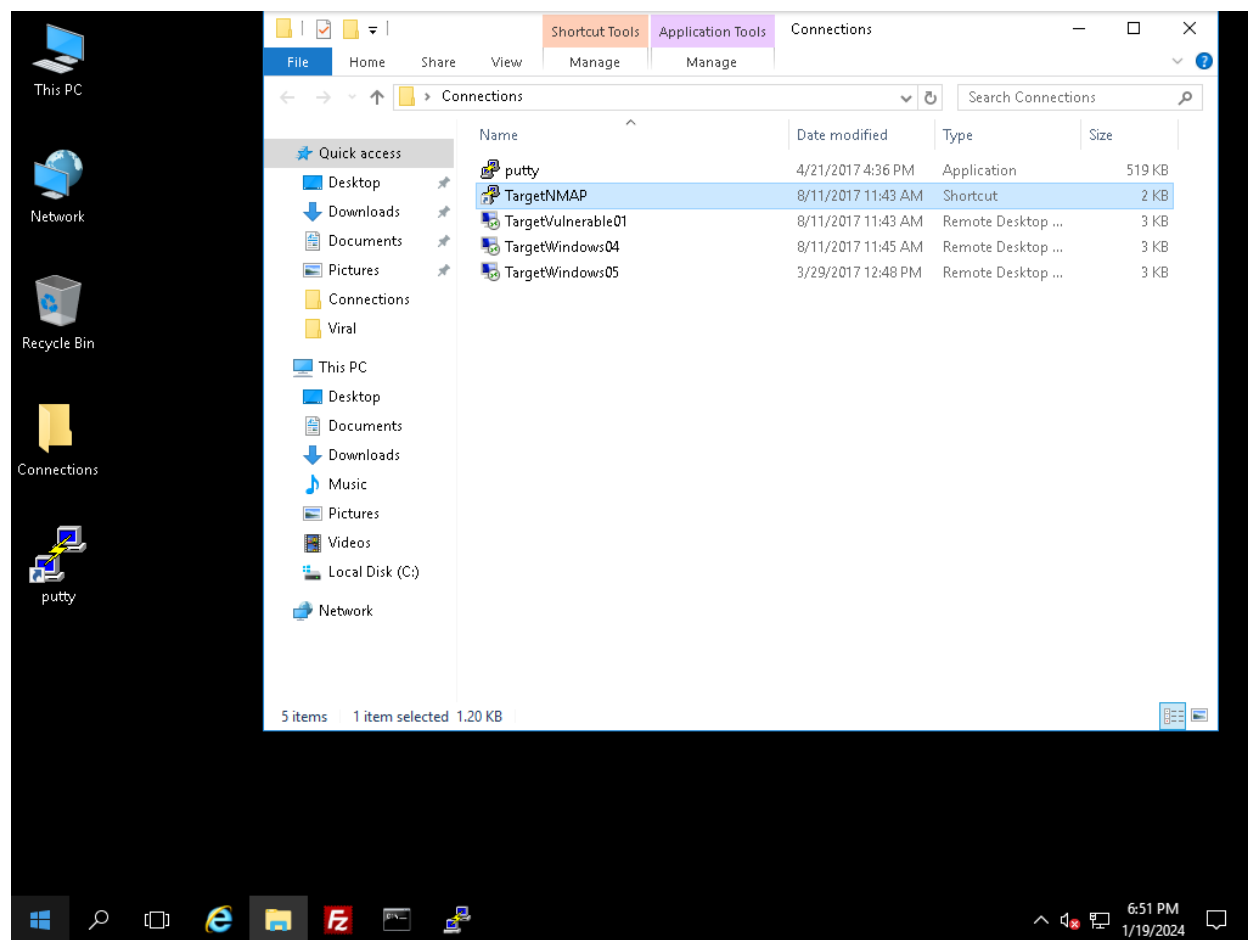


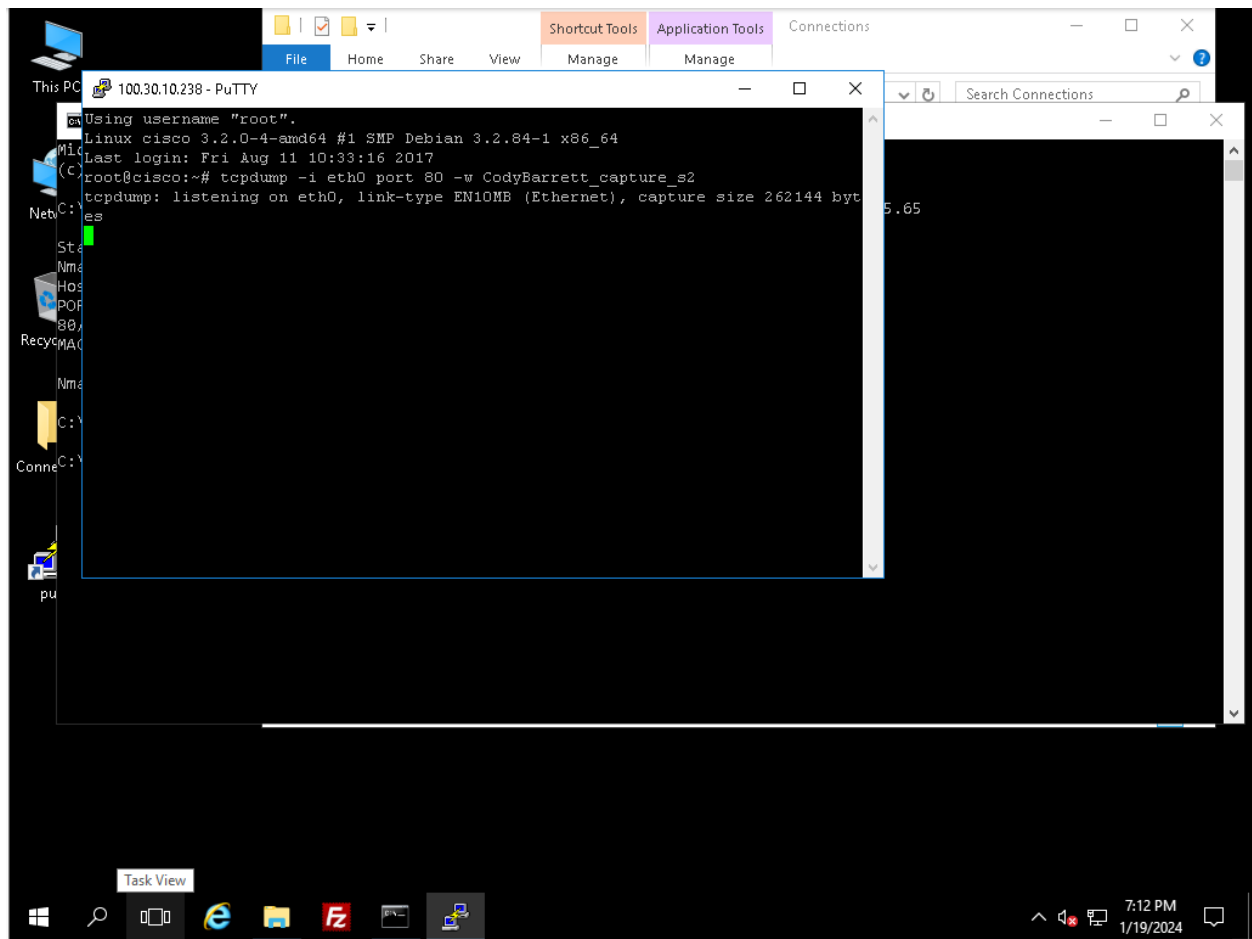
Cody J Barrett

## Lab 1: Assessing and Securing Systems on a Wide Area Network (WAN)

### Part 1: Scan the Wide Area Network



A shortcut is used to start a connection to a target system via PuTTY.



