Eric Guzman
Hacking and Penetration Testing

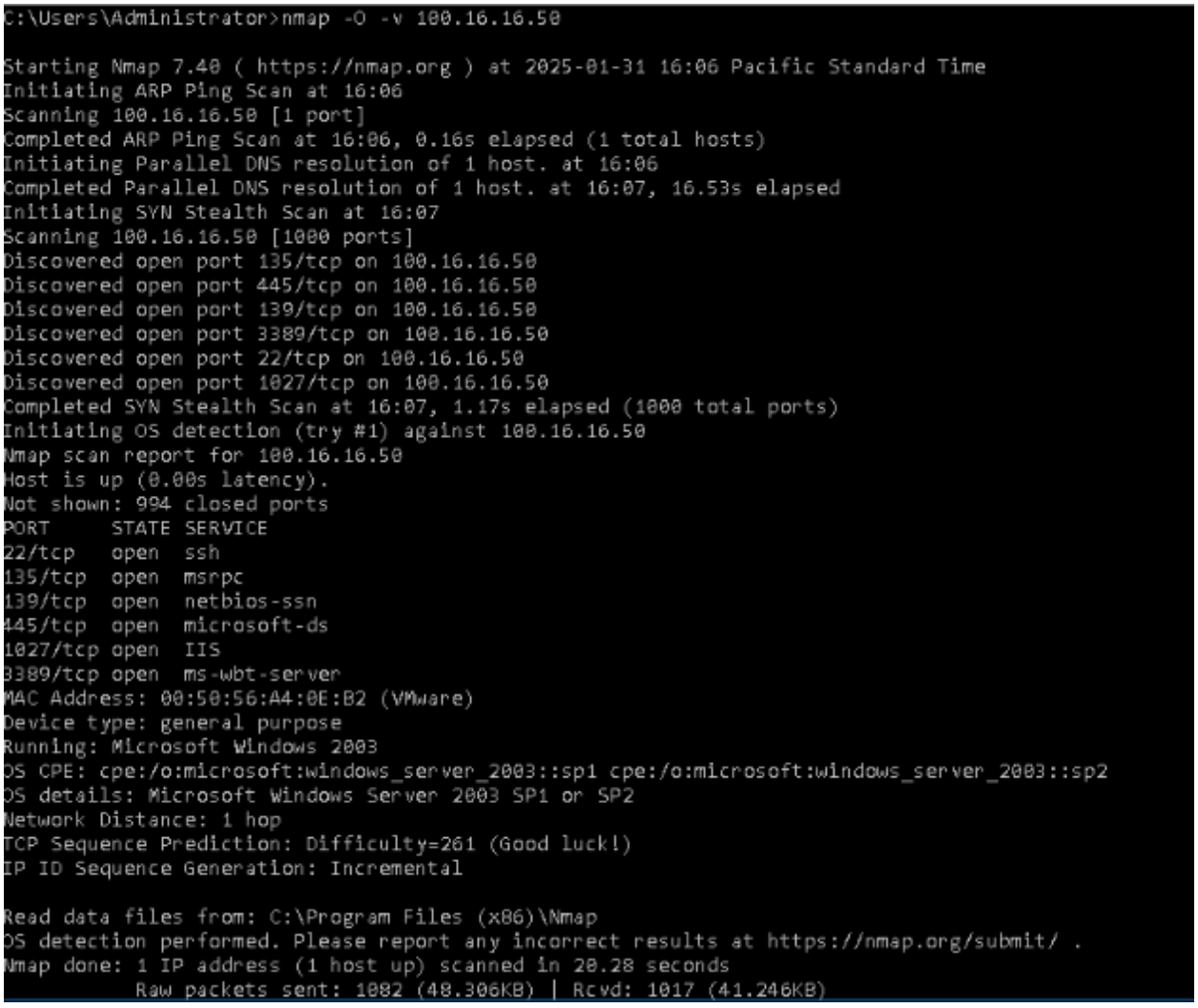
1/31/25
Professor Foti

Assessing and Securing Systems on a Wide Area Network (WAN)
Hacker Techniques, Tools, and Incident Handling, Third Edition - Lab 01

Section 1: Hands-On Demonstration

Part 1: Scan the Wide Area Network

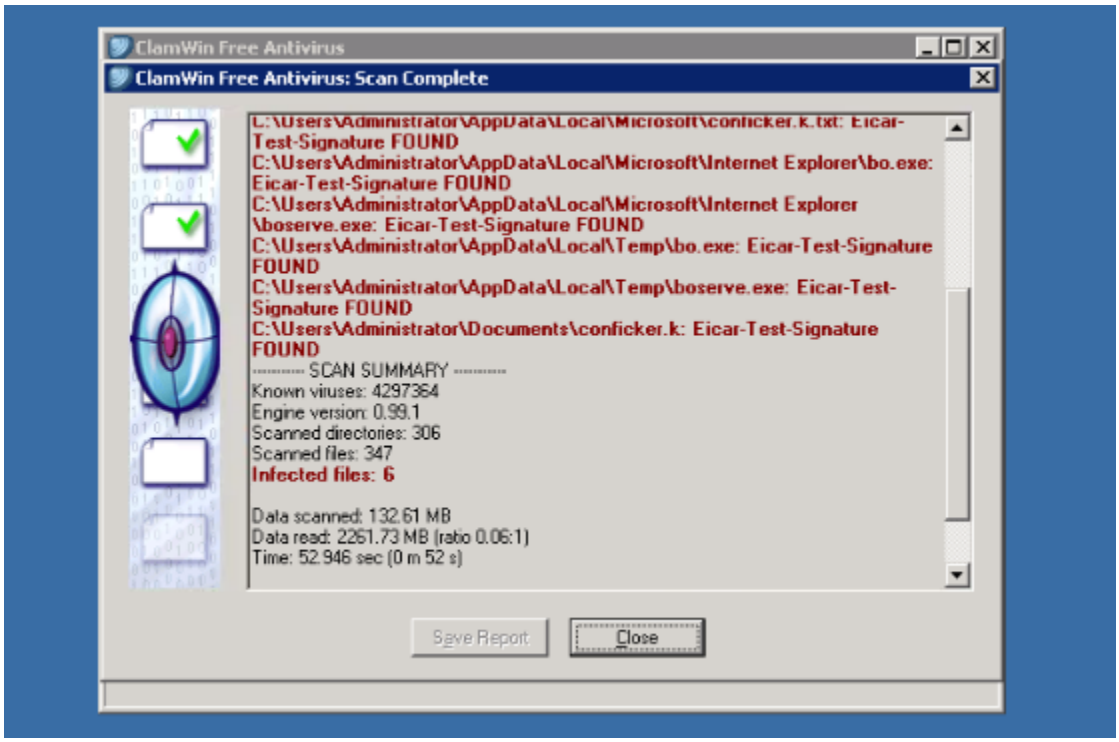
(3) Make a screen capture showing the results of the Nmap OS scan for 100.16.16.50 and paste it into your Lab Report file.



