Lingaya's Vidyapeeth

Deemed-to-be-University u/s 3 of UGC Act 1956, Government of India
NAAC ACCREDITED
Approved by MHRD / AICTE / PCI / BCI / COA / NCTE
Nachauli, Jasana Road, Faridabad- 121002 (Haryana)
Website: www.lingayasvidyapeeth.edu.in | Ph: 0129-2598200-05

COURSE PLAN & COURSE DATA SHEET

PROGRAM: B.Tech (Cyber Security)	DEGREE: B.Tech
COURSE: Ethical Hacking	SEMESTER: 6th CREDITS: 3
COURSE CODE: CS-320 REGULATION:	COURSE TYPE: CORE
COURSE AREA/DOMAIN: Computer Applications	CONTACT HOURS: 42
CORRESPONDING LAB COURSE CODE (IF ANY): CS-370	LAB COURSE NAME (IF ANY): Ethical Hacking LAB

PROGRAM EDUCATIONAL OBJECTIVES:

Program Educational Objectives for a course or program focused on ethical hacking aim to prepare students for successful careers in the field of cybersecurity, with a specific focus on ethical hacking practices. Here are potential Program Educational Objectives for an ethical hacking program:

1. **Technical Proficiency:** Graduates will demonstrate a high level of technical proficiency in ethical hacking methodologies, tools, and techniques, enabling them to identify and mitigate security vulnerabilities in information systems.
2. **Cybersecurity Expertise:** Graduates will possess a deep understanding of cybersecurity principles, including network security, web application security, wireless security, and system security, allowing them to address a wide range of potential threats.
3. **Ethical Hacking Competence:** Graduates will be proficient in conducting ethical hacking assessments, including penetration testing, vulnerability assessments, and security audits, while adhering to legal and ethical standards.
4. **Critical Thinking and Problem-Solving:** Graduates will develop strong critical thinking and problem-solving skills to analyse complex security issues, identify potential risks, and recommend effective countermeasures to protect information systems.

SYLLABUS:

UNIT	DETAILS	HOURS
I	**INTRODUCTION TO ETHICAL HACKING:** Ethical Hacking Fundamental concepts, Threat actors, Methodology : Reconnaissance, Footprinting, Scanning, Enumeration techniques, exploitation, record cleaning and post incident report. DNS and subdomain Enumeration, Credential and uncredentialed scan. Security threats : Virus, worm, trojan, remote access trojan and malwares. Threat models. Zero day and security policies. OSINT and SOINT basics. Cyber threat intelligence(CTI) and Threat hunting . Testing methodologies : White box, black box and Grey box. Teaming concept : Red team and Blue team. Rootkit, Common and control unit. CWE, CVE,OWASP and SANS. Introduction to Hacking Distros.	7
II	**SOFTWARE ATTACK AND PERSISTENT THREATS:** Password Attacks: Bruteforce attack, Pass the hash, rainbow table and password spraying. Cryptographic attacks. XSS, CSRF, Buffer overflow, Common injection attacks: SQL injection, LDAP injection, code injection, XML and Directory traversal attack. Privilege escalation : Vertical and Horizontal. Malware based attack: Ransomware, adware, spyware, keylogger, logic bombs, RAT, Polymorphic and armored virus. Advanced persistent threats (APT).	8
III	**NETWORK AND WEB BASED HACKING:** Network hacking: Spoofing, ARP spoofing, DNS spoofing, DNS cache poisoning, DNS hijacking, Port Scanning, Sniffing, MIMT, DOS and DDOS, Clickjacking, Session hijacking , URL jacking and typosquatting. Web-application Scanning and attacking techniques: Rate limiting, SPF record and mail server misconfiguration, local and remote file inclusion, URL redirection, Server side request forgery, remote code injection and common authentication bypass techniques and attacks based on Physical Security. Linux and Windows system hacking.	9
IV	**WIRELESS HACKING:** Introduction: Wireless technologies, Communication over Bluetooth, Wifi, NFC. Wireless monitoring, Packet analysis, WiFi Sniffing techniques, WEP/WPA cracking, Tools for wireless hacking. Wireless attacks : Rogue AP, Eviltrin , jamming, Bluejacking and bluesnarfing. Social engineering attacks : Phishing, whishing, whaling, spear phishing, smsing , skimming, dumpster diving, tailgating, piggybacking and bating.	11
V	**REPORT WRITING and MITIGATION:** Introduction to Report Writing and Mitigation, requirements for low level reporting and high level reporting of Penetration testing results, proof of concepts, expert summary, scope of attacks, disclaimers, declarations, Non-disclosure agreement (NDA), and Mitigation of issues identified including tracking.	7
	TOTAL HOURS	42

