Learning Outcomes-based Curriculum Framework
(as per NEP)

For

Diploma in Cyber Security and Ethical Hacking
(1 Year/2 Semester Program)

Department of Computer Science and Engineering
Faculty of Engineering and Technology
Chaudhary Devi Lal University
Sirsa-125055
2025

Programme Educational Objectives (PEOs)

PEO-1: Develop Professional Competence and Career Growth
Within five years, alumni will have progressed into professional roles (e.g., Security Analyst, Penetration Tester, Network Security Engineer, SOC Analyst) in industry, government, startups, or academic settings, demonstrating technical proficiency, critical thinking, and innovation in cybersecurity domains.

PEO-2: Demonstrate Ethical Conduct and Leadership
Graduates will exercise ethical integrity, adhere to legal frameworks, and uphold best practices in cybersecurity, while actively participating in professional communities, leading small teams, or mentoring junior practitioners.

PEO-3: Engineer Innovative Security Solutions
They will utilise acquired expertise to design, deploy, and manage secure systems, employing principles of cryptography, forensics, vulnerability assessment, and incident response to solve real-world challenges and innovate security practices.

PEO-4: Pursue Lifelong Learning and Advanced Specialisation
Alumni will engage in continuous learning through acquiring advanced certifications, pursuing higher education, research, or upskilling to remain ahead of emerging technologies and threat landscapes.

Program Outcomes (POs): Upon completion of the diploma, students will be able to:

1. **PO-1 Technical Foundations** – Apply principles of networking, operating systems, programming, and hardware fundamentals in cybersecurity contexts.
2. **PO-2 Ethical Hacking and Vulnerability Assessment** – Perform penetration tests, vulnerability scans, and security audits using standard tools.
3. **PO-3 Secure Systems Design** – Develop and implement security solutions including firewalls, IDS/IPS, encryption, and secure coding practices.
4. **PO-4 Incident Response and Forensics** – Investigate security incidents, perform digital forensics, and apply incident handling protocols.
5. **PO-5 Legal and Ethical Standards** – Recognise relevant laws, regulations, and ethical responsibilities in cybersecurity practices.
6. **PO-6 Communication and Teamwork** – Communicate effectively with technical and non-technical stakeholders and collaborate in teams.
7. **PO-7 Lifelong Learning** – Engage in self-directed learning for professional growth and technology updates.
8. **PO-8 Risk Analysis and Management** – Assess risks, recommend mitigation strategies, and implement governance frameworks.

Table 1: Semester-wise course codes, course titles, workload and credits

Course Code	Course Title	Workload		Credit	Max. Marks
		L	P		
Semester - 1					
DCSEH-11	IT Hardware and Network Infrastructure	3	2	4	100
DCSEH-12	Principles of Information and Cyber Security	3	2	4	100
DCSEH-13	Python Programming for Security	3	2	4	100
DCSEH-14	Operating System Security	3	2	4	100
	Total	12	8	16	400
Semester - 2					
DCSEH-21	Cyber Laws and Privacy Framework in India	4	-	4	100
DCSEH-22	Fundamentals of Ethical Hacking	4	-	4	100
DCSEH-23	Threat Monitoring and Penetration Testing Lab	-	8	4	100
DCSEH-24	Project Work	-	-	4	100
	Total	8	8	16	400

Semester I

DCSEH-11: IT Hardware and Network Infrastructure							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Theory	03	03	Lecture	50	25 (15 / 5 / 5)	3 Hours	TEE/MTE/ Assignment/ Attendance
Practical	01	02	Practical	25	-	3 Hours	TEE (Expt, Lab Record, Viva)

Instructions to paper setter for term-end theory examination: There shall be NINE questions in total. Question number one will be compulsory and will consist of FIVE short/objective-type questions from the complete syllabus. In addition, there shall be EIGHT questions (two questions from each unit). The student will attempt one question from each unit in addition to the compulsory question. All questions will be of TEN marks each.

The paper setter will set the paper in both English and Hindi/ mixed mode languages. Accordingly, students can also write the answers the same way.

Course Objectives:

Understand the architecture of computers and components.
Learn fundamentals of network infrastructure and configuration.
Gain hands-on experience with networking devices.
Understand LAN, WAN, and internet technologies.

Course Outcomes:

CO1: Identify and describe computer hardware components.
CO2: Demonstrate understanding of networking concepts and protocols.
CO3: Configure basic LAN and wireless setups.
CO4: Work with networking devices like routers and switches.

