

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:**

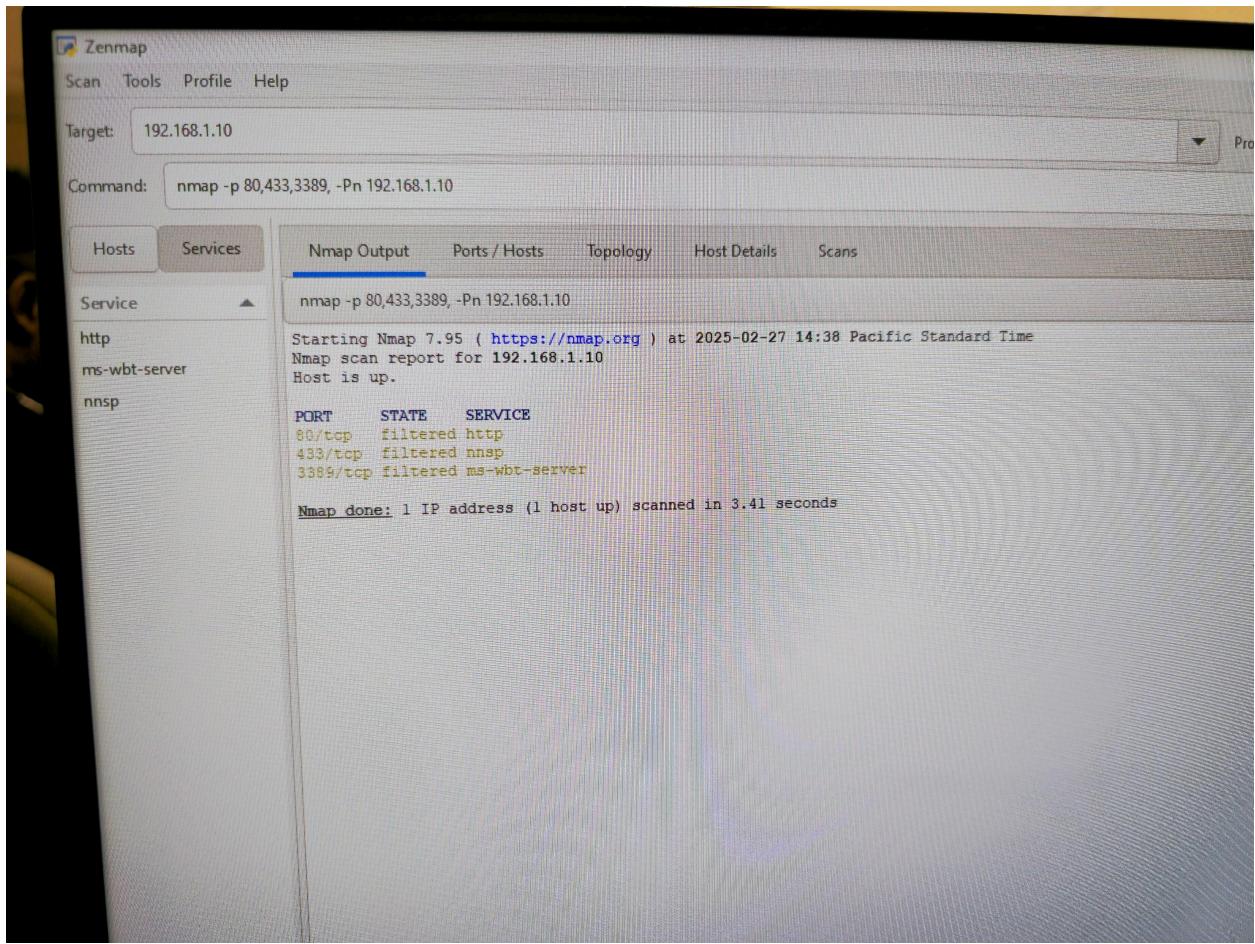
After verifying we successfully installed nmap on the pc, the next thing we do is run a simple scan on the virtual machine's IP address to identify open ports: nmap 192.168.1.10.

