

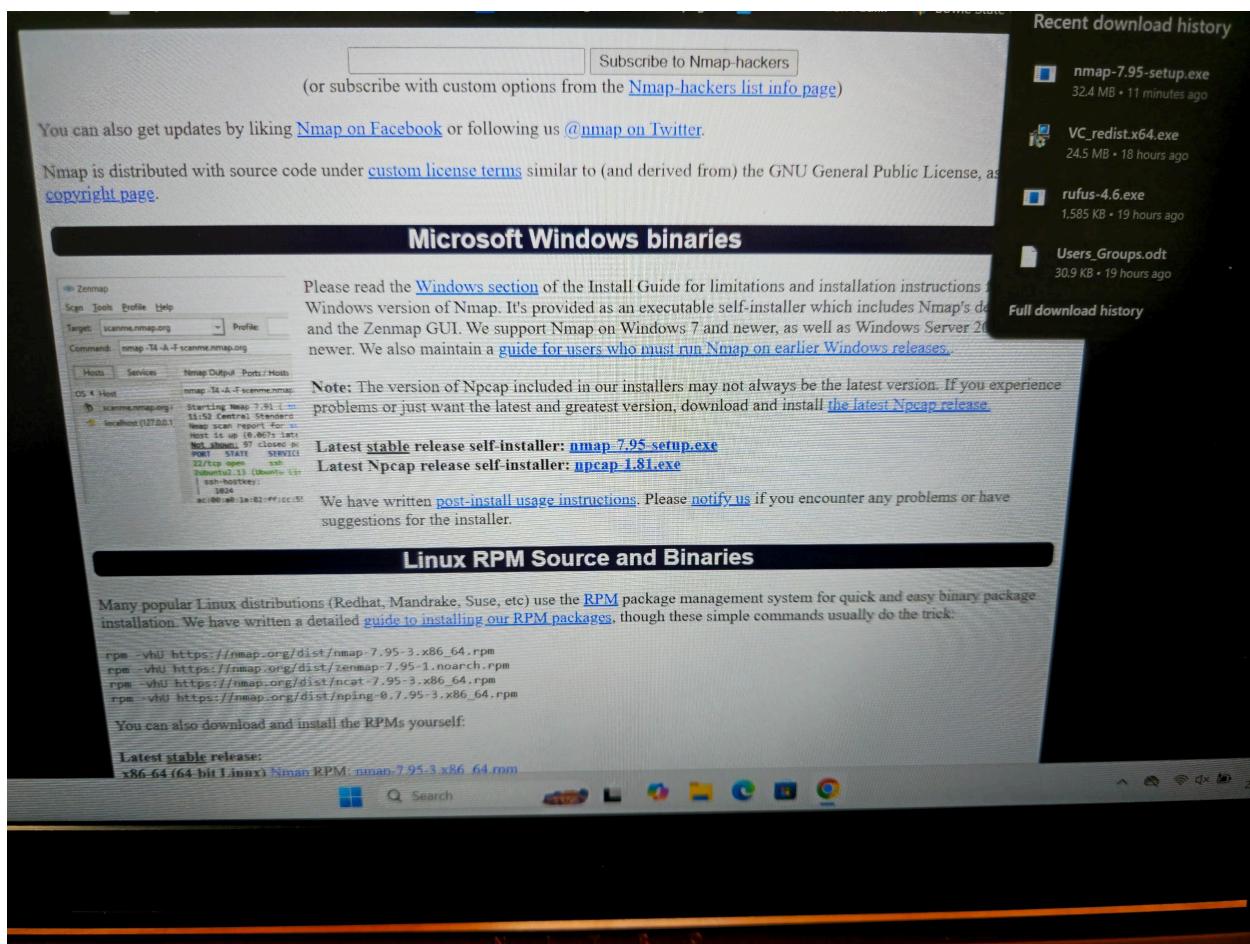
Branden, Malachi
Doctor Latson
2/27/25
CTEC 402

