Network Security Threats Report

Name: -Deepanshu Semwal

FIELD: -BTECH CSE CYBER SECURITY

YEAR: -2026

***Disclaimer:**

This project uses only publicly available data for educational purposes.

Self-Declaration

I, **Deepanshu Semwal**, hereby declare that this project entitled **“***Network Security Threats Report* **”** is my original work and has been carried out by me as a **self-initiated project**. This project is based on my own research, learning, and understanding of concepts related to **Network security and online investigation**.

I further declare that this project has not been submitted previously to any university, institution, or organization for the award of any degree, diploma, or certification. All the information, data, and references used in this project have been properly acknowledged wherever applicable.

I take full responsibility for the authenticity and originality of the content presented in this project.

Name: Deepanshu Semwal
Course: B.Tech (CSE – Cybersecurity)
Date: 13-JANUARY-2026

Table of Contents

1. Introduction

Network security is a critical component of modern information technology infrastructure, designed to protect data, devices, and networks from unauthorized access, misuse, or theft. As organizations increasingly rely on digital systems for communication, commerce, and operations, the threat landscape continues to evolve, presenting new challenges and risks.

This report provides a comprehensive overview of three common network security threats: **Denial-of-Service (DoS) attacks, Man-in-the-Middle (MITM) attacks**, and **Spoofing attacks**. Each threat is examined in terms of its mechanics, real-world impact, and practical mitigation strategies. The goal is to equip readers with a clear understanding of these threats and the measures necessary to defend against them.

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

2.1 How It Works

A Denial-of-Service (DoS) attack aims to make a network resource unavailable to its intended users by overwhelming it with excessive traffic or resource requests. A Distributed Denial-of-Service (DDoS) attack is a more powerful variant that uses multiple compromised systems (often part of a botnet) to launch a coordinated attack against a single target. Common methods include:

- **Volume-Based Attacks**: Flooding the target with massive amounts of traffic (e.g., UDP floods, ICMP floods).
- **Protocol Attacks:** Exploiting weaknesses in network protocols (e.g., SYN floods, Ping of Death).
- **Application Layer Attacks**: Targeting specific applications or services (e.g., HTTP floods, Slowloris).

2.2 Impact

- **Service Disruption**: Critical services become unavailable, leading to operational downtime.
- **Financial Losses**: Revenue loss, especially for e-commerce and online service providers.
- **Reputation Damage**: Loss of customer trust and brand credibility.
- **Resource Exhaustion**: Increased infrastructure costs due to scaling or mitigation efforts.

2.3 Real-World Example

In October 2016, a massive DDoS attack targeted **Dyn**, a major DNS provider. The attack, executed via the **Mirai botnet** (composed of IoT devices), disrupted access to popular websites such as Twitter, Netflix, Reddit, and GitHub for several hours. This incident highlighted the vulnerability of critical internet infrastructure and the potential scale of IoT-based attacks.

2.4 Mitigation Strategies

- **Traffic Filtering**: Use firewalls and intrusion prevention systems (IPS) to block malicious traffic.
- **Rate Limiting**: Implement thresholds for incoming requests to prevent resource exhaustion.
- **DDoS Protection Services**: Leverage cloud-based mitigation services like **Cloudflare**, **AWS Shield**, or **Akamai Prolexic**.
- **Redundancy and Scalability**: Design networks with failover mechanisms and scalable resources.
- **Monitoring and Alerting**: Deploy real-time monitoring tools to detect and respond to anomalous traffic patterns.

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

3.1 How It Works

In a Man-in-the-Middle attack, an attacker secretly intercepts and relays communication between two parties who believe they are directly communicating with each other. The attacker can eavesdrop, alter, or inject malicious data into the communication stream. Common techniques include:

- **ARP Spoofing**: Redirecting traffic by falsifying ARP messages on a local network.
- **DNS Spoofing**: Redirecting domain name queries to malicious IP addresses.
- **SSL Stripping**: Downgrading HTTPS connections to HTTP to intercept unencrypted data.
- **Wi-Fi Eavesdropping**: Setting up rogue access points or exploiting public Wi-Fi networks.

3.2 Impact

- **Data Theft**: Sensitive information such as login credentials, financial data, or personal details can be stolen.
- **Session Hijacking**: Attackers can take over authenticated sessions to impersonate users.
- **Data Manipulation**: Messages or transactions can be altered without detection.
- **Loss of Privacy**: Confidential communications are exposed.

3.3 Real-World Example

In 2017, a widespread MITM attack targeted banking customers through **rogue mobile apps** and compromised public Wi-Fi hotspots. Attackers intercepted two-factor authentication (2FA) codes and drained bank accounts. This attack underscored the risks of using unsecured networks for sensitive transactions.

