VNR VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY HYDERABAD

B.TECH. MINOR IN CYBER SECURITY

TENTATIVE COURSE STRUCTURE AND SYLLABUS

(Applicable from the academic year 2021-2022)

V SEMESTER (III YEAR I SEMESTER) **R19**

Course Code	Title of the Course	L	T	P/D	Contact Hours/ Week	Credits
19MC1CY01	Principles of Information Security	3	0	0	3	3
19MC2CY01	Principles of Information Security Laboratory	0	0	3	3	1.5
Total		**3**	**0**	**3**	**6**	**4.5**

VI SEMESTER (III YEAR II SEMESTER) **R19**

Course Code	Title of the Course	L	T	P/D	Contact Hours/ Week	Credits
19MC1CY02	Foundations of Cyber Security	3	1	0	4	4
Total		**3**	**1**	**0**	**4**	**4**

VII SEMESTER (IV YEAR I SEMESTER) **R19**

Course Code	Title of the Course	L	T	P/D	Contact Hours/ Week	Credits
19ME1CY01	Ethical Hacking	3	0	0	3	3
19ME1CY02	Digital Forensics					
19ME2CY01	Ethical Hacking Laboratory	0	0	3	3	1.5
19ME2CY02	Digital Forensics Laboratory					
Total		**3**	**0**	**3**	**6**	**4.5**

VIII SEMESTER (IV YEAR II SEMESTER) **R19**

Course Code	Title of the Course	L	T	P/D	Contact Hours/ Week	Credits
19ME1CY03	Security Incident and Response Management	3	0	0	3	3
19ME1CY04	Mobile Security					
19ME1CY05	IoT Security					
19ME1CY06	Blockchain Technologies					
19ME1CY07	Authentication Techniques Cloud Security					
19MP1CY01	Mini-Project	0	0	4	4	2
Total		**3**	**0**	**4**	**7**	**5**

VNR VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

B.Tech. Minor (CYS) V Semester	**L**	**T/P/D**	**C**
	3	**0**	**3**

(19MC1CY01) PRINCIPLES OF INFORMATION SECURITY

COURSE OBJECTIVES:

- To understand computer networks, security attacks, services, and mechanisms
- To describe various cryptosystems- symmetric key cryptography and public key cryptography
- To apply authentication services, mechanisms, and secure hash algorithms
- To be familiar with the concepts of email security, IDS, SSL, TLS, viruses, and Firewalls

COURSE OUTCOMES: After completion of the course, the student should be able to

CO-1: Analyse the concepts of Computer Networks, Cryptography, Information security and its applications

CO-2: Build a security model to prevent and detect the attacks using various mechanisms

CO-3: Examine the authenticity of the messages, communicate securely and investigate non-repudiation

CO-4: Apply the concepts of SSL, TLS, firewalls and establish trusted systems

UNIT – I:

Introduction to Computer Networks, Network hardware, Network software, OSI and TCP/IP Reference models, Security attacks, Security Services and Mechanisms.

UNIT – II:

Integer Arithmetic, Modular Arithmetic, Traditional Symmetric Key Ciphers, Data Encryption Standard (DES), Advanced Encryption Standard (AES).

UNIT – III:

Mathematics of Cryptography: Primes, Primality Testing, Factorization, Chinese Remainder Theorem, Asymmetric Cryptography: Introduction, RSA Cryptosystem, Rabin Cryptosystem, Elliptic Curve Cryptosystem.

UNIT – IV:

Message Integrity and Message Authentication: Message Authentication Code (MAC), SHA-512 - Digital Signatures.

UNIT – V:

Security at the Application Layer: PGP and S/MIME. Security at Transport Layer: SSL and TLS. -Principles of IDS and Firewalls.

UNIT – VI:

Intrusion detection – password management – Viruses and related Threats – Virus Counter measures – Firewall Design Principles – Trusted Systems.

TEXTBOOKS:

1. Computer Networks, Andrew S Tanenbaum, David J. Wetherall, 5th Edition,

Pearson Education/PHI
2. Cryptography & Network Security, Behrouz A. Forouzan, Special Indian Edition, TMH

REFERENCES:

1. Network Security Essentials (Applications and Standards), William Stallings, Pearson Education
2. Cryptography and Network Security – Principles and Practices, William Stallings, 4th Edition, Prentice Hall of India, 2005
3. Security in Computing, Charles B. Pfleeger, Shari Lawrence Pfleeger, 3rd Edition, Pearson Education, 2003

