Based on the uploaded examination paper **(BMC106: Cyber Security)**, here are the comprehensive answers for every question listed[1111].

SECTION A

Instructions: Attempt all questions in brief. ($2 \times 7 = 14$ Marks) [2]

a. What is meant by Information System?

Answer: An Information System (IS) is an organized combination of hardware, software, infrastructure, data, and people that is configured to collect, manipulate, store, and process data into information. Its goal is to support operations, management, and decision-making within an organization.

b. What is CIA?

Answer: CIA stands for the Confidentiality, Integrity, and Availability triad, which is the core model for information security:

- **Confidentiality:** Preventing unauthorized disclosure of information.
- **Integrity:** Preventing unauthorized modification of information.
- **Availability:** Ensuring information is available to authorized users when needed.

c. What is an Information?

Answer: Information is data that has been processed, organized, structured, or presented in a given context so as to make it useful. While data is raw facts and figures, information implies meaning and value to the receiver.

d. Define Access Control.

Answer: Access Control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization by strictly limiting access to systems and data based on authentication and authorization.

e. What is meant by Intellectual Property?

Answer: Intellectual Property (IP) refers to creations of the mind, such as inventions, literary and artistic works, designs, and symbols, names, and images used in commerce. In cyber security, IP rights are protected through mechanisms like copyrights, patents, and trademarks to prevent digital theft and piracy.

f. What is the need of having Application Security?

Answer: Application security is needed to protect software applications from external threats. Since applications are often accessible over networks (like the internet), they are vulnerable

to attacks. Security measures at the application level ensure that code is not hijacked, data is not stolen, and the application functions as intended without manipulation.

g. What are the features of Ecommerce System?

Answer: Key features of an E-commerce system include:

- **Ubiquity:** Available everywhere, at any time.
- **Global Reach:** Transactions cross cultural and national boundaries.
- **Interactivity:** Two-way communication between merchant and consumer.
- **Personalization:** Tailoring messages and products to specific individuals.

SECTION B

Instructions: Attempt all questions below (based on the "Attempt any three" section, but all are answered here for completeness). ($7 \times 3 = 21$ Marks) 3

a. Describe on Threats to Information Systems.

Answer:

Threats to information systems are potential events or actions that could cause harm to the hardware, software, data, or network. They are generally categorized as:

- **Malware Attacks:** Viruses, worms, trojans, and ransomware designed to damage or disable computers.
- **Phishing/Social Engineering:** Manipulating people into giving up confidential information (passwords, bank details).
- **Denial of Service (DoS):** Flooding a system with traffic to shut it down.
- **Insider Threats:** Employees or contractors misusing their authorized access.
- **Physical Threats:** Theft of hardware, damage from fire/water, or power failures.

b. Explain in detail on Cyber security.

Answer:

Cyber Security is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money, or interrupting normal business processes.

- **Scope:** It encompasses Network Security, Application Security, Information Security, and Operational Security.
- **Importance:** With the increasing reliance on digital systems and the storage of sensitive data (PII, PHI, IP), cyber security is critical to prevent financial loss, reputational damage, and legal liabilities.
- **Countermeasures:** It involves implementing firewalls, encryption, identity management, and regular security audits.

c. Is it necessary to develop Policies? Why?

Answer:

Yes, developing security policies is strictly necessary. A security policy is a written document in an organization outlining how to protect the organization from threats and how to handle them when they occur.

Why it is needed:

- **Governance:** It defines the rules and behavior expected from all users.
- **Compliance:** It ensures the organization meets legal and regulatory requirements (like GDPR or HIPAA).
- **Consistency:** It ensures security is applied consistently across the organization rather than in an ad-hoc manner.
- **Accountability:** It establishes who is responsible for what, making it easier to manage incidents.

d. What are the threats in E-Payment System?

