**Research Report on Common Network Security Threats**

**Objective**

This report provides a detailed understanding of common network security threats including:

- Denial of Service (DoS) attacks

- Man-in-the-Middle (MITM) attacks

- Spoofing attacks

The report explains how each attack works, its impact on systems and organizations, real-world examples, and mitigation strategies.

**1. Denial of Service (DoS) Attacks**

A Denial-of-Service (DoS) attack is a cyberattack where an attacker makes a computer or network resource unavailable to its intended users. This is achieved by disrupting services, either temporarily or permanently, by overwhelming the target with traffic or invalid requests.

**How it works**

Attackers send a massive number of packets to a server.

The server becomes overloaded and cannot respond to legitimate user requests.

Some DoS attacks use botnets in a Distributed DoS (DDoS) attack.

**Impacts**

**Website & app downtime:** Users can't access services or make purchases.

**Network slowdown:** Too much traffic causes delays or crashes.

**System overload:** CPU, memory, or bandwidth gets consumed.

**Customer trust drops:** People may stop relying on the service.

**Bad publicity:** Negative reviews or media coverage can harm the brand.

**Migitation Techniques**

* **Use firewalls, ACLs, and load balancers to block and distribute traffic.**
* **Monitor network traffic to detect unusual spikes or malicious IPs.**
* **Limit the number of requests per IP to prevent flooding.**
* **Deploy Web Application Firewalls (WAF) to filter harmful traffic.**
* **Use CDNs and cloud-based tools to absorb and spread traffic loads.**
* **Filter or block protocol-based attacks like UDP, ICMP, and DNS floods.**

**Real World Example**

A notable real-life example of a DDoS attack is the one that hit Amazon Web Services (AWS) in February 2020. The attack, which reached 2.3 terabits per second, was one of the largest DDoS attacks ever recorded, according to multiple sources. Hackers exploited vulnerable CLDAP servers to amplify the attack and flood AWS's network. While AWS successfully mitigated the attack and prevented significant disruptions, it highlighted the scale and potential impact of modern DDoS attacks.

**2. Man-in-the-Middle (MITM) Attacks**

A Man-in-the-Middle (MITM) attack is a type of cyberattack where an attacker secretly intercepts and potentially alters communication between two parties, often without either party's knowledge. The attacker inserts themselves into the communication channel, acting as a go-between to eavesdrop on and manipulate the data being exchanged.

**How it works**

The attacker secretly intercepts communication between two parties.

Messages are passed along, possibly altered or injected with malicious content.

The attacker impersonates each side using fake IPs or certificates.

Sensitive info like passwords or financial data is stolen or tampered with.

**Impacts**

**Data Theft:** Attackers can steal login credentials, financial info, and private data.

**Session Hijacking:** They may hijack sessions to impersonate users and gain unauthorized access.

**Data Manipulation:** MITM attacks can alter messages or inject malware into communications.

**Identity Theft:** Stolen data can be used to impersonate individuals or take over accounts.

**Business Impact:** Organizations may face data leaks, legal issues, and financial losses.

**Operational Disruption:** Attacks can disrupt services and compromise entire networks.

**Reputation Damage:** Exposure of confidential info harms customer trust and brand image.

**Migitation Techniques**

* Use HTTPS and TLS to encrypt all communications.
* Enable multi-factor authentication (MFA).
* Verify digital certificates to avoid fake websites.
* Avoid public Wi-Fi or use a secure VPN.
* Use DNSSEC to protect against DNS spoofing.
* Keep all software and systems updated regularly.

**Real World Example**

In 2013, Edward Snowden leaked documents he obtained while working as a consultant at the National Security Administration (NSA). The documents showed that the [NSA pretended to be Google](https://www.cnet.com/news/nsa-disguised-itself-as-google-to-spy-say-reports/) by intercepting all traffic with the ability to spoof SSL encryption certification. The NSA used this MitM attack to obtain the search records of all Google users, including all Americans, which was illegal domestic spying on U.S. citizens.

**3. Spoofing Attacks**

A spoofing attack is a type of cyberattack where a malicious actor disguises their identity to appear as a trusted source, often with the goal of gaining unauthorized access to systems, data, or networks. This deception can involve impersonating email addresses, IP addresses, websites, or even phone numbers, tricking individuals or systems into believing the attacker's false identity.

**How It Works**

Attacker forges the source address of communication.

The system assumes the spoofed identity is trusted.

Can lead to phishing, data theft, or further network intrusion.

**Impact**

Individuals face financial fraud, identity theft, and privacy breaches due to spoofing.

It can damage personal reputation through impersonation or leaked sensitive info.

Businesses risk data breaches, financial loss, and brand reputation damage.

Spoofing can target supply chains, causing widespread operational disruption.

Legal penalties may arise if companies fail to protect customer data.

Operations may halt due to fraud or system compromise.

Phone and GPS spoofing can deceive users and disrupt services or navigation.

**Migitation Techniques**

* **Use email authentication protocols** like SPF, DKIM, and DMARC to prevent email spoofing.
* **Enable multi-factor authentication (MFA)** to secure accounts even if credentials are stolen.
* **Verify website URLs and use HTTPS** to avoid falling for fake or cloned websites.
* **Educate users** about phishing, suspicious links, and social engineering tricks.
* **Use anti-spoofing and intrusion detection systems** to monitor and block spoofed traffic.
* **Regularly update software and firmware** to fix vulnerabilities used in spoofing attacks.

**Real World Example**

Fast forward to 2017, and the cybersecurity arena witnessed a heist that seemed straight out of a high-tech thriller. In an audacious move, attackers orchestrated a DNS spoofing attack on multiple Brazilian banks. This was no ordinary feat; the hackers meticulously compromised the bank’s DNS hosting service, laying the groundwork for a grand deception.

Over a span of approximately five hours, they executed their plan with chilling precision, **redirecting all 36 of the bank’s domains to fraudulent websites.** This attack wasn’t just about stealing data; it was about hijacking an entire online identity.