Teacher Centric Approach

TC1: Chalk and Talk, TC2: PPT, TC3: Video Lectures TC4: Blended learning

Learner Centric Approach:

LC1: Assignment. LC2: Mini project. LC3: Quiz/Class test. LC 4: Seminar on recent trends.

LC5: Group Task. LC6: Others

DETAILED SESSION PLAN

Lecture session/ Number	Topics to be covered	CO addressed	Teacher Centric Approach	Learner Centric Approach	References	Relevance with POs and PSOs
1	Ethical Hacking Fundamental concepts.		TC1, TC2	LC1,LC3	T1/T2/R1	1
2	Threat actors, Methodology : Reconnaissance		TC1,TC2	LC1,LC3	T1/T2/T3/R1	1
3	Footprinting, Scanning, Enumeration techniques		TC1,TC2	LC1,LC3	T1/T2/R1/R2	2
4	Exploitation, record cleaning and post incident report. DNS and Subdomain Enumeration, Credential and uncredentialed scan.		TC1,TC2	LC1,LC3,LC4	T1/T2/T3/R1/R2	2
5	Security threats : Virus, worm, trojan, remote access trojan and malwares. Threat models. Zero day and security policies.		TC1,TC2	LC1,LC3	T1/T2/T3/R1/R2	2
6	Various Threat Models.		TC1,TC2	LC1,LC3	T1/T2/R1/R2/R3	1
7	Zero day and security policies. OSINT and SOINT basics.		TC1,TC2	LC1,LC3,LC4	T1/T2/T3/R1/R2	
8	Cyber threat intelligence (CTI) and Threat hunting. Testing methodologies.		--	--	--	2

9	White box, black box and Grey box. Teaming concept		TC1,TC2	LC1,LC3,LC4	T1/T2/T3/R1/R2	2
10	Red team and Blue team. Rootkit, Common and control unit. CWE, CVE,OWASP and SANS. Introduction to Hacking Distros.		TC1,TC2	LC1,LC3	T1/T2/T3/R1/R2	2
11	Password Attacks		TC1,TC2	LC1,LC3,LC2	T1/T2/T3/R1/R3	1
12	Bruteforce attack, Pass the hash		TC1,TC2	LC1,LC3,LC2	T1/T2/R1/R3	2
13	rainbow table and password spraying		--	--	--	
14	Cryptographic attacks. XSS, CSRF, Buffer overflow, Common injection attacks:		TC1,TC2	LC1,LC3	T1/T2/R1/R3	1
15	SQL injection, LDAP injection, code injection, XML and Directory traversal attack. Privilege escalation		TC1,TC2	LC1,LC3	T1/T2/T3/R1/R2	2
16	Vertical and Horizontal. Malware based attack		TC1,TC2	LC1,LC3	T1/T2/T3/R1/R3	2
17	Ransomware, adware, spyware, keylogger, logic bombs, RAT		TC1,TC,2	LC1,LC3	T1/T2/T3/R1/R3	2
18	Polymorphic and armored virus. Advanced persistent threats (APT).		TC1,TC2	LC1,LC3	T1/T2/R1/R2	2
19	Network hacking		TC1,TC2	LC1,LC3	T1/T2/R1/R2	
20	Spoofing, ARP spoofing		--	--	--	1
21	DNS spoofing, DNS cache poisoning		TC1, TC2	LC1,LC3	T1/T2/T3/R1/R3	2
22	DNS hijacking, Port Scanning, Sniffing, MIMT		TC1,TC2	LC1,LC3	T1/T2/T3/R1/R3	2
23	DOS and DDOS, Clickjacking, Session hijacking , URL jacking and typosquatting. Web-application Scanning and attacking techniques		TC1,TC2	LC1,LC3, LC4	T1/T2/T3/R1/R2	2

