Section A: Short Answer Questions

1. What is the fundamental function of a proxy server?

Answer: A proxy server acts as an intermediary that sits between a user's device and the internet. It receives a user's request, forwards it to the internet, and then sends the website's response back to the user.

---

2. What is the main difference between how a computer virus and a worm spread?

Answer: The main difference is that a virus requires a host (like an executable file) and human support to spread from one device to another. In contrast, a worm can self-replicate and travel across a network on its own without needing a host file or human action.

---

3. What is the primary goal of steganography?

Answer: The primary goal of steganography is to conceal the very existence of a secret message. Instead of just encrypting it, the message is hidden within another seemingly innocent file, like an image or audio file.

---

4. What can an attacker achieve with a successful SQL injection attack?

Answer: A successful SQL injection attack allows an attacker to read sensitive data from a database. They can also use SQL queries to modify, add, update, or delete records within that database.

---

5. What is credential stuffing and what makes this attack effective?

Answer: Credential stuffing is an attack where hackers use known username and password combinations obtained from previous data breaches to try and gain access to other accounts. The attack is effective because many users reuse the same password across different services.

---

6. In the context of cybersecurity, what is a backdoor?

Answer: A backdoor is an undocumented method used to bypass normal cybersecurity measures and gain access to a computer system or device.

---

7. Who is the specific target of a "whaling" phishing attack?

Answer: A whaling attack specifically targets the head of a company, such as the CEO or CFO.

---

8. What happens during a buffer overflow?

Answer: A buffer overflow occurs when the amount of data being written to a buffer (a temporary memory region) exceeds its storage capacity. This causes the excess data to overwrite adjacent memory locations.

Section B: Long Answer Questions with Real-World Examples

Q1: Explain the anatomy of a targeted spear phishing attack. How does it differ from general email phishing, and what are its potential consequences for an organization?

Answer:

Spear phishing is a highly effective and dangerous form of cyber attack because, unlike general phishing that blasts out thousands of generic emails, it targets a specific organization or individual. The attacker acts less like a random fisherman and more like a hunter, carefully stalking their prey before launching the attack.

The anatomy of a spear phishing attack involves several calculated steps:

1. **Reconnaissance:** Before sending any emails, the attacker first gathers detailed information about the target. They might scour social media like LinkedIn, company websites, and press releases to learn names, job titles, reporting structures, and even details about recent projects.

2. **Crafting the Bait:** Using the gathered intelligence, the attacker crafts a malicious email that appears highly credible. They often impersonate a legitimate identity, such as a manager or a trusted vendor. The email will use correct names and internal jargon to look authentic.

3. **The Attack:** The email is sent to the specific target. The goal is often to trick the employee into transferring a large sum of money, revealing confidential data, or installing malware on their system. The message often creates a sense of urgency to pressure the victim into acting without thinking.

Real-World Example: Imagine an employee named **Priya** works in the finance department of a manufacturing company. A cybercriminal targets her company and discovers from LinkedIn that her boss is the CFO, Mr. Sharma. The attacker spoofs an email that looks exactly like it's from Mr. Sharma's account.

The email reads: *"Priya, I'm in a rush heading to a client meeting. We need to process an urgent wire transfer for our new supplier, 'Innovate Logistics,' to avoid project delays. Please transfer ₹15 Lakhs to the account details in the attached invoice immediately. I'm counting on you."*

Because the email uses her boss's name, mentions a plausible scenario (a new supplier), and creates urgency, Priya might bypass normal verification procedures and process the payment. The money goes directly to the attacker's account, and the company suffers a significant financial loss. This is considered the most successful type of phishing attack.

The primary consequence for an organization is direct **financial loss**. Additionally, a successful attack can lead to a **data breach** if credentials are stolen, or a **malware infection** that could compromise the entire network, leading to further reputational and financial damage.

Q2: Compare and contrast software and hardware keyloggers. Provide a real-world scenario where each type could be used to steal sensitive information.

Answer: A **keylogger** is a malicious program or device designed to monitor and log every keystroke a user makes on their keyboard. This form of spyware is a cybercriminal's tool for capturing sensitive information like banking details, login credentials, and credit card numbers. Keyloggers are broadly categorized into two main types: software and hardware.

