Branden Solomon
Malachi Clark
3/13/25
Doctor Latson
CTEC 402

Final Case Study Reports

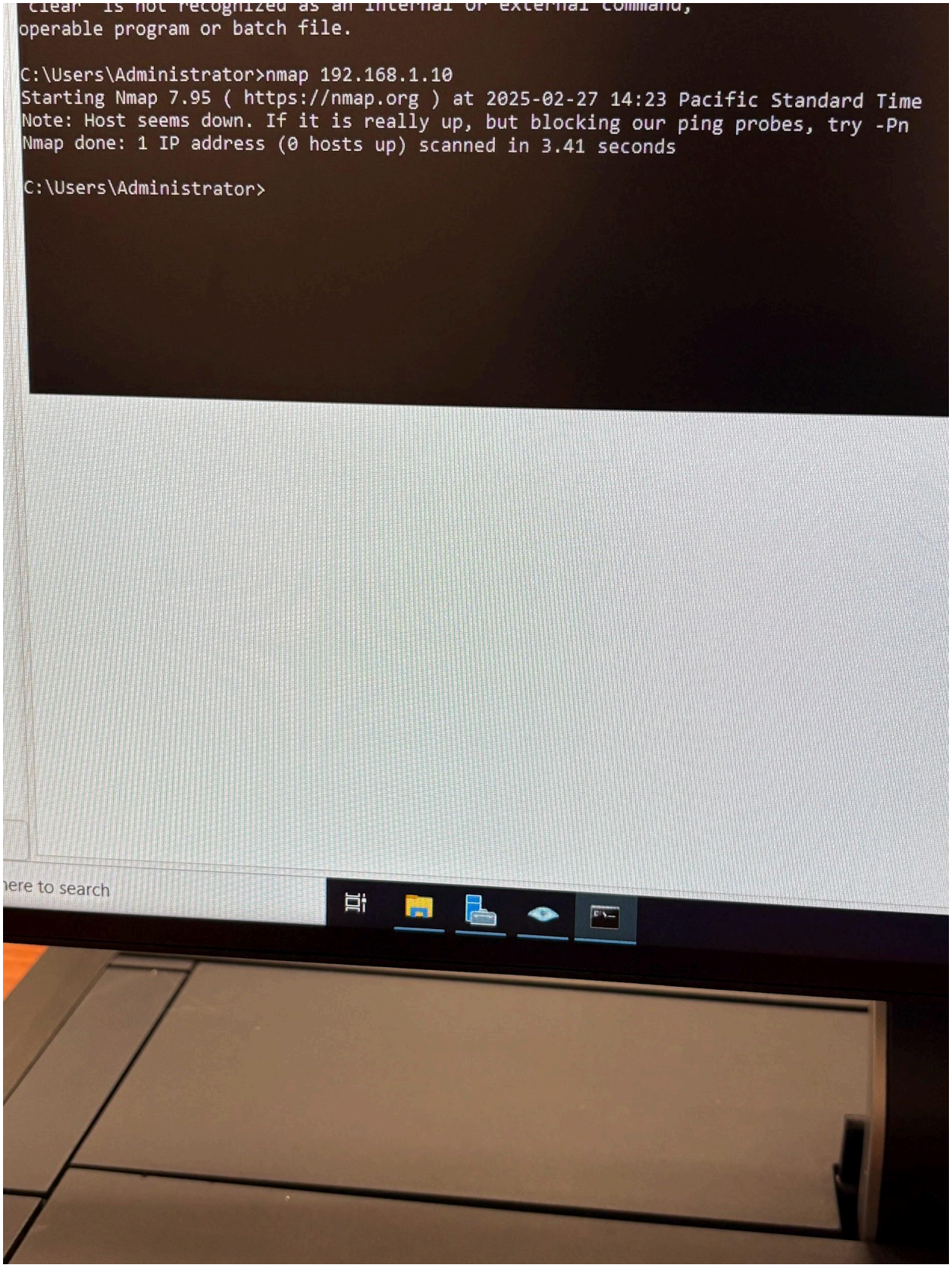
Nmap Summary

Step 1: Scan for Open Ports Using Nmap

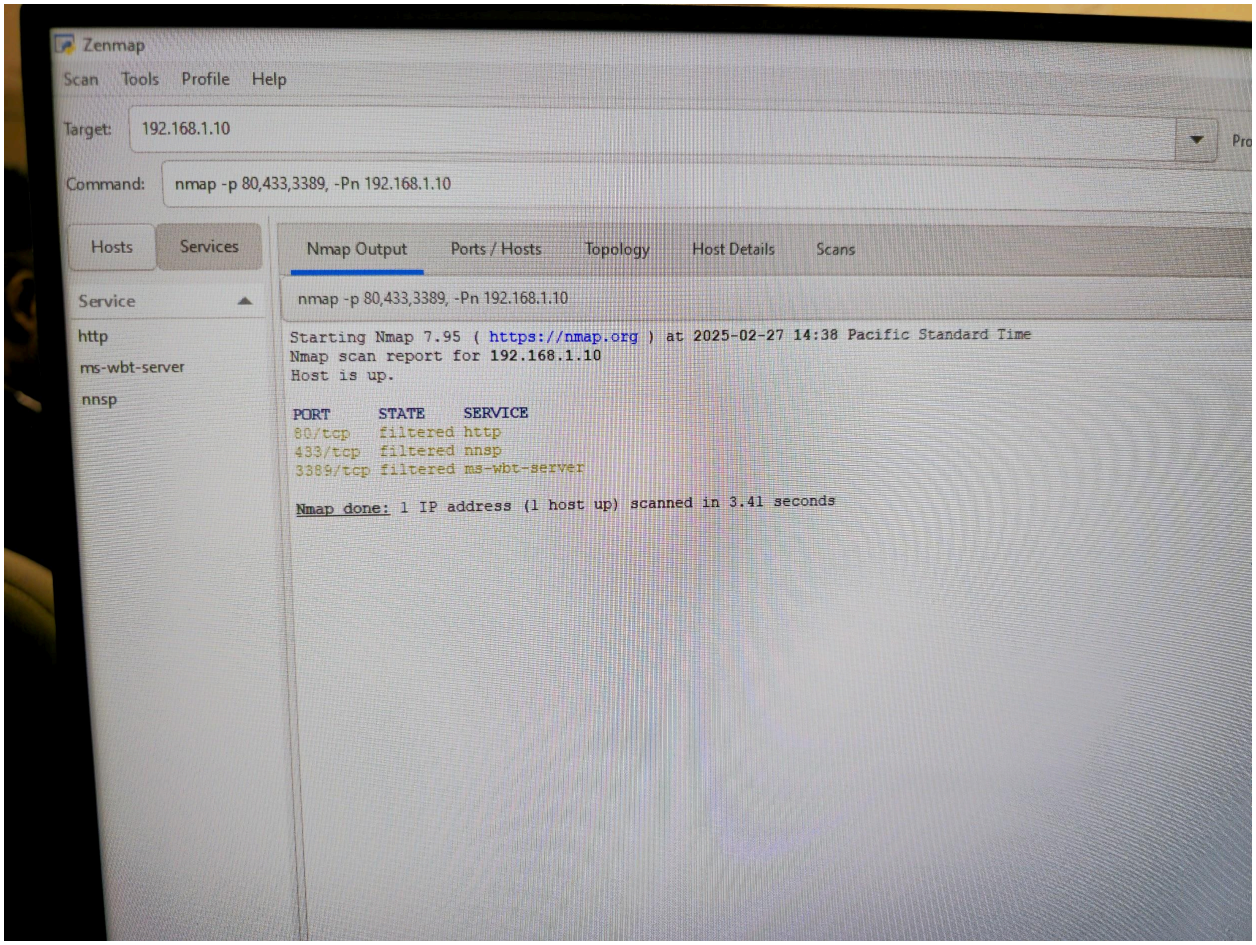
Now that Nmap is installed, you can begin performing scans to identify open ports and potential vulnerabilities.

Basic Scan for Open Ports:

After verifying we successfully installed nmap on the pc, the next thing we do is run a simple scan on the virtual machine's IP address to identify open ports: nmap 192.168.1.10.


