# Ethical Hacker’s Guide to Network Security Threats

## Network Security Threats Report

### ✅ Objective

This report provides a comprehensive overview of common network security threats, focusing on: - Denial of Service (DoS) Attacks - Man-in-the-Middle (MITM) Attacks - Spoofing Attacks

We will explore how each threat works, real-world examples, their potential impact, and strategies to mitigate them.

# 1. Denial of Service (DoS) Attacks

## What is a DoS Attack?

A Denial of Service (DoS) attack is a cyber attack that aims to make a network service or machine unavailable to its intended users by overwhelming it with excessive traffic.

## How it Works :

- Attackers flood the target with traffic or send information that triggers a crash.
- Resources are exhausted (e.g., bandwidth, memory), causing service disruptions.

## Impact :

- Downtime of critical services
- Loss of customer trust
- Financial loss
- Vulnerability to further attacks

## Mitigation :

- Use firewalls and intrusion detection systems (IDS)
- Implement rate limiting
- Use anti-DDoS services (e.g., Cloudflare, AWS Shield)
- Monitor and log abnormal traffic patterns

## Real-World Example :

In 2016, the Dyn DNS provider was hit by a massive DDoS attack using the Mirai botnet, disrupting major sites like Twitter, Reddit, Netflix, and GitHub.

---

## 2. Man-in-the-Middle (MITM) Attacks

### What is a MITM Attack?

A MITM attack occurs when an attacker secretly intercepts and possibly alters the communication between two parties without their knowledge.

### How it Works:

- Attackers position themselves between the victim and the server.
- They intercept, eavesdrop, or modify data in real-time.
- Can be done using ARP spoofing, DNS spoofing, or fake Wi-Fi hotspots.

### Impact:

- Theft of sensitive information (passwords, credit cards)
- Session hijacking
- Unauthorized data manipulation

### Mitigation:

- Use HTTPS and SSL/TLS encryption
- Enable VPNs for secure communication
- Implement public key infrastructure (PKI)
- Use multi-factor authentication (MFA)

### Real-World Example:

In 2011, DigiNotar, a Dutch certificate authority, was compromised. Fake certificates were used in MITM attacks against Gmail users in Iran.

---

## 3. Spoofing Attacks

### What is Spoofing?

Spoofing is a tactic where attackers disguise themselves as a trusted entity to gain unauthorized access to systems or data.

### Types of Spoofing:

- IP Spoofing: Faking IP addresses
- Email Spoofing: Sending fake emails to phish credentials
- DNS Spoofing: Redirecting traffic to malicious websites
- ARP Spoofing: Linking attacker MAC with legitimate IP

### Impact:

- Unauthorized access
- Spread of malware or phishing campaigns
- Network disruption

### Mitigation:

- Use packet filtering firewalls
- Implement email authentication protocols (SPF, DKIM, DMARC)
- Secure DNS with DNSSEC
- Monitor ARP tables for anomalies

### Real-World Example:

In 2013, the SEA (Syrian Electronic Army) used spoofed emails to compromise social media accounts of media outlets like AP, leading to false news reports and a temporary dip in stock markets.

## ✅ Conclusion

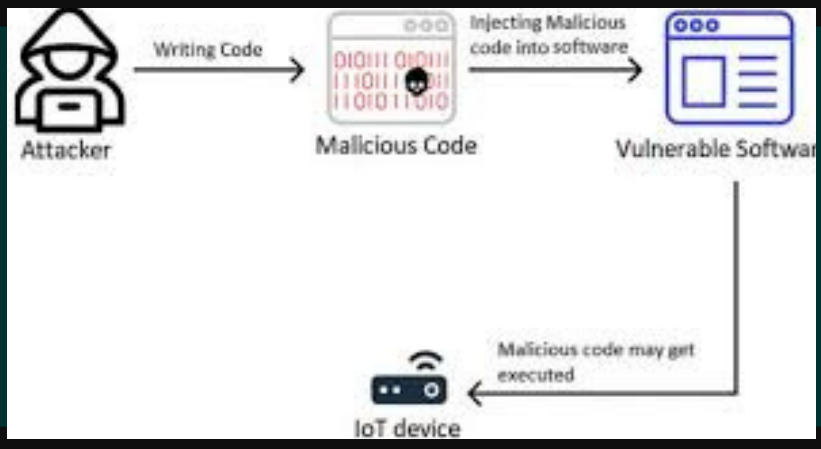
Network security threats like DoS, MITM, and spoofing are serious concerns in today's digital landscape. By understanding how these attacks work and applying preventive measures such as encryption, firewall rules, and secure protocols, organizations can significantly reduce their risk exposure.

