MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu.

Estd. 2000

IQAC

MUST KNOW CONCEPTS

MKC

MCA

2021-22

Course Code & Course Name : 19CAC06 & Cyber Security

Year/Sem/Sec : II / III / -

S.No.	Term	Notation (Symbol)	Concept / Definition / Meaning / Units / Equation / Expression	Units
Unit-I : Planning For Cyber Security				
1.	Cyber security	--	It is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.	I
2.	Virus	--	It is a program that is loaded onto your computer without your knowledge and runs against your wishes.	I
3.	Malware	--	It is any software that infects and damages a computer system without the owner's knowledge or permission.	I
4.	Hacker	--	It is a person who breaks into computers, usually by gaining access to administrative controls.	I
5.	Trojan horses	--	Email viruses that can duplicate themselves, steal information, or harm the computer system.	I
6.	Password Cracking	--	Hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.	I
7.	Communication security	--	Protecting organization communication media, technology, and content.	
8.	Network security	--	It is the protection of networking components, connection and content.	I

9.	Information Security	--	Protection of information and its critical elements , including the systems and hardware that use , store or transmit that information.	I
10.	Availability	--	It guarantees that systems, applications and data are available to authenticated users when they need them.	I
11.	Integrity	--	It refers to the accuracy and completeness of data.	I
12.	Authenticity	--	It is assurance that a message, transaction, or other exchange of information is from the source it claims to be from.	I
13.	Non-repudiation	--	It ensures that no party can deny that it sent or received a message via encryption and/or digital signatures or approved some information.	I
14.	Confidentiality	--	It ensures that sensitive information are accessed only by an authorized person and kept away from those not authorized to possess them.	I
15.	Accountability	--	The principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information.	I
16.	Cyberspace	--	It is the environment in which communication over computer networks occurs.	I
17.	ISMS(Information Security Management System)	--	It is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives.	I
18.	Cyber Security standards	--	It may be defined as the set of rules that an organization has to comply in order to gain right for some particular things like for accepting online payment, for storing patient data and so on.	I

19.	Payment Card Industry Data Security Standard (PCI DSS)	--	A standard of the PCI Security Standards Council, provides guidance for maintaining payment security.	I
20.	Next-generation firewalls (NGFW)	--	Network security systems that can detect and block sophisticated attacks by enforcing security policies at the application, port, and protocol level.	I
21.	Operational security (OPSEC)	--	It is an analytical and risk management process that identifies the organization's critical information and developing a protection mechanism to ensure the security of sensitive information.	I
22.	Vulnerability	--	It is a threat that can be exploited by an attacker to perform unauthorized actions.	I
23.	Information Risk Management (IRM)	--	It is a form of risk mitigation through policies, procedures, and technology that reduces the threat of cyber attacks from vulnerabilities and poor data security and from third-party vendors.	I
24.	Risk Assessment	--	Used to identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.	I
25.	Security Policy	--	It is the statement of responsible decision makers about the protection mechanism of a company crucial physical and information assets.	I
Unit-II : Security Controls				
26.	Physical Security	--	It is the protection of personnel, data, hardware, etc., from physical threats that could harm, damage, or disrupt business operations or impact the confidentiality, integrity, or availability of systems and/or data.	II
27.	Preventive Controls	--	Attempt to prevent an incident from occurring.	II
28.	Detective Controls	--	Attempt to detect incidents after they have occurred.	II
29.	Corrective Controls	--	Attempt to reverse the impact of an incident.	II

30.	Deterrent controls	--	Attempt to discourage individuals from causing an incident.	II
31.	Honeypot	--	It looks like a real computer system, with applications and data, fooling cyber criminals into thinking it's a legitimate target.	II
32.	Intrusion Detection System (IDS)	--	It is a network security technology originally built for detecting vulnerability exploits against a target application or computer.	II
33.	Organizational Security Policy	--	Formal statement of rules by which people given access to organization's technology and information assets must abide.	II
34.	Computer Security Incident Response Teams(CSIRT)	--	A service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity.	II
35.	Information Asset	--	Everything that has a value to the organization.	II
36.	Public Data	--	This type of data is freely accessible to the public.	II
37.	Internal-only Data	--	This type of data is strictly accessible to internal company personnel or internal employees who are granted access.	II
38.	Confidential Data	--	Access to confidential data requires specific authorization and/or clearance.	II
39.	Restricted Data	--	It includes data that, if compromised or accessed without authorization, which could lead to criminal charges and massive legal fines or cause irreparable damage to the company.	II
40.	Document Management Systems	--	It provide an organized structure for your digital documents.	II
41.	Access Control Lists (ACL)	--	ACLs are used for limiting access to sensitive files for only those who need it.	II
42.	Packet-Filtering Firewalls	--	Compare each packet it receives to a set of pre-determined criteria and blocks them if it perceives them as a potential threat.	II
43.	Stateful Inspection Firewalls	--	These firewalls assess each packet and also check whether it is part of an approved TCP handshake.	II
44.	Security Information and Event Management (SIEM)	--	A SIEM system may be rules-based or use a statistical correlation engine to detect anomalies.	II