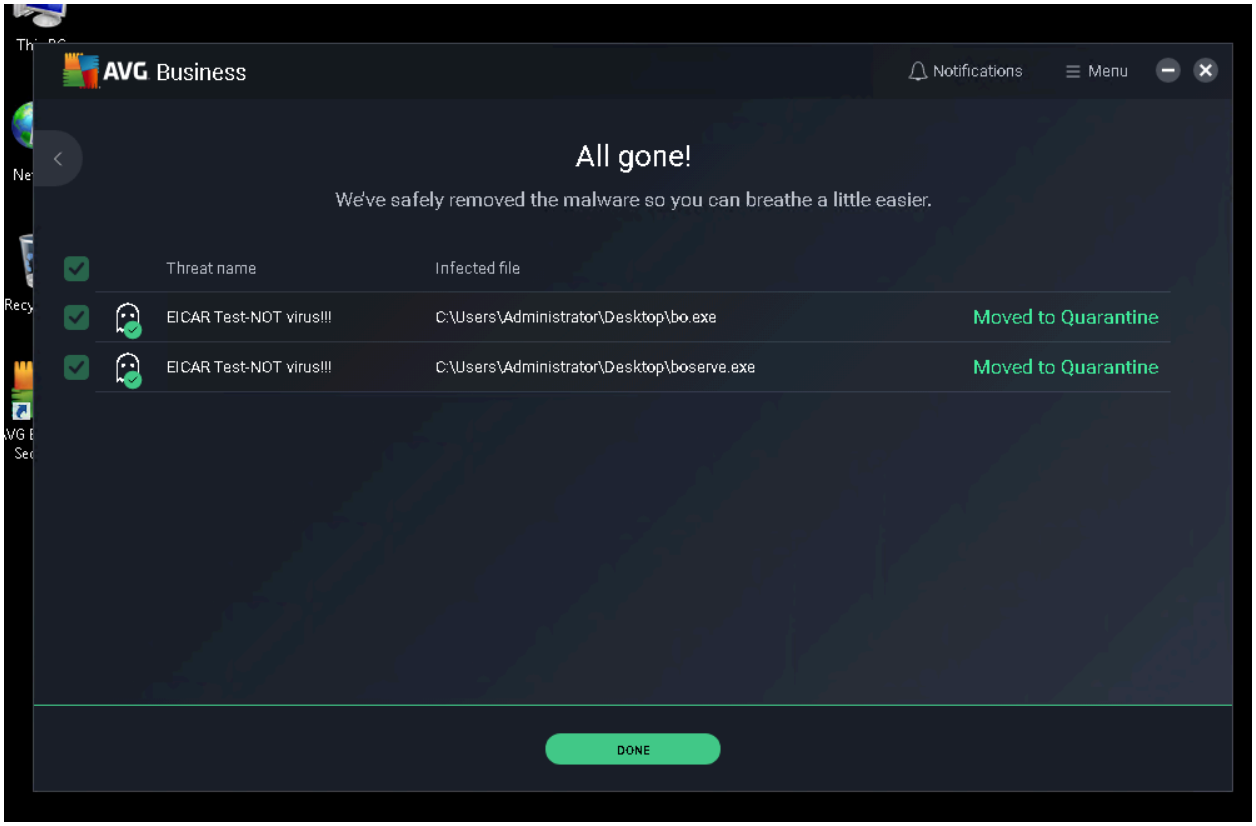
```
C:\Users\Administrator>nmap -O -v 100.16.16.50

Starting Nmap 7.40 ( https://nmap.org ) at 2025-01-31 16:06 Pacific Standard Time
Initiating ARP Ping Scan at 16:06
Scanning 100.16.16.50 [1 port]
Completed ARP Ping Scan at 16:06, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:06
Completed Parallel DNS resolution of 1 host. at 16:07, 16.53s elapsed
Initiating SYN Stealth Scan at 16:07
Scanning 100.16.16.50 [1000 ports]
Discovered open port 135/tcp on 100.16.16.50
Discovered open port 445/tcp on 100.16.16.50
Discovered open port 139/tcp on 100.16.16.50
Discovered open port 3389/tcp on 100.16.16.50
Discovered open port 22/tcp on 100.16.16.50
Discovered open port 1027/tcp on 100.16.16.50
Completed SYN Stealth Scan at 16:07, 1.17s elapsed (1000 total ports)
Initiating OS detection (try #1) against 100.16.16.50
Nmap scan report for 100.16.16.50
Host is up (0.00s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1027/tcp open  IIS
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:A4:0E:B2 (VMware)
Device type: general purpose
Running: Microsoft Windows 2003
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.28 seconds
           Raw packets sent: 1082 (48.306KB) | Rcvd: 1017 (41.246KB)
```

Part 2: Clean Vulnerable Systems

(9) Make a screen capture showing the details of the threat to TargetWindows04 and paste it into your Lab Report file.

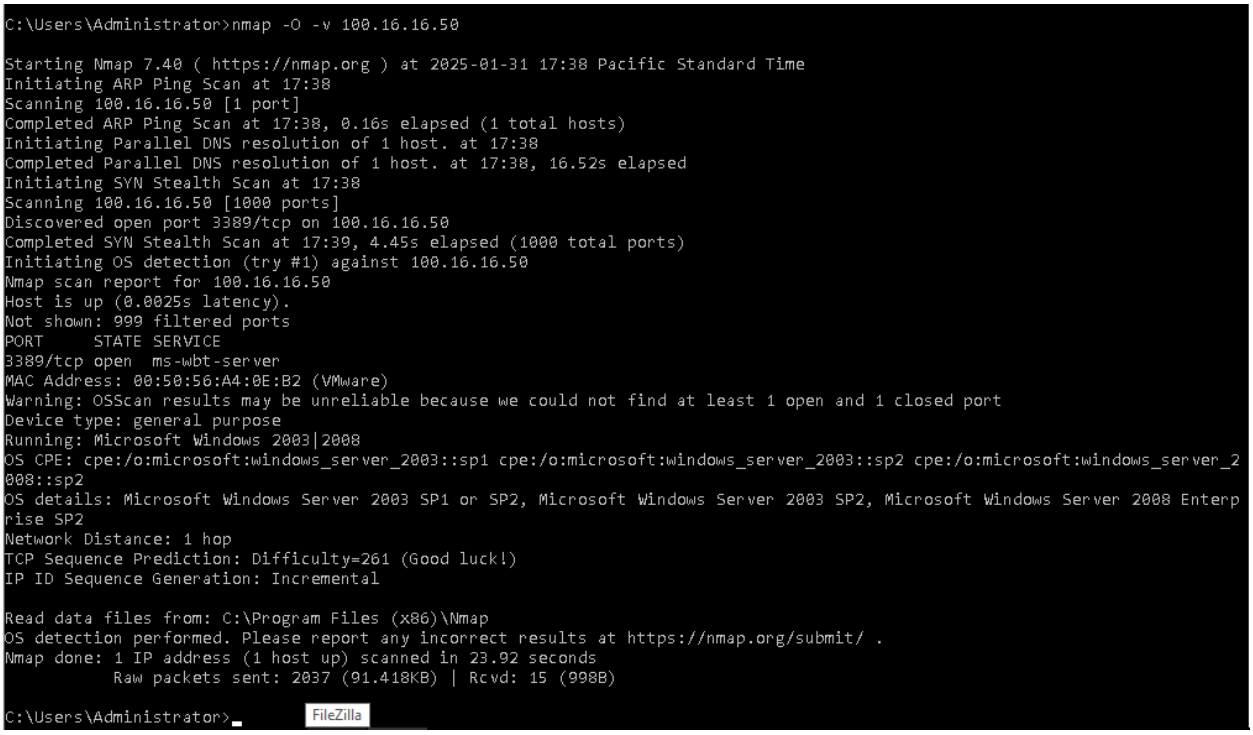


(20) Make a screen capture showing the details of the threats to TargetWindows05 and paste it into your Lab Report file.



