LESSON PLAN 2025-26(SUMMER)

NAME OF THE TEACHER : DEEPAK KUMAR BARDA, LECT(STAGE-II. CSE)

Subject: **INTERNET SECURITY(CSEPE 204/Th 5)**
Program: Diploma in Computer Science and Engineering
Semester: 4th
Total Contact Hours: 45
Total Marks: 100
Assessment: Internal Assessment – 30, End Term – 70

After completion of the course, the students will be able to:
CO1: Describe key principles of information security, including confidentiality, integrity, and availability.
CO2: Describe common cryptographic techniques such as symmetric and asymmetric encryption, hashing,and public key infrastructure.
CO3: Explain network security threats, such as malware, DoS, and phishing.
CO4: Demonstrate the ability to implement secure web applications by applying best practices to prevent vulnerabilities like SQL injection, XSS, and CSRF.
CO5: Analyze the security posture of operating systems by developing security policies, incident response strategies.
CO6: Evaluate emerging security challenges in modern technologies such as IoT, cloud computing, and mobile applications.

Lesson No.	UNIT	Topic/Sub-Topic	Learning Objective	Activity	Homework	COURSE OBJECTIVE
UNIT-1-: Overview of Information security: (8 Hours)						
1	I	Definition of Information Security	Define Information Security and its necessity in the modern digital landscape.	"The Cost of a Leak": Group discussion on recent high-profile data breaches.	Research one major data breach from the last 2 years.	**CO1**
2	I	The CIA Triad	Understand and apply the core pillars: Confidentiality, Integrity, and Availability.	Scenario Mapping: Categorize various security failures into C, I, or A.	Identify one personal example of a "Availability" failure you've faced.	C01
3	I	Malware & Hacking	Distinguish between types of malware (viruses, worms, ransomware) and hacking methods.	"Identify the Bug": Matching symptoms of an infected PC to specific malware	Write a 200-word summary on how Ransomware functions.	C01
4	I	Social Engineering	Identify Phishing, Smishing, and Vishing tactics used to exploit human psychology.	Spot the Phish": Analyze a series of emails to find red flags (URL masking, urgency).	Create a "Fake Phishing Email" to test a classmate in the next session.	CO2

5	I	Network Attacks	Understand DoS/DDoS attacks and Man-in-the-Middle (MitM) interceptions.	Visualizing the Flow: Draw a diagram of how a DDoS attack overwhelms a server.	Research the difference between a DoS and a DDoS attack.	CO2
6	I	Policies & Practices	Learn the components of a strong security policy (Passwords, MFA, Updates).	Policy Audit: Review a sample "Acceptable Use Policy" and find 3 loopholes.	Set up Multi-Factor Authentication (MFA) on one personal account.	CO1
7	I	Risk Management	Learn to identify, assess, and mitigate risks using qualitative measures.	Risk Matrix: Create a 3×3 grid to rank risks by Likelihood vs. Impact	List 3 digital assets you own and rank their risk level.	CO1
8	I	ISO 27001 & NIST	Overview of global security standards and compliance frameworks.	Compliance Check: Map the CIA Triad pillars to specific NIST functions.	Final Reflection: How has your view on digital privacy changed?	CO1
UNIT-2:- Cryptography: (8 hours)						
9	II	Intro to Cryptography	Understand CIA triad (Confidentiality, Integrity, Availability) and history.	"Scytale" Challenge: Decrypt a message using a paper strip and pencil.		CO3
10	II	Symmetric Encryption	Differentiate between Stream and Block ciphers; understand shared keys.	Manual "Substitution Cipher" exercise (Caesar Cipher).		CO3
11	II	DES & AES	Understand Feistel networks and the SP-network (Substitution-Permutation).	Visualizing AES rounds (SubBytes, ShiftRows, MixColumns).		CO3
12	II	Asymmetric Crypto	Grasp the concept of Public/Private key pairs and Trapdoor functions.	The "Padlock Analogy": Simulating key exchange without sharing a key.		CO3

