SYLLABUS PROPOSED FOR

DIPLOMA IN CYBER SECURITY

[NSQF LEVEL-5]

PROGRAMME EDUCATIONAL OBJECTIVES (PEO's):

1) Candidates will be equipped for entry-level professions in cybersecurity or related businesses.

2) Candidates will exhibit the ability to engage in lifelong learning and adapt to changing technology and challenges in the cybersecurity domain.

3) Candidates will demonstrate strong professional ethics, effective communication skills, and the capacity to collaborate in different groups.

4) Candidates will have the analytical and critical thinking abilities necessary to effectively identify, analyze, and resolve cybersecurity concerns.

5) Candidates will have the fundamental knowledge and abilities required to seek additional education and career advancement possibilities in cybersecurity and associated fields.

PROGRAMME OUTCOMES(PO'S):

1) Demonstrate understanding of fundamental concepts, principles, and practices in cybersecurity.

2) Apply techniques to secure information systems, protect data, and mitigate cybersecurity risks.

3) Implement measures to secure network infrastructures and defend against network-based attacks.

4) Identify and analyze cyber threats, vulnerabilities, and incidents to proactively protect systems and networks.

5) Recognize ethical, legal, and regulatory issues related to cybersecurity and adhere to professional codes of conduct.

PROGRAMME SPECIFIC OUTCOMES (PSO's):

1. Cybersecurity Fundamentals: Candidates will demonstrate a comprehensive understanding of core concepts, theories, and principles in cybersecurity, including encryption, authentication, access control, and security protocols.

2. Cyber Threat Analysis and Detection: Candidates will be proficient in identifying, analyzing, and classifying cyber threats, including malware, phishing attacks, and insider threats, using various tools and techniques.

3. Security Controls Implementation: Candidates will be able to implement security controls and measures to safeguard information systems, networks, and applications against cyber threats, vulnerabilities, and attacks.

4. Incident Response and Recovery: Candidates will possess the skills to effectively respond to cybersecurity incidents, contain breaches, conduct digital forensics investigations, and restore affected systems to normal operation.

5. Network Security Administration: Candidates will be competent in administering secure network infrastructures, configuring firewalls, intrusion detection/prevention systems (IDS/IPS), and implementing secure network architectures.

6. Secure Software Development Practices: Candidates will demonstrate proficiency in applying secure coding practices, conducting secure code reviews, and integrating security into the software development lifecycle (SDLC) to develop resilient and secure software applications.

7. Compliance and Regulatory Frameworks: Candidates will understand the legal and regulatory requirements relevant to cybersecurity, including data protection laws, industry standards (e.g., PCI DSS, HIPAA), and compliance frameworks (e.g., NIST, ISO/IEC 27001).

8. Security Awareness and Training: Candidates will possess the skills to promote cybersecurity awareness, deliver training programs, and educate stakeholders on security best practices, policies, and procedures.

EMPLOYBILITY:

A one-year cyber security diploma holder can have various employability roles depending on their skills, specialization, and experience level. Here are some potential roles they could pursue:

1. Junior Cyber Security Analyst: Assist in monitoring networks, analyzing security incidents, and implementing security measures.

2. Security Operations Center (SOC) Analyst: Work in a SOC to detect, analyze, and respond to security incidents, as well as conduct vulnerability assessments.

3. IT Security Technician: Support the implementation and maintenance of security systems, such as firewalls, antivirus software, and intrusion detection systems.

4. Security Consultant: Provide advice and recommendations to clients on improving their security posture, conducting risk assessments, and developing security policies and procedures.

5. Security Awareness Trainer: Develop and deliver training programs to educate employees about security best practices and raise awareness about potential threats.

SEMESTER I

COURSE TITLE: CYBER SECURITY TECHNIQUES

COURSE OBJECTIVES:

1. Learn about cryptographic techniques and protocols used to secure data and communications.
2. Understand the fundamental concepts and principles of cybersecurity, including threats, vulnerabilities, and risk management.
3. Understand the importance of security policies, procedures, and compliance standards in maintaining a secure computing environment.
4. Gain hands-on experience with security tools and technologies, such as firewalls, intrusion detection systems, and vulnerability scanners.
5. Explore different types of cyber-attacks, such as malware, phishing, and denial-of-service attacks, and learn how to detect and mitigate them.
6. Develop critical thinking and problem-solving skills to analyze and respond to security incidents effectively.

COURSE OUTCOMES:

1. Identify and assess security risks and vulnerabilities in computing systems and networks.
2. Implement security measures to protect against common cyber threats and attacks.
3. Use cryptographic techniques to secure data and communications.
4. Configure and deploy security tools and technologies to monitor and defend against cyber attacks.
5. Develop and implement security policies and procedures to mitigate risks and ensure compliance with industry standards and regulations.
6. Analyze and respond to security incidents, including malware infections, data breaches, and unauthorized access attempts.
7. Demonstrate knowledge of key cybersecurity concepts, terminology, and principles.
8. Communicate effectively about cybersecurity issues and solutions to technical and non-technical stakeholders.

Unit 1 (12 Hours)

Introduction to cyber security, information security, network security, application and system security, Threats to Information Systems, Information Assurance, Security Risk Analysis, Security Principles or Security Goals (CIA Principle), Security Services, Security Mechanism

Security Technique: Cryptography & Steganography, Active & Passive Attacks. Hardware & network Basics, Basic terminologies in cyber security: Cloud, Software, Domain, VPN, IP Address, Exploit, Breach, Firewall, Malware, Virus, Ransomware, Trojan Horse, Worm, Bot/Botnet, Spyware, Rootkit, DDOS, Phishing/Spear Phishing, Encryption. Security Threats - Viruses, Worms, Trojan Horse, Bombs, Trapdoors, Spoofs, E-mail viruses, Macro viruses, Malicious Software, Network and Denial of Services Attack

Unit 2: (12 Hours)

System Hacking Concepts: Gaining access, cracking passwords, vulnerability exploitation, escalating privileges, hiding files, clearing logs, Data Security Considerations: Backups, Archival Storage and Disposal of Data Security Technologies: Firewall and VPNs, Intrusion Detection, Access Control Security

Unit 3: (12 Hours)

Web Security Introduction: A web security forensic lesson, Introduction to different web attacks. Overview of N-tier web applications, Web Hacking Basics HTTP & HTTPS URL, Web under the Cover, Overview of Java security Reading the HTML source, Applet Security Servlets Security Symmetric and Asymmetric Encryptions.

Unit 4: (12 Hours)

Cloud Security: Introduction to Cloud Computing, migrating into a Cloud, Enriching the 'Integration as a Service' Paradigm for the Cloud Era, The Enterprise Cloud Computing Paradigm.

Cluster: Admin Server & Managed Server Infrastructure as a Service (IAAS) & Platform and Software as a Service (PAAS / SAAS) Virtual machines provisioning and Migration services, On the Management of Virtual machines for Cloud Infrastructures, Enhancing Cloud Computing Environments using a cluster as a Service, Secure Distributed Data Storage in Cloud Computing, Aneka, Comet Cloud, T-Systems', Workflow Engine for Clouds, Understanding Scientific Applications for Cloud Environments.

Unit-5: (12 Hours)

General Procedure adopted for Cyber Attacks: Reconnaissance: Foot printing concepts and methodology, foot printing using -search engines, web services, social networking sites, website, email, whois, DNS, network, foot printing by social engineering, foot printing tools, foot printing counter measures. Scanning: concept, host discovery, OS discovery, scanning beyond IDS and Firewall, Drawing network diagram. Enumeration: Concepts and Techniques, NetBIOS Enumeration.

