

SILVER OAK UNIVERSITY									
Program	BTech				Branch/Spec.	Cyber Security			
Semester	III				Version	1			
Effective from Academic Year			2020 - 21		Effective for the batch Admitted in			June 2020	
Subject code	CSF302		Subject Name		Basics of Metasploit Framework				
Teaching scheme					Examination scheme (Marks)				
(Per week)	Lecture(DT)		Practical(Lab.)		Total		Internal	External	Practical
	L	TU	P	TW		Marks	30	70	50
Credit	4	0	1	0	5	Total			150
Hours	4	0	2	0	6				
Theory syllabus									
Unit	Content								Hrs
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
2	Metasploit Components: Anatomy and Structure of Metasploit, Metasploit Components, Understanding the MSFconsole, Variables in Metasploit								10
3	Information Gathering with Metasploit: Enumerating protocols, Password sniffing, Advanced recon with Shodan, Passive Info. Gathering, Active info. Gathering, 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								12
4	Meterpreter-1 and Client Side Exploitation-1: 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, Need of client side attacks, the msfvenom utility, Metasploit macro Exploits, Exploiting a Windows, machine, Social engineering with Metasploit, Browser Autopwn.								8