3.4 Mitigation Strategies

- **Encryption:** Enforce **HTTPS/TLS** for all web traffic and use **VPNs** for secure remote access.
- **Certificate Pinning**: Ensure applications validate server certificates to prevent spoofing.
- **Network Segmentation**: Limit the scope of potential attacks by isolating sensitive network segments.
- **Multi-Factor Authentication (MFA**): Add an extra layer of security beyond passwords.
- **User Awareness**: Educate users about the risks of public Wi-Fi and encourage the use of trusted networks.

4. Spoofing Attacks

4.1 How It Works

Spoofing involves an attacker masquerading as a trusted entity by falsifying data such as IP addresses, email addresses, or DNS records. Common types include:

- **IP Spoofing**: Forging the source IP address in network packets to hide the attacker's identity or impersonate another system.
- **Email Spoofing**: Sending emails with a forged sender address to trick recipients into revealing information or downloading malware.
- **DNS Spoofing**: Corrupting DNS cache to redirect users to malicious websites.
- **Caller ID Spoofing**: Falsifying caller information in VoIP or telephone systems.

4.2 Impact

- **Phishing Success**: Spoofed emails or websites increase the effectiveness of phishing campaigns.
- **Unauthorized Access**: Attackers can bypass IP-based access controls.
- **Malware Distribution**: Spoofed domains or emails can deliver ransomware or trojans.
- **Reputation Hijacking:** Legitimate brands can be impersonated, damaging trust.

4.3 Real-World Example

In 2015, a **DNS spoofing attack** targeted several Brazilian banks. Attackers compromised DNS servers to redirect customers to fake banking sites, harvesting login credentials and financial data. The attack affected thousands of users and resulted in significant financial losses.

4.4 Mitigation Strategies

- **DNSSEC:** Implement DNS Security Extensions to ensure DNS responses are authenticated.
- **Email Authentication Protocols**: Use **SPF**, **DKIM**, and **DMARC** to verify email senders.
- **Ingress/Egress Filtering**: Configure routers to block packets with spoofed IP addresses.
- **Network Monitoring**: Deploy tools to detect anomalies in traffic patterns or DNS queries.
- **User Training**: Educate users to verify URLs, email senders, and certificate details.

5. Additional Common Network Security Threats (Brief Overview)

While DoS, MITM, and spoofing are focal points, other significant threats include:

- **Phishing**: Deceptive attempts to obtain sensitive information via fraudulent emails or websites.
- **Malware**: Malicious software such as viruses, worms, ransomware, and spyware.
- **Insider Threats**: Malicious or negligent actions by employees or trusted individuals.
- **Zero-Day Exploits**: Attacks targeting vulnerabilities unknown to vendors or the public.

6. Comprehensive Mitigation Framework

To defend against the evolving threat landscape, organizations should adopt a **layered security approach**:

1. **Preventive Controls**:
   - Firewalls, intrusion prevention systems (IPS), and antivirus software.
   - Strong authentication mechanisms (MFA, biometrics).
   - Regular software updates and patch management.

2. **Detective Controls**:
   - Security Information and Event Management (SIEM) systems.
   - Network traffic analysis and anomaly detection.
   - Regular vulnerability assessments and penetration testing.

3. **Corrective Controls**:
   - Incident response plans and disaster recovery procedures.
   - Data backups and restoration capabilities.

- Legal and regulatory compliance measures.

4. **Awareness and Training**:
   - Continuous cybersecurity education for employees.
   - Simulated phishing exercises and security drills.
   - Clear security policies and acceptable use agreements.

7. Conclusion

Network security threats such as DoS/DDoS, MITM, and spoofing attacks pose significant risks to organizations of all sizes. Understanding how these attacks work, their potential impact, and effective mitigation strategies is essential for building resilient and secure network infrastructures.

By implementing a combination of technical controls, security best practices, and ongoing user education, organizations can reduce their vulnerability to these threats and respond effectively when incidents occur. As cyber threats continue to evolve, a proactive and adaptive security posture will remain crucial for safeguarding digital assets and maintaining trust in an interconnected world.

8. References

1. National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity*.
2. Cisco. *2023 Cybersecurity Threat Trends Report*.
3. Cloudflare. *Understanding DDoS Attacks*.
4. OWASP. *Man-in-the-Middle Attack Cheat Sheet*.
5. Internet Engineering Task Force (IETF). *DNS Security Extensions (DNSSEC*).
6. Verizon. *2023 Data Breach Investigations Report*.
7. SANS Institute. *Network Security Resources*.
8. CERT Division (SEI). *Mitigating Network Attacks*.