Semester: V

Vulnerability Assessment & Penetration Testing
Category: PROFESSIONAL CORE COURSE ELECTIVE-I
(Group-B)
(Theory)

Course Code	**:**			**CIE**	**:**	**100 Marks**
Credits: L:T:P	**:**	**3:0:0**		**SEE**	**:**	**100 Marks**
Total Hours	**:**	**45L**		**SEE Duration**	**:**	**3 Hours**

Unit-I	**09 Hrs**
Introduction to Vulnerability Assessment & Penetration Testing: Why you need to understand your enemy's tactics, recognizing the gray areas in security, Vulnerability Assessment and Penetration Testing. Penetration Testing and Tools: Social Engineering Attacks: How a social engineering attack works, conducting a social engineering attack, common attacks used in penetration testing, preparing yourself for face-to-face attacks, defending against social engineering attacks.	
Unit – II	**09 Hrs**
Physical Penetration Attacks: Why a physical penetration is important, conducting a physical penetration, Common ways into a building, Defending against physical penetrations. Insider Attacks: Conducting an insider attack, Defending against insider attacks. Metasploit: The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch Exploits, Exploiting Clients Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit.	
Unit –III	**09 Hrs**
Managing a Penetration Test: planning a penetration test, structuring a penetration test, execution of a penetration test, information sharing during a penetration test, reporting the results of a Penetration Test. Basic Linux Exploits: Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, Exploit Development Process. Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory Protections (XPSP3, Vista 7 and Server2008), By passing Windows Memory Protections.	
Unit –IV	**09 Hrs**
Web Application Security Vulnerabilities: Overview of top web application security vulnerabilities, Injection vulnerabilities, cross-Site scripting vulnerabilities, the rest of the OWASP Top Ten SQL Injection vulnerabilities, Cross-site scripting vulnerabilities. Vulnerability Analysis: Passive Analysis, Source Code Analysis, Binary Analysis.	
Unit –V	**09 Hrs**
Client-Side Browser Exploits: Why client-side vulnerabilities are interesting, Internet explorer security concepts, history of client- side exploits and latest trends, finding new browser-based vulnerabilities heap spray to exploit, protecting your self from clients side exploit. Malware Analysis: Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware.	

Course Outcomes: After completing the course, the students will be able to: -	
CO 1	Recognize and categorize different types of vulnerabilities across software, networks, and human factors.
CO 2	Demonstrate adeptness in employing various penetration testing methodologies and techniques.
CO 3	Evaluate the risk associated with identified vulnerabilities, considering severity, exploitability, and potential impact.
CO 4	Follow a systematic approach encompassing reconnaissance, scanning, exploitation, and post-exploitation phases.
CO 5	Generate detailed reports outlining discovered vulnerabilities, their severity levels, and actionable mitigation recommendations.

Reference Books	
1.	“Gray Hat Hacking: The Ethical Hackers Handbook”, Allen Harper, Stephen Sims, Michael Baucom ,3rd Edition, Tata McGraw-Hill. ISBN-10- 9390385296, 2020
2.	“The Web Application Hacker’s Handbook, Discovering and Exploiting Security flaws”, Dafydd Suttard, Marcus pinto, 2nd Edition, Wiley Publishing, ISBN-13- 978-1118026472, 2011
3.	“Penetration Testing: Hands on Introduction to Hacking”, Georgia Weidman, 1stEdition, No Starch Press, ISBN-10 : 1593275641, 2020.
4.	“The Pen Tester Blueprint Starting a Career as an Ethical Hacker”, L. Wylie, Kim Crawly, 1stEdition, Wiley Publications, ISBN-13- 978-1119684305, 2020

RUBRIC FOR THE CONTINUOUS INTERNAL EVALUATION (THEORY)		
#	**COMPONENTS**	**MARKS**
1.	**QUIZZES:** Quizzes will be conducted in online/offline mode. **TWO QUIZZES** will be conducted & Each Quiz will be evaluated for 10 Marks adding up to 20 Marks. **THE SUM OF TWO QUIZZES WILL BE CONSIDERED AS FINAL QUIZ MARKS.**	**20**