JECRC™
UNIVERSITY
BUILD YOUR WORLD

School of Engineering

Syllabi and Course Structure

B. Tech. (Computer Science & Engineering)
(Cyber Security-EC Council)

(2025-2029)
Academic Programme

July 2025

BCO173B	**Certified Secure Computer User**	**2-0-0 [2]**

Course Outcomes:

CO1: Understand the need and importance of data security.

CO2: Ability to implement Operating System security measures.

CO3: Understand the threats associated with email communications and safeguarding against them.

CO4: Ability to make informed decisions for securing cloud, mobile devices and network connections.

CO5: Knowledge of Data Backup and Disaster Recovery.

Syllabus:

Module	**Topics**
Module 1. Introduction To Data Security	●Data–Digital Building Blocks ● Importance of Data in the Information Age ● Threats to Data ● Data Security ● Potential Losses Due to Security Attacks ● Implementing Security
Module 2. Securing Operating Systems	● Guidelines to Secure Windows ● Guidelines to Secure Mac OS X
Module 3. Malware and Antiviruses	● What is Malware ● Types of Malware ● Symptoms of Malware Infection ● Antivirus ● Configuring and Using Antivirus Software ● How to Test If an Antivirus is Working
Module 4. Internet Security	● Understanding Web Browser Concepts ● Understanding IM Security ● Understanding Child Online Safety
Module 5. Security On Social Networking Sites	● Understanding Social Networking Concepts ● Understanding Various Social Networking Security Threats ● Understanding Facebook Security Settings ● Understanding Twitter Security Settings
Module 6. Securing Email Communications	● Understanding Email Security Concepts ● Understanding Various Email Security Threats ● Understanding Various Email Security Procedures
Module 7. Securing Mobile Devices	● Understanding Mobile Device Security Concepts ● Understanding Threats to a Mobile Device ● Understanding Various Mobile Security Procedures ● Understanding How to Secure iPhone and iPad Devices ● Understanding How to Secure Android Devices ● Understanding How to Secure Windows Device ● Mobile Security Tools

Module 8. Securing The Cloud	● The Concept of Cloud ● How Cloud Works ● Threats to Cloud Security ● Safeguarding Against Cloud Security Threats ● Cloud Privacy Issues ● Addressing Cloud Privacy Issues ● Choosing a Cloud Service Provider
Module 9. Securing Network Connections	● Understanding Various Networking Concepts ● Understanding Setting Up a Wireless Network in Windows ● Understanding Setting Up a Wireless Network in Mac ● Understanding Threats to Wireless Network Security and Countermeasures ● Measures to Secure Network Connections
Module 10. Data Backup and Disaster Recovery	● Data Backup Concepts ● Types of Data Backups ● Windows Backup and Restore Procedures ● MAC OS X Backup and Restore Procedures ● Understanding Secure Data Destruction

CO-PO Mapping:

Course Outcomes	***Program Outcomes***												***Program Specific Outcomes***		
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	PSO1	PSO2	PSO3
CO1	L	M	M	H	H	M		H	M	L		H	H	H	H
CO2	L	M	M	H	H	M		H	M	L		H	H	H	H
CO3	L	M	M	H	H	M		H	M	L		H	H	H	H
CO4	L	M	M	H	H	M		H	M	L		H	H	H	H
CO5	L	M	M	H	H	M		H	M	L		H	H	H	H

BCO506A	**INTRODUCTION TO LINUX LAB**	**0-0-2 (1)**

List of Experiments

1. Comparison between Linux and other Operating Systems, Applications of Linux Operating System.
2. Linux Architecture- Shell, Kernel, System calls.
3. Internal & External commands in Linux.
    - Internal commands- echo, type, etc.
    - External commands- ls, cp, mv, rm, cat, etc
    - Other commands –clear, who, cal, date, bc, man, passwd
4. Working with files & directories.
    - Know the categories of files.
    - Directory related Commands – pwd, mkdir, rmdir, cd, ls
    - Manipulating Absolute paths and Relative paths using cd command.
    - File related Commands – cat, cp, mv, rm, comm, cmp, diff, tar, umask, wc
5. Basic File attributes.
    - Listing attributes of a file: ls and its options
    - File Permissions: Absolute and Relative permissions
    - Manipulating File permissions using chmod command
    - Manipulating File ownership using chown command
    - Manipulating Hard-link and Soft-link using ln command
6. Learn to use vi editor.
    - Three modes of vi editor.
    - Input mode commands.
    - Command mode commands.
    - Ex mode commands.
7. Process Management commands.
    - Process creation, status, Identifying process, ps -f &its options,
    - Running process in background, Job control, and Process termination.
    - Changing process priority, scheduling process (Usage of sleep and wait commands)
8. Introduction to shell programming.

Course Outcome (CO):

At the end of this course, students will demonstrate ability to:

CO1: Identify and use UNIX/Linux utilities

CO2: Effectively use the UNIX/Linux system to accomplish typical personal, office, technical, and software development tasks.

CO3: Understand the concepts of process and related commands.

CO4: Describe the basic file system in Linux and its file attributes.

CO5: Understand the commands related to Shell programming.

BCO 339A	**EC-Council Certified Security Specialist**	**4-0-0 [4]**

Course Outcomes:

CO1: Identify information security threats which reflect on the security posture of the organization

CO2: Knowledge of networks and various components of the OSI and TCP/IP model

CO3: Identify different types of cryptographic principles, cryptography attacks, and cryptanalysis tools.

