CSE 3157: Penetration Testing Workshop

	ITER, SIKSHA 'O' ANUSANDHAN **(Deemed to be University)**		**LESSON PLAN**
Programme	**B.Tech.**	Academic Year	**2024-25**
Department	**Cybersecurity**	Semester	**5**
Credit	**4**	Grading Pattern	**5**
Subject Code	**CSE 3157**		
Subject Name	**Penetration Testing Workshop**		
Weekly Course Format	**0L-8P**		
Subject Coordinator (s)	**Dr. Bharat Jyoti Ranjan Sahu & Dr. Rourab Paul**		

Text Books(s):

(1) Penetration Testing with Kali Linux: Learn Hands-on Penetration Testing Using a Process-Driven Framework, Pranav Joshi, Deepayan Chanda. BPB Publications.

(2) Penetration testing A Hands-On Introduction to Hacking, Georgia Weidman, No Starch Press.

(3) Kali Linux 2: Windows Penetration Testing, Wolf Halton and Bo Weaver, PACKT Publishers.

Course Outcomes	Students will be able to	
	CO1	Remember (kali) Linux Basic Commands, Understand Basic Concepts of Pen Test, Scripting (Python, Shell, Power shell, Ruby, Java)
	CO2	Develop Proficiency on exploitation tools Measploit, netcraft, Information gathering, DNS Reconnaissance, Searching EMail Address, Maltego, Port Scanning
	CO3	Investigate Vulnerabilities: Nmap Scripting Engine, Web Application Scanning, Manual Analysis
	CO4	Perform Pen Test on Vulnerable Machines (DC7, Kioptrix, Digital World.local, HackinOS, Sunset:Nightfall, Mumbai:1), Network traffic Capture, Burp Suite, Bypass Antivirus
	CO5	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
	CO6	Analysis Post Exploitation situation: Meterpreter, Create post Exploitation report, structure, objectives Export to Word, , Client Side Exploitation

CSE 3157: Penetration Testing Workshop

Sl.No.	Lessons/Topics to be covered	Book Reference (sections)	Mapping with COs	Home Work/ Assignments/ Quizzes
1	Introduce the grading pattern, credit, classes and lab session of the course. Motivation behind the course. Introduction to Penetration Testing	Joshi Ch.1	CO1	
2	Script Writing Examples with Python, Shell	Weidman Ch 2	CO1	
3	Script Writing Examples with Power shell, Ruby, Java	Weidman Ch 2	CO1	
4	Kali Linux Basic Commands for Pen Test	Weidman Ch 3	CO1	
5	Introduction to Metasploit framework, module, payloads, types of shell, setting payload	Weidman Ch 4	CO2	Assignments 1
6	Metasploit with smb and netbios	Bo Weaver Ch. 3	CO2	
7	Metasploit Auxiliary Modules: scanner, spoof, admin, dos, fuzzers	Weidman Ch. 4	CO2	
8	Metasploit in Python Environment		CO1	Assignments 2
9	Information Gathering: netcraft, whois lookups,	Weidman Ch. 5	CO2	
10	DNS and nslookup	Weidman Ch. 5	CO2	
11	Searching for Email Address, Maltego	Weidman Ch. 5	CO2	
12	Port Scanning with nmap, python script with nmap	Weidman Ch. 5	CO5	Assignments 3
13	nmap script Engine	Weidman Ch. 6	CO3	
14	nmap script Engine in python environment		CO3	Quiz 1
15	Introduction to Nessus	Weidman Ch. 6	CO3	

CSE 3157: Penetration Testing Workshop

Sl.No.	Lessons/Topics to be covered	Book Reference (sections)	Mapping with COs	Home Work/ Assignments/ Quizzes
16	Web Application Exploitation: robot.txt. .htaccess, cross-site scripting	**Bo Weaver Ch. 4**	**CO3**	
17	Buffer Overflow & SQL Injection	**Bo Weaver Ch. 4**	**CO3**	**Assignments 4**
18	Attacking XAMPP, Manual Analysis	**Weidman Ch. 6**	**CO3**	
19	Search and Destroy with Burp Suite	**Bo Weaver Ch. 4**	**CO4**	
20	Network traffic Capture with tcpdump, wireshark, filter traffic	**Bo Weaver Ch. 5 & Weidman Ch. 7**	**CO4**	
21	Spoofing Network traffic: Ettercap	**Weidman Ch. 6**	**CO4**	
22	ARP Basic, ARP Poisoning, IP Forwarding	**Weidman Ch. 7**	**CO5**	**Quiz 2**
23	DNS Spoof, DNS Poisoning	**Weidman Ch. 7**	**CO5**	
24	SSL Basic	**Weidman Ch. 7**	**CO5**	
25	SSL Attack	**Weidman Ch. 7**	**CO4**	**Assignments 5**
26	Password Attack, xHydra	**Bo Weaver Ch. 6**	**CO5**	
27	Password & Hash	**Weidman Ch. 9**	**CO5**	

CSE 3157: Penetration Testing Workshop

Sl.No.	Lessons/Topics to be covered	Book Reference (sections)	Mapping with COs	Home Work/ Assignments/ Quizzes
28	Exploit Buffer Overflow, phpmyadmin, TFTP	**Weidman Ch. 8**	**CO5**	**Assignments 6**
29	Client Side Exploitations: Avoid metasploit script, Browser Exploitation	**Weidman Ch. 10**	**CO6**	
30	Social Engineering Tool kits	**Weidman Ch. 11**	**CO5**	
31	Social Engineering Tool kits	**Weidman Ch. 11**	**CO5**	
32	Bypass Antivirus, msfvenom, Custom Cross Compiling	**Weidman Ch. 12**	**CO4**	**Quiz 3**
33	Encryption Executable with hyperion, Python shellcode injection with veil-evasion	**Weidman Ch. 12**	**CO4**	**Assignment 7**
34	Introduction to Wireless Attack, Monitor mode, capture packets	**Weidman Ch. 15**	**CO5**	
35	Open Wireless, WEP Weakness, Cracking WEP Keys, WPA2	**Weidman Ch. 15**	**CO5**	
36	Pen Test on Vulnerable Machiines : DC7, Kioptrix	**Joshi Ch. 6**	**CO4**	
37	Pen Test on Vulnerable Machines : Digital World.local, HackinOS	**Joshi Ch. 6**	**CO4**	
38	Pen Test on Vulnerable Machines : Sunset:Nightfall, Mumbai:1	**Joshi Ch. 6**	**CO4**	
39	Post Exploitation: meterpreter,, metasploit post exploitation modules	**Weidman Ch. 13**	**CO6**	
40	Post Exploitation: mAdding Code, local information gathering etc.	**Weidman Ch. 13**	**CO6**	**Assignment 8**
41	Project	**NA**	**CO1-CO6**	**Project**
42	Project	**NA**	**CO1-CO6**	**Project**
43	Project	**NA**	**CO1-CO6**	**Project**