**SILVER OAK UNIVERSITY**
**Silver Oak College of Computer Application**
**Master of Science Cyber Security & Digital Forensics**
**Course Name: Metasploit Framework -II**
**Course Code: 1040147236**
**Semester: 3rd**

**Prerequisite:** A foundational understanding of networking concepts, TCP/IP protocols, and operating systems (Linux and Windows), along with basic command-line proficiency

**Course Objective:** The Metasploit Framework (MSF) contains a collection of exploits. It's an infrastructure that one can build upon and utilize for one's custom needs. The goal is to teach you an advanced level of practical penetration testing.

**Teaching Scheme:**

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

**Contents:**

| Unit No. | Course Contents | Teaching Hours | % Weightage |
|---|---|---|---|
| 1 | **Meterpreter-2:** Setting up multiple communication channels with the target, Meterpreter anti-forensics, the get-desktop and keystroke sniffing, Meterpreter resource scripts, Meterpreter timeout control, Meterpreter Sleep Control, Meterpreter transports, Interacting with the registry, Meterpreter API and mixings, Injecting VNC server remotely, Enabling remote Desktop | 10 | 24 |
| 2 | **Server-Side Exploitation:** Exploiting a Linux server, exploiting a Windows machine, Exploiting Common services, Enabling remote Desktop | 10 | 24 |
| 3 | **Client-Side Exploitation**: Bypassing antivirus and IDS/IPS, Human interface device attacks, HTA attack, Backdooring executables using a MITM attack, Creating a Linux trojan, File format based Exploitation-PDF and Word, Creating an Android backdoor. | 11 | 26 |
| 4 | **Wireless Network penetration Testing:** Metasploit and wireless, understanding an evil twin attack, Configuring metasploit, Wireless MITM attacks, SMB relay attacks | 6 | 14 |

| | | | |
|---|---|---|---|
| 5 | **Advanced Post-Exploitation Techniques for Maintaining Access** Persistence mechanisms and techniques, Advanced pivoting and lateral movement, Data exfiltration and stealth, Advanced Exploitation Scenarios and Evasion Techniques, Bypassing advanced security mechanisms (ASLR, DEP, etc.), Exploiting zero-day vulnerabilities,Evasion techniques against modern defensive tools and technologies | 5 | 12 |

**Course Outcomes:**

| Sr. No. | CO-Statement | Unit No |
|---|---|---|
| CO-1 | Demonstrate proficiency in applying advanced penetration techniques utilizing Meterpreter, showcasing synthesis, analysis, and evaluation skills. | 1 |
| CO-2 | Execute server-side exploits on both Linux and Windows servers with adeptness, exemplifying application and analysis capabilities. | 2 |
| CO-3 | Effectively employ client-side exploits to circumvent defenses, highlighting synthesis and application prowess.. | 3 |
| CO-4 | Conduct comprehensive wireless network penetration tests, integrating knowledge and displaying adept evaluation skills.. | 4 |
| CO-5 | Apply critical analysis to persistence mechanisms, advanced pivoting, lateral movement, data exfiltration, and stealth techniques. | 5 |

**Teaching & Learning Methodology:**

1. Competency-based Learning
2. Cooperative-based Learning
3. Problem - based Learning
4. Design Thinking

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

| Sr. No. | Tutorial Name |
|---|---|
| 1 | Meterpreter anti-forensics |
| 2 | The getdesktop and keystroke sniffing |
| 3 | Interacting with the registry |
| 4 | Meterpreter API and mixins |
| 5 | Injecting VNC server remotely |
| 6 | Enabling remote Desktop |
| 7 | Exploiting a Linux server |
| 8 | Exploiting a Windows machine |
| 9 | Exploiting Common services |
| 10 | Bypassing antivirus and IDS/IPS |
| 11 | Exploiting web applications and misconfigured services |

**Books Recommended:**


1. Moore H. D., “Metasploit Penetration Testing Cookbook”, Packet Publishing
2. Sagar Rahalkar, Nipun Jaswal, “Metasploit Revealed Secrets of the Expert Pentester-Build your Defense against Complex Attacks”, Packet Publishing


**CO-PO-PSO Matrix:**

| Co. No. | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PSO1 | PSO2 |
|---|---|---|---|---|---|---|---|---|---|
| CO-1 | 3 | 2 | 1 | 1 | 1 | | | 1 | 2 |
| CO-2 | 1 | 2 | 3 | 2 | 1 | | | 3 | 2 |
| CO-3 | 1 | 2 | | 3 | | | | 1 | 3 |
| CO-4 | 2 | 3 | 2 | 1 | | 1 | | 2 | 2 |
| CO-5 | 2 | 1 | 2 | 1 | | | | 1 | 2 |