Reference Books:

- Security Analysis and Portfolio Management by Donald E. Fischer
- Professional Pen Testing for Web Applications by Andres Andreu
- Foundations of Security: What Every Programmer Needs to Know by by Christoph Kern (Author), Anita Kesavan (Author), Neil Daswani
- Cloud Computing by M N Rao, PHI Publication, 1st edition.
- Cloud Computing Bible, Wiley Publication

COURSE TITLE: CYBER SECURITY TECHNIQUES – LAB

List of Practical's:

> **NOTE:** The list suggests sample program set. Hence, the concerned staff may modify the list as needed (Minimum 13).

1.Recovering the content of a virus infected storage media device.

2.Password cracking using open-source tools.

3.Learning different type of attacks.

4.Study of firewall and implementation of protection mechanism.

5.Service Development & usage over cloud using open source.

6.Managing cloud computing resources.

7.Detecting Trojan Attacks using open-source tools.

8.Implementing Foot printing using open-source tools.

9.Implementing Fingerprinting using open-source tools.

10.Implementing Poisoning & Exploitation using open-source tools.

COURSE TITLE: INTRODUCTION TO ETHICAL HACKING

COURSE OBJECTIVES:

1. Learn effective strategies for conducting ethical hacking assessments and penetration tests.
2. Understand the importance of documentation, reporting, and ethical guidelines in ethical hacking practice.
3. Understand the ethical considerations and legal framework surrounding hacking and penetration testing.
4. Gain knowledge of common hacking techniques and tools used by both attackers and ethical hackers.
5. Develop practical skills in identifying and exploiting security vulnerabilities in systems and networks.

COURSE OUTCOMES:

1. Demonstrate an understanding of the ethical and legal implications of hacking and penetration testing.
2. Identify and exploit common security vulnerabilities in systems and networks.
3. Use a variety of hacking tools and techniques to assess the security posture of target systems.
4. Analyze and interpret the results of ethical hacking assessments to prioritize and remediate vulnerabilities.
5. Communicate effectively about ethical hacking assessments, findings, and recommendations.

Unit 1: Introduction to Ethical Hacking (12 Hours)

Overview of hacking and penetration testing**,** Ethical considerations and legal framework**,** Different types of hackers and their motivations, Introduction to ethical hacking methodologies and tools

Unit 2: Information Gathering and Foot printing (12 Hours)

Passive and active reconnaissance techniques, Open-source intelligence (OSINT) gathering, Foot printing tools and methodologies, Identifying target assets and attack surface

Unit 3: Scanning and Enumeration (12 Hours)

Network scanning techniques and tools, Host discovery and enumeration, Service enumeration and version detection, Vulnerability scanning and assessment

Unit 4: Exploitation and post-exploitation (12 Hours)

Common attack vectors and exploitation techniques, exploiting web applications and servers, Privilege escalation and lateral movement, maintaining access and covering tracks

Unit 5: Reporting and Ethics (12 Hours)

Documentation and reporting of ethical hacking assessments, Ethical guidelines and codes of conduct for ethical h ackers, Legal considerations and liabilities, Career paths and professional certifications in ethical hacking

Reference Books:

1. "CEH Certified Ethical Hacker All-in-One Exam Guide" by Matt Walker
2. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto
3. "Metasploit: The Penetration Tester's Guide" by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni
4. "Hacking: The Art of Exploitation" by Jon Erickson
5. "Penetration Testing: A Hands-On Introduction to Hacking" by Georgia Weidman
6. "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy" by Patrick Engebretson

COURSE TITLE: COMPUTER NETWORKS AND SECURITY

COURSE OBJECTIVES:

1. To understand the basic principles and concepts of computer networks.
2. To comprehend the principles of network security and common security threats.
3. To analyze and evaluate different security mechanisms and technologies.
4. To apply network security techniques to design and implement secure networks.
5. To develop critical thinking and problem-solving skills in the context of network security.

COURSE OUTCOMES:

1. Describe the architecture and components of computer networks.
2. Analyze network protocols and their functions.
3. Identify common network security threats and vulnerabilities.
4. Design and configure firewalls and intrusion detection systems.
5. Develop network security policies to mitigate security risks.
6. Evaluate the effectiveness of network security measures.
7. Apply cryptographic techniques for ensuring data confidentiality and integrity.
8. Implement authentication and access control mechanisms.

Unit I: Introduction to Computer Network (12 Hours)

Fundamentals of Computer Networks- Definition of computer networks, Types of networks (LAN, WAN, MAN, etc.), Network architectures (client-server, peer-to-peer, etc.)

Network Models: OSI and TCP/IP - Overview of OSI (Open Systems Interconnection) model, Overview of TCP/IP model, Comparison between OSI and TCP/IP models

Data Transmission and Network Protocols - Basics of data transmission (encoding, modulation, etc.), Introduction to common network protocols (TCP, UDP, HTTP, etc.), Packet switching vs. circuit switching

Unit II: Network Security Fundamentals (12 Hours)

Basics of Network Security- Definition and importance of network security, Threats and vulnerabilities in computer networks, Security goals: confidentiality, integrity, availability (CIA triad)

Cryptography in Network Security- Introduction to cryptography, Symmetric and asymmetric encryption, Hash functions and digital signatures

Authentication, Authorization, and Access Control- Principles of authentication and authorization, Access control mechanisms (DAC, MAC, RBAC), Multi-factor authentication (MFA)

Unit III: Network Protocols and Technology (12 Hours)

Common Network Protocols - Detailed study of TCP/IP suite (IP, TCP, UDP, ICMP, etc.), Application layer protocols (HTTP, FTP, SMTP, etc.), Network layer protocols (IPv4, IPv6, ICMP)

IP Addressing and Subnetting - Basics of IP addressing (IPv4 and IPv6), Subnetting and supernetting, Private and public IP addresses

Routing and Switching - Routing algorithms (distance vector, link-state), Introduction to routers and switches, VLANs (Virtual LANs) and VLAN trunking

Unit IV: Network Security Mechanisms (12 Hours)

Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) - Types of firewalls (packet filtering, stateful inspection, etc.), Intrusion detection vs. intrusion prevention, Configuration and management of firewalls and IDS/IPS

Virtual Private Networks (VPNs) and Secure Remote Access - Principles of VPNs and tunneling protocols (IPsec, SSL/TLS), Remote access VPN vs. site-to-site VPN, Secure Socket Layer (SSL) and Transport Layer Security (TLS)

Network Security Best Practices - Security policies and procedures, Security awareness training, Incident response planning and execution

Unit V: Secured Network Management and Incident Response (12 Hours)

Network Management Protocols and Tools - SNMP (Simple Network Management Protocol), Syslog and log management, Network monitoring tools (Wireshark, Nagios, etc.)

Incident Response and Handling - Incident response phases (preparation, detection, containment, recovery, lessons learned), Handling security incidents (data breaches, malware outbreaks, etc.), Forensic investigation techniques

Security Assessment and Penetration Testing - Vulnerability assessment vs. penetration testing, Methodologies (OSSTMM, OWASP, etc.), Reporting and remediation of security vulnerabilities

Reference Books:

1. "Computer Networking: A Top-Down Approach" by James F. Kurose and Keith W. Ross
2. "Computer Networks" by Andrew S. Tanenbaum and David J. Wetherall
3. "Network Security Essentials: Applications and Standards" by William Stallings
4. "Cryptography and Network Security: Principles and Practice" by William Stallings
5. "Computer Networking: Principles, Protocols and Practice" by Olivier Bonaventure
6. "Network Security: Private Communication in a Public World" by Charlie Kaufman, Radia Perlman, and Mike Speciner
7. "Incident Response & Computer Forensics" by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia

COURSE TITLE: NETWORK PROGRAMMING - LAB

List of Practical's (Based on Computer Network and Security)

NOTE: The list suggests sample program set. Hence, the concerned staff may modify the list as needed (Minimum 13).