Part 3: Reduce the Attack Surface on the Windows 2003 Server

(25) Make a screen capture showing the new Nmap scan results for TargetVulnerable01 and the reduced attack surface and paste it into your Lab Report file.

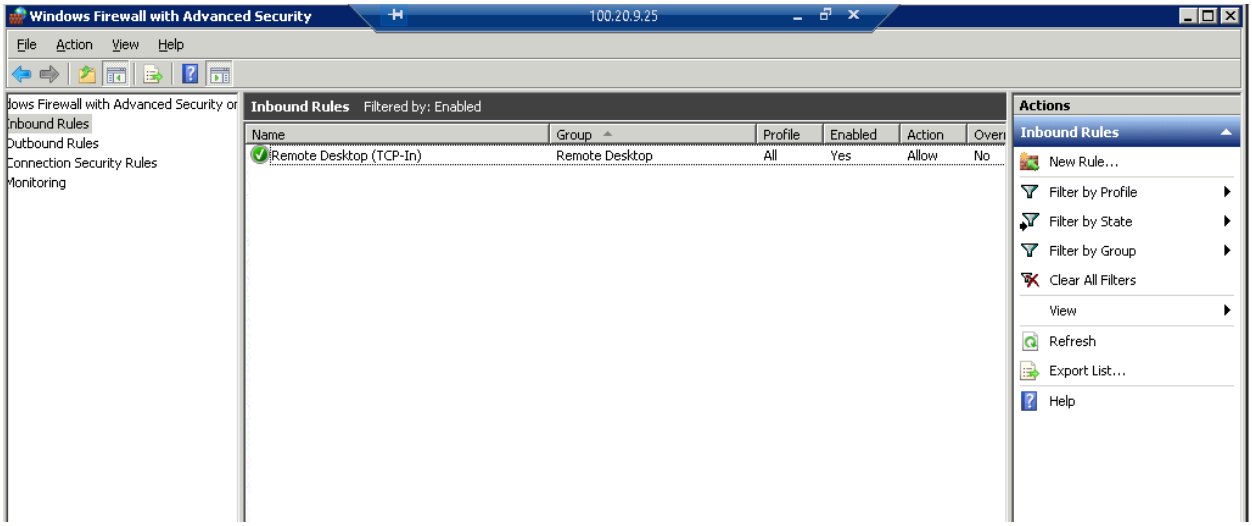


(26) In your Lab Report file, compare the results of the two scans for this computer and explain how your actions in Part 3 of this lab hardened security on this machine.

The second nmap scan shows that I disabled vulnerable ports like port 445, 135, 139, 22, and 1027, significantly reducing the attack surface on this system. I only left port 3389 open, which is needed to RDP into it. I also limited the RDP access to specific IP addresses which only lets certain IPs RDP into the system. This configuration keeps this system more secure than it was while maintaining its functionality.

Part 4: Reduce the Attack Surface on the Windows 2008 Server

(6) Make a screen capture showing the remaining enabled Inbound Rule and paste it into your Lab Report file.



(24) Make a screen capture showing the Nmap scan results and the reduced attack surface for TargetWindows04 and paste it into your Lab Report file.

```
C:\Users\Administrator>nmap -O -v 100.20.9.25

Starting Nmap 7.40 ( https://nmap.org ) at 2025-01-31 17:53 Pacific Standard Time
Initiating ARP Ping Scan at 17:53
Scanning 100.20.9.25 [1 port]
Completed ARP Ping Scan at 17:53, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:53
Completed Parallel DNS resolution of 1 host. at 17:54, 16.55s elapsed
Initiating SYN Stealth Scan at 17:54
Scanning 100.20.9.25 [1000 ports]
Discovered open port 3389/tcp on 100.20.9.25
Completed SYN Stealth Scan at 17:54, 4.78s elapsed (1000 total ports)
Initiating OS detection (try #1) against 100.20.9.25
Retrying OS detection (try #2) against 100.20.9.25
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
WARNING: RST from 100.20.9.25 port 3389 -- is this port really open?
Nmap scan report for 100.20.9.25
Host is up (0.00s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:A4:15:EA (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|printer|broadband router|router|firewall
Running (JUST GUESSING): Motorola embedded (92%), Konica Minolta embedded (86%), D-Link embedded (86%), Adtran embedded (85%)
, ZyXEL ZyNOS 3.X (85%)
OS CPE: cpe:/h:motorola:rfs_6000 cpe:/h:konicaminolta:1600f cpe:/h:dlink:di-808hv cpe:/h:adtran:total_access_904 cpe:/o:zyxel
:zynos:3.62
Aggressive OS guesses: Motorola RFS 6000 wireless switch (92%), Konica Minolta 1600f printer (86%), D-Link DI-808HV router (8
6%), Adtran Total Access 904 router (85%), ZyXEL ZyWALL 2 firewall or Prestige 660HW-61 ADSL router (ZyNOS 3.62) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.44 seconds
```

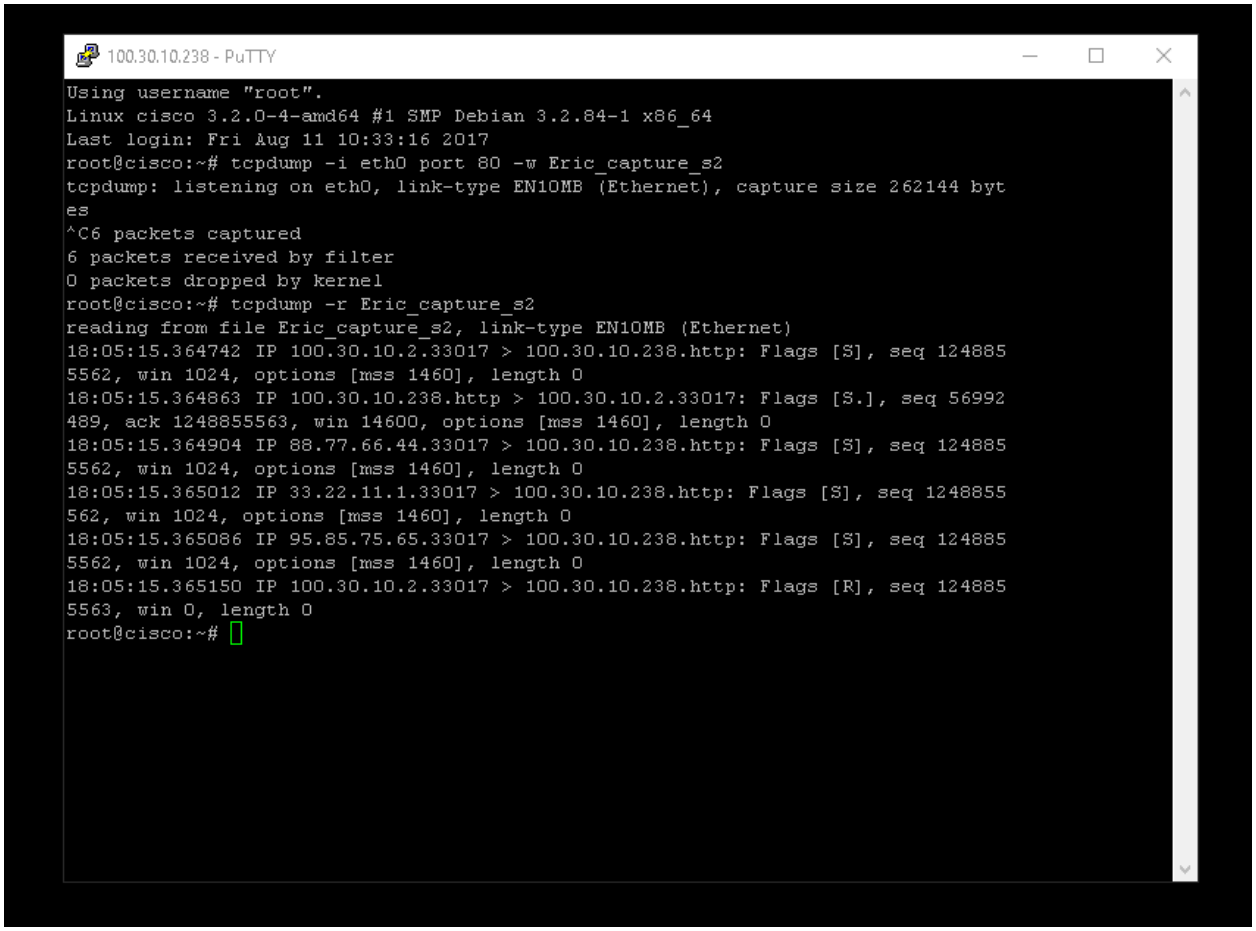
(25) In your Lab Report file, compare the results of the two scans for this computer and explain how your actions in Part 4 of this lab hardened security on this machine.