'clear' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Administrator>nmap 192.168.1.10
Starting Nmap 7.95 (https://nmap.org) at 2025-02-27 14:23 Pacific Standard Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.41 seconds
C:\Users\Administrator>
here to search

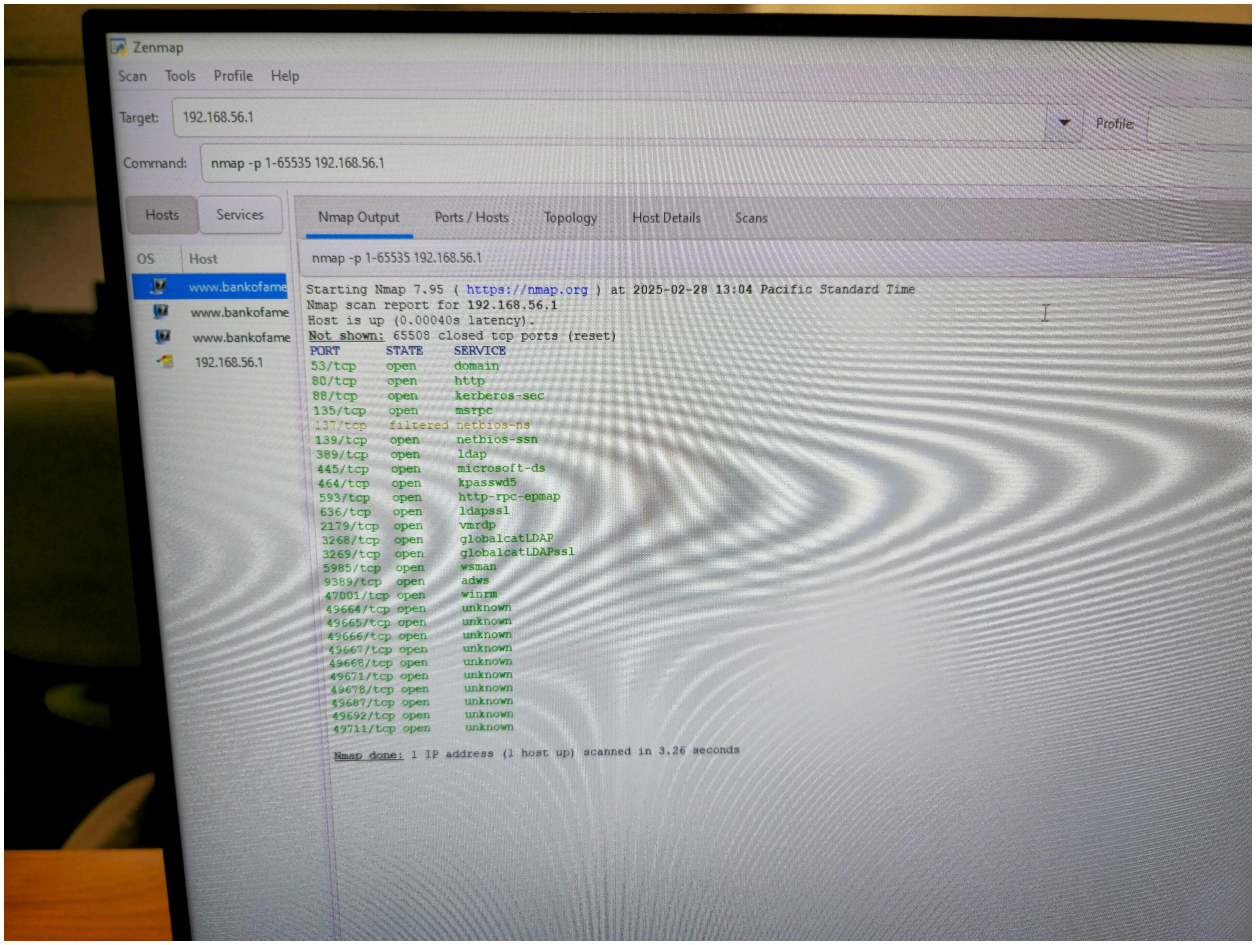
Scan Specific Ports



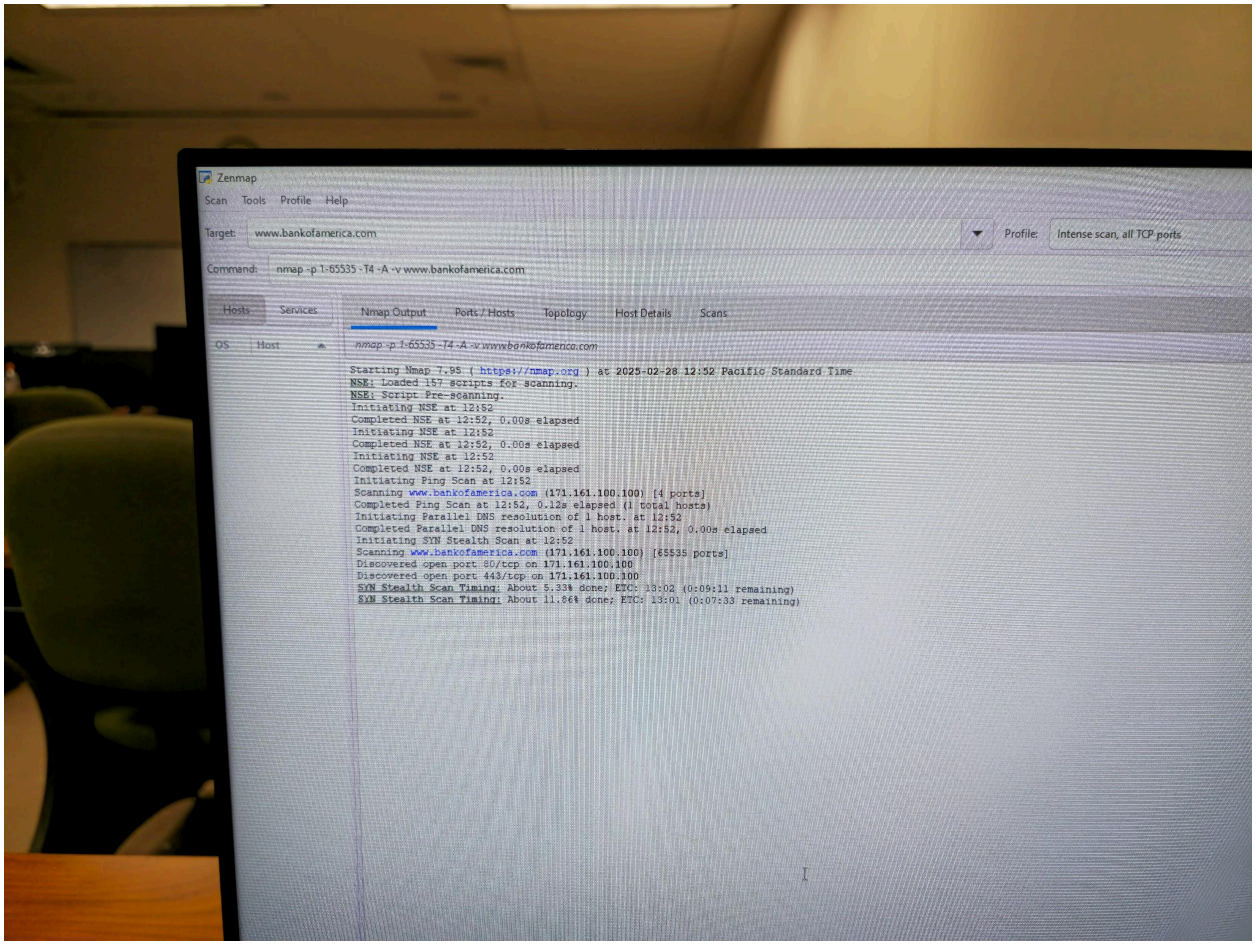
Step 2: Scan for Vulnerabilities Using Nmap Scripting Engine (NSE)

Scan for Common Vulnerabilities:

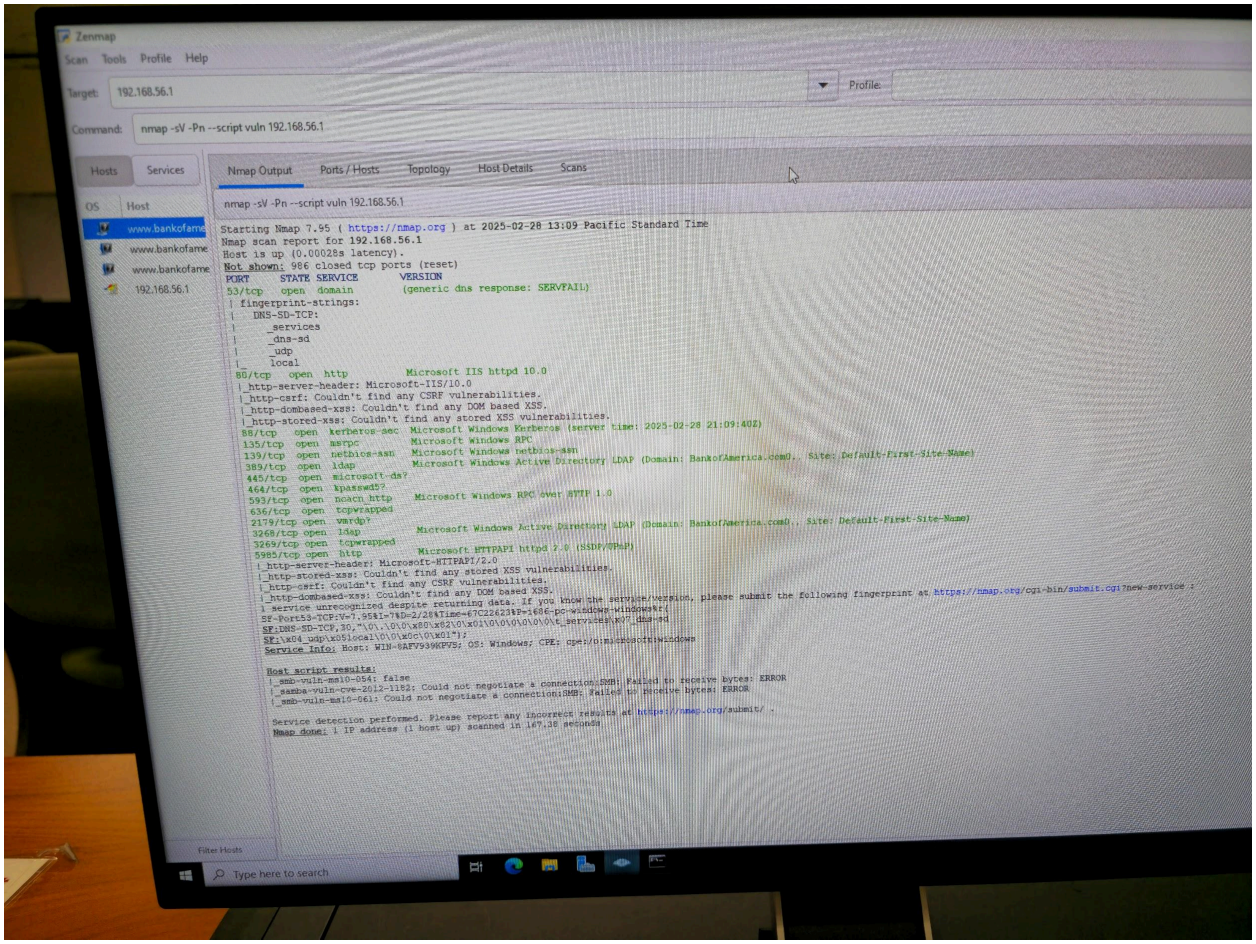
Branden:


Zenmap
Scan Tools Profile Help
Target: 192.168.56.1
Profile:
Command: nmap -p 1-65535 192.168.56.1
Hosts Services
OS Host
www.bankofame
www.bankofame
www.bankofame
192.168.56.1
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -p 1-65535 192.168.56.1
Starting Nmap 7.95 (https://nmap.org) at 2025-02-28 13:04 Pacific Standard Time
Nmap scan report for 192.168.56.1
Host is up (0.00040s latency).
Not shown: 65508 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
135/tcp open msrpc
137/tcp filtered netbios-ns
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
2179/tcp open vmrdp
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
5985/tcp open wsman
9389/tcp open adws
47001/tcp open winrm
49664/tcp open unknown
49665/tcp open unknown
49666/tcp open unknown
49667/tcp open unknown
49668/tcp open unknown
49671/tcp open unknown
49678/tcp open unknown
49687/tcp open unknown
49692/tcp open unknown
49711/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 3.26 seconds