45.	Mobile Device Management(MDM)	--	MDM software allows for remote monitoring and control of mobile device access to the network.	II
46.	User Authentication	--	It is a process that allows a device to verify the identity of someone who connects to a network resource.	II
47.	Peripheral Ports	--	Device interfaces used to connect peripheral devices, such as CDs/DVDs, printers, user interface devices (e.g., keyboard, mouse, displays), and serial devices, such as handheld maintenance and diagnostic devices.	II
48.	User Interface Attacks	--	Generally target command-line interfaces and desktop applications to access OS resources or to manipulate the control system and its data.	II
49.	Mobile Device Security	--	It is a combination of strategies and tools that secure mobile devices against security threats.	II
50.	Phishing	--	Attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, in an electronic communication.	II
Unit-III : Cyber Security For Business Applications And Networks				
51.	Application management (AM)	--	It is the process of managing the operation, maintenance, versioning and upgrading of an application throughout its life cycle.	III
52.	Application life cycle management (ALM)	--	It is the process by which information technology and software development organizations create, deploy, and operate software over its full life cycle.	III
53.	Application Portfolio Management (APM)	--	It is the practice of governing and optimizing inventories of software applications to achieve precise business objectives.	III
54.	Application performance management (APM)	--	It is concerned with how well an application meets its intended purpose and performs as expected.	III
55.	Application Security	--	Use of software, hardware, and procedural solutions to protect applications from external threats.	III

56.	End User Developed Applications	--	Applications that are developed by end users, usually in a non-controlled IT environment.	III
57.	System Access	--	It is the capability that restricts access to business applications, mobile devices, systems, and networks to authorized individuals for specific business purposes.	III
58.	Multifactor Authentication	--	It refers to the use of more than one of the authentication means in the preceding list.	III
59.	Password-Based Authentication	--	The system compares the password to a previously stored password for that user ID, maintained in a system password file.	III
60.	Specific Account Attack	--	An attacker targets a specific account and submits password guesses until the correct password is discovered.	III
61.	Password Cracking	--	It is the process of recovering secret passwords stored in a computer system or transmitted over a network.	III
62.	Blacklist	--	A list of discrete entities, such as hosts, applications, or passwords, that have been previously determined to be associated with malicious activity and are not approved for use within an organization and/or information system.	III
63.	Biometric Authentication	--	Attempts to authenticate an individual based on his or her unique physical characteristics.	III
64.	Presentation Attack	--	Attempts to mimic a biometric feature to sufficient fidelity so it is accepted as valid by the system—an attack known as biometric spoofing.	III
65.	Access control	--	The process of granting or denying specific requests for obtaining and using information and related information processing services to enter specific physical facilities.	III
66.	Access Control Policy	--	Dictates what types of access are permitted, under what circumstances, and by whom.	III
67.	Role-Based Access Control	--	It is based on the roles that users assume in a system rather than on the user's identity.	III

68.	Virtualization	--	It refers to a technology that provides an abstraction of the computing resources used by some software, which thus runs in a simulated environment called a virtual machine (VM).	III
69.	Networked Storage	--	It is a term used to describe a storage device (usually many devices paired together) that is available over a network.	III
70.	Network Attached Storage (NAS)	--	NAS systems are networked appliances that contain one or more hard drives that are shared with multiple, heterogeneous computers.	III
71.	Security Management	--	It is concerned with generating, distributing, and storing encryption keys.	III
72.	Firewall Policy	--	Description of how an organization's firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types, based on the organization's information security policies.	III
73.	IPsec(Internet Protocol Security)	--	It is a set of Internet standards that augment both versions of IP that are in current use (IPv4 and IPv6) with security features.	III
74.	Instant Messaging	--	It is a communications service in which short messages appear in pop-up screens as soon as they are received, thereby commanding the recipient's immediate attention.	III
75.	Voice over IP (VoIP)	--	It involves the transmission of speech across IP-based network.	III
Unit-IV : Technical Security				
76.	Supply chain cyber security	--	It refers to efforts to enhance cyber security within the supply chain.	IV
77.	Blockchain technology	--	It is an emerging trend which has the potential to enhance transparency and efficiency, along with a high level of data-security across multiple trading partners.	IV

