ELECTIVE-3

ETHICAL HACKING & PENTRATION TESTING

Subject Code: CS34321CS	Subject Type: Elective
Evaluation Scheme: MSE(30), TA(20), ESE(50)	L-T-P: 3-0-0

Pre-Requisites: Computer Networks, Operating System, and Programming

Course Objective: To enable students to be part of such a team that can conduct the security assessment of an organization through the process of ethical hacking. This course will introduce the students, the idea of security assessment of systems and networks under investigation and how to perform them under the legal and ethical framework.

Course Outcomes: At the end of the course, the student will be able to

CO-1	Understand the basic concepts of network, host, services and vulnerability gathering techniques employed by an attacker.
CO-2	Apply tools for network footprinting including stealth scanning.
CO-3	Analyze system installations for vulnerabilities that could be exploited by an adversary.
CO-4	Design secure system installations that can withstand adversarial attacks.
CO-5	Extend existing tools for network and systems protection.

Course Articulation Matrix:

CO/PO	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	3	2	2	2	3	2
CO-2	3	3	3	3	3	3
CO-3	3	3	3	2	3	2
CO-4	3	2	2	1	2	1
CO-5	3	3	2	1	3	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Unit-1: Network & Security Foundations

Review of Network Fundamentals, Network Topologies, Network Components, TCP/IP Networking Basics, TCP/IP Protocol Stack (DNS, SNMP, TCP, UDP, IP, ARP, RARP, ICMP), Ethernet, Subnet Masking, Subnetting, Supernetting, Security Basics (Attributes, Mechanisms, Attack Taxonomy), CIA Triad, Threats, Vulnerabilities, Attacks

Unit-2: Intelligence Gathering & Footprinting

Intelligence Gathering (Learning about target business, organizational structure, business partners, company names, partner organizations, DNS names, servers), Search engines, Financial databases, Business reports, WHOIS, RWHOIS, Domain name registries and registrars, Web archives, Cloud reconnaissance, Active & Passive Footprinting, Network and system footprinting, Tools for network footprinting, Mining DNS host names and IP addresses, Firewall mapping, Social media reconnaissance, Social engineering, archive.org, Neo trace, DNS Footprinting, whois databases, ping, port scanners, Email footprinting, Email tracking, Google hacking (Google dorks), Traceroute, Verification of collected information, Countermeasures against footprinting

Unit-3: Scanning, Enumeration & Vulnerability Assessment

Scanning (goals, types, sniffing with tcpdump, network tracing, port scanning, OS fingerprinting, version scanning, identifying open ports), Nmap, ping, Angry IP, Masscan, Friendly Pinger, Nikto, Netsparker, WPScan, Eyewitness, ZAP, BurpSuite, OpenVAS, Nessus, Nexpose, Qualys, HCL AppScan, Stealth scanning (scanning beyond an IDS), Network diagram generation (Network Topology Mapper, OpManager, LANState), Proxy servers, TOR network, HTTP tunneling, SSH tunneling, Anonymizers, Enumeration (extracting usernames via email IDs, SNMP, Windows user groups, DNS zone transfer), Default passwords, SuperScan, Route Analysis Tools, SNMP Enumeration, Mitigation of reconnaissance attacks

Unit-4: Exploitation & Post-Exploitation

Network based exploitation using Metasploit (compromising vulnerable systems, pivoting, pilfering), Detection of IP Spoofing, Common web vulnerabilities (Cross-site scripting, OS and command injection, Buffer overflows, SQL injection, race conditions, OWASP Top 25), SQLMap, Password attacks and management, Exploitation techniques, Post-exploitation concepts (pivoting, lateral movement), Reporting and remediation

Learning Resources:

Text and Reference Books:

1. Slavio, John. Hacking: A Beginners' Guide to Computer Hacking, Basic Security, and Penetration Testing. CreateSpace Independent Publishing Platform, 2016.
2. Diogenes, Yuri, and Dr. Erdal Ozkaya. Cybersecurity – Attack and Defense Strategies: Counter Modern Threats and Employ State-of-the-Art Tools and Techniques to Protect Your Organization Against Cybercriminals, 2nd Edition. Packt Publishing, 2019.
3. Alassouli, Hidaia Mahmood. Footprinting, Reconnaissance, Scanning and Enumeration Techniques of Computer Networks. Blurb Publishers, 2020.
4. Shimonski, Robert. Cyber Reconnaissance, Surveillance and Defense, 1st Edition. Syngress, 2014.
5. Sikorski, Michael, and Andrew Honig. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press, 2012.