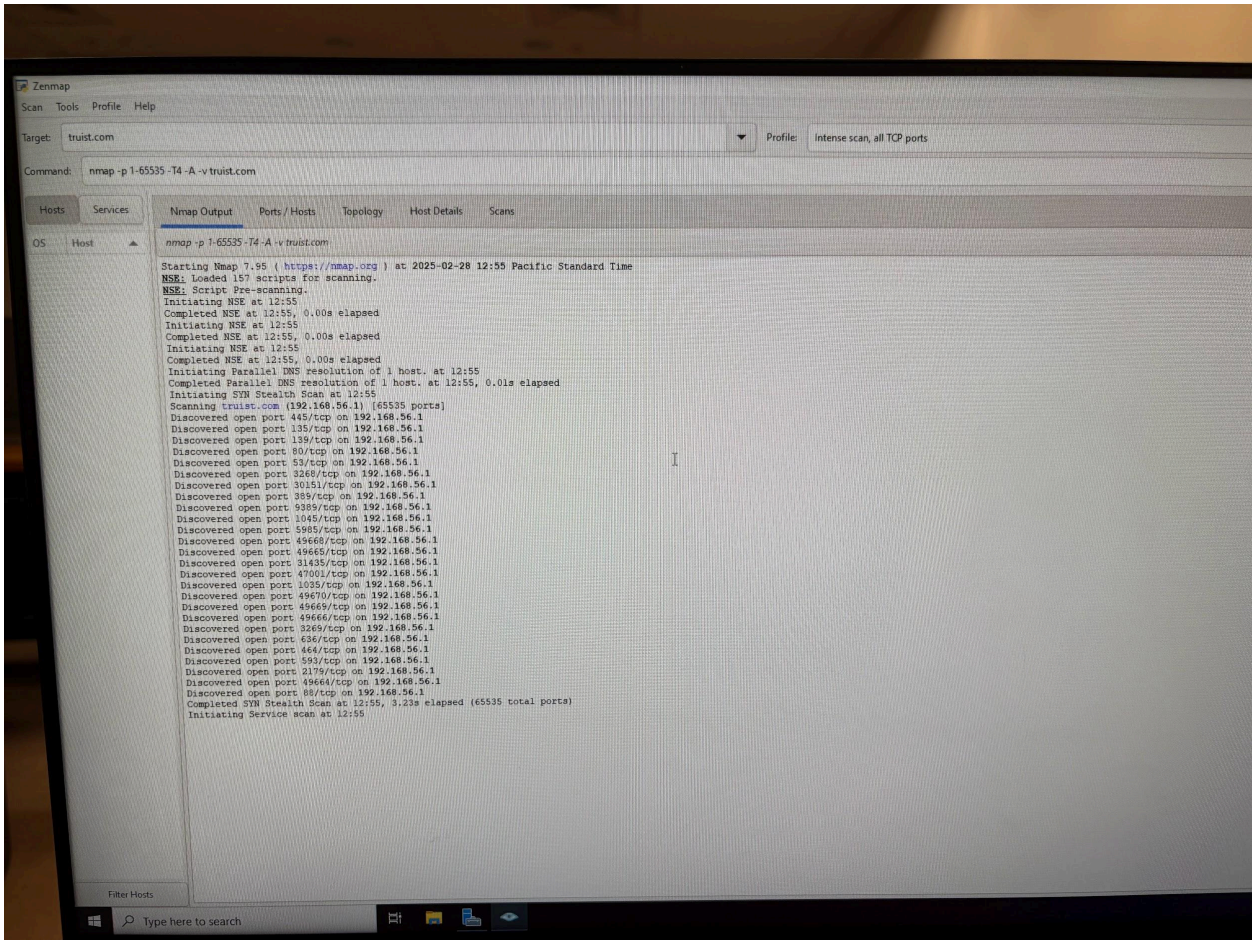
Scan Open Ports

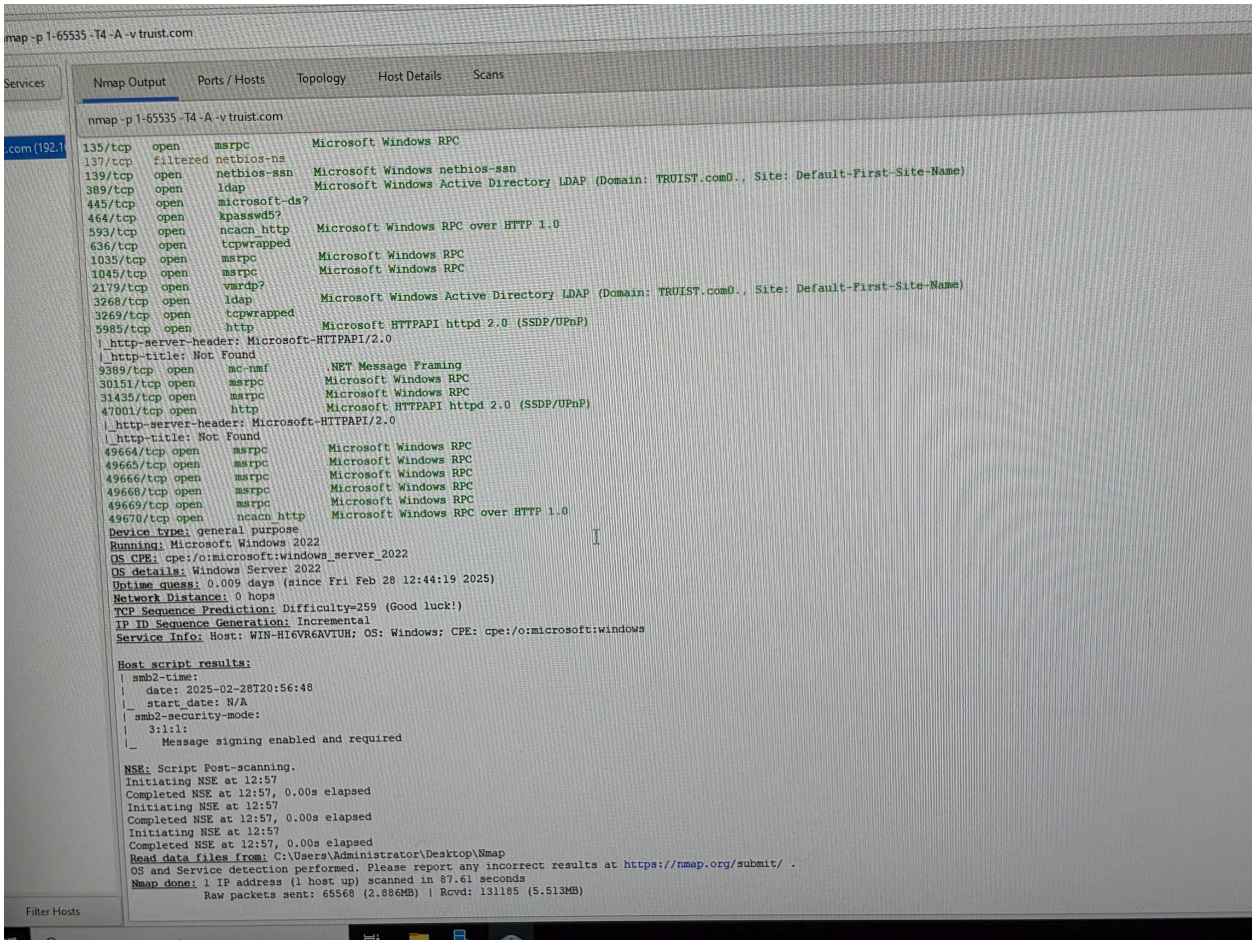


Scan for Vulnerabilities and Services:

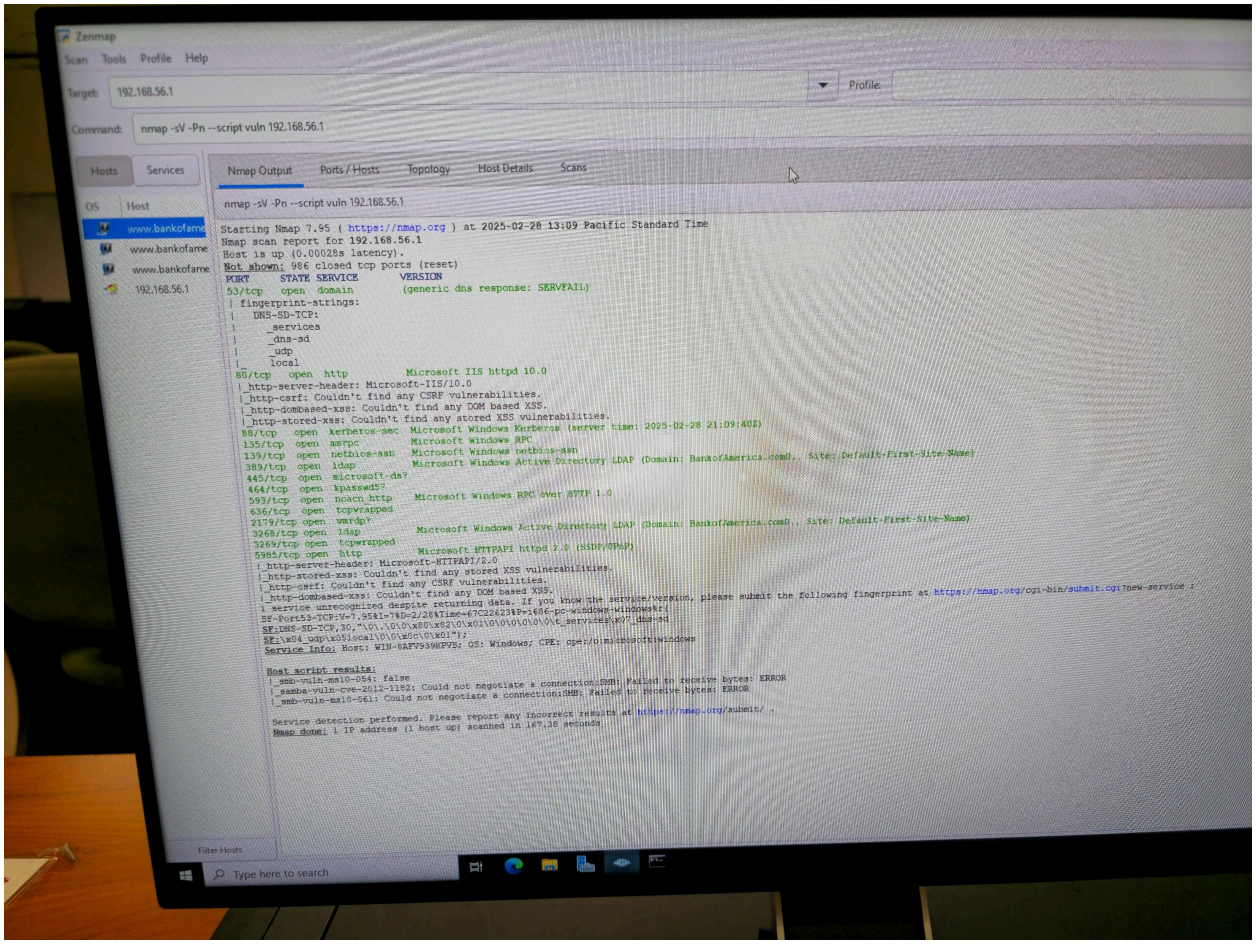


Malachi:
Scan Open Ports:


Zenmap
Scan Tools Profile Help
Target: truist.com
Profile: Intense scan, all TCP ports
Command: nmap -p 1-65535 -T4 -A -v truist.com
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
nmap -p 1-65535 -T4 -A -v truist.com
Starting Nmap 7.95 (https://nmap.org) at 2025-02-28 12:55 Pacific Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:55
Completed NSE at 12:55, 0.00s elapsed
Initiating NSE at 12:55
Completed NSE at 12:55, 0.00s elapsed
Initiating NSE at 12:55
Completed NSE at 12:55, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 12:55
Completed Parallel DNS resolution of 1 host. at 12:55, 0.01s elapsed
Initiating SYN Stealth Scan at 12:55
Scanning truist.com (192.168.56.1) [65535 ports]
Discovered open port 445/tcp on 192.168.56.1
Discovered open port 135/tcp on 192.168.56.1
Discovered open port 139/tcp on 192.168.56.1
Discovered open port 80/tcp on 192.168.56.1
Discovered open port 53/tcp on 192.168.56.1
Discovered open port 3268/tcp on 192.168.56.1
Discovered open port 30151/tcp on 192.168.56.1
Discovered open port 389/tcp on 192.168.56.1
Discovered open port 9389/tcp on 192.168.56.1
Discovered open port 1045/tcp on 192.168.56.1
Discovered open port 5985/tcp on 192.168.56.1
Discovered open port 49668/tcp on 192.168.56.1
Discovered open port 49665/tcp on 192.168.56.1
Discovered open port 31435/tcp on 192.168.56.1
Discovered open port 47001/tcp on 192.168.56.1
Discovered open port 1035/tcp on 192.168.56.1
Discovered open port 49670/tcp on 192.168.56.1
Discovered open port 49669/tcp on 192.168.56.1
Discovered open port 49666/tcp on 192.168.56.1
Discovered open port 3269/tcp on 192.168.56.1
Discovered open port 636/tcp on 192.168.56.1
Discovered open port 464/tcp on 192.168.56.1
Discovered open port 593/tcp on 192.168.56.1
Discovered open port 2179/tcp on 192.168.56.1
Discovered open port 49664/tcp on 192.168.56.1
Discovered open port 88/tcp on 192.168.56.1
Completed SYN Stealth Scan at 12:55, 3.23s elapsed (65535 total ports)
Initiating Service scan at 12:55
Filter Hosts
Type here to search



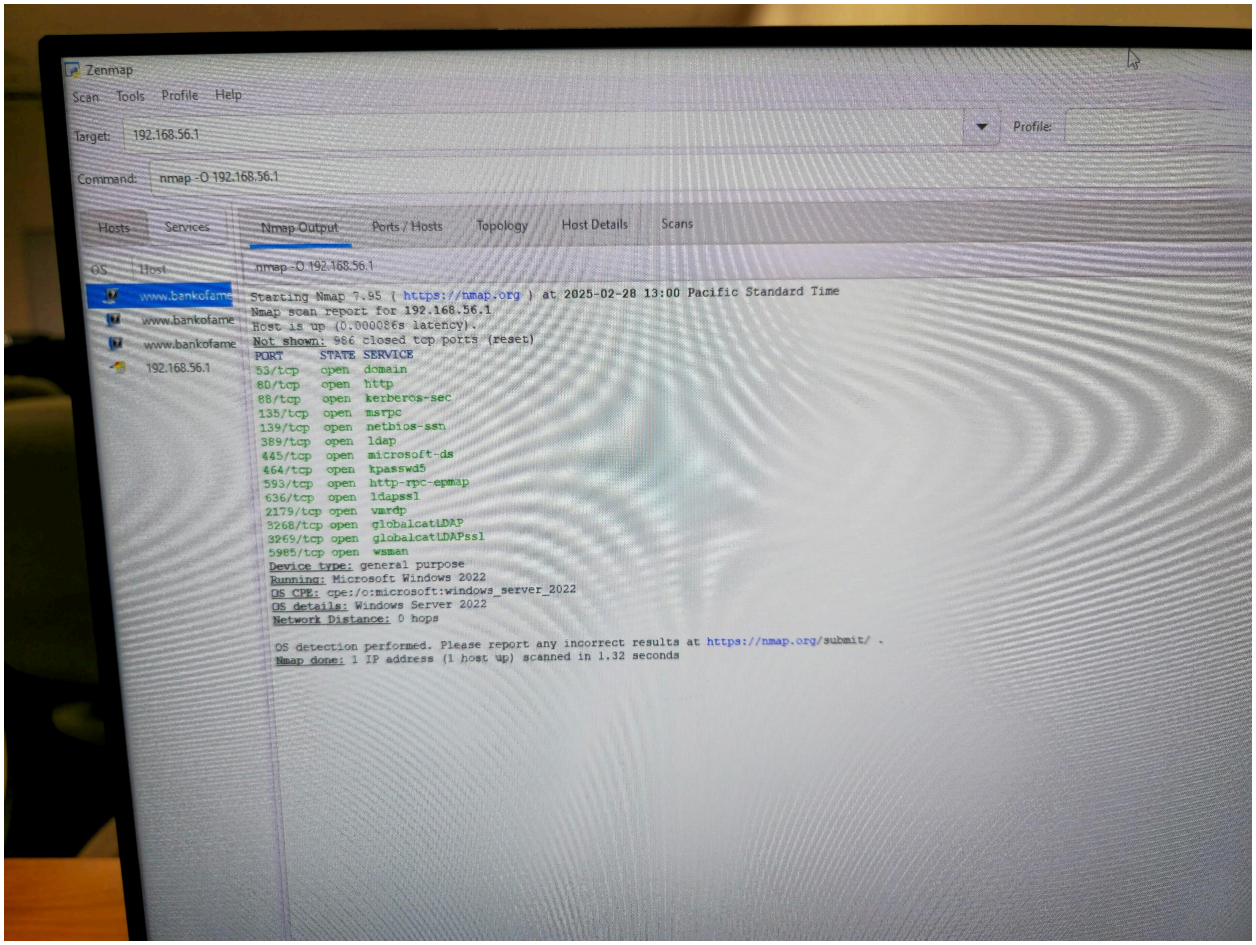
Scan for Vulnerabilities and Services:



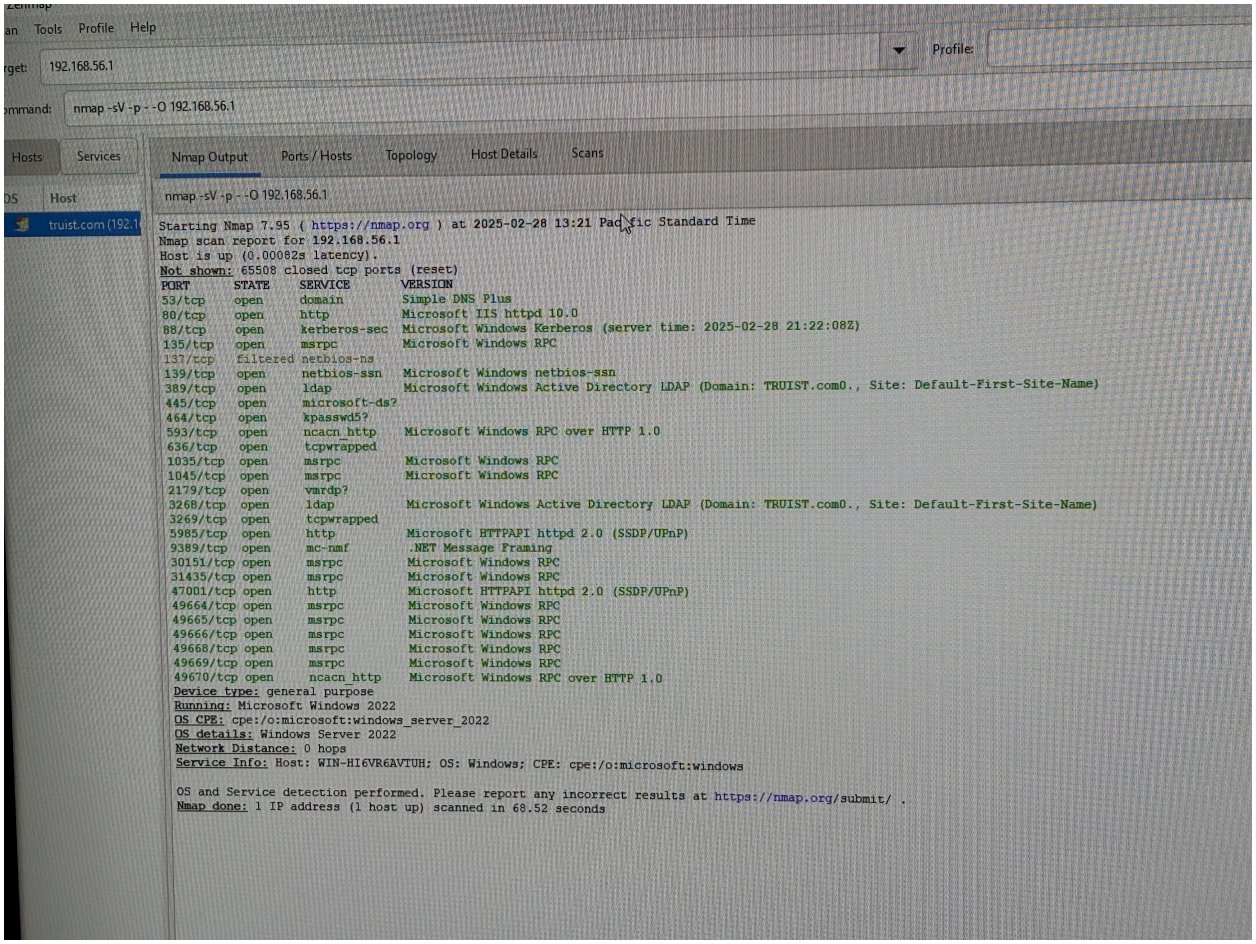
Step 3: Scan for Operating System Detection