78.	Cloud security	--	It is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion.	IV
79.	Distributed Denial of Service (DDoS)	--	These attacks shut down a service by overwhelming it with data so that users cannot access their accounts, such as bank accounts or email accounts.	IV
80.	Malware Protection	--	Protecting against a broad range of malware and including options for virus removal will protect your computer, your privacy and your important documents from attack.	IV
81.	Worm	--	It is a stand-alone malware software that actively transmits itself over a network to infect other computers and can copy itself without infecting files.	IV
82.	Screen-locking Ransomware	--	It blocks screens on Windows or Android devices with a false accusation in harvesting illegal content, trying to scare the victims into paying up a fee.	IV
83.	Encryption-based Ransomware	--	It is a type of ransomware that encrypts all files on an infected machine.	IV
84.	Backdoor	--	Method of bypassing normal authentication procedures, usually over a connection to a network such as the Internet.	IV
85.	Rootkits	--	Software packages known as rootkits allow this concealment, by modifying the host's operating system so that the malware is hidden from the user.	IV
86.	Application Sandboxing	--	Ensure that all code of unknown origin is run within a ‘sandbox’ that prevents access to other resources unless the user explicitly grants permission.	IV
87.	Firewall	--	It is a network security device that filters incoming and outgoing network traffic based on predetermined rules.	IV
88.	Intrusion Prevention System(IPS)	--	It is a device that inspects traffic, detects it, classifies and then proactively stops malicious traffic from attack.	IV
89.	Signature-based IDS	--	It monitors packets in the Network and compares with pre-configured and pre-determined attack patterns known as signatures.	IV

90.	Digital Rights Management (DRM)	--	It is a way to protect copyrights for digital media.	IV
91.	Cryptography	--	It is the science of keeping information secure by transforming it into form that unintended recipients cannot understand.	IV
92.	Symmetric key or private key Cryptography	--	Uses a single key for both encryption and decryption, which is also called symmetric encryption.	IV
93.	Substitution Cipher	--	Replaces bits, characters, or blocks of characters of the plaintext with different bits, characters, or blocks.	IV
94.	Transposition Cipher	--	It does not replace the original text with different text, but rather moves or scrambles the original values around.	IV
95.	Steganography	--	It is a technique that facilitates the hiring of a message that is to be kept secret inside other messages.	IV
96.	Incident Response (IR) plan	--	It is the guide for how your organization will react in the event of a security breach.	IV
97.	Digital Forensics	--	It is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law.	IV
98.	Disk Forensics	--	It deals with extracting data from storage media by searching active, modified, or deleted files.	IV
99.	Network Forensics	--	It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.	IV
100.	Business Continuity Plan (BCP)	--	It is a document that outlines how a business will continue operating during an unplanned disruption in service.	IV
Unit-V : Security Assessment				
101.	Network Security Assessment	--	It is an audit designed to find security vulnerabilities that are at risk of being exploited, could cause harm to business operations or could expose sensitive information.	V

102.	Vulnerability assessment	--	It shows organizations where their weaknesses are.	V
103.	Penetration test	--	It is designed to mimic an actual cyber attack or social engineering attack such as phishing, spear phishing or whaling.	V
104.	Network scanning	--	A comprehensive scan of all your network's ports and other attack vectors.	V
105.	Network Enumeration	--	The discovery of hosts or devices on a network that can fingerprint the operating system of remote hosts.	V
106.	Security Audit	--	It is a systematic evaluation of the security of a company's information system by measuring how well it conforms to an established set of criteria.	V
107.	Internal audits	--	In these audits, a business uses its own resources and internal audit department.	V
108.	External audits	--	With these audits, an outside organization is brought in to conduct an audit.	V
109.	Audit	--	It is a way to validate that an organization is adhering to procedures and security policies set internally, as well as those that standards groups and regulatory agencies set.	V
110.	Test	--	It is a procedure to check that a specific system is working as it should.	V
111.	Assessment	--	It is a planned test such as a risk or vulnerability assessment. It looks at how a system should operate and then compares that to the system's current operational state.	V
112.	Cyber security Performance Management	--	It is the process of evaluating your cyber security program's maturity based on top-level risks and the associated level of investment needed to improve your security to meet regulatory requirements and business outcomes.	V