Software Keyloggers:

- **What they are:** These are computer programs developed to steal passwords and other data from a victim's computer. They can be installed through phishing emails, malicious downloads, or by exploiting software vulnerabilities. They work silently in the background, recording keystrokes and sending the logs to the attacker.
- **Real-World Scenario: Rohan**, a college student, uses a computer at a public internet cafe to apply for a scholarship. A week earlier, another user was tricked into downloading what they thought was a free movie file, which secretly installed a **software keylogger**. As Rohan fills out the application form, the keylogger records everything he types: his name, address, AADHAAR number, and the password for his email account. The cybercriminal later retrieves this data and uses it to commit identity theft.

Hardware Keyloggers:

- **What they are:** These are physical devices that are not dependent on any software. They are often small circuits or connectors that intercept the signal between the keyboard and the computer. A common type is a **USB keylogger**, which looks like a small USB connector placed between the keyboard's USB cable and the computer's port. Because they are hardware-based, they cannot be detected by anti-virus software.
- **Real-World Scenario:** An insider threat at a large corporation wants to steal a senior executive's network credentials. During a quiet evening, the malicious employee gains brief physical access to the executive's office. They unplug the executive's keyboard, plug in a small **USB keylogger**, and then plug the keyboard into the keylogger. The device is barely noticeable. The next day, the executive works as usual, and the hardware keylogger records every password, email, and confidential memo they type. The malicious employee retrieves the device a few days later, gaining access to invaluable trade secrets.

Key Differences:

- **Detection:** Software keyloggers can be detected and removed by anti-virus and anti-keylogger software, whereas hardware keyloggers are invisible to such software.
- **Access:** Software keyloggers can be deployed remotely over the internet. Hardware keyloggers require the attacker to have physical access to the target machine to install and retrieve the device.

Q3: Explain the difference between a DoS and a DDoS attack. Use a real-world analogy and a technical example to illustrate why DDoS attacks are significantly more dangerous and difficult to mitigate.

Answer: A **Denial of Service (DoS)** attack is a cyber attack where the goal is to make a website or online service unavailable for its intended users. A **Distributed Denial of Service (DDoS)** attack has the same goal but uses a different, more powerful method.

- **DoS Attack:** In a standard DoS attack, a **single computer** sends a massive amount of traffic to a victim's computer or server, overwhelming it and shutting it down.
- **DDoS Attack:** A DDoS attack uses **multiple compromised computers**, often thousands of them, known as a **botnet**. These computers work together to flood the target system with a massive volume of traffic from many different locations at once.

Real-World Analogy: Imagine a small local coffee shop with one entrance.

- A **DoS attack** is like one person standing in the doorway, intentionally blocking anyone else from entering or leaving. The shop owner can easily identify the single person causing the problem and have them removed.
- A **DDoS attack** is like a massive, coordinated flash mob of thousands of people all trying to rush through that same single doorway at once. They block the entrance completely, and the owner can't possibly identify and remove each individual because they are coming from every direction. The coffee shop is effectively shut down.

Technical Example & Key Differences: Let's say an e-commerce website, "ShopOnline.in," is the target.

- In a **DoS attack**, an attacker uses one powerful server to bombard ShopOnline.in with data packets. The website's security team will see a huge flood of traffic coming from a **single IP address**. While this can slow the site down, it's **easy to trace** and can be **blocked easily** by creating a firewall rule to drop all traffic from that one malicious IP.
- In a **DDoS attack**, the attacker activates their **botnet**. Thousands of infected computers (bots) from all over the world simultaneously start sending traffic to ShopOnline.in.
  - **Volume & Speed:** The volume of traffic is immense, far more than in a DoS attack, and the attack is much faster.
  - **Difficulty to Block:** It is extremely **difficult to block** this attack because the malicious traffic is coming from thousands of legitimate-looking IP addresses. Blocking each one individually is impossible, and it's hard to distinguish the bad traffic from real customers.
  - **Difficulty to Trace:** The attack is also **difficult to trace** because the attacker is hidden behind the army of compromised botnet computers.

This distributed nature is what makes DDoS attacks more challenging and dangerous, capable of taking down even large, well-protected websites for extended periods.