Answer:

Electronic payment systems face specific high-stakes threats:

- **Phishing & Spoofing:** Creating fake payment pages to steal credit card numbers.
- **Data Interception (Sniffing):** Attackers capturing data packets as they travel between the user and the bank.
- **Man-in-the-Middle (MitM) Attacks:** An attacker secretly relays and possibly alters the communication between two parties who believe they are communicating directly.
- **Database Breaches:** Hackers compromising the merchant's server to steal stored customer payment data.
- **Fraud:** Use of stolen credentials to make unauthorized purchases.

e. Explain in detail on Firewall? How it provides Security to Hardware and software.

Answer:

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.

- **How it works:** It acts as a barrier between a private internal network and the public internet. It analyzes data packets and decides whether to allow or block them.
- **Security for Hardware:** It prevents external attackers from gaining control over physical servers and endpoints by blocking unauthorized ports.
- **Security for Software:** It blocks malicious traffic (like malware payloads) from reaching applications and prevents applications from sending unauthorized data out (preventing data exfiltration).

SECTION C

Instructions: Attempt all parts (Options provided in the exam are typically "Any one," but both are answered below). ($7 \times 5 = 35$ Marks) [4]

Question 3

a. What is a Risk? What are the ways in which the Risk can be Evaluated.

Answer:

Risk in cyber security is the potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability. It is often expressed as:

$$Risk = Threat \times Vulnerability \times Asset Value$$
Risk Evaluation Methods:

1. **Quantitative Risk Assessment:** Assigns numerical values (monetary cost) to risks. It uses metrics like Single Loss Expectancy (SLE) and Annualized Rate of Occurrence (ARO).
2. **Qualitative Risk Assessment:** Uses subjective judgment to categorize risks based on probability and impact (e.g., Low, Medium, High). It often uses a Risk Matrix.
3. **Hybrid Assessment:** A combination of both to balance precision with efficiency.

b. Explain in detail on VPN and its types.

Answer:

A Virtual Private Network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

- **Mechanism:** It creates a secure, encrypted "tunnel" for data to travel through.
- **Types of VPNs:**
    1. **Remote Access VPN:** Allows individual users to connect to a private network from a remote location (e.g., employees working from home).
    2. **Site-to-Site VPN:** Connects entire networks to each other (e.g., a branch office network connecting to the head office network).

Question 4

a. Explain various security standards.

Answer:

Security standards are established frameworks that help organizations implement effective security controls.

- **ISO/IEC 27001:** The international standard for Information Security Management Systems (ISMS). It provides a systematic approach to managing sensitive company information.

- **NIST Cybersecurity Framework:** A voluntary framework primarily for critical infrastructure, focusing on Identify, Protect, Detect, Respond, and Recover.
- **PCI-DSS (Payment Card Industry Data Security Standard):** A set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.
- **HIPAA:** Standard for protecting sensitive patient health information (in the healthcare sector).

b. Why we need cyber laws in India? Define any 2 laws that you feel is necessary.

Answer:

Need for Cyber Laws:

With the rise of "Digital India," cyber crimes like fraud, cyberstalking, and data theft have increased. Cyber laws are needed to:

1. Provide a legal framework for electronic commerce.
2. Define cyber crimes and prescribe punishments (deterrence).
3. Protect privacy and intellectual property rights in the digital domain.

Key Laws:

1. **The Information Technology (IT) Act, 2000:** The primary law in India dealing with cybercrime and electronic commerce. It covers digital signatures, cyber offenses (like hacking and source code tampering), and adjudication.
2. **Digital Personal Data Protection (DPDP) Act, 2023:** (Recent and necessary) This law focuses on the processing of digital personal data, recognizing the right of individuals to protect their personal data and the necessity to process such data for lawful purposes.

Question 5

a. What is the need for having information security? Explain the levels.

Answer:

Need: Information security is vital to maintain business continuity, prevent data breaches, protect reputation, and avoid financial losses.

