# *Report on Common Network Security Threats*

## Objective

The objective of this report is to explore and analyze common network security threats. Each threat is discussed, accompanied by an explanation of its operation, potential impact, real-world cases where the threat has been observed, and effective mitigation strategies to prevent or limit the damage.

## 1. Denial of Service (DoS) and Distributed Denial of Service (DDoS)

* A DoS attack floods a system with more traffic than it can handle, making services unavailable to legitimate users. DDoS is a more advanced form, where multiple machines (often a botnet) coordinate the attack, significantly increasing its scale.
* **Impacts**:

- Services crash or become unreachable.

- Businesses may suffer financial loss and customer trust issues.

- In severe cases, even the network infrastructure may be affected.

* **Real-World Example**: In 2018, GitHub faced a massive DDoS attack reaching 1.35 Tbps, briefly knocking its servers offline. The attack was amplified through unsecured Memcached servers.
* **Preventive Measures**:

- Deploying Content Delivery Networks (CDNs) to absorb traffic surges.

- Using rate-limiting mechanisms to restrict requests per user.

- Setting up firewalls and intrusion detection systems to filter traffic.

- Partnering with DDoS protection services like Cloudflare or Akamai.

## 2. Phishing

* Phishing involves sending misleading emails or messages that falsely appear to come from a trusted source. The aim is to deceive users into revealing sensitive information such as login credentials or financial details.
* **Impacts**:

- Loss of personal or organizational data.

- Unauthorized access to accounts or financial theft.

- This could result in larger data breaches if organizational credentials are stolen.

* **Real-World Example**: Between 2013 and 2015, attackers defrauded Google and Facebook of over $100 million using fake invoices and emails impersonating a real vendor.
* **Preventive Measures**:
* - Educating users to recognize suspicious links and emails.
* - Enabling two-factor authentication (2FA) to reduce account compromise risks.
* - Using advanced spam filters and domain verification mechanisms like SPF and DKIM.
* - Regular phishing simulation exercises to test user awareness.

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

* In a MITM attack, the attacker secretly intercepts and possibly alters communication between two parties. This can happen on unsecured networks, allowing attackers to steal sensitive data or inject malicious content.
* **Impacts**:

- Stolen login credentials, personal data, or financial information.

- Unauthorized transactions or altered communication.

- Loss of trust in communication platforms.

* **Real-World Example**: Lenovo’s "Superfish" adware in 2015 acted as a MITM by intercepting HTTPS traffic with its root certificate, compromising encrypted web sessions.
* **Preventive Measures:**

- Ensuring websites use HTTPS and enabling HSTS headers.

- Using secure, encrypted communication protocols like TLS.

- Avoid using public Wi-Fi or using a VPN when connecting.

- Implementing certificate pinning to prevent fake certificate usage.

## 4. Spoofing (IP and MAC Spoofing)

* Spoofing involves disguising a malicious device as a trusted one by faking its IP or MAC address. This allows the attacker to bypass filters or impersonate legitimate users or systems.
* **Impacts**:

- Attackers may gain unauthorized access to networks or services.

- Can be used to launch further attacks, such as MITM or DoS.

- Can disrupt or hijack network communications.

* **Real-World Example**: In a “Smurf Attack,” attackers used IP spoofing to send ICMP requests to a network’s broadcast address with the victim’s IP, resulting in overwhelming traffic to the victim.
* **Preventive Measures**:

- Enabling packet filtering to reject spoofed traffic.

- Implementing port security on switches.

- Using authentication protocols that don’t rely solely on IP or MAC addresses.

- Monitoring network traffic for unusual behavior or patterns.

## 5. SQL Injection (SQLi)

* SQL injection exploits vulnerable input fields by injecting SQL queries that interact directly with the database. If not properly sanitized, attackers can retrieve or manipulate confidential data.
* **Impact**:

- Unauthorized access to or manipulation of databases.

- Potential full control over web applications.

- Leakage of user credentials or sensitive business data.

* **Real-World Example**: Heartland Payment Systems experienced a major data breach in 2008, where attackers used SQL injection as part of their method to steal millions of credit card records.
* **Preventive Measures**:

- Using parameterized queries and prepared statements in web applications.

- Validating and sanitizing user inputs.

- Implementing a Web Application Firewall (WAF).

- Regularly testing applications through code audits and penetration testing.

## Conclusion

The threats discussed in this report are among the most frequent and damaging in the field of network security. Each threat operates differently but shares the common goal of exploiting system vulnerabilities. By implementing strong security practices, updating systems regularly, and educating users, organizations can greatly reduce their risk exposure. Network security is an ongoing process and must evolve alongside emerging threats.