# Cyber Security

## Question 1

### 1. What is cyber security?

Cyber security is the practice of protecting computers, networks, data, and digital systems from unauthorized access, attacks, damage, or theft. It includes techniques, tools, and processes that ensure the safety and integrity of digital information.

---

### 2. What is steganography?

Steganography is the technique of hiding secret information inside another non-secret file such as an image, audio, video, or text so that the existence of the information remains hidden. Unlike encryption, it hides the message instead of converting it.

---

### 3. What is Reconnaissance?

Reconnaissance is the first phase of a cyber attack in which an attacker gathers information about the target system, network, or organization. It includes collecting details like IP addresses, open ports, and technologies used. It helps attackers plan the actual attack.

---

### 4. What is phishing?

Phishing is a social engineering technique where attackers send fraudulent emails, messages, or websites to trick users into revealing sensitive information such as passwords, bank details, or OTPs.

---

### 5. What is cyber stalking?

Cyber stalking is the use of the internet or digital devices to harass, threaten, or monitor someone repeatedly. It includes sending threatening messages, tracking someone's online activities, or spreading false information about them.

---

### 6. Define cyber attack.

A cyber attack is any deliberate attempt by an individual or group to breach the security system of a computer, network, or device to cause damage, steal information, or disrupt services.

---

**Question 2**

**1. Computer Forensic**

Computer forensics is a branch of digital forensics that involves identifying, collecting, analyzing, and preserving digital evidence from computers and electronic devices. It is used in cybercrime investigations to recover deleted files, analyze logs, trace attackers, and present evidence in court.

---

**2. Discuss various password cracking techniques**

Password cracking techniques are methods used to recover or guess passwords. Common techniques include:

- **Brute Force Attack** – trying all possible combinations until the correct password is found.
- **Dictionary Attack** – using a list of common words or passwords.
- **Rainbow Table Attack** – using pre-computed hash tables to match password hashes.
- **Phishing** – tricking the user into revealing their password.
- **Shoulder Surfing** – observing someone typing their password.
- **Keylogging** – using malware to record keystrokes.

---

**3. What is SQL Injection and countermeasures?**

SQL Injection is a code-injection attack where an attacker inserts malicious SQL queries into an input field to access or manipulate a database. It can lead to data theft, deletion, or unauthorized login.

**Countermeasures:**

- Use **prepared statements** and **parameterized queries**
- **Input validation** (accept only allowed characters)
- **Stored procedures**
- Disable error messages that reveal database information
- Use **Web Application Firewalls (WAF)**

- Regular security audits and patching

---

**Question 3**

**1. Explain a real-life example of cyber security**

Example:
**Ransomware attack on a hospital.**
Hackers encrypt hospital data such as patient records and demand money to release it. Cyber security tools like antivirus, backups, firewalls, and employee awareness training protect the hospital from such attacks. This shows how cyber security protects real-world systems that people rely on.

---

**2. What is domain name? Give example.**

A domain name is the human-readable name of a website used instead of an IP address. It helps users easily access websites.

**Example:**
google.com, amazon.in, wikipedia.org

---

**3. Active and passive attack in detail**

**Active Attack**

An active attack attempts to alter, modify, or damage data or systems.
Examples: DoS attack, Man-in-the-Middle, SQL Injection.
Attackers interact directly with the target.

**Passive Attack**

A passive attack only involves monitoring or eavesdropping on communication without affecting data.
Examples: sniffing, traffic analysis.
Attackers collect information silently.

---

**Question 4**

**1. Discuss DoS attack in detail**

A Denial of Service (DoS) attack is an attempt to make a system, website, or network unavailable to users by overwhelming it with excessive traffic or requests. The server

becomes overloaded and cannot respond to legitimate users.
Types include:

- **Volume-based attacks** (flooding bandwidth)
- **Protocol attacks** (exploiting server resources)
- **Application-layer attacks** (targeting specific applications)

The main goal is **service disruption**, not data theft.

---

**2. What is CIA model? Explain three concepts.**

The CIA model is a fundamental principle of cyber security that stands for **Confidentiality, Integrity, Availability**.

- **Confidentiality** – Ensures information is accessible only to authorized users. (Example: encryption)
- **Integrity** – Ensures data is accurate and unaltered. (Example: hashing, checksums)
- **Availability** – Ensures systems and data are available when needed. (Example: backups, load balancing)

---

**Question 5**

**1. The IT Act**

The Information Technology Act (IT Act) is an Indian law passed in 2000 to provide legal recognition to electronic documents, digital signatures, and to define and punish cybercrimes. It covers hacking, identity theft, cyber terrorism, and online fraud.

---

**2. The ITA 2000 Sections (important ones)**

Some key sections include:

- **Section 43** – Penalty for unauthorized access, damage, or downloading.
- **Section 66** – Computer-related offences (hacking, data theft).
- **Section 66C** – Identity theft.
- **Section 66D** – Cheating by personation, commonly used for online fraud.
- **Section 67** – Publishing obscene content online.

- **Section 69** – Government power to intercept or monitor data.

(Write only the important ones as required.)

---

**3. Social Media**

Social media refers to online platforms that allow people to create, share, and interact with content and communicate with others. Examples include Facebook, Instagram, X (Twitter), YouTube, and WhatsApp. It plays a major role in communication, marketing, education, and entertainment but also creates risks like cyber bullying, misinformation, and privacy issues.