Vulnerabilities and Service Configuration Documentation

Step 1: Install Nmap on Windows Server 2022

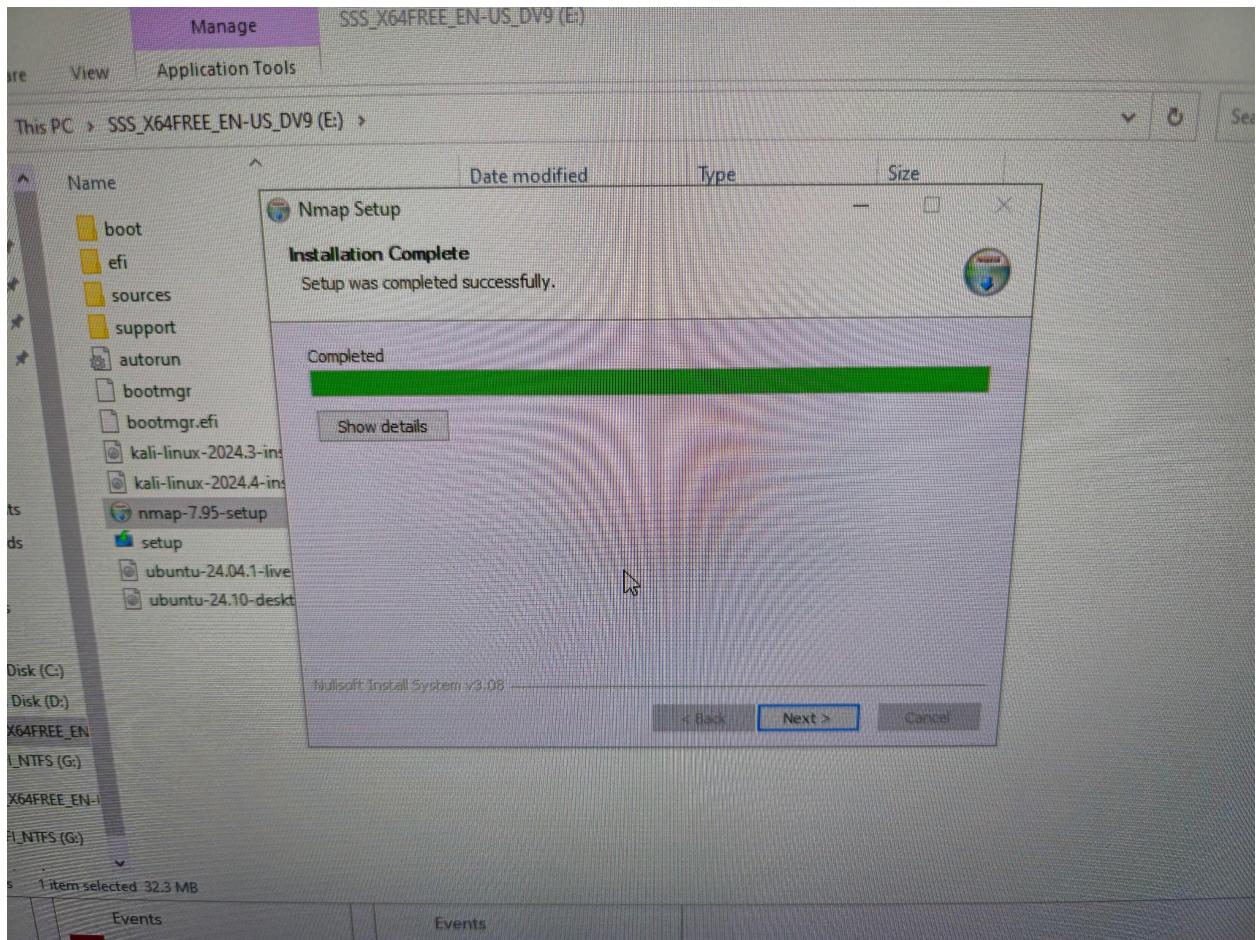
Download Nmap:

The first thing our team did was visit the official Nmap download page:
<https://nmap.org/download.html>. We download the Windows version of Nmap, which comes as an installer (**nmap-<version>-setup.exe**).



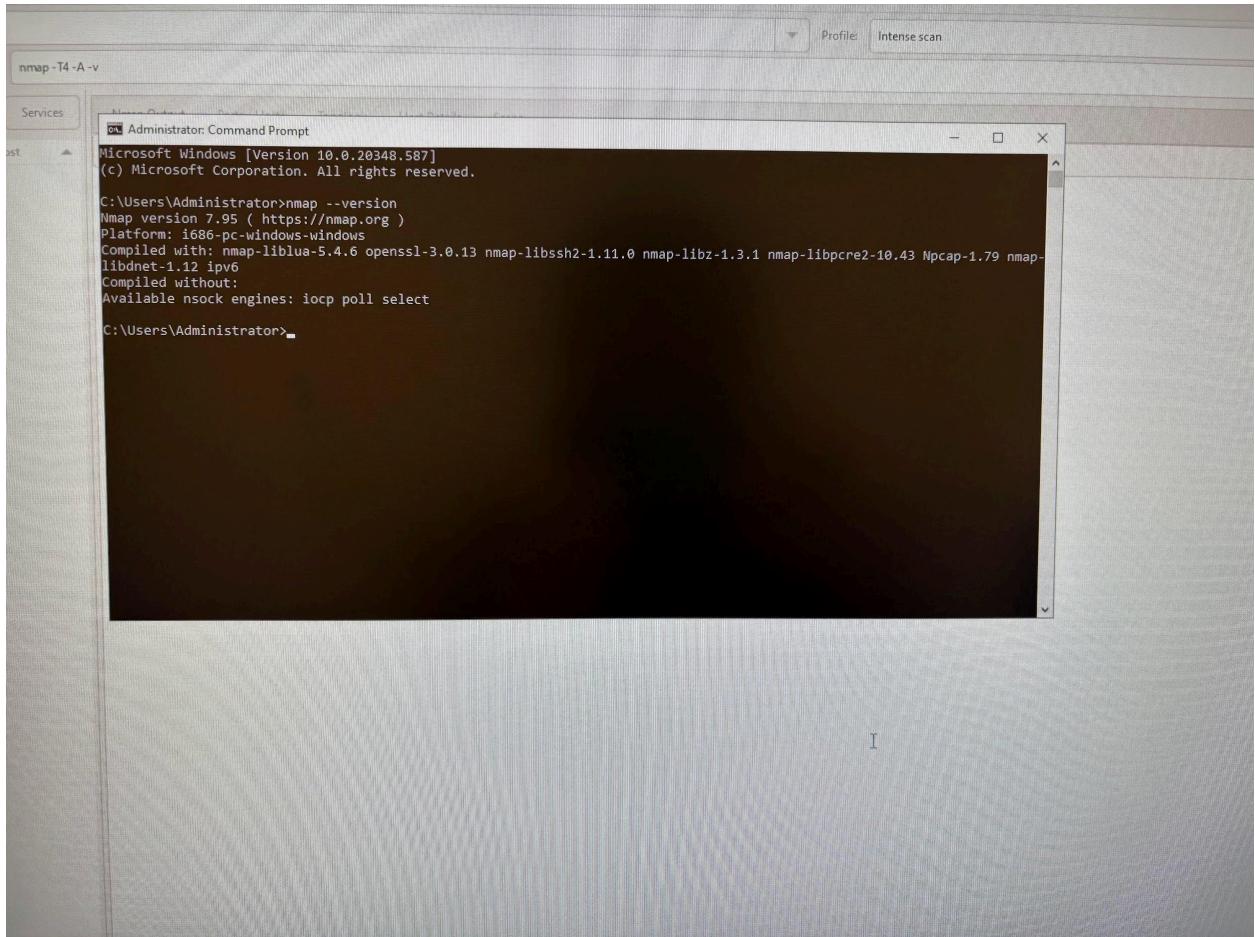
Run the Installer:

We double-click the downloaded .exe file to begin the installation. We follow the installation wizard: Accept the default settings unless you need a specific configuration. Ensure that the **Nmap executable** is added to your system's **PATH** so that you can use it from the command line.



