**Topic: Cyber security threats**

Reading Time: 15 mins

**·        Note\* Highlight important/core points while reading**

·        Read the content and write the answers given in the document in your words, to get the solid grip on topic.

**Cyber Security Threats**

Cyber security threats refer to **any malicious activity** that attempts to damage, steal, or gain unauthorized access to computer systems, networks, or data. These threats can come from hackers, malware, and various cyberattacks.

**Types of Cyber Security Threats**

**1. Brute Force Attacks**

* A **trial-and-error method** used to guess passwords.
* The attacker systematically tries different combinations until the correct one is found.
* Automated software can try **millions of passwords per second**.
* **Prevention:** Use strong passwords with uppercase, lowercase, numbers, and special characters.

**2. Data Interception (Man-in-the-Middle Attack)**

* Data is **intercepted** while being transferred over a network.
* Attackers **steal sensitive information** (e.g., login credentials, financial data).
* Often happens on **public Wi-Fi networks**.
* **Prevention:** Use **encrypted connections (HTTPS, VPNs)** and avoid public Wi-Fi for sensitive transactions.

**3. Distributed Denial of Service (DDoS) Attacks**

* Attackers use **multiple computers (botnets)** to send overwhelming traffic to a website or network.
* The target system **becomes slow or crashes**, making it unavailable for users.
* Often used to **disrupt businesses, banks, and government services**.
* **Prevention:** Use **firewalls, load balancers, and traffic filtering tools**.

**4. Hacking**

* The act of **gaining unauthorized access** to computer systems or networks.
* **Black-hat hackers** exploit security vulnerabilities for **malicious purposes**.
* **White-hat hackers** help identify weaknesses to **improve security**.
* **Prevention:** Regular **software updates**, **strong authentication**, and **intrusion detection systems (IDS)**.

**5. Malware (Malicious Software)**

Malware is **software designed to harm** or exploit a computer system. Types include:

|  |  |
| --- | --- |
| **Type** | **Description** |
| **Viruses** | Attach to legitimate files and spread when opened. |
| **Worms** | Self-replicating malware that spreads without user action. |
| **Trojan Horse** | Disguised as legitimate software but has a hidden malicious function. |
| **Spyware** | Secretly collects user data (e.g., keystrokes, login details). |
| **Adware** | Displays unwanted advertisements, often leading to malicious sites. |
| **Ransomware** | Encrypts user files and demands a ransom for decryption. |

* **Prevention:** Use **antivirus software**, avoid suspicious downloads, and enable **firewall protection**.

**6. Phishing**

* A cyberattack where hackers **trick users into giving personal information** (e.g., passwords, credit card details).
* Usually done via **fake emails or websites** pretending to be legitimate.
* Example: An email from “your bank” asking you to reset your password on a **fake website**.
* **Prevention:**
  + Verify sender emails before clicking links.
  + Never enter credentials on unknown websites.
  + Use **email spam filters**.

**7. Pharming**

* Redirects users from a legitimate website to a **fake, malicious website**.
* Users **unknowingly enter** login credentials on the fake site.
* Often used to **steal banking details**.
* **Prevention:**
  + Use **DNS protection software**.
  + Always check the URL before entering sensitive data.
  + Enable **multi-factor authentication (MFA)**.

**8. Social Engineering**

* Attackers manipulate people into **revealing confidential information**.
* Methods include:
  + **Pretexting**: Pretending to be a trusted person to get information.
  + **Baiting**: Offering something attractive (e.g., a free download) to trick users into installing malware.
  + **Tailgating**: Following someone into a restricted area without proper authentication.
* **Prevention:**
  + Always verify identities before sharing information.
  + Educate employees about security awareness.
  + Implement **access controls** for sensitive data.

**A-Rated Questions/Answers By Examiner**

**Q1: What is a brute force attack, and how can it be prevented?**

**Answer:**A **brute force attack** is a method where an attacker repeatedly tries different password combinations until they guess the correct one.  
**Prevention:**

* Use **strong passwords** with uppercase, lowercase, numbers, and symbols.
* Enable **account lockout** after multiple failed attempts.
* Use **two-factor authentication (2FA)**.

**Q2: What is a DDoS attack, and how does it affect websites?**

**Answer:**A **DDoS (Distributed Denial of Service) attack** floods a website with excessive traffic, causing it to slow down or crash.  
**Effects:**

* Websites become **unavailable** to users.
* Businesses lose revenue and customers.
* Servers may **overheat or fail**.  
  **Prevention:**
* Use **firewalls and traffic filters**.
* Deploy **load balancing** to distribute traffic evenly.

**Q3: How does phishing work, and how can users protect themselves?**

**Answer:**Phishing tricks users into revealing **sensitive information** through fake emails or websites.  
**Protection:**

* Do not click on **unknown links or attachments**.
* Verify website URLs before entering personal details.
* Use **email spam filters**.

**Q4: What is ransomware, and why is it dangerous?**

**Answer:**Ransomware is a **type of malware** that **encrypts user files** and demands payment to unlock them.  
**Dangers:**

* Users **lose access to important files**.
* Hackers may **delete or leak sensitive data**.  
  **Prevention:**
* Regularly **back up important files**.
* Avoid clicking on **suspicious email links**.
* Use **antivirus and firewall protection**.

**Q5: What is social engineering, and how do hackers use it?**

**Answer:**  
Social engineering manipulates people into **revealing confidential information** by pretending to be someone trustworthy.  
**Examples:**

* **Pretexting**: Pretending to be an IT support person.
* **Baiting**: Offering fake rewards (e.g., free software) to spread malware.  
  **Prevention:**
* Always verify identities before sharing information.
* Train employees on cybersecurity awareness.
* Use **access control measures** to protect data.

### Write your Answers on your Notebook and Verify it on Next Screen

**Q6: How does malware spread, and what are the best practices to prevent it?**

**Q7: What is the difference between phishing and pharming attacks?**

**Q8: How do hackers use man-in-the-middle (MITM) attacks, and how can they be prevented?**

**Q9: What are the risks of weak passwords, and how can users create strong ones?**

**Q10: How do organizations protect themselves from DDoS attacks?**

**6. Answer:** Malware spreads through infected email attachments, malicious websites, and software downloads.  
**Prevention:**

* Avoid clicking on suspicious links or downloading unknown files.
* Install and update antivirus software.
* Enable firewalls to block unauthorized access.

**7. Answer:**

* **Phishing** tricks users into revealing personal data via fake emails or websites.
* **Pharming** redirects users from legitimate websites to malicious ones without their knowledge.  
  **Prevention:** Verify URLs, use multi-factor authentication (MFA), and enable DNS security.

**8. Answer:** MITM attacks intercept communication between two parties to steal sensitive data.  
**Prevention:**

* Use HTTPS and encrypted communication.
* Avoid using public Wi-Fi for financial transactions.
* Enable VPNs for secure data transmission.

**9. Answer:** Weak passwords can be easily cracked by brute force attacks, leading to data breaches.  
**Best Practices for Strong Passwords:**

* Use a mix of uppercase, lowercase, numbers, and special characters.
* Avoid common words or personal information.
* Use a password manager for secure storage.

**10. Answer:** Organizations use various security measures to prevent DDoS attacks:

* Deploy firewalls and intrusion detection systems (IDS).
* Use content delivery networks (CDNs) to distribute traffic.
* Implement rate limiting and load balancing to manage high traffic volumes.