This second nmap scan shows that we once again reduced the open ports on the system. We disabled many networking rules, significantly decreasing the attack surface for any malicious actor trying to exploit this system. We only left RDP open once again which we need.

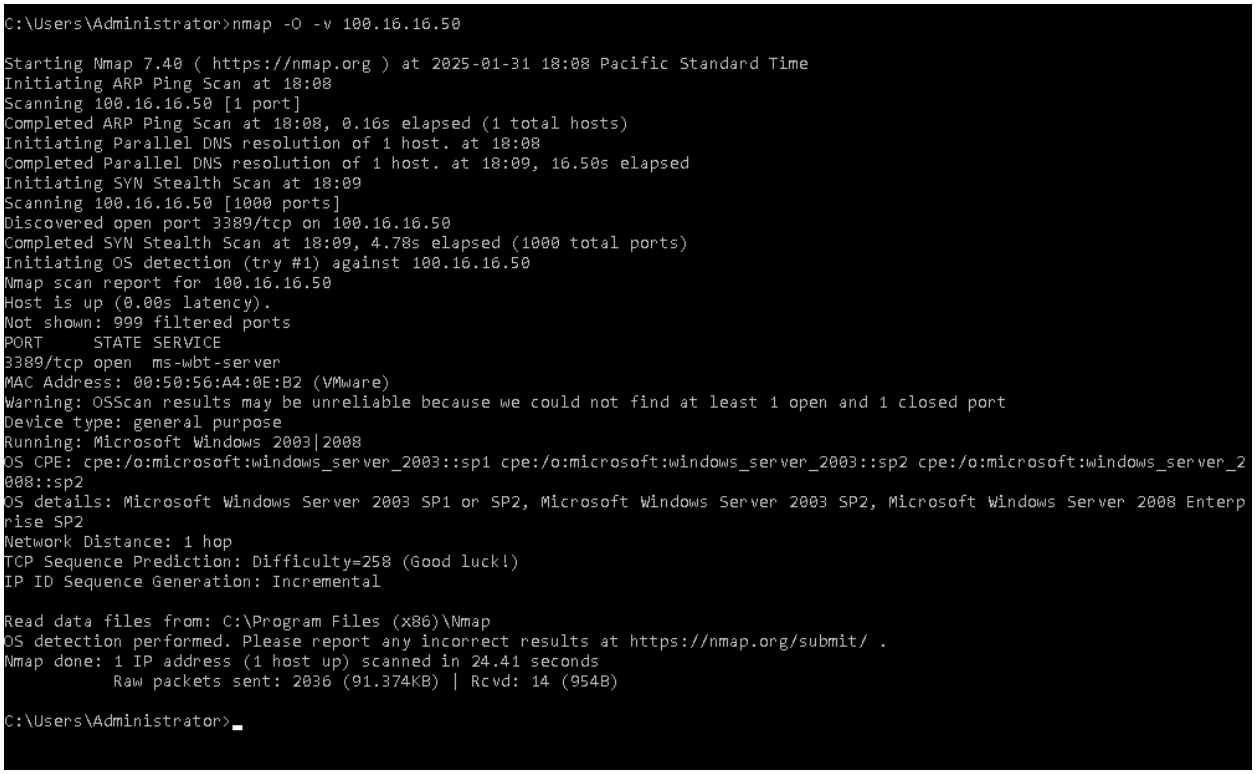
Section 2: Applied Learning

Part 1: Scan the Wide Area Network

(8) Make a screen capture showing the decoy IP addresses and paste it into your Lab Report file.

