MARRI LAXMAN REDDY
INSTITUTE OF TECHNOLOGY AND MANAGEMENT
(AN AUTONOMOUS INSTITUTION)
(Approved by AICTE, New Delhi & Affiliated to JNTUH, Hyderabad)
Accredited by NAAC with 'A' Grade & Recognized Under Section 2(f) & 12(B) of the UGC act,1956

Department of Computer Science and Engineering

B.Tech. with Honour Degree Program in Cyber Security

Marri Laxman Reddy Institute of Technology & Management
Dundigal, Quthbullapur Mandal, Hyderabad -500043, India

MARRI LAXMAN REDDY
INSTITUTE OF TECHNOLOGY AND MANAGEMENT
(AN AUTONOMOUS INSTITUTION)
(Approved by AICTE, New Delhi & Affiliated to JNTUH, Hyderabad)
Accredited by NAAC with 'A' Grade & Recognized Under Section 2(f) & 12(B) of the UGC act,1956

B.Tech. with Honour Degree Program in Cyber Security

Course Structure (2024-25)

(Applicable for 2024-2025 Batch-R24 Syllabus)

S. No.	Sem	Course Code	Course Title	Course Area	Hours Per Week			Credits	Scheme of Examination Maximum Marks		
					L	T	P		Internal (CIE)	External (SEE)	Total
1	V	245HDCSE501	Principles of Information Security	PC	4	0	0	4	40	60	100
2	V	245HDCSE530	Principles of Information Security Lab	PC	0	0	2	1	40	60	100
3	VI	245HDCSE502	Foundations of Cyber Security	PC	4	0	0	4	40	60	100
4	VI	245HDCSE503	Ethical Hacking	PC	4	0	0	4	40	60	100
5	VI	245HDCSE531	Ethical Hacking Lab	PC	0	0	2	1	40	60	100
6	VII	245HDCSE504	Security Incident & Response Management	PC	3	0	0	3	40	60	100
7	VIII		Project	PS	3	0	0	3	100	-	100
		Total Credits			**18**	**0**	**2**	**20**	**380**	**420**	**700**

Department of Computer Science Engineering
B.Tech Cyber Security (Honour)

Principles of Information Security

III Year-I Semester

L	T	P	C
4	0	0	4

Prerequisites

1. A course on "Mathematics"

Objectives:

1. To understand the fundamentals of Computer Networks.
2. To understand the fundamentals of Cryptography.
3. To understand various symmetric and asymmetric encryption algorithms.
4. To understand Mathematics of cryptography, IDS and Firewalls.
5. To apply algorithms used for message integrity and authentication.

Outcomes

1. Demonstrate the knowledge of Computer networks, cryptography, information security concepts and applications.
2. Ability to apply security principles in system design.

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 stander (DES), advanced encryption standerd (AES)

UNIT III

Mathematics of cryptography: primes, primality testing, factorization, Chinese reminder 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.

Text Books:

1. Computer Networks, Andrew S Tanenbaum, David. J. Wetherall, 5th edition, Person Education/PHI.
2. Cryptography & Network Security by Behrouz A. Forouzan Special Indian Edition, TMH.

Reference Book:

1. Network Security Essentials (Applications and Standards), William Stallings Pearson Education.

Department of Computer Science Engineering
B.Tech Cyber Security (Honour)

Principles of Information Security Lab

III Year-I Semester

L	T	P	C
0	0	2	1

Prerequisites

A course on "Mathematics"

Objectives

1. To apply algorithms on various symmetric and asymmetric encryption algorithms.
2. To demonstrate IDS tools.
3. To apply algorithms used for message integrity and authentication.

Lab Exercises

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

Text Books:

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

Reference Book:

1. Cryptography and Network Security by Behrouz A. Forouzan.

Department of Computer Science Engineering
B.Tech Cyber Security (Honour)

Foundations of Cyber Security

III Year-II Semester

L	T	P	C
4	0	0	4

Pre-requisites:

- Knowledge in information security and applied cryptography.
- Knowledge in Operating Systems.

Course Objectives:

1. To introduce security attacks.
2. To get an exposure to malwares.
3. To gain knowledge on Intrusion detection & prevention systems.

Course Outcomes: Students will learn the fundamental concepts required in the field of cyber 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—Key loggers, Phishing, Spyware, Payload—Stealthing— Backdoors, Rootkits, Counter measures.