1.Brute force attack using open-source tools.

2. Identifying network attacks using Nmap, Metasploit.

3. Selecting a Capture Interface and creating the first pcap file using Wireshark.

4. Using Capture filters in Wireshark.

5.Finding a Text String in a Trace File using Wireshark.

6.Understanding Packet Loss and Recovery process.

7.Identifying DOS & DDOS Attack.

8. VPN & VOIP pen testing using open-source tools.

9. Demonstration of IDS using snort or any other open-source tool.

10.Demonstration of IPS using snort or any other open-source tool.

COURSE TITLE: PENETRATION TESTING WITH LINUX – LAB

OBJECTIVES:

1. Learn how to identify vulnerabilities in networks, systems, and applications.
2. Understand the fundamentals of penetration testing methodologies.
3. Understand the importance of documentation and reporting in penetration testing.
4. Gain proficiency in using Linux-based tools for penetration testing.
5. Develop skills in exploiting vulnerabilities ethically and responsibly.

OUTCOMES:

1. Proficiency in using tools like Nmap, Metasploit, Wireshark, and Burp Suite on Linux.
2. Ability to conduct comprehensive penetration tests on target systems.
3. Understanding of common vulnerabilities such as SQL injection, XSS, CSRF, etc.
4. Competence in exploiting vulnerabilities to gain unauthorized access.
5. Skill in generating detailed reports outlining findings and recommendations.
6. Enhanced understanding of network security principles and defense mechanisms.

Practical List:

NOTE: The list suggests sample program set. Hence, the concerned staff may modify the list as needed (Minimum 13).

1. Perform a network reconnaissance using Nmap to discover hosts and open ports on a target network.
2. Use Wireshark to capture and analyze network traffic, identifying potential security vulnerabilities.
3. Exploit a known vulnerability (e.g., SQL injection) in a web application using tools like SQLMap.
4. Conduct a wireless penetration test using tools like Aircrack-ng to crack WEP or WPA/WPA2 passwords.
5. Employ Metasploit to exploit a vulnerable service or application on a target system.
6. Perform a web application security assessment using Burp Suite, identifying and exploiting vulnerabilities such as XSS or CSRF.
7. Utilize Hydra or Medusa to perform password brute-force attacks against services like SSH or FTP.
8. Implement social engineering techniques (e.g., phishing) to gain unauthorized access to a system or network.
9. Set up and configure a honeypot using tools like Cowrie or Dionaea to detect and analyze malicious activity.
10. Document findings and generate a comprehensive penetration testing report, including vulnerabilities discovered, exploitation steps, and recommendations for mitigation.

Reference Books:

1. "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy" by Patrick Engebretson.
2. "Penetration Testing: A Hands-On Introduction to Hacking" by Georgia Weidman.
3. "Metasploit: The Penetration Tester's Guide" by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni.
4. "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning" by Gordon Fyodor Lyon.

COURSE TITLE: FUNDAMENTALS OF CYBER LAWS

Course Objectives:

Throughout the course, students will be expected to demonstrate their understanding of Cyber Law by being able to do each of the following:

1. Understand various key paradigms for Cyber Law and Cyber Crimes.
2. Familiarize themselves with the Information Technology Act 2000 and Investigations in Cyber Crimes.
3. Understand the Human Rights Perspective of Cyber Crimes, Precautions, and Preventions.

Course Outcomes:

After Successful completion of this course, the student would be able to:

1. Understand fundamentals of Cyber Crime and Cyber Law.
2. Describe the Impact of IT Act and Forms of Cyber Crimes.
3. Understand Computer and Cyber Crimes in the Indian Perspective.
4. Understand the Role of IT Act and Investigations in Cyber Crimes.
5. Understand Cyber Crimes Evidences and its preventions.
6. Understand Human Rights Perspective of Cyber Crime and its Prevention and Precautions.

Unit I: Information Technology and Cyber Crimes (9 Hours)

Information Technology and Cyber Crimes: An Introduction, Information Technology: Definition & Perspectives, Growth & Future, Dimensions, and Influence on Lives.

Impact of Information & Technology, Regulation of Cyberspace, Legal Aspects of Regulation, Influence of Technology on Criminality, Forms of Cyber Crimes.

Unit II: Computer & Cyber Crimes, Indian Response (9 Hours)

Computer & Cyber Crimes: Terminological Aspects, Opportunities to Cyber Criminals, Motives of Offenders, Problems affecting Prosecution, Cyber Crime: challenges and prevention control, Indian Information Act 2000, Preamble & Coverage, Nature of Offences and Penalties, Future Prospects and Needs.

Unit III: Mens Rea and Criminal Liability, Investigations in Cyber Crimes (9 Hours)

Introduction, Historical Perspectives, Mens Rea in Indian Criminal Law, Abetment of Offence, Criminal Liability and Role of Mens Rea in Indian Information Technology Act 2000, Investigations in Cyber Crimes: Implication and Challenges, Procedural Aspects, Issues, Complications & Challenges concerning Cyber Crimes, Problems and Precautionary measures for Investigations.

Unit IV: Cyber Crimes: Discovery and Appreciation of Evidences, Prevention (9 Hours)

Introduction, Law of Evidence: An Introduction, Evidences in Cyber Crime: Challenges and Implications, Computer Generated Evidences and their Admissibility, Judicial Interpretations of Computer-related Evidence, Prevention of Cyber Crimes: Introduction, International Services on Discovery and Recovery of Electronic and Internet Evidence, IOCE, OECD Initiatives, Efforts of G& and G8 Groups, Efforts of WTO, WIPO, Interpol and its measures, Efforts in India.

Unit V: Human Rights Perspectives in Cyber Crimes, Precaution and Prevention (9 Hours)

Introduction, Ideological Aspects, Fundamental rights and Civil Liberties, Various Issues and Challenges, Cyber Crime Precaution and Prevention: Introduction, Awareness and Law Reforms, Improving Criminal Justice Administration, Increasing International Cooperation, Curricular Endeavours and Checking Kids Net Addiction, Role of Guardians, Mobile Pornography, Self-Regulation in Cyberspace.

Text Book:

- Dr. Pramod Kumar Singh, Book Enclave, Jaipur, India, ISBN: 978-81-8152-163-7 “Laws on Cyber Crimes”.

Reference Books:

1. Rahul Sharma, "Cyber Law: Indian Perspective"
2. Pawan Duggal, “Text Book on Cyber Law”, Universal Law Publishing, Second Edition, 2016
3. Prashant Mali, “Cyber Law and Cyber Crimes Simplified”, Cyber Info media, 2017
4. Dr. R. K. Bangia "Cyber Law and Information Technology Act"
5. Vakul Sharma "Information Technology Law and Practice"

COURSE TITLE: INTELLECTUAL PROPERTY RIGHTS IN CYBERSPACE

COURSE OUTCOMES:

- The students once they complete their academic projects, they get awareness of acquiring the patent
- They also learn to have copyright for their innovative works.
- They also get the knowledge of plagiarism in their innovations which can be questioned legally.

UNIT I: Understanding and Overview of the IPR Regine:

Meaning of property, Origin, Nature, Meaning of Intellectual Property Rights

Introduction to TRIPS and WTO. –Intellectual Property Rights, Domain Names and Trademark Disputes: Concept of Trademarks in Internet Era, Cyber Squatting, Reverse Hijacking, Jurisdiction in Trademark Disputes **(9 hours)**

UNIT II: Copyright in the Digital Medium, Copyright in Computer Programmes, Copyright and WIPO Treaties, Concept of Patent Right, Relevant Provisions of Patent Act 1970, Sensitive Personal Data or Information (SPDI) in Cyber Law, SPDI Definition and Reasonable Security Practices in India.

