Sant Gadge Baba Amravati University Amravati
B.Sc. Cyber Security(Semester-V) NEP

Sr. No	Type	Subject Code	Subject	Teaching and Learning Scheme					Duration of Exam Hrs	Examination and Evaluation Scheme							
				Teaching Period per week				Credits		Maximum Marks					Minimum passing Marks		
				L	T	P	Total Hrs			External		Internal		Total marks	External	Internal	Total
										Th	Pr	Th	Pr				
1	Core	N5CS1	Cyber Threat Intelligence	3	-	-	03	03	03	50	-	30	-	80	20	12	32
2	Core	N5CS2	Secured System Administration	3	-	-	03	03	03	50	-	30	-	80	20	12	32
3	Core	N5CS3	Cloud Security	3	-	-	03	03	03	50	-	30	-	80	20	12	32
4	DSE	N5CS4	Professional Elective 3	3	-	-	03	03	03	50	-	30	-	80	20	12	32
5	SEC/LAB	N5CS5	Cloud Security Lab	-	-	2	04	02	-	-	25	-	25	50	10	10	20
6	SEC/LAB	N5CS6	Secured System Administration - Lab	-	-	2	04	02	-	-	25	-	25	50	10	10	20
7	SEC/LAB	N5CS7	LAB Based on Elective 3	-	-	2	04	02	-	-	25	-	25	50	10	10	20
8	SEC	N5CS8	Seminar	-	-	1	02	01	-	-	-	-	50	50	-	20	20
9	SEC	N5CS9	Project Phase I	-	-	2	04	02	-	-	-	-	50	50	-	20	20
10	Assessment Hours						05										
	TOTAL						**35**	**21**						**570**			
Sem -V Total Credit			**21**	**Total Marks**				**570**									

Professional Elective 3: Network Security, Cryptocurrency and Block Chain Technology

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

Sant Gadge Baba Amravati University Amravati

B.Sc. Cyber Security(Semester-VI) NEP

Sr. No	Type	Subject Code	Subject	Teaching and Learning Scheme					Duration of Exam Hrs	Examination and Evaluation Scheme							
				Teaching Period per week				Credits		Maximum Marks					Minimum passing Marks		
				L	T	P	Total Hrs			External		Internal		Total marks	External	Internal	Total
										Th	Pr	Th	Pr				
1	Core	N6CS1	Malware Analysis	3	-	-	03	03	03	50	-	30	-	80	20	12	32
2	Core	N6CS2	Penetration Testing	3	-	-	03	03	03	50	-	30	-	80	20	12	32
3	Core	N6CS3	Web Application Security	3	-	-	03	03	02	50	-	30	-	80	20	12	32
4	SEC/LAB	N6CS4	Penetration Testing-LAB	-	-	2	04	02	-	-	25	-	25	50	10	10	20
5	SEC/LAB	N6CS5	Malware Analysis -LAB	-	-	2	04	02	-	-	25	-	25	50	10	10	20
6	SEC/LAB	N6CS6	Web Application Security -LAB	-	-	2	04	02	-	-	25	-	25	50	10	10	20
7	SEC	N6CS7	Internship	-	-	-	-	02	-					-	-	-	
8	SEC	N6CS8	Project Phase II	-	-	4	08	04	-	-	50	-	50	100	20	20	40
	Assessment Hours						06										
	TOTAL						**35**	**21**						**490**			
Sem -VI Total Credit			**21**	**Total Marks**				**490**									

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

Faculty: Science and Technology

Syllabus Prescribed for Three Year Six Semester UG Programme

B.Sc. CYBER SECURITY Part – III [NEP]

SEMESTER-V

Title: CYBER THREAT INTELLIGENCE
Type: Core
Credits: 03

Total Marks-80		Course Code: N5CS1	(Total Number of Periods) Hrs
Theory Exam Marks :50	Internal Marks:30	Min Passing:32	45

COURSE OBJECTIVES:

- To learn basic fundamentals of cyber threat intelligence.
- To demonstrate how cyber has changed the nature of intelligence collection.
- To analyze the cyber threats at different levels.
- To learn how to collect cyber threat data.

SYLLABUS:

Unit	Content
Unit 1: Defining Cyber Threat Intelligence	The Need for Cyber Threat Intelligence: The menace of targeted attacks, The monitor-and-respond strategy, Why the strategy is failing, Cyber Threat Intelligence Defined, Key Characteristics: Adversary based, Risk focused, Process oriented, Tailored for diverse consumers, The Benefits of Cyber Threat Intelligence. **12 Hours**
Unit 2:Developing Cyber Threat Intelligence Requirements	Assets That Must Be Prioritized: Personal information, Intellectual property, Confidential business information, Credentials and IT systems information, Operational systems. Adversaries: Cybercriminals, Competitors and cyber espionage agents, Hacktivists. Intelligence Consumers: Tactical users, Operational users, Strategic users. **11 Hours**
Unit 3: Collecting Cyber Threat Information	Level 1: Threat Indicators, File hashes and reputation data, Technical sources: honeypots and scanners, Industry sources: malware and reputation feeds. Level 2: Threat Data Feeds, Cyber threat statistics, reports, and surveys, Malware analysis. Level 3: Strategic Cyber Threat Intelligence, Monitoring the underground, Motivation and intentions, Tactics, techniques, and procedures. **11 Hours**
Unit 4: Analyzing and Disseminating Cyber Threat Intelligence:	Information versus Intelligence, Validation and Prioritization: Risk scores, Tags for context, Human assessment. Interpretation and Analysis: Reports, Analyst skills, Intelligence platform, Customization. Dissemination: Automated feeds and APIs, Searchable knowledge base, Tailored reports. **11 Hours**