The command “tcpdump -i eth0 port 80 -w CodyBarrett\_capture\_s2” is used to start capturing network traffic over port 80 to a file named CodyBarrett\_capture\_s2.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

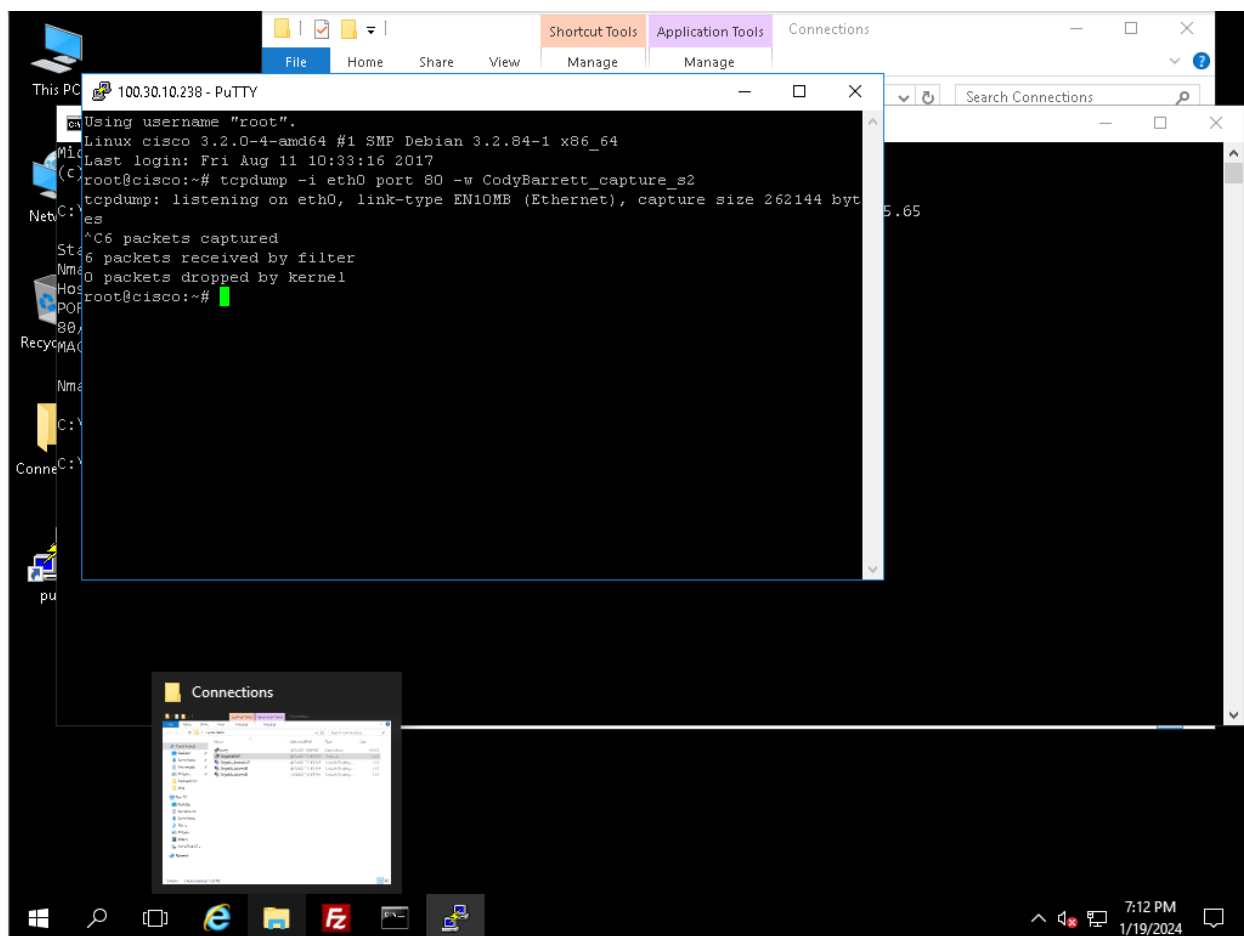
C:\Users\Administrator>nmap -sS -p 80 100.30.10.238 -D 88.77.66.44,33.22.11.1,95.85.75.65

Starting Nmap 7.40 ( https://nmap.org ) at 2024-01-19 18:50 Pacific Standard Time
Nmap scan report for 100.30.10.238
Host is up (0.00s latency).
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:50:56:AB:73:0E (VMware)