(9 hours)

UNIT III: Types of Intellectual Property Rights

1. The Copyrights Act, 1957 (“Copyright Act”)
2. The Trade Marks Act, 1999 (“Trade marks Act”)
3. The Patents Act, 1970 (“Patents Act”)
4. The Design Act, 2000 (“Design Act”)
5. The Geographical Indications of Goods (Registration and Protection) Act, 1999 (“GI Act”)
6. The Protection of Plant Varieties and Farmer’s Rights Act, 2001 (“Plant Varieties Act”)
7. The Semiconductor Integrated Circuits Layout- Design Act, 2000 (“SICLD Act”)

International overview on intellectual property, international – trade mark law, copy right law, international patent law, and international development in trade secrets law. **(9 hours)**

UNIT IV: PATENT RIGHTS AND COPY RIGHTS— Origin, Meaning of Patent, Types, Inventions which are not patentable, Registration Procedure, Rights and Duties of Patentee, Assignment and licence, Restoration of lapsed Patents, Surrender and Revocation of Patents, Infringement, Remedies & Penalties **(9 hours)**

UNIT V: BASIC TENENTS OF INFORMATION TECHNOLOGY ACT-2000 – IT Act - Introduction E-Commerce and legal provisions E- Governance and legal provisions Digital signature and Electronic Signature. Cybercrimes, **(9 hours)**

HANDS-ON(LAB) SESSIONS:

NOTE: The list suggests sample program set. Hence, the concerned staff may modify the list as needed (Minimum 10).

1. **Patent Workshop**:
    - Understanding patent documentation.
    - Patent search exercises using online databases.
    - Analysis of patent claims and infringement scenarios.
2. **Trademark Workshop**:
    - Identifying trademarks and service marks.
    - Hands-on exercises for trademark searches.
    - Trademark registration process simulation.
3. **Copyright Workshop**:
    - Copyright basics and fair use principles.
    - Analyzing copyright licenses and permissions.
    - Copyright infringement case studies.
4. **Trade Secret Workshop**:
    - Understanding trade secret protection.
    - Developing strategies for protecting trade secrets within a business.
    - Case studies on trade secret misappropriation.
5. **IP Licensing and Contracts**:
    - Drafting IP licensing agreements.
    - Negotiation exercises for IP contracts.
    - Role-playing scenarios for resolving IP disputes.
6. **Enforcement and Litigation**:
    - Mock IP infringement litigation.
    - Participating in mediation and arbitration sessions.
    - Understanding the role of intellectual property in legal proceedings.
7. **IP Management and Strategy**:
    - Developing an IP strategy for a hypothetical company.
    - Analyzing case studies of successful IP management.
    - Role-playing exercises for IP portfolio management.
8. **Guest Speakers and Industry Insights**:
    - Inviting IP professionals, attorneys, or industry experts for guest lectures.
    - Q&A sessions with professionals working in IP-related fields.
    - Networking opportunities for students to connect with professionals.

REFERENCE BOOKS:

1. Intellectual Property Rights and the Law, Gogia Law Agency, by Dr. G.B. Reddy
2. Law relating to Intellectual Property, Universal Law Publishing Co, by Dr.B .L.Wadehra
3. IPR by P. Narayanan
4. Law of Intellectual Property, Asian Law House, Dr.S.R. Myneni.
5. Intellectual property right, Deborah. E. Bouchoux, Cengage learning.
6. Intellectual property right – Unleashing the knowledge economy, Prabuddha Ganguli, Tata McGraw Hill Publishing company ltd.

COURSE TITLE: INFORMATION ETHICS

COURSE OBJECTIVES:

1. Understand the concept of information ethics and its importance in contemporary society.
2. Explore the ethical implications of information technology, including privacy, security, and access.
3. Examine ethical theories and frameworks relevant to information ethics.
4. Analyze case studies and real-world examples of ethical dilemmas in information management.
5. Develop critical thinking skills to evaluate ethical issues related to information dissemination, manipulation, and control.

COURSE OUTCOMES:

1. Ability to articulate the principles and concepts of information ethics.
2. Proficiency in applying ethical theories and frameworks to analyze and resolve ethical dilemmas in information management.
3. Competence in identifying ethical issues related to information privacy, security, and access.
4. Capacity to critically evaluate the ethical implications of information technology and digital media.
5. Understanding of the cultural and global dimensions of information ethics.
6. Ability to propose strategies and policies for addressing emerging ethical challenges in the digital age.

Unit 1: Introduction to Information Ethics (9 Hours)

Definition and scope of information ethics, Historical development and theoretical foundations, Importance of information ethics in contemporary society

Unit 2: Ethical Issues in Information Technology (09 Hours)

Privacy and data protection, Security and cybersecurity, Intellectual property rights, Access to information and digital divide

Unit 3: Ethical Theories and Frameworks (9 Hours)

Utilitarianism, deontology, virtue ethics, Ethical decision-making models, Professional codes of ethics in information-related fields

Unit 4: Case Studies in Information Ethics (9 Hours)

Analysis of ethical dilemmas in information management, Ethical considerations in information dissemination, manipulation, and control, Impact of emerging technologies on ethical practices

Unit 5: Global Perspectives and Emerging Challenges (9 Hours)

Cultural differences in information ethics, Globalization and information ethics, Ethical challenges posed by artificial intelligence, big data, and social media

HANDS-ON(LAB) SESSIONS FOR INFORMATION ETHICS COURSE:

NOTE: The list suggests sample program set. Hence, the concerned staff may modify the list as needed (Minimum 10).

1. **Privacy Workshop:**
    - Have students explore privacy settings on popular social media platforms and discuss the implications of sharing personal information online.
    - Conduct a hands-on exercise where students analyze privacy policies of different websites and identify potential risks to user privacy.
2. **Data Protection Exercise:**
    - Design a hands-on activity where students learn about data protection laws and regulations.
    - Have students create and implement data protection policies for a fictional organization, considering principles like data minimization, encryption, and user consent.
3. **Digital Footprint Analysis:**
    - Ask students to conduct a hands-on analysis of their digital footprints, including social media posts, online activities, and digital interactions.
    - Guide students in reflecting on the ethical implications of their digital presence and strategies for managing their online identities responsibly.
4. **Case Study Discussions:**
    - Provide case studies related to ethical dilemmas in information management, such as data breaches, misinformation, or surveillance.
    - Facilitate hands-on group discussions where students analyze the cases, identify ethical issues, and propose solutions or ethical frameworks to address them.
5. **Ethical Decision-Making Exercise:**
    - Present students with hypothetical scenarios involving ethical challenges in information technology or digital media.
    - Engage students in a hands-on exercise where they discuss and debate the ethical considerations, weigh different perspectives, and make decisions based on ethical principles.
6. **Digital Literacy Workshops:**
    - Offer hands-on workshops on digital literacy skills, including critical thinking, media literacy, and fact-checking techniques.
    - Provide practical exercises where students evaluate the credibility of online sources, identify misinformation, and discern bias in digital content.
7. **Online Privacy Tools Exploration:**
    - Introduce students to privacy-enhancing tools and technologies, such as VPNs, encrypted messaging apps, or ad blockers.
    - Allow students to explore and experiment with these tools hands-on, understanding their functionality and impact on privacy.
8. **Design Thinking for Ethical Solutions:**
    - Use a design thinking approach to brainstorm and prototype ethical solutions to real-world information ethics challenges.
    - Facilitate hands-on activities where students collaborate in interdisciplinary teams to ideate, prototype, and present their ethical solutions.

