TASK 4: RESEARCH REPORT: COMMON NETWORK SECURITY THREATS

1. INTRODUCTION

From banking and communication to cloud services and business operations, almost everything today relies on some form of computer network. That makes them very valuable targets for an attacker. Some of the most common and damaging network threats include DoS, MITM attacks, and various forms of spoofing.

This report details how these threats work, why they are important, real-world events that demonstrate them, and practical methods of defending against them.

2. Denial-of-Service (dos) and Distributed Denial-of-Service (ddos) Attacks

2.1 How These Attacks Work

DoS: An attack aimed at overwhelming a system so legitimate users cannot have access to it. DDoS: A larger variant in which thousands, or even millions, of compromised devices-as part of a botnet-flood a target all at once.

Common techniques

- **Volumetric attacks:** These overwhelm networks with massive traffic, such as UDP or ICMP floods.
- **Amplification attacks:** Leverage open services-such as DNS or NTP-to reflect a large amount of traffic on to a target.
- **Protocol attacks:** Exploit weaknesses in TCP/IP, such as SYN floods.
- **Application-layer attacks:** Attack web servers with normal-appearing yet high-volume HTTP requests, for instance Slowloris.

2.2 Impact

- The services become slow or unreachable.
- Financial losses: Downtime, SLA violations, lost customers.
- Over-spilled infrastructure burdening the nearby system.
- Attackers may use DDoS as a diversion while attacking the network.
- Long-term loss of trust and reputation.

2.3 Real-World Example

- **Mirai Botnet Attack (2016):** Tens of millions of insecure IoT devices were infected and used to launch a massive DDoS attack on DNS provider Dyn, which took down many major websites—Twitter, Netflix, GitHub, Reddit—for hours.

2.4 Mitigation

- DDoS protection services: Cloudflare, AWS Shield, Akamai
- Deploy rate limiting and web application firewalls.
- Perform traffic filtering at routers and collaborate with ISPs.
- Enable SYN cookies and harden TCP/IP stacks.
- Distribute services geographically using CDNs.
- Continuously monitor the network to identify unexpected spikes at the earliest possible moment.
- Prepare an incident response playbook for DDoS scenarios.

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

3.1 How These Attacks Work

Man-in-the-middle attack: This is when an intruder steps between the two communicating parties without their knowledge. They can intercept, read, or modify data in transit.

Common MITM vectors:

- ARP Poisoning: Redirecting traffic within a local network.
- Fake Wi-Fi hotspots: Users connect, thinking it is safe.
- SSL stripping: Downgrade HTTPS to HTTP.
- Malicious or compromised routers.

3.2 Impact

- Stolen login credentials or sensitive data.
- Tampered messages or altered transactions.
- Taking over accounts by account hijacking.
- Malware injected into legitimate traffic.

3.3 Real-World Example

- **Superfish Incident (2015):** Many laptops were shipped with adware that installed a root certificate, which made HTTPS interception possible. Attackers could mimic secure sites and steal private information.

3.4 Mitigation

- Always use encrypted connections: HTTPS, SSH, TLS-based e-mail.
- Enable HSTS to prevent SSL stripping.
- Use VPNs on public networks.
- Validate certificates; do not accept browser warnings.
- Implement DNS over HTTPS or DNSSEC.
- Monitor LANs for duplicated IP addresses-a common MITM sign.
- Educate users about untrusted Wi-Fi networks.

4. SPOOFING ATTACKS

Spoofing is an act of pretending to be someone or something else to gain access, mislead systems, or redirect communication.

4.1 IP spoofing

How it works:

It changes the source IP address in packets in order to mask an attacker's identity or impersonate another machine. Most often used for DDoS amplification.

Impact:

- Bypasses IP-based access controls.
- Hides the attackers during network abuse.

Remediation:

- Implement ingress and egress filtering (BCP 38)
- Never use IP addresses as an authentication factor.

4.2 ARP Spoofing (ARP Poisoning)

How it works:

Attackers use spoofed ARP messages to link their MAC addresses with the IP addresses of an intended host, thus intercepting local network traffic.

Impact:

- MITM attacks.
- Data tampering and credential theft.

Mitigation:

- Enable Dynamic ARP Inspection on switches.
- Use static ARP entries for critical systems.
- Adopt 802.1X and network segmentation.

4.3 DNS Spoofing / Cache Poisoning

How it works:

Attackers inject fake DNS records, allowing users to be directed to malicious websites even when the correct URL is typed.

Impact:

- Credential theft and phishing.
- Malware distribution.

Mitigation:

- Use DNSSEC to validate records.
- Use trusted DNS resolvers.
- Harden authoritative DNS servers.

4.4 Email Spoofing

How it works:

Attackers forge the "From" address in emails to impersonate trusted individuals or organizations.

Impact:

- Phishing and Business Email Compromise:
- Financial fraud and data leakage.

Mitigation:

- Set up SPF, DKIM, and DMARC.
- Train users to recognize suspicious e-mails.
- Use multi-factor authentication for sensitive approvals.

5. OTHER NOTABLE NETWORK THREATS

While not the primary focus, these threats are often found accompanying or enabling the attacks:

- Phishing and social engineering
- Session hijacking
- Port scanning and reconnaissance
- Ransomware spread via network shares
- Zero-day vulnerabilities in network-facing services

These require strong patching practices, endpoint protection, and network segmentation.

6. PREVENTIVE MEASURES

- A good defense involves several layers:
- Technical Controls
- Firewalls, IDS/IPS, VPNs, and secure switches.
- Enforce HTTPS and TLS everywhere.
- Patch and update your systems regularly.
- Employ multi-factor authentication for user access.
- Segment your networks to limit lateral movements.
- Monitoring & Response
- Log collection and real-time alerts.
- Regular security audits and penetration testing Keep tested backups.
- Prepare an incident response plan.
- User Awareness Teach users to avoid suspicious links.
- Encourage the use of caution when using public Wi-Fi.
- Encourage the reporting of suspicious activity.

7. CONCLUSION

DoS, MITM, and spoofing attacks continue to be significant threats because they exploit weaknesses in communication, trust, and network design. No single solution can block all attacks, but a layered approach, combining encryption, authentication, filtering, monitoring, and user education, greatly reduces risk. Organizations that remain proactive, monitor their network, and practice good security hygiene are in a better position to contain or repel such threats.