CO-PO Matrix:

CO \ PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	2	2	1	1	0	0	0
CO2	3	3	2	2	1	0	0	0
CO3	2	3	3	2	2	1	0	0
CO4	3	3	3	2	1	1	1	1

Detailed Syllabus:

Unit 1: Introduction to IT Hardware

Basic Computer Components: CPU, Memory (RAM, ROM), Storage Devices (HDD, SSD), Motherboard, Input/Output Devices.
Peripheral Devices and their security considerations.
Introduction to different types of servers (web, database, file) and their components.

Unit 2: Network Fundamentals

Introduction to Computer Networks: LAN, WAN, MAN.
Network Topologies: Bus, Star, Ring, Mesh.
OSI Model and TCP/IP Model: Layers, protocols at each layer (HTTP, HTTPS, FTP, DNS, DHCP, SMTP, POP3, IMAP).
IP Addressing: IPv4, IPv6, Subnetting.
Concept of Ports.

Unit 3: Network Devices and Infrastructure

Network Devices: Hubs, Switches, Routers, Modems, Firewalls, Access Points.
Network Cabling: UTP, STP, Fiber Optic.
Wireless Networking: Wi-Fi standards.
Network Services: DNS, DHCP, VPN, NAT.

Unit 4: Virtualization and Cloud Basics

Introduction to Virtualization: Virtual Machines, Hypervisors (Type 1, Type 2).
Benefits of virtualization in cybersecurity.
Basic concepts of Cloud Computing: IaaS, PaaS, SaaS.
Public, Private, Hybrid Clouds.

Suggested Readings:

1. Andrew S. Tanenbaum, "Computer Networks"
2. Behrouz A. Forouzan, "Data Communications and Networking"
3. Scott Mueller, "Upgrading and Repairing PCs"
4. "CompTIA A+ Core 1 and Core 2 Exam Cram" by David L. Prowse
5. "CompTIA Network+ N10-008 Cert Guide" by Anthony Sequeira
6. "Computer Networking: A Top-Down Approach" by James Kurose and Keith Ross

List of Lab Exercises (only indicative)

Lab 1-2: IT Hardware Familiarization and Assembly: Identify computer components, basic assembly/disassembly of a PC, connecting peripherals.

Lab 3-4: Network Cable Crimping and Configuration: Crimping UTP cables (straight-through, crossover), configuring basic network settings (IP address, subnet mask, gateway).

Lab 5-6: Network Device Configuration: Basic configuration of a router/switch (password, IP address, basic routing/VLANs).

Lab 7-8: Windows Security Hardening: User account management, Firewall configuration, Local Security Policy settings, Event Viewer analysis.

Lab 9-10: Linux Security Hardening: User and group management, File permissions (chmod, chown), SSH hardening, UFW firewall configuration.

Lab 11-12: Basic Network Scanning and Analysis: Using ping, ipconfig/ifconfig, netstat, tracert/traceroute to understand network connectivity.

DCSEH-12: Principles of Information and Cyber Security							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Theory	03	03	Lecture	50	25 (15 / 5 / 5)	3 Hours	TEE/MTE/ Assignment/ Attendance
Practical	01	02	Practical	25	-	3 Hours	TEE (Expt, Lab Record, Viva)

Instructions to paper setter for term-end theory examination: There shall be NINE questions in total. Question number one will be compulsory and will consist of FIVE short/objective-type questions from the complete syllabus. In addition, there shall be EIGHT questions (two questions from each unit). The student will attempt one question from each unit in addition to the compulsory question. All questions will be of TEN marks each.

The paper setter will set the paper in both English and Hindi/ mixed mode languages. Accordingly, students can also write the answers the same way.

Course Objectives:

Understand core principles of information security.Identify various cyber threats and attack vectors.Explore security models, cryptography, and authentication.Learn incident response and risk management.

Course Outcomes:

CO1: Explain core principles of information security.
CO2: Identify cyber threats and their impacts.
CO3: Understand authentication and encryption mechanisms.
CO4: Develop basic response strategies to security incidents.

CO-PO Matrix:

CO \ PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	2	2	1	0	0	0	0
CO2	3	3	2	2	1	1	0	0
CO3	3	3	3	2	2	1	0	0
CO4	2	3	3	2	2	2	1	1

Detailed Syllabus:

Unit 1: Information Security Principles

Confidentiality, Integrity, Availability (CIA Triad).
Authentication, Authorization, Accounting (AAA).
Non-repudiation.
Risk Management: Identification, Assessment, Mitigation.
Security Policies, Standards, Guidelines, Procedures.
Physical Security.