REFERENCE BOOKS:

1. "Ethics in Information Technology" by George Reynolds
2. "Information Ethics: Privacy, Property, and Power" by Adam D. Moore
3. "Understanding Information Ethics" by Luciano Floridi
4. "The Ethics of Information" by Luciano Floridi
5. "Cyber Ethics: Morality and Law in Cyberspace" by Richard A. Spinello and Herman T. Tavani

COURSE TITLE: COMMUNICATION SKILLS - I

COURSE OBJECTIVE:

1. To train and prepare the students to seek and find employment in various field.
2. To develop communicative competence in students
3. To impart knowledge, ideas and concepts in the technicalities of proper pronunciation, structure, appropriate use and style of the English language as well as the application areas of English Communication.
4. To expose the students to the employment opportunities, challenges and job roles.

COURSE OUTCOME:

At end of the course students would be able to :

1. understand communication skills of English language
2. Formulate/ compose his own sentences and able to speak English Language.
3. collaborate with others students in English.
4. communicate properly their ideas and concepts in English.

Unit	Content
Unit 1:	○ Articles ○ Prepositions ○ Tenses ○ Subject – Verb Agreement **(11 Hours)**
Unit 2:	○ Meeting People ○ Exchanging Greetings and Taking Leave ○ Introducing Yourself **(11 Hours)**
Unit 3: Prose	○ The Home Coming – Rabindranath Tagore ○ A Lesson My Father Taught Me – APJ Abdul Kalam ○ How I Became a Public Speaker – George Bernard Shaw **(11 Hours)**
Unit 4: Poetry	○ The quality of Mercy – William Shakespeare ○ The Mountain and the Squirrel – R.W. Emerson ○ Where the Mind is Without Fear – Rabindranath Tagore **(12 Hours)**

Skill Enhancement Module: `

- Spot Visit and preparing a report – Visit to Super Market, Bus Stand, Railway Station, Bank, Medical Shop, Bakery etc.

- Interview of a dignitary and writing a report in dialogue form

  (Skill Enhancement module will be of 20 marks. This module will be internally assessed flexibly on thebasis of Class tests, assignments, seminar, reading material, project, survey, group discussion, Study tour, MCQ, Open Book exam (OBE), etc.)

TEXT BOOK: -

Pathmaker: A Textbook for College Students [ISBN 989354421778] Edited by Board of Editors, Sant Gadge Baba Amravati University, Amravati. Publisher: Orient BlackSwan Pvt L

SEMESTER II

COURSE TITLE: CRYPTOGRAPHY

COURSE OBJECTIVES:

1. Introduce students to the fundamental concepts and principles of cryptography, including encryption, decryption, and cryptographic algorithms.
2. Explore various cryptographic techniques such as symmetric encryption, asymmetric encryption, hashing, digital signatures, and cryptographic protocols.
3. Teach students how to analyze the security of cryptographic algorithms and protocols, including their strengths, weaknesses, and vulnerabilities.
4. Illustrate the practical applications of cryptography in securing data transmission, authentication, digital signatures, secure communication protocols, and data integrity.
5. Discuss key management principles, including key generation, distribution, storage, and revocation, and their importance in cryptographic systems.
6. Introduce students to the concepts and components of PKI, including certificate authorities, digital certificates, and certificate revocation lists.

COURSE OUTCOMES:

1. Students will demonstrate an understanding of the fundamental principles and concepts of cryptography, including encryption, decryption, and cryptographic algorithms.
2. Students will be able to apply cryptographic techniques such as symmetric and asymmetric encryption, hashing, and digital signatures to secure data and communication channels.
3. Students will be proficient in analyzing the security of cryptographic algorithms and protocols, identifying vulnerabilities, and evaluating cryptographic systems' overall security.
4. Students will develop the skills necessary to implement cryptographic solutions for securing data transmission, authentication, and ensuring data integrity in real-world scenarios.
5. Students will comprehend the concepts and components of PKI and its role in establishing trust, securing communication channels, and enabling secure digital transactions.

Unit I: Classical Ciphers (12 hours)

Ceaser Cipher, Vegnere Cipher, Rail-fence Cipher, Row Transposition Cipher. Requirement and Basic Properties, Main Challenges, Confidentiality, Integrity, Availability, Non-Repudiation, Encryption Techniques: Plaintext, Cipher text, Substitution & Transposition techniques, Encryption & Decryption, Types of attacks, Key range & Size.

Unit II: Secret Key Cryptography (12 hours)

Data Encryption Standard-Symmetric Ciphers (Stream Cipher &Block cipher) Advanced Encryption Standard (AES)-Triple DES-Blowfish, RC4, RC5/RC6 family.

Unit III: Public Key Cryptography (12 Hours)

Principles of public key cryptosystems-The RSA algorithm-Key management -Diffie Hellman Key exchange, Elgamal Algorithm, Polynomial Arithmetic, Elliptic curve arithmetic-Elliptic curve cryptography, cryptanalysis.

Unit IV: Cryptocurrency (12 Hours)

Bitcoin introduction, working, blockchain crucial to bitcoin, block chain operation with bitcoins, bitcoin glossary, bitcoin wallets, setup for bitcoin payments, bitcoin mining.

Unit V: Message authentication code and Hash Functions (12 hours)

Message authentication code Authentication functions, Hash functions- Hash Algorithms (MD5, Secure Hash Algorithm), Digital signatures (Authentication protocols, Digital signature Standard). Digital Certificate and Public Key Infrastructure.

Reference Books:

1. Delfs, H. & Knebl, H. (2001). Introduction to Cryptography: Principles and Applications. Springer-Verlag Berlin and Heidelberg GmbH & Co.

2. Stallings, W. (2010). Cryptography and network security: Principles and practice (5th ed.) Boston: Prentice Hall.

3. Menezes, A.J., Oorschot, P. Van & Vanstone, S.A. (1997). The Handbook of Applied Cryptography. CRC Press.

4. Schneier, B. (1995). Applied cryptography, Protocols, algorithms and source code in C (2nd ed.). New York: John Wiley & Sons.

COURSE TITLE: DIGITAL FORENSIC AND SECURITY

COURSE OBJECTIVES:

1. To introduce students to the principles and practices of digital forensics and cybersecurity.
2. To provide hands-on experience in collecting, preserving, and analyzing digital evidence.
3. To develop critical thinking and problem-solving skills through practical case studies and simulations.
4. To prepare students for careers in digital forensics, cybersecurity, law enforcement, and related fields.

COURSE OUTCOMES:

1. The role of investigator and lab requirements in Digital Forensics.
2. Data Acquisition methods, tools and storage formats of digital evidence.
3. Collecting, Preserving and Seizing of various digital evidences.
4. Validating and Testing of evidences using various methods.
5. The techniques in developing standard methods of network forensics.

UNIT I: Computer Forensics and Investigations (12 Hours)

Understanding Computer Forensics, Preparing for Computer Investigations, Taking A Systematic Approach, Procedure for Corporate High- Tech Investigations, Understanding Data Recovery Workstations and Software Office and Laboratory, Understanding Forensics Lab Certification Requirements Determining the Physical Requirements for a Computer, Forensics Lab Selecting a Basic Forensic Workstation

UNIT II: Data Acquisition (12 hours)

Understanding Storage Formats for Digital Evidence, Determining the Best Acquisition Method, Contingency Planning for Image Acquisitions, Using Acquisition Tools, Validating Data Acquisition, Performing RAID Data Acquisition, Using Remote Network Acquisition Tools, Using Other Forensics Acquisition Tools

UNIT III: Processing Crime and Incident Scenes (12 Hours)

Identifying Digital Evidence, Collecting the Evidence in Private-Sector Incident Scenes, Processing law Enforcement Crime Scenes, preparing fora Search, securing a Computer Incident or Crime Scene, Seizing Digital evidence at the crime Scene, Storing Digital evidence, obtaining a Digital Hash, Current Computer Forensics Tools, Evaluating Computer Forensics Tool Needs, Computer Forensics Software Tools, Computer Forensics Hardware Tools.