COURSE OUTCOMES:

- Examine the history and development of cyber intelligence operations and how those operations can integrate with other intelligence collection.
- Threat Study the technique to Develop Cyber Threat Intelligence Requirements.
- Evaluate the benefits and risks of the current cyber intelligence structure.
- Use the attributes of computer network exploitation, defense and attack within the intelligence context.

TEXT BOOK:

- Friedman, J., & Bouchard, M. (2015). ***Definitive Guide to Cyber Threat Intelligence: Using Knowledge about Adversaries to Win the War against Targeted Attacks*.** CyberEdge Group.

REFERENCE BOOK:

- Dalziel, H. (2014). ***How to define and build an effective cyber threat intelligence capability***. Syngress.
- Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., & Shakarian, P. (2017). ***Darkweb cyber threat intelligence mining***. Cambridge University Press.
- Gourley Bob, 2014, **—The Cyber Threat‖**, Create space Independent Pub.

Title: SECURED SYSTEM ADMINSTRATION
Type: Core
Credits: 03

Total Marks-80		Course Code: N5CS2	(Total Number of Periods) Hrs
Theory Exam Marks :50	Internal Marks:30	Min Passing:32	45

COURSE OBJECTIVES:

- To understand the principles, concepts, and challenges involved in network and system administration.
- To develop knowledge of system components, user administration, authentication, and access control mechanisms.
- To learn configuration management, maintenance procedures, troubleshooting, and security mechanisms for secure systems.
- To understand secure network services, monitoring, backup, recovery, and analytical administration practices.

SYLLABUS:

Unit	Content
Unit 1: Introduction to System Administration and Security Fundamentals	Introduction to Network and System Administration, Goals of System Administration, Applying Technology in an Environment, Human Role in Systems, Ethical Issues, Challenges of System Administration, Computer Security Concepts, Security Attacks, Security Services, Security Standards. **11 Hours**
Unit 2: System Components and User Administration	Computer System Components, Operating System Concepts, Processes and Filesystems, Host Management, Networked Hosts and Client–Server Computing, User Accounts and Groups, Login Environment, Authentication Concepts, Access Control and Permissions, Password Management, User Environment Configuration. **11 Hours**
Unit 3: Configuration, Maintenance and System Protection	Models of System Administration, Configuration Management, System Maintenance, Automation Concepts, Fault Diagnosis and Troubleshooting, System Integrity and Reliability, Intrusion Concepts, Malicious Software, Firewall Characteristics and Types, System Protection Practices. **11 Hours**
Unit 4: Network Services and Analytical Administration	Network Services, Application Level Services, Secure Shell (SSH), Transport Level Security Concepts, Logging and Monitoring, Backup and Recovery Concepts, Performance Analysis, Analytical System Administration, Network Management Security. **11 Hours**

COURSE OUTCOMES:

After successful completion of this course, students will be able to:

- Explain the concepts, policies, and security principles involved in system administration.
- Apply host management, user administration, authentication, and access control techniques in computing systems.

- Implement configuration management, maintenance, troubleshooting, and system security practices.
- Analyze network services, secure administration methods, monitoring, and recovery mechanisms for secure system operations.

TEXT BOOK:

- Principles of Network and System Administration — Mark Burgess, John Wiley & Sons Ltd., Second Edition, 2004, ISBN: 9780470868072.

REFERENCE BOOKS:

- The Practice of System and Network Administration — Thomas A. Limoncelli, Christina J. Hogan, and Strata R. Chalup, Pearson Education, Second Edition, 2007.
- UNIX and Linux System Administration Handbook — Evi Nemeth, Garth Snyder, Trent R. Hein, and Ben Whaley, Pearson Education, Fifth Edition, 2017.
- Windows Server Administration Fundamentals — William Panek, Wiley Publication, Second Edition, 2019.
- Network Security Essentials — William Stallings, Pearson Education, Sixth Edition, 2017.
- Analytical Network and System Administration — Mark Burgess, Wiley Publication, 2004.

Title: CLOUD SECURITY
Type: Core
Credits: 03

Total Marks-80		Course Code: N5CS3	(Total Number of Periods) Hrs
Theory Exam Marks :50	Internal Marks:30	Min Passing:32	45

COURSE OBJECTIVES:

- To introduce Cloud Computing terminology, definitions, and concepts
- To understand security design and architectural considerations in Cloud
- To understand Identity and Access Control mechanisms
- To apply best practices using cloud security design patterns
- To monitor, audit, and manage cloud applications securely

SYLLABUS:

