exploits, Payloads, Shells, Metasploit),, Network Penetration Testing (Wireless attacks WEP/WPA, MITM, ARP spoofing Pivoting), Web Application Penetration Testing (SQLi, Command injection, XSS,, CSRF, Session hijacking, SSRF), Post-Exploitation & Lateral Movement (Privilege escalation, Persistence, Data exfiltration).	8
5	**Reporting & Remediation** Documentation & Reporting (Structuring pentest report, Technical findings vs. executive summaries),, Remediation Strategies (Patch management, Hardening, WAF, IPS),, Verification & Retesting, Continuous monitoring, DevSecOps CI/CD integration, Incident Response Integration, Penetration testing certifications (OSCP, CEH, eCPPT),, trends (AI-based detection, automated scanning).	8
Total Hours		**45**

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Gather public information on a simulated target using OSINT techniques. Tool: Geth (Go Ethereum) – Open-source.	2
2	**Practical 2** Test DNS server misconfigurations, enumerate DNS records, and perform DNS Zone Transfer. Tools: Remix IDE – Browser-based open-source Solidity IDE.	2
3	**Practical 3** Run a web application scanner on a vulnerable test site like DVWA to identify security flaws. Tools: OWASP ZAP, Nessus, OpenVAS, DVWA.	2
4	**Practical 4** Validate automated scan results manually and identify false positives/negatives. Tools: Burp Suite, Manual browser testing, Exploit-DB.	2
5	**Practical 5** Demonstrate UI redressing (clickjacking) attack and demonstrate hidden button click exploitation. Tools: Custom HTML/JavaScript, Burp Suite.	2
6	**Practical 6** Identify and exploit privilege escalation flaws in a Linux or Windows test environment. Tools: LinPEAS, WinPEAS, Metasploit, GTFOBins.	2
7	**Practical 7** Capture and crack WPA2 handshakes in a controlled lab environment. Tool: Hyperledger Fabric – Open-source blockchain platform.	2
8	**Practical 8** Exploit SQL injection or cross-site scripting on a deliberately vulnerable web application. Tools: Burp Suite, SQLmap, DVWA, WebGoat.	2
9	**Practical 9** Move laterally within a virtual environment and set up a pivot to attack another subnet. Tools: Metasploit (route/pivot), SSH tunneling, ProxyChains.	2
10	**Practical 10** Compile findings from the above exercises into a professional-style penetration test report, including remediation steps. Tools: Word/LibreOffice Writer, CVSS calculator, DREAD/OWASP Risk Rating.	2
Total Hours		**20**

Textbook :

1 The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Dafydd Stuttard and Marcus Pinto, Kindle Store,, 2007

References:

1 Penetration Testing: A Hands-On Introduction to Hacking, Penetration Testing: A Hands-On Introduction to Hacking, Georgia Weidman, No Starch Press, 2014

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
0.00	7.00	40.00	33.00	20.00	0.00

Instructional Method:

1 The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

2 The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.

3 Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.

4 Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1 "OWASP Testing Guide" by OWASP Foundation