Task 3: Networking Basics for Cyber Security

Tool Used: Wireshark (Windows)

Introduction

In this task, live network traffic was captured using Wireshark to understand how devices communicate over a network. The goal was to build a strong foundation in networking concepts used in cyber security.In this task, live network traffic was captured using Wireshark to understand how devices communicate over a network. The goal was to build a strong foundation in networking concepts used in cyber security.In this task, live network traffic was captured using Wireshark to understand how devices communicate over a network. The goal was to build a strong foundation in networking concepts used in cyber security.

Packet Sniffing

Packet sniffing is the process of intercepting and logging network packets. Wireshark allows us to analyze packet contents and detect potential threats or vulnerabilities.Packet sniffing is the process of intercepting and logging network packets. Wireshark allows us to analyze packet contents and detect potential threats or vulnerabilities.Packet sniffing is the process of intercepting and logging network packets. Wireshark allows us to analyze packet contents and detect potential threats or vulnerabilities.

TCP Handshake

The TCP three-way handshake was observed. This process establishes a reliable connection between a client and a server using SYN, SYN-ACK, and ACK packets.The TCP three-way handshake was observed. This process establishes a reliable connection between a client and a server using SYN, SYN-ACK, and ACK packets.The TCP three-way handshake was observed. This process establishes a reliable connection between a client and a server using SYN, SYN-ACK, and ACK packets.

TCP vs UDP

TCP ensures reliable and ordered delivery of data, while UDP is faster but does not guarantee delivery. Understanding the difference helps in identifying the type of traffic captured.TCP ensures reliable and ordered delivery of data, while UDP is faster but does not guarantee delivery. Understanding the difference helps in identifying the type of traffic captured.TCP ensures reliable and ordered delivery of data, while UDP is faster but does not guarantee delivery. Understanding the difference helps in identifying the type of traffic captured.

DNS Analysis

DNS traffic was captured to observe how domain names are translated into IP addresses. This is useful for detecting suspicious domain queries or malicious connections.DNS traffic was captured to observe how domain names are translated into IP addresses. This is useful for detecting suspicious domain queries or malicious connections.DNS traffic was captured to observe how domain names are translated into IP addresses. This is useful for detecting suspicious domain

queries or malicious connections.

HTTP vs HTTPS

Plain-text HTTP traffic can be read directly, while HTTPS traffic is encrypted using TLS. This demonstrates why HTTPS is considered more secure for transmitting sensitive data.Plain-text HTTP traffic can be read directly, while HTTPS traffic is encrypted using TLS. This demonstrates why HTTPS is considered more secure for transmitting sensitive data.Plain-text HTTP traffic can be read directly, while HTTPS traffic is encrypted using TLS. This demonstrates why HTTPS is considered more secure for transmitting sensitive data.

Process Monitoring

Monitoring active network processes helps in identifying unusual or malicious activity. This is a key step in securing and hardening an operating system.Monitoring active network processes helps in identifying unusual or malicious activity. This is a key step in securing and hardening an operating system.Monitoring active network processes helps in identifying unusual or malicious activity. This is a key step in securing and hardening an operating system.

Conclusion

Through this task, the ability to capture and analyze network packets was developed. These skills are essential for understanding network-based attacks and improving cyber security awareness.Through this task, the ability to capture and analyze network packets was developed. These skills are essential for understanding network-based attacks and improving cyber security awareness.Through this task, the ability to capture and analyze network packets was developed. These skills are essential for understanding network-based attacks and improving cyber security awareness.

Author: Mohammed Nihal