Task 4: Research Report on Common Network Security Threats

Objective:
Write a comprehensive research report on common network security threats such as DoS attacks, Man-in-the-Middle (MITM) attacks, and spoofing.

What is a Network?

A network is a system of interconnected devices (such as computers, servers, smartphones, routers, and switches) that communicate with each other to share data, resources, and services.

In simpler terms — think of it as a digital road system where data packets travel between devices, just like vehicles move between locations.

Key Components of a Network

- Nodes – Devices like computers, printers, or servers.
- Links – Physical (cables, fiber optics) or wireless (Wi-Fi, Bluetooth) connections between nodes.
- Protocols – Rules that define how data is transmitted (e.g., TCP/IP).
- Network Devices – Routers, switches, and firewalls that manage traffic.

Types of Networks

- LAN (Local Area Network) – Covers a small area (e.g., office, home).
- WAN (Wide Area Network) – Spans large geographic areas (e.g., the Internet).
- MAN (Metropolitan Area Network) – Covers a city or region.
- PAN (Personal Area Network) – Very short range (e.g., Bluetooth).

Why Networks Are Important

- Enable communication (email, chat, video calls)
- Facilitate resource sharing (files, printers, internet)
- Support collaboration and remote work
- Power modern services like cloud computing

What is the threat in terms of network ?

In terms of network security, a threat is any potential danger or malicious activity that can exploit a vulnerability in a network system to harm its data, operations, or users.

It doesn't have to be an actual attack — even the *possibility* of an attack is considered a threat.

Key Points

- Threat ≠ Attack → A threat is the *possibility* of something harmful happening, while an attack is the *actual* act of exploiting a vulnerability.
- Threats can be intentional (e.g., hacking, malware) or unintentional (e.g., human error, hardware failure).
- In network security, threats target confidentiality, integrity, and availability of data — known as the CIA Triad.

Examples of Network Threats

- Malware infections (viruses, worms, ransomware)
- Unauthorized access (hacking)
- Eavesdropping (intercepting network traffic)
- Denial-of-Service attacks
- Data theft or leakage
- Phishing and social engineering

Categories of Network Threats

1. Physical Threats – Hardware damage from natural disasters, theft, or sabotage.
2. Technical Threats – Software vulnerabilities, protocol weaknesses, misconfigurations.
3. Human-based Threats – Insider threats, phishing, accidental data leaks.

What is attack?

In network security, an attack is a deliberate action carried out by an individual or program to exploit vulnerabilities in a network, system, or application, with the goal of causing harm, stealing data, disrupting services, or gaining unauthorized access.

Unlike a threat (which is just the possibility of harm), an attack is the *actual execution* of that harm.

Key Points

- Attack = Threat in Action
- Always intentional (malicious), unlike some threats that may be accidental.
- Can be launched from inside (insider attacks) or outside (external attackers).
- Targets the CIA Triad:
    - Confidentiality – Stealing private data
    - Integrity – Altering data
    - Availability – Disrupting services

Common Types of Network Attacks

- Denial-of-Service (DoS) – Overloading a system to make it unavailable.
- Man-in-the-Middle (MITM) – Intercepting communications between two parties.
- Spoofing – Pretending to be a trusted source.
- Phishing – Tricking users into revealing sensitive info.
- Malware Attacks – Using malicious software to compromise systems.

Attack Lifecycle (Typical Steps)

1. Reconnaissance – Gathering information about the target.
2. Scanning – Identifying vulnerabilities.
3. Exploitation – Using weaknesses to gain access.
4. Maintaining Access – Installing backdoors or persistence.
5. Covering Tracks – Hiding evidence of the attack.

What is vulnerability?

A vulnerability is a security weakness, flaw, or misconfiguration in software, hardware, or network systems that could be exploited by an attacker to compromise confidentiality, integrity, or availability of data and services.

It can arise from:

- Software bugs (coding errors)
- Weak passwords
- Outdated systems
- Misconfigured security settings

Example:

- An unpatched operating system that allows hackers to run malicious code remotely.

In short:

> A vulnerability is the gap in your defenses; an attack is when someone uses that gap against you.

Common Network security threats and Attacks and Mitigation Measures

1. DDoS (Distributed Denial of Service)

Intro:

A DDoS attack is like a traffic jam on a busy road, but instead of cars, it's internet traffic flooding a website or server.

What it does:

It sends a huge amount of fake requests to a website or service, making it too busy to respond to real users.

How it works:

- The attacker controls many infected computers (called a botnet).
- All these computers send traffic to the target at the same time.

- The target server gets overloaded and slows down or crashes.

Effect:

- Website or service becomes unavailable.
- Businesses lose customers and money.
- Can harm a company's reputation.