CO4: Fundamentals of ethical hacking and pen testing

CO5: Understanding E-mail crime, computer forensics and writing investigative reports

Syllabus:

Module 1	Information Security Fundamentals
Module 2	Networking Fundamentals
Module 3	Secure Network Protocols
Module 4	Information Security Threats and Attacks
Module 5	Social Engineering
Module 6	Hacking Cycle
Module 7	Identification, Authentication, and Authorization
Module 8	Cryptography
Module 9	Firewalls
Module 10	Intrusion Detection System
Module 11	Data Backup
Module 12	Virtual Private Network
Module 13	Wireless Network Security
Module 14	Web Security
Module 15	Ethical Hacking and Pen Testing
Module 16	Incident Response
Module 17	Computer Forensics Fundamentals
Module 18	Digital Evidence
Module 19	Understanding File Systems
Module 20	Windows Forensics
Module 21	Network Forensics and Investigating Network Traffic
Module 22	Steganography
Module 23	Analyzing Logs
Module 24	E-mail Crime and Computer Forensics
Module 25	Writing Investigative Report

CO-PO Mapping:

Course Outcomes	***Program Outcomes***												***Program Specific Outcomes***		
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	PSO1	PSO2	PSO3
CO1	L	M	M	H	H	M		H	M	L		H	H	H	H
CO2	L	M	M	H	H	M		H	M	L		H	H	H	H
CO3	L	M	M	H	H	M		H	M	L		H	H	H	H
CO4	L	M	M	H	H	M		H	M	L		H	H	H	H
CO5	L	M	M	H	H	M		H	M	L		H	H	H	H

BCO 317A	Certified Network Defender	4-0-0 [4]

Course Outcomes:
CO1: Ability to understand network security management
CO2: Ability to deploy Security Devices
CO3: Ability to implement Host Security
CO4: Ability to secure the Network Perimeter
CO5: Ability to respond to Incidents in network

Syllabus:

Module 01: **Network Attacks and Defence Strategies**	This module introduces you to different network-based attacks faced by the organization to understand their working and develop Defence strategies.
Module 02: **Administrative Network Security**	It involves developing or updating security infrastructure and continuously monitoring networks for any suspicious actions or unauthorized access
Module 03: **Technical Network Security**	Implementing authentication and protection controls for user verification to avoid theft of sensitive information or data. Introducing the concept of zero trust and its effectiveness in maintaining a better security posture
Module 04: **Network Perimeter Security**	Implementation and management of perimeter devices like firewalls, Intrusion Detection Systems, Intrusion Prevention Systems
Module 05: **Endpoint Security-Windows Systems**	Security of end-user devices and entry points by implying endpoint security on Windows devices.
Module 06: **Endpoint Security-Linux Systems**	Securing entry points or end-user devices by ensuring endpoint security on Linux devices
Module 07: **Endpoint Security- Mobile Devices**	Securing entry points or end-user devices by ensuring endpoint security on mobile devices
Module 08: **Endpoint Security-IoT Devices**	Fundamentals of IoT, IoT threats and security using endpoint security implementation
Module 09: **Administrative Application Security**	Understanding the methodologies of administrative application security and its importance to minimize the security-related vulnerabilities in the application
Module 10: **Data Security**	Implementing policies to safeguard data from unauthorized access using various techniques like encryption, hashing, tokenization, and other key management practices. Concept of data storage, data classification, data masking, retention and destruction

Module 11: **Enterprise Virtual Network Security**	In-depth understanding of virtualization, related threats, and security. Essentials of software-defined network (SDN) security, network function virtualization (NFV) security
Module 12: **Enterprise Cloud Network Security**	Introduction to cloud computing, threats, challenges and security across cloud platforms, concepts of container security, docker security, and Kubernetes security
Module 13: **Enterprise Wireless Network Security**	Understanding of wireless network security essentials, threats, attacks, and countermeasures.
Module 14: **Network Traffic Monitoring and Analysis**	Analysis and monitoring of logs from various perimeter network devices to identify any anomalies in the traffic.
Module 15: **Network Logs Monitoring and Analysis**	Analyzing the events generated by various devices in the network to identify signs of any suspicious activity or a potential incident
Module 16: **Incident Response and Forensic Investigations**	Understanding of incident management response process and methodologies to be followed in case of security incidents. Understanding of forensics investigation techniques and tools used for analysis.
Module 17: **Business Continuity and Disaster Recovery**	Understanding the importance of BCP and DR, related concepts and procedures required to allow smooth functioning of operations in case of a disaster
Module 18: **Risk Anticipation with Risk Management**	Risk management process, analyzing various risks that the organization is susceptible to and developing policies to manage them.
Module 19: **Threat Assessment with Attack Surface Analysis**	Analyzing the threats and attack vectors to develop solutions for their countermeasures
Module 20: **Threat Prediction with Cyber Threat Intelligence**	Developing a proactive approach by understanding various frameworks aiding in threat intelligence to anticipate the kinds of attacks hackers could use to gain access to the network.

CO-PO Mapping:

Course Outcomes	***Program Outcomes***												***Program Specific Outcomes***		
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	PSO1	PSO2	PSO3
CO1	L	M	M	H	H	M		H	M	L		H	H	H	H
CO2	L	M	M	H	H	M		H	M	L		H	H	H	H
CO3	L	M	M	H	H	M		H	M	L		H	H	H	H
CO4	L	M	M	H	H	M		H	M	L		H	H	H	H
CO5	L	M	M	H	H	M		H	M	L		H	H	H	H

BCO652A	INTRODUCTION TO CYBER CRIMES & LAW	3-0-0 [3]

OBJECTIVES:

- Understand the fundamentals of cyber law and cyber security, including the scope, jurisdiction, and differences between cyber and conventional crimes.
- Identify and analyze various types of cyber-crimes and threats, such as phishing, hacking, cyber terrorism, IoT attacks, and digital frauds.
- Interpret legal and regulatory frameworks, including the IT Act, electronic records, digital signatures, and data protection laws like GDPR and Indian regulations.

