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: Metasploit Framework -I
Course Code: 1040147110
Semester: 2nd

Prerequisite: Foundational Knowledge of Networking**,** Proficiency in Operating Systems**,** Understanding of Cybersecurity Fundamentals**,** Basic Programming Skills**,** Experience with Virtualization

Course Objective: The objective of the Metasploit Framework -I course is to provide students with a comprehensive understanding and practical skills in utilizing Metasploit for ethical hacking, penetration testing, and vulnerability assessment. By exploring Metasploit's architecture, modules, and exploit techniques, students will learn to identify, exploit, and remediate security vulnerabilities while adhering to ethical and legal standards. Mastery of Metasploit's capabilities will enable students to contribute to cybersecurity efforts, improve incident response readiness, and pursue advanced certifications, thereby advancing their careers in cybersecurity.

Teaching Scheme:

Teaching Scheme				
L	T	P	Contact Hours	Credit
3	1	0	4	4

Content:

Unit No.	Course Contents	Teaching Hours	% Weightage
1	**Introduction to Metasploit:** Importance of Penetration Testing, Vulnerability Assessment vs Penetration Testing, the need for a penetration testing framework, Installing Metasploit on Windows, Installing Metasploit on Linux	10	24
2	**Metasploit Components:** Anatomy and Structure of Metasploit, Metasploit Components, Understanding the MSF console, Variables in Metasploit	10	24
3	**Information Gathering with Metasploit:** Enumerating protocols, Password sniffing, Advanced recon with Shodan, Passive Info. gathering & Active info. Gathering, Port scanning, The Nmap way	12	28

4	**Understanding Modules:** Types of Metasploit modules: Exploits, Payloads, Auxiliary, Encoders, Nops, and Post-exploitation modules. Structure and components of a Metasploit module. Module Search and Use, Searching for modules. Detailed walkthrough of using an exploit module. Selecting and configuring payloads. Exploitation Process.Information Gathering, Using auxiliary modules for scanning and enumeration.Integrating with external tools (Nmap, Nessus).Vulnerability scanning. Scanning for vulnerabilities using Metasploit.Understanding scan results and identifying exploitable targets.Exploitation Techniques Setting up and running exploits.Handling different types of payloads (bind, reverse, meterpreter).	10	24

Course Outcomes:

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

Teaching & Learning Methodology: -

1. Lectures with live practical example using Projector and Computer
2. Experiments shall be performed in the laboratory related to course contents

List of Tutorials: **Total Hours: 14**

Sr. No.	Tutorials Name
1.	Configuring and launching Msfconsole for Metasploit Framework.
2.	Learn to enumerate and exploit FTP and SSH services.
3.	Create custom payloads using Msfvenom in Metasploit.
4.	Exploiting Android devices using Msfvenom-generated payloads.
5.	A technique for bypassing UAC and using Metasploit’s macro exploits.
6.	Exploiting a Windows 11, Social engineering with Metasploit
7.	Conduct a simulated penetration test using Metasploit to identify vulnerabilities in a mock industrial control system environment.
8.	Utilize Metasploit to exploit known vulnerabilities in a controlled lab environment, demonstrating

	practical understanding of penetration testing techniques.

Major Equipment:

1. Computer System
2. LAN cable

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