COURSE TEMPLATE

1. **Department:**	**Department of Computer Science and Engineering**			
2. **Course Name:** Cyber Security		3. **Course Code**	4. **L-T-P**	5. **Credits**
		CSL422	3-0-2	4
6. **Type of Course (Check one):**	Programme Core ✔	Programme Elective ☐	Open Elective ☐	
7. **Pre-requisite(s), if any:** Basic knowledge of networking				
8. **Frequency of offering (check one):** Odd ☐	Even ✔	Either semester ☐	Every semester ☐	
9. **Focus:** Employability ✔	Entrepreneurship ☐	Skill Development ✔	Basic Knowledge ☐	

10. **Brief Syllabus:**

This course gives a practical oriented approach to the ethical hacking world whilst including essential theoretical details. This course will take the basic hacking tools and techniques to the next level and encourages students to solve complex problems that penetration testers solve in the real world. It starts with different ways of gathering information about the target, identify various vulnerabilities and consequently discusses various ways to exploit these vulnerabilities and gain access of victim system. Thereafter, it includes several methods to escalate privileges and maintain access of victim system

Total lecture, Tutorial and Practical Hours for this course (Take 15 teaching weeks per semester): 75

	Practice	
Lectures: 45 hours	**Tutorials:** 0 hours	**Lab Work:** 30 hours

11. **Course Outcomes (COs)**

Possible usefulness of this course after its completion i.e. how this course will be practically useful to him once it is completed.

CO 1	**Memorize** the important concepts of information and networking essential for ethical hacking purpose	L1
CO 2	**Identify** various reconnaissance tools to gather information from various publicly available information to **understand** the target environment.	L1,L2
CO 3	**Identify** scanning tools to conduct comprehensive network sweeps, port scans and OS fingerprinting. Student should able to **correlate** these tools on various parameters.	L1, L4
CO 4	**Apply** penetration testing tools to exploit vulnerable systems	L3
CO 5	**Formulate** steps to maintain access and cover tracks	L6

12. **UNIT WISE DETAILS**		**No. of Units: 5**
Unit Number: 1	**Title: Introduction**	**No. of hours: 4**
Content Summary: What is Data, Information, places of data, Security Triangle, key terms, Types of Information, Cyber Terrorism, Defacement, Cyber laws, Network Terminologies, Introduction to network, Network Protocols, IP address, IP subnet, classes, NAT, DHCP Server, Types of network, Ports, VPN, Proxy Servers		
Unit Number: 2	**Title: Information Gathering/Footprinting**	**No. of hours: 6**
Content Summary: Vulnerability Assessment and Penetration Testing, Phases of Penetration Testing, Cyber Kill Chain, Information gathering tools: Web, Windows and Kali based tools, DNS Enumeration tools, Google Dorks		
Unit Number: 3	**Title: Scanning and its types**	**No. of hours: 8**
Content Summary: Scanning and Enumeration: OS Fingerprinting, Port Scanning: Nmap, Network Scanning: Wireshark, Cookies, Vulnerability Scanning: Nessus, Nikto		
Unit Number: 4	**Title: Gaining Access**	**No. of hours: 20**
Content Summary: Gaining access, Login bypass- Linux and Windows, Malware, Trojan, Keylogger, Linux basics, Crunch tool, Metasploit, Attacks using Metasploitable 2, Attack Windows 7 using Metasploit		
Unit Number: 5	**Title: Maintaining Access and Covering Tracks**	**No. of hours: 7**
Content Summary: Maintaining Access with Metasploit: Initial Compromise, Privilege Escalation, Establishing Persistent Access, Returning to the Victim Machine, Pivoting To Maintain Access, Metasploit Persistent door, Covering Tracks		

13. **Brief Description of Self-learning components by students (through books/resource material etc.):**

- Metasploit Exploits
- 5 exploits from exploit-db

14. **Books Recommended:**

Textbooks:

1. McClure S., Bray J.S. and Kurtz G., Hacking Exposed 7: Network Security Secrets and Solutions. 1st ed. Tata McGraw Hill, 2012.

Reference Books:

1. Rafay Baloch, Ethical Hacking and Penetration Testing Guide, Reprint, CRC Press, 2019
2. Graham J., Howard R., Olson R., Cyber Security Essentials, 1st ed. CRC Taylor and Francis, 2010.

Reference websites: (nptel, swayam, coursera, edx, udemy, lms, official documentation weblink)

- https://www.cybrary.it/course/web-application-pen-testing/
- https://www.cybrary.it/course/advanced-penetration-testing/
- https://www.cybrary.it/course/ethical-hacking/

Practical Content

Sr. No.	Title of the Experiment	Software/ Hardware Based	Unit Covered	Time Required
1	Perform reconnaissance to find all the relevant information on selected websites using 10 network information gathering tools.	Software Based	2	2 hours
2	Gather information using Social Networking sites and google Dorks	Software Based	2	2 hours
3	Perform Network Scanning using NMAP in windows and ZENMAP in kali Linux	Software Based	2	2 hours
4	Use Nessus tool to find all the vulnerabilities with its level and generate a report for an organization	Software Based	3	2 hours
5	(i) Install Wireshark and apply filters to gather different information (ii) Perform Session hijacking/ find credentials of unsecure real time website using Wireshark	Software Based	3	2 hours
6	Create Trojan and Exploit victim's machine by taking its complete access	Software Based	3	2 hours
7	Track keystrokes of victim machine using Keylogger	Software Based	3	2 hours
8	Execute basic commands of Linux. Use CHMOD command to change the privileges and permissions Generate Word list from using wordlist generator ZAP	Software Based	3	2 hours
9	Perform Windows Login Bypass in virtual machine	Software Based	4	2 hours

10	Perform Kali Linux Login Bypass in virtual machine	Software Based	4	1 hour
11	Exploit windows to gain access of victim's machine using Metasploit framework	Software Based	4	2 hours
12	Exploit Windows 7 using Metasploit	Software Based	4	1 hour
Value Added Experiments				
1	Perform steps to remove the tracks in windows and kali Linux	Software Based	5	2 hours

Project (To be done as individual/in group): No

Evaluation Scheme (Choose one related to the course)

TYPE OF COURSE	PARTICULAR	ALLOTTED RANGE OF MARKS	PASS CRITERIA
Theory+ Practical (L-T-P/L-0-P)	Minor Test	15%	Must Secure 30% Marks Out of Combined Marks of Major Test Plus Minor Test with Overall 40% Marks in Total.
	Major Test	35%	
	Continuous Evaluation Through Class Tests/Practice/Assignments/Presentation/Quiz	10%	
	Online Quiz	5%	
	Lab Work	35%	

Mapping of PO's and CO's

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	2	3	2	3	3	2	2	3	2	3	-	3	2	2	2
CO2	2	3	2	3	3	2	2	3	2	3	1	3	2	3	2
CO3	2	2	2	3	3	2	2	3	1	3	1	3	2	2	2
CO4	3	2	2	3	3	2	2	3	2	2	2	3	2	3	3
CO5	2	2	2	3	3	3	2	3	2	3	2	3	2	3	3