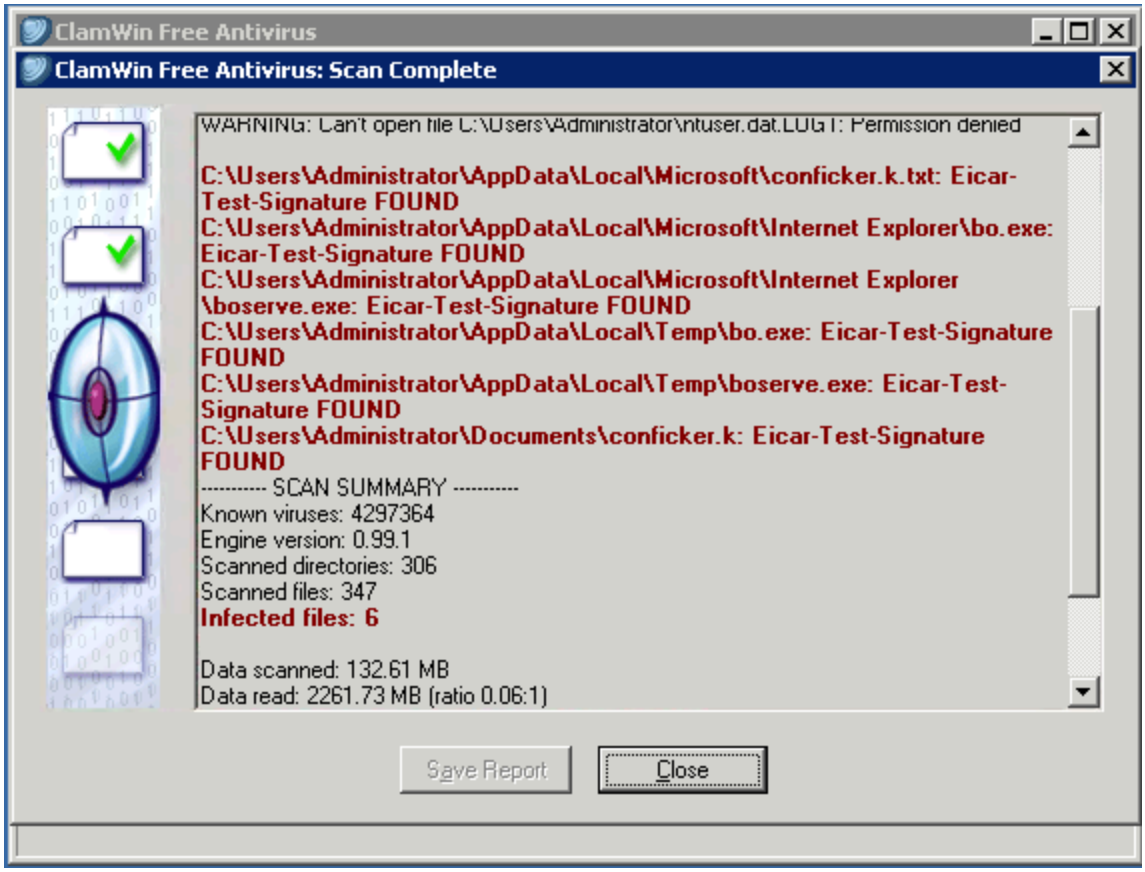


(11) Make a screen capture showing the results of the Nmap OS scan for TargetVulnerable01 and paste it into your Lab Report file.



Part 2: Clean Vulnerable Systems

(8)Make a screen capture showing the details of the threat to TargetWindows04 and paste it into your Lab Report file.

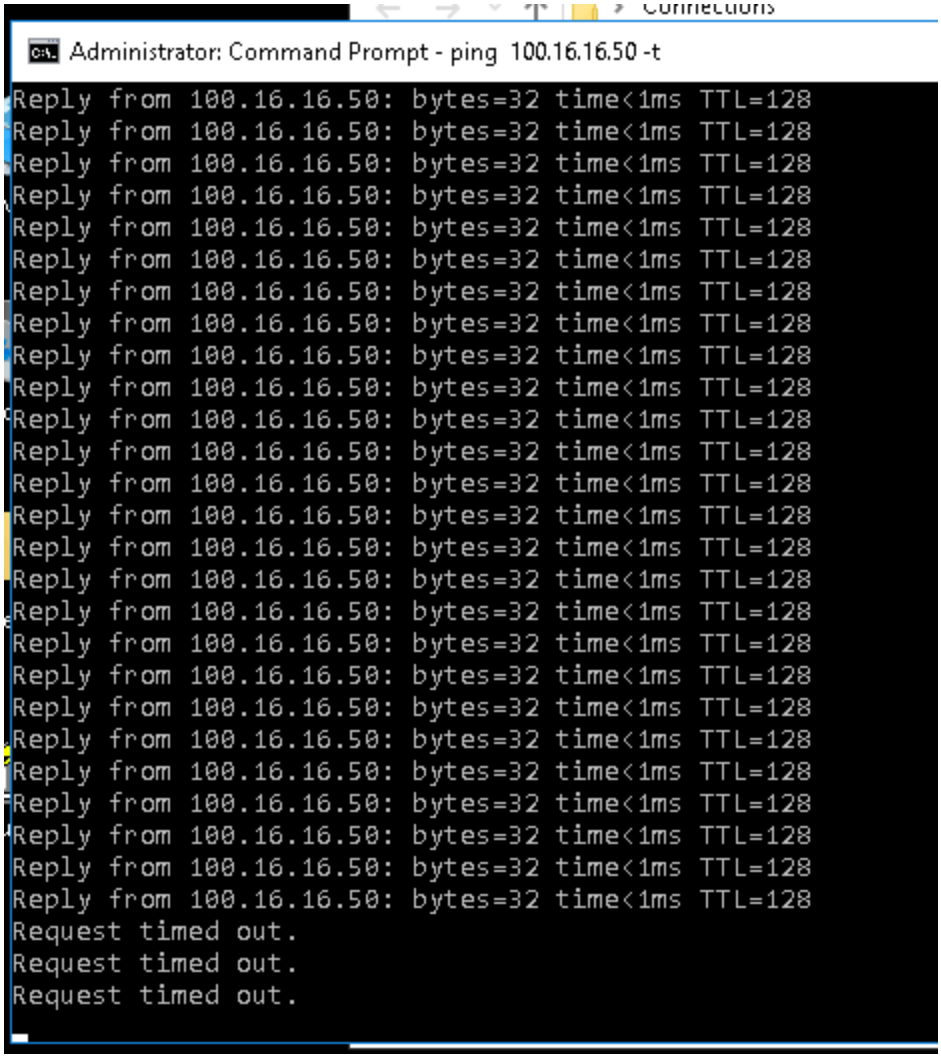


(14) In your Lab Report, document the details associated with the threats.

The AVG scan I ran found and removed multiple threats from the system, moving all infected files to quarantine. The identified threats were "EICAR Test-NOT virus!!!" associated with the files bo.exe, codered.ndis, conficker.k, and trojan-dropper.i, all located in the \\tsclient\C:\Users\Administrator\Desktop\viral directory. Each of these files was successfully isolated so that they could not harm the system. This makes sure that the system is now free from these potential vulnerabilities and is better secured against any malicious activities.

Part 3: Reduce the Attack Surface on the Windows 2003 Server

(20) Make a screen capture showing the timed out ping of TargetVulnerable01 and paste it into your Lab Report file.



(28) Make a screen capture showing the new Nmap scan results for TargetVulnerable01 and the reduced attack surface and paste it into your Lab Report file.

```
C:\Users\Administrator>nmap -O -v 100.16.16.50

Starting Nmap 7.40 ( https://nmap.org ) at 2025-01-31 19:17 Pacific Standard Time
Initiating ARP Ping Scan at 19:17
Scanning 100.16.16.50 [1 port]
Completed ARP Ping Scan at 19:17, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:17
Completed Parallel DNS resolution of 1 host. at 19:17, 16.55s elapsed
Initiating SYN Stealth Scan at 19:17
Scanning 100.16.16.50 [1000 ports]
Discovered open port 3389/tcp on 100.16.16.50
Completed SYN Stealth Scan at 19:17, 4.45s elapsed (1000 total ports)
Initiating OS detection (try #1) against 100.16.16.50
Nmap scan report for 100.16.16.50
Host is up (0.00s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:A4:0E:B2 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2003
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows Server 2003 SP1 or SP2, Microsoft Windows Server 2003 SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.28 seconds
           Raw packets sent: 2043 (92.396KB) | Rcvd: 13 (672B)

C:\Users\Administrator>
```

(29) In your Lab Report file, compare the results of the two scans for this computer and explain how your actions in Part 3 of this lab hardened security on this machine.