We identify the operating system and other details of the server by typing the command nmap -O 192.168.156.1

Branden:

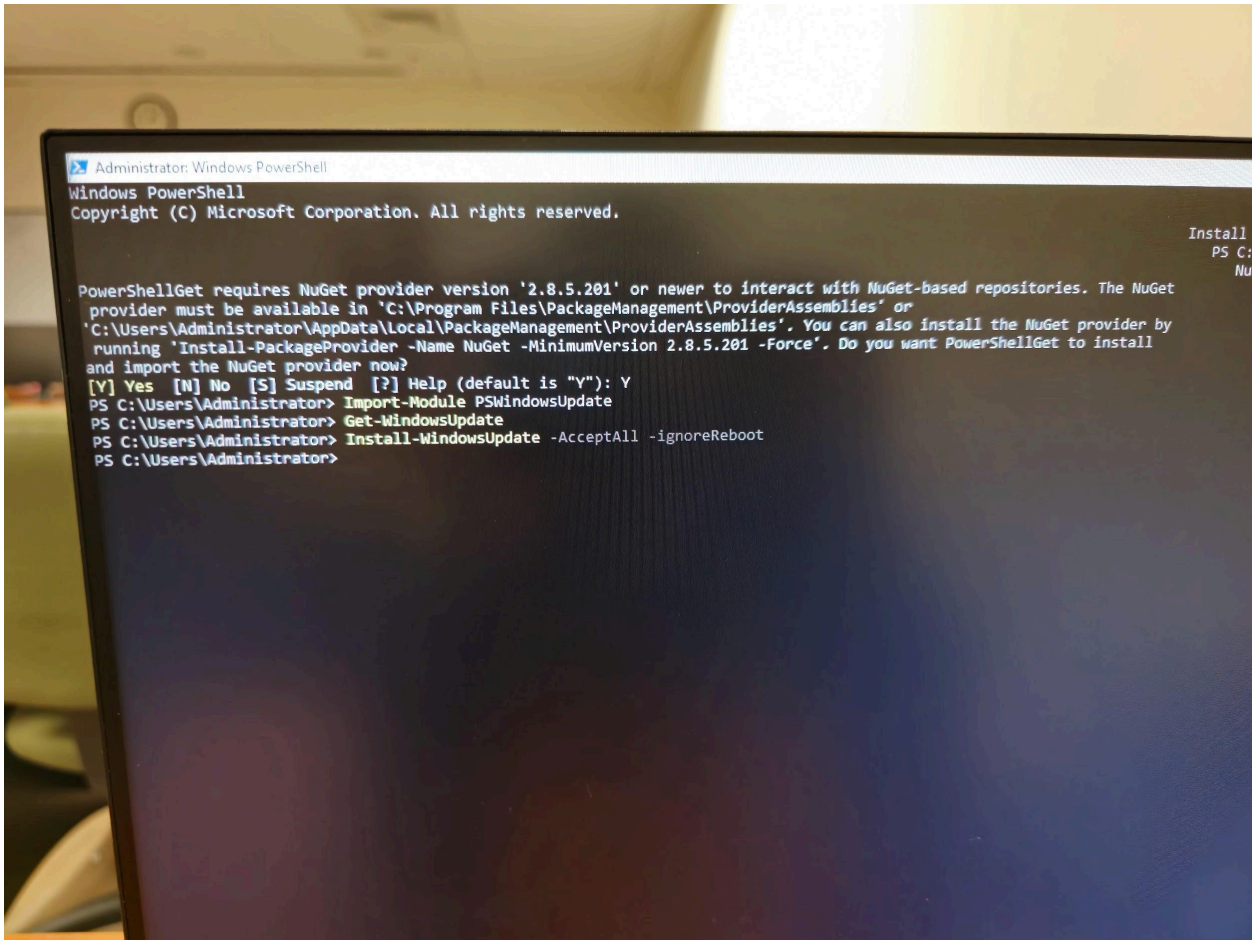


Malachi:

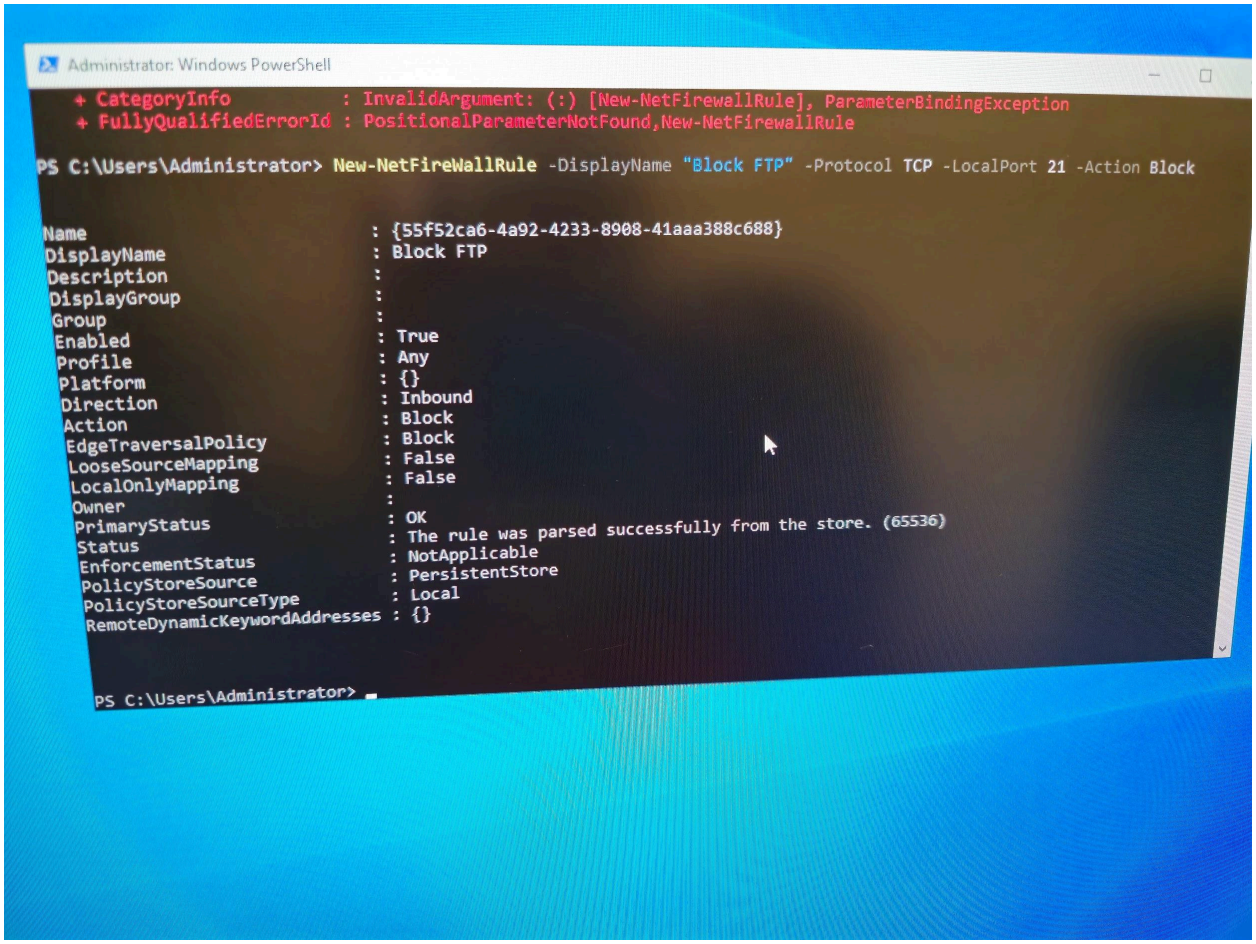


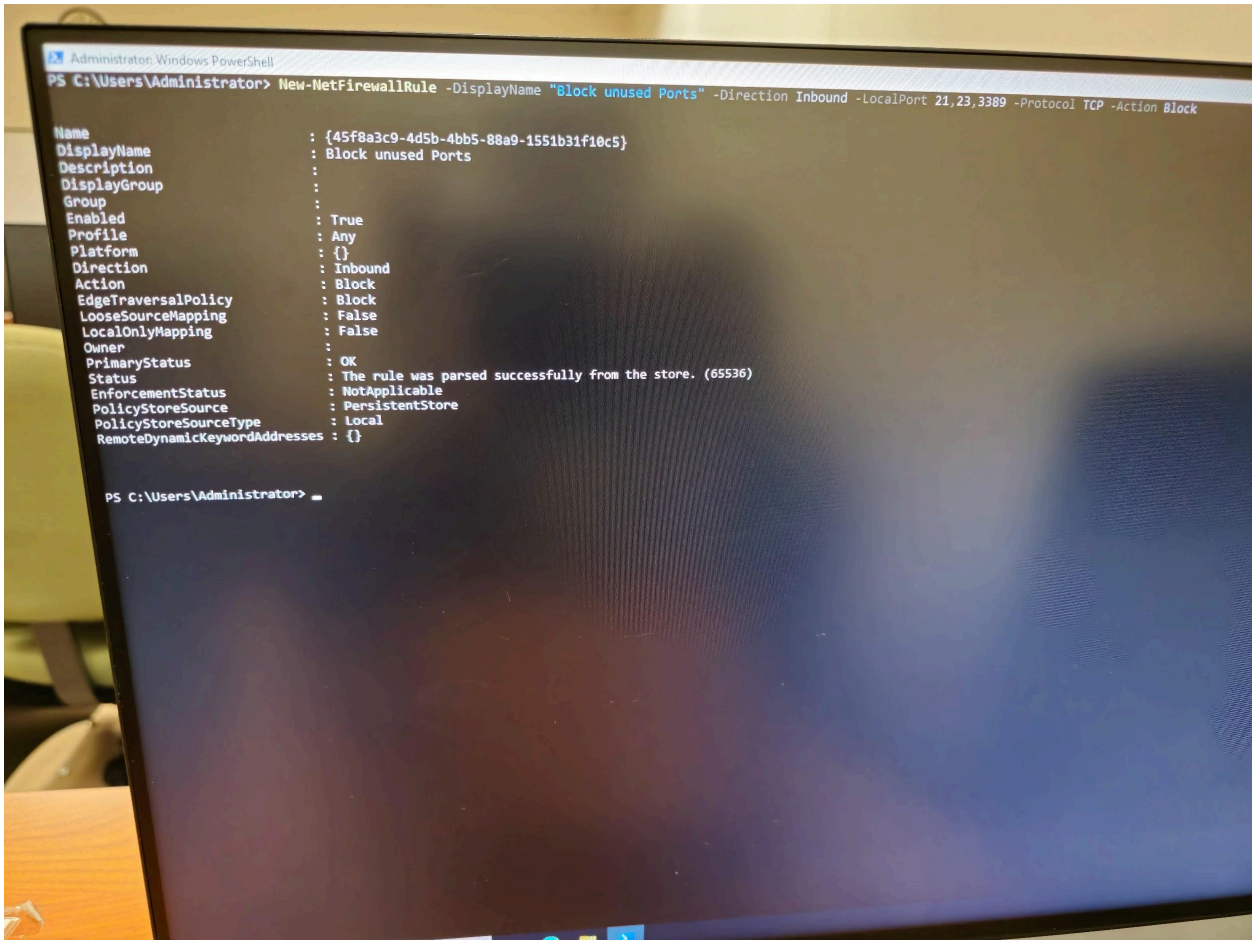
Step 4: Patch & Secure the Server

Apply Windows Updates

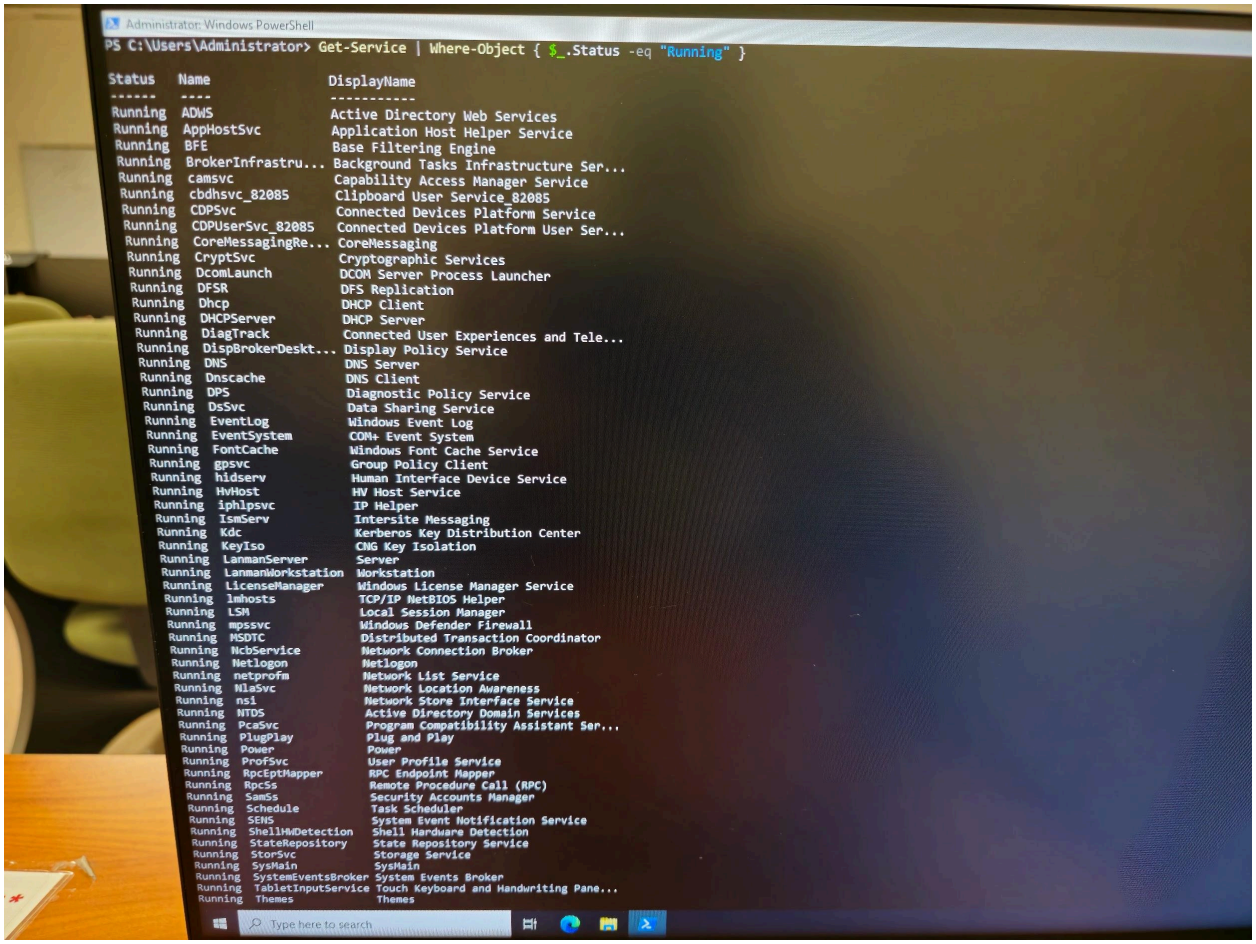


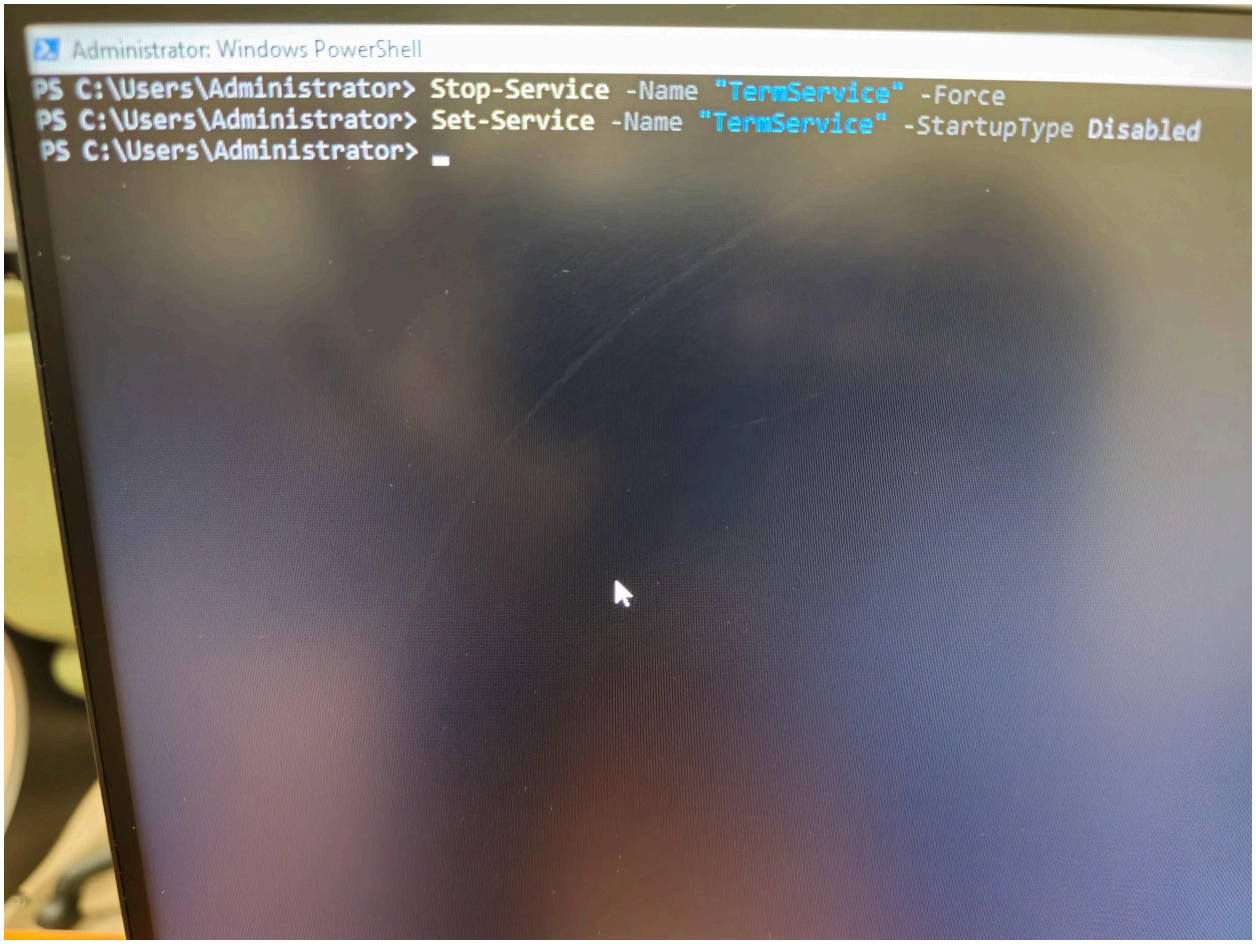
Firewall Configuration


Administrator: Windows PowerShell
+ CategoryInfo : InvalidArgument: (:) [New-NetFirewallRule], ParameterBindingException
+ FullyQualifiedErrorId : PositionalParameterNotFound,New-NetFirewallRule
PS C:\Users\Administrator> New-NetFireWallRule -DisplayName "Block FTP" -Protocol TCP -LocalPort 21 -Action Block
Name : {55f52ca6-4a92-4233-8908-41aaa388c688}
DisplayName : Block FTP
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Block
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
RemoteDynamicKeywordAddresses : {}
PS C:\Users\Administrator>



Disable Unused Services


Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-Service | Where-Object { $_.Status -eq "Running" }
Status Name DisplayName
Running ADWS Active Directory Web Services
Running AppHostSvc Application Host Helper Service
Running BFE Base Filtering Engine
Running BrokerInfrastru... Background Tasks Infrastructure Ser...
Running camsvc Capability Access Manager Service
Running cbdhsvc_82085 Clipboard User Service_82085
Running CDPSvc Connected Devices Platform Service
Running CDPUserSvc_82085 Connected Devices Platform User Ser...
Running CoreMessagingRe... CoreMessaging
Running CryptSvc Cryptographic Services
Running DcomLaunch DCOM Server Process Launcher
Running DFSR DFS Replication
Running Dhcp DHCP Client
Running DHCPServer DHCP Server
Running DiagTrack Connected User Experiences and Tele...
Running DispBrokerDeskt... Display Policy Service
Running DNS DNS Server
Running Dnscache DNS Client
Running DPS Diagnostic Policy Service
Running DsSvc Data Sharing Service
Running EventLog Windows Event Log
Running EventSystem COM+ Event System
Running FontCache Windows Font Cache Service
Running gpsvc Group Policy Client
Running hidserv Human Interface Device Service
Running HvHost HV Host Service
Running iphlpsvc IP Helper
Running IsmServ Intersite Messaging
Running Kdc Kerberos Key Distribution Center
Running KeyIso CNG Key Isolation
Running LanmanServer Server
Running LanmanWorkstation Workstation
Running LicenseManager Windows License Manager Service
Running lmhosts TCP/IP NetBIOS Helper
Running LSM Local Session Manager
Running mpssvc Windows Defender Firewall