Unit	Content
Unit 1: Fundamentals of Cloud Security Concepts	Overview of Cloud Security. Security Services: Confidentiality, Integrity, Authentication, Non-repudiation, Access Control. Basics of Cryptography: Conventional (Symmetric) Cryptography, Public Key Cryptography, Hash Functions, Authentication Mechanisms, Digital Signatures. **10 Hours**
Unit 2: Security Design and Architecture for Cloud	Security design principles for Cloud Computing. Comprehensive Data Protection. End-to-End Access Control. Common attack vectors and threats. Network and Storage Security. Secure Isolation Strategies. Virtualization Security Strategies. Inter-tenant Network Segmentation Strategies. Data Protection Strategies: Data retention, deletion and archiving procedures, Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key Management. **11 Hours**
Unit 3: Access Control and Identity Management	Access control requirements for Cloud Infrastructure. User Identification. Authentication and Authorization. Role-Based Access Control (RBAC). Multi-Factor Authentication (MFA). Single Sign-On (SSO). Identity Federation. Identity Providers and Service Consumers. Storage and Network Access Control Options. OS Hardening and Minimization. Verified and Measured Boot. Intrusion Detection and Prevention Systems. **11 Hours**
Unit 4: Cloud Security Design Patterns, Monitoring and Management	Introduction to Design Patterns. Cloud Security Design Patterns: Cloud Bursting, Geo-tagging, Secure Cloud Interfaces, Cloud Resource Access Control, Secure On-Premise Internet Access, Secure External Cloud. Monitoring and Auditing: Proactive Activity Monitoring, Incident Response, Monitoring Unauthorized Access, Malicious Traffic, Abuse of System

	Privileges, Events and Alerts. Auditing and Management: Record Generation, Reporting, Tamper-proof Audit Logs, Quality of Service (QoS), Secure Management, User Management, Identity Management, Security Information and Event Management (SIEM). **13 Hours**

COURSE OUTCOME:

- Understand the cloud concepts and fundamentals.
- Explain the security challenges in the cloud.
- Define cloud policy and Identity and Access Management.
- Understand various risks and audit and monitoring mechanisms in the cloud.
- Define the various architectural and design considerations for security in the cloud.

TEXT BOOK:

- Raj Kumar Buyya , James Broberg, andrzejGoscinski, "Cloud Computing:", Wiley 2013
- Dave shackleford, "Virtualization Security", SYBEX a wiley Brand 2013.
- Mather, Kumaraswamy and Latif, "Cloud Security and Privacy", OREILLY 2011

REFERENCE BOOK:

- Mark C. Chu-Carroll ―Code in the Cloud‖,CRC Press, 2011
- Mastering Cloud Computing Foundations and Applications Programming RajkumarBuyya, Christian Vechhiola, S. ThamaraiSelvi

Title: PROFESSIONAL ELECTIVE 3
Type: DSE
Credits: 03

Total Marks-80		Course Code: N5CS4	(Total Number of Periods) Hrs
Theory Exam Marks :50	Internal Marks:30	Min Passing:32	45

SUBJECT 1 – NETWORK SECURITY
COURSE OBJECTIVES:

- To understand fundamental concepts of network security, threats, and vulnerabilities.
- To study classical and modern encryption techniques used to secure data.
- To learn public key cryptography and authentication mechanisms.
- To analyze security protocols used in networks, email, and web applications.
- To develop knowledge of firewalls and practical network defense strategies.

SYLLABUS:

Unit	Content
Unit I: Introduction to Network Security & Threats	Security Trends and Challenges; Security Services and Security Attacks; Security Mechanisms; Model for Network Security; Authorization and Key Concepts; Malicious Software (Viruses, Worms, Trojan Horses); Multilevel Model of Security; Legal and Ethical Issues **11 Hours**
Unit II: Classical & Symmetric Cryptography	Symmetric Cipher Model; Substitution Techniques; Transposition Techniques; Block Cipher Principles; Data Encryption Standard (DES); Introduction to Modern Symmetric Encryption Concepts **11 Hours**
Unit III: Public Key Cryptography & Authentication	Principles of Public Key Cryptosystems; RSA Algorithm; Message Authentication Concepts; Authentication Functions; Message Authentication Codes (MAC); Hash Functions; Digital Signatures; Authentication Systems Overview; Password-Based and Address-Based Authentication; Cryptographic Authentication Protocols; Trusted Intermediaries; Authentication of People

	12 Hours
Unit IV: Network & Web Security Mechanisms	E-mail Security (PGP, S/MIME); IP Security Overview and Architecture; Web Security Concepts; Firewalls (Packet Filters, Application-Level Gateways, Encrypted Tunnels, Comparison); Web Issues (URLs/URIs, HTTP, Cookies); Web Security Problems and Threats **11 Hours**

COURSE OUTCOMES:

- Identify various types of security threats, attacks, and vulnerabilities in networks.
- Apply classical and modern encryption techniques for secure communication.
- Explain and implement public key cryptography and RSA-based systems.
- Analyze authentication mechanisms and message integrity techniques.
- Evaluate network security solutions such as firewalls, IP security, and web security protocols.

TEXT BOOK:

- Applied network security monitoring: collection, detection, and analysis chris sanders
- Network Security Essentials: Applications and Standards William Stallings

REFERENCE BOOK:

- Network Security: Private Communication in a Public World, Second Edition: Charlie Kaufman; Radia Perlman; Mike Speciner (Prentice Hall)
- Cryptography and Networking Security Principles & Practice (fourth edition) Willam Stallings
- The fundamentals of New Security - John F. Chavwan, Artch. House
- The Internet Security Guide Book - Juaniata.