Verify Installation:

We went to the command prompt to verify we successfully installed the nmap setup but typing (nmap –version).



Step 2: 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.

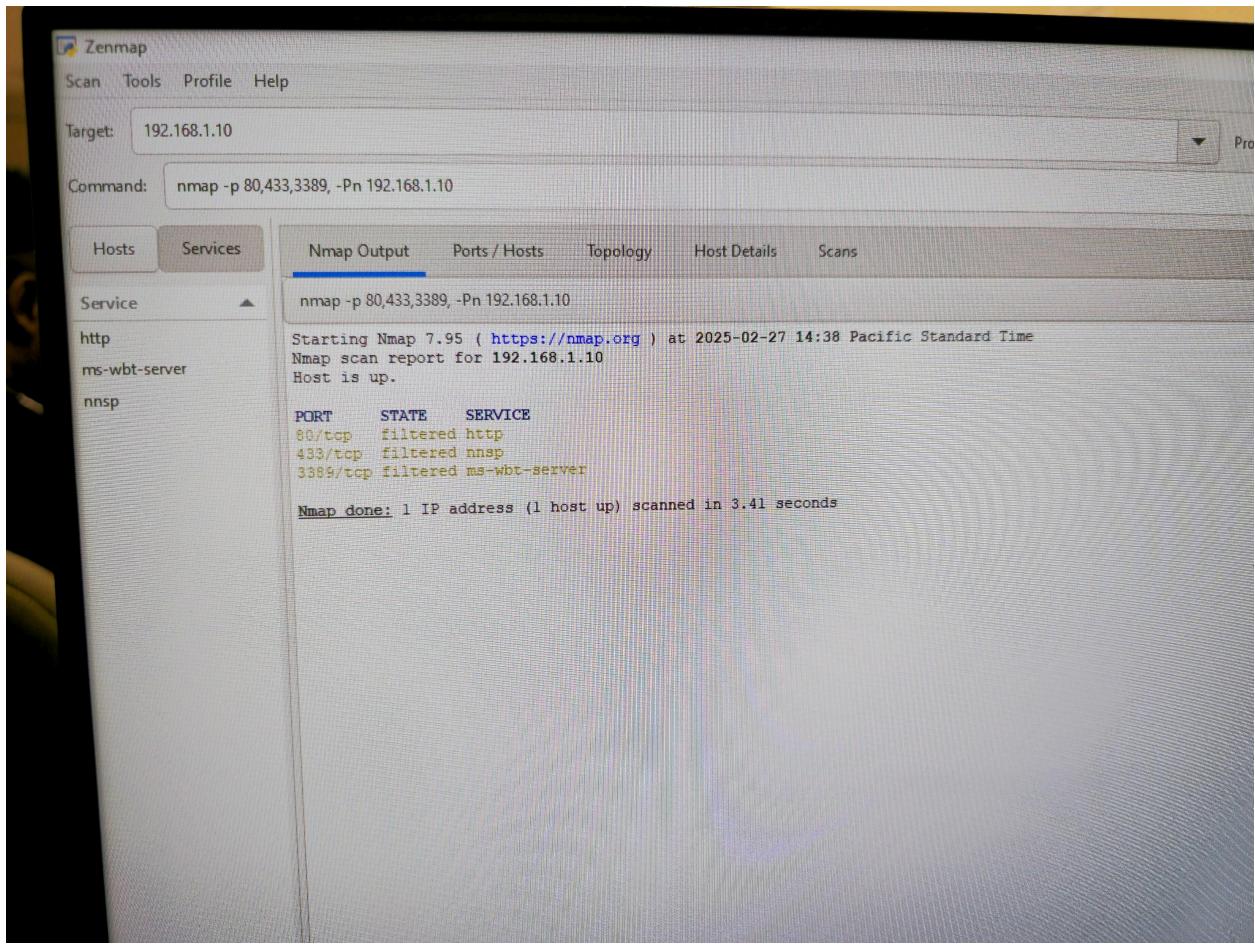
```
clear is not recognized as an internal or external command,  
operable program or batch file.
```

```
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:

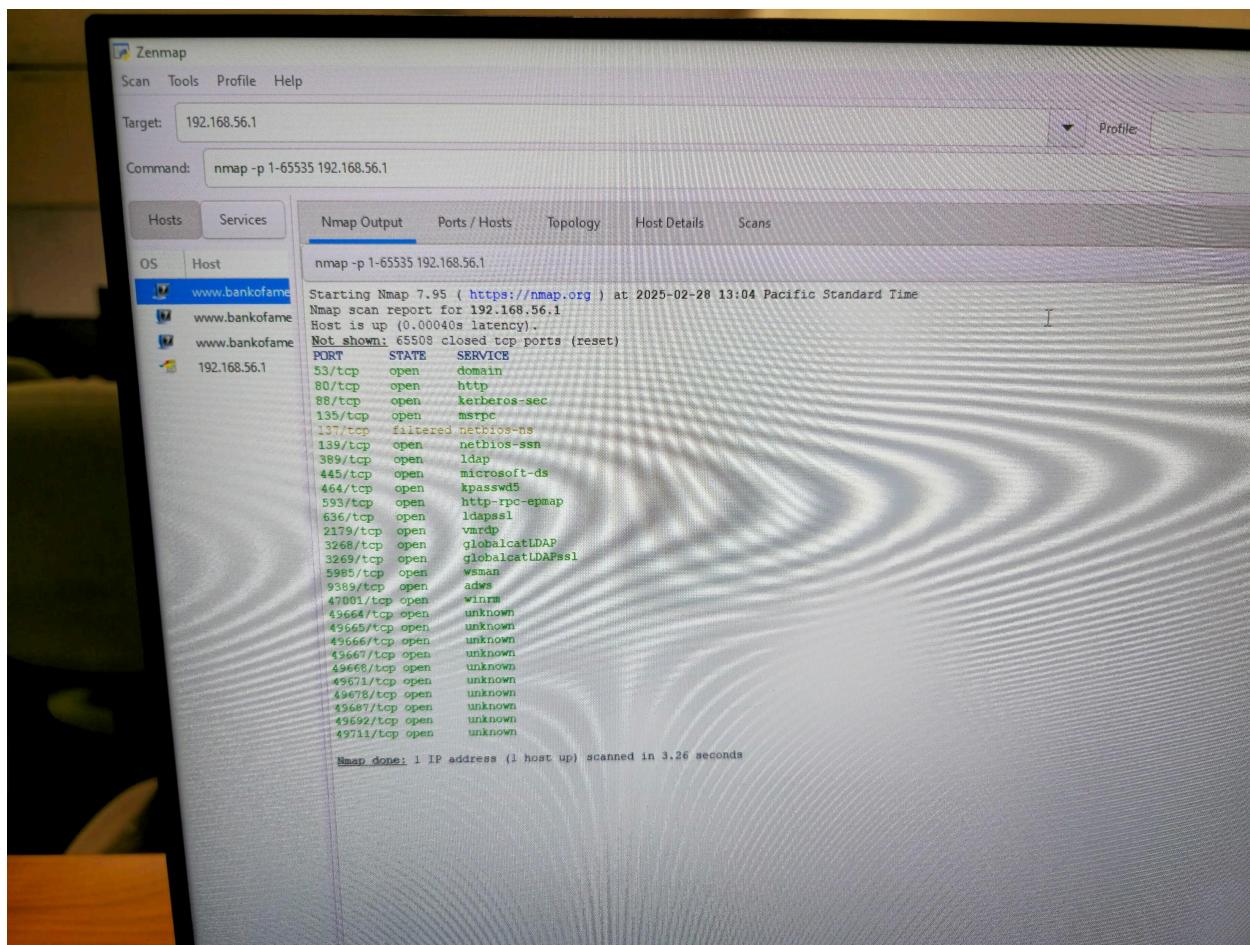
Service	Port	State	Protocol	Service
http	80/tcp	filtered	tcp	http
ms-wbt-server	433/tcp	filtered	tcp	nnsp
nnsp	3389/tcp	filtered	tcp	ms-wbt-server

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

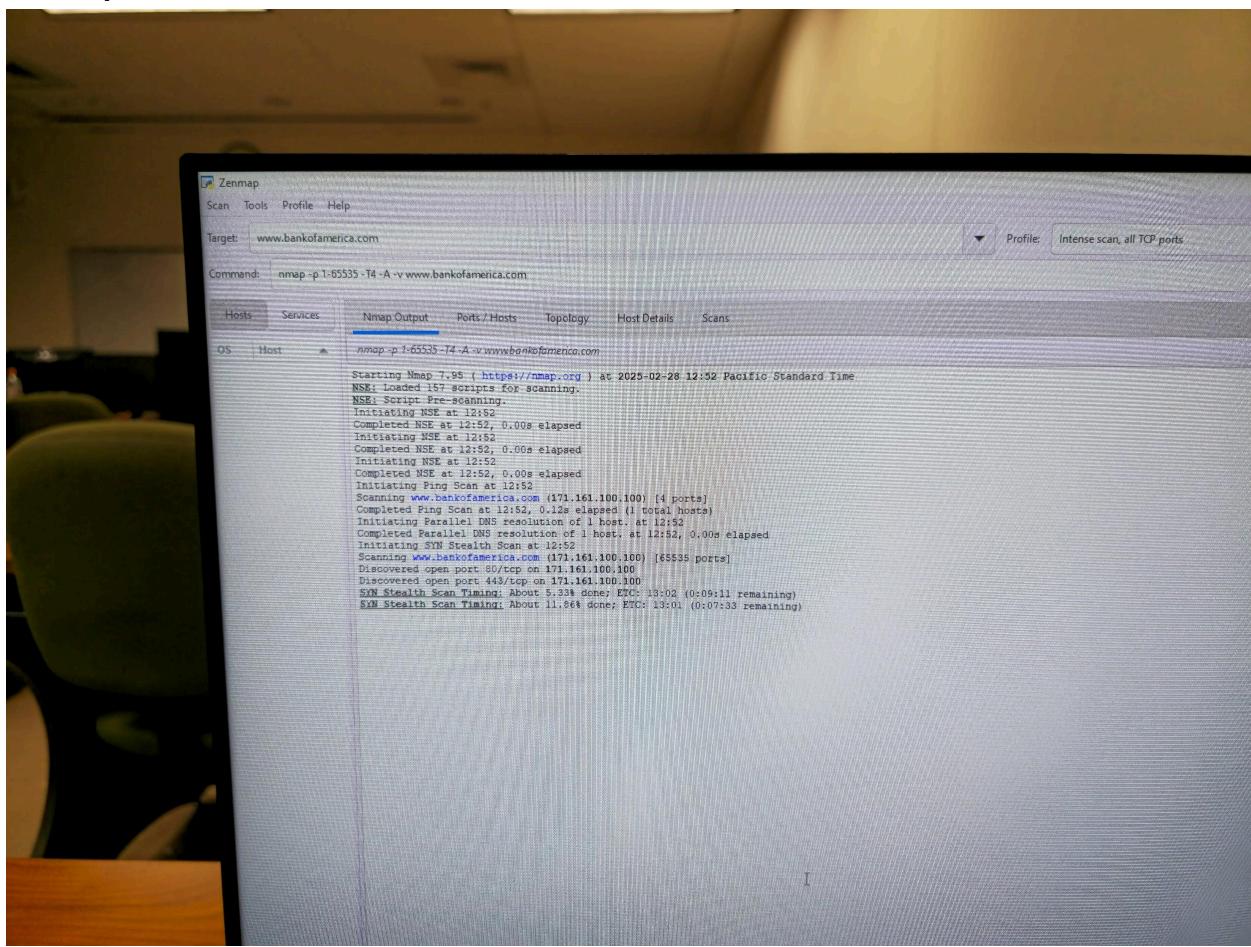
Step 3: Scan for Vulnerabilities Using Nmap Scripting Engine (NSE)

Scan for Common Vulnerabilities:

Branden:



Scan Open Ports



The screenshot shows the Zenmap interface with the following details:

- Target:** www.bankofamerica.com
- Command:** nmap -p 1-65535 -T4 -A -v www.bankofamerica.com
- Profile:** Intense scan, all TCP ports
- Hosts:** OS Host
- Nmap Output:** The output window displays the Nmap command and its progress:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-28 12:52 Pacific Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:52
Completed NSE at 12:52, 0.00s elapsed
Initiating NSE at 12:52
Completed NSE at 12:52, 0.00s elapsed
Initiating NSE at 12:52
Completed NSE at 12:52, 0.00s elapsed
Initiating NSE at 12:52
Completed NSE at 12:52, 0.00s elapsed
Initiating Ping Scan at 12:52
Scanning www.bankofamerica.com (171.161.100.100) (4 ports)
Completed Ping Scan at 12:52, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 12:52
Completed Parallel DNS resolution of 1 host at 12:52, 0.00s elapsed
Initiating SYN Stealth Scan at 12:52
Scanning www.bankofamerica.com (171.161.100.100) [65535 ports]
Discovered open port 80/tcp on 171.161.100.100
Discovered open port 443/tcp on 171.161.100.100
SYN Stealth Scan Timing: About 5.33% done; ETC: 13:02 (0:09:11 remaining)
SYN Stealth Scan Timing: About 11.86% done, ETC: 13:01 (0:07:33 remaining)
```

