**🛡 Network Security Threats Report:**

**Author**: Abhay R. Gaikwad

**Task**: Research on Common Network Security Threats

**Date**: 04/07/2025

**Internship Requirement**: ✅ Completed

---

**🎯 Objective:**

To provide a concise overview of common network security threats—DoS, Man-in-the-Middle (MITM), and Spoofing—along with their impact, real-world examples, and prevention techniques.

---

**⚠ 1. Denial-of-Service (DoS) Attack:**

**What is it?**

A DoS attack floods a server or network with traffic, making it slow or unavailable.

**Real Example:**

GitHub (2018) – Hit by a 1.35 Tbps attack using memcached servers.

**Impact:**

1. Service outages
2. Financial and reputational loss

**Prevention:**

1. Rate limiting
2. Firewalls
3. Cloud-based DDoS protection (e.g., Cloudflare, AWS Shield)

---

**👥 2. Man-in-the-Middle (MITM) Attack:**

**What is it?**

An attacker secretly intercepts communication between two systems.

**Real Example:**

1. Superfish (2015) – Lenovo laptops intercepted HTTPS traffic using fake certificates.

**Impact:**

1. Credential theft
2. Data manipulation

**Prevention:**

1. HTTPS/TLS encryption
2. VPN on public Wi-Fi
3. SSL certificate pinning

---

**🕵 3. Spoofing Attacks**

**What is it?**

The attacker pretends to be a trusted source by faking identity (IP, ARP, DNS, Email).

**Real Example:**

1. Kaminsky DNS Attack (2008) – Redirected users to malicious sites via DNS spoofing.

**Impact:**

1. Unauthorized access
2. Misdirected traffic
3. Phishing/malware delivery

**Prevention:**

1. Use DNSSEC
2. Enable ARP inspection
3. Apply SPF, DKIM, DMARC for emails

---

**✅ Summary Table:**

|  |  |  |
| --- | --- | --- |
| **Threat** | **Impact** | **Prevention** |
| DoS | Service disruption | Rate limits, DDoS tools |
| MITM | Data theft, hijacking | HTTPS, VPN, encryption |
| Spoofing | Traffic redirection | DNSSEC, ARP/DNS protection |

---

**📁 Deliverable**

1. network\_security\_threats\_report.md ✅