```
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



Zenmap interface showing the results of a port scan on host 192.168.1.10. The command used was nmap -p 80,433,3389, -Pn 192.168.1.10. The output shows the following services and their states:

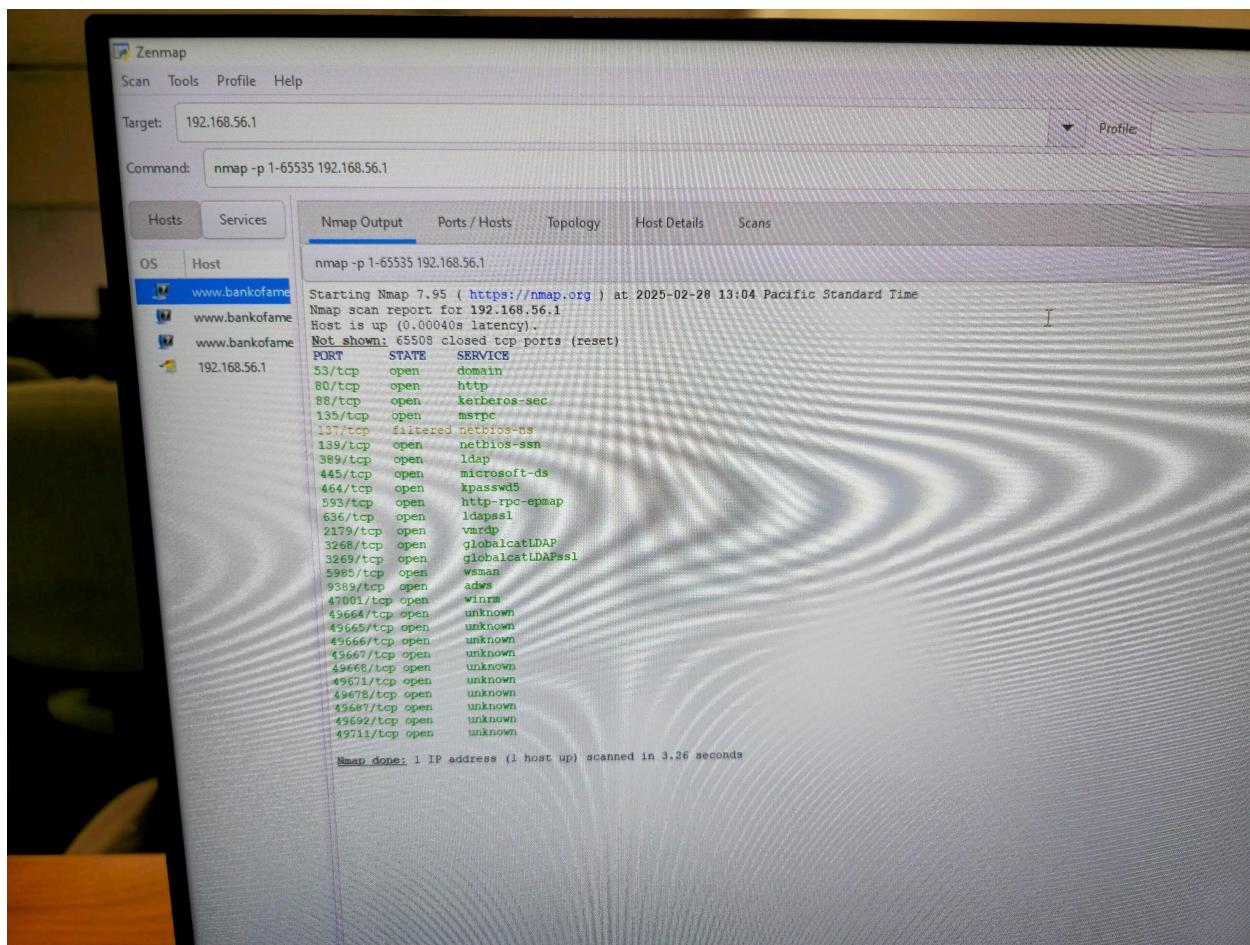
Service	Port	State	Protocol	Service
http	80/tcp	filtered	tcp	http
ms-wbt-server	433/tcp	filtered	tcp	nnsp
nnsp	3389/tcp	filtered	tcp	ms-wbt-server

The scan report indicates that the host is up and provides a summary of the completed scan.

