



MANGALAYATAN
UNIVERSITY
Learn Today to Lead Tomorrow

NAAC
GRADE A+
Accredited University

MCA

Master of Computer Applications



Contact us

www.mangalayatan.in
www.mude.ac.in


Advance Cyber Security

CSM-6212

Credit - 4

Course Objectives

The Primary Objective of Advanced Cyber Security is to Equip Individuals with the Knowledge, Skills, and Tools Necessary to Protect Digital Assets, Networks, and Information Systems from Cyber Threats and Attacks.



Through Advanced Training in Cyber-security Concepts, Techniques, and Technologies, this Course Aims to Enable Participants to Identify, Assess, and Mitigate a Wide Range of Cyber Risks and Vulnerabilities Effectively.

By Delving into Topics Such as Threat Intelligence, Penetration Testing, Incident Response, Cryptography, and Secure Coding Practices, the Course Aims to Empower Cyber-security Professionals to Safeguard Organizations' Data, Privacy, And Reputation in an Increasingly Complex and Dynamic Threat Landscape.

Course

Outcomes



Apply IT Act (Cyber Law) to the Given Case/Problem and Infer from the Given Case and Analyze the Gap if It Exists.



Analyze the Working of Cyber Security Principles in Designing the System.



Develop a Strategy (Physical, Logical or Administrative Controls) to Mitigate the Problem and Articulate Consequences on Society and National Economy.



Examine Relevant Network Defense / Web Application Tools to Solve Given Cyber Security Problems and Evaluate Its Suitability.



Investigate the Influence of Block Chain Technology for the Cyber Security Problem and Evaluate Its Role.

Block I

Introduction to Cyber Crime and Laws

Unit 1

Introduction, Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security

Unit 2

Cybercriminals, Classifications of Cyber Crimes

Unit 3

Criminals Plan Them- Introduction, How Criminals Plan the Attacks

Unit 4

Cybercafé and Cybercrimes, Botnets, Attack Vector

Unit 5

Basic Text Markup, Images, Hypertext Links, Lists

Block II

Tools and Methods Used in Cybercrime

Unit 6

Introduction, Proxy Server and Anonymizers,
Password Cracking

Unit 7

Key Loggers and Spyware, Virus and Worms

Unit 8

Trojan and Backdoors, Steganography

Unit 9

DOS and DDOS Attack

Block III

Phishing and Identity Theft

Unit 10

Introduction, Phishing- Methods of Phishing

Unit 11

Phishing Techniques, Phishing Toolkits and Spy Phishing.
Identity Theft - PII

Unit 12

Types of Identity Theft, Techniques of ID Theft

Unit 13

Digital Forensics Science, Need for Computer Cyber forensics

Block IV

Command Lines and Backtracking

Unit 14

Unix Command Lines, Backtrack Linux

Unit 15

Mac Ports, Cygwin

Unit 16

Windows Power Shell, Net Cat Commands

Unit 17

Net Cat Uses, SSH

Block V

Network Defense Tools and Block Chain Technology

Unit 18

Firewalls and Packet Filters: Firewall Basics,
Packet Filter Vs Firewall

Unit 19

Firewall Protects a Network, Packet Characteristic to Filter,
Stateless Vs Stateful Firewalls

Unit 20

Network Address Translation (NAT) and Port Forwarding,
the basic of Virtual Private Networks

Book Reference:



Anti-Hacker Tool Kit (Indian Edition) by Mike Shema, Publication McGraw Hill. (Chapters: 2, 7, 8, 11) 2014, 4th Edition.



Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole and Sunit Belpure, Publication Wiley 2011.



Yogesh Singh, “Software Testing”, Cambridge University Press, New York.



Marc Roper, “Software Testing”, McGraw-Hill Book Co., London.



Boris Beizer, “Software System Testing and Quality Assurance”, Van Nostrand Reinhold, New York.