Measures to take:

- Use a DDoS protection service (like Cloudflare, AWS Shield).
- Increase server bandwidth and capacity.
- Set up firewall rules to block suspicious traffic.
- Monitor traffic for unusual spikes.

2. MITM (Man-in-the-Middle) Attack

Intro:

This is like someone secretly listening and changing your conversation while you talk to a friend.

What it does:

The attacker intercepts communication between two parties and can:

- Read the data.
- Change the data before sending it.
- Steal sensitive information (passwords, banking details).

How it works:

- The attacker positions themselves between you and the service you're using.
- Could be done on insecure Wi-Fi or by hijacking a network.

- Data passes through the attacker without you noticing.

Effect:

- Sensitive data can be stolen.
- Accounts can be hacked.
- Fraudulent transactions may occur.

Measures to take:

- Always use HTTPS websites.
- Avoid public Wi-Fi without a VPN.
- Enable end-to-end encryption for messages.
- Keep devices updated with the latest security patches.

3. Spoofing

Intro

Spoofing is pretending to be someone or something else to trick people or systems.

What it does:

- The attacker changes their identity (like email address, IP address, or phone number) to look legitimate.
- Common types: Email spoofing, Caller ID spoofing, IP spoofing.

How it works:

- The attacker sends fake information that looks real.
- For example, an email looks like it's from your bank, but it's actually from the attacker.
- Victim is tricked into clicking links or giving sensitive info.

Effect:

- Victims can share passwords or bank details with the attacker.
- Can lead to malware infections.
- Businesses can lose customer trust.

Measures to take:

- Use email authentication protocols (SPF, DKIM, DMARC).
- Verify sender identity before responding or clicking links.
- Use firewalls and intrusion detection systems.
- Educate users about phishing and spoofed messages.
- Don't use public wifies or internet without knowing the source.

Real life examples of the attacks:

1. DDoS (Distributed Denial of Service)

Example:

- In 2016, the Dyn DNS DDoS attack took down major websites like Twitter, Netflix, PayPal, and Reddit.
- The attack was carried out using the Mirai botnet, made up of thousands of infected IoT devices (like security cameras and routers).
- Result: Many big websites were inaccessible for hours.

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

Example:

- In 2013, hackers used a MITM attack on Turkish Airlines Wi-Fi to intercept passenger credentials when they logged in to unsecured websites.
- Attackers sat between the users and the network, capturing usernames and passwords.

- Result: Stolen accounts and data leakage.

3. Spoofing

Example:

- In 2014, hackers sent email spoofing messages to Snapchat employees pretending to be the CEO.
- The fake email requested employee payroll data.
- Result: Sensitive payroll information for many employees was leaked.

Common threats and attacks these day:

1. Phishing Attacks

- Fake emails, messages, or websites trick people into revealing sensitive info like passwords or bank details.
- Often disguised as official messages from banks, companies, or government.

2. Ransomware

- Malicious software that locks or encrypts your files and demands payment (ransom) to unlock them.
- Example: WannaCry ransomware attack in 2017.

3. Malware

- Any malicious software (viruses, worms, Trojans, spyware) designed to damage or steal data.
- Can spread through email attachments, downloads, or infected USB drives.

4. DDoS (Distributed Denial of Service)

- Overloading a website or server with traffic so it crashes or becomes unavailable.
- Often used against businesses, governments, and online services.

5. MITM (Man-in-the-Middle)

- Hackers secretly intercept and change communication between two parties.
- Common on insecure public Wi-Fi networks.

6. Spoofing

- Pretending to be someone else (email, IP address, phone number) to trick victims.
- Often used with phishing to seem more believable.

7. Credential Stuffing

- Hackers use stolen username-password combinations from one breach to try logging in to other accounts (since many people reuse passwords).

8. SQL Injection

- Inserting malicious code into a website's database query to access or alter data.
- Can steal user info, delete data, or take over the website.

9. **Zero-Day Exploits**

- Attacks that take advantage of unknown software vulnerabilities before developers can fix them.

10. Insider Threats

- Employees or contractors intentionally or accidentally leak sensitive data or cause security damage.

Conclusion:
Cyberattacks like DDoS, Man-in-the-Middle, and Spoofing are some of the most common threats to network security today. They work in different ways — some overwhelm systems, some secretly intercept communications, and others pretend to be trusted sources — but all can cause serious harm such as service downtime, data theft, financial loss, and reputational damage.

Preventing these attacks requires a combination of **technical defenses** (like firewalls, encryption, and monitoring tools) and **good security practices** (like keeping systems updated, using strong authentication, and educating users). By staying aware of these threats and implementing proper measures, individuals and organizations can greatly reduce the risk of becoming a victim.

References

- Cloudflare – DDoS Attacks
- OWASP – MITM Attacks
- NIST – Cybersecurity Framework