Course Code	**Course Title**	**Credits**	**Lectures /Week**
USCSP6042	**Ethical Hacking - Practical**	**1**	**3**
1	Google and Whois Reconnaissance • Use Google search techniques to gather information about a specific target or organization. • Utilize advanced search operators to refine search results and access hidden information. • Perform Whois lookups to retrieve domain registration information and gather details about the target's infrastructure.		
2	Password Encryption and Cracking with CrypTool and Cain and Abel • Password Encryption and Decryption: o Use CrypTool to encrypt passwords using the RC4 algorithm. o Decrypt the encrypted passwords and verify the original values. • Password Cracking and Wireless Network Password Decoding: o Use Cain and Abel to perform a dictionary attack on Windows account passwords. o Decode wireless network passwords using Cain and Abel's capabilities.		
3	Linux Network Analysis and ARP Poisoning • Linux Network Analysis: o Execute the ifconfig command to retrieve network interface information. o Use the ping command to test network connectivity and analyze the output. o Analyze the netstat command output to view active network connections. o Perform a traceroute to trace the route packets take to reach a target host. • ARP Poisoning: o Use ARP poisoning techniques to redirect network traffic on a Windows system. o Analyze the effects of ARP poisoning on network communication and security.		
4	Port Scanning with NMap • Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open. • Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their characteristics. • Analyze the scan results to gather information about the target system's network services.		
5	Network Traffic Capture and DoS Attack with Wireshark and Nemesy • Network Traffic Capture: o Use Wireshark to capture network traffic on a specific network interface. o Analyze the captured packets to extract relevant information and identify potential security issues.		

	• Denial of Service (DoS) Attack: o Use Nemesy to launch a DoS attack against a target system or network. o Observe the impact of the attack on the target's availability and performance.
6	Persistent Cross-Site Scripting Attack • Set up a vulnerable web application that is susceptible to persistent XSS attacks. • Craft a malicious script to exploit the XSS vulnerability and execute arbitrary code. • Observe the consequences of the attack and understand the potential risks associated with XSS vulnerabilities.
7	Session Impersonation with Firefox and Tamper Data • Install and configure the Tamper Data add-on in Firefox. • Intercept and modify HTTP requests to impersonate a user's session. • Understand the impact of session impersonation and the importance of session management.
8	SQL Injection Attack • Identify a web application vulnerable to SQL injection. • Craft and execute SQL injection queries to exploit the vulnerability. • Extract sensitive information or manipulate the database through the SQL injection attack.
9	Creating a Keylogger with Python • Write a Python script that captures and logs keystrokes from a target system. • Execute the keylogger script and observe the logged keystrokes. • Understand the potential security risks associated with keyloggers and the importance of protecting against them.
10	Exploiting with Metasploit (Kali Linux) • Identify a vulnerable system and exploit it using Metasploit modules. • Gain unauthorized access to the target system and execute commands or extract information. • Understand the ethical considerations and legal implications of using Metasploit for penetration testing.