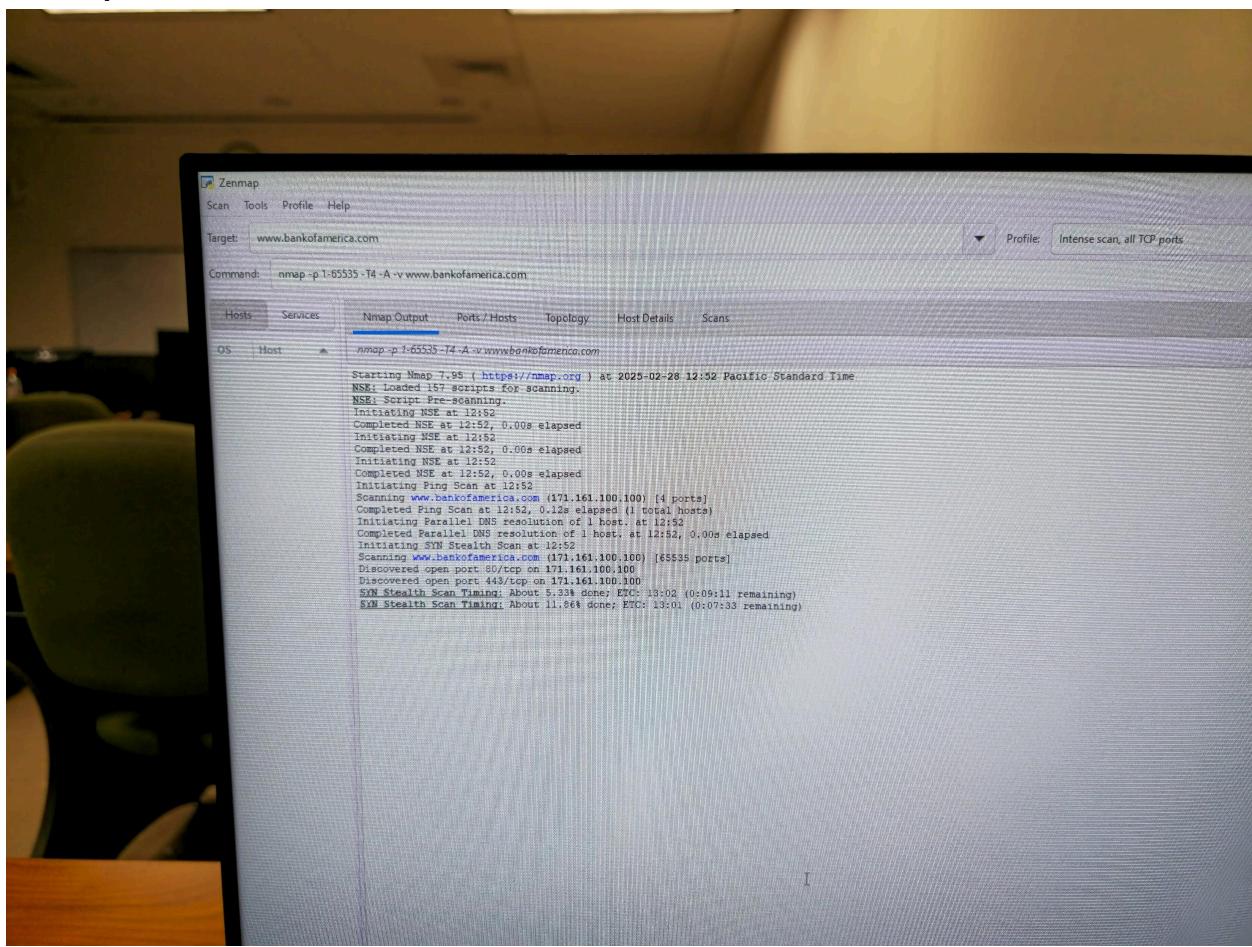
## Step 2: Scan for Vulnerabilities Using Nmap Scripting Engine (NSE)

**Scan for Common Vulnerabilities:**

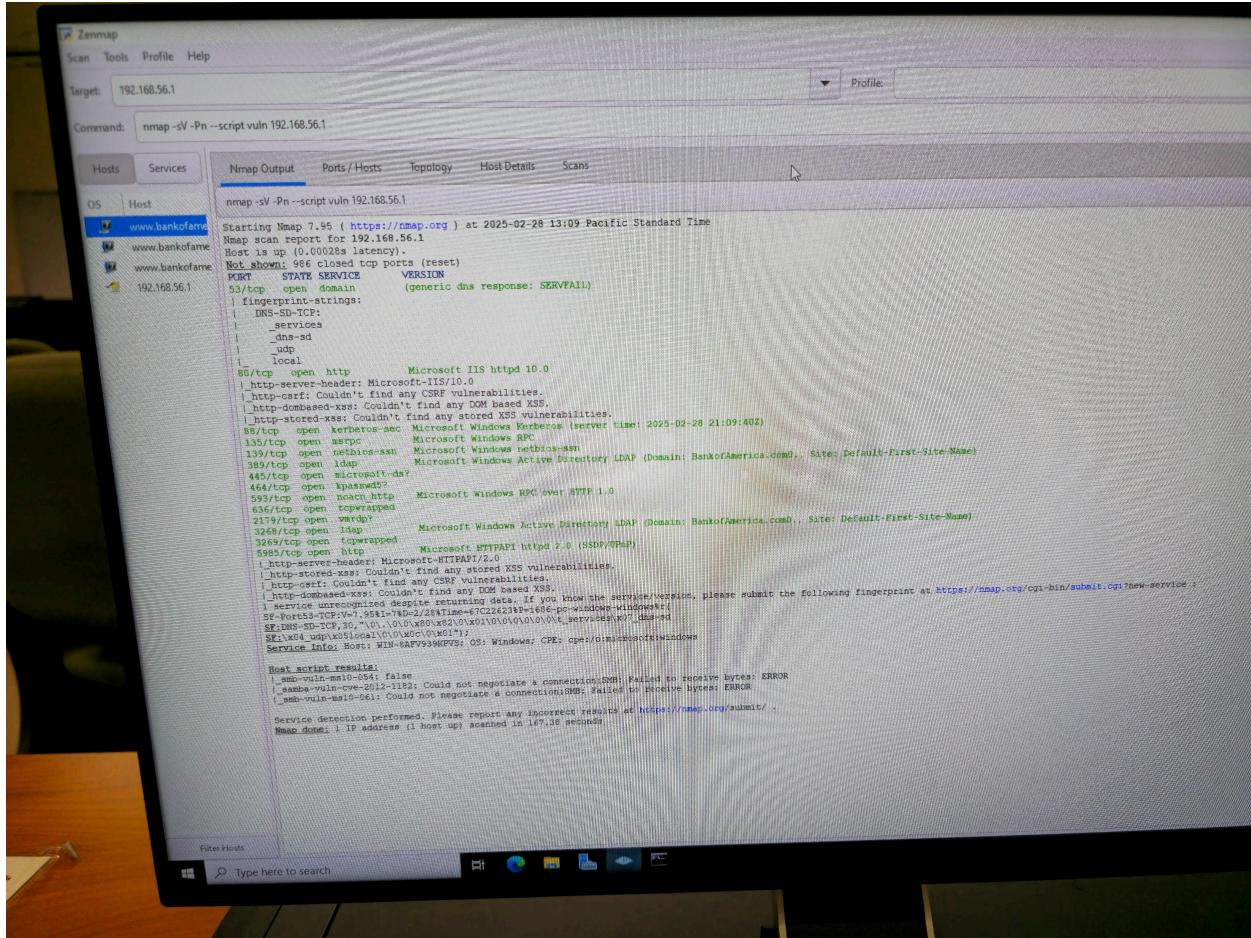
## Branden:



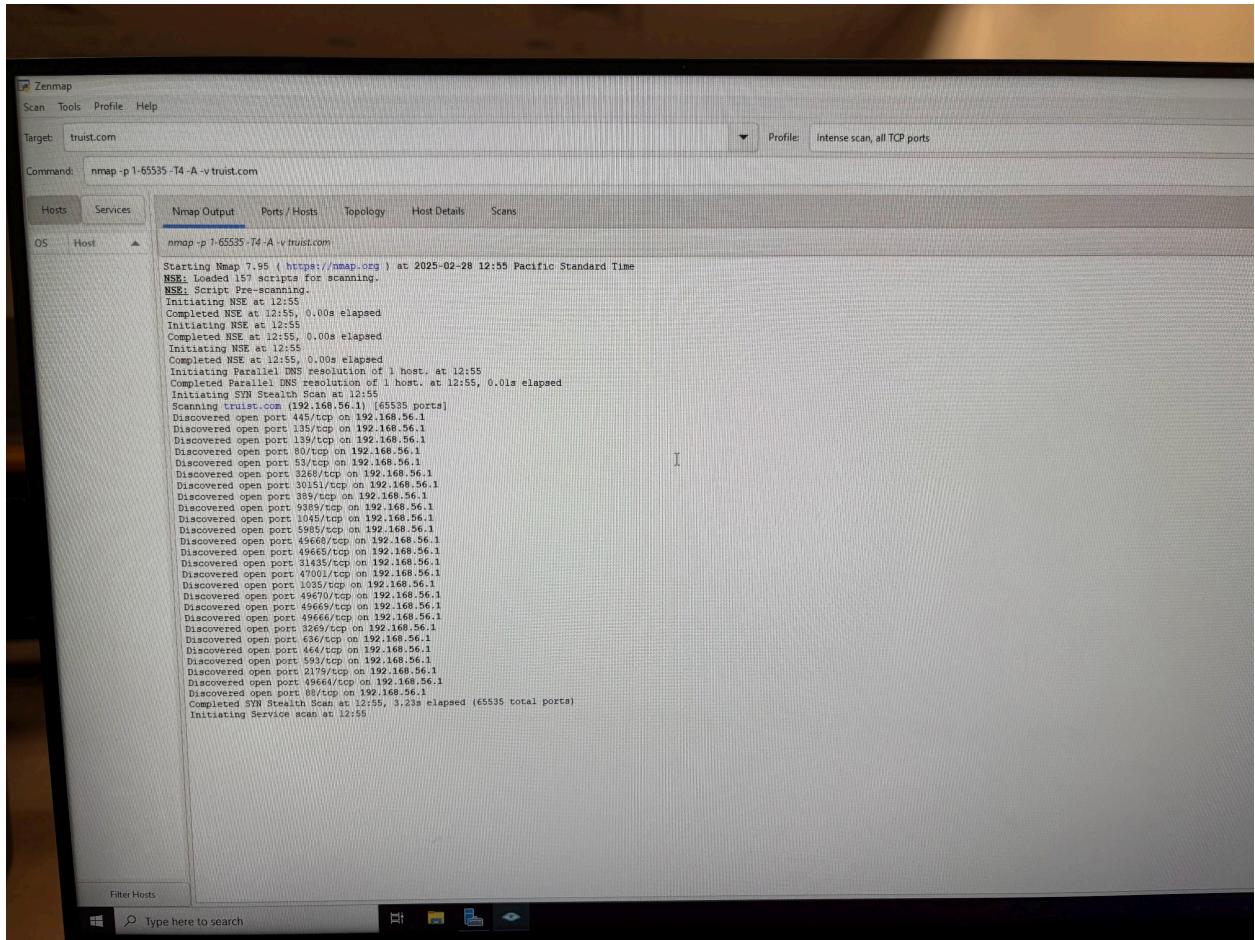
## Scan Open Ports



## Scan for Vulnerabilities and Services:



## **Malachi: Scan Open Ports:**



```

nmap -p 1-65535 -T4 -A -v truist.com

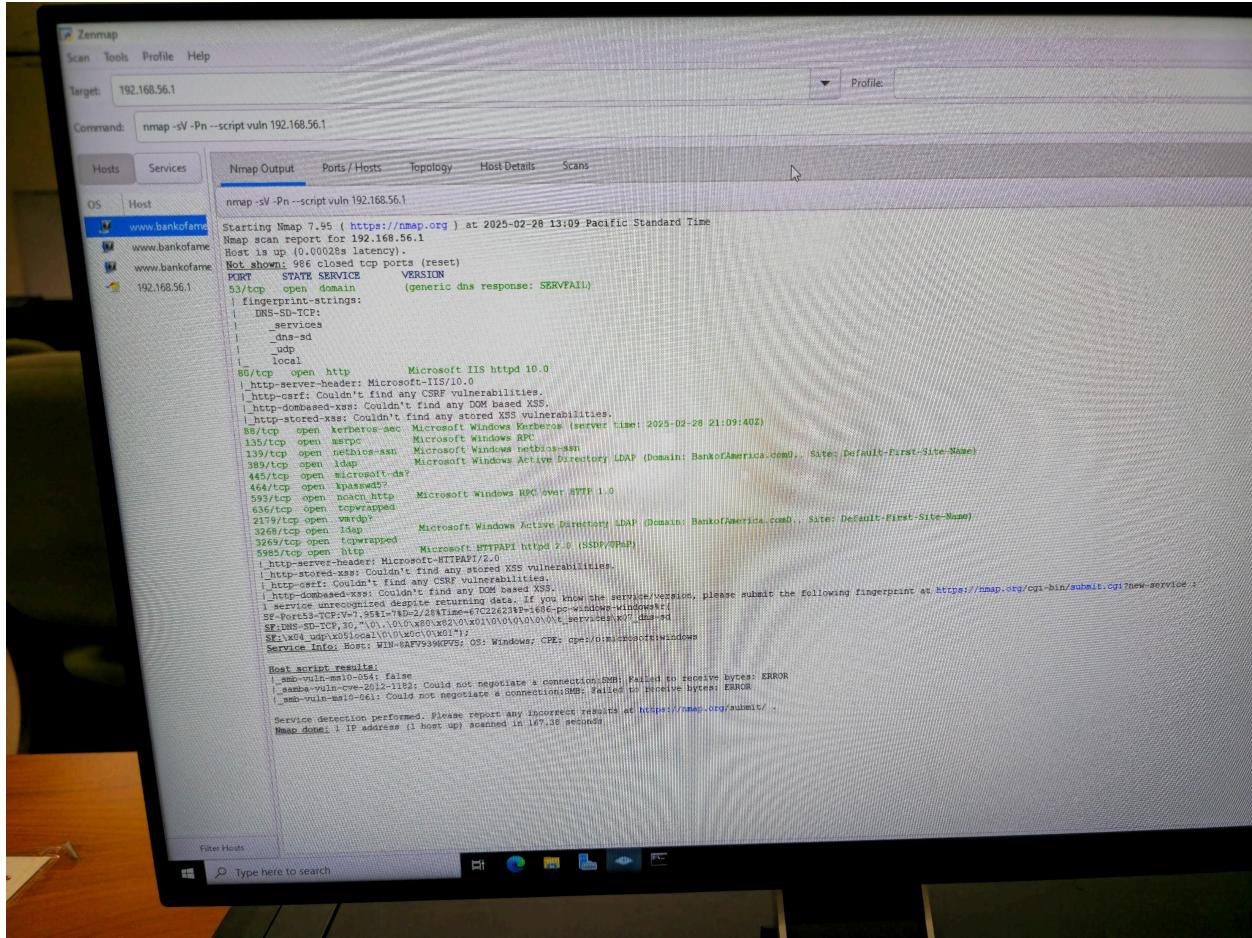
Services Nmap Output Ports / Hosts Topology Host Details Scans
.com (192.168.1.11) nmap -p 1-65535 -T4 -A -v truist.com