UNIT IV: Validating and Testing Forensics Software (12 hours)

Computer Forensics Analysis and Validation, Determining What Data to Collect and Analyze, Validating Forensic Data, Addressing Data-Hiding Techniques, Performing Remote Acquisition, data carving, Recovering Graphics and Network Forensics, Recognizing a Graphics File, Understanding Data Compression, Locating and

Recovering Graphics Files, live Memory forensics (RAM), Understanding Copyright Issues with Graphics, Network Forensic, social media forensics.

UNIT V: Advanced Topics and Practical Applications (12 hours)

Developing Standard Procedure for Network Forensics, Using Network Tools, Examining Honeynet Project, E-mail Investigations, Cell Phone and Mobile Device Forensics, Exploring the Role of E- mail in Investigations, Exploring the Role of Client and Server in E-mail, Investigating E-mail Crimes and Violations, Understanding E-mail Servers, Using Specialized E-mail Forensics Tools, Understanding Mobile Device Forensics, Understanding Acquisition Procedure for Cell Phones and Mobile Devices

Reference Book:

1. “Guide to computer forensics and investigation”4th edition by Amelia Philips, Bill Nelsonand Christopher Steuart.
2. "Computer Forensics: Investigating Data and Image Files" by EC-Council
3. "Digital Forensics: Principles and Practices" by S. Kumar and S. Yadav
4. "Cybersecurity and Cyberforensics" by Alok K. Gupta
5. "Investigating Cyber Law and Cyber Forensics" by Yatindra Singh
6. "Handbook of Digital Forensics and Investigation" by Eoghan Casey

COURSE TITLE: WEB SECURITY

COURSE OBJECTIVES:

1. To understand the fundamentals of web application security
2. To focus on wide aspects of secure development and deployment of web applications
3. To learn how to build secure APIs
4. To learn the basics of vulnerability assessment and penetration testing
5. To get an insight about Hacking techniques and Tools

COURSE OUTCOMES:

1. Understanding the basic concepts of web application security and the need for it.
2. Be acquainted with the process for secure development and deployment of web applications
3. Acquire the skill to design and develop Secure Web Applications that use Secure APIs
4. Be able to get the importance of carrying out vulnerability assessment and penetration testing
5. Acquire the skill to think like a hacker and to use hackers tool sets.

Unit I :Fundamentals Of Web Application Security (9 Hours)

The history of Software Security-Recognizing Web Application Security Threats, Web Application Security, Authentication and Authorization, Secure Socket layer, Transport layer Security, Session Management-Input Validation

Unit II: Secure Development And Deployment (9 Hours)

Web Applications Security - Security Testing, Security Incident Response Planning,The Microsoft Security Development Lifecycle (SDL), OWASP Comprehensive Lightweight Application Security Process (CLASP), The Software Assurance Maturity Model (SAMM)

Unit III: Secure API Development (9 Hours)

API Security- Session Cookies, Token Based Authentication, Securing Natter APIs: Addressing threats with Security Controls, Rate Limiting for Availability, Encryption, Audit logging, Securing service-to-service APIs: API Keys , OAuth2, Securing Microservice APIs: Service Mesh, Locking Down Network Connections, Securing Incoming Requests.

Unit IV: Vulnerability Assessment And Penetration Testing (9 Hours)

Vulnerability Assessment Lifecycle, Vulnerability Assessment Tools: Cloud-based vulnerability scanners, Host-based vulnerability scanners, Network-based vulnerability scanners, Databasebased vulnerability scanners, Types of Penetration Tests: External Testing, Web Application Testing, Internal Penetration Testing, SSID or Wireless Testing, Mobile Application Testing.

Unit V: Hacking Techniques And Tools (9 hours)

Social Engineering, Injection, Cross-Site Scripting(XSS), Broken Authentication and Session Management, Cross-Site Request Forgery, Security Misconfiguration, Insecure Cryptographic Storage, Failure to Restrict URL Access, Tools: Comodo, OpenVAS, Nexpose, Nikto, Burp Suite, etc. 30

Reference Books:

1. Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, First Edition, 2020, O'Reilly Media, Inc.
2. Bryan Sullivan, Vincent Liu, Web Application Security: A Beginners Guide, 2012, The McGraw-Hill Companies.
3. Neil Madden, API Security in Action, 2020, Manning Publications Co., NY, USA.
4. Michael Cross, Developer's Guide to Web Application Security, 2007, Syngress Publishing, Inc.
5. Ravi Das and Greg Johnson, Testing and Securing Web Applications, 2021, Taylor & Francis Group, LLC.

COURSE TITLE: CLOUD COMPUTING FUNDAMENTALS AND SECURITY(E1)

COURSE OBJECTIVES:

1. To understand the principles of cloud architecture, models and infrastructure.
2. To understand the concepts of virtualization and virtual machines.
3. To gain knowledge about virtualization Infrastructure.
4. To explore and experiment with various Cloud deployment environments.
5. To learn about the security issues in the cloud environment.

COURSE OUTCOMES:

1. Understand the design challenges in the cloud.
2. Apply the concept of virtualization and its types.
3. Experiment with virtualization of hardware resources and Docker.
4. Develop and deploy services on the cloud and set up a cloud environment.
5. Explain security challenges in the cloud environment

Unit I: Cloud Architecture Models And Infrastructure(9 Hours)

Cloud Architecture: System Models for Distributed and Cloud Computing – NIST Cloud Computing Reference Architecture – Cloud deployment models – Cloud service models; Cloud Infrastructure: Architectural Design of Compute and Storage Clouds – Design Challenges

Unit II: Virtualization Basics(9 Hours)

Virtual Machine Basics , Taxonomy of Virtual Machines , Hypervisor , Key Concepts , Virtualization structure , Implementation levels of virtualization , Virtualization Types: Full Virtualization , Para Virtualization , Hardware Virtualization , Virtualization of CPU, Memory and I/O devices.

Unit III: Virtualization Infrastructure & Docker(9 Hours)

Desktop Virtualization , Network Virtualization , Storage Virtualization , System-level of Operating Virtualization , Application Virtualization , Virtual clusters and Resource Management , Containers vs. Virtual Machines , Introduction to Docker , Docker Components , Docker Container , Docker Images and Repositories.

Unit IV: Cloud Deployment Environment (9 Hours)

Google App Engine, Amazon AWS, Microsoft Azure; Cloud Software Environments, Eucalyptus, OpenStack

Unit V: Cloud Security (9 hours)

Cloud application software lifecycle, application security in an IaaS, PaaS and SaaS environment and its protection.

Virtualization System-Specific Attacks: Guest hopping – VM migration attack – hyperjacking. Data Security and Storage; Identity and Access Management (IAM) - IAM Challenges - IAM Architecture and Practice.

Reference Books:

1. Kai Hwang, Geoffrey C Fox, Jack G Dongarra, "Distributed and Cloud Computing, From Parallel Processing to the Internet of Things", Morgan Kaufmann Publishers, 2012.
2. James Turnbull, "The Docker Book", O'Reilly Publishers, 2014.
3. Krutz, R. L., Vines, R. D, "Cloud security. A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, 2010.

COURSE TITLE: APPLICATION AND NETWORK SECURITY (E2)

COURSE OBJECTIVES:

1. To understand the basic concepts of security
2. To understand the concept of authentication protocols and digital signatures.
3. To learn various methods and protocols to understand the cryptography.
4. To learn various network security attacks.
5. To understand the IP and Web security.

COURSE OUTCOMES:

1. Describe computer and network security fundamental concepts and principles.
2. Acquire the knowledge of various authentication protocols, key exchange mechanism, and digital certificates.
3. To get better knowledge on fundamental concepts of cryptography, encryption and hashing techniques.
4. Identify and assess different types of threats and attacks such as social engineering, rootkit, and botnets,etc.
5. Acquire Demonstrate the ability to select among available network security technology and protocols such as IDS, firewalls, SSL , TLS, etc.