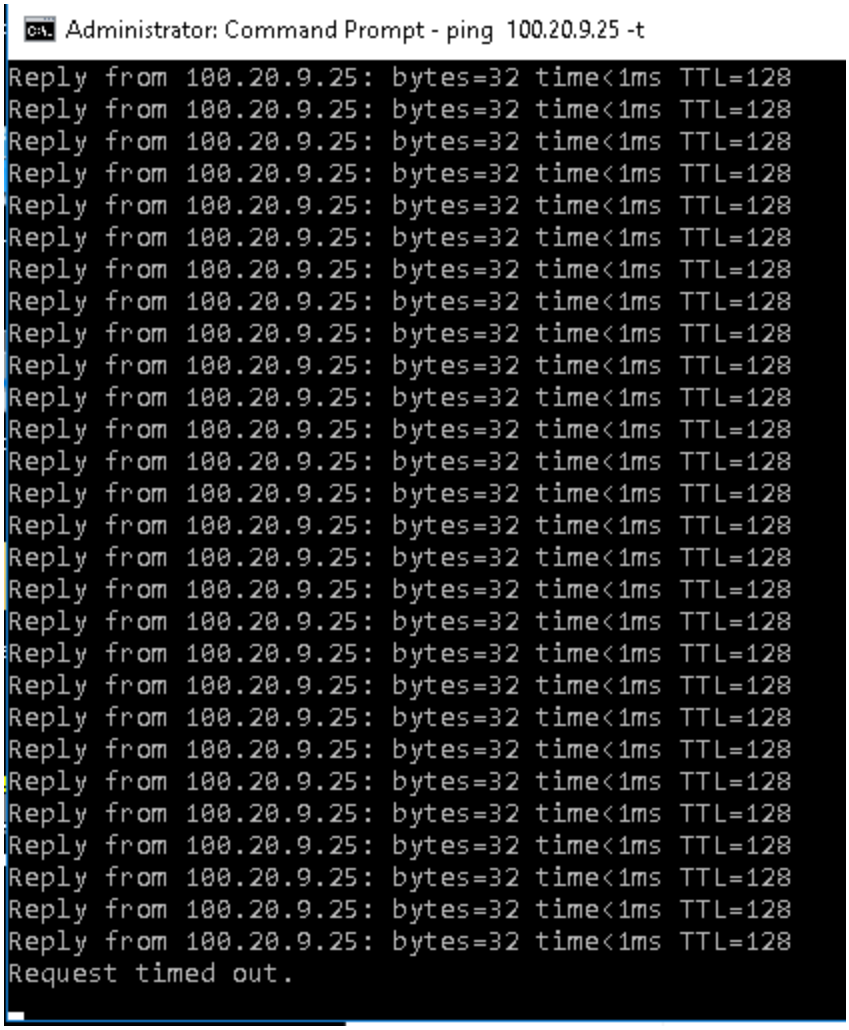
This new nmap scan for TargetVulnerable01 shows a significantly smaller attack surface. We pretty much did the same thing we did in section 1 but took a different approach. We closed all unnecessary ports besides the 3389 RDP port which stayed open. This system is only allowed to be accessed by the host, not any other machine, host or address. We have significantly reduced the amount of attack vectors by doing this.

Part 4: Reduce the Attack Surface on the Windows 2008 Server

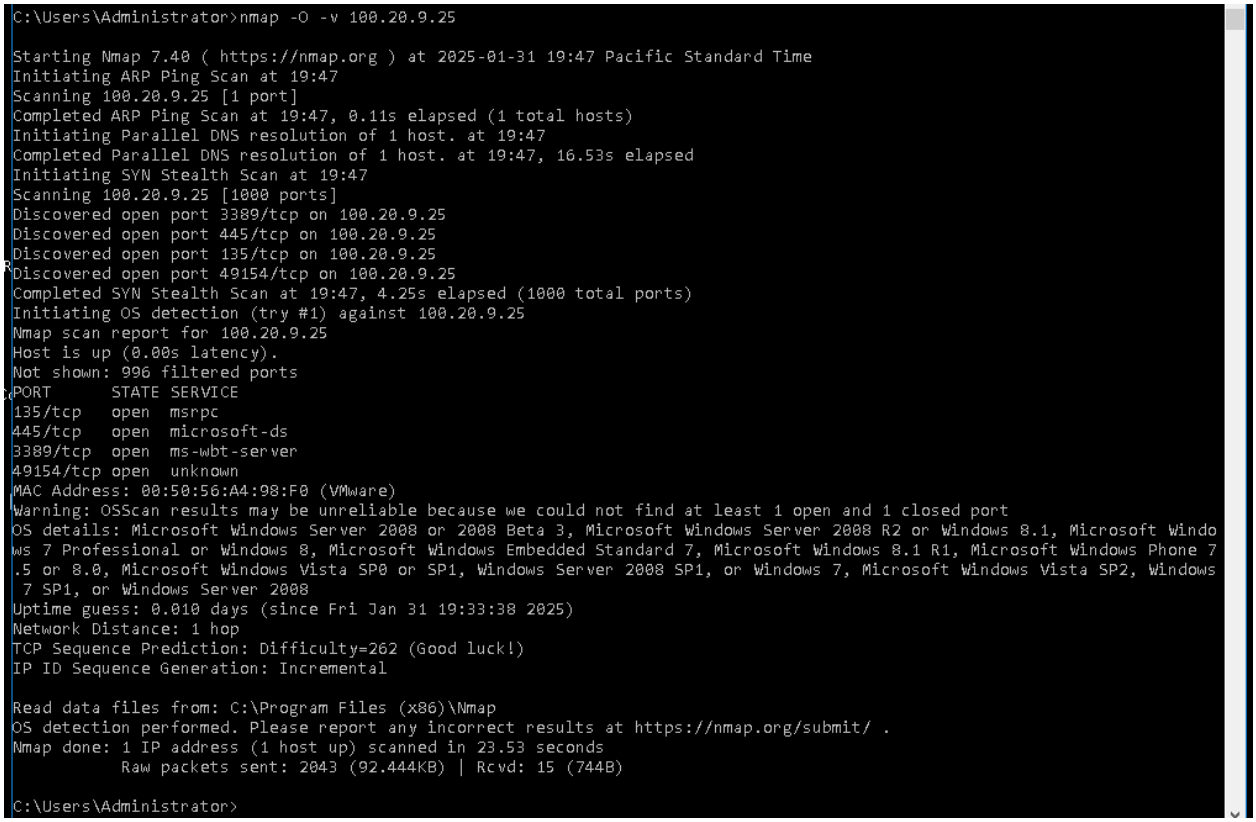
(7) Make a screen capture showing the Remote Desktop rule within the rules.txt file and paste it into your Lab Report file.

```
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            RPC
RemotePort:                           Any
Edge traversal:                       No
Action:                               Allow

Rule Name:                            Remote Volume Management - Virtual Disk Service (RPC)
----------------------------------------------------------------------
Enabled:                              No
Direction:                            In
Profiles:                             Domain,Private,Public
Grouping:                             Remote Volume Management
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            RPC
RemotePort:                           Any
Edge traversal:                       No
Action:                               Allow

Rule Name:                            Remote Desktop (TCP-In)
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            In
Profiles:                             Domain,Private,Public
Grouping:                             Remote Desktop
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            3389
RemotePort:                           Any
Edge traversal:                       No
Action:                               Allow

Rule Name:                            Routing and Remote Access (PPTP-Out)
----------------------------------------------------------------------
Enabled:                              No
Direction:                            Out
Profiles:                             Domain,Private,Public
Grouping:                             Routing and Remote Access
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            Any
RemotePort:                           1723
Edge traversal:                       No
Action:                               Allow

Rule Name:                            Routing and Remote Access (PPTP-In)
```

(17) Make a screen capture showing the timed out ping of TargetWindows04 and paste it into your Lab Report file.



(20) Make a screen capture showing the Nmap scan results and the reduced attack surface for TargetWindows04 and paste it into your Lab Report file.