Scan for Vulnerabilities and Services:

Zenmap

Scan Tools Profile Help

Target: 192.168.56.1

Command: nmap -sV -Pn --script vuln 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 -sV -Pn --script vuln 192.168.56.1

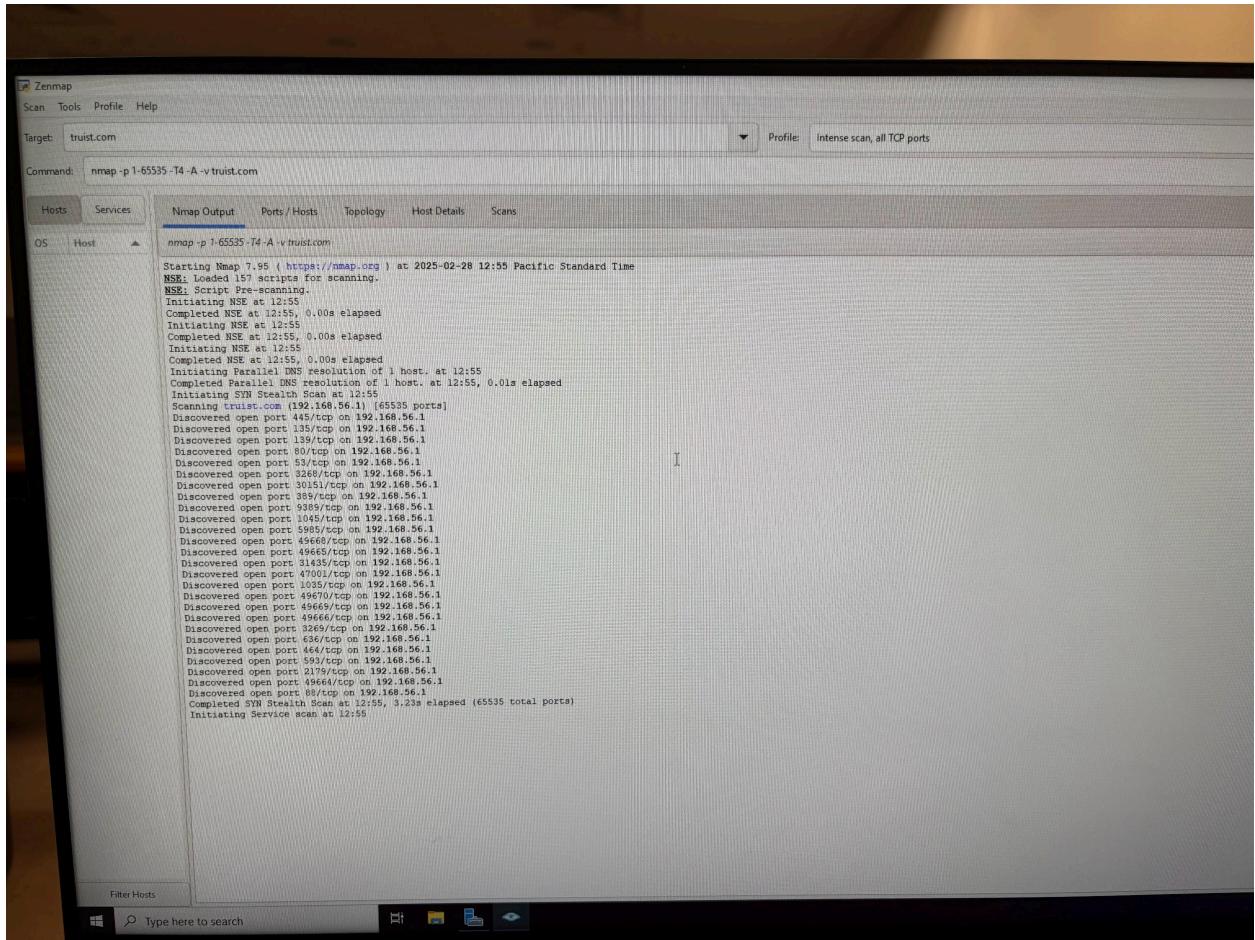
Starting Nmap 7.95 (https://nmap.org) at 2025-02-28 13:09 Pacific Standard Time

Nmap scan report for 192.168.56.1

Host is up (0.00028s latency).

