Network Security Lab – Final Project Summary

Prepared by: Judy Raj

Overview

This project, completed as part of Coursera's Network Security Fundamentals course, demonstrates core competencies in designing subnet-based network architectures, capturing and analyzing network traffic, and configuring Windows Defender Firewall rules to manage HTTP, HTTPS, and FTP access. The total assignment carried 50 points across multiple technical tasks.

Task Summary

Task	Description	Points
1	Design a subnetted network diagram with router, switch, and 3 subnets (Admin, Sales, IT).	5
2	Calculate subnet addresses and masks for each department.	15
3	Capture and analyze HTTP/HTTPS traffic using Wireshark.	10
4.1–4.6	Configure Windows Defender Firewall rules for FTP and HTTP access control.	20

Skills Demonstrated

• Network Design and Subnetting
• Firewall Configuration and Access Control
• Wireshark Traffic Capture and Protocol Analysis
• Understanding of HTTP, HTTPS, and FTP protocols
• Applied Network Security Troubleshooting

Outcome

The project demonstrates proficiency in securing network environments through structured subnetting, effective traffic monitoring, and proactive firewall rule configuration. It reflects practical application of cybersecurity fundamentals to protect systems and data integrity.

References

Coursera – Network Security Fundamentals (TechSafe, Ltd. Lab Simulation)
Microsoft Documentation – Windows Defender Firewall with Advanced Security
Wireshark User Guide – HTTPS/HTTP Packet Analysis