Unit 2: Introduction to Cyber Security

Definition and Scope of Cybersecurity.
Key components of a robust cybersecurity framework.
Roles and responsibilities in cybersecurity.
Cybersecurity vs. Information Security.
Common Security Breaches and their impact.

Unit 3: Cyber Threats and Attacks

Types of Cyber Threats: Malware (Viruses, Worms, Trojans, Ransomware, Spyware, Adware), Phishing, Spear Phishing, Whaling.
Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
Man-in-the-Middle (MITM) attacks.
SQL Injection, Cross-Site Scripting (XSS).
Social Engineering techniques.
Advanced Persistent Threats (APTs).

Unit 4: Basic Cyber Security Countermeasures

Antivirus and Anti-malware software.
Firewalls (Hardware and Software).
Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).
Strong Passwords and Multi-Factor Authentication (MFA).
Data Backup and Recovery.
Security Awareness Training.

Suggested Readings:

1. William Stallings, "Cryptography and Network Security"
2. Nina Godbole and Sunit Belapure, "Cyber Security"
3. Charles P. Pfleeger, "Security in Computing"
4. "CompTIA Security+ SY0-601 Cert Guide" by David L. Prowse (for foundational security concepts)
5. "Hacking: The Art of Exploitation" by Jon Erickson (for deeper understanding of exploitation, more advanced)
6. "The Official (ISC)2 CISSP CBK Reference" (for broader information security concepts, advanced)

7. "Cyber Security: A Practitioner's Guide to Cyber Risks and Threats" by Paul Dorey, Jeremy Hintz, David Livingston

List of Lab Exercises (indicative list):

Lab 1: The CIA Triad and Access Control: Use a virtual machine to set up user permissions on a shared folder to enforce confidentiality, integrity, and availability.

Lab 2: Risk Assessment and Mitigation: Conduct a basic risk assessment for a hypothetical scenario, identify threats and vulnerabilities, and propose mitigation strategies.

Lab 3: Security Policy Analysis: Analyze a real-world security policy, identify its key components, and create a checklist for new employees based on the policy.

Lab 4: Malware Analysis (Safe Environment): Use a sandboxing tool in a controlled virtual environment to analyze the behavior of pre-approved, non-destructive malware samples.

Lab 5: Phishing Simulation (Controlled Environment): Use a local web server to demonstrate the mechanics of a phishing attack by creating a fake login page and discussing how to identify it.

Lab 6: SQL Injection Attack Simulation: Use a vulnerable web application to demonstrate how to perform a SQL injection attack and discuss its prevention.

Lab 7: Firewall Configuration and Rules: Configure a software firewall on a virtual machine to block specific ports and IP addresses, and verify the rules using a network scanning tool.

Lab 8: Multi-Factor Authentication (MFA) Implementation: Set up and demonstrate multi-factor authentication on a service to understand its security benefits.

Lab 9: Data Backup and Recovery Simulation: Perform a data backup of important files on a virtual machine, simulate data loss, and restore the files from the backup.

DCSEH-13: Python Programming for Security							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Theory	03	03	Lecture	50	25 (15 / 5 / 5)	3 Hours	TEE/MTE/ Assignment/ Attendance
Practical	01	02	Practical	25	-	3 Hours	TEE (Expt, Lab Record, Viva)

Instructions to paper setter for term-end theory examination: There shall be NINE questions in total. Question number one will be compulsory and will consist of FIVE short/objective-type questions from the complete syllabus. In addition, there shall be EIGHT questions (two questions from each unit). The student will attempt one question from each unit in addition to the compulsory question. All questions will be of TEN marks each.

The paper setter will set the paper in both English and Hindi/ mixed mode languages. Accordingly, students can also write the answers the same way.

Course Objectives:

Learn basic Python programming constructs.
Understand scripting for automation in security.
Utilize libraries for network and security tasks.

Course Outcomes:

CO1: Write Python scripts using control structures.
CO2: Develop file-handling and pattern-matching scripts.
CO3: Create network-based scripts for packet analysis.
CO4: Automate basic security tasks using Python.