135/tcp open msrpc Microsoft Windows RPC
137/tcp filtered netbios-ns Microsoft Windows netbios-ssn
139/tcp open netbios-ssn Microsoft Windows Active Directory LDAP (Domain: TRUIST.COM., Site: Default-First-Site-Name)
389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: TRUIST.COM., Site: Default-First-Site-Name)
445/tcp open microsoft-ds?
464/tcp open kpasswd5?
4913/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped Microsoft Windows RPC
1038/tcp open msrpc Microsoft Windows RPC
1045/tcp open msrpc Microsoft Windows RPC
2179/tcp open vncrdp?
3260/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: TRUIST.COM., Site: Default-First-Site-Name)
3269/tcp open tcpwrapped Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp open nc-nmf .NET Message Framing
30151/tcp open msrpc Microsoft Windows RPC
31435/tcp open msrpc Microsoft Windows RPC
47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open msrpc Microsoft Windows RPC
49665/tcp open msrpc Microsoft Windows RPC
49666/tcp open msrpc Microsoft Windows RPC
49668/tcp open msrpc Microsoft Windows RPC
49669/tcp open msrpc Microsoft Windows RPC
49670/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
Device type: general purpose
Running: Microsoft Windows 2022
OS CPE: cpe:/o:microsoft:windows_server_2022
OS details: Windows Server 2022
Uptime guess: 0.009 days (since Fri Feb 28 12:44:19 2025)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: WIN-HIGVRGAUTUH; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-02-28T20:56:48
|   start date: N/A
|   smb2-security-mode:
|     3:1:1
|     Message signing enabled and required
NSE: Script Post-scanning.
