



SILVER OAK UNIVERSITY

School of Technology, Design and Computer Application

Silver Oak College of Computer Application

Department of Computer Application

Master of Science Cyber Security & Digital Forensics

Course Name: Practical-2(Metasploit Framework-I)

Course Code: 1040147112

Semester: 2nd

Prerequisite: Foundational Knowledge of Networking. Proficiency in Operating Systems. Understanding of Cyber security Fundamentals. Basic Programming Skills

Course Objective: The objective of the Metasploit Framework - I course is to equip students with practical skills in using Metasploit for ethical hacking, penetration testing, and vulnerability assessment. By mastering its tools and techniques, students learn to identify, exploit, and remediate security vulnerabilities, advancing their careers in cyber security.

Teaching Scheme:

Teaching Scheme				
L	T	P	Contact Hours	Credit
0	0	8	8	4

List of Experiments:

Total Hours:112

Sr. No.	Practicals Name
1.	Install Metasploit on both Windows and Linux operating systems.
2.	Perform protocol enumeration, password sniffing, and reconnaissance using Metasploit tools.
3.	Conduct host discovery and enumeration of various protocols such as SMB, SSH, FTP, SMTP, SNMP, HTTP, and WinRM.
4.	Learn the basics of Meterpreter, including core commands and file system operations.
5.	Use Meterpreter to dump password hashes and crack them using tools like John the Ripper.
6.	Execute shell commands through Meterpreter for system interaction and manipulation.
7.	Practice various methods to escalate privileges on compromised systems using Meterpreter.
8.	Perform exploitation using Metasploit modules and explore post-exploitation activities like lateral movement and data exfiltration.
9.	Learn how to document findings, generate reports, and effectively communicate results in penetration testing reports.
10.	Use Metasploit to scan for open ports and services on your local network

11.	Set up vulnerable applications on your computer and use Metasploit to exploit them, demonstrating real-world vulnerability exploitation.
12.	Hands-on experience with an exploit module.
13.	Exploitation Techniques and Payload Handling.
14.	Case Study on Penetration Testing.

Course Outcomes:

Sr. No.	CO-Statement
CO-1	Describe the importance of penetration testing and differentiate between vulnerability assessment and penetration testing.
CO-2	Utilize Metasploit components effectively by identifying their anatomy, structure, and understanding the functionalities of MSFconsole and variables within Metasploit.
CO-3	Evaluate different methods of information gathering such as passive and active techniques,
CO-4	Demonstrate competency in effectively utilizing various Metasploit modules for vulnerability scanning, exploitation.

Major Equipment:

1. Computer System
2. LAN cable

Teaching & Learning Methodology: -

1. Projector and Computer
2. Experiments shall be performed in the laboratory related to course contents

Books Recommended:

1. Metasploit Penetration Testing Cookbook-Packt Publishing
2. Metasploit Revealed _ Secrets of the Expert Pentester - Build your Defense against Complex Attacks-Packt Publishing

CO-PO-PSO MATRIX:

Co. No	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2
CO-1	3	2	1	2		1		1	3
CO-2	2	2	2	1				2	2
CO-3	2	3	3	2				2	2
CO-4	3	2	1	2				2	2