24	Rate limiting, SPF record and mail server misconfiguration, local and remote file inclusion		TC1,TC2	LC1,LC3	T1/T2/T3/R1/R2	2
25	URL redirection, Server side request forgery		TC1,TC2	LC1,LC3	T1/T2/T3/R1/R2	2
24	remote code injection and common authentication bypass techniques and attacks based on Physical Security		TC1,TC2	LC1,LC3	T1/T2/R1/R2	2
25	Linux and Windows system hacking.		--	--	--	2
26	Introduction to Wireless technologies		TC1,TC2	LC1,LC3	T1/T2/R1/R3	1
27	Communication over Bluetooth		TC1,TC2	LC1,LC3,LC5	T1/T2/R1/R3	1
28	Wifi, NFC. Wireless monitoring		TC1,TC2	LC1,LC3,LC5	T1/T2/R1/R2	
29	Packet analysis, WiFi Sniffing techniques		TC1,TC2	LC1,LC3,LC5	T1/T2/R1/R2	1
30	WEP/WPA cracking, Tools for wireless hacking. Wireless attacks		TC1,TC2	LC1,LC3,LC5	T1/T2/R1/R2	2
31	Rogue AP, Eviltrin , jamming, Bluejacking and bluesnarfing		TC1,TC2	LC1,LC3	T1/T2/R2/R3	2
32	jamming, Bluejacking and bluesnarfing. Social engineering attacks		TC1,TC2	LC1,LC3	T2/T3/R1/R2	2
33	Phishing, whishing, whaling, spear phishing, smsing , skimming, dumpster diving, tailgating, piggybacking and bating		--	--	T1/T2/T3/R1/R2	2
34	Introduction to Report Writing and Mitigation		--	--	--	
35	requirements for low level reporting and high level reporting of Penetration testing results		TC1, TC2	LC1,LC3	T1/T2/T3/R1/R3	2
36	proof of concepts, expert summary, scope of attacks, disclaimers, declarations		TC1,TC2	LC1,LC3	T1/T2/T3/R1/R3	2
37	Non-disclosure agreement (NDA)		TC1,TC2	LC1,LC3, LC4	T1/T2/T3/R1/R2	2

38	Mitigation of issues identified including tracking.		TC1,TC2	LC1,LC3	T1/T2/T3/R1/R2	2
39	Ethical Hacking Fundamental concepts.		TC1,TC2	LC1,LC3	T1/T2/T3/R1/R2	2
40	Threat actors, Methodology : Reconnaissance		TC1,TC2	LC1,LC3	T1/T2/R1/R2	2
41	Revision Class		--	--	--	
42	Final Assessment		--	--	--	

TEXT/REFERENCE BOOKS:

T/R	BOOK TITLE/AUTHORS/PUBLICATION
1	Baloch, R., Ethical Hacking and Penetration Testing Guide, CRC Press, 2015.
2	Beaver, K., Hacking for Dummies, 3rded. John Wiley and sons., 2013.
3	McClure S., Scambray J., and Kurtz G, Hacking Exposed. Tata McGraw-Hill Education,6the Edition, 2009.
4	International Council of E-Commerce Consultants by Learning, Penetration Testing.
5	Network and Perimeter Testing Ec-Council/ Certified Security Analyst Vol. 3 of Penetration Testing, Cenage Learning, 2010.

# WEB SOURCE REFERENCES (W):

1	Geeksforgeeks
2	www.coursera.com
3	www.simplilearn.com

COURSE PRE-REQUISITES:

C.CODE	COURSE NAME	DESCRIPTION	SEM
-	Basic knowledge of computers	-	-
-	Legal aspects of hacking	-	-

COURSE OBJECTIVES:

1. **Understand Cybersecurity Fundamentals:** Develop a solid understanding of fundamental concepts in cybersecurity, including threats, vulnerabilities, attacks, and defense mechanisms.
2. **Explore Networking Basics:** Gain knowledge of networking protocols, architectures, and communication mechanisms to understand how systems are connected and potential points of vulnerability.
3. **Learn Operating System Security:** Explore the security features and vulnerabilities associated with various operating systems, including both Windows and Unix/Linux.
4. **Study Web Application Security:** Understand common vulnerabilities in web applications and learn techniques to secure web servers and applications.
5. **Master Ethical Hacking Techniques:** Learn ethical hacking methodologies, tools, and techniques for penetration testing, vulnerability assessment, and security auditing.

