Course Syllabus
Gyanmanjari College of Computer Application
Semester-2 (MCA)

Subject: Network and Cyber Security - MCAXX11511

Type of course: Minor Stream

Prerequisite: Basic Knowledge of Network

Rationale:

- Protection Against Cyber Threats
- Data Privacy and Confidentiality.
- National Security.
- Technological Advancements
- Education and Awareness

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks					Total Marks
				Theory Marks		Practical Marks		CA	
CI	T	P	C	ESE	MSE	V	P	ALA	
3	0	2	4	60	30	10	20	30	150

Legends: CI-Class Room Instructions; T – Tutorial; P - Practical; C – Credit; ESE - End Semester Examination; MSE- Mid Semester Examination; V – Viva; CA - Continuous Assessment; ALA- Active Learning Activities.

Course Content:

Sr. No	Course content	Hrs	% Weightage
1	**Introduction to Network Security & Cyber Security** Concepts: Network Security and its need, CIA (Confidentiality, Integrity, Availability), AAA (Authentication, Authorization, Accounting), Working of DNS, DHCP, IDS (Intrusion Detection System), IPS (Intrusion Prevention System), Firewall and its types, Web Proxies, Internet Security Protocols	9	20

2	**Cryptography Techniques** Cryptography, Cryptanalysis, Model for Network Security, OSI Security Architecture, Security Service, Security Mechanism, Security Attack, Symmetric Cipher Model (Conventional Encryption), Classification of Cryptography: Symmetric Key Cryptography (Substitution techniques: Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polyalphabetic Ciphers, One-Time Pad), Transposition techniques.	10	20
3	**Cryptography & IP Security** Key Terms: Encryption, Decryption, Plain Text, Cipher Text, Secret Code, Stream ciphers and block ciphers, Data Encryption standard (DES) with example, AES (Advanced Encryption Standard), Secret Key Cryptography, Public Key Cryptography, Digital Signatures, IP Security Architecture – Authentication Header, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange (IKE).	10	20
4	**Network Security Assessment** Passive Information Gathering: IP Address & Domain Identification, Port Scanning and its techniques, Port Scanning Tools (Nmap, Zenmap, Superscan), OS Fingerprinting – Active & Passive.Traffic Capturing Tools (Wireshark), Packet Analysis, Protocol Analysis, Traffic Timeline Analysis	8	20
5	**Introduction to Cyber Crime and Law** Cyber Crimes, Types of Cybercrime, Hacking, Attack vectors, Cyberspace and Criminal Behavior, Clarification of Terms, Traditional Problems Associated with Computer Crime, Introduction to Incident Response, Digital Forensics, Computer Language, Network Language, Realms of the Cyber world, A Brief History of the Internet, Recognizing and Defining Computer Crime, temporary Crimes, Computers as Targets, Contaminants and Destruction of Data, Indian IT ACT 2000.	8	20

Continuous Assessment:

Sr. No	Active Learning Activities	Marks
1	**Simulation:** Student have to create a network simulation in Packet Tracer tool on given problem and upload image of that network on GMIU Web Portal.	10
2	**Interview Preparation Test:** An Interview Preparation Test based on networking will be taken on the GMIU Web Portal.	10

3	**Review Paper:** Students have to prepare review paper and prepare PDF and upload it on GMIU web portal. Students have to perform this activity in group (Maximum 4 students in one group)	10
Total		30

Suggested Specification table with Marks (Theory):60

Distribution of Theory Marks **(Revised Bloom's Taxonomy)**						
Level	Remembrance (R)	Understanding (U)	Application (A)	Analyze (N)	Evaluate (E)	Create (C)
Weightage	30%	25%	25%	10%	10%	0

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Course Outcome:

After learning the course the students should be able to:	
CO1	Understand various network security and cyber security concepts, devices used to enhance security of networks.
CO2	Get Knowledge about various Classification of Cryptography, Symmetric Cipher Model, Substitution techniques and Transposition techniques.
CO3	Understand various devices present across network, identify the open ports on the active devices, identify the OS information and banner information of various servers.
CO4	Grasp ideas of various devices present across network, identify the open ports on the active devices, identify the OS information of various servers and machines. Learn and capture traffic from the active network, analyze packets & protocols.
CO5	Learn and analyze the cyber laws

List of Practical

Sr.No	Title	Unit No.	Approx. Hrs. Req
1.	Implement Caesar cipher encryption-decryption.	II	2
2.	Implement Monoalphabetic cipher encryption-decryption.	II	2
3.	Implement Playfair cipher encryption-decryption.	II	2
4.	Implement Polyalphabetic cipher encryption-decryption.	II	2
5.	Implement Hill cipher encryption-decryption.	II	2

6.	Implement Simple DES Algorithm.	III	4
7.	Implement Simple AES Algorithm.	III	4
8.	Perform various encryption-decryption techniques with cryptool.	II	2
9.	Implement a digital signature algorithm.	III	2
10.	Perform port scanning using various methods & techniques provided by Nmap or Zenmap.	IV	2
11.	Implement a packet capturing tool (Wireshark) and capture the real time traffic.	IV	2

Instructional Method:

The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

From the content 10% topics are suggested for flipped mode instruction.

Students will use supplementary resources such as online videos, NPTEL/SWAYAM videos, e-courses, Virtual Laboratory.

The internal evaluation will be done on the basis of Active Learning Assignment.

Practical/Viva examination will be conducted at the end of semester for evaluation of performance of students in laboratory.

Reference Books:

[1] **Cryptography and Network Security**: **Principles and Practice** - William Stallings - Pearson Publication
[2] **Build Your Own Security Lab**: **A Field Guide for Network Testing** - Nicholas Marsh - Wiley Publishing
[3] **Networking Monitoring And Analysis**: **A Protocol Approach to Troubleshooting** - ED Wilson- Prentice Hall PTR
[4] **Network Security Assessment**: **Know your Network**- Chris McNab- O'Reilly Publication