Initiating NSE at 12:57
Completed NSE at 12:57, 0.00m elapsed
Initiating NSE at 12:57
Completed NSE at 12:57, 0.00s elapsed
Initiating NSE at 12:57
Completed NSE at 12:57, 0.00s elapsed
Read data files from: C:\Users\Administrator\Desktop\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.61 seconds
Raw packets sent: 65568 (2.886MB) | Rcvd: 131185 (5.513MB)

```

## 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:

The screenshot shows the Zenmap interface with the following details:

- Scan Menu:** Scan, Tools, Profile, Help
- Target:** 192.168.56.1
- Command:** nmap -O 192.168.56.1
- Hosts:** OS Host
- Services:** www.bankofame, www.bankofame, www.bankofame, 192.168.56.1
- Selected Tab:** Nmap Output
- Content:**

```
nmap -O 192.168.56.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-28 13:00 Pacific Standard Time
Nmap scan report for 192.168.56.1
Host is up (0.00026s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
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  vncrdp
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
Device type: general purpose
Running: Microsoft Windows 2022
OS CPE: cpe:/o:microsoft:windows_server_2022
OS details: Windows Server 2022
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
```

## Malachi:

```

zenmap
File Tools Profile Help
Target: 192.168.56.1
Command: nmap -sV -p - -O 192.168.56.1
Profile: 

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
DS Host truist.com (192.168.56.1)

nmap -sV -p - -O 192.168.56.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-28 13:21 Pacific Standard Time
Nmap scan report for 192.168.56.1
Host is up (0.00082s latency).
Not shown: 65508 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
53/tcp    open     domain      Simple DNS Plus
80/tcp    open     http        Microsoft IIS httpd 10.0
88/tcp    open     kerberos-sec Microsoft Windows Kerberos (server time: 2025-02-28 21:22:08Z)
135/tcp   open     msrpc      Microsoft Windows RPC
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open     ldap        Microsoft Windows Active Directory LDAP (Domain: TRUIST.com0., Site: Default-First-Site-Name)
445/tcp   open     microsoft-ds?
464/tcp   open     kpasswd5?
593/tcp   open     ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp   open     tcpwrapped
1035/tcp  open     msrpc      Microsoft Windows RPC
1045/tcp  open     msrpc      Microsoft Windows RPC
2179/tcp  open     vrdp?
3268/tcp  open     ldap        Microsoft Windows Active Directory LDAP (Domain: TRUIST.com0., Site: Default-First-Site-Name)
3269/tcp  open     tcpwrapped
5985/tcp  open     http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open     mc-nmf    .NET Message Framing
30151/tcp open     msrpc      Microsoft Windows RPC
31435/tcp open     msrpc      Microsoft Windows RPC
47001/tcp open     http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open     msrpc      Microsoft Windows RPC
49665/tcp open     msrpc      Microsoft Windows RPC
