NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	B.Tech. Computer Science and Engineering
Course Code:	2CSDE87
Course Title:	Ethical Hacking and Vulnerability Assessment
Course Type:	Departmental Elective
Year of Introduction:	2021-22

Credit Scheme

L	T	Practical Component				C
		LPW	PW	W	S	
2	0	2	-	-	-	3

Course Learning Outcomes (CLO):

At the end of the course, students will be able to –

1. summarize the core concepts related to malware, hardware and software vulnerabilities and their causes
2. choose state-of-the-art tools to exploit the vulnerabilities related to computer system and networks
3. experiment with various tools to exploit web applications
4. solve the security issues in web applications

Syllabus: **Total Teaching hours: 30**

Unit	Syllabus	Teaching hours
Unit-I	**Working of Hackers:** Invading PCs, Script Kiddies, Working of Personal Hacker Protection **Working of Spyware and Antispyware:** Introduction to Spywares, Detection Escapism, Invading Privacy, Hijacking home page and search pages, working of dialers, working of keyloggers and rootkits, following spyware money trail, working of anti-spyware **Websites and privacy:** Working of Cookies, Web bugs, Websites, Websites building personal profiles **Dangers of Internet Search:** Working of Google, Individual Know-how	05
Unit-II	**Wi-Fi security dangers and protections:** Working of Wi-Fi, Invading Wi-Fi Networks, hotspots, Evil Twin Hacks and Protections **Working of Spam**: Dangers of spam, Hiding identity and identification, Working 1of Anti-spam software **Denial of Service** Attacks and Protection Virtual Private Networks, Web Blocking and Parental Controls,	05

	Personal Firewalls and Proxies SQL Injection, SQL Injection, sim spoofing, ATM card skimmers, eSIMS	
Unit-III	**Phishing Attacks**: Working of Phishing, following phishing money trail, protection against phishing attacks **Zombies and Trojan Horses**: Working of Zombies and Bot Networks, Working of Trojan Horses, Zombie Money Trail, Working of Zombie and Trojan Protection **Security Dangers in Browsers**: Hackers exploit Networks, Protection against browser based attacks **Worms and viruses**: Working of viruses and worms, antivirus software	06
Unit-IV	**Vulnerability assessment**: Nessus, OpenVAS, Nexpose, web application scanning tools **Penetration testing tools**: Metasploit, Canvas, Writing custom exploits	04
Unit-V	**Defense in Depth**: Host-based and Network-based defenses (Firewalls, Intrusion Detection/Prevention)	03
Unit-VI	**Network analysis**: TcpDump, Wireshark, Netflow **Securing and hardening systems**: Bastille, CIS, MS Baseline	03
Unit-VII	**Incident response and investigation**: Log review, Log management and correlation, incident response process and tools	02
Unit-VIII	**Cloud security**: Tools to assess and monitor cloud-based system security	02

Self-Study: The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents

Suggested Readings/ References:

1. Preston Galla, How Personal and Internet Security Work, Que Publications
2. Alfred Basta and Wolf Halton, Computer Security Concepts, Issues and Implementation, Cengage Learning
3. Shon Harris, Allen Harper, Chris Eagle and Jonathan Ness, Gray Hat Hacking: The Ethical Hackers' Handbook, TMH Edition
4. Jon Erickson, Hacking: The Art of Exploitation, SPD
5. Peltier, T. R., Peltier, J., & Blackley, J. A., Managing a Network Vulnerability Assessment. CRC Press
6. Caswell, B., Beale, J., Ramirez, G., & Rathaus, N., Nessus, Snort, and Ethereal Power Tools: Customizing Open Source Security Applications, Elsevier

Suggested List of Experiments:

Sr. No.	Practical Title	Hours
1	To implement fake authentication on an application	02
2	To crack the WPA-2 key using aircrack – ng	02
3	To perform ARP Spoofing attack	02
4	To detect ARP Poisoning attacks and other suspicious activities in the network using Wireshark	02
5	To hack a Remote Server Using a Basic Metasploit Exploit	04
6	To gain control over the target computer using client-side attacks	02
7	To perform external vulnerability scanning using Shodan, Qualys & Nmap	04
8	To perform internal vulnerability scanning using MBSA, Nmap, Nessus, Fing & Superscan & OpenVAS	04
9	To create a persistent reverse shell with Metasploit	04
10	To demonstrate security misconfiguration Attacks and Defences using a simple application / project.	04

Suggested Case List: -NA-