Levels of Information Security:

1. **Physical Security:** Protecting the actual hardware (servers, datacenters) from theft, fire, or unauthorized physical entry.
2. **Network Security:** Protecting the networking infrastructure (routers, switches) from unauthorized access (e.g., Firewalls, VPNs).
3. **System/OS Security:** Hardening the operating systems (patch management, access controls).

4. **Application Security:** Ensuring software is free from vulnerabilities (bugs, code flaws).[6]
5. **User/Personal Security:** Training e[7]mployees to recognize phishing and practice good hygiene (passwords).

b. Explain Cryptography in Detail.

Answer:

Cryptography is the science of protecting information by transforming it into a secure format.

- **Process:** It involves **Encryption** (converting Plaintext to Ciphertext) and **Decryption** (converting Ciphertext back to Plaintext).
- **Goals:** It ensures Confidentiality (only authorized can read), Integrity (data hasn't changed), Non-repudiation (sender cannot deny sending), and Authentication.
- **Types:**
    - **Symmetric:** Same key for encryption and decryption.
    - **Asymmetric:** Different keys (Public and Private) for encryption and decryption.
    - **Hashing:** One-way conversion for integrity checks.

Question 6

a. Explain General Information system in detail.

Answer:

A General Information System is a conceptual framework describing how information is managed. It follows a cyclic process:

1. **Input:** Capturing or collecting raw data from within the organization or from its external environment.
2. **Processing:** Converting this raw input into a more meaningful form (classifying, calculating, sorting).
3. **Output:** Transferring the processed information to the people who will use it or to the activities for which it will be used.
4. **Storage:** Maintaining data and information in an organized manner for later use.
5. **Feedback:** Output that is returned to appropriate members of the organization to help them evaluate or correct the input stage.

b. Write in detail on Software Piracy and Software Licensing.

Answer:

- **Software Piracy:** The unauthorized use, copying, distribution, or modification of software.

    - *Types:* End-user piracy (using more copies than licensed), Internet piracy (downloading illegal copies), Pre-installed piracy (vendors selling computers with illegal software).
- **Software Licensing:** A legal instrument governing the use or redistribution of software.
    - *Proprietary License:* Grants the right to use software but ownership remains with the creator (e.g., Microsoft Windows). Source code is closed.
    - *Open Source License:* Grants users the right to use, study, change, and distribute the software and its source code (e.g., GPL, MIT licenses).

Question 7

a. What are the various security threats in Applications?

Answer:

Applications are primary targets for attackers. Common threats include:

1. **SQL Injection (SQLi):** Attackers insert malicious SQL code into input fields to manipulate the backend database.
2. **Cross-Site Scripting (XSS):** Attackers inject malicious scripts into web pages viewed by other users.
3. **Buffer Overflow:** Overwriting memory to crash a program or execute malicious code.
4. **Cross-Site Request Forgery (CSRF):** Tricking a user into executing unwanted actions on a web application where they are currently authenticated.
5. **Broken Authentication:** Weak session management allowing attackers to compromise passwords or keys.

b. Write in detail on symmetric and asymmetric key algorithm.

Answer:

These are the two main types of encryption algorithms.

1. Symmetric Key Algorithm (Secret Key Cryptography):

- **Concept:** Uses a single shared key for both encryption and decryption.
- **Speed:** Very fast and efficient for large amounts of data.
- **Key Distribution:** The main challenge is securely sharing the key.
- **Examples:** AES (Advanced Encryption Standard), DES.

2. Asymmetric Key Algorithm (Public Key Cryptography):

- **Concept:** Uses a pair of mathematically related keys: a **Public Key** (K_{pub}) for encryption and a **Private Key** (K_{priv}) for decryption.
- **Security:** Solves the key distribution problem because the public key can be shared openly.
- **Speed:** Slower and more computationally intensive than symmetric.

- **Examples:** RSA, ECC (Elliptic Curve Cryptography).