113.	Security Ratings	--	It can also be used as part of a third-party risk management program to measure the effectiveness of a vendor’s security program and expose cyber risk across the supply chain.	V
114.	Risk Report	--	It imparts information about the company's most pressing risks at the moment.	V
115.	Project-level Reporting	--	It covers risks that are relevant to the scope of the project work, and external factors that may affect the project in some way.	V
116.	Program Risk Reporting	--	When a project is part of a program, the program manager will also have a record of relevant program-level risks.	V
117.	Portfolio-level Risk Reporting	--	It is a way of showing the aggregated risk profile for all the projects and programs in the portfolio.	V
118.	Business-level Risk Reporting	--	Some businesses include operational activity in the scope of the portfolio.	V
119.	Sarbanes-Oxley (SOX)	--	It was passed by the United States Congress in 2002 to protect shareholders and the general public from accounting errors and fraudulent practices, and to improve the accuracy of corporate disclosures.	V
120.	California Consumer Privacy Act (CCPA)	--	It is a new law that became effective on January 1 2020, designed to enhance consumer privacy rights and protection for residents in the state of California by imposing rules on how businesses handle their personal information.	V
121.	Gramm-Leach-Bliley Act (GLBA)	--	It is a United States federal law requiring financial institutions to explain how they share and protect their customers' nonpublic personal information.	V
122.	Federal Information Security Management Act of 2002 (FISMA)	--	It is a United States federal law that defines a comprehensive framework to protect government information, operations, and assets against natural and man made threats.	V

123.	Cyber security Risk Assessment	--	It is about understanding, managing, controlling, and mitigating cyber security risk.	V
124.	Configuration management (CM)	--	It is a systems engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.	V
125.	Compliance Monitoring Plan	--	The plan should aim to address all the risks identified, however, the largest risks should be prioritized first.	V
Placement Questions				
126.	Threat	--	It is any form of hazard that has the potential to destroy or steal data, disrupt operations, or cause harm in general.	
127.	Risk	--	The probability of a threat and the consequence of a vulnerability are combined to form risk.	
128.	Cross-Site Scripting (XSS)	--	It is a web security flaw that allows an attacker to manipulate how users interact with a susceptible application.	
129.	Virtual Private Network(VPN)	--	It enables you to connect your computer to a private network, establishing an encrypted connection that hides your IP address, allowing you to safely share data and access the web while safeguarding your online identity.	
130.	Black Hat Hackers	--	Attempt to obtain unauthorized access to a system in order to disrupt its operations or steal critical data.	
131.	White Hat Hackers	--	As part of penetration testing and vulnerability assessments, they never intend to harm a system; rather, they strive to uncover holes in a computer or network system.	
132.	Grey Hat Hackers	--	Combine elements of both black and white hat hacking.	
133.	Botnet	--	It is a collection of internet-connected devices, such as servers, PCs, and mobile phones, that are infected with malware and controlled by it.	
134.	Null Session	--	It occurs when a user is not authorized using either a username or a password.	

135.	Brute Force Attack	--	It is a cryptographic assault that uses a trial-and-error approach to guess all potential combinations until the correct data is discovered.	
136.	Shoulder Surfing	--	It is a form of physical assault that entails physically peering at people's screens while they type information in a semi-public space.	
137.	Man-In-The-Middle Attack	--	A cyber threat in which a cybercriminal wiretaps a communication or data transmission between two people.	
138.	SSL (Secure Sockets Layer)	--	It is a secure technology that allows two or more parties to communicate securely over internet.	
139.	Sniffing	--	It is a technique for evaluating data packets delivered across a network. This can be accomplished through the use of specialized software or hardware.	
140.	System Hardening	--	It refers to a set of tools and procedures for managing vulnerabilities in an organization's systems, applications, firmware, and other components.	
141.	Domain Name System (DNS) Attack	--	DNS hijacking is a sort of cyber attack in which cyber thieves utilize weaknesses in the Domain Name System to redirect users to malicious websites and steal data from targeted machines.	
142.	Address Resolution Protocol Poisoning	--	It is a sort of cyber-attack that uses a network device to convert IP addresses to physical addresses.	
143.	SQL injection	--	It is a typical attack in which fraudsters employ malicious SQL scripts to manipulate backend databases and get access to sensitive data.	
144.	Hypertext Transfer Protocol Secure(HTTPS)	--	It is a combination of HTTP and SSL that uses encryption to create a more secure surfing experience.	
145.	Active Reconnaissance	--	It is a type of computer assault in which an intruder interacts with the target system in order to gather information about weaknesses.	

146.	Data Leakage	--	It is an intentional or unintentional transmission of data from within the organization to an external unauthorized destination.	
147.	Port Blocking	--	Restricting the users from accessing a set of services within the local area network.	
148.	Cognitive Cybersecurity	--	It is an application of AI technologies patterned on human thought processes to detect threats and protect physical and digital systems.	
149.	Two-Factor Authentication	--	Referred to as dual-factor authentication or two-step verification where the user provides two authentication factors for protecting both user credentials and resources while accessing.	
150.	Cross-site Request Forgery(CSRF)	--	Where an attacker tricks a victim into performing actions on their behalf.	

Faculty Prepared **Signature**

Mrs.C.Radha

HoD