13	II	RSA & ECC	Understand prime factorization (RSA) vs. Elliptic Curve math.	Calculating a simplified RSA key pair using small prime numbers.		CO3
14	II	Hashing & Digital Signatures	Learn one-way functions, collision resistance, and non-repudiation.	Using a tool (like HashCalc) to see how changing 1 bit changes the whole hash.		CO3
15	II	PKI & Certificates	Understand Trust Models, CAs (Certificate Authorities), and X.509.	Role-play: The "Chain of Trust" from Root CA to End User.		CO3
16	II	SSL/TLS Protocols	Synthesize all previous topics into the "TLS Handshake" process.	Wireshark analysis: Observing a 3-way handshake and encrypted		
UNIT-3:-Network Security: :(8 hours)						
17	III	Network Vulnerabilities	Identify common network attacks (DoS, MITM, Sniffing).	Packet Sniffing Lab: Use Wireshark to capture and view unencrypted (HTTP) traffic.		CO3
18	III	Firewall Fundamentals	Understand Packet Filtering, Stateful Inspection, and Proxy firewalls.	Rule Creation: Draft an Access Control List (ACL) to block specific IPs and ports.	What is the major cost associated with swapping? (Hint: disk I/O).	CO3
19	III	Firewall Configuration	Master the concepts of DMZ (Demilitarized Zone) and NAT.	.Network Mapping: Design a secure network layout with a DMZ and internal LAN.	Given a logical address, page size, and page table, calculate the corresponding physical address.	CO3
20	III	IDS vs. IPS	Distinguish between detection (passive) and prevention (active).	Snort Simulation: Review sample "Snort" logs to identify a simulated port scan.	How does segmentation aid in protection and sharing of code?	CO3
21	III	VPN Principles	Understand tunneling, encryption, and remote access vs. site-to-site	Understand tunneling, encryption, and remote access vs. site-to-site		CO3

22	III	IPsec Protocol	Deep dive into AH (Authentication) and ESP (Encapsulation) headers.	Header Breakdown: Deconstruct an IPsec packet to identify where encryption occurs.		CO3
23	III	SSL/TLS & HTTPS	Understand the Transport Layer handshake and certificate verification.	Handshake Trace: Follow a live browser-to-server TLS 1.3 handshake step-by-step.		CO3
24	III	Integrated Defense	Synthesize all tools into a "Defense in Depth" strategy.	Tabletop Exercise: Respond to a simulated multi-stage network breach scenario.	What is "thrashing"? How can it be detected and prevented?	CO3
UNIT 4:- Security in Operating Systems: (7 hours)						
25	IV	User Authentication	Compare Multi-Factor (MFA) vs. Single-Factor; evaluate password strength.	Password Stress Test: Use a strength checker to see how "salting" and length impact crack time.	List and describe 6 common file operations (e.g., create, read, write, delete).	CO3
26	IV	Access Control Models	Differentiate between DAC (Discretionary), MAC (Mandatory), and RBAC (Role-Based).	Permission Matrix: Assign "Read/Write/Execute" roles for a mock medical clinic database.	What is an "index"? How does it help with file access?	CO3
27	IV	File System Security	Understand NTFS/ext4 permissions and the role of Metadata in security.	ACL Investigation: Use command line (icacls or chmod) to find "hidden" permissions on a file.	What is the main problem with a single-level directory structure?	CO3
28	IV	OS Encryption	Distinguish between File-Level (EFS) and Full-Disk Encryption (BitLocker/FileVault).	Encryption Lab: Encrypt a USB drive and attempt to read it on a "guest" machine.	How does an acyclic-graph structure allow for file sharing? What is a "link" or "shortcut"?	CO3
29	IV	Hardening Techniques	Learn to disable unnecessary services, close ports, and remove "bloatware."	Attack Surface Reduction: Use a checklist to "harden" a fresh Windows/Linux install.	What is a "mount point"? What happens when you mount a USB drive?	CO3

