Research Report on Common Network Security Threats

# Objective

This report provides a comprehensive understanding of major network security threats, explaining how each threat operates, the damage it can cause, and the strategies that can be used to mitigate them. Real-world examples are included to highlight their relevance.

# 1. Man-in-the-Middle (MITM) Attacks

A Man-in-the-Middle attack occurs when an attacker secretly intercepts communication between two parties. By doing so, the attacker can steal, modify, or inject malicious data without either party being aware.

## Impact:

- Theft of login credentials and personal information  
- Altered communications or unauthorized transactions  
- Loss of trust in communication systems

## Real-World Example:

In 2011, hackers used fake SSL certificates to intercept Gmail traffic in Iran, compromising thousands of user accounts.

## Mitigation Strategies:

- Enforce HTTPS and HSTS protocols  
- Use secure communication channels like VPNs and TLS  
- Avoid public Wi-Fi or use VPNs on unsecured networks  
- Apply certificate pinning in applications

# 2. SQL Injection (SQLi)

SQL Injection is a type of code injection attack where malicious SQL commands are inserted into input fields. These commands exploit vulnerabilities in database systems to retrieve, alter, or delete data.

## Impact:

- Unauthorized access to database contents  
- Data leakage or manipulation  
- Full control over application backend

## Real-World Example:

In 2012, attackers exploited SQL injection on Yahoo! Voices, leaking over 450,000 user credentials.

## Mitigation Strategies:

- Use prepared statements and parameterized queries  
- Validate and sanitize all user inputs  
- Employ web application firewalls (WAFs)  
- Perform routine code audits and penetration tests

# 3. Phishing

Phishing is a social engineering attack where attackers impersonate legitimate entities through emails, websites, or messages to trick users into revealing sensitive data such as passwords or credit card details.

## Impact:

- Loss of confidential data  
- Unauthorized access to accounts  
- Large-scale data breaches and financial loss

## Real-World Example:

In 2020, a phishing campaign led to Twitter accounts of high-profile figures being hijacked for cryptocurrency scams.

## Mitigation Strategies:

- Train users to recognize suspicious emails  
- Use multi-factor authentication (MFA)  
- Deploy anti-phishing filters and domain validation tools  
- Conduct phishing simulations regularly

# 4. Spoofing (IP and MAC Spoofing)

Spoofing attacks occur when an attacker disguises their identity by forging IP or MAC addresses. This allows them to bypass security filters and impersonate trusted devices.

## Impact:

- Unauthorized access to networks  
- Facilitation of further attacks such as MITM or DoS  
- Communication hijacking

## Real-World Example:

Attackers in Smurf attacks use IP spoofing to flood victims with ICMP replies, disrupting services.

## Mitigation Strategies:

- Apply packet filtering and ingress/egress controls  
- Enable port security and DHCP snooping  
- Use strong authentication not reliant on IP/MAC  
- Monitor network traffic for unusual behavior

# 5. Malware

Malware refers to any software designed to damage, disrupt, or gain unauthorized access to systems. Types include viruses, worms, trojans, spyware, and ransomware.

## Impact:

- Theft or encryption of sensitive data  
- System downtime or damage  
- Propagation to other systems or networks

## Real-World Example:

The 2017 NotPetya malware caused widespread disruption globally, affecting companies like Maersk and FedEx.

## Mitigation Strategies:

- Regularly update software and operating systems  
- Use advanced antivirus and endpoint protection tools  
- Limit user privileges and segment networks  
- Keep frequent backups stored offline

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

DoS and DDoS attacks aim to overwhelm systems with excessive traffic, rendering services unavailable to legitimate users. DDoS attacks are launched using multiple systems simultaneously, making them harder to mitigate.

## Impact:

- Service unavailability  
- Loss of revenue and trust  
- Potential hardware and network damage

## Real-World Example:

In 2020, Amazon AWS mitigated a 2.3 Tbps DDoS attack, the largest on record at the time.

## Mitigation Strategies:

- Use DDoS protection services and load balancers  
- Implement rate limiting and firewalls  
- Deploy redundant systems and CDNs  
- Monitor and analyze traffic patterns

# Conclusion

Network threats are growing more advanced and pervasive. Understanding the nature of each threat and applying layered security practices are essential for maintaining digital safety. Organizations must continuously monitor their systems, educate their users, and evolve their defenses to stay ahead of potential attackers.