CO-PO Matrix:

CO \ PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	2	1	1	0	0	0	0
CO2	3	3	2	1	1	0	0	0
CO3	3	3	3	2	2	1	0	0
CO4	2	3	3	2	3	1	1	0

Detailed Syllabus:

Unit I: Python Basics for Security

Introduction to Python: Data types, control structures, functions, modules
Working with files and directories
Exception handling and logging
Introduction to Python Virtual Environments
Installing packages via pip (e.g., requests, scapy, nmap)

Unit II: Networking and Reconnaissance Automation

Using Python for socket programming
Port scanning using Python and Nmap module
Banner grabbing and service enumeration
DNS queries and WHOIS lookups
HTTP request automation using requests, urllib

Unit III: Cryptography and Hashing

Understanding hashing algorithms: MD5, SHA1, SHA256
Implementing symmetric encryption using PyCryptodome
Password hashing and verification
Using Python for file integrity monitoring
Basic steganography and data encoding/decoding

Unit IV: Forensics and Malware Analysis with Python

Log file parsing and regex filtering
File metadata and timestamps extraction
Using pefile, yara, and pyshark for malware analysis
Memory and process inspection (using psutil)
Writing basic scripts for browser artifact extraction
Report generation and JSON/CSV parsing

Suggested Tools and Libraries:

Python 3.x, pip, venv, Scapy, PyCryptodome, Nmap, YARA, PEfile, psutil, requests, pyshark, BeautifulSoup, os, shutil

Suggested Readings and Resources:

1. Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers – TJ O'Connor
2. Black Hat Python – Justin Seitz
3. Python for Offensive PenTest – Hussam Khrais
4. Python 3 Documentation – https://docs.python.org/3/
5. Online Labs: Hack The Box, TryHackMe (Python rooms)

List of Lab Exercises (only indicative)

Lab 1-2: Python Basics: Hands-on exercises on variables, data types, control flow, functions.

Lab 3-4: File Handling and String Manipulation: Reading/writing files, parsing text, regular expressions for log parsing.

Lab 5-6: Network Programming with Sockets: Developing a simple TCP/UDP client and server.

Lab 7-8: Simple Port Scanner and Banner Grabbing: Implementing a basic port scanner and extracting service banners.

Lab 9-10: Password Generator and Hashing Utility: Creating scripts to generate strong passwords and compute hash values (MD5, SHA256).

Lab 11-12: Basic System Automation Scripts: Scripts to check system info, manage processes, or perform simple file operations.

DCSEH-14: Operating System Security							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Theory	03	03	Lecture	50	25 (15 / 5 / 5)	3 Hours	TEE/MTE/ Assignment/ Attendance
Practical	01	02	Practical	25	-	3 Hours	TEE (Expt, Lab Record, Viva)

Instructions to paper setter for term-end theory examination: There shall be NINE questions in total. Question number one will be compulsory and will consist of FIVE short/objective-type questions from the complete syllabus. In addition, there shall be EIGHT questions (two questions from each unit). The student will attempt one question from each unit in addition to the compulsory question. All questions will be of TEN marks each.

The paper setter will set the paper in both English and Hindi/ mixed mode languages. Accordingly, students can also write the answers the same way.

Course Objectives:

Understand OS architecture and components.
Study security features in Windows, Linux, iOS, and Android.
Learn system hardening and access control techniques.

Course Outcomes:

CO1: Understand core OS concepts and security roles.
CO2: Apply access control in Windows and Linux.
CO3: Configure security settings on mobile platforms.
CO4: Implement system hardening techniques.

CO-PO Matrix:

CO \ PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	2	1	1	0	0	0	0
CO2	3	3	2	2	1	1	1	0
CO3	3	3	2	2	2	1	1	0
CO4	2	3	3	2	2	1	1	1

Detailed Syllabus:

Unit 1: Introduction to OS Security

Goals of OS Security: Confidentiality, Integrity, Availability.
User and Group Management.
File System Permissions.
Authentication and Authorization Mechanisms.
Security patches and updates.

Unit 2: Windows Operating System Security

User Account Control.
Windows Firewall configuration.
Group Policy Management Editor (gpedit.msc) for security settings.
Registry Editor for security configurations.
Windows Security Baselines and templates.
Disk Encryption (BitLocker).
Windows Event Viewer for security auditing.
Introduction to PowerShell for security tasks.

Unit 3: Linux Operating System Security

Linux File System Permissions (chmod, chown).
User and Group management in Linux.
Sudoers file configuration.
SSH Hardening.
Firewall (UFW, Iptables) configuration.
SELinux and AppArmor (basic concepts).
Log file analysis in Linux.
Introduction to shell scripting for security automation.