UNIT 1	**Introduction to Cyber World**: Introduction to Cyber World, Cyber Security V/s Cyber Law, Types of Cyber Threats, Difference between Cyber Crimes and Conventional Crimes, Areas Comes under Cyber Law, Jurisdiction area of cyber law
UNIT 2	**Cyber Crimes**: Piracy, Phishing, hacking of information, Data Breach, CSS Attacks, Cyber Harassments, SQL Injection, Identity Hack, Cyber terrorism, DOS, Insider Attacks, Dark Web using TOR, Credit Card/Debit Card/UPI Hackings, Cyber Stalking, Cyber bullying, Eaves dropping attack, online libel/slander, Social Engineering, Cryptojacking, Virtual Currency Fraud, Vishing (Voice phising), IOT Attacks, Phone Hacking.
UNIT 3	**Definitions under IT Act, 2000**: Concept of Internet, Web Centric Business, E-Business, Electronic Governance, Cyber jurisdiction. Contemporary Business, Issues in Cyber Space, Security risks: Instant messaging platform, social networking sites, mobile applications and Internet of Things (IOT). Domain name dispute and their resolution, E- forms; EMoney, Electronic Money Transfer, Privacy of Data and Secure Ways of Operation in Cyber Space.
UNIT 4	**Electronic Records**: Authentication of Electronic Records; Legal Recognition of Electronic Records; Legal Recognition of Digital Signatures; Applications and usage of electronic records and Digital Signatures in Government and its Agencies; Retention of Electronic Records, Intermediaries and their liabilities; Attribution, Acknowledgement and Dispatch of Electronic Records, Secure Electronic Records and Digital Signature
UNIT 5	**Regulatory Framework**: Regulation of Certifying Authorities; Appointment and Functions of Controller; License to issue Digital Signatures Certificate; Renewal of License; Controller's Powers; Procedure to be Followed by Certifying Authority; Issue, Suspension and Revocation of Digital Signatures Certificate, Duties of Subscribers; Penalties and Adjudication; Appellate Tribunal; Offences; Overview of GDPR and Indian data protection regime.

Course Outcomes:

- **CO1:** Understand the foundational concepts of the cyber world, key differences between cyber law and cyber security, and jurisdictional aspects of cyber law.
- **CO2:** Identify and assess various forms of cyber crimes, attack methods, and emerging threats in the digital ecosystem.
- **CO3:** Interpret key definitions and provisions of the IT Act, 2000, and analyze cyber risks in modern digital platforms and technologies.
- **CO4:** Explain the legal recognition, authentication, and use of electronic records and digital signatures in cyberspace.

- **CO5:** Evaluate the regulatory framework for certifying authorities, digital signature management, cyber offences, and data protection laws.

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	M	M				M		H				M	H		M
CO2	H	H			M	H		H				M	H	M	H
CO3	H	H			M	H		H				M	H	M	H
CO4		M			H	M		H				M	M	M	
CO5	M	H				H	M	H			M	H	H		M

TEXT BOOKS:

1. Godbole, N., & Belapure, S. (2011). Cyber security: Understanding cyber crimes, computer forensics and legal perspectives. New Delhi, India: Wiley India Pvt. Ltd.
2. Narasimham, S. V. L., & Janakiraman, T. A. (2013). Information security and cyber laws. Cengage Learning India Pvt. Ltd.

REFERENCE BOOKS:

1. Gupta, M. (2019). Information security and cyber laws. New Delhi, India: Khanna Publishing.
2. Talat, F. (2016). Cyber law in India. Kluwer Law International.
3. Sharma, V. (2020). The Information Technology Act, 2000: Bare act with short comments. New Delhi, India: Universal Law Publishing.
4. Bansal, A. (2018). Fundamentals of cyber security. New Delhi, India: Pearson Education.

BCO 434A	**INFORMATION SECURITY**	**3-0-0 [3]**

Objectives:

- To explain the objectives of information security
- To analyse the trade-offs inherent in security
- To describe the enhancements made to IPv4 by IPSec
- To understand the basic categories of threats to computers and networks
- To discuss issues for creating security policy for a large organization

UNIT 1	Information Security: Introduction, History of Information security, What is Security, CNSS Security Model, Components of Information System, Balancing Information Security and Access, Approaches to Information Security Implementation, The Security Systems Development Life Cycle.
UNIT 2	Cryptography: Concepts and Techniques, symmetric and asymmetric key cryptography, steganography, Symmetric key Ciphers: DES structure, DES Analysis, Security of DES, variants of DES
UNIT 3	Message Authentication and Hash Functions: Authentication requirements and functions, MAC and Hash Funtions, MAC Algorithms: Secure Hash Algorithm, Whirlpool, HMAC, Digital signatures, X.509, Kerberos
UNIT 4	Security at layers(Network, Transport, Application): IPSec, Secure Socket Layer(SSL), Transport Layer Security(TLS), Secure Electronic Transaction(SET), Pretty Good Privacy(PGP), S/MIME
UNIT 5	Inruders, Virus and Firewalls: Intruders, Intrusion detection, password management, Virus and related threats, Countermeasures, Firewall design principles, Types of firewalls

COURSE OUTCOMES:

CO1: Explain the objectives of information security and analyze the importance of information Security in real world.

CO2: Analyse the trade-offs inherent in security and designing and analysis of different encryption Algorithms.

CO3: Implementation of MAC and Hash functions, security at different layers of a network

CO4: Understand the basic categories of threats to computers and networks and explore different types of intruders and viruses.

CO5: Discuss issues for creating security policy for a large organization

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcom e	**Program Outcome**												**Program Specific Outcome**		
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO1 2	PSO 1	PSO 2	PSO 3
CO1	H	H					M					M			M
CO2	H	H	H	M								M		M	
CO3	H			L									H		
CO4	L				H						M			L	
CO5	M				H	H	H	M		L	M				M

H = Highly Related; M = Medium L=Low

Text Books:

1. Stalling Williams: Cryptography and Network Security: Principles and Practices, 4th Edition,
Pearson Education, 2006.
2. Kaufman Charlie et.al; Network Security: Private Communication in a Public World, 2nd Ed.,
PHI/Pearson.

Reference Books:

1. Pieprzyk Josef and et.al; Fundamentals of Computer Security, Springer-Verlag, 2008.
2. Trappe & Washington, Introduction to Cryptography, 2nd Ed. Pearson.

