Branch: B.Sc.(IT)	Semester-VI
Subject Code: 6103	Lecture: 04 Credit: 04
Course Opted	Core Course -20
Subject Title	ETHICAL HACKING

Course Objectives:

- To learn system hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities.
- To learn about different types of malwares (Trojan, Virus, worms, etc.), system auditing for malware attacks, malware analysis, and countermeasures.
- Learning Packet sniffing techniques to discover network vulnerabilities and countermeasures to defend sniffing. Social engineering techniques and how to identify theft attacks to audit human level vulnerabilities and suggest social engineering countermeasures.
- To learn DoS/DDoS attack techniques and tools to audit a target and DoS/DdoS countermeasures.
- To learn Session hijacking techniques to discover network-level session management, authentication/authorization, cryptographic weaknesses, and countermeasures.
- To learn about Web server attacks and a comprehensive attack methodology to audit vulnerabilities in web server infrastructure, and countermeasures.

Course Outcomes:

- Better understanding of pitfalls in network & system security.
- Testing network security and its various entities by attacking the target network.
- Network security engineers capable of dealing with real world security threats.

Modules	Sr. No.	Topic and Details	No of Lectures Assigned	Marks Weightage %
UNIT - I	1	**Introduction to Ethical Hacking, Ethics, and Legality:** Defining Ethical Hacking, Understanding the Purpose of Ethical Hacking, An Ethical Hacker's Skill Set Ethical Hacking Terminology, The Phases of Ethical Hacking, Identifying Types of Hacking Technologies Identifying Types of Ethical Hacks, Understanding Testing Types, How to Be Ethical, Performing a Penetration Test	2	5
	2	**Gathering Target Information: Reconnaissance, Footprinting, and Social Engineering:** Reconnaissance, Understanding Competitive Intelligence, Information-Gathering Methodology, Footprinting Using Google to Gather Information, Understanding DNS Enumeration, Understanding Whois and ARIN Lookups, Identifying Types of DNS Records, Using Traceroute in Footprinting, Understanding Email Tracking, Understanding Web	3	5

		Spiders, Social Engineering, The Art of Manipulation, Types of Social Engineering-Attacks, Social-Engineering Countermeasures		
	3	**Gathering Network and Host Information: Scanning and Enumeration:** Scanning, Scanning Methodology, Ping Sweep Techniques, nmap Command Switches, Scan Types, TCP Communication Flag Types, War-Dialing Techniques, Banner Grabbing and OS Fingerprinting Techniques, Scanning Anonymously, Enumeration, Null Sessions, SNMP Enumeration, Windows 2000 DNS Zone Transfer	3	5
	4	**System Hacking: Password Cracking, Escalating Privileges, and Hiding Files:** The Simplest Way to Get a Password, Types of Passwords, Passive Online Attacks, Active Online Attacks, Offline Attacks, Nonelectronic Attacks, Cracking a Password, Understanding the LAN Manager Hash Cracking Windows 2000 Passwords, Redirecting the SMB Logon to the Attacker, SMB Relay MITM Attacks and Countermeasures, NetBIOS DoS Attacks, Password-Cracking Countermeasures Understanding Keyloggers and Other Spyware Technologies, Escalating Privileges, Executing Applications. Buffer Overflows, Understanding Rootkits, Planting Rootkits on Windows 2000 and XP Machines, Rootkit Embedded TCP/IP Stack, Rootkit Countermeasures, Hiding Files, NTFS File Streaming, NTFS Stream Countermeasures, Understanding Steganography Technologies, Covering Your Tracks and Erasing Evidence	5	10
UNIT - II	5	**Trojans, Backdoors, Viruses, and Worms:** Trojans, Backdoors, Viruses, and Worms, Trojans and Backdoors, Overt and Covert Channels, Types of Trojans, How Reverse-Connecting Trojans Work, How the Netcat Trojan Works, Trojan Construction Kit and Trojan Makers, Trojan Countermeasures, Checking a System with System File Verification, Viruses and Worms, Types of Viruses, Virus Detection Methods	3	6
	6	**Gathering Data from Networks: Sniffers:** Understanding Host-to-Host Communication, How a Sniffer Works, Sniffing Countermeasures, Bypassing the Limitations of Switches, How ARP Works, ARP Spoofing and Poisoning Countermeasures, Wireshark Filters, Understanding MAC Flooding and DNS Spoofing	2	4
	7	**Denial of Service and Session Hijacking:** Denial of Service and Session Hijacking, Denial of Service, How DDoS Attacks Work, How BOTs/BOTNETs Work, Smurf and SYN Flood Attacks, DoS/DDoS Countermeasures, Session Hijacking, Sequence prediction, Dangers Posed by Session Hijacking, Preventing Session Hijacking	2	5