SUBJECT 2 – CRYPTOCURRENCY AND BLOCK CHAIN TECHNOLOGY

COURSE OBJECTIVES:

- To understand the fundamentals of Blockchain technology
- To learn various blockchain protocols and consensus algorithms
- To study Bitcoin and cryptocurrency mechanisms
- To explore Blockchain platforms like Hyperledger Fabric and Ethereum
- To analyze real-world Blockchain applications and use cases

SYLLABUS:

Unit	Content
Unit I: Introduction to Blockchain	Blockchain and Public Ledgers; Blockchain as Public Ledger; Structure of Block; Transactions; The Chain and Longest Chain Rule; Permissioned Blockchain Model; Cryptographic Hash Functions; Properties of Hash Functions; Hash Pointers; Merkle Trees **11 Hours**
Unit II: Bitcoin and Cryptocurrency	Basics of Cryptocurrency; Creation of Coins; Payments and Double Spending; FORTH (precursor to Bitcoin scripting); Bitcoin Scripts; Bitcoin P2P Network; Transactions in Bitcoin Network; Block Mining; Block Propagation and Relay **11 Hours**
Unit III: Consensus Mechanisms & Bitcoin Consensus	Bitcoin Consensus; Proof of Work (PoW) and Hashcash; Bitcoin PoW; Attacks on PoW; Monopoly Problem; Proof of Stake (PoS); Proof of Burn; Proof of Elapsed Time; Bitcoin Miner; Mining Difficulty; Mining Pools; Permissioned Model and Use Cases**11 Hours**
Unit IV: Blockchain Platforms & Applications	Hyperledger Fabric Architecture (v1.1); Chaincode; Ethereum Network; Ethereum Virtual Machine (EVM); Transaction Fees; Mist Browser; Ether and Gas; Solidity; Smart Contracts; Truffle; Decentralized Applications (DApps);

	NFTs; Applications in Supply Chain, Logistics, Smart Cities, Finance, Banking, Insurance; **12 Hours**

COURSE OUTCOMES:

- Understand emerging abstract models for Blockchain Technology
- Identify major research challenges and technical gaps existing between theory and practice in the crypto currency domain.
- It provides conceptual understanding of the function of Blockchain as a method of securing distributed ledgers, how consensus on their contents is achieved, and the new applications that they enable.
- Apply hyperledger Fabric and Ethereum platform to implement the Block chain Application.

TEXT BOOK:

- Bashir and Imran, Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks, 2017.
- Andreas Antonopoulos, "Mastering Bitcoin: Unlocking Digital Cryptocurrencies", O'Reilly,

REFERENCE BOOK:

- Daniel Drescher, "Blockchain Basics", First Edition, Apress, 2017.
- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, 2016.
- Melanie Swan, "Blockchain: Blueprint for a New Economy", O'Reilly, 2015
- Ritesh Modi, "Solidity Programming Essentials: A Beginner's Guide to Build Smart Contracts for Ethereum and Blockchain", Packt Publishing.
- Handbook of Research on Blockchain Technology, published by Elsevier Inc. ISBN: 9780128198162, 2020.

Title: CLOUD SECURITY LAB
Type: SEC/LAB
Credits: 02

Total Marks-80		Course Code: N5CS5	(Total Number of Periods) Hrs
External Marks :25	Internal Marks:25	Min Passing:20	60

NOTE:

- Based on N5CS3.
- The list suggests the program set. Hence, the concerned staff may modify the list as needed (minimum 15).

LIST OF PRACTICLES:

1. Simulate a cloud scenario using CloudSim and run a scheduling algorithm
2. Simulate resource management and load balancing using CloudSim
3. Simulate log generation and perform log forensics using CloudSim
4. Simulate a secure file sharing system using CloudSim
5. Implement SLA-aware and fault-tolerant scheduling in CloudSim
6. Implement data anonymization techniques over a simple dataset (masking, k-anonymization, etc.)
7. Implement hybrid encryption (AES + RSA) for secure data transmission
8. Implement a digital signature mechanism for file integrity and authentication
9. Implement password hashing with salting using secure hash algorithms
10. Implement an encryption algorithm to protect images
11. Implement an image obfuscation mechanism (blur, pixelation, etc.)
12. Implement a role-based access control (RBAC) mechanism in a specific scenario
13. Implement an attribute-based access control (ABAC) mechanism based on a scenario
14. Implement a multi-factor authentication (MFA) system using password and OTP
15. Implement a token-based authentication system using JWT/OAuth

16. Simulate a key management system (KMS) for secure key generation and storage
17. Implement data protection techniques such as tokenization and data redaction
18. Develop a log monitoring system with alert generation and incident management
19. Develop a basic SIEM system with log aggregation and tamper-proof logging
20. Simulate a basic cloud environment setup using CloudSim (datacenter, VMs, cloudlets)

Title: Secured System Administration – LAB
Type: SEC/LAB
Credits: 02

Total Marks-50		Course Code: N5CS6	(Total Number of Periods) Hrs
External Marks :25	Internal Marks:25	Min Passing:20	60

NOTE:

- Based on N5CS2.
- The list suggests the program set. Hence, the concerned staff may modify the list as needed (minimum 15).