BCO 435A	**INFORMATION SECURITY LAB**	**0-0-1 [1]**

1. Write a python program to allow user input for a CNSS model component and display a brief description of its role.
2. Write a python program to create a dictionary of information system components and let the user query their definitions.
3. Write a python program to implement a basic Caesar cipher for encrypting and decrypting short messages.
4. Write a python program to simulate sharing a symmetric key between two parties using simple input/output.
5. Write a python program to hide a secret word within an ordinary sentence (basic text steganography) and retrieve it.
6. Write a python program to generate a SHA256 hash of a given text input.
7. Write a python program that calculates and displays the MD5 hash of a password entered by the user.
8. Write a python program to generate a random password of specified length and display it to the user.
9. Write a python program that checks if a password meets minimum strength requirements and prints validation results.
10. Write a python program to prompt for a password and display possible common character substitutions for strengthening.
11. Write a python program that scans a fake log file and prints all entries that contain the phrase "failed login".
12. Write a python program to simulate checking if a password was leaked (fake dataset).
13. Write a python program to create a simple strength meter that ranks a password as “weak,” “medium,” or “strong” based on length and diversity.
14. Write a python program to model basic allow/block firewall logic: let the user input IPs and say if they are allowed or blocked, based on a list.

Course Outcomes:

CO 1. Implement basic and intermediate encryption techniques.
CO 2. Automate cybersecurity tasks using Python scripts.
CO 3. Solve real-world security problems with Python.
CO 4. Simulate security models using Python programming.
CO 5. Analyze security data and detect threats effectively.

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcome	**Program Outcome**												**Program Specific Outcome**		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	M	H	M	M	M					M			H	M	L
CO2		M		M	H					M			H	H	L
CO3	M	H	M	M	M					M			H	M	L
CO4	M	M	M	H	M					M			H		L
CO5	M	H	M	M	M					H			H		L

H = Highly Related; M = Medium L=Low

BCO 319A	Certified Ethical Hacker	4-0-0 [4]

Course Outcomes:

CO1: Identify legal and ethical issues related to vulnerability and penetration testing.
CO2: Plan vulnerability assessment and penetration test for a network.
CO3: Determine ways to assess the effectiveness of security policies and procedures.
CO4: Evaluate various techniques and tools used in network scanning.
CO5: Describe best practices for securing Android, iOS, and Windows OS devices.

Syllabus:

Module 01: Introduction to Ethical Hacking	Elements of Information Security, Cyber Kill Chain Methodology, MITRE ATT&CK Framework, Hacker Classes, Ethical Hacking, Information Assurance (IA), Risk Management, Incident Management, PCI DSS, HIPPA, SOX, GDPR
Module 02: Footprinting and Reconnaissance	Foot printing on the target network using search engines, web services, and social networking sites. Website, email, whois, DNS, and network foot printing on the target network
Module 03: Scanning Networks	Perform host, port, service, and OS discovery on the target network. Perform scanning on the target network beyond IDS and firewall
Module 04: Enumeration	NetBIOS, SNMP, LDAP, NFS, DNS, SMTP, RPC, SMB, and FTP Enumeration
Module 05: Vulnerability Analysis	Vulnerability research using vulnerability scoring systems and databases. Vulnerability assessment using various vulnerability assessment tools
Module 06: System Hacking	Online active online attack to crack the system’s password. Buffer overflow attack to gain access to a remote system. Escalate privileges using privilege escalation tools. Escalate privileges in linux machine. Hide data using steganography. Clear Windows and Linux machine logs using various utilities. Hiding artifacts in Windows and Linux machines
Module 07: Malware Threats	Malware, Components of Malware, APT, Trojan, Types of Trojans, Exploit Kits, Virus, Virus Lifecycle, Types of Viruses, Ransomware, Computer Worms, Fileless Malware, Malware Analysis, Static Malware Analysis, Dynamic Malware Analysis, Virus Detection Methods, Trojan Analysis, Virus Analysis, Fileless Malware Analysis, Anti-Trojan Software, Antivirus Software, Fileless Malware Detection Tools
Module 08: Sniffing	Network Sniffing, Wiretapping, MAC Flooding, DHCP Starvation Attack, ARP Spoofing Attack, ARP Poisoning, ARP Poisoning Tools, MAC Spoofing, STP Attack, DNS Poisoning, DNS Poisoning Tools, Sniffing Tools, Sniffer Detection Techniques, Promiscuous Detection Tools
Module 09: Social Engineering	Social Engineering, Types of Social Engineering, Phishing, Phishing Tools, Insider Threats/Insider Attacks, Identity Theft

Module 10: Denial-of-Service	DoS Attack, DDoS Attack, Botnets, DoS/DDoS Attack Techniques, DoS/DDoS Attack Tools, DoS/DDoS Attack Detection Techniques, DoS/DDoS Protection Tools
Module 11: Session Hijacking	Session Hijacking, Types of Session Hijacking, Spoofing, Application-Level Session Hijacking, Man-in-the-Browser Attack, Client-side Attacks, Session Replay Attacks, Session Fixation Attack, CRIME Attack, Network Level Session Hijacking, TCP/IP Hijacking, Session Hijacking Tools, Session Hijacking Detection Methods, Session Hijacking Prevention Tools
Module 12: Evading IDS, Firewalls, and Honeypots	Bypass Windows Firewall. Bypass firewall rules using tunnelling. Bypass antivirus
Module 13: Hacking Web Servers	Web Server Operations, Web Server Attacks, DNS Server Hijacking, Website Defacement, Web Cache Poisoning Attack, Web Server Attack Methodology, Web Server Attack Tools, Web Server Security Tools, Patch Management, Patch Management Tools
Module 14: Hacking Web Applications	Web Application Architecture, Web Application Threats, OWASP Top 10 Application Security Risks – 2021, Web Application Hacking Methodology, Web API, Webhooks, and Web Shell, Web API Hacking Methodology, Web Application Security
Module 15: SQL Injection	SQL Injection, Types of SQL injection, Blind SQL Injection, SQL Injection Methodology, SQL Injection Tools, Signature Evasion Techniques, SQL Injection Detection Tools
Module 16: Hacking Wireless Networks	Wireless Terminology, Wireless Networks, Wireless Encryption, Wireless Threats, Wireless Hacking Methodology, Wi-Fi Encryption Cracking, WEP/WPA/WPA2 Cracking Tools, Bluetooth Hacking, Bluetooth Threats, Wi-Fi Security Auditing Tools, Bluetooth Security Tools
Module 17: Hacking Mobile Platforms	Mobile Platform Attack Vectors, OWASP Top 10 Mobile Risks, App Sandboxing, SMS Phishing Attack (SMiShing), Android Rooting, Hacking Android Devices, Android Security Tools, Jailbreaking iOS, Hacking iOS Devices, iOS Device Security Tools, Mobile Device Management (MDM), OWASP Top 10 Mobile Controls, Mobile Security Tools.
Module 18: IoT Hacking	IoT Architecture, IoT Communication Models, OWASP Top 10 IoT Threats, IoT Vulnerabilities, IoT Hacking Methodology, IoT Hacking Tools, IoT Security Tools, IT/OT Convergence (IIOT), ICS/SCADA, OT Vulnerabilities, OT Attacks, OT Hacking Methodology, OT Hacking Tools, OT Security Tools
Module 19: Cloud Computing	Cloud Computing, Types of Cloud Computing Services, Cloud Deployment Models, Fog and Edge Computing, Cloud Service Providers, Container, Docker, Kubernetes, Serverless Computing, OWASP Top 10 Cloud Security Risks, Container and Kubernetes Vulnerabilities, Cloud Attacks, Cloud Hacking, Cloud Network Security, Cloud Security Controls, Cloud Security Tools
Module 20: Cryptography	Cryptography, Encryption Algorithms, MD5 and MD6 Hash Calculators, Cryptography Tools, Public Key Infrastructure (PKI), Email Encryption, Disk Encryption, Cryptanalysis, Cryptography Attacks, Key Stretching