30	IV	Auditing & Logging	Identify critical events to monitor (Logons, File Access, Privilege escalation).	Log Hunting: Analyze a Windows Event Viewer log to find a "failed login" brute-force attempt.	What do the r, w, and x permissions mean for a file? What do they mean for a directory?	CO3
31	IV	Security Monitoring	Explore SIEM (Security Information & Event Management) and EDR tools.	Dashboard Creation: Map out which OS alerts should trigger an immediate admin email.	What is the "superblock"? What information does it contain?	CO3
UNIT-5 - Web security:(7 hours)						
32	V	SQL Injection (SQLi)	Understand how unsanitized data manipulates database queries.	The "1=1" Hack: Use a mock login page to bypass authentication using ' OR 1=1 --.	Why do we need a storage hierarchy? Why not just have one large, fast memory?	CO4
33	V	XSS & CSRF	Differentiate between script injection (XSS) and forged requests (CSRF).	Cookie Stealing: Execute a script that "pops" an alert box containing the user's session cookie.	Define seek time, rotational latency, and transfer time.	CO4
34	V	Secure Coding Practices	Master Input Validation, Output Encoding, and the OWASP Top 10.	Code Review: Identify vulnerabilities in a "broken" snippet of PHP or JavaScript code.	What is the main problem with the SSTF (Shortest Seek Time First) algorithm? (Hint: starvation).	CO4
35	V	HTTP Headers & Security	Learn about HSTS, CSP (Content Security Policy), and X-Frame-Options.	Header Analysis: Use browser DevTools to inspect the security headers of top websites (Google, Banks).	Solve a new disk scheduling problem using FCFS, SSTF, SCAN, and C-SCAN.	CO4
36	V	Web App Firewalls (WAF)	Understand Layer 7 filtering vs. traditional Layer 3/4 firewalls.	WAF Rule Design: Create a rule to block "User-Agents" commonly used by malicious bots.	How does swap space management relate to virtual memory?	CO4
37	V	Penetration Testing	Understand the ethics and methodology of a professional "Pentest."	Capture The Flag (CTF): A mini-competition to find a "hidden flag" on a vulnerable web app.		
38	V	RAID Types	Explain the concept of RAID. Describe RAID 0 (striping), RAID 1 (mirroring), and RAID 5 (parity).	Diagram: Draw the disk layouts for RAID 0, 1, and 5. Discuss pros/cons (speed, redundancy).	Which RAID level provides the best redundancy? Which provides the best speed? Which provides a balance?	CO4

UNIT-6 Security Policies and Incident Response: (7 Hours)						
39	VI	Security Policies	Draft policies for Access Control, Data Privacy, and AUP..	Policy Workshop: Write a 1-page "Acceptable Use Policy" for a company's new AI tools.	List and explain the four necessary conditions for deadlock (Mutual Exclusion, Hold & Wait, No Preemption, Circular Wait).	CO5
40	VI	BCP & DRP	IR Lifecycle: Prep & ID	Learn to identify an incident and set up an Incident Response Team (CSIRT).	For each of the four conditions, propose one strategy to prevent it.	CO5
41	VI	Containment & Eradication	Master strategies to "stop the bleed" and remove the threat root cause.	Scenario Play: A laptop is infected with ransomware; decide: pull the plug or keep it on?	What is the difference between "deadlock prevention" and "deadlock avoidance"?	CO5
42	40	Recovery & Post-Incident	Understand system restoration and the "Lessons Learned" phase.	Understand system restoration and the "Lessons Learned" phase.	Solve a new Banker's Algorithm problem.	CO5
43	VI	Digital Forensics	Learn the chain of custody and "dead" vs. "live" forensics.	Imaging Lab: Use a tool (like FTK Imager Lite) to create a bit-by-bit copy of a folder.	Why do many common desktop OSes (like Windows and Linux) primarily use the Ostrich Algorithm?	CO5
44	VI	Legal & Ethics	Navigate GDPR, HIPAA, and the ethics of "hacking back.	Ethical Debate: Discuss the ethics of monitoring employee keystrokes for "security."	List two ways to recover from a deadlock once it is detected. What are the pros and cons of each?	CO5

Deepak L M
22.12.2025
Signature of Teacher

Deepak L M
22/12/2025
Signature of HOD