**Week 1: Introduction to Networking & Network Security**

**Objective:** Understand basic network components, models, and security principles.

**Task # 05: List common types of network attacks (e.g., DoS, ARP Spoofing, Phishing, MITM).**

**Solution:**

1. Denial of Service (DoS) / Distributed Denial of Service (DDoS)
   * Description: An attack aimed at making a machine or network resource unavailable to its intended users by overwhelming it with a flood of traffic or requests, thereby disrupting services. DDoS attacks use multiple compromised computer systems to launch the attack.
2. ARP Spoofing (Address Resolution Protocol Spoofing)
   * Description: A malicious technique where an attacker sends falsified ARP messages over a local area network (LAN). This links the attacker's MAC address with the IP address of a legitimate network device, allowing the attacker to intercept, modify, or stop data in transit.
3. Phishing
   * Description: A type of social engineering attack where an attacker attempts to trick individuals into revealing sensitive information (like usernames, passwords, credit card details) by masquerading as a trustworthy entity in electronic communication, often via email or text messages.
4. Man-in-the-Middle (MITM) Attack
   * Description: An attack where the attacker secretly intercepts and relays communications between two parties who believe they are communicating directly with each other. The attacker can then eavesdrop on, or even alter, the conversation without either party being aware.
5. Malware Attacks (e.g., Viruses, Worms, Ransomware)
   * Description: Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems.
     + Viruses: Attach to legitimate programs and spread when those programs are executed.
     + Worms: Self-replicating malware that spreads across networks independently.
     + Ransomware: Encrypts a victim's files and demands a ransom payment to restore access.
6. SQL Injection
   * Description: A code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g., to dump database contents to the attacker).
7. Cross-Site Scripting (XSS)
   * Description: A type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. This allows attackers to bypass access controls and impersonate users.
8. Brute-Force Attack
   * Description: A trial-and-error method used to obtain information such as user passwords or decryption keys. An automated system systematically checks all possible combinations until the correct one is found.