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcomes	***Program Outcomes***												***Program Specific Outcomes***		
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	PSO1	PSO2	PSO3
CO1	L	M	M	H	H	M		H	M	L		H	H	H	H
CO2	L	M	M	H	H	M		H	M	L		H	H	H	H
CO3	L	M	M	H	H	M		H	M	L		H	H	H	H
CO4	L	M	M	H	H	M		H	M	L		H	H	H	H
CO5	L	M	M	H	H	M		H	M	L		H	H	H	H

BCO 188A	Cyber Forensic & investigation	3-0-0 (3)

Objective:

- To study the fundamentals of Computer Forensics
- To learn, analyze and validate Forensics Data
- To study the tools and tactics associated with Cyber Forensics

UNIT 1	File systems, Microsoft file structure, Examining NTFS disks, Microsoft BitLocker, Third Party Disk Encryption Tools, Windows Registry, Start-up Tasks, Virtual Machines, Macintosh file structure and boot process, UNIX and Linux disk structures and boot processes. Other Disk structures (CD, SCSI, IDE and SATA devices)
UNIT 2	Commercial Forensic Tools (Encase, FTK), Advanced Features of forensic tools (search, encryption and decryption, data carving), windows registry, memory analysis, advanced file system analysis (deleted and hidden data, metadata, temporary file, unknown\executable file analysis), applied decryption.
UNIT 3	Graphic files: recognition, lossless and lossy data compression, locating and recovering graphic files, Identifying unknown file formats.
UNIT 4	Virtual Machines, Network Forensics, Network tools, E-mail Investigation, E-mail forensics tools, Mobile Device Forensic.
UNIT 5	Computer Investigation,Evidence acquisition, Processing crime and Incidence scene, Preserving, Analysis, Digital forensic investigation procedures, Report writing, Ethics

COURSE OUTCOMES: At the end of the course, the student should be able to:

CO1: Understand the fundamentals of Computer Forensics

CO2: Learn the issues of Data Acquisition and Data Recovery

CO3: Explore networking in cyber forensics

CO4: Learn to analyze and validate forensics data

CO5: Be familiar with forensic tools and case studies

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcome	**Program Outcome**												**Program Specific Outcome**		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H	M		H									H		
CO2	H	H				M						H	H	L	
CO3	H	H		H									M		
CO4	H	M	H		M	L		M				M		M	H
CO5	M		H		H						L				H

H = Highly Related; M = Medium L=Low

Text Books –

1. Computer Evidence - Collection and Preservation.Brown, C.L.T. Course Technology CENGAGE Learning.
2. Guide to Computer Forensics And Investigations Nelson, Bill ; Phillips, Amelia; Enfinger, Frank; Steuat, Christopher Thomson Course Technology.
3. Scene of the Cybercrime. Shinder, Debra Littlejohn and Tittel, Syngress

Reference Books:

1. Computer Forensics – Computer Crime Scene Investigation.Vacca, John R. Charles River Media
2. Bunting, Steve and William Wei. EnCase Computer Forensics: The Official EnCE: EnCase Certifed Examiner Study Guide. Sybex, 2006
3. Prosise, Chris, Kevin Mandia, and Matt Pepe. Incident Response: Computer Forensics. McGraw-Hill,
4. Casey, Eoghan, ed. Handbook of Computer Crime Investigation, Forensic Tools and Technology, Academic press
5. Carrier, Brian. File System Forensic Analysis. Addison-Wesley Professional

BCO 189A	Web and Android Security	3-0-1 [4]

OBJECTIVES:

- Introduce the concept of web application security concerns and its related issues.
- To familiarize the students with various types of analysis techniques, attacks and tools.
- To introduce the various android application architecture and Security concerns.
- To introduce the various types of mobile attacks.

UNIT 1	Web applications: Introduction to web applications, Web application hacking, Overview of browsers, extensions, and platforms.Attacks, detection evasion techniques, and countermeasures for the most popular web platforms, including IIS, Apache, PHP, and ASP.NET Attacks and countermeasures for common web authentication mechanisms, including password-based, multifactor (e.g., CAPTCHA), and online authentication services like Windows Live ID.
UNIT 2	Advanced session analysis, hijacking, and fixation techniques, cross-site scripting, SQL injection, classic categories of malicious input, Overlong input (like buffer overflows), canonicalization attacks (like the infamous dot-dot-slash), and meta characters (including angle brackets, quotes, single quote, double dashes, percent, asterisk, underscore, newline, ampersand, pipe, and semicolon), beginner-to-advanced SQL injection tools and techniques, stealth-encoding techniques and input validation/ output-encoding countermeasures.
UNIT 3	Introduction to Android Applications and Mobile App Security: History of Android, Understanding Android Hardware and Software Architecture, Understanding Android Security Model. Understanding Android Permission Model for Application Security, Sandboxing, Codesigning, Encryption, rooting Devices, Understanding APK Understanding Directories and Files on an APK 9
UNIT 4:	Mobile Application Attacks 1: Setting up Mobile App PentestingEnvironment,Interact with the Devices, Starting with Drozer,UnderstandingAndroidManifest.xml,Configuring, Burp and Traffic Interception,Traffic Interception Bypass, Weak Server Side Controls,Insecure Data Storage,Insufficient Transport Layer Protection,Unintended Data Leakage,Poor Authentication & Authorization 10
UNIT 5	Mobile Application Attacks 2: Broken Cryptography,Client Side Injections,Security Decisions via Untrusted Input,Improper Session Handling,Lack of Binary Protection,ExploitingDebuggableApplications,DeveloperBackdoor,Location spoofing to download location restricted apps,Configuring Live Device for Penetration Testing,Mitigation Approach for all Vulnerabilities.

