Sant Gadge Baba Amravati University
Diploma in Cyber Security (1 Year) [NEP NSQF-Level 5]

Sr-No.	Type	Subject Code	Subject	Teaching Scheme (Hrs./Week)					Examination and Evaluation Scheme							
				Th	Pr.	Total	Credits	Exam-Duration (Hrs.)	Max. Marks				Total Marks	Min. Passing Marks		
									External Marks		Internal Marks			External	Internal	Total
									TH	PR	TH	PR				
		SEMESTER -I														
1	Core Skill	N1DCS1	Cyber Security Techniques	3	-	3	3	3	50	-	30	-	80	20	12	32
2	Core Skill	N1DCS2	Introduction to Ethical Hacking	3	-	3	3	3	50	-	30	-	80	20	12	32
3	Core Skill	N1DCS3	Computer Network and Security	3	-	3	3	3	50	-	30	-	80	20	12	32
4	Core Skill	N1DCS4	Fundamentals of Cyber Laws	3	-	3	3	3	50	-	30	-	80	20	12	32
5	SEC/lab	N1DCS5	Cyber Security Techniques - LAB	-	4	4	2	-	-	25	-	25	50	10	10	20
6	SEC/lab	N1DCS6	Network programming - LAB	-	4	4	2	-	-	25	-	25	50	10	10	20
7	SEC/lab	N1DCS7	Penetration testing with Linux	-	4	4	2	-	-	25	-	25	50	10	10	20
8	GE	N1DCS8	Communication Skills I	3	-	3	3	3	50	-	30	-	80	20	12	32
9	SEC/LAB	N1DCS9	Communication Skills-LAB	-	2	2	1	-	-	-	-	20	20	-	10	10
10	Assessment Hours					6										
	TOTAL					**35**	**22**						**570**			
		SEMESTER -II														
1	Core Skill	N2DCS1	Cryptography	3	-	3	3	3	50	-	30	-	80	20	12	32
2	Core Skill	N2DCS2	Digital Forensic and Security	3	-	3	3	3	50	-	30	-	80	20	12	32
3	Core Skill	N2DCS3	Web Security	3	-	3	3	3	50	-	30	-	80	20	12	32
4	DSE	N2DCSE1 N2DCSE2	E1: Cloud Computing fundamentals and Security E2 : Application and Network Security	3	-	3	3	3	50	-	30	-	80	20	12	32
5	SEC	N2DCS4	LAB based on N2DCS 1,2,3	-	4	4	2	-	-	25	-	25	50	10	10	20
6	SEC	N2DCS5	Project/Internship*	-	4	4	2	-	-	25	-	25	50	10	10	20
7	SEC	N2DCS6	LAB based on N2DCSE1/E2	-	4	4	2	-	-	25	-	25	50	10	10	20
8	SEC	N2DCS8	Cyber Attacks and Counter Measures-LAB		4	4	2	-	-	25	-	25	50	10	10	20
9	GE	N2DCS8	Cyber Ethics	2		2	2	2	50	-	30	-	80	20	12	32
10	Assessment Hours					6										
	TOTAL					**36**	**22**						**600**			

***Internship : Two Credits will be Awarded for Minimum 60Hrs of internship**

Faculty: Science and Technology

Syllabus Prescribed for 1 Year Diploma in Cyber Security UG Programme

[NEP-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

Title: Cyber Security Techniques

Type: Core Skill

Credits: 3

Total Marks-80		Course Code: N1DCS1	(Total Number of Periods) Hrs
Theory Exam Marks :50	Internal Marks:30	Min Passing:32	45

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.

Unit 1 (11 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. 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: (11 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: (11 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.

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

Title: Cyber Security Techniques - LAB

Type: SEC/LAB

Credits: 2

Total Marks-50		Course Code: N1DCS5	(Total Number of Periods) Hrs
External Marks:25	Internal Marks:25	Min Passing:20	60

List of Practical's:

NOTE: The list suggests sample program set. Hence, the concerned staff may modify the list as needed (Minimum 15).

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.

Title: Introduction to Ethical Hacking

Type: Core Skill

Credits: 3

Total Marks-80		Course Code: N1DCS2	(Total Number of Periods) Hrs
Theory Exam Marks :50	Internal Marks:30	Min Passing:32	45

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 (11 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 (11 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 (11 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

Reporting and Ethics: Documentation and reporting of ethical hacking assessments, Ethical guidelines and codes of conduct for ethical hackers.