VNR VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

B.Tech. Minor (CYS) V Semester	**L**	**T/P/D**	**C**
	0	**3**	**1.5**

(19MC2CS01) PRINCIPLES OF INFORMATION SECURITY LABORATORY

COURSE PRE-REQUISITES: A course on "Mathematics"

COURSE OBJECTIVES:

- To apply algorithms used for data encryption and decryption
- To demonstrate IDS Tools
- To apply algorithms used for message Integrity and Authentication of data
- To understand various protocols for information security to protect against the threats in the networks

COURSE OUTCOMES: After completion of the course, the student should be able to

CO-1: Implement various encryption and decryption algorithms
CO-2: Identify the emerging areas in information security
CO-3: Interpret good security practices for information security
CO-4: Demonstrate the process of data protection from various threats .

EXERCISES:

1. Write a program to perform encryption and decryption using the following substitution ciphers
   a) Caeser cipher
   b) Play fair cipher
   c) Hill Cipher
2. Write a program to implement the DES algorithm
3. Write a program to implement RSA algorithm
4. Calculate the message digest of a text using the SHA-1 algorithm
5. Working with sniffers for monitoring network communication (Wireshark)
6. Configuring S/MIME for email communication
7. Using Snort, perform real time traffic analysis and packet logging

TEXT BOOKS:

1. Cryptography and Network Security, William Stallings 3rd Edition, Pearson Education
2. Applied Cryptography, Bruce Schneier

REFERENCES:

1. Cryptography and Network Security, Behrouz A. Forouzan
2. Security in Computing, Charles B. Pfleeger, Shari Lawrence Pfleeger, 3rd Edition, Pearson Education, 2003

VNR VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

B.Tech. Minor (CYS) VI Semester	**L**	**T/P/D**	**C**
	3	**1**	**4**

(19MC1CY02) FOUNDATIONS OF CYBER SECURITY

COURSE OBJECTIVES:

- To introduce security attacks and access management
- To get an exposure to malwares, social engineering and counter measures
- To gain knowledge on Intrusion detection & prevention systems
- To understand software security and human resources security issues

COURSE OUTCOMES: After completion of the course, the student should be able to
CO-1: Categorize security threats and able to implement access control strategies
CO-2: Understand malicious software and apply methods to protect from denial-of-service attacks
CO-3: Analyze intrusion detection systems and configure firewalls
CO-4: Develop secure coding, infrastructure security and human resources security

UNIT – I:

Overview: Computer Security Concepts, Threats, Attacks, and Assets, Security Functional Requirements, Fundamental Security Design Principles, Attack Surfaces and Attack Trees, Computer Security Strategy.

Access Control: Access Control Principles, Subjects, Objects, and Access Rights, Discretionary Access Control, Example: UNIX File Access Control, Role-Based Access Control, Attribute-Based Access Control, Identity, Credential, and Access Management, Trust Frameworks, Case Study: RBAC System for a Bank.

UNIT – II:

Malicious Software: Types of Malicious Software (Malware), Advanced Persistent Threat, Propagation—Infected Content—Viruses, Propagation—Vulnerability Exploit—Worms, Propagation—Social Engineering—Spam E-Mail, Trojans, Payload—System Corruption, Payload—Attack Agent— Zombie, Bots, Payload—Information Theft—Keyloggers, Phishing, Spyware, Payload—Stealthing—Backdoors, Rootkits, Counter measures

UNIT – III:

Denial-of-Service Attacks: Denial-of-Service Attacks, Flooding Attacks, Distributed Denial-of-Service Attacks, Application-Based Bandwidth Attacks, Reflector and Amplifier Attacks, Defenses Against Denial-of-Service Attacks, Responding to a Denial-of-Service Attack. Buffer Overflow: Stack Overflows, Defending Against Buffer Overflows, Other Forms of Overflow Attacks.

UNIT – IV:

Intrusion Detection: Intruders, Intrusion Detection, Analysis Approaches, Host-Based Intrusion Detection, Network-Based Intrusion Detection, Distributed or Hybrid Intrusion Detection, Intrusion Detection Exchange Format, Honeypots, Example System: Snort. Firewalls and Intrusion Prevention Systems: The Need for Firewalls, Firewall Characteristics and Access Policy, Types of Firewalls, Firewall Basing, Firewall Location and Configurations, Intrusion Prevention Systems, Example: Unified Threat

Management Products.

UNIT – V:

Software Security: Software Security Issues, Handling Program Input, Writing Safe Program Code, Interacting with the Operating System and Other Programs, Handling Program Output. Physical and Infrastructure Security: Overview, Physical Security Threats, Physical Security Prevention and Mitigation Measures, Recovery from Physical Security Breaches, Example: A Corporate Physical Security Policy, Integration of Physical and Logical Security.