LIST OF PRACTICLES:

1 Study the basic components of a computer system and identify CPU, memory, storage devices, network devices, and peripheral devices.
2 Study different operating systems and explore basic operating system functions (process, memory, file, and device management).
3 Demonstrate file system operations: create, copy, move, rename, and delete files/directories using operating system commands.
4 Explore system processes and monitor running processes using system tools/commands.
5 Study host management and identify hostname, IP address, MAC address, and network configuration details.
6 Configure and create user accounts and groups in the operating system environment.
7 Perform user account management operations: modify, lock/unlock, enable/disable, and delete user accounts.
8 Study authentication mechanisms and configure password policies for users.
9 Configure file and folder access permissions and implement access control mechanisms.
10 Study user login environments and customize user profiles/environment variables.
11 Demonstrate system configuration management and system maintenance activities.
12 Create simple scripts for automating repetitive system administration tasks.
13 Perform fault diagnosis and troubleshooting of common system and network problems.
14 Study malicious software concepts and analyze system protection mechanisms.
15 Configure and study firewall settings and implement basic security rules.
16 Study logging, monitoring, backup, and recovery concepts using system administration tools.
17 Implement a CPU Scheduling Algorithm (FCFS, SJF, Round Robin) and analyze system performance.
18 Implement a Disk Scheduling Algorithm (FCFS, SSTF, SCAN, C-SCAN) and compare seek time performance.
19 Design a Password Strength Checking Algorithm and classify passwords based on security criteria.
20 Implement a Login Authentication Algorithm using username and password validation.
21 Design a User Access Control Algorithm for assigning permissions to users and groups.
22 Implement a File Backup Scheduling Algorithm to automate backup operations.
23 Develop a Log Analysis Algorithm for identifying failed login attempts and suspicious activities.
24 Design a Fault Detection Algorithm for identifying system failures from monitoring data.
25 Implement a Network Traffic Monitoring Algorithm for identifying abnormal activity patterns.
26 Develop a Firewall Rule Matching Algorithm for packet filtering and access control.

Title: LAB Based on Elective 3
Type: SEC/LAB
Credits: 02

Total Marks-50		Course Code: N5CS7	(Total Number of Periods) Hrs
External Marks :25	Internal Marks:25	Min Passing:20	60

NOTE:

- Based on N5CS4.
- The list suggests the program set. Hence, the concerned staff may modify the list as needed (minimum 15).

Subject 1 – NETWORK SECURITY

1. Study and demonstrate different types of network security attacks (DoS, phishing, malware)
2. Implement basic security services (confidentiality, integrity, authentication) in a sample system
3. Simulate different types of malware (virus, worm, Trojan) behavior in a controlled environment
4. Analyze network traffic and identify suspicious activity using packet capture tools
5. Study legal and ethical issues in network security with case analysis
6. Implement substitution cipher techniques (Caesar cipher, monoalphabetic cipher)
7. Implement transposition cipher techniques (rail fence, columnar transposition)
8. Implement Data Encryption Standard (DES) algorithm
9. Implement Advanced Encryption Standard (AES) algorithm
10. Compare performance of symmetric encryption algorithms (DES vs AES)
11. Implement RSA algorithm for encryption and decryption
12. Implement hash functions (MD5, SHA-256) for data integrity
13. Implement Message Authentication Code (MAC) for message verification
14. Implement digital signature scheme using hash and RSA
15. Implement password-based authentication system with secure storage
16. Configure and demonstrate firewall rules (packet filtering)
17. Simulate secure email communication using PGP concepts
18. Study and simulate IP security (IPSec) concepts
19. Analyze HTTP protocol, cookies, and identify web security vulnerabilities
20. Implement a simple secure web communication system using HTTPS (SSL/TLS)

SUBJECT 2 – CRYPTOCURRENCY AND BLOCK CHAIN TECHNOLOGY

1. Study and demonstrate the working of blockchain as a public ledger
2. Implement a basic blockchain structure (block, hash, previous hash)
3. Simulate transactions and add them to blocks in a blockchain
4. Implement cryptographic hash functions (SHA-256) and analyze their properties
5. Implement Merkle Tree construction for transaction verification
6. Simulate cryptocurrency transactions and wallet system
7. Demonstrate the concept of double spending and its prevention
8. Implement a simple Bitcoin-like transaction script system
9. Study and simulate Bitcoin P2P network communication
10. Simulate block mining process with nonce and hash calculation
11. Implement Proof of Work (PoW) consensus mechanism
12. Simulate mining difficulty adjustment in blockchain
13. Study and simulate attacks on PoW (51% attack concept)
14. Implement a basic Proof of Stake (PoS) mechanism
15. Analyze and simulate mining pools and reward distribution
16. Develop and deploy a simple smart contract using Solidity
17. Implement and test smart contracts using Truffle
18. Simulate transactions on the Ethereum network (test network)
19. Develop a basic decentralized application (DApp)
20. Implement a blockchain-based application for supply chain or voting system

Title: SEMINAR
Type: SEC
Credits: 01

Total Marks-50	Course Code: N5CS8		(Total Number of Periods) Hrs
	Internal Marks:50	Min Passing:20	30

Objectives

1. To develop presentation and communication skills among students.
2. To enhance analytical and research abilities in emerging areas of Data Analytics and related technologies.
3. To encourage independent learning and technical discussion.
4. To improve confidence in presenting technical topics before an audience.