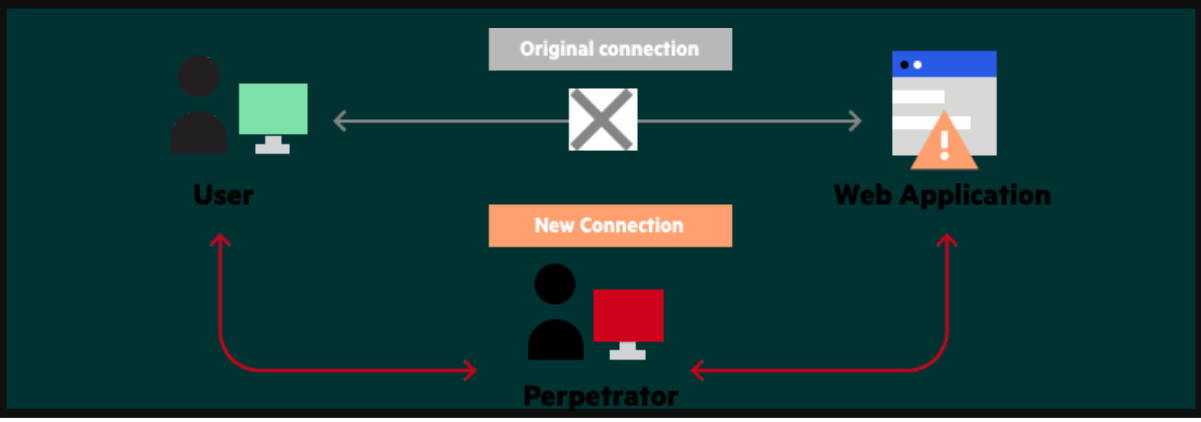
Key Takeaways: - Always keep systems and software updated. - Educate users about phishing and spoofing. - Invest in robust cybersecurity infrastructure.

---

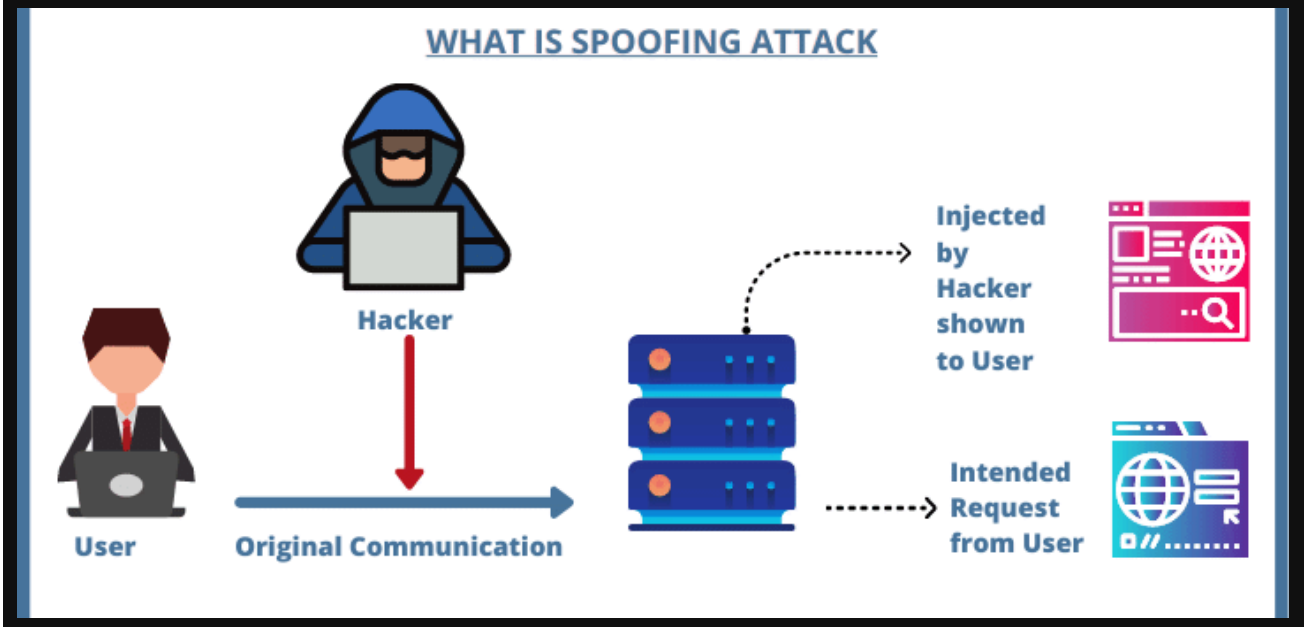
## GitHub Deliverable

**Filename:** network_security_threats_report.md
**Contains:** Structured report with threats, real-world examples, and countermeasures.




Man in the middle


WHAT IS SPOOFING ATTACK
Hacker
User
Original Communication
Injected by Hacker shown to User
Intended Request from User