Task 4: Research Report on Common Network Security Threats

Internship Program: OASIS Infobyte (OIBSIP)
Submitted by: Alfiya Siddiqui
Task: Network Security Threats

□ 1. Introduction

Network security is an important aspect of protecting computer networks from unauthorized access, misuse, and attacks.
With the increasing use of the internet and digital communication, networks have become vulnerable to various security threats.

Network security threats are malicious activities that aim to compromise the confidentiality, integrity, or availability of network systems.
This report discusses common network security threats, their impact, real-world examples, and preventive measures.

□ 2. Types of Network Security Threats

2.1 Denial of Service (DoS) and Distributed Denial of Service (DDoS)

A Denial of Service (DoS) attack occurs when an attacker floods a network or server with excessive traffic, making it unavailable to legitimate users.
A Distributed Denial of Service (DDoS) attack is more severe, as it uses multiple compromised systems to launch the attack simultaneously.

Effects:

- Server downtime
- Service unavailability
- Financial loss

2.2 Man-in-the-Middle (MITM) Attacks

In a Man-in-the-Middle attack, an attacker secretly intercepts communication between two parties without their knowledge.
This attack is common in unsecured public Wi-Fi networks.

Risks:

- Data theft
- Credential stealing
- Communication manipulation

Task 4: Research Report on Common Network Security Threats

2.3 Spoofing

Spoofing is a technique where an attacker impersonates a trusted entity to gain unauthorized access to a network.

Common types:

- IP spoofing
- Email spoofing
- ARP spoofing

2.4 Packet Sniffing / Eavesdropping

Packet sniffing involves capturing data packets traveling through a network to extract sensitive information such as usernames and passwords.

Impact:

- Loss of sensitive data
- Privacy violation

2.5 DNS Spoofing / Poisoning

DNS spoofing redirects users from legitimate websites to malicious ones by corrupting DNS records.

Consequences:

- Phishing attacks
- Malware infections

□ 3. Impact of Network Security Threats

Network security threats can cause serious damage to organizations and individuals, including:

- Data breaches
- Financial losses
- Damage to reputation
- Legal and compliance issues

Task 4: Research Report on Common Network Security Threats

□ 4. Real-World Examples

- Large-scale DDoS attacks on banking and e-commerce websites
- MITM attacks in public Wi-Fi hotspots
- DNS spoofing attacks used for phishing scams

□ 5. Mitigation and Preventive Measures

To protect networks from security threats, the following measures can be implemented:

- Use firewalls and intrusion detection systems
- Encrypt network communication
- Regularly update software and systems
- Implement strong authentication methods

□ 6. Best Practices for Organizations

Organizations should follow these best practices:

- Conduct regular security audits
- Provide cybersecurity training to employees
- Monitor network traffic continuously
- Maintain regular data backups

□ 7. Conclusion

Network security threats pose significant risks to modern digital systems.
Understanding common threats and implementing preventive measures is essential for maintaining secure and reliable networks.
By following best practices and using appropriate security tools, organizations can minimize the impact of these threats.

□ 8. References

- Cisco Networking Academy
- Cloudflare Security Resources
- Kaspersky Cybersecurity Reports

Task 4: Research Report on Common Network Security Threats