Task 4:-

Common Network Security Threats – Research Report

1. Introduction

Modern computer networks are the backbone of communication, business operations, cloud services, and critical infrastructure. As networks grow in scale and complexity, they also become attractive targets for attackers. Network security threats aim to disrupt services, steal sensitive data, or gain unauthorized access to systems.

This report explores **common network security threats**, focusing on **Denial of Service (DoS/DDoS) attacks**, **Man-in-the-Middle (MITM) attacks**, and **Spoofing attacks**. For each threat, we explain how it works, its impact, real-world examples, and effective mitigation techniques.

---

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

2.1 Description

A **Denial of Service (DoS)** attack attempts to make a system, server, or network unavailable by overwhelming it with traffic or resource-consuming requests. When the attack originates from multiple compromised systems simultaneously, it is known as a **Distributed Denial of Service (DDoS)** attack.

2.2 How It Works

Attackers flood a target with excessive traffic such as:

- TCP SYN requests (SYN flood)
- UDP packets
- ICMP echo requests (Ping flood)
- HTTP/HTTPS requests at the application layer

The target system exhausts its bandwidth, CPU, memory, or connection limits, preventing legitimate users from accessing the service.

2.3 Impact

- Service downtime and loss of availability
- Financial losses due to business disruption
- Damage to organizational reputation
- Increased operational costs for recovery

2.4 Real-World Example

- **GitHub DDoS Attack (2018):** GitHub experienced a massive 1.35 Tbps DDoS attack using memcached amplification, temporarily disrupting services.
- **Dyn DNS Attack (2016):** A DDoS attack using IoT botnets (Mirai) disrupted major websites like Twitter, Netflix, and Reddit.

2.5 Mitigation and Prevention

- Deploy DDoS protection services (Cloudflare, AWS Shield)
- Use rate limiting and traffic filtering
- Configure firewalls and intrusion prevention systems (IPS)
- Implement load balancing and redundancy
- Monitor network traffic for anomalies

---

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

3.1 Description

A **Man-in-the-Middle (MITM)** attack occurs when an attacker secretly intercepts and possibly alters communication between two parties who believe they are communicating directly.

3.2 How It Works

MITM attacks are commonly executed through:

- ARP spoofing
- DNS poisoning
- Rogue Wi-Fi access points
- SSL/TLS stripping

The attacker positions themselves between the victim and the server, capturing credentials, session cookies, or sensitive data.

3.3 Impact

- Theft of login credentials and personal data
- Financial fraud and identity theft
- Unauthorized system access
- Compromise of confidential communications

3.4 Real-World Example

- **Public Wi-Fi Attacks:** Attackers set up fake Wi-Fi hotspots in public places to intercept user traffic.
- **Superfish Incident (2015):** Preinstalled adware on laptops intercepted HTTPS traffic by installing rogue certificates.

3.5 Mitigation and Prevention

- Use HTTPS with valid TLS certificates
- Enable certificate pinning where possible
- Avoid unsecured public Wi-Fi networks
- Use VPNs for encrypted communication
- Implement network monitoring and ARP inspection

---

4. Spoofing Attacks

4.1 Description

Spoofing involves impersonating a trusted entity by falsifying identity information such as IP addresses, MAC addresses, DNS records, or email headers.

4.2 Types of Spoofing

- **IP Spoofing:** Forging source IP addresses
- **ARP Spoofing:** Associating attacker MAC with victim IP
- **DNS Spoofing:** Redirecting users to malicious websites
- **Email Spoofing:** Forging sender email addresses

4.3 How It Works

Attackers manipulate network protocols that lack strong authentication, tricking systems into accepting malicious traffic as legitimate.

4.4 Impact

- Session hijacking
- Phishing and malware delivery
- Data interception
- Network redirection and fraud

4.5 Real-World Example

- **DNS Cache Poisoning Attacks:** Users are redirected to fake banking websites to steal credentials.
- **Email Spoofing in Phishing Campaigns:** Attackers impersonate organizations to distribute malware or steal data.

4.6 Mitigation and Prevention

- Implement DNSSEC
- Use email authentication standards (SPF, DKIM, DMARC)
- Enable dynamic ARP inspection
- Apply ingress and egress traffic filtering
- Use strong authentication mechanisms

---

5. Comparative Summary of Threats

Threat Type	Primary Goal	Common Techniques	Key Impact
DoS/DDoS	Disrupt availability	Traffic flooding	Service downtime
MITM	Intercept communication	ARP/DNS spoofing	Data theft
Spoofing	Impersonation	IP/DNS/Email forgery	Fraud & redirection

---

6. Conclusion

Network security threats such as DoS, MITM, and spoofing attacks pose serious risks to organizations and individuals. Understanding how these attacks work and implementing layered security controls is essential for protecting network infrastructure. Proactive monitoring, encryption, authentication mechanisms, and security best practices significantly reduce the risk of successful attacks.

---

7. References

- OWASP Top 10
- NIST Network Security Guidelines
- Cloudflare Security Learning Center
- CERT-In Advisories