PTW ASSIGNMENT 5

Penetration Testing Workshop (CSE 3157)

Programme: B.Tech. (CSE - CYBERSECURITY) **Semester: 6th**
Last Date: 23/5/2025

Course Outcomes/ Subject Learning Outcomes	*Taxonomy Level	Question Number	Marks
Remember (kali) Linux Basic Commands, Understand Basic Concepts of Pen Test, Scripting (Python, Shell, Power shell, Ruby, Java)			
Develop Proficiency on exploitation tools Measploit, netcraft, Information gathering, DNS Reconnaissance, Searching EMail Address, Maltego, Port Scanning			
Investigate Vulnerabilities: Nmap Scripting Engine, Web Application Scanning, Manual Analysis			
Perform Pen Test on Vulnerable Machines (DC7, Kioptrix, Digital World.local, HackinOS, Sunset:Nightfall, Mumbai:1), Network traffic Capture, Burp Suite, Bypass Antivirus	L3-L5	4-5	
Perform and Evaluate Attacks: ARP Cache Poisoning, DNS Cache Poisoning, SSL Attack, Exploiting phpMyAdmin, Buffer Overflow, Password Attacks, SQL Injection, wireless attacks, social engineering toolkits			
Analysis Post Exploitation situation: Meterpreter, Create post Exploitation report, structure, objectives Export to Word, Client Side Exploitation	L3-L6	4-7	

*Bloom's taxonomy levels: Knowledge (L1), Understanding (L2), Application (L3), Analysis (L4), Evaluation (L5), Creation (L6)

1. Describe auto pawn attack and related payloads. What data can be gathered with auto pawn attack from the victim?
2. How to attach a payload with a pdf file. Mimic the target user, download pdf and run it. W rite commands and attach screenshots. Send email multiple accounts (inform your friends about it).
3. How to crack WEP passkey. Set a WEP passkey and follow the process.
4. How does WEP work? Explain the encryption and description process with Proper diagram and an example.
5. Describe a step-by-step process to crack WPA/WPA2 password.
6. (Optional) Describe the memory layout for program execution. List all the general purpose register. Show with an example diagram how functions are loaded into stack area and returned to the calling point after execution.
7. (Optional) Demonstrate memory hijacking with overflowtext.c (Refer page 365, Gergia Weidman, Penetration Testing Book)

Course outcomes (COs) satisfying program outcomes (POs) and program specific outcomes (PSOs)

POs & PSOs COs	1	2	3	4	5	6	7	8	9	10	11	12	PSO$_1$	PSO
CO 1													2	
CO 2														
CO 3														
CO 4														
CO 5														
CO 6														