Unit 4: Mobile OS Security (iOS and Android)

Basic security features of iOS: App Store security, Face ID/Touch ID.
Basic security features of Android: Permissions model, Google Play Protect, Device encryption.
Common mobile attack vectors and mitigation strategies (e.g., malicious apps, insecure Wi-Fi).

Suggested Readings:

1. William Stallings, "Operating Systems: Internals and Design Principles"
2. Brian Ward, "How Linux Works"
3. Andrew S. Tanenbaum, "Modern Operating Systems"
4. "Practical Linux Forensics A Guide for Digital Investigators" by Bruce Nikkel (relevant for Linux hardening)
5. "Windows Internals" (series of books by Mark Russinovich, highly technical but good for deeper understanding)
6. Official Microsoft and Linux Foundation documentation/guides on security.

List of Lab Exercises (indicative only):

Lab 1: User, Group, and File System Management: Create user accounts and groups on both a Windows and a Linux virtual machine. Assign users to groups and then use file system permissions (NTFS permissions on Windows, `chmod`/`chown` on Linux) to enforce different levels of access to specific files and folders.

Lab 2: Authentication and Patch Management: Configure strong password policies and account lockout policies on a Windows VM. In a separate exercise, demonstrate the process of checking for and applying security updates on both a Windows and a Linux VM, explaining the importance of a regular patching cycle.

Lab 3: Windows Firewall and User Account Control: On a Windows virtual machine, configure the Windows Firewall to block a specific application from accessing the internet and to block all incoming traffic on a particular port. Also, change the User Account Control (UAC) settings and observe the difference in user prompts when attempting to install software.

Lab 4: Group Policy and Security Baselines: Use the Group Policy Management Editor (`gpedit.msc`) on a Windows VM to enforce a complex password policy and disable USB storage access. Introduce the concept of a security baseline and demonstrate how to apply a pre-configured security template.

Lab 5: Disk Encryption and Event Logging: Enable BitLocker on a partition of a Windows virtual machine and demonstrate the encryption/decryption process. In a separate exercise, use the Windows Event Viewer to filter for and analyze security-related events, such as failed logon attempts.

Lab 6: Linux Permissions and Sudoers File: On a Linux virtual machine, use `chmod` and `chown` to modify file permissions and ownership. Then, edit the `/etc/sudoers` file to grant a standard user account specific administrative privileges for a single command, without giving them full `sudo` access.

Lab 7: SSH Hardening and Firewall Configuration: Configure SSH on a Linux VM to disable root login, change the default port, and use key-based authentication instead of passwords. Use a Linux firewall (e.g., UFW or Iptables) to block all incoming traffic except for the newly configured SSH port.

Lab 8: Log Analysis and Shell Scripting: Analyze log files in `/var/log` to identify failed login attempts or other suspicious activity. Write a basic shell script that automates a simple security task, such as checking for the existence of a specific user or a suspicious file.

Lab 9: Mobile OS Security Features: Using an Android emulator (e.g., Android Studio) and a demonstration with a physical iOS device, explore and configure the built-in security features. This includes demonstrating the permissions model for a newly installed app on Android and setting up biometric authentication (Face ID/Touch ID) and device encryption on iOS.

Lab 10: Mobile Security Threats: Simulate a common mobile threat by downloading a pre-approved, benign application from an untrusted source on an Android emulator. Analyze the app's requested permissions and discuss the potential risks of such a download. Discuss mitigation strategies, such as the importance of using official app stores and being wary of insecure Wi-Fi.

Semester II

DCSEH-21: Cyber Laws and Privacy Framework in India							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Theory	04	04	Lecture	70	30	3 Hours	TEE/MTE/ Assignment/ Attendance
					20 5 5		

Instructions to paper setter for term-end theory examination: There shall be NINE questions in total. Question number one will be compulsory and will consist of SEVEN short/objective-type questions from the complete syllabus. In addition, there shall be EIGHT questions (two questions from each unit). The student will attempt one question from each unit in addition to the compulsory question. All questions will be of FOURTENN marks each.

The paper setter will set the paper in both English and Hindi/ mixed mode languages. Accordingly, students can also write the answers the same way.