Not shown: 996 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	(generic dns response: SERVFAIL)
80/tcp	open	http	Microsoft IIS httpd 10.0
139/tcp	open	netbios-ssn	Microsoft Windows NetBIOS Service (server time: 2025-02-28 21:09:40Z)
389/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: BankofAmerica.com, Site: Default-First-Site-Name)
445/tcp	open	microsoft-ds?	
464/tcp	open	kpasswd?	
593/tcp	open	http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
2179/tcp	open	vardp	
3269/tcp	open	ldaps	Microsoft Windows Active Directory LDAP (Domain: BankofAmerica.com, Site: Default-First-Site-Name)
3269/tcp	open	tcpwrapped	
3270/tcp	open	http	Microsoft HTTPAPI httpd 7.0 (SSDPI/HPAPI)
443/tcp	open	https	Microsoft IISHTTPAPI/1.2.0
4443/tcp	open	https	Microsoft IISHTTPAPI/1.2.0
587/tcp	open	smtp	
635/tcp	open	tcpwrapped	
873/tcp	open	ssh	
1354/tcp	open	msrpc	
1394/tcp	open	msrpc	
1434/tcp	open	msrpc	
1435/tcp	open	msrpc	
1436/tcp	open	msrpc	
1437/tcp	open	msrpc	
1438/tcp	open	msrpc	
1439/tcp	open	msrpc	
1441/tcp	open	msrpc	
1442/tcp	open	msrpc	
1443/tcp	open	msrpc	
1444/tcp	open	msrpc	
1445/tcp	open	msrpc	
1446/tcp	open	msrpc	
1447/tcp	open	msrpc	
1448/tcp	open	msrpc	
1449/tcp	open	msrpc	
1450/tcp	open	msrpc	
1451/tcp	open	msrpc	
1452/tcp	open	msrpc	
1453/tcp	open	msrpc	
1454/tcp	open	msrpc	
1455/tcp	open	msrpc	
1456/tcp	open	msrpc	
1457/tcp	open	msrpc	
1458/tcp	open	msrpc	
1459/tcp	open	msrpc	
1460/tcp	open	msrpc	
1461/tcp	open	msrpc	
1462/tcp	open	msrpc	
1463/tcp	open	msrpc	
1464/tcp	open	msrpc	
1465/tcp	open	msrpc	
1466/tcp	open	msrpc	
1467/tcp	open	msrpc	
1468/tcp	open	msrpc	
1469/tcp	open	msrpc	
1470/tcp	open	msrpc	
1471/tcp	open	msrpc	
1472/tcp	open	msrpc	
1473/tcp	open	msrpc	
1474/tcp	open	msrpc	
1475/tcp	open	msrpc	
1476/tcp	open	msrpc	
1477/tcp	open	msrpc	
1478/tcp	open	msrpc	
1479/tcp	open	msrpc	
1480/tcp	open	msrpc	
1481/tcp	open	msrpc	
1482/tcp	open	msrpc	
1483/tcp	open	msrpc	
1484/tcp	open	msrpc	
1485/tcp	open	msrpc	
1486/tcp	open	msrpc	
1487/tcp	open	msrpc	
1488/tcp	open	msrpc	
1489/tcp	open	msrpc	
1490/tcp	open	msrpc	
1491/tcp	open	msrpc	
1492/tcp	open	msrpc	
1493/tcp	open	msrpc	
1494/tcp	open	msrpc	
1495/tcp	open	msrpc	
1496/tcp	open	msrpc	
1497/tcp	open	msrpc	
1498/tcp	open	msrpc	
1499/tcp	open	msrpc	
1500/tcp	open	msrpc	
1501/tcp	open	msrpc	
1502/tcp	open	msrpc	
1503/tcp	open	msrpc	
1504/tcp	open	msrpc	
1505/tcp	open	msrpc	
1506/tcp	open	msrpc	
1507/tcp	open	msrpc	
1508/tcp	open	msrpc	
1509/tcp	open	msrpc	
1510/tcp	open	msrpc	
1511/tcp	open	msrpc	
1512/tcp	open	msrpc	
1513/tcp	open	msrpc	
1514/tcp	open	msrpc	
1515/tcp	open	msrpc	
1516/tcp	open	msrpc	
1517/tcp	open	msrpc	
1518/tcp	open	msrpc	
1519/tcp	open	msrpc	
1520/tcp	open	msrpc	
1521/tcp	open	msrpc	
1522/tcp	open	msrpc	
1523/tcp	open	msrpc	
1524/tcp	open	msrpc	
1525/tcp	open	msrpc	
1526/tcp	open	msrpc	
1527/tcp	open	msrpc	
1528/tcp	open	msrpc	
1529/tcp	open	msrpc	
1530/tcp	open	msrpc	
1531/tcp	open	msrpc	
1532/tcp	open	msrpc	
1533/tcp	open	msrpc	
1534/tcp	open	msrpc	
1535/tcp	open	msrpc	
1536/tcp	open	msrpc	
1537/tcp	open	msrpc	
1538/tcp	open	msrpc	
1539/tcp	open	msrpc	
1540/tcp	open	msrpc	
1541/tcp	open	msrpc	
1542/tcp	open	msrpc	
1543/tcp	open	msrpc	
1544/tcp	open	msrpc	
1545/tcp	open	msrpc	
1546/tcp	open	msrpc	
1547/tcp	open	msrpc	
1548/tcp	open	msrpc	
1549/tcp	open	msrpc	
1550/tcp	open	msrpc	
1551/tcp	open	msrpc	
1552/tcp	open	msrpc	
1553/tcp	open	msrpc	
1554/tcp	open	msrpc	
1555/tcp	open	msrpc	
1556/tcp	open	msrpc	
1557/tcp	open	msrpc	
1558/tcp	open	msrpc	
1559/tcp	open	msrpc	
1560/tcp	open	msrpc	
1561/tcp	open	msrpc	
1562/tcp	open	msrpc	
1563/tcp	open	msrpc	
1564/tcp	open	msrpc	
1565/tcp	open	msrpc	
1566/tcp	open	msrpc	
1567/tcp	open	msrpc	
1568/tcp	open	msrpc	
1569/tcp	open	msrpc	
1570/tcp	open	msrpc	
1571/tcp	open	msrpc	
1572/tcp	open	msrpc	
1573/tcp	open	msrpc	
1574/tcp	open	msrpc	
1575/tcp	open	msrpc	
1576/tcp	open	msrpc	
1577/tcp	open	msrpc	
1578/tcp	open	msrpc	
1579/tcp	open	msrpc	
1580/tcp	open	msrpc	