COURSE OUTCOMES:

CO1: Learn web application security concerns and its related issues.
CO2: Develop the Secure web applicationwith helpvarious of analysis techniques and knowledge of different attacks and tools.
CO3: Understand android application architecture and Security issues.
CO4: Know about various types of mobile attacks and to deal with these attacks and develop the secure application
CO5: Able to under the concepts testing, debugging.

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcome	**Program Outcome**												**Program Specific Outcome**		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H	H		M									H		L
CO2	H	H	H		M	L				L		L	H	M	
CO3	H			L	M		L		L				H		M
CO4	H		H			L				M		L		M	
CO5	H	M	H		M	L				M		L	H	M	

Text Books:

1. Hacking Exposed Web Applications, 3rd edition, JOEL SCAMBRAY, VINCENT LIU, CALEB SIMA
2. The Web Application Hacker's Handbook Discovering and Exploiting Security Flaws By DafyddStuttard, Marcus Pinto
3. Mobile device security: A comprehensive guide to securing your information in a moving world. Boca Raton, FL: Auerbach Publications - Fried, S.

Reference Books:

1. Rich Bowen, Ken Coar, “Apache Cookbook”, O’Reilly
2. Open Web Application Security Project. A Guide to Building Secure Web Applications and Web Services. http://www.owasp.org/index.php/Category:OWASP_Guide_Project
3. 2 The web application hacker’s handbook: Discovering and exploiting security flaws (2nd ed.). Indianapolis, IN: Wiley, John & Sons - Stuttard, D. & Pinto, M.
4. Mobile application security. New York: McGraw-Hill Companies - Dwivedi, H., Clark, C., &Thiel, D.

BCO 461A	Web and Android Security Lab	3-0-1 [4]

List of Exercises:

1. Setting up Mobile App PentestingEnvironment,interact with the Devices, Starting with Drozer
2. Configuring, Burp and Traffic Interceptionof Mobile Applications between client and server
3. Configuring Live Device for Penetration Testing,Mitigation Approach for all Vulnerabilities.
4. Performing static Analysis of Mobile Application using MOBSF
5. Perform the jailbreak/Root the Android phone and get admin level Privilege by using tools such as Superoneclick, superboot.
6. PerformingCross-application scripting error in Android Browser which leads to hacking the devices.
7. Detect application communication vulnerabilities and perform exploitation usingComDroid.
8. Perform Jailbreaking on iOS Devices.
9. Unlock the iPhone using tools such as iphonesimfree and anySIM.
10. Perform a method to send Malicious Payload to the victims iPhone and check whether you can take over the control the victim's phone.
11. Perform Man-in-the-Middle attack by intercepting the Wireless parameter of iPhone on wireless network.
12. Perform social engineering Attack method and send the malicious link and SMS tricks which contains Malicious web page.
13. Develop Backdoor, Location spoofing to download location restricted apps.
14. Performing dynamic analysis to find API/Web services vulnerabilities.
15. Performing reverse engineering on android applications
16. Performing network communication attacks in Android and iOS.
17. Performing authentication and session management attacks.

Course Outcomes (COs):

CO1: Understand and configure mobile app pentesting tools and environments.
CO2: Analyze and exploit vulnerabilities in Android and iOS applications.
CO3: Perform static and dynamic analysis of mobile applications for security assessment.
CO4: Demonstrate techniques for rooting, jailbreaking, and privilege escalation on mobile devices.
CO5: Conduct network and social engineering attacks for penetration testing on mobile platforms.

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcome	**Program Outcome**												**Program Specific Outcome**		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	M	H	M	M	H					M			H	H	L
CO2		H	H	M	M					M			H	M	L
CO3	M	H	M	H	H					M			H	M	L
CO4	M	M	M	M	H					M			H		L
CO5		M		M	H					H			H		L

BCO 653A	Advanced Cyber Security Techniques	3-0-0 [3]

OBJECTIVES:

- To provide foundational knowledge of network security principles, cryptography, and system-level protections.
- To explore attacker methodologies, exploitation tactics, and motivations behind modern cyber threats.
- To equip students with techniques to detect, analyze, and respond to malicious code and intrusion attempts.

UNIT 1	Cyber Security Fundamentals: Network and Security Concepts- Information Assurance Fundamentals, Basic Cryptography, Symmetric Encryption, Public Key Encryption, The Domain Name System (DNS), Firewalls, Virtualization, Radio-Frequency Identification, Microsoft Windows Security Principles: Windows Tokens, Window Messaging, Windows Program, The Windows firewalls
UNIT 2	Attacker Techniques and Motivations: How Hackers Cover Their Tracks (Antiforensics) How and Why Attackers Use Proxies, Tunneling Techniques, Fraud Techniques, Threat Infrastructure
UNIT 3	Exploitation: Techniques to Gain a Foothold, Misdirection- Shellcode, Integer Overflow Vulnerabilities, Stack-Based Buffer Overflows, Format String Vulnerabilities, SQL Injection, Malicious PDF Files, Race Conditions, Web Exploit Tools, DoS Conditions, Brute Force and Dictionary Attacks, Reconnaissance and Disruption Methods, Cross-Site Scripting (XSS)
UNIT 4	Malicious Code: Self-Replicating Malicious Code- Worms, Viruses. Evading Detection and Elevating Privileges- Obfuscation, Virtual Machine Obfuscation, Persistent Software Techniques, Rootkits, Spyware, Attacks against Privileged User Accounts and Escalation of Privileges, Token Kidnapping, Virtual Machine Detection.
UNIT 5	Stealing Information and Exploitation- Form Grabbing, Man-in-the-Middle Attacks, DLL Injection, Browser Helper Objects Defence and Analysis Techniques: Memory Forensics, Honeypots, Malicious Code Naming, Automated Malicious Code Analysis Systems, Intrusion Detection Systems

Course Outcomes:

CO1: Understand and apply the fundamentals of network security, encryption techniques, and system-level defense mechanisms.