Guidelines

1. Each student shall select a seminar topic related to Course or other Interdisciplinary and emerging technologies related to Computer Science and IT.
2. The seminar topic must be approved by the concerned faculty guide/coordinator.
3. Students should conduct literature survey and collect information from books, journals, research papers, and authentic online resources.
4. Each student shall prepare:
    - Seminar Report
    - PowerPoint Presentation
5. Duration of presentation shall be minimum 10 minutes followed by question-answer session.
6. Students are encouraged to use charts, graphs, case studies, and demonstrations wherever applicable.
7. Attendance and active participation during seminar sessions are compulsory.

Title: PROJECT PHASE I
Type: SEC
Credits: 02

Total Marks-50	Course Code: N5CS9		(Total Number of Periods) Hrs
	Internal Marks:50	Min Passing:20	60

Guidelines

1. The Project Phase I may be carried out individually or in a group of maximum 2 students.
2. The project topic should be related to the course, interdisciplinary domains, Data Analytics, or emerging technologies in Computer Science and IT.
3. The selected project should address a real-world problem, research problem, case study, or innovative application.
4. Each student/group shall work under the guidance of an internal project guide approved by the department.
5. Students are encouraged to select industry-oriented, research-based, or socially relevant projects.
6. Project Phase I shall mainly focus on the following activities:
    - Problem Identification
    - Literature Survey
    - Requirement Analysis
    - Feasibility Study
    - System Design / Architecture Design
    - Project Planning and Methodology
7. Students shall prepare and submit:
    - Project Synopsis
    - System Design Document
    - Project Plan and Timeline

Faculty: Science and Technology

Syllabus Prescribed for Three Year Six Semester UG Programme

B.Sc. CYBER SECURITY Part – III [NEP]

SEMESTER-VI

Title: MALWARE ANALYSIS
Type: Core
Credits: 03

Total Marks-80		Course Code: N6CS1	(Total Number of Periods) Hrs
Theory Exam Marks :50	Internal Marks:30	Min Passing:32	45

COURSE OBJECTIVES:

- To introduce the fundamentals of malware, types and its effects
- To enable to identify and analyse various malware types by static analysis
- To enable to identify and analyse various malware types by dynamic analysis
- To deal with detection, analysis, understanding, controlling, and eradication of malware

SYLLABUS:

Unit	Content
Unit 1: Introduction and Basic Analysis	Goals of Malware Analysis, AV Scanning, Hashing, Finding Strings, Packing and Obfuscation, PE file format, Static, Linked Libraries and Functions, Static Analysis tools, Virtual Machines and their usage in malware analysis, Sandboxing, Basic dynamic analysis, Malware execution, Process Monitoring, Viewing processes, Registry snapshots **12 Hours**
Unit 2: Advanced Static Analysis	The Stack, Conditionals, Branching, Rep Instructions, Disassembly, Global and local variables, Arithmetic operations, Loops, Function Call Conventions, C Main Method and Offsets. Portable Executable File Format, The PE File Headers and Sections, IDA Pro, Function analysis, Graphing, The Structure of a Virtual Machine, Analyzing Windows programs, Anti-static analysis techniques, obfuscation, packing, metamorphism, polymorphism. **11 Hours**
Unit 3: Advanced Dynamic Analysis	Live malware analysis, dead malware analysis, analyzing traces of malware, system calls, api calls, registries, network activities. Anti-dynamic analysis techniques, VM detection techniques, Evasion techniques, , Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wireshark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching **11 Hours**
Unit 4: Malware Functionality	Downloaders and Launchers, Backdoors, Credential Stealers, Persistence Mechanisms, Handles, Mutexes, Privilege Escalation, Covert malware launching- Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection **11 Hours**

COURSE OUTCOMES:

- Understand the various concepts of malware analysis and their technologies used.
- Possess the skills necessary to carry out independent analysis of modern malware samples using both static and dynamic analysis techniques
- Understand the methods and techniques used by professional malware analysts
- To be able to safely analyze, debug, and disassemble any malicious software by malware analysis

TEXT BOOK:

- Michael Sikorski and Andrew Honig, "Practical Malware Analysis" by No Starch Press, 2012,ISBN: 9781593272906
- Bill Blunden, "The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System", Second Edition,Jones & Bartlett Publishers, 2009.

REFERENCE BOOK:

- Jamie Butler and Greg Hoglund, "Rootkits: Subverting the Windows Kernel" by 2005, Addison-Wesley Professional.
- Bruce Dang, Alexandre Gazet, Elias Bachaalany, SébastienJosse, "Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation", 2014.