UNIT – VI:

Human Resources Security: Security Awareness, Training, and Education, Employment Practices and Policies, E-Mail and Internet Use Policies, Computer Security Incident Response Teams. Legal and Ethical Aspects: Cybercrime and Computer Crime, Intellectual Property, Privacy, Ethical Issues.

TEXT BOOKS:

1. Computer Security: Principles and Practice, William Stallings, Prentice Hall; 2014
2. Foundations of Security: What Every Programmer Needs to Know by Neil Daswani, Christoph Kern and Anitha Kesavan, Apress publisher, 2007

REFERENCES:

1. The ethical hacking guide to corporate security, Ankit Fadia, McMillan India
2. Software Security: Building Security In, G. McGraw, Addison Wesley, 2006

VNR VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

B.Tech. Minor (CYS) VII Semester	**L**	**T/P/D**	**C**
	3	**0**	**3**

(19ME1CY01) ETHICAL HACKING

COURSE OBJECTIVES:

- To learn concepts, techniques, and tools they need to deal with Ethical Hacking
- To understand the basic concepts of enumerations in Ethical Hacking
- To identify the importance of advanced hacking techniques and their countermeasures
- To be familiar with the concepts of Exploitation and Deliverable

COURSE OUTCOMES: After completion of the course, the students should be able to
CO-1: Apply the knowledge of tools available to support an ethical hacking
CO-2: Implement the knowledge of interpreting the results of a controlled attack
CO-3: Understand the role of politics, inherent & imposed limitations, and metrics for planning of a test
CO-4: Evaluate techniques related for the enumeration and exploitation

UNIT – I:

Introduction: Hacking Impacts, The Hacker Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration
Information Security Models: Computer Security, Network Security, Service Security, Application Security, Security Architecture
Information Security Program: The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking

UNIT – II:

The Business Perspective: Business Objectives, Security Policy, Previous Test Results, Business Challenges Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement

UNIT – III:

Preparing for a Hack: Technical Preparation, Managing the Engagement Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance

UNIT – IV:

Enumeration: Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase

UNIT – V:

Exploitation: Intuitive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, RootKits, applications, Wardialing, Network, Services and Areas of Concern

UNIT – VI:

Deliverable: The Deliverable, The Document, Overall Structure, Aligning Findings, Presentation Integration: Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy, Conclusion

TEXT BOOK:

1. The Ethical Hack: A Framework for Business Value Penetration Testing, James S. Tiller, Auerbach Publications, CRC Press

REFERENCES:

1. Ethical Hacking and Countermeasures Attack Phases, EC-Council, Cengage Learning
2. Hands-On Ethical Hacking and Network Defense, Michael Simpson, Kent Backman, James Corley, Cengage Learning

VNR VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

B.Tech. Minor (CYS) VII Semester	**L**	**T/P/D**	**C**
	3	**0**	**3**

(19ME1CY02) DIGITAL FORENSICS

COURSE OBJECTIVES:

- To learn the concepts of the rapidly changing and fascinating field of computer forensics
- To be familiar with the technical expertise and the knowledge required to investigate, detect, and prevent digital crimes
- To identify the approaches on digital forensics legislations, digital crime, forensics processes and procedures
- To understand perceptions of E-evidence collection, preservation, network forensics, art of steganography and mobile device forensics

COURSE OUTCOMES: After completion of the course, the students should be able to

CO-1: Understand relevant legislation and codes of ethics

CO-2: Apply the methods of computer forensics, digital detective, policies, and procedures

CO-3: Implement the approaches of E-evidence, tools, and environment

CO-4: Evaluate the methodologies of e-mail, web forensics and network forensics

UNIT – I:

Digital Forensics Science: Forensics science, computer forensics, and digital forensics.

Computer Crime: Criminalistics as it relates to the investigative process, analysis of cyber criminalistics area, holistic approach to cyber-forensics

UNIT – II:

Cyber Crime Scene Analysis: Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation

UNIT – III:

Evidence Management & Presentation: Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, explain what the normal case would look like, define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause.

UNIT – IV:

Computer Forensics: Prepare a case, begin an investigation, understand computer forensics, workstations and software, Conduct an investigation, Complete a case, Critique a case

UNIT – V:

Network Forensics: open-source security tools for network forensic analysis, requirements for preservation of network data.

UNIT – VI:

Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008.

