Course Code	Course Title	Credits	Lectures /Week
USCS6042	**Ethical Hacking**	**2**	**3**

About the Course: This course provides an in-depth exploration of ethical hacking and penetration testing methodologies. Students will learn about hacking technology types, the phases of ethical hacking, footprinting, social engineering, system hacking, web server and application vulnerabilities, wireless hacking, and more. The course emphasizes hands-on lab exercises and real-world scenarios to develop practical skills in identifying and mitigating security vulnerabilities.

Course Objectives:

- Understand the terminology and concepts related to ethical hacking and penetration testing.
- Explore various hacking technologies and the skills required to become an ethical hacker.
- Learn the different phases involved in ethical hacking and the methodologies used in penetration testing.
- Gain knowledge of common hacking techniques, such as footprinting, scanning, enumeration, and session hijacking.
- Develop proficiency in identifying and exploiting vulnerabilities in web servers, web applications, and wireless networks.

Learning Outcomes:

After successful completion of this course, students would be able to

- Apply ethical hacking methodologies to conduct comprehensive security assessments and penetration tests.
- Perform effective footprinting and reconnaissance techniques to gather critical information about target systems.
- Identify and exploit vulnerabilities in various network and system components using appropriate tools and techniques.
- Evaluate the security posture of web servers, web applications, and wireless networks, and recommend appropriate countermeasures.
- Demonstrate an understanding of ethical and legal considerations in conducting ethical hacking activities and adhere to professional codes of conduct.

Unit	Topics	No of Lectures
I	**Introduction:** Terminology, Hacking Technology Types, Ethical Hacking Phases, Hacktivism, Hacker Classes, Skills Required for an Ethical Hacker, Vulnerability Research, Ways to Conduct Ethical Hacking **Footprinting:** Definition, Information Gathering Methodology, Competitive Intelligence, DNS Enumeration, Whois and ARIN Lookups, Types of DNS Records, Traceroute in Footprinting, E-Mail Tracking **Social Engineering:** Common Types Of Attacks **Scanning and Enumeration:** Port Scanning, Network Scanning, Vulnerability Scanning, CEH Scanning Methodology, Ping Sweep Techniques, Nmap Command Switches, SYN, Stealth, XMAS, NULL,	**15**

	IDLE, FIN Scans, Anonymizers, HTTP Tunneling Techniques, IP Spoofing Techniques, SNMP Enumeration, Steps Involved in Enumeration	
II	**System Hacking:** Password-Cracking Techniques, Types of Passwords, Keyloggers and Other Spyware Technologies, Escalating Privileges, Rootkits **Sniffers:** Protocols Susceptible to Sniffing, Active and Passive Sniffing, ARP Poisoning, MAC Flooding, DNS Spoofing Techniques, Sniffing Countermeasures **Denial of Service:** Types of DoS Attacks, Working of DoS Attacks, BOTs/BOTNETs, "Smurf" Attack, "SYN" Flooding, DoS/DDoS Countermeasures **Session Hijacking:** Spoofing vs. Hijacking, Types, Sequence Prediction, Steps, Prevention **Hacking Web Servers:** Web Server Vulnerabilities, Attacks against Web Servers, Patch Management Techniques, Web Server Hardening	**15**
III	**Web Application Vulnerabilities:** Web Application Hacking, Web Application Threats, Google Hacking, Countermeasures **Web-Based Password Cracking Techniques:** Authentication Types, Password Crackers, Countermeasures **SQL Injection:** Steps, SQL Server Vulnerabilities, Countermeasures **Buffer Overflows:** Types, Stack-Based Buffer Overflows, Mutation Techniques **Wireless Hacking:** WEP, WPA Authentication Mechanisms, and Cracking Techniques, Wireless Sniffers, Rogue Access Points, Wireless Hacking Techniques, Securing Wireless Networks **Penetration Testing Methodologies:** Methodologies, Steps, Automated Tools, Pen-Test Deliverables	**15**

Textbook(s):

1. CEH official Certfied Ethical Hacking Review Guide, Wiley India Edition

Additional Reference(s):

1. Certified Ethical Hacker: Michael Gregg, Pearson Education
2. Certified Ethical Hacker: Matt Walker, TMH.