Title: PENETRATION TESTING
Type: Core
Credits: 03

Total Marks-80		Course Code: N6CS2	(Total Number of Periods) Hrs
Theory Exam Marks :50	Internal Marks:30	Min Passing:32	45

COURSE OBJECTIVES:

- Introduce Vulnerability Assessment and Penetration Testing
- To be familiar with the Penetration Testing and Tools
- To get an exposure to Metasploit exploitation tool, Linux exploit and Windows exploit
- To gain knowledge on Web Application Security Vulnerabilities, Vulnerability analysis and Malware analysis

SYLLABUS:

Unit	Content
Unit I: Fundamentals of Ethical Hacking & Social Engineering	Ethics of ethical hacking; attacker mindset; vulnerability assessment and penetration testing (VAPT); social engineering attacks; conducting attacks; common penetration testing techniques; face-to-face attacks; defense strategies; ethical and legal issues **11 Hours**
Unit II: Physical, Insider Attacks & Penetration Testing Tools	Physical penetration testing; building access methods; defense against physical attacks; insider threats; defenses; Metasploit framework; exploit execution; client-side attacks; Meterpreter; automation and scripting **11 Hours**
Unit III: Penetration Testing Management & Exploitation	Penetration testing planning; agreements; execution and reporting; Linux stack operations; buffer overflows; Windows exploitation; SEH; memory protections; bypass techniques; debugging and exploit development **11 Hours**
Unit IV: Web Security & Malware Analysis	Web application vulnerabilities; injection attacks; XSS; OWASP Top 10; source and binary analysis; browser-based exploits; heap spraying; malware collection; honeynet analysis; malware detection and protection **12 Hours**

COURSE OUTCOMES:

At the end of the course, the student will be able to:

- Explain the ethical considerations and legal implications in conducting ethical hacking activities using appropriate tools.
- Analyze social engineering, physical penetration and insider attacks using automating penetration testing processes.
- Identify report penetration tests effectively to develop and execute Linux and Windows exploits, bypassing memory protections.
- Illustrate web application security vulnerabilities to conduct vulnerability analysis.
- Inspect protection against client-side browser exploits.

TEXT BOOK:

1. Gray Hat Hacking - The Ethical Hackers Handbook, Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams, 3rd Edition, Tata McGraw-Hill.

REFERENCE BOOK:

1. The Web Application Hacker's Hand Book - Discovering and Exploiting Security flaws, Dafydd Suttard, Marcuspinto,1st Edition, Wiley Publishing.
2. Penetration Testing: Hands-on Introduction to Hacking, Georgia Weidman, 1st Edition, No 5 Starch Press.
3. The Pen Tester Blueprint - Starting a Career as an Ethical Hacker, L. Wylie, Kim Crawly,1st Edition, Wiley Publications.

Title: WEB APPLICATION SECURITY
Type: Core
Credits: 03

Total Marks-80		Course Code: N6CS3	(Total Number of Periods) Hrs
Theory Exam Marks :50	Internal Marks:30	Min Passing:32	45

COURSE OBJECTIVES:

- Understand fundamental concepts of web application security, including common threats, vulnerabilities, and defense mechanisms.
- Apply secure software development lifecycle practices to design, build, and deploy secure web applications.
- Design and implement secure APIs using modern authentication, authorization, and encryption techniques.
- Perform vulnerability assessment and penetration testing using industry-standard tools and methodologies.
- Analyze attacker techniques and think from a hacker's perspective to proactively identify and mitigate security risks.

SYLLABUS:

Unit	Content
Unit I: Fundamentals of Web Application Security	History and evolution of software security; Web application security concepts and importance; Common web application threats; Authentication and Authorization mechanisms; Secure communication using SSL/TLS; Session management and security; Input validation and secure coding basics. **10 Hours**
Unit II: Secure Development and Deployment	Secure web application architecture; Security testing techniques (static and dynamic); Security incident response planning; Secure Software Development Lifecycle models – Microsoft SDL, OWASP CLASP, Software Assurance Maturity Model (SAMM); Best practices for secure deployment. **10 Hours**
Unit III: Secure API Development and	API security fundamentals; Session cookies and token-based authentication; API security controls and threat mitigation; Rate limiting; Encryption

Protection	techniques; Audit logging and monitoring; Securing service-to-service APIs (API Keys, OAuth 2.0); Securing microservices (service mesh, network security, request validation); Injection attacks; Cross-Site Scripting (XSS); Cross-Site Request Forgery (CSRF); Broken authentication and session management. **13 Hours**
Unit IV: Vulnerability Assessment, Penetration Testing and Tools	Vulnerability Assessment lifecycle; Types of scanners (cloud-based, host-based, network-based, database-based); Penetration testing methodology; Social engineering; Security misconfiguration; Insecure cryptographic storage; Failure to restrict URL access; Tools: OpenVAS, Nexpose, Nikto, Burp Suite, Comodo. **12 Hours**

COURSE OUTCOMES:

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

TEXT BOOK:

- Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, First Edition, 2020, O'Reilly Media, Inc.

REFERENCE BOOK:

- Bryan Sullivan, Vincent Liu, Web Application Security: A Beginners Guide, 2012, The McGraw-Hill Companies.
- Neil Madden, API Security in Action, 2020, Manning Publications Co., NY, USA.
- Michael Cross, Developer's Guide to Web Application Security, 2007, Syngress Publishing, Inc.
- Ravi Das and Greg Johnson, Testing and Securing Web Applications, 2021, Taylor & Francis Group, LLC.

Title: PENETRATION TESTING-LAB
Type: SEC/LAB
Credits: 02

Total Marks-80		Course Code: N6CS4	(Total Number of Periods) Hrs
External Marks :25	Internal Marks:25	Min Passing:20	60

NOTE:

- Based on N6CS3.
- The list suggests the program set. Hence, the concerned staff may modify the list as needed (minimum 15).