CO2: Analyze attacker behavior, techniques, and infrastructure used in concealing cyber activities.

CO3: Evaluate and demonstrate common exploitation techniques including buffer overflows, SQL injection, and XSS.

CO4: Identify various types of malicious code and techniques used to evade detection and escalate privileges.

CO5: Examine methods for information theft and explore defense mechanisms like memory forensics and IDS.

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H	M			H	M						M	H	M	M
CO2	H	H			H	H		M				M	H	H	H
CO3	H	H			H	M						M	H	H	H
CO4	H	H			H	M		M				M	H	H	H
CO5	H	H			H	H		M				M	H	H	H

TEXT BOOKS:

1. Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.
2. Schneier, B. (2015). Applied cryptography: Protocols, algorithms, and source code in C (20th anniversary ed.). Wiley.

REFERENCE BOOKS:

1. Mayank Bhusan, Rajkumar Singh Rathore, Aatif Jamshed, “Fundamental of Cyber Security (Principles, Theory and Practices) BPB Publications 2018.
2. Skoudis, E., & Liston, T. (2006). Counter hack reloaded: A step-by-step guide to computer attacks and effective Defences (2nd ed.). Prentice Hall.
3. Seitz, J., & others. (2021). Gray hat hacking: The ethical hacker's handbook (6th ed.). McGraw-Hill Education.
4. Bejtlich, R. (2013). The practice of network security monitoring: Understanding incident detection and response. No Starch Press.

BCO 654A	**Application of AI in Cyber Security**	**3-0-0 [3]**

OBJECTIVE:

- To study various AI terminologies in Cyber security
- Understand the various threats and attacks in cyber world
- To be familiar with different types of attacks and AI techniques to detect them
- Study and compare real-world attacks and AI to solve them
- To understand ethical challenges and enforcements of laws in Cyber attacks

UNIT 1	Introduction of AI in Cyber Security: AI, Machine learning, and Deep learning within cyber security, What AI and machine learning can do for cyber security, How AI is used in cyber security, Examples of machine learning in cyber security, Use of Artificial Intelligence in Cyber Security, The Future of Cyber security, Impact of AI on Cyber security, How They Will Shape the Future.AI systems' support to cyber security, Major techniques in the use of AI for system robustness, resilience, and response,
UNIT 2	Cyber security for AI : Classification of AI Attacks based on attack motivation, Integrity Attack, Availability Attack, Replication Attack, Confidentiality Attack , Classification of AI attacks based on target ,Classification of AI attacks based on attacker capabilities ,Handling AI Attack, Social Media Attacks , Secure AI , Available Software Resources. Case Study of Cybercrime: Official Website of Maharashtra Government Hacked, Indian Banks Lose Millions of Rupees, Parliament Attack, Pune City Police Bust Nigerian Racket, E-mail spoofing instances, The Indian Case of online Gambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.
UNIT 3	AI Techniques for Cyber Security : Introduction, Malware Detection and Analysis, Intrusion Detection Systems (IDS) , Generative Adversarial Networks, Attack Detection , Trustworthiness of data, Artificial Intelligence and Hardware Security, Consideration for adoption of AI , Typical use cases.
UNIT 4	**Applications from real world: Study of some applications** AI-powered threat detection, Detection of sophisticated cyber-attacks, Reducing Threat Response Time**, AI-based Antivirus Software, Fighting AI Threats, Email Monitoring ,U**sing machine learning to analyze mobile endpoints, to enhance human analysis and automate repetitive security tasks.
UNIT 5	Ethics and Laws in Applications of AI in Cyber world :Ethical considerations related to AI in cyber security, Standards on Cyber Security Using AI ,Current and future AI laws: accountability, audit ability, and regulatory enforcement, Existing legal frameworks in cyber security and major policy issues, Risk-assessment policies and suitability testing, privacy and data governance ,**Pitfalls of AI in cyber law.**

Course Outcome:

CO1. Understand role of AI in Cyber Security

CO2. Understand various threats and attacks in cyber world

CO3. Compare and analyze types of attacks and AI techniques to detect them

CO4. Able to understand the real world application requirement and develop it.

CO5. Understand ethical challenges and enforcements of laws for Cyber Security

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcome	**Program Outcome**												**Program Specific Outcome**		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H	M										H			
CO2	M	M										H			
CO3	H	H										H	L	M	
CO4	H	M	H					M				H	M	L	
CO5	M	M						M				H	M		

H = Highly Related; M = Medium; L = Low

Text Book:

1. Nina Godbole and SunitBelpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley

2. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018

BCO 655A	Network & Cloud Security	3-0-0 [3]

OBJECTIVES:

- To understand the principles of secure network and cloud architecture, including protocol vulnerabilities and wireless security.
- To implement layered defense strategies, risk management, and authentication models in enterprise and cloud environments.
- To develop practical skills in vulnerability assessment, penetration testing, and digital forensics in real-world security operations.