Unit I: Overview of System Security (9 Hours)

Computer security Concepts, Security Functional requirements, Fundamental security design principles,

Attack surfaces and attack trees, Computer security strategy.

Unit II: Software security and Trusted systems (9 Hours)

Buffer Overflow attacks, Other Overflow attacks, Software security issues, Secure code writing, Handling program input and output, introduction Operating System security, System security planning and Maintenance

Unit III: IT Security Management and Risk Assessment (9 Hours)

IT Security management, Risk analysis, Security planning and Polies, Symmetric algorithm and Message policies, Message Authentication, Physical and infrastructural security, Human resource security, Security Audit.

Unit IV: Network Security (9 Hours)

Internet Security protocols and standard, Internet authentication Applications, Wireless network security

Unit V: Database Security (9 hours)

Database management system, Need for database security, Database access control, SQL injection Attacks, Inference, Database Inference.

Reference Books:

1. "Computer_Security_Principles_and_Practice_(3rd_Edition)" Willims Stalling and Lawrie brown
2. Shema, M. & Adam. (2010). Seven deadliest web application attacks. Amsterdam: Syngress Media.
3. Stuttard, D. & Pinto, M. (2011). The web application hacker's handbook: Discovering and exploiting security flaws (2nd ed). Indianapolis, IN: Wiley, John & Sons.
4. Heiderich, M., Nava E.A.V., Heyes, G., & Lindsay, D. (2011). Web application obfuscation. Amsterdam: Syngress Media,U.S.
5. Sullivan, Bryan (2012). Web Application Security, A Beginner's Guide. McGraw- Hill Education.

COURSE TITLE: LAB – 4 (BASED ON CORE SUBJECTS)

Minimum 12 experiments / programming assignments must be completed based on the respective syllabus

(2DCS1,2DCS2,2DCS3).

COURSE TITLE: LAB – 5 (BASED ON DSE SUBJECTS)

Minimum 12 experiments / programming assignments must be completed based on the respective syllabus

(2DCS E1/ 2DCS E2).

COURSE TITLE: E-COMMERCE LEGAL ISSUES

UNIT I Introduction to Electronic Commerce (9 Hours)

Introduction to Electronic Commerce: Meaning, nature and scope; Channels of e - commerce; Business applications of e - commerce; Global trading environment and adoption of e-commerce.

Business Models of E-commerce and Infrastructure; B2B, B2C, B2G and other models of e-commerce; Applications of e-commerce to supply chain management; product and service digitization; Remote servicing, procurement, and online marketing and advertising E-commerce, resources and infrastructure planning.

UNIT II Business to Consumer E-Commerce Applications (9 Hours)

Business to Consumer E-commerce Applications: Cataloging; Order planning and order generation; Cost estimation and pricing; Order receipt and accounting; Order selection and prioritization: Order scheduling, fulfilling and delivery, Order billing and payment Management; Post sales services.

UNIT III Business to Business E-Commerce (9 Hours)

Business to Business E-Commerce: Need and alternative models of B2B e-commerce; Using Public and private computer networks for B2B trading: EDI and paperless trading: characteristic features of EDI service arrangement; Internet based EDI; EDI architecture and standards; Costs of EDI infrastructure; Reasons for slow acceptability of EDI for trading; E-marketing – Traditional web Promotion: Web counters; Web advertisements.

UNIT IV Electronic Payment Systems and Order Fulfillment (9 hours)

Electronic Payment Systems and Order Fulfillment: Types of payment systems - e-cash and currency servers, e-cheques, credit cards, smart cards, electronic purses and debit cards; Operational, credit and legal risks of e-payment, Risk management options for e-payment systems; Order fulfillment for e – commerce.

UNIT V Security Issues in E-Commerce (9 hours)

Security Issues in E-Commerce: Security risks of e-commerce- Types and sources of threats; Protecting electronic commerce assets and intellectual property; Firewalls; Client server network security; Data and message security; Security tools; Digital identity and electronic signature; Encryption approach to e-commerce security.

Salient provisions for Security and Privacy, ; Legal and Regulatory Environment for e-commerce, cyber laws in India and their limitations Taxation and e -commerce; Management of Risk: Introduction, Introduction to Risk Management, Disaster Recovery Plans, Risk Management Paradigm

HANDS-ON (LAB) SESSIONS:

NOTE: The list suggests sample program set. Hence, the concerned staff may modify the list as needed (Minimum 10).

1. **Setting Up an Online Store**: Students can create their own online store using platforms like Shopify, WooCommerce, or Magento. They'll learn to set up product listings, customize the store design, and configure payment gateways.
2. **Product Photography and Editing**: Teach students how to take professional product photos using smartphones or cameras. Then, introduce them to basic photo editing techniques using software like Adobe Photoshop or free alternatives like GIMP.
3. **SEO Optimization**: Guide students through the process of optimizing product listings for search engines. They can learn keyword research, on-page SEO techniques, and how to write compelling product descriptions.
4. **Social Media Marketing**: Students can create social media accounts for their online store and develop a marketing strategy. They'll learn how to create engaging content, run targeted ads, and analyze performance metrics.
5. **Customer Relationship Management (CRM)**: Introduce students to CRM tools like HubSpot or Salesforce. They can learn to manage customer data, track interactions, and automate email campaigns to improve customer retention.
6. **Payment Gateway Integration**: Walk students through the process of integrating payment gateways like PayPal, Stripe, or Square into their online store. They'll learn about payment processing fees, security measures, and refund policies.
7. **Order Fulfillment and Inventory Management**: Teach students how to manage orders, process payments, and track inventory levels using e-commerce platforms. They can simulate real-world scenarios like handling returns and managing backorders.
8. **Analytics and Reporting**: Show students how to set up Google Analytics for their online store and interpret key metrics like traffic sources, conversion rates, and average order value. They can use this data to make informed business decisions.
9. **Responsive Web Design**: Explain the importance of responsive design for e-commerce websites, and teach students how to create mobile-friendly layouts using HTML, CSS, and JavaScript.
10. **Customer Support and Feedback**: Role-play different customer support scenarios and teach students how to respond professionally to inquiries, complaints, and feedback. They can also learn how to solicit customer reviews and testimonials.

COURSE TITLE: CYBER ATTACK AND COUNTER MEASURES

COURSE OBJECTIVES:

1. Understand the various types and motivations behind cyber attacks.
2. Acquire knowledge of cybersecurity principles and risk management practices.
3. Identify common attack techniques and tools used by cybercriminals.
4. Develop skills to implement effective cybersecurity measures and defense strategies.
5. Learn incident response procedures and techniques for mitigating the impact of cyber attacks.

COURSE OUTCOMES:

1. Students will be able to analyze and assess cybersecurity risks within an organization.
2. Students will demonstrate proficiency in using cybersecurity tools for attack detection and prevention.
3. Students will be capable of implementing cybersecurity best practices to protect networks and systems.
4. Students will develop the ability to respond effectively to cyber incidents and facilitate recovery.
5. Students will gain a comprehensive understanding of cybersecurity concepts and their practical applications.