Course Objectives:

To understand the evolution of cyber laws in India.
To examine various provisions of the Information Technology Act.
To explore the interface of privacy, surveillance, and digital rights.
To analyze the BNS (Bharatiya Nyaya Sanhita) and BNSS (Bharatiya Nagarik Suraksha Sanhita) in cybersecurity contexts.

Course Outcomes:

CO1: Explain the key provisions of the Information Technology Act, 2000, and its role in regulating cyber activities.
CO2: Describe the legal framework for data privacy in India, particularly the Digital Personal Data Protection Act, 2023.
CO3: Analyze the relevance of Bharatiya Nyaya Sanhita (BNS) and Bharatiya Nagarik Suraksha Sanhita (BNSS) to cybercrime investigation and prosecution.
CO4: Understand ethical considerations and intellectual property rights in the context of cybersecurity.

CO-PO Matrix:

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	2	-	-	-	3	-	-	-
CO2	2	-	-	-	3	-	-	-
CO3	2	-	-	-	3	-	-	-
CO4	1	-	-	1	3	-	-	-

Detailed Syllabus:

Unit 1: Introduction to Cyber Law in India

Need and Importance of Cyber Laws.
Information Technology Act, 2000 (IT Act): Overview, Amendments.
Digital Signatures and Electronic Governance.
Cyber Crimes: Definitions and Penalties under IT Act. (Sections related to cyber fraud,hacking, data theft, publishing obscene content).
Jurisdiction in Cyber Space.

Unit 2: Privacy Laws in India

Right to Privacy as a Fundamental Right (Puttaswamy Judgement).
Digital Personal Data Protection Act, 2023 (DPDPA): Key provisions, obligations of Data Fiduciaries, rights of Data Principals, Data Protection Board of India.
Sensitive Personal Data or Information (SPDI) Rules.
Data Localization concepts.
Consent and Notice requirements under DPDPA.

Unit 3: BNS and BNSS - Cybersecurity Aspects

Overview of BNS (replacing IPC) and BNSS (replacing CrPC).
Provisions in BNS related to cyber offenses (e.g., electronic evidence, digital evidence tampering, specific cybercrime definitions if explicitly covered).
Provisions in BNSS related to investigation, evidence collection, and trial procedures for cybercrimes (e.g., audio-video recording of search, forensic investigations).
Interplay between IT Act, DPDPA, BNS, and BNSS in addressing cybercrime.

Unit 4: Intellectual Property and Ethical Considerations

Copyright, Trademark, Patent in Digital Domain.
Cyber Squatting, Domain Name Disputes.
Ethics in Cybersecurity: Professional codes of conduct, responsible disclosure, ethical hacking guidelines.
Case studies of major cybercrime incidents and their legal implications.

Suggested Readings:

1. Vakul Sharma, "Information Technology Law and Practice"
2. Talat Fatima, "Cyber Crimes"
3. Pavan Duggal, "Cyber Law: The Indian Perspective"
4. "Information Technology Act, 2000" (Bare Act and commentaries)
5. "Digital Personal Data Protection Act, 2023" (Bare Act and analysis)
6. "Bharatiya Nyaya Sanhita (BNS)" and "Bharatiya Nagarik Suraksha Sanhita (BNSS)" (Relevant sections pertaining to cybercrime)
7. "Cyber Law and Cyber Crimes" by Prof. S.R. Bhansali

DCSEH-22: Fundamentals of Ethical Hacking							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Theory	04	04	Lecture	70	30 (20 / 5 / 5)	3 Hours	TEE/MTE/ Assignment/ Attendance

Instructions to paper setter for term-end theory examination: There shall be NINE questions in total. Question number one will be compulsory and will consist of SEVEN short/objective-type questions from the complete syllabus. In addition, there shall be EIGHT questions (two questions from each unit). The student will attempt one question from each unit in addition to the compulsory question. All questions will be of FOURTEEN marks each.

The paper setter will set the paper in both English and Hindi/ mixed mode languages. Accordingly, students can also write the answers the same way.

Course Objectives:

To understand the fundamentals of ethical hacking.
To learn reconnaissance and footprinting techniques.
To perform vulnerability assessment and penetration testing.

Course Outcomes:

CO1: Understand the phases and methodologies of ethical hacking and penetration testing.
CO2: Utilize tools and techniques for reconnaissance and network scanning to gather information about targets.
CO3: Explain common system hacking techniques and exploitation concepts.
CO4: Describe vulnerabilities in wireless networks and common social engineering attacks, along with their countermeasures.

