# Network Security Analyst Portfolio — Day 5 & 6

## 🧠 Day 5 — Network Port Security and Firewall Configuration

Objective:  
To identify open ports on a local system, analyze potential vulnerabilities, and secure the system using Windows Firewall rules.

Tools Used:  
- Command Prompt / PowerShell  
- Nmap  
- Netstat  
- Windows Defender Firewall (netsh advfirewall)

Procedure:

1. Ran `netstat -ano | findstr LISTENING` to identify all active listening ports and associated process IDs.
2. Used `nmap -sT -Pn 127.0.0.1` and `nmap -sT -Pn <local IP>` to scan open TCP ports on the system.
3. Identified open and potentially vulnerable ports (135, 139, 445) — commonly exploited for SMB, RPC, and NetBIOS attacks.
4. Configured firewall rules to block these ports:  
   netsh advfirewall firewall add rule name="Block RPC (135)" dir=in action=block protocol=TCP localport=135  
   netsh advfirewall firewall add rule name="Block NetBIOS (139)" dir=in action=block protocol=TCP localport=139  
   netsh advfirewall firewall add rule name="Block SMB (445)" dir=in action=block protocol=TCP localport=445
5. Verified the firewall rules using:  
   netsh advfirewall firewall show rule name=all | findstr "Block"

Result:  
- The system’s vulnerable ports were successfully blocked.  
- Outbound and inbound network traffic was restricted based on custom security policies.  
- Demonstrated understanding of port management and basic network hardening.

Key Skills Demonstrated:  
✅ Network Scanning  
✅ Port and Protocol Analysis  
✅ Windows Firewall Configuration  
✅ System Hardening

## 🌐 Day 6 — Subnetting and Wireshark Network Traffic Analysis

Objective:  
To understand IP subnetting for efficient network design and to analyze live network traffic using Wireshark.

Tools Used:  
- PowerShell  
- Subnet Calculator  
- Wireshark

Procedure:

1. Practiced subnetting on a Class C network (192.168.1.0/24) into four /26 subnets to improve network segmentation.
2. Verified current system IP and subnet configuration:  
    ipconfig /all
3. Saved network configuration output for documentation:  
    ipconfig /all > C:\Users\user\Desktop\network\_info.txt
4. Opened Wireshark and captured live traffic for 2 minutes.
5. Applied filters to isolate protocols:  
    - tcp  
    - udp  
    - http  
    - ip.addr == 8.8.8.8
6. Saved the capture as `day6\_capture.pcapng`.

Result:  
- Successfully analyzed real-time network packets.  
- Identified different protocols and packet types.  
- Understood how subnetting affects IP distribution and communication.

Key Skills Demonstrated:  
✅ Subnetting & IP Planning  
✅ Packet Capturing & Analysis  
✅ Wireshark Filtering  
✅ Documentation of Network Configurations

📁 Files Included for Portfolio:  
- day5\_firewall\_rules.txt (optional)  
- day6\_capture.pcapng  
- network\_info.txt  
- Screenshots of Nmap & Wireshark results