**Research Report on Common Network Security Threats**

**Table of Contents**

1. Executive Summary
2. Introduction
3. Denial-of-Service (DoS) Attacks
4. Man-in-the-Middle (MITM) Attacks
5. Spoofing Attacks
6. Comparative Analysis
7. Recommendations for Network Security
8. Conclusion
9. References

**1. Executive Summary**

* Focus: DoS, MITM, and Spoofing attacks
* Threat to: Data integrity, availability, confidentiality
* Goal: Understand mechanisms, impacts, and countermeasures
* Relevance: Critical for building secure networks across all sectors

**2. Introduction**

* **Cyber threats** are growing with technological dependence
* Attackers exploit network **vulnerabilities**
* Focus of this report:
  + DoS (including DDoS)
  + MITM (data interception and manipulation)
  + Spoofing (identity falsification)

**3. Denial-of-Service (DoS) Attacks**

**Overview**

* Overloads services to make them **unavailable**
* DDoS = Coordinated attacks from multiple systems

**Types**

| **Type** | **Example** |
| --- | --- |
| Volume-based | UDP/ICMP Floods |
| Protocol Attacks | SYN Floods, Ping of Death |
| Application-layer | HTTP Floods |

**Methods of Execution**

* **Botnets**: Compromised device networks
* **Amplification**: Small request → large response
* **Reflection**: Spoofing victim’s IP

**Real-World Examples**

* **GitHub (2018)**: 1.35 Tbps via Memcached
* **Dyn DNS (2016)**: Used Mirai botnet, disrupted Twitter, Netflix, etc.

**Mitigation**

* Rate limiting, traffic filtering
* DDoS protection services (Cloudflare, Akamai)
* Redundancy & failover systems
* IDS/IPS implementation

**4. Man-in-the-Middle (MITM) Attacks**

**Overview**

* Attacker intercepts or alters communication
* Acts as both **sender** and **receiver**

**Techniques**

* **Packet sniffing**
* **Session hijacking**
* **SSL stripping**
* **DNS spoofing**
* **Wi-Fi eavesdropping**

**Examples**

* **Fake Wi-Fi hotspots** in public places
* **NSA PRISM**: State-sponsored MITM
* **Equifax breach (2017)**: Session hijacking

**Detection & Prevention**

* HTTPS/TLS encryption
* VPNs for secure communication
* Multi-factor authentication (MFA)
* DNSSEC for integrity

**5. Spoofing Attacks**

**Overview**

* Impersonation to deceive systems or users

**Types**

| **Type** | **Description** |
| --- | --- |
| IP Spoofing | Fakes IP address |
| Email Spoofing | Fakes sender’s email |
| ARP Spoofing | Links attacker MAC to victim IP |
| DNS Spoofing | Redirects users to malicious IPs |

**Real-World Incidents**

* **Stuxnet**: Used spoofed certificates
* **2020 Twitter hack**: Email spoofing
* **University attacks**: ARP spoofing to steal data

**Mitigation**

* Packet filtering
* SSL/TLS for authentication
* Email protocols: SPF, DKIM, DMARC
* ARP inspection & static entries

**6. Comparative Analysis**

| **Attack Type** | **Goal** | **Method** | **Risk Level** | **Mitigation Complexity** |
| --- | --- | --- | --- | --- |
| **DoS/DDoS** | Disrupt services | Overload/protocols | **High** | Moderate to High |
| **MITM** | Intercept/alter data | Session hijack, sniffing | **High** | **High** |
| **Spoofing** | Deceive systems | Identity falsification | Medium–High | Medium |

**7. Recommendations for Network Security**

✅ **Regular Monitoring** – Use IDS/IPS  
✅ **User Awareness** – Phishing training, security policies  
✅ **Encryption** – TLS 1.3, VPNs, DNSSEC  
✅ **Network Segmentation** – Limit breach impact  
✅ **Timely Updates** – Patch vulnerabilities  
✅ **Redundancy** – Backup and failover systems

**8. Conclusion**

* DoS, MITM, and spoofing are **critical threats**
* Require **multi-layered defenses**
* Importance of:
  + Technical safeguards
  + Human vigilance
  + Incident response readiness

**9. References**

* OWASP (2024). *Top 10 Network Security Threats* – [owasp.org](https://owasp.org)
* US-CERT (2023). *Denial-of-Service Attacks* – [us-cert.cisa.gov](https://us-cert.cisa.gov)
* Cloudflare (2024). *DDoS Attack Guide* – [cloudflare.com](https://cloudflare.com)
* NIST (2022). *MITM Standards* – [nist.gov](https://nist.gov)
* Krebs on Security (2016). *Dyn DNS Analysis* – [krebsonsecurity.com](https://krebsonsecurity.com)
* Microsoft Security Blog (2023). *Spoofing Mitigation* – [security.microsoft.com](https://security.microsoft.com)