LIST OF PRACTICLES:

1. Study ethical hacking principles and legal boundaries in cybersecurity
2. Simulate social engineering attacks (phishing or pretexting demo)
3. Demonstrate defense techniques against social engineering attacks
4. Perform basic physical penetration analysis (case study simulation)
5. Study insider attack scenarios and mitigation techniques
6. Install and configure Metasploit Framework
7. Perform basic exploitation using Metasploit console
8. Automate simple attacks using Metasploit modules
9. Demonstrate Meterpreter session and post-exploitation tasks
10. Perform Linux buffer overflow simulation
11. Study stack operations and exploit generation in Linux

12. Demonstrate Windows program debugging and exploitation basics
13. Study Structured Exception Handling (SEH) in Windows
14. Analyze Windows memory protection mechanisms and bypass concepts
15. Perform web application vulnerability testing (SQL Injection)
16. Demonstrate Cross-Site Scripting (XSS) attack and prevention
17. Perform source code analysis for vulnerability detection
18. Perform binary analysis for security flaws
19. Simulate browser-based exploit and heap spray concept
20. Collect and analyze malware behavior using controlled environment

Title: MALWARE ANALYSIS – LAB
Type: SEC/LAB
Credits: 02

Total Marks-50		Course Code: N6CS5	(Total Number of Periods) Hrs
External Marks :25	Internal Marks:25	Min Passing:20	60

NOTE:

- Based on N6CS2.
- The list suggests the program set. Hence, the concerned staff may modify the list as needed (minimum 15).

LIST OF PRACTICLES:

1. Experimentation on Initial Infection Vectors and Malware Discovery
2. Implementation on Sandboxing Malware and Gathering Information From Runtime Analysis
3. Implementation on Portable Executable (PE32) File Format
4. Implementation on Executable Metadata and Executable Packers
5. Experimentation on Malware Self - Defense, Compression, and Obfuscation Techniques
6. Experimentation on Malware behaviour analysis
7. Experimentation on analyzing Malicious Microsoft Office and Adobe PDF Documents
8. Experimentation on Mobile malware analysis
9. Experimentation on Packing and Unpacking of malware
10. Experimentation on Rootkit AntiForensics and Covert Channels
11. Experimentation on Modern Rootkit Analysis
12. Experimentation on Malware traffic analysis

Title: WEB APPLICATION SECURITY – LAB
Type: SEC/LAB
Credits: 02

Total Marks-50		Course Code: N6CS6	(Total Number of Periods) Hrs
External Marks :25	Internal Marks:25	Min Passing:20	60

NOTE:

- Based on N6CS4.
- The list suggests the program set. Hence, the concerned staff may modify the list as needed (minimum 15).

1. Study and demonstrate common web application threats (SQL Injection, XSS, CSRF) using a sample app
2. Implement user authentication and authorization (login system with roles)
3. Demonstrate secure communication using SSL/TLS (HTTPS setup)
4. Implement secure session management (session ID, timeout, cookies)
5. Perform input validation and demonstrate prevention of injection attacks
6. Design a secure web application architecture (3-tier or MVC model)

7. Perform static application security testing using SonarQube or similar tool
8. Perform dynamic application security testing using OWASP ZAP
9. Prepare a security incident response plan for a web application
10. Study and compare secure SDLC models (Microsoft SDL, OWASP CLASP, SAMM)
11. Deploy a web application securely on a server with best practices
12. Develop a REST API with token-based authentication (JWT)
13. Implement API security using OAuth 2.0 concepts
14. Implement rate limiting to prevent API abuse
15. Demonstrate protection against XSS and CSRF attacks
16. Implement secure session cookies and token handling
17. Implement audit logging and monitoring for API requests
18. Perform vulnerability scanning using OpenVAS
19. Perform web application testing using Burp Suite
20. Conduct penetration testing on a sample web application and prepare a report

Title: INTERNSHIP
Type: SEC
Credits: 02

Total Credits = 2	Course Code: N6CS7	(Total Number of Periods) Hrs

Note:
Internship will be conducted after Ist semester till Vth semester in vacations for minimum 60 hrs. It's 2 credits will be reflected in final semester credit grade report.

Title: PROJECT PHASE II
Type: SEC
Credits: 04

Total Marks-50		Course Code: N6CS8	(Total Number of Periods) Hrs
External Marks:50	Internal Marks:50	Min Passing:40	

Guidelines

1. The Project Phase II shall be a continuation of Project Phase I.
2. Students shall implement the system/application designed during Phase I under the guidance of the approved project guide.
3. The project must demonstrate originality, practical implementation, and applicability to real-world scenarios.
4. Students are encouraged to use modern tools, frameworks, datasets, and emerging technologies during implementation.
5. Project Phase II shall include the following activities:
    - System Implementation / Development
    - Testing and Validation
    - Result Analysis and Performance Evaluation
    - Deployment / Demonstration (if applicable)
    - Documentation and Report Preparation
    - Conclusion and Future Scope
6. The final submission shall include:
    - Complete Project Report
    - Source Code / Dataset / Implementation Details
    - User Manual (if applicable)
    - Project Presentation and Demonstration