COURSE TITLE	**METASPLOIT FRAMEWORK**
COURSE CODE	**01CC0605**
COURSE CREDITS	**3**

Objective:

1 Students can gain knowledge of the Metasploit Framework and explore different security aspects of Vulnerability Assessment and Penetration Testing (VAPT) and its relevant domains, understand different domains of red teaming, explore different attacking methods used in red teaming security, and gain knowledge of different security tools and techniques of penetration testing.

Course Outcomes: After completion of this course, student will be able to:

1 Apply Metasploit Framework tools and modules for reconnaissance, scanning, and vulnerability assessment.

2 Perform exploitation and post-exploitation activities using Meterpreter and other Metasploit components.

3 Analyze system vulnerabilities, attack vectors, and penetration testing results in controlled environments.

4 Evaluate exploitation techniques and defensive mechanisms to assess system security.

5 Design and develop customized exploits and penetration testing workflows using the Metasploit Framework.

Pre-requisite of course: Cybersecurity Fundamentals. Basic Networking Knowledge. Ethical and Legal Awareness.

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
2	0	2	50	30	20	25	25

Contents : Unit	Topics	Contact Hours
1	**Introduction to Metasploit** Importance of Penetration Testing, Vulnerability Assessment vs Penetration, Testing, the need for a penetration testing framework, Installing Metasploit on Windows & Linux	6
2	**Metasploit Components** Anatomy and Structure of Metasploit, Graphical Structure of MSF, Libraries, Interfaces, Metasploit Components, Auxiliaries, Exploits, Encoders, Payloads, Post, Nops, Understanding the MSFconsole, Variables in Metasploit (LHOST, LPORT, RHOST, RPORT)	6

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
3	**Information Gathering with Metasploit** Enumerating protocols, Password sniffing, Advanced recon with Shodan, Passive Info. gathering, Active info. gathering, 5 Port scanning- The Nmap way, Host discovery with ARP Sweep, UDP Service Sweeper, SMB scanning and enumeration, Detecting SSH versions, FTP scanning, SMTP enumeration, SNMP Enumeration, HTTP Scanning, WinRM scanning and brute forcing.	6
4	**Meterpreter-1** What is Meterpreter?, Meterpreter core commands, Meterpreter file system commands, Meterpreter networking commands, Meterpreter system commands, Dumping the Hashes and cracking with JTR (John the ripper), Shell command, Privilege escalation, MSF VENOM	7
5	**Post-Exploitation** Privilege escalation, Metasploit Macro Exploits, Exploiting a Windows machine, Social engineering with Metasploit, Browser Auto pwn	7
Total Hours		**32**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Study the architecture and different modules of the Metasploit Framework to understand its working mechanism in Kali Linux. Gain familiarity with various module types such as exploits, payloads, auxiliary, and post modules used in penetration testing.	2
2	**Practical 2** Perform protocol enumeration using Metasploit integrated with Nmap. Analyze the identified services and protocols to determine potential vulnerabilities in the target system.	2
3	**Practical 3** Perform network scanning using Metasploit with Nmap. Identify live hosts and open ports within a network to understand the attack surface.	2
4	**Practical 4** Gather information about a target website using Metasploit modules and Nmap. Analyze server details, technologies, and possible entry points for further assessment.	2
5	**Practical 5** Perform SMB scanning and enumeration using Metasploit. Identify shared resources, system information, and possible misconfigurations in SMB services.	2

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
6	**Practical 6** Perform privilege escalation using Metasploit modules. Analyze system weaknesses that allow elevation of access rights after initial compromise.	2
7	**Practical 7** Demonstrate exploitation of a target system using a malicious PDF generated through Metasploit. Understand how file-based payload delivery can be used to gain access in a controlled environment.	2
8	**Practical 8** Identify FTP-related vulnerabilities and exploit the target system using Metasploit. Evaluate weak configurations and outdated services that can be leveraged during exploitation.	2
9	**Practical 9** Exploit a target system using msfvenom and Meterpreter to establish a reverse TCP connection. Understand the process of payload generation, delivery, and session handling for remote access in a controlled environment.	2
10	**Practical 10** Perform WinRM scanning and brute-force attacks using Metasploit. Analyze authentication mechanisms and identify weaknesses such as poor credential management in remote access services.	2
Total Hours		**20**

Textbook :

1 Metasploit Penetration Testing Cookbook, Abhinav singh, Packt Publishing, 2012

References:

1 Metasploit Revealed _ Secrets of the Expert Pentester - Build your Defense against Complex Attacks, Metasploit Revealed _ Secrets of the Expert Pentester - Build your Defense against Complex Attacks, -, Packt Publishing, -

2 Introduction to Network Security, Introduction to Network Security, Neal Krawetz, CENGAGE Learning, 2007

3 Metasploit: The Penetration Tester's Guide, Metasploit: The Penetration Tester's Guide, David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni., Kindle Store, 2011

Suggested Theory Distribution:

The suggested theory distribution as per Bloom’s taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery

Remember / Knowledge	Understand	Apply	Analyze	Evaluate	Higher order Thinking / Creative
0.00	5.00	25.00	30.00	20.00	20.00

Instructional Method:

1. The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.
2. The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.
3. Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.
4. Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1. “Advanced Penetration Testing: Hacking the World's Most Secure Networks” by Wil Allsopp
2. “Mastering Metasploit” by Nipun Jaswal

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)