49666/tcp open     msrpc      Microsoft Windows RPC
49668/tcp open     msrpc      Microsoft Windows RPC
49669/tcp open     msrpc      Microsoft Windows RPC
49670/tcp open     ncacn_http Microsoft Windows RPC over HTTP 1.0
Device type: general purpose
Running: Microsoft Windows 2022
OS CPE: cpe:/o:microsoft:windows_server_2022
OS details: Windows Server 2022
Network Distance: 0 hops
Service Info: Host: WIN-HIGVR6AVTUH; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.52 seconds

```

## Step 4: Patch & Secure the Server

### Apply Windows Updates

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or 'C:\Users\Administrator\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
PS C:\Users\Administrator> Import-Module PSWindowsUpdate
PS C:\Users\Administrator> Get-WindowsUpdate
PS C:\Users\Administrator> Install-WindowsUpdate -AcceptAll -ignoreReboot
PS C:\Users\Administrator>
```

## Firewall Configuration

```
+ 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>
```

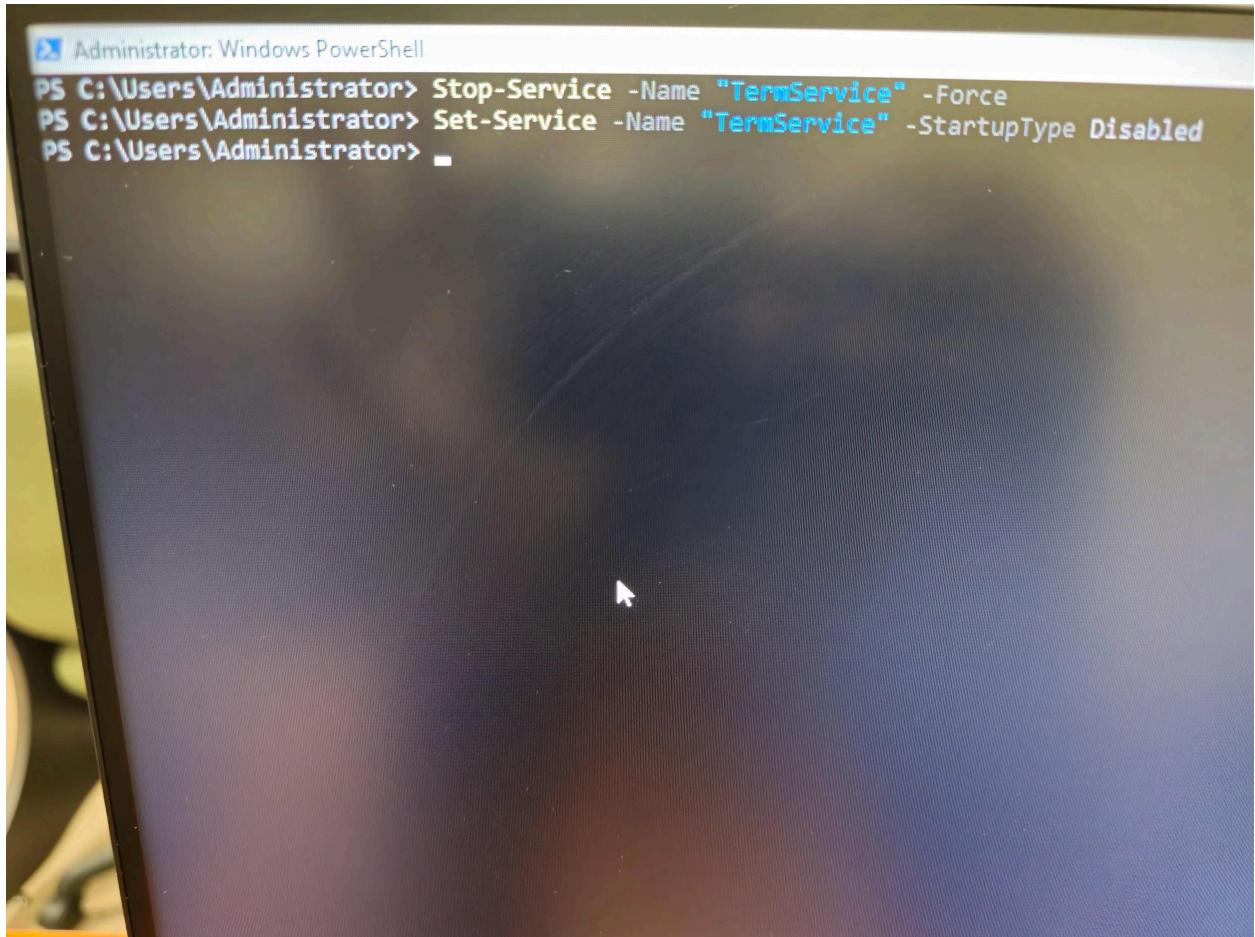
```
Administrator: Windows PowerShell
PS C:\Users\Administrator> New-NetFirewallRule -DisplayName "Block unused Ports" -Direction Inbound -LocalPort 21,23,3389 -Protocol TCP -Action Block

Name          : {45f8a3c9-4d5b-4bb5-88a9-1551b31f10c5}
DisplayName   : Block unused Ports
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   BrokerInfrast... Background Tasks Infrastructure Ser...
Running   camsvc         Capability Access Manager Service
Running   cbdhsvc_82085 Clipboard User Service_82085
Running   CDPSvc         Connected Devices PlatForm Service
Running   CDPUUserSv...  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   iiphisvc      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   lmmos          TCP/IP NetBIOS Helper
Running   Lsm            Local Security Manager
Running   msrssvc        Windows Defender Firewall
Running   NSDTC          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   pcdSvc         Program Compatibility Assistant Ser...
Running   PlugPlay       Plug and Play
Running   Power          Power
Running   ProfSvc        User Profile Service
Running   RpcCpthMapper  RPC Endpoint Mapper
Running   RpcCs          Remote Procedure Call (RPC)
Running   Sans           Security Accounts Manager
Running   Schedule       Task Scheduler
Running   SCHS           System Event Notification Service
Running   ShellHDetection Shell Hardware Detection
Running   StateRepository State Repository Service
Running   StorSvc         Storage Service
Running   SysMain         System Main
Running   SystemEventsBroker System Events Broker
Running   TabletinPutService Touch Keyboard and Handwriting Pane...
Running   Themes          Themes
```



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Stop-Service -Name "TermService" -Force
PS C:\Users\Administrator> Set-Service -Name "TermService" -StartupType Disabled
PS C:\Users\Administrator>
```

## 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.