UNIT 1	Network Security and Cloud Essentials: Need for a defensible network architecture, emphasizing timely threat detection, sensitive data protection, and understanding protocol vulnerabilities, Defensible Network Architecture, Protocols and Packet Analysis, Virtualization, Cloud, and AI Essentials, Securing Wireless Networks
UNIT 2	Defence in Depth: Constituents of Risk: Confidentiality, Integrity and Availability, Strategies for Defence-in-Depth, Core Security Strategies, Defence-in-Depth in the Cloud, Zero Trust Methodology, Variable Trust, IAAA: Identification, Authentication, Authorization, Accountability, Single Sign On (SSO): Traditional On-Premise and Cloud (SAML and OAuth)
UNIT 3	Vulnerability Management and Response: Introduction to Vulnerability Assessments, Steps to Perform a Vulnerability Assessment, Criticality and Risks, Password Management, Password Techniques, Password (Passphrase) Policies, Multi-Factor Authentication, Adaptive Authentication, Privileged Access Management: On-Premise and Cloud.
UNIT 4	Penetration Testing: Introduction, Red Team, Adversary Emulation, Purple Team, External and Internal Penetration Testing, Web Application Penetration Testing, Social Engineering, Mobile Device Testing, Internet of Things Testing, Penetration Testing Process, Overview of Penetration Testing Tools (Nmap, Metasploit, Meterpreter)
UNIT 5	Security Operations and Digital Forensics: Logging Overview, Log Collection Architecture, Log Filtering, Problems with Logging Standards, Log Analysis, Log Aggregation and SIEM, Key Logging Activities, Digital Forensics in Practice, The Investigative Process, Examples of Examining Forensics Artifacts, Incident Handling Fundamentals, Multi-Step Process for Handling an Incident, Threat Hunting

Course Outcomes:

CO1: Understand defensible network architecture, cloud security essentials, and protocol analysis for secure systems.
CO2: Apply risk-based defense strategies including Zero Trust, SSO, and access control in enterprise environments.
CO3: Conduct vulnerability assessments and implement authentication and privilege management techniques.
CO4: Perform penetration testing using red/purple team approaches and common security testing tools.
CO5: Analyze logs, conduct digital forensics, and implement incident handling and threat hunting techniques.

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
CO1	H	M			H	M						M	H	M	M
CO2	H	H			H	H		H				M	H	H	H
CO3	H	H			H	M		M				M	H	H	H
CO4	H	H			H	M		M				M	H	H	H
CO5	H	H			H	H		M				M	H	H	H

Textbooks:

1. Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.
2. Stallings, W. (2020). Network security essentials: Applications and standards (6th ed.). Pearson.

Reference Books:

1. Weidman, G. (2014). Penetration testing: A hands-on introduction to hacking. No Starch Press.
2. Stuttard, D., & Pinto, M. (2011). The Web Application Hacker's Handbook: Finding and exploiting security flaws (2nd ed.). Wiley.
3. Bejtlich, R. (2013). The practice of network security monitoring: Understanding incident detection and response. No Starch Press.
4. Altheide, C., & Carvey, H. (2011). Digital forensics with open source tools. Syngress.
5. Gilman, E., & Barth, D. (2017). Zero trust networks: Building secure systems in untrusted networks. O'Reilly Media.

BCO 656A	**Advanced Cyber Security Lab**	**0-0-1 [1]**

List of Programs:

1. Writing simple Python scripts for tasks like string manipulation, reading from and writing to files, basic network communication.
2. Implementing basic encryption and decryption algorithms in Python Caesar cipher, AES, DES
3. Using python to generate and verify hashes (MD5, SHA-256) for files and messages.
4. Building a simple Python Client-Server application, understanding sockets.
5. Writing a python script to capture and analyze network packets (using libraries like Scapy or PySpark
6. Creating a web scraper in Python to gather data from websites (using BeautifulSoup, Selenium)
7. Simple penetration testing tasks using Python (Eg: port scanning, vulnerability scanning with tools like Nmap in Python.
8. Using python to interact with security-related APIs (eg. VirusTotal, Shodan)
9. Writing python scripts for basic static malware analysis (file signature analysis, string extraction).
10. Developing a simple IDS using Python.

Course Outcomes:

CO1: Develop Python scripts for string handling, file I/O operations, and implementing basic encryption/decryption.

CO2: Generate and verify cryptographic hashes and build client-server applications using sockets in Python.

CO3: Use Python to capture, analyze network traffic, and perform basic port/vulnerability scanning.

CO4: Automate data collection via web scraping and integrate Python scripts with security APIs like Shodan, VirusTotal.

CO5: Write Python scripts for basic malware analysis and build a simple intrusion detection system (IDS).

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H	M	M		H							M	H	H	M
CO2	H	H			H	M						M	H	H	M
CO3	H	H			H	M						M	H	H	H
CO4	M	M			H	M						M	H	H	H
CO5	H	H			H	M		M				M	H	H	H

BCO 657A	**Network Security Lab**	**0-0-1 [1]**

1. Study of different wireless network components and features of any one of the Mobile Security Apps.
2. Study of the features of firewall in providing network security and to set Firewall Security in windows.
3. Develop a Packet Sniffer using scapy or pyshark (Capture and analyze network packets (TCP, UDP, ICMP).
4. Develop a Protocol Vulnerability Checker (Detect weak protocols like Telnet, FTP over plain text using socket).
5. Develop a Wireless Network Scanner (List nearby Wi-Fi networks using scapy or wifi module).
6. Write a python script for CIA Triad Demonstration (File integrity checker- SHA256 hashing for integrity, encryption for confidentiality, role-based access simulation for availability).
7. Write a python script for OAuth2.0 Flow Demonstration (via requests-oauthlib).
8. Develop a Vulnerability Scanner with nmap (integration via subprocess). Scan for open ports, known services, and possible exploits.
9. Develop a Password Strength Analyzer using python
10. Develop a Email Phishing Simulator using Python and send crafted phishing emails (safely, within localhost) using smtplib.

Course Outcomes:

CO1: Examine the components of wireless networks and evaluate the security features of mobile apps and firewalls.
CO2: Develop packet sniffing and network traffic analysis tools using Python libraries like Scapy and PyShark.
CO3: Implement tools to detect insecure protocols and scan nearby wireless networks using Python scripting.
CO4: Demonstrate security concepts such as the CIA triad and OAuth 2.0 authorization using hands-on Python scripts.
CO5: Create tools for vulnerability scanning, password strength analysis, and phishing simulation in a secure setup.

MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	M	M			H	M		M				M	H	M	M
CO2	H	H			H	M						M	H	H	H
CO3	H	H			H	M						M	H	H	H
CO4	H	H			H	M		M				M	H	H	H
CO5	H	H	M		H	H		H				M	H	H	H