Recent trends in mobile forensic technique and methods to search and seizure electronic evidence

TEXT BOOK:

1. The Basics of Digital Forensics, John Sammons, Elsevier
2. Computer Forensics: Computer Crime Scene Investigation, John Vacca, Laxmi Publications

REFERENCES:

1. Learn Computer Forensics: A Beginner's Guide to Searching, Analyzing, and Securing Digital Evidence, William Oettinger, 1st Edition, Packt Publishing, 2020, ISBN: 1838648178
2. Cybercrime and Digital Forensics: An Introduction, Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar, Routledge

VNR VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

B.Tech. Minor (CYS) VII Semester	**L**	**T/P/D**	**C**
	0	**3**	**1.5**

(19ME2CY01) ETHICAL HACKING LABORATORY

COURSE OBJECTIVES:

- To introduce the methodologies framework tools of ethical hacking to get awareness in enhancing the security
- To get knowledge on various attacks and their detection
- To understand various security tools

COURSE OUTCOMES: After completion of the course, the student should be able to

CO-1: Gain the knowledge of the use and availability of tools to support an ethical hack

CO-2: Gain the knowledge of interpreting the results of a controlled attack

CO-3: Apply various tools to provide security against attacks

LIST OF EXPERIMENTS:

1. Set Up a honey pot and monitor the honey pot on network
2. Write a script or code to demonstrate SQL injection attacks
3. Create a social networking website login page using phishing techniques
4. Write a code to demonstrate DoS attacks
5. Install rootkits and study variety of options
6. Study of Techniques uses for Web Based Password Capturing.
7. Install jcrypt tool (or any other equivalent) and demonstrate Asymmetric, Symmetric Crypto algorithm, Hash and Digital/PKI signatures studied in theory Network Security and Management
8. Implement Passive scanning, active scanning, session hijacking, cookies extraction using Burp suit tool

TEXT BOOK:

1. The Ethical Hack: A Framework for Business Value Penetration Testing, James S. Tiller, Auerbach Publications, CRC Press

REFERENCES:

1. Ethical Hacking and Countermeasures Attack Phases, EC-Council, Cengage Learning
2. Hands-On Ethical Hacking and Network Defense, Michael Simpson, Kent Backman, James Corley, Cengage Learning

VNR VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

B.Tech. Minor (CYS) VII Semester	**L**	**T/P/D**	**C**
	0	**3**	**1.5**

(19ME2CY02) DIGITAL FORENSICS LABORATORY

COURSE OBJECTIVES:

- To provide a comprehensive overview of collecting, investigating, preserving, and presenting evidence of cybercrime left in digital storage devices, emails, browsers, mobile devices using different Forensics tools
- To understand file system basics and where hidden files may lie on the disk, as well as how to extract the data and preserve it for analysis
- To understand some of the tools of e-discovery
- To understand the network analysis, Registry analysis and analyse attacks using different forensics tools

COURSE OUTCOMES: After completion of the course, the student should be able to
CO-1: Learn the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrongdoing
CO-2: Learn the file system storage mechanisms and retrieve files in hidden format
CO-3: Learn the use of computer forensics tools used in data analysis
CO-4: Learn how to find data that may be clear or hidden on a computer disk, find the open ports for the attackers through network analysis, Registry analysis

LIST OF EXPERIMENTS:

1. Perform email analysis using the tools like Exchange EDB viewer, MBOX viewer and View user mailboxes and public folders, Filter the mailbox data based on various criteria, Search for particular items in user mailboxes and public folders
2. Perform Browser history analysis and get the downloaded content, history saved logins, searches, websites visited etc using Foxton Forensics tool, Dumpzilla.
3. Perform mobile analysis in the form of retrieving call logs, SMS log, all contacts list using the forensics tool like SAFT
4. Perform Registry analysis and get boot time logging using process monitor tool
5. Perform Disk imaging and cloning the using the X-way Forensics tools
6. Perform Data Analysis i.e History about open file and folder, and view folder actions using List view activity tool
7. Perform Network analysis using the Network Miner tool.
8. Perform information for incident response using the crowd Response tool
9. Perform File type detection using Autopsy tool
10. Perform Memory capture and analysis using the Live RAM capture or any forensic tool

TEXT BOOKS:

1. Real Digital Forensics for Handheld Devices, E. P. Dorothy, Auerbach Publications, 2013
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012

REFERENCES:

1. Handbook of Digital Forensics and Investigation, E. Casey, Academic Press, 2010
2. Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, C. H. Malin, E. Casey and J. M. Aquilina, Syngress, 2012
3. The Best Damn Cybercrime and Digital Forensics Book Period, J. Wiles and A. Reyes, Syngress, 2007