Running MSDTC Distributed Transaction Coordinator
Running NcbService Network Connection Broker
Running Netlogon Netlogon
Running netprofm Network List Service
Running NlaSvc Network Location Awareness
Running nsi Network Store Interface Service
Running NTDS Active Directory Domain Services
Running PcaSvc Program Compatibility Assistant Ser...
Running PlugPlay Plug and Play
Running Power Power
Running ProfSvc User Profile Service
Running RpcEptMapper RPC Endpoint Mapper
Running RpcSs Remote Procedure Call (RPC)
Running SamSs Security Accounts Manager
Running Schedule Task Scheduler
Running SENS System Event Notification Service
Running ShellHWDetection Shell Hardware Detection
Running StateRepository State Repository Service
Running StorSvc Storage Service
Running SysMain SysMain
Running SystemEventsBroker System Events Broker
Running TabletInputService Touch Keyboard and Handwriting Pane...
Running Themes Themes
Type here to search



NMAP Summary

Open ports and outdated services are two fundamental vulnerabilities that an Nmap scan can reveal, each posing significant security risks if not properly managed. Open ports refer to network ports that are accessible and listening for incoming connections, potentially exposing services to external threats. Attackers can exploit unnecessary ports to gain unauthorized access or launch attacks if they remain open. For instance, an open **Telnet (port 23)** connection allows plaintext credential transmission, making it easy for attackers to intercept login details. In contrast, an open **RDP (port 3389)** can be targeted for brute-force attacks, ransomware infections, or unauthorized remote control. Similarly, outdated services pose a serious security risk because older software versions often contain well-documented vulnerabilities that attackers can easily exploit. Running outdated web servers like **Apache 2.4.49**, for example, exposes the system to path traversal exploits, which allow attackers to access restricted files on the server. Another critical example is **SMBv1**, an outdated file-sharing protocol that was exploited by the **EternalBlue** vulnerability, enabling the infamous **WannaCry ransomware attack** to spread globally. Both open ports and outdated services significantly increase an organization's attack surface, making it crucial to conduct regular network scans, close unnecessary ports, and keep software and services up to date to mitigate potential threats.