TASK1:

Network Security Basics

Introduction:

This report provides a comprehensive overview of the fundamentals of network security, focusing on the identification of common threats and the implementation of basic security measures. The goal is to establish a foundational understanding of how to protect a small network from potential vulnerabilities.

Types of Network Threats:

A variety of threats can compromise network security. Some of the most common include:

- **Viruses**: These are malicious software programs that attach themselves to other executable programs. They can replicate and spread to other computers, causing damage or disruption
- **Worms**: Similar to viruses, worms can replicate and spread independently. They often exploit vulnerabilities in network protocols to propagate rapidly
- **Trojans**: These are malicious programs disguised as legitimate software. They often provide a backdoor for attackers to gain unauthorized access to a system
- **Phishing Attacks:** These are attempts to deceive individuals into revealing sensitive information, such as passwords or credit card numbers. Phishing emails or websites often mimic legitimate organizations to trick users

Basic Security Concepts:

To mitigate these threats, it is essential to understand fundamental security concepts:

- **Firewalls:** Hardware or software devices that filter network traffic to block unauthorized access.
- **Encryption:** The process of encoding data to make it unreadable to unauthorized parties.
- **Secure Network Configurations:** Proper settings and configurations to protect a network from vulnerabilities.

Implementing Basic Security Measures:

To secure a small network, the following measures were implemented:

- **Firewall Configuration:** A basic firewall (Windows Defender Firewall) was enabled and configured to block unauthorized traffic.

- **Password Management:** Default passwords were changed to stronger, unique values.
- **Network Encryption:** WPA2 or WPA3 encryption was enabled to protect wireless network communications.

Network Traffic Analysis:

I used Wireshark to capture and analyze network traffic. This allowed me identification of different traffic types (e.g., HTTP, DNS) and the detection of any suspicious activity that might indicate a security threat.

Findings and Recommendations:

The analysis revealed that the implemented security measures protect the network from common threats. However, additional measures could be considered for larger, more complex networks, such as:

- **Intrusion Detection Systems (IDS):** Software that monitors network traffic for signs of intrusion.
- **Virtual Private Networks (VPNs):** Encrypted tunnels that can protect data transmitted over public networks.
- **Regular Updates:** Keeping software and operating systems up-to-date with the latest security patches.

Conclusion:

Understanding network security fundamentals is crucial for protecting valuable data and resources. By implementing basic security measures and regularly monitoring network traffic, individuals and organizations can significantly reduce the risk of cyberattacks.