1581/tcp	open	msrpc	
1582/tcp	open	msrpc	
1583/tcp	open	msrpc	
1584/tcp	open	msrpc	
1585/tcp	open	msrpc	
1586/tcp	open	msrpc	
1587/tcp	open	msrpc	
1588/tcp	open	msrpc	
1589/tcp	open	msrpc	
1590/tcp	open	msrpc	
1591/tcp	open	msrpc	
1592/tcp	open	msrpc	
1593/tcp	open	msrpc	
1594/tcp	open	msrpc	
1595/tcp	open	msrpc	
1596/tcp	open	msrpc	
1597/tcp	open	msrpc	
1598/tcp	open	msrpc	
1599/tcp	open	msrpc	
1600/tcp	open	msrpc	
1601/tcp	open	msrpc	
1602/tcp	open	msrpc	
1603/tcp	open	msrpc	
1604/tcp	open	msrpc	
1605/tcp	open	msrpc	
1606/tcp	open	msrpc	
1607/tcp	open	msrpc	
1608/tcp	open	msrpc	
1609/tcp	open	msrpc	
1610/tcp	open	msrpc	
1611/tcp	open	msrpc	
1612/tcp	open	msrpc	
1613/tcp	open	msrpc	
1614/tcp	open	msrpc	
1615/tcp	open	msrpc	
1616/tcp	open	msrpc	
1617/tcp	open	msrpc	
1618/tcp	open	msrpc	
1619/tcp	open	msrpc	
1620/tcp	open	msrpc	
1621/tcp	open	msrpc	
1622/tcp	open	msrpc	
1623/tcp	open	msrpc	
1624/tcp	open	msrpc	
1625/tcp	open	msrpc	
1626/tcp	open	msrpc	
1627/tcp	open	msrpc	
1628/tcp	open	msrpc	
1629/tcp	open	msrpc	
1630/tcp	open	msrpc	
1631/tcp	open	msrpc	
1632/tcp	open	msrpc	
1633/tcp	open	msrpc	
1634/tcp	open	msrpc	
1635/tcp	open	msrpc	
1636/tcp	open	msrpc	
1637/tcp	open	msrpc	
1638/tcp	open	msrpc	
1639/tcp	open	msrpc	
1640/tcp	open	msrpc	
1641/tcp	open	msrpc	
1642/tcp	open	msrpc	
1643/tcp	open	msrpc	
1644/tcp	open	msrpc	
1645/tcp	open	msrpc	
1646/tcp	open	msrpc	
1647/tcp	open	msrpc	
1648/tcp	open	msrpc	
1649/tcp	open	msrpc	
1650/tcp	open	msrpc	
1651/tcp	open	msrpc	
1652/tcp	open	msrpc	
1653/tcp	open	msrpc	
1654/tcp	open	msrpc	
1655/tcp	open	msrpc	
1656/tcp	open	msrpc	
1657/tcp	open	msrpc	
1658/tcp	open	msrpc	
1659/tcp	open	msrpc	
1660/tcp	open	msrpc	
1661/tcp	open	msrpc	
1662/tcp	open	msrpc	
1663/tcp	open	msrpc	
1664/tcp	open	msrpc	
1665/tcp	open	msrpc	
1666/tcp	open	msrpc	
1667/tcp	open	msrpc	
1668/tcp	open	msrpc	
1669/tcp	open	msrpc	
1670/tcp	open	msrpc	
1671/tcp	open	msrpc	
1672/tcp	open	msrpc	
1673/tcp	open	msrpc	
1674/tcp	open	msrpc	
1675/tcp	open	msrpc	
1676/tcp	open	msrpc	
1677/tcp	open	msrpc	
1678/tcp	open	msrpc	
1679/tcp	open	msrpc	
1680/tcp	open	msrpc	
1681/tcp	open	msrpc	
1682/tcp	open	msrpc	
1683/tcp	open	msrpc	
1684/tcp	open	msrpc	
1685/tcp	open	msrpc	
1686/tcp	open	msrpc	
1687/tcp	open	msrpc	
1688/tcp	open	msrpc	
1689/tcp	open	msrpc	
1690/tcp	open	msrpc	
1691/tcp	open	msrpc	
1692/tcp	open	msrpc	
1693/tcp	open	msrpc	
1694/tcp	open	msrpc	
1695/tcp	open	msrpc	
1696/tcp	open	msrpc	
1697/tcp	open	msrpc	
1698/tcp	open	msrpc	
1699/tcp	open	msrpc	
1700/tcp	open	msrpc	
1701/tcp	open	msrpc	
1702/tcp	open	msrpc	
1703/tcp	open	msrpc	
1704/tcp	open	msrpc	
1705/tcp	open	msrpc	
1706/tcp	open	msrpc	
1707/tcp	open	msrpc	
1708/tcp	open	msrpc	
1709/tcp	open	msrpc	
1710/tcp	open	msrpc	
1711/tcp	open	msrpc	
1712/tcp	open	msrpc	
1713/tcp	open	msrpc	
1714/tcp	open	msrpc	
1715/tcp	open	msrpc	
1716/tcp	open	msrpc	
1717/tcp	open	msrpc	
1718/tcp	open	msrpc	
1719/tcp	open	msrpc	
1720/tcp	open	msrpc	
1721/tcp	open	msrpc	
1722/tcp	open	msrpc	
1723/tcp	open	msrpc	
1724/tcp	open	msrpc	
1725/tcp	open	msrpc	
1726/tcp	open	msrpc	
1727/tcp	open	msrpc	
1728/tcp	open	msrpc	
1729/tcp	open	msrpc	
1730/tcp	open	msrpc	
1731/tcp	open	msrpc	
1732/tcp	open	msrpc	
1733/tcp	open	msrpc	
1734/tcp	open	msrpc	
1735/tcp	open	msrpc	
1736/tcp	open	msrpc	
1737/tcp	open	msrpc	
1738/tcp	open	msrpc	
1739/tcp	open	msrpc	
1740/tcp	open	msrpc	
1741/tcp	open	msrpc	
1742/tcp	open	msrpc	
1743/tcp	open	msrpc	
1744/tcp	open	msrpc	
1745/tcp	open	msrpc	
1746/tcp	open	msrpc	
1747/tcp	open	msrpc	
1748/tcp	open	msrpc	
1749/tcp	open	msrpc	
1750/tcp	open	msrpc	
1751/tcp	open	msrpc	
1752/tcp	open	msrpc	
1753/tcp	open	msrpc	
1754/tcp	open	msrpc	
1755/tcp	open	msrpc	
1756/tcp	open	msrpc	
1757/tcp	open	msrpc	
1758/tcp	open	msrpc	
1759/tcp	open	msrpc	
1760/tcp	open	msrpc	
1761/tcp	open	msrpc	
1762/tcp	open	msrpc	
1763/tcp	open	msrpc	
1764/tcp	open	msrpc	
1765/tcp	open	msrpc	
1766/tcp	open	msrpc	



```

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:

```

Nmap 7.95 ( https://nmap.org ) at 2025-02-28 13:09 Pacific Standard Time
Nmap scan report for 192.168.56.1
Host is up (0.00028s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  (generic dns response: SERVFAIL)
| fingerprint-strings:
|   DNS-SD-TCP:
|     _services
|     _dns-sd
|     _udp
|     _local
80/tcp    open  http    Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-csrft: Couldn't find any CSRF vulnerabilities.
| http-dombased-xss: Couldn't find any DOM based XSS.
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.
88/tcp    open  kerberos-sec Microsoft Kerberos (server time: 2025-02-28 21:09:40Z)
139/tcp   open  netbios-ssn Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap    Microsoft Windows Active Directory LDAP (Domain: BankofAmerica.com, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd??
593/tcp   open  http    Microsoft Windows RPC over HTTP 1.0
656/tcp   open  tcpwrapped
2179/tcp  open  vncdpy?
3268/tcp  open  ldap    Microsoft Windows Active Directory LDAP (Domain: BankofAmerica.com, Site: Default-First-Site-Name)
3269/tcp  open  http    Microsoft HTTPAPI httpd 7.0 (SSPI/SPAPI)
5222/tcp  open  http    Microsoft HTTPAPI httpd 7.0 (SSPI/SPAPI)
|_http-server-header: Microsoft-HTTPAPI/7.0
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-csrft: Couldn't find any CSRF vulnerabilities.
| http-dombased-xss: Couldn't find any DOM based XSS.
|_service-unrecognized: Despite returning data, if you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service=:
SF-Port53-TCP-FN=7,ST=1,T=1,U=1,S=7C22A231-161F-4C9B-BE8D-5E8203461000,V=0.0.0.0,N=_service53,_id=1
SF-Port53-TCP-FN=7,ST=1,T=1,U=1,S=7C22A231-161F-4C9B-BE8D-5E8203461000,V=0.0.0.0,N=_service53,_id=1
Service Info: Host: WIN-8AFV939K6PV3; OS: Windows; CPE: cpe:/microsoft:windows

Host script results:
| smb-vuln-ms10-054: false
| samba-vuln-cve-2012-1182: Could not negotiate a connection(SMB). Failed to receive bytes: ERROR
| smb-vuln-ms10-061: Could not negotiate a connection(SMB). Failed to receive bytes: ERROR

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 167.36 seconds

```

Step 4: 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 Type:** Nmap -O
- Target:** 192.168.56.1
- Command:** nmap -O 192.168.56.1
- Hosts:** www.bankofame (Host)
- Services:** 192.168.56.1
- Ports Open:**

PORT	STATE	SERVICE
53/tcp	open	domain
80/tcp	open	http
88/tcp	open	kerberos-sec
135/tcp	open	microsoft-ds
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	vardp
3268/tcp	open	globalcatLDAP
3269/tcp	open	globalcatLDAPssl
5985/tcp	open	wman
- OS Detection:** Microsoft Windows 2022
- Network Distance:** 0 hops
- Notes:** 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 5: 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   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   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   PcaSvc        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   SENS          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   TabletinPutBroker 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>
```