	8	**Web Hacking: Google, Web Servers, Web Application Vulnerabilities, and Web-Based Password Cracking Techniques:** How Web Servers Work, Types of Web Server Vulnerabilities, Attacking a Web Server, Patch-Management Techniques, Web Server Hardening Methods, Web Application Vulnerabilities, Web Application Threats and Countermeasures, Google Hacking, Web-Based Password-Cracking Techniques, Authentication Types, Password Attacks and Password Cracking	5	10
UNIT - III	9	**Attacking Applications: SQL Injection and Buffer Overflows:** SQL Injection, Finding a SQL Injection Vulnerability, The Purpose of SQL Injection, SQL Injection Using Dynamic Strings, SQL Injection Countermeasures, Buffer Overflows, Types of Buffer Overflows and Methods of Detection, Buffer Overflow Countermeasures	5	10
	10	**Wireless Network Hacking:** Wi-Fi and Ethernet, Authentication and Cracking Techniques, Using Wireless Sniffers to Locate SSIDs, MAC Filters and MAC Spoofing, Rogue Access Points, Evil Twin or AP Masquerading, Wireless Hacking Techniques, Securing Wireless Networks	5	10
	11	**Physical Site Security:** Components of Physical Security, Understanding Physical Security, Physical Site Security Countermeasures, What to Do After a Security Breach Occurs	2	5
	12	**Hacking Linux Systems:** Compiling a Linux Kernel, GCC Compilation Commands, Installing Linux Kernel Modules Linux Hardening Methods	3	5
UNIT - IV	13	**Bypassing Network Security: Evading IDSs, Honeypots, and Firewalls:** Types of IDSs and Evasion Techniques, Firewall Types and Honeypot Evasion Techniques	2	5
	14	**Cryptography:** Cryptography and Encryption Techniques, Types of Encryption, Stream Ciphers vs. Block Ciphers, Generating Public and Private Keys, Other Uses for Encryption, Cryptography Algorithms, Cryptography Attacks.	3	5
	15	**Performing a Penetration Test:** Defining Security Assessments, Penetration Testing, Penetration Testing Steps, The Pen Test Legal Framework, Automated Penetration Testing Tools, Pen Test Deliverables	5	10
		TOTAL	**50**	**100**

Text Book:

1. CEH Certified Ethical Hacker Study Guide by Kimberly Graves (Wiley)2010.

Reference Books:

1. Hacking: The Art of Exploitation, 2nd Edition, by Jon Erickson

2. Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman
3. Hacking: 4 Books in 1- Hacking for Beginners, Hacker Basic Security, Networking Hacking, Kali Linux for Hackers by Erickson Karnel and CODING HOOD,2019
4. Learn Ethical Hacking from Scratch: Your stepping stone to penetration testing by Zaid Sabih,2018 Packt Publishing Limited
5. Atul Kahate, Cryptography and Network Security, McGraw Hill
6. Kaufman, C., Perlman, R.,& Speciner, M., .Network Security, Private Communication in a Public world, 2nd ed., Prentice Hall PTR, 2002
7. Stallings, W., .Cryptography and Network Security: Principles and Practice, 3rd ed., Prentice Hall PTR., 2003
8. Stallings, W., .Network Security Essentials: Applications and Standards, Prentice Hall, 2000