Denial-of-Service Attacks: Denial-of-Service Attacks, Flooding Attacks, Distributed Denial-of- Service Attacks, Application-Based Bandwidth Attacks, Reflector and Amplifier Attacks, Defences 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 - III

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 – IV

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 - V

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 BOOK:

1. William Stallings, "Computer Security: Principles and Practice", Prentice Hall. Prentice Hall; 2014.

REFERENCE BOOKS:

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

Department of Computer Science Engineering
B.Tech Cyber Security (Honour)

ETHICAL HACKING

B.Tech. III Year II Sem **L T P C**
4 0 0 4

Course Objectives:

- The aim of the course is to introduce the methodologies and framework of ethical hacking for enhancing the security.
- The course includes-Impacts of Hacking; Types of Hackers; Information Security Models;
- Information Security Program; Business Perspective; Planning a Controlled Attack; Framework of Steps (Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Deliverable and Integration)

Course Outcomes:

- Gain the knowledge of the use and availability of tools to support an ethical hack
- Gain the knowledge of interpreting the results of a controlled attack
- Understand the role of politics, inherent and imposed limitations and metrics for planning of a test
- Comprehend the dangers associated with penetration testing

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. **Exploitation:** Intutive Testing,

Evasion, Threads and Groups, Operating Systems, Password Crackers, RootKits, applications, Wardialing, Network, Services and Areas of Concern.

UNIT – V

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

TEXT BOOK:

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

REFERENCE BOOKS:

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

Department of Computer Science Engineering
B.Tech Cyber Security (Honour)

ETHICAL HACKING LAB

B.Tech. III Year II Sem.

L	T	P	C
0	0	2	1

Course Objectives

- The aim of the course is 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

Course Outcomes

- Gain the knowledge of the use and availability of tools to support an ethical hack
- Gain the knowledge of interpreting the results of a controlled attack

List of Experiments

1. Install rootkits and study variety of options
2. Study of Techniques uses for Web Based Password Capturing.
3. 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
4. Implement Passive scanning, active scanning, session hizaking, cookies extraction using
5. Burp suit tool
6. Use a cryptographic algorithm to encrypt and decrypt passwords.
7. Use google and whois for reconnaissance.
8. Use NMAP scanner to perform port scanning of various forms.
9. Perform ARP poisoning for windows.
10. Simulate cross-site scripting attack.
11. Session impersonation using Firefox and Tamper Data add-on.
12. Create a simple Keylogger using python.
13. Using Metasploit to exploit using Linux.

Department of Computer Science Engineering
B.Tech Cyber Security (Honour)

SECURITY INCIDENT AND RESPONSE MANAGEMENT

B.Tech. IV Year I Sem. **L T P C**
3 - - 3

Prerequisites:
- Knowledge in information security and applied cryptography.

Course Objectives:
1. Introduce preparation of inevitable incident and incident detection and characterization.
2. To get an exposure to live data collection, Forensic duplication.
3. To gain knowledge on data analysis including Windows and Mac OS Systems.

Course Outcomes:
1. Learn how to handle the incident response management.
2. Perform live data collection and forensic duplication.
3. Identify network evidence.
4. Analyze data to carry out investigation.

UNIT - I

Introduction: Preparing for the Inevitable incident: Real world incident, IR management incident handbook, Pre-incident preparation, Preparing the Organization for Incident Response, Preparing the IR team, Preparing the Infrastructure for Incident Response. Incident Detection and Characterization: Getting the investigation started on the right foot, collecting initial facts, Maintenance of Case Notes, Understanding Investigative Priorities. Discovering the scope of incident: Examining initial data, Gathering and reviewing preliminary evidence, determining a course of action, Customer data loss scenario, Automated clearing fraud scenario.

UNIT - II

Data Collection: Live Data Collection: When to perform live response, Selecting a live response tool, what to collect, collection best practices, Live data collection on Microsoft Windows Systems, Live Data Collection on Unix-Based Systems. Forensic Duplication: Forensic Image Formats, Traditional duplication, Live system duplication, Duplication of Enterprise Assets.

UNIT - III

Network Evidence: The case for network monitoring, Types for network monitoring, Setting Up a Network Monitoring System, Network Data, Analysis, Collect Logs Generated from Network Events. Enterprise Services: Network Infrastructure Services, Enterprise Management Applications, Web servers, Database Servers

UNIT - IV

Data Analysis: Analysis Methodology: Define Objectives, Know your data, Access your data, Analyse your data, Evaluate Results. Investigating Windows Systems: NTFS and File System analysis, Prefetch, Event logs, Scheduled Tasks, The Windows Registry, Other Artifacts of Interactive Sessions, Memory Forensics, Alternative Persistence Mechanisms.

UNIT - V

Investigating Mac OS X Systems: HFS+ and File System Analysis, Core Operating systems data. Investigating Applications: What is Application Data?, Where is application data stored?, General Investigation methods, Web Browser, Email Clients,

Instant Message Clients.

TEXT BOOKS:

1. "Incident Response and Computer Forensics", Jason T. Luttgens, Mathew Pepe
   and Kevin Mandia, 3rd Edition, Tata McGraw-Hill Education.
2. "Cyber Security Incident Response-How to Contain, Eradicate, and Recover
   from Incidents", Eric. C. Thompson, Apress.

REFERENCE BOOKS:

1. "The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk", N.K. McCarthy, Tata McGraw-Hill.