(21) In your Lab Report file, compare the results of the two scans for this computer and explain how your actions in Part 4 of this lab hardened security on this machine.

The second nmap scan of TargetWindows04 shows how after applying security rules, we made the attack surface smaller. We configured the firewall and added specific security rules to only allow certain traffic through. We made the same adjustments but from the command prompt this time. We closed ports and left the RDP port (3389) open just like we have this entire lab.

Section 3: Lab Challenge and Analysis

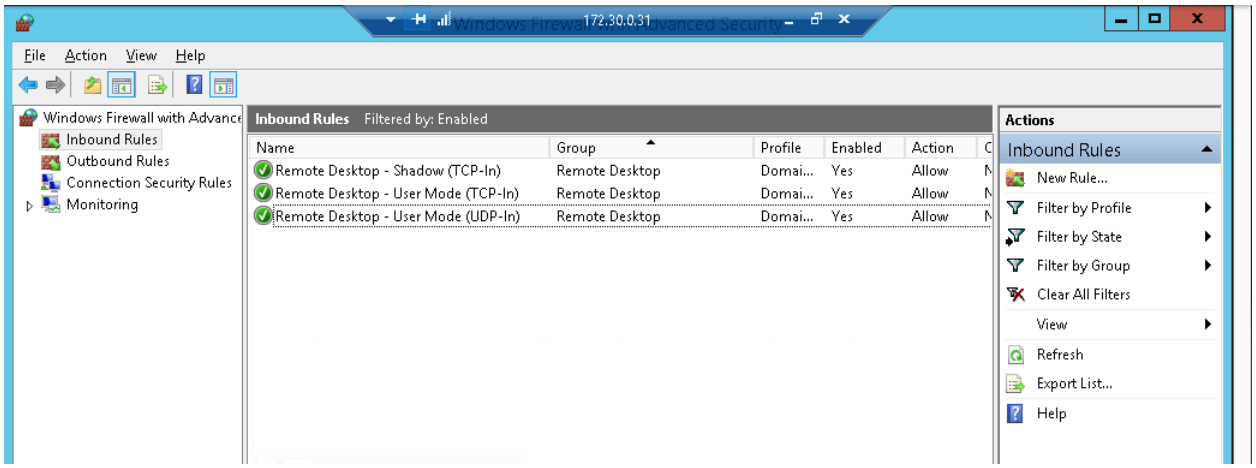
(1) Explain how the Back Orifice (BO) virus was named and why it can still be dangerous.

The back orifice virus was named that as a play on words that references Microsoft backoffice. It is able to get into systems undetected, allowing remote attackers to get full access to a system infected by the virus. It is a very old exploit but should not be overlooked as many legacy systems are used and could be exploited using it.

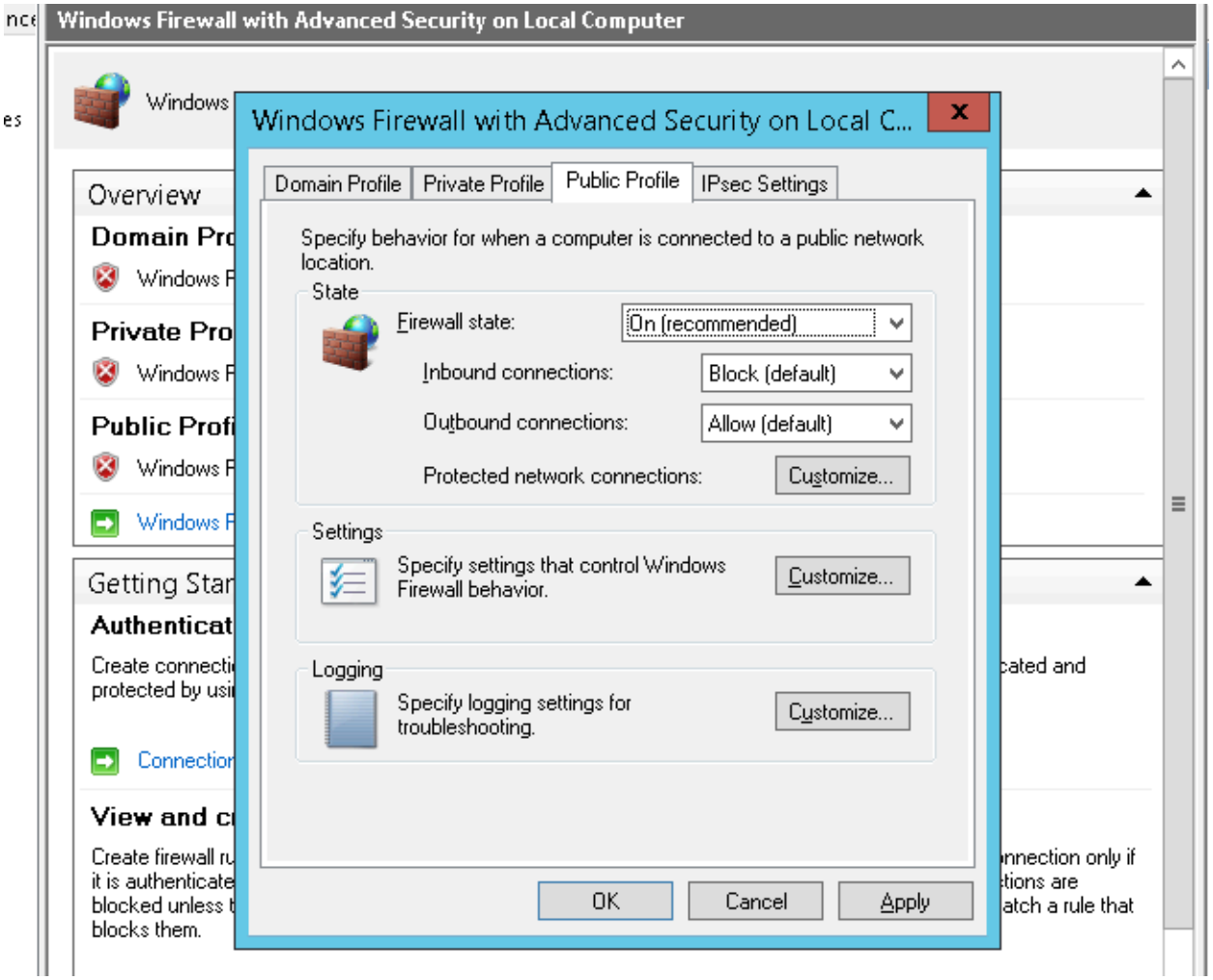
(2) Use the Internet to identify the netsh command (for both Windows 2003 and Windows 2008 firewalls) that will enable file sharing.

The command that enables file sharing for windows 2003 firewalls is “netsh firewall set service type = FILEANDPRINT mode = ENABLE” , and for windows 2008 firewalls it is “netsh advfirewall firewall set rule group=”File and Printer Sharing” new enable=Yes”.