CO-PO Matrix:

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	1	1	3	2	-	-	-
CO2	2	2	2	3	-	-	-	-
CO3	2	1	1	3	-	-	-	1
CO4	2	1	-	2	1	-	-	-

Detailed Syllabus:

Unit 1: Ethical Hacking and Malware Fundamentals

Ethical Hacking vs. Malicious Hacking
Types of Hackers: White Hat, Black Hat, Grey Hat
Hacking Phases: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks
Legal and Ethical Considerations
Penetration Testing: Scope, Rules of Engagement
Introduction to Malware: Types, Characteristics, Propagation
Anti-malware Techniques: Antivirus, EDR

Unit 2: Reconnaissance, Scanning, and Exploitation

Passive and Active Reconnaissance
Footprinting Techniques and Tools
Network Scanning with Nmap (port, OS detection, service enumeration)
Vulnerability Assessment Tools: Nessus, OpenVAS (conceptual overview)
Enumeration Techniques: SNMP, LDAP, SMTP
Password Attacks: Brute-force, Dictionary, Rainbow Tables
Tools: John the Ripper, Hydra (overview)

Unit 3: Wireless Hacking, Social Engineering, and Security Tools

Wireless Security Protocols: WEP, WPA/WPA2/WPA3
Wireless Hacking Tools: Aircrack-ng Suite (conceptual)
Social Engineering Attacks: Pretexting, Phishing, Tailgating, etc.
Countermeasures for Social Engineering
Network Analysis: Wireshark, Snort/Suricata (conceptual)
Kali Linux Tools Overview
Penetration Testing Tools: Burp Suite, Hydra, John the Ripper (overview)

Suggested Readings and Resources:

1. EC-Council. *Certified Ethical Hacker (CEH) Official Courseware*.
2. Michael Sikorski, Andrew Honig. *Practical Malware Analysis*.
3. Kali Linux Documentation and Offensive Security Resources.

DCSEH-23: Threat Monitoringand Penetration Testing Lab							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Practical	04	08	Lab-based	100	-	3 Hours	TEE (Expt, Lab record, Viva)

Course Objectives:

1. To provide extensive hands-on experience in ethical hacking methodologies, from reconnaissance to exploitation and post-exploitation.
2. To familiarize students with industry-standard cybersecurity tools for network scanning, vulnerability assessment, and penetration testing.
3. To equip students with practical skills in network traffic, performing basic malware analysis, and monitoring systems for suspicious activities.
4. To enable students to simulate and respond to real-world attack scenarios, conduct basic web application security testing.

Course Outcomes (COs):

CO1: Perform comprehensive reconnaissance and information gathering, and conduct advanced network and vulnerability scans using industry-standard tools.
CO2: Demonstrate various system exploitation techniques, including password cracking and leveraging frameworks like Metasploit, in controlled environments.
CO3: Analyze network traffic, perform basic static and dynamic malware analysis, and monitor systems for intrusions and file integrity.
CO4: Identify and test common web application vulnerabilities, analyze email headers for phishing, and apply foundational incident response techniques, including exploring SIEM tools and file recovery.

CO-PO Matrix:

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	2	2	1	3	3	1	1	1
CO2	2	2	1	3	3	1	1	1
CO3	1	2	1	3	3	1	1	1
CO4	1	1	1	2	3	2	2	2

Detailed Syllabus: The following list is only indicative.

Lab 1-2: Kali Linux Familiarization: Introduction to Kali Linux environment, basic commands, updating tools.
Lab 3-4: Information Gathering and Reconnaissance: Using whois, nslookup, dig, OSINTtools for footprinting.
Lab 5-6: Network Scanning with Nmap: Advanced Nmap usage (port scanning, OS detection, service version detection, script scanning).
Lab 7-8: Vulnerability Scanning (OpenVAS/Nessus on a VM): Setting up and running a vulnerability scan against a target machine.
Lab 9-10: Password Cracking (John the Ripper/Hydra on a VM): Cracking simple password hashes and remote login credentials.
Lab 11-12: Exploitation with Metasploit Framework (on a controlled VM): Basics of using Metasploit to exploit a known vulnerability.
Lab 13-14: Web Application Vulnerability Scanning (using Burp Suite Free Edition on a controlled web application): Identifying common web vulnerabilities like XSS, SQLi (conceptual understanding and observation).