COURSE OUTCOMES:

S.NO	DESCRIPTION	PO(1..12) MAPPING	PSO(1..3) MAPPING
CO1	Illustrate the ethical hacking concepts which will provide them with in–depth understanding of the web application vulnerabilities and exploitation techniques.	PO1,PO2	PSO1
CO2	Identify wide range of attacks in a Networking environment.	PO1,PO2,PO3	PSO1,PSO2
CO3	Create a security assessment and penetration testing report.	PO1,PO2,PO3,PO4,PO5	PSO1,PSO2
CO4	Describe Wireless hacking.	PO1,PO2,PO3	PSO1,PSO2
CO5	Prepare a well-defined vulnerability report along with remediation techniques.	PO1,PO2,PO3,PO4,PO5	PSO1,PSO2
COURSE OVERALL PO/PSO MAPPING:			

COURSE OUTCOMES VS POs MAPPING (DETAILED; HIGH:3; MEDIUM:2; LOW:1)**:**

S.NO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	2	1	-	-	-	-	-	-	1	-	-	-	2	-	1
CO2	2	1	1	2	-	-	1	1	-	-	1	-	2	1	-
CO3	2	2	1	1	1	-	-	2	-	1	-	-	2	2	-
CO4	2	1	1	-	-	1	1	1	-	-	1	1	2	2	1
CO5	2	1	1	1	1	-	-	-	1	1	1	-	2	2	-

** For Entire Course, PO & PSO Mapping*

POs & PSO REFERENCE:

PO1	Engineering Knowledge	PO7	Environment & Sustainability	PSO 1	Foundation of mathematical concepts: To use mathematical methodologies to crack problem using suitable mathematical analysis, data structure and suitable algorithm.
PO2	Problem Analysis	PO8	Ethics	PSO 2	Foundation of Computer System: The ability to interpret the fundamental concepts and methodology of computer systems. Students can understand the functionality of hardware and software aspects of computer systems.
PO3	Design & Development	PO9	Individual & Team Work	PSO 3	Foundations of Software development: The ability to grasp the software development lifecycle and methodologies of software systems. Possess competent skills and knowledge of software design process. Familiarity and practical proficiency with a broad area of programming concepts and provide new ideas and innovations towards research.
PO4	Investigations	PO10	Communication Skills		
PO5	Modern Tools	PO11	Project Mgt. & Finance		
PO6	Engineer & Society	PO12	Life Long Learning		

COs VS POs MAPPING JUSTIFICATION:

S.NO	PO/PSO MAPPED	LEVEL OF MAPPING	JUSTIFICATION
Cxxx.1			

Cxxx.2			
Cxxx.3			
Cxxx.4			
Cxxx.5			
Cxxx*			

GAPS IN THE SYLLABUS - TO MEET INDUSTRY/PROFESSION REQUIREMENTS, POs & PSOs:

SNO	DESCRIPTION	PROPOSED ACTIONS
1	**IoT Security:** Investigate the security challenges associated with the Internet of Things (IoT). Explore vulnerabilities in IoT devices, protocols, and ecosystems. Understand how to secure and test the security of connected devices and the potential impact of insecure IoT systems on overall cybersecurity.	Need to be Covered in extra session
2	**Cloud Security:** Dive into the security considerations of cloud computing. Understand the shared responsibility model and explore techniques for securing data, applications, and infrastructure in cloud environments. Learn about cloud-specific vulnerabilities and best practices for securing cloud-based systems.	Need to be Covered in extra session
3	**Mobile Security:** Explore the security threats and vulnerabilities in mobile applications and devices. Understand the techniques used in mobile application penetration testing and mobile device security assessments. Consider the implications of mobile security in the context of Bring Your Own Device (BYOD) policies.	Need to be Covered in extra session
4	**Machine Learning and AI in Security:** Investigate the role of machine learning and artificial intelligence in cybersecurity. Understand how these technologies are used for threat detection, anomaly detection, and behavior analysis. Explore the ethical considerations surrounding the use of AI in cybersecurity and potential adversarial attacks.	Need to be Covered in extra session
5	**Blockchain Security:** Study the security aspects of blockchain technology, especially in the context of cryptocurrencies and smart contracts. Explore potential vulnerabilities and attack vectors related to blockchain-based systems. Understand how to conduct security assessments on blockchain applications and networks.	Need to be Covered in extra session

