# NETWORK SECURITY THREATS

## 1. Denial-of-Service (DoS) Attack

**Overview:** A Denial-of-Service (DoS) attack is a cyberattack where an attacker floods a network, server, or service with excessive traffic or resource requests, causing it to slow down or crash. The goal is to make the system unavailable to legitimate users.

**How it Works**

- The attacker sends huge volumes of fake traffic or malware formed packets.
- The target server becomes overloaded and stops responding to real users.
- DoS attacks exploit limited system resources like bandwidth, memory, or CPU.

**Impact**

- Website or server becomes slow or unreachable.
- Business losses due to downtime.
- Damage to reputation and user trust.

**Mitigation & Prevention**

- Enable rate limiting and traffic filtering.
- Use DDoS protection services (Cloudflare, AWS Shield).
- Configure firewalls and IDS/IPS to block abnormal traffic.

**Real-World Example**

**GitHub DoS Attack (2018):** GitHub was hit with one of the largest recorded DoS attacks (1.35 Tbps) using misconfigured Memcached servers, causing temporary service disruptions.

## 2. Man-in-the-Middle (MITM) Attack

**Overview:** A Man-in-the-Middle (MITM) attack occurs when an attacker secretly intercepts and manipulates communication between two parties. The victims believe they are communicating directly, but the attacker is actually controlling the data flow.

**How it Works**

- The attacker positions themselves between the victim and the server, often using Wi-Fi spoofing, ARP poisoning, or DNS spoofing.
- They intercept credentials, cookies, financial data, or inject malicious content into the communication.

**Impact**

- Theft of login credentials, credit card details, or session cookies.
- Unauthorized access to accounts.
- Loss of privacy and sensitive information.
- Malware injection through modified traffic.

**Mitigation & Prevention**

- Use HTTPS/TLS and enable HSTS.
- Avoid public Wi-Fi or use a VPN.
- Enable ARP protection and secure network segmentation.

**Real-World Example**

**Equifax MITM Vulnerability (2017):** Equifax's dispute portal used outdated TLS configurations, making it vulnerable to MITM interception and contributing to a massive data breach affecting 147 million people.

## 3. Spoofing Attack

**Overview:** Spoofing is when an attacker disguises themselves as a trusted device or user by falsifying digital information such as IP addresses, MAC addresses, emails, or DNS responses.

**How the Attack Works**

- The attacker forges identity data (IP/MAC/Email/DNS entries) to impersonate a legitimate source.
- Victims unknowingly interact with the attacker, who can redirect traffic, steal data, or bypass security controls.

**Impact**

- Unauthorized access to systems
- Redirection to malicious websites

- Credential theft and session hijacking
- Breakdown of trust within a network

**Mitigation / Prevention**

- Use DNSSEC, SPF, DKIM, and DMARC.
- Enable ARP inspection and strict firewall filtering.
- Monitor DNS and ARP tables for suspicious changes.

**Real-World Example**

**2016 Brazilian Bank DNS Spoofing Attack:** Hackers changed the bank's DNS records, redirecting customers to a fake site for hours, stealing banking credentials and personal data.

## 4. Phishing Attack

**Overview:** Phishing is a social engineering attack where attackers trick users into revealing sensitive information by pretending to be a trusted source via emails, messages, or fake websites.

**How it Works**

- Attackers send fake emails or links that look legitimate, prompting users to enter passwords, OTPs, or financial details.
- They may also use cloned websites or malicious attachments to capture data or install malware.

**Impact**

- Credential theft and account compromise.
- Financial fraud and unauthorized transactions.
- Spread of malware through malicious attachments.

**Mitigation & Prevention**

- Enable email filtering and anti-phishing tools
- Train users to verify links and sender addresses
- Use multi-factor authentication (MFA)

**Real-World Example**

**Google & Facebook Phishing Scam (2013–2015):** Attackers tricked both companies into paying over $100 million by sending fake invoices and emails impersonating legitimate vendors.

## 5. Malware Attack

**Overview:** Malware is malicious software (like viruses, worms, ransomware, trojans) designed to damage systems, steal data, or gain unauthorized access.

### How It Works

- Attackers spread malware through infected email attachments, malicious downloads, USB devices, or compromised websites.
- Once executed, it can encrypt data, steal credentials, create backdoors, or spread across the network.

### Impact

- Data theft, corruption, or encryption.
- System slowdown or complete shutdown.
- Unauthorized remote access by attackers.

### Mitigation & Prevention

- Update and patch systems regularly.
- Use antivirus/EDR solutions.
- Block suspicious downloads and email attachments.

### Real-World Example

**WannaCry Ransomware Attack (2017):** Spread globally using the SMB vulnerability (EternalBlue), affecting over 200,000 systems across 150 countries, including hospitals and businesses.

## 6. Ransomware Attack

**Overview:** Ransomware is malicious software that encrypts a victim's files and demands payment (usually cryptocurrency) to restore access.

### How it Works

- Attackers spread ransomware through phishing emails, malicious links, or exploited vulnerabilities.
- Once inside, it encrypts files, locks systems, and displays a ransom note demanding payment.

**Impact**

- Total loss of data if no backups exist.
- Financial losses from ransom and downtime.
- Major operational disruption in organizations.

**Mitigation & Prevention**

- Maintain offline and regular backups.
- Patch vulnerabilities and update software.
- Use endpoint protection tools and network segmentation.

**Real-World Example**

**Colonial Pipeline Attack (2021):** Ransomware hit the pipeline operator, halting fuel distribution across the U.S. East Coast and resulting in a $4.4 million ransom payment.

## 7. Brute-Force Attack

**Overview:** A brute-force attack is when an attacker repeatedly tries many username–password combinations until they guess the correct one and gain unauthorized access.

**How It Works**

- Attackers use automated tools to try thousands or millions of passwords rapidly.
- Weak, reused, or default credentials make systems easy to break into.

**Impact**

- Account takeover and unauthorized access to confidential data
- Data theft or manipulation.
- System slowdown due to repeated login attempts.

**Mitigation & Prevention**

- Enforce strong password policies and use MFA (Multi-Factor Authentication)
- Enable account lockout after failed attempts

- Monitor login anomalies in SIEM
- Deploy rate limiting on login endpoints

**Real-World Example**

**Dropbox Breach (2012):** Attackers used brute-forced passwords from leaked credentials, compromising over 68 million user accounts.