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

Title: Computer Network and Security

Type: Core Skill

Credits: 3

<table>
<tr><th colspan="2">Total Marks-80</th><th colspan="2">Course Code: N1DCS3</th><th>(Total Number of Periods) Hrs</th></tr>
<tr><td><b>Theory Exam Marks :50</b></td><td colspan="2"><b>Internal Marks:30</b></td><td><b>Min Passing:32</b></td><td><b>45</b></td></tr>
</table>

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.

Unit I: Introduction to Computer Network (11 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 (11 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 (11 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

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

Title: Network Programming - Lab

Type: SEC/LAB

Credits: 2

Total Marks-50		Course Code: N1DCS6	(Total Number of Periods) Hrs
External Marks:25	Internal Marks:25	Min Passing:20	60

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 15).

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.

Title: Penetration Testing With Linux

Type: SEC/LAB

Credits: 2

Total Marks-50		Course Code: N1DCS7	(Total Number of Periods) Hrs
External Marks:25	Internal Marks:25	Min Passing:20	60

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.

Practical List:

NOTE: The list suggests sample program set. Hence, the concerned staff may modify the list as needed (Minimum 15).

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.

Programme: Diploma in Cyber Security

Title: Fundamentals Of Cyber Laws

Type: Core Skill

Credits: 3

<table>
<tr><th colspan="2">Total Marks-80</th><th colspan="2">Course Code: N1DCS4</th><th>(Total Number of Periods) Hrs</th></tr>
<tr><td><b>Theory Exam Marks :50</b></td><td colspan="2"><b>Internal Marks:30</b></td><td><b>Min Passing:32</b></td><td><b>45</b></td></tr>
</table>

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: Computer & Cyber Crimes, Indian Response (11 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 II: Mens Rea and Criminal Liability, Investigations in Cyber Crimes (11 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 III: Cyber Crimes: Discovery and Appreciation of Evidences, Prevention (11 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 IV: Human Rights Perspectives in Cyber Crimes, Precaution and Prevention (12 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"

Title: Communication Skills - I

Type: GE

Credits: 3

Total Marks-80	**Course Code: N1DCS8**	**(Total Number of Periods) Hrs: 45(T)**
Theory Exam Marks :50	**Theory Internal Marks:30**	**Min Passing:32**

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

TEXT BOOK:-

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

Title: Communication Skills-LAB

Type: SEC/LAB

Credits: 1

<table>
<tr><td><b>Total Marks-20</b></td><td colspan="2"><b>Course Code: N1DCS9</b></td><td><b>(Total Number of Periods) Hrs: 30</b></td></tr>
<tr><td colspan="2"><b>Theory Internal Marks:20</b></td><td colspan="2"><b>Min Passing:10</b></td></tr>
</table>

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

LIST OF PRACTICAL

1. Letter writing formal and informal
2. Email
3. Resume
4. Making Request
5. Responding to thanks
6. Blog writing
7. Application writing
8. Question tags
9. Zero suffix and infix
10. Requesting

SEMESTER-II

Title: Cryptography

Type: Core Skill

Credits: 3

Total Marks-80		Course Code: N2DCS1	(Total Number of Periods) Hrs
Theory Exam Marks :50	Internal Marks:30	Min Passing:32	45

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.

Unit I: Classical Ciphers (11 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 (11 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 (11 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.

Message authentication code and Hash Functions: Message authentication code Authentication functions, Hash functions- Hash Algorithms (MD5, Secure Hash Algorithm), Digital signatures (Authentication protocols, Digital signature Standard).

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.

Title: Digital Forensic and Security

Type: Core Skill

Credits: 3

<table>
<tr><td colspan="2"><b>Total Marks-80</b></td><td colspan="2"><b>Course Code: N2DCS2</b></td><td><b>(Total Number of Periods) Hrs</b></td></tr>
<tr><td><b>Theory Exam Marks :50</b></td><td colspan="2"><b>Internal Marks:30</b></td><td><b>Min Passing:32</b></td><td><b>45</b></td></tr>
</table>

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 (11 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 (11 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 (11 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.

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

Title: Web Security

Type: Core Skill

Credits: 3

Total Marks-80		Course Code: N2DCS3	(Total Number of Periods) Hrs
Theory Exam Marks :50	Internal Marks:30	Min Passing:32	45

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(12 hours)

Vulnerability Assessment Lifecycle, Vulnerability Assessment Tools: Cloud-based vulnerability scanners, Host-based vulnerability scanners, Network-based vulnerability scanners, Databasebased vulnerability scanners.

Hacking Techniques And Tools : 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.