Unit 1: Introduction to Cyber Attacks (9 Hours)

- Overview of cyber attacks: types, motivations, and targets
- Asset, threat and risk management
- Oraganization security & frameworks
- Common attack vectors: malware, phishing, DoS/DDoS, social engineering
- Case studies of notable cyber attacks
- Information security governance

Unit 2: Cybersecurity Fundamentals (9 Hours)

- Principles of cybersecurity: confidentiality, integrity, availability
- Risk assessment and management in cybersecurity
- Legal and ethical considerations in cybersecurity

Unit 3: Cyber Attack Techniques and Tools (9 Hours)

- Understanding attack techniques: reconnaissance, exploitation, privilege escalation, etc.
- Introduction to common attack tools: Metasploit, Wireshark, Nmap, etc.
- Hands-on exercises: simulated attacks and penetration testing

Unit 4: Cyber Defense Strategies (9 Hours)

- Network security fundamentals: firewalls, intrusion detection/prevention systems (IDS/IPS)
- Endpoint security: antivirus software, endpoint detection and response (EDR)
- Security best practices: encryption, multi-factor authentication, secure coding

Unit 5: Incident Response and Recovery (9 Hours)

- Incident response procedures: preparation, detection, containment, eradication, recovery
- Post-incident analysis and lessons learned
- Business continuity planning and disaster recovery

Hands-on Exercises:

NOTE: The list suggests sample program set. Hence, the concerned staff may modify the list as needed (Minimum 10).

1. Simulated cyber-attack scenarios using penetration testing tools.
2. Configuring and testing network security measures such as firewalls and IDS/IPS.
3. Incident response simulations to practice detection, containment, and recovery procedures.
4. Case studies and group discussions on recent cyber-attacks and defence strategies.
5. Phishing Simulation: Set up a controlled phishing simulation where students receive emails designed to trick them into revealing sensitive information or clicking on malicious links. Teach them how to identify phishing attempts and report suspicious emails.
6. Malware Analysis: Provide students with malware samples (in a controlled environment) and guide them through the process of analyzing their behavior. They can use tools like Wireshark, IDA Pro, or VirusTotal to understand how malware operates and how to mitigate its effects.
7. Network Penetration Testing: Set up a lab environment with vulnerable systems and networks, and task students with conducting penetration tests. They'll learn how to identify and exploit security vulnerabilities, and how to recommend mitigations to improve network security.
8. Web Application Security: Guide students through common web application vulnerabilities like SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF). They can use tools like Burp Suite or OWASP ZAP to identify and exploit these vulnerabilities in a controlled environment.
9. Incident Response Simulation: Simulate a cyber attack scenario (e.g., ransomware infection or data breach) and have students respond as if they were part of a real incident response team. They'll learn how to contain the incident, preserve evidence, and restore normal operations.
10. Firewall Configuration and Management: Set up a lab environment with firewall appliances or software, and teach students how to configure firewall rules to block unauthorized traffic and protect network resources. They can also learn how to monitor firewall logs for suspicious activity.
11. Secure Coding Practices: Teach students secure coding practices to prevent common vulnerabilities like buffer overflows, input validation errors, and insecure file handling. They can practice writing secure code in languages like C/C++, Java, or Python.
12. Encryption and Cryptography: Introduce students to encryption algorithms and cryptographic protocols, and teach them how to implement encryption in software applications. They can practice encrypting and decrypting data using tools like OpenSSL or GPG.
13. Security Awareness Training: Conduct security awareness training sessions covering topics like password hygiene, social engineering tactics, and data protection best practices. Students can participate in interactive exercises and quizzes to reinforce their learning.
14. Vulnerability Management: Show students how to use vulnerability scanning tools like Nessus or OpenVAS to identify security weaknesses in systems and networks. They can learn how to prioritize and remediate vulnerabilities to reduce the risk of exploitation.

Reference Book:

1. "Hacking: The Art of Exploitation" by Jon Erickson
2. "The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto
3. "Network Security Essentials: Applications and Standards" by William Stallings
4. "Cybersecurity: Attack and Defense Strategies" by Yuri Diogenes and Erdal Ozkaya

5. "Incident Response & Computer Forensics" by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia

COURSE TITLE: COMMUNICATION SKILLS IN ENGLISH - II

COURSE OBJECTIVE :

1. To train and prepare the students to seek and find employment in various field.
2. To develop communicative competence in students
3. To impart knowledge, ideas and concepts in the technicalities of proper pronunciation, structure, appropriate use and style of the English language as well as the application areas of English Communication.
4. To expose the students to the employment opportunities, challenges and job roles.

COURSE OUTCOME:

At end of the course students would be able to

1. Understand the paragraph, prose, poetry and communication skills .
2. Formulate/ compose his own sentences and able to speak English Language.
3. Collaborate with others students in English.
4. Communicate properly their ideas and concepts in English.

Unit	Content
Unit 1:	1) Question Tags 2) Synonyms and Antonyms 3) Prefixes, Suffixes, Zero Suffix and Infix **(11 Hours)**
Unit 2:	1) Making Requests and Responding to Requests 22 2) Thanking Someone and Responding to Thanks 3) Developing a Thoughts **(11 Hours)**
Unit 3:	1) On the Rule of the Road – A.G. Gardiner 2) A Simple Philosophy – Seathl 3) The Thief – Ruskin Bond **(11 Hours)**
Unit 4:	1) The World is Too Much With Us – William Wordsworth 2) Love's Philosophy – P.B.Shelley 3) Success is Counted Sweetest – Emily Dickinson **(12 Hours)**

Skill Enhancement module:

Blog Writing, Presentation on a topic from prescribed prose/poem (Skill Enhancement module will be of 20 marks. This module will be internally assessed flexibly on the basis of Class tests, assignments, seminar, reading material, project, survey, group discussion, Study tour, MCQ, Open Book exam (OBE), etc.

TEXT BOOKS: -

A Textbook for College Students [ISBN 989354421778] Edited by Board of Editors, Sant Gadge Baba Amravati University, Amravati Publisher : Orient BlackSwan Pvt Ltd

PROJECT WORK:

Students pursuing a Diploma in Cybersecurity are required to undertake a project that demonstrates their understanding and application of cybersecurity concepts, techniques, and tools. The project work serves as a culmination of their learning experience and allows them to showcase their skills in a practical setting. Below are some footnotes regarding the project work for the syllabus:

1. **Project Proposal Submission:** Students are required to submit a project proposal outlining the scope, objectives, methodology, and expected outcomes of their project. The proposal should be reviewed and approved by the faculty before proceeding with the project.
2. **Project Selection:** Students have the flexibility to choose a project topic within the domain of cybersecurity based on their interests and career aspirations. The project could focus on areas such as network security, cryptography, digital forensics, incident response, or ethical hacking.
3. **Project Execution:** Students are expected to demonstrate proficiency in planning, executing, and documenting their project work. This involves conducting research, implementing appropriate methodologies and techniques, and adhering to best practices in cybersecurity.
4. **Hands-on Implementation:** The project should incorporate hands-on implementation, where students apply theoretical concepts learned in the classroom to real-world scenarios. This may involve setting up a lab environment, performing experiments, conducting security assessments, or developing security solutions.
5. **Documentation and Reporting:** Students are required to maintain detailed documentation throughout the project, including design documents, implementation logs, test results, and analysis findings. A final project report summarizing the entire project lifecycle, including methodology, findings, challenges, and recommendations, should be submitted.
6. **Presentation and Defense:** Upon completion of the project, students are expected to deliver a presentation to the faculty and peers, highlighting the key aspects of their project. They should be prepared to answer questions and defend their methodology, findings, and conclusions.
7. **Evaluation Criteria:** The project work will be evaluated based on various criteria, including the relevance of the topic, technical depth, creativity, quality of implementation, documentation clarity, presentation skills, and overall contribution to the field of cybersecurity.
8. **Ethical Considerations:** Students must adhere to ethical guidelines and principles throughout the project work, ensuring that their activities do not violate privacy, integrity, or confidentiality laws and regulations. Any ethical concerns or potential risks should be addressed and mitigated appropriately.

Internship:

Internship will be conducted after Ist semester in vacations for minimum 60 hrs. It’s 2 credits will be reflected in final semester credit grade report.