PROPOSED ACTIONS: TOPICS BEYOND SYLLABUS/ASSIGNMENT/INDUSTRY VISIT/GUEST LECTURER/NPTEL ETC

# TOPICS BEYOND SYLLABUS/ADVANCED TOPICS/DESIGN:

1	Investigate the security challenges associated with the Internet of Things (IoT). Explore vulnerabilities in IoT devices, protocols, and ecosystems. Understand how to secure and test the security of connected devices and the potential impact of insecure IoT systems on overall cybersecurity.
2	Dive into the security considerations of cloud computing. Understand the shared responsibility model and

	explore techniques for securing data, applications, and infrastructure in cloud environments. Learn about cloud-specific vulnerabilities and best practices for securing cloud-based systems.
3	Explore the security threats and vulnerabilities in mobile applications and devices. Understand the techniques used in mobile application penetration testing and mobile device security assessments. Consider the implications of mobile security in the context of Bring Your Own Device (BYOD) policies.
4	Investigate the role of machine learning and artificial intelligence in cybersecurity. Understand how these technologies are used for threat detection, anomaly detection, and behavior analysis. Explore the ethical considerations surrounding the use of AI in cybersecurity and potential adversarial attacks.
5	Study the security aspects of blockchain technology, especially in the context of cryptocurrencies and smart contracts. Explore potential vulnerabilities and attack vectors related to blockchain-based systems. Understand how to conduct security assessments on blockchain applications and networks.

DELIVERY/INSTRUCTIONAL METHODOLOGIES:

☐ CHALK & TALK	☐ STUD. ASSIGNMENT	☐ WEB RESOURCES	☐ NPTEL/OTHERS
☐ LCD/SMART BOARDS	☐ STUD. SEMINARS	☐ ADD-ON COURSES	☐ WEBNIARS

ASSESSMENT METHODOLOGIES-DIRECT

☐ ASSIGNMENTS	☐ STUD. SEMINARS	☐ TESTS/MODEL EXAMS	☐ UNIV. EXAMINATION
☐ STUD. LAB PRACTICES	☐ STUD. VIVA	☐ MINI/MAJOR PROJECTS	☐ CERTIFICATIONS
☐ ADD-ON COURSES	☐ OTHERS		

ASSESSMENT METHODOLOGIES-INDIRECT

☐ ASSESSMENT OF COURSE OUTCOMES (BY FEEDBACK, ONCE)	☐ STUDENT FEEDBACK ON FACULTY (TWICE)
☐ ASSESSMENT OF MINI/MAJOR PROJECTS BY EXT. EXPERTS	☐ OTHERS

# INNOVATIONS IN TEACHING/LEARNING/EVALUATION PROCESSES:

1. **Technology Integration:** Embrace and integrate technology tools in the classroom to enhance the learning experience. This can include interactive whiteboards, educational apps, virtual reality, and online collaboration platforms. Utilizing technology allows for more dynamic and interactive lessons, catering to diverse learning styles.
2. **Personalized Learning Paths:** Implement personalized learning approaches that cater to individual student needs and pace of learning. Adaptive learning platforms and data analytics can help tailor educational content, assignments, and assessments based on the strengths and weaknesses of each student, promoting a more customized learning experience.
3. **Active Learning Strategies:** Move away from traditional lecture-based approaches and incorporate active learning strategies. This involves engaging students in hands-on activities, group discussions, problem-solving exercises, and real-world projects. Active learning fosters critical thinking, collaboration, and practical application of knowledge.
4. **Blended Learning Models:** Adopt blended learning models that combine face-to-face instruction with online resources. This allows for flexibility in learning, enabling students to access materials at their own pace outside the classroom. Flipped classrooms, where students learn new concepts online and engage in discussions and activities during class, are an example of a blended learning approach.
5. **Assessment Innovation:** Rethink assessment methods to go beyond traditional exams and quizzes. Explore alternative forms of assessment, such as project-based assessments, portfolios, presentations, and peer assessments.

Additionally, incorporate formative assessments and feedback throughout the learning process to help students track their progress and make improvements.

Prepared by	**Approved by**
Ms. Tanya Chauhan	**(HOD)**