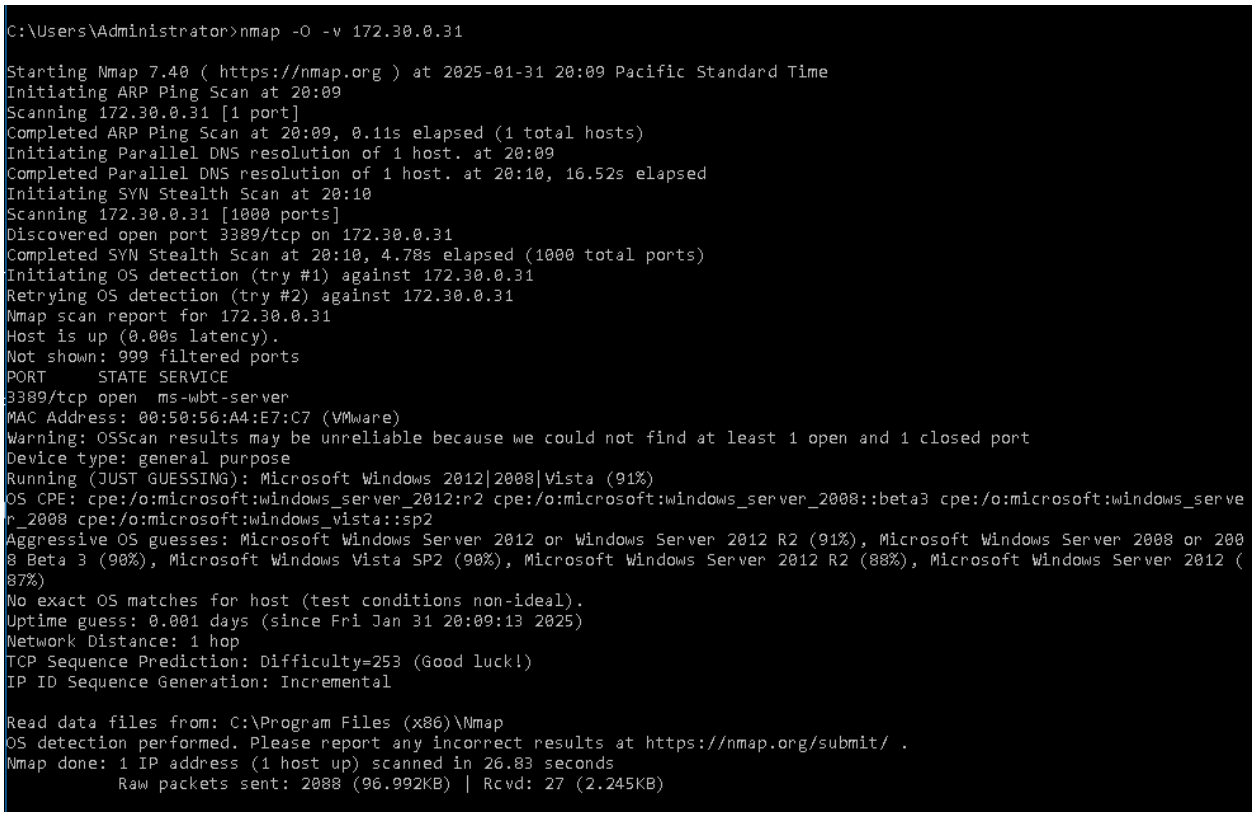
(3.1) Launch the Windows Firewall with Advanced Security on TargetWindows05, close all ports except Remote Desktop, repeat the nmap scans, and document results with screen captures.



I first disabled all rules not pertaining to RDP.

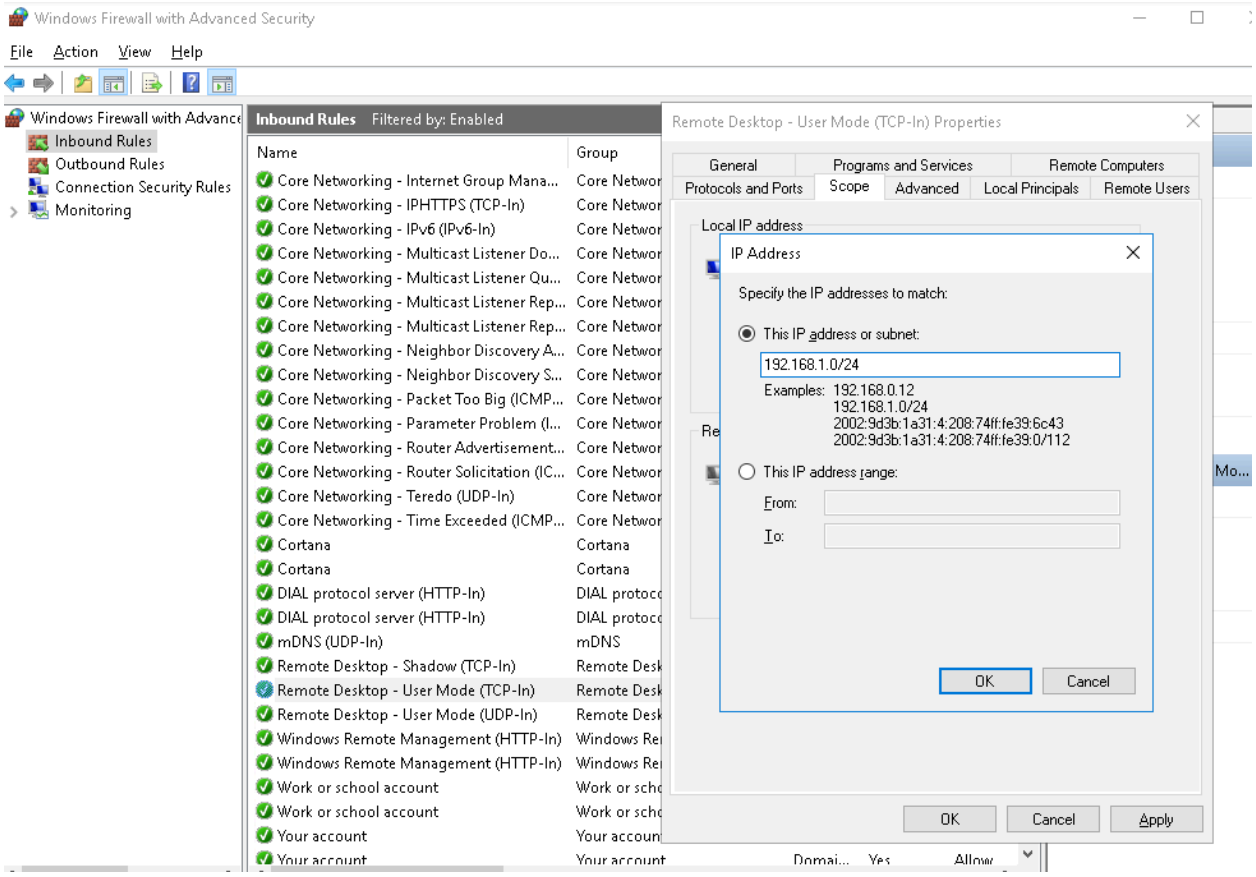


Then I enabled the firewall on all three profiles.



And here is the nmap scan showing only the RDP port is open on TargetWindows05.

(3.2) Launch the Windows Firewall with Advanced Security on the vWorkstation, limit Remote Desktop services, research best practices, and document firewall changes with screen captures.



For this part I went into the firewall rules and modified the rule named Remote Desktop for TCP-in and restricted access to the 192.168.1.0/24 subnet. This is a best practice to try and mitigate unauthorized access via RDP. Only hosts that are in the defined subnet will have access to RDP connections to the vWorkstation.