Title: Cloud Computing Fundamentals and Security(E1)

Type: DSE

Credits: 3

Total Marks-80		Course Code: N2DCSE1	(Total Number of Periods) Hrs
Theory Exam Marks :50	Internal Marks:30	Min Passing:32	45

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. Explain security challenges in the cloud environment

Unit I: Cloud Architecture Models And Infrastructure (11 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 (11 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 (11 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 V: Cloud Security (12 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.

Title: Application And Network Security (E2)

Type: DSE

Credits: 3

Total Marks-80		Course Code: N2DCE2	(Total Number of Periods) Hrs
Theory Exam Marks :50	Internal Marks:30	Min Passing:32	45

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 (11 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 (11 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 (11 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 (12 hours)

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

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.

Title: LAB based on N2DCS 1,2,3

Type: SEC

Credits: 2

Total Marks-50		Course Code: N2DCS4	(Total Number of Periods) Hrs
External Marks :25	Internal Marks:25	Min Passing:20	60

Minimum 15 experiments / programming assignments must be completed based on the respective syllabus (N2DCS1,N2DCS2,N2DCS3).

Title: LAB based on N2DCSE1/E2

Type: SEC

Credits:2

Total Marks-50		Course Code: N2DCS6	(Total Number of Periods) Hrs
External Marks :25	Internal Marks:25	Min Passing:20	60

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

Minimum 15 experiments / programming assignments must be completed based on the respective syllabus (N2DCS E1/ N2DCS E2).

Title: Cyber Ethics

Type: GE

Credits: 2

Total Marks-80	Course Code: N2DCS8	(Total Number of Periods) Hrs: 30
Theory Exam Marks :50	Theory Internal Marks:30	Min Passing:32

COURSE OUTCOME:

Upon completion of this course, the students should be able to:

1. Understand the ethical values and principles underlying cyber activities.
2. understand the historical development and current governance structures of the Internet.
3. Evaluate the complexities of free speech and content control issues in cyberspace.
4. Examine the legal and moral dimensions of intellectual property in the digital realm.

Unit	Content
Units I: The Internet and Ethical Values	Cyber ethics and the “Law of the Horse”, Iron Cage or Gateway to Utopia? Ethical Values and the Digital Frontier, Utilitarianism, Contract Rights (Contractarianism), Moral Duty (Pluralism), New Natural Law, Postscript on

	Moral Theory, Floridi's Macro-ethics , Normative Principles: Autonomy, Nonmaleficence, Beneficence, Justice **(7 Hours)**
Unit II: Regulating and Governing the Internet	A Short History of the Internet, The Internet's Current Architecture, The World Wide Web, Electronic Commerce, Gatekeepers and Search Engines, Social Networking, Social Problems and Social Costs: The Invisible Hand, Regulating the Net: The Visible Hand, A "Bottom-Up" Approach: The Power of Code, Internet Governance, Contested Sovereignty in Cyberspace **(8 Hours)**
Unit III: Free Speech and Content Controls in Cyberspace	Speech and Internet Architecture, Pornography in Cyberspace: Public Policy Overview, Automating Content Controls, New Censors and Controversies. Hate Speech and Online Threats, Anonymous Speech, The Ethics of Blogging, Spam as Commercial Free Speech, Government Censorship and the Fate of Political Speech **(7 Hours)**
Unit IV: Intellectual Property in Cyberspace	Background on Intellectual Property What Is Intellectual Property? Legal Protection for Intellectual Property, Moral Justifications for Intellectual Property, Recent Legislation. Issues for the Internet and Networking Technologies: Copyright and the Digital Dilemma, Software Ownership and the Open-Source Code Movement, Digital Rights Architectures, Business Method Patents in Cyberspace, Patents and Smartphones, Domain Names and Interconnectivity Issues. **(8 Hours)**

TEXT BOOK:

1. "CYBERETHICS Morality and Law in Cyberspace" by Richard A. Spinello.

REFERENCE:

1. "Ethics in Information Technology" by George Reynolds
2. "Digital Ethics: Rethinking Responsibility in Technology" by Jessica Powell

Title: Cyber Attack And Counter Measures-LAB

Type: SEC

Credits:2

Total Marks-50		Course Code: N2DCS6	(Total Number of Periods) Hrs
External Marks :25	**Internal Marks:25**	**Min Passing:20**	**60**

NOTE: The list suggests sample program set. Hence, the concerned staff may modify the list as needed (Minimum 15).

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.

Programme: Diploma Cyber Security

Title: PROJECT/INTERNSHIP

Type: SEC

Credits: 2

Total Marks-50		Course Code: N2DCS5	(Total Number of Periods) Hrs
External Marks :25	Internal Marks: -25	Min Passing:20	60

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.