Penetration Testing Exercises:

Lab 1: Introduction to Kali Linux and Setup of Lab Environment (VMware/VirtualBox)
Tools Used: Kali Linux, VirtualBox

Lab 2: Network Scanning and Enumeration
Tools Used: Nmap, Zenmap

Lab 3: Vulnerability Scanning and Reporting
Tools Used: Nessus, OpenVAS

Lab 4: Traffic Analysis and Packet Capturing
Tools Used: Wireshark, tcpdump

Lab 5: Password Cracking and Hash Analysis
Tools Used: John the Ripper, Hashcat

Lab 6: Static and Dynamic Analysis of Suspicious Executables
Tools Used: PE Studio, VirusTotal

Lab 7: Log Monitoring and Intrusion Detection
Tools Used: Snort, OSSEC

Lab 8: Web Application Security Testing (XSS, SQL Injection, etc.)
Tools Used: OWASP ZAP, Burp Suite

Lab 9File Integrity Monitoring and Alerting
Tools Used: Tripwire

Lab 10: Phishing Detection
Tools Used: AnyMailFinder, PhishTool

Lab 11: Exploring Incident Response with SIEM Tools
Tools Used: ELK Stack, Splunk (Free Tier)

Lab 14: Simulate an End-to-End Attack-Defense Workflow
Tools Used: Combined use of Wireshark, Nmap, Snort, Splunk

DCSEH-24: Project Work							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Practical	04	-	-	100	-	-	TEE (Project Report and Presentation/Viva)

Course Objectives: To enable students to apply their acquired knowledge and skills to a real-world cybersecurity problem or a simulated ethical hacking scenario.

Course Outcomes:

CO1: Apply theoretical and practical cybersecurity knowledge to solve a real-world problem.
CO2: Design, implement, and evaluate a cybersecurity solution or conduct a simulated security assessment.
CO3: Analyze project outcomes, identify limitations, and propose future enhancements.
CO4: Document project work effectively and present findings professionally.

CO-PO Matrix:

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	3	3	3	2	2	2	2
CO2	2	3	3	3	1	2	2	2
CO3	2	2	2	2	1	1	1	1
CO4	1	1	1	1	2	1	1	1

Detailed Syllabus: Students will work individually or in small groups (2-3 students) on a project related to cybersecurity.Project topics can include:

- Developing a security tool using Python.
- Performing a penetration test on a simulated vulnerable network/application (e.g., using DVWA, Metasploit able).
- Creating a detailed incident response plan for a hypothetical scenario.
- Implementing security hardening for a specific operating system or network.
- Research and presentation on emerging cyber threats or security technologies.

Project Type Examples:

- Penetration Testing on Simulated Network
- Android Malware Detection Using Pythonb
- IoT Security Dashboard

– Web Vulnerability Scanner

Project Phases:

Phase 1: Problem Definition and Literature Review: Identify a problem, define scope, research existing solutions.
Phase 2: Design and Planning: Design the solution architecture, plan execution steps.
Phase 3: Implementation/Execution: Develop code, configure systems, perform tests.
Phase 4: Testing and Evaluation: Test the solution, evaluate its effectiveness.
Phase 5: Documentation and Presentation: Prepare a comprehensive report, present findings, and demonstrate the project.

Sample Project Topics (Indicative List)

1. Design and Implementation of a Secure Wireless Network for a Small Office
2. Penetration Testing and Security Audit of a Simulated Web Application
3. Developing a Vulnerability Scanner for Local Network Devices
4. Building a Custom Firewall using Open Source Tools
5. Detection of Phishing Attacks using Machine Learning
6. Design of a Secure File Sharing System using Encryption
7. Developing an Android App with Built-in Anti-Malware Features
8. IoT Device Honeypot: Deploying and Logging Attacker Behavior
9. Web Application Firewall Implementation using ModSecurity
10. Simulating a Red Team vs. Blue Team Environment in a Virtual Lab
11. Creating a Threat Intelligence Dashboard with Real-Time Alerts
12. Automated Reconnaissance and Reporting Toolkit in Python
13. Digital Forensic Analysis of a Compromised Windows Machine
14. Developing a Browser Plugin to Prevent Clickjacking and XSS
15. Security Analysis of a Cloud-Based File Storage Application
16. Design of a SIEM (Security Information and Event Management) System
17. Simulation of a Social Engineering Attack and Counter-Strategies
18. Python-based Tool for Detecting SQL Injection Vulnerabilities
19. End-to-End Implementation of a Secure IoT Home Network

Note: Work on the project will start at the outset of the second semester.