OIBSIP INTERNSHIP: TASK 4

Research Report on Common Network Security Threats

Name: Sagma Kalim Akhtar

Email: sagmakalimakhtar@gmail.com

Date: January 22, 2026

Subject: Analysis of DoS, MITM, and Spoofing Attacks.

1. Introduction

Modern organizations rely heavily on computer networks to deliver services, store sensitive data, and support daily operations. As networks grow in size and complexity, they become attractive targets for cyber attackers. Network security threats can disrupt services, steal data, or allow unauthorized access to systems.

This report explains three common network security threats**, such as Denial of Service (DoS/DDoS) attacks, Man-in-the-Middle (MITM) attacks, and Spoofing attacks**. Each threat is discussed from a defender's perspective, focusing on how the attack works, its impact, real-world examples, and effective detection and mitigation techniques.

2. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

How the Attack Works

A Denial of Service (DoS) attack aims to make a system, server, or network unavailable to legitimate users. The attacker floods the target with excessive traffic or requests, exhausting system resources such as bandwidth, CPU, or memory.

In a Distributed Denial of Service (DDoS) attack, the traffic comes from multiple compromised systems (often called a botnet). Because the requests originate from many different sources, DDoS attacks are harder to block than simple DoS attacks.

Impact on Systems and Networks

- Service downtime and loss of availability
- Financial losses due to interrupted business operations
- Damage to an organization's reputation
- Increased operational costs for recovery and mitigation

For critical services, even a few minutes of downtime can have serious consequences.

Real World Example

In 2016, the **Dyn DNS DDoS attack** disrupted major websites such as Twitter, Netflix, and GitHub. Attackers used a botnet of compromised IoT devices to flood Dyn's infrastructure, causing widespread service outages across the internet.

Detection and Mitigation

Detection:

- Sudden spikes in network traffic
- Repeated requests from multiple IP addresses
- Alerts from IDS/IPS and network monitoring tools

Mitigation:

- Rate limiting and traffic filtering
- DDoS protection services (e.g., CDN-based mitigation)
- Firewalls and intrusion prevention systems
- Network redundancy and load balancing

3. Man-in-the-Middle (MITM) Attacks

How the Attack Works

In a Man-in-the-Middle (MITM) attack, the attacker secretly intercepts and possibly alters communication between two parties who believe they are communicating directly with each other. The attacker positions themselves between the client and the server.

This often happens on unsecured networks, such as public Wi-Fi, where attackers can capture unencrypted traffic or redirect users to malicious systems.

Common MITM Techniques

- **ARP spoofing:** Redirecting local network traffic to the attacker
- **DNS spoofing:** Sending users to fake websites
- **SSL stripping:** Downgrading secure HTTPS connections to HTTP
- **Rogue Wi-Fi access points:** Fake hotspots that capture traffic

Real-World Example

Public Wi-Fi MITM attacks have been widely reported, where attackers set up fake hotspots in airports or cafes. Victims unknowingly connect to these networks, allowing attackers to capture login credentials and sensitive information.

Detection and Mitigation

Detection:

- Certificate warnings in browsers
- Unexpected changes in network behavior
- IDS alerts for ARP or DNS anomalies

Mitigation:

- Enforcing HTTPS and TLS encryption
- Using VPNs on untrusted networks
- Implementing secure DNS and certificate validation
- Network monitoring and ARP inspection

4. Spoofing Attacks

Types of Spoofing

- IP spoofing
- ARP spoofing
- DNS spoofing
- Email spoofing

How Spoofing Works

Spoofing attacks involve an attacker impersonating a trusted system, device, or user by falsifying identity information. The goal is to gain unauthorized access, redirect traffic, or trick users into trusting malicious sources.

By pretending to be a legitimate entity, attackers can bypass security controls or launch further attacks such as MITM or phishing.

Real-World Example

DNS spoofing attacks have been used to redirect users from legitimate banking websites to fake login pages. Victims unknowingly enter their credentials, which are then captured by attackers.

Detection and Mitigation

Detection:

- Mismatched IP or MAC address records
- DNS inconsistencies
- Suspicious email headers and sender domains

Mitigation:

- Packet filtering and ingress/egress filtering
- DNS security extensions (DNSSEC)
- Email authentication (SPF, DKIM, DMARC)
- Network segmentation and monitoring

5. Conclusion

Network security threats such as DoS/DDoS, MITM, and spoofing attacks remain common and dangerous in modern environments. These attacks primarily target availability, confidentiality, and trust within networks.

For defenders and SOC analysts, early detection, continuous monitoring, and layered security controls are essential. Understanding how these attacks work enables security teams to respond faster, reduce impact, and strengthen overall network resilience.

6. References

- Cloudflare Learning Center - Network Attacks
- Cisco Security - Network Threat Defense
- OWASP - Man-in-the-Middle Attack Documentation
- NIST - Cybersecurity Framework
- Krebs on Security - Real-world cyber attack analysis