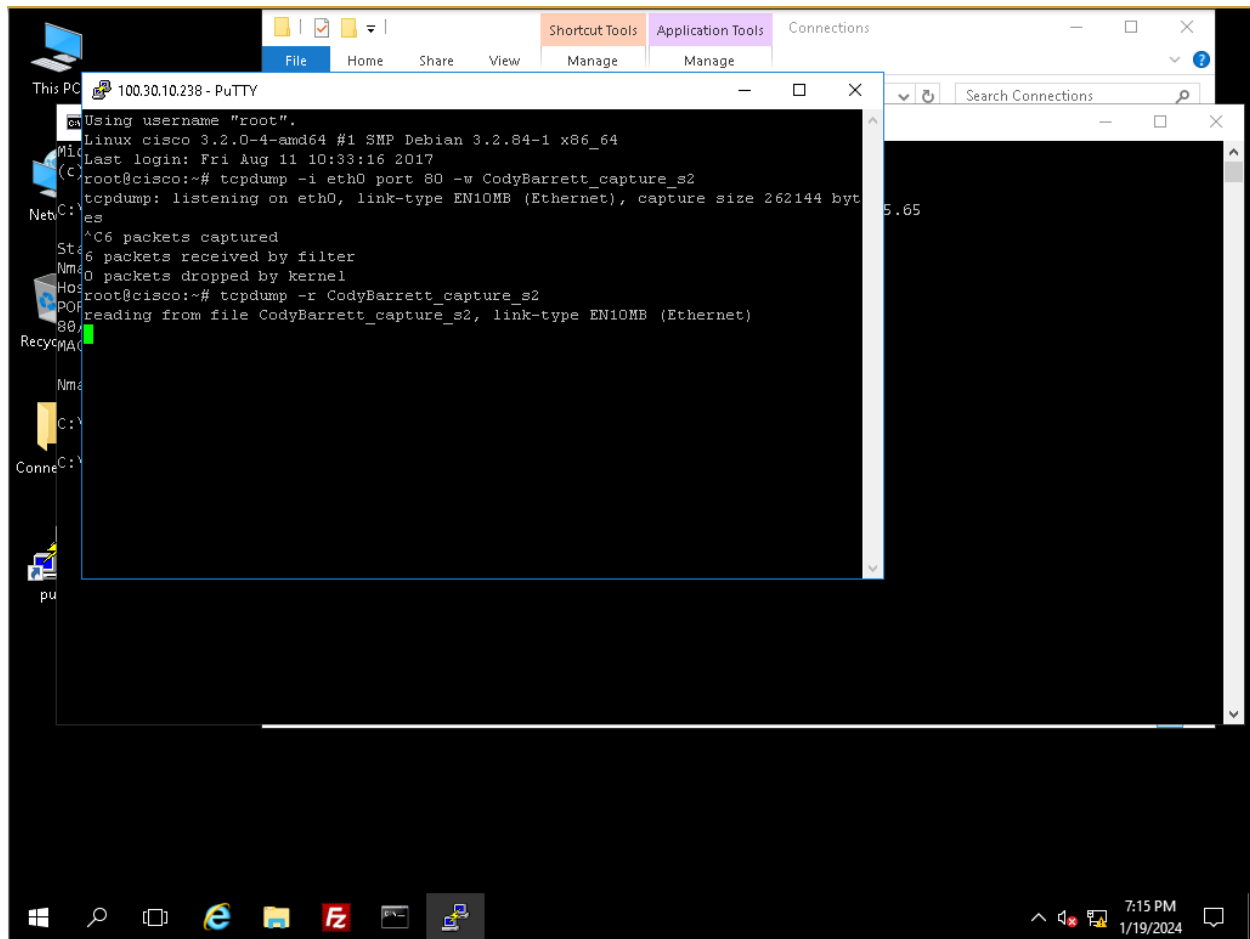
Nmap done: 1 IP address (1 host up) scanned in 16.94 seconds

C:\Users\Administrator>
C:\Users\Administrator>
```

In a CMD window, the command “nmap -sS -p 80 100.30.10.238 -D 88.77.66.44,33.22.11.1,95.85.75.65” is used to start a stealth scan on the system with the IP address of 100.30.10.238. This command also uses 88.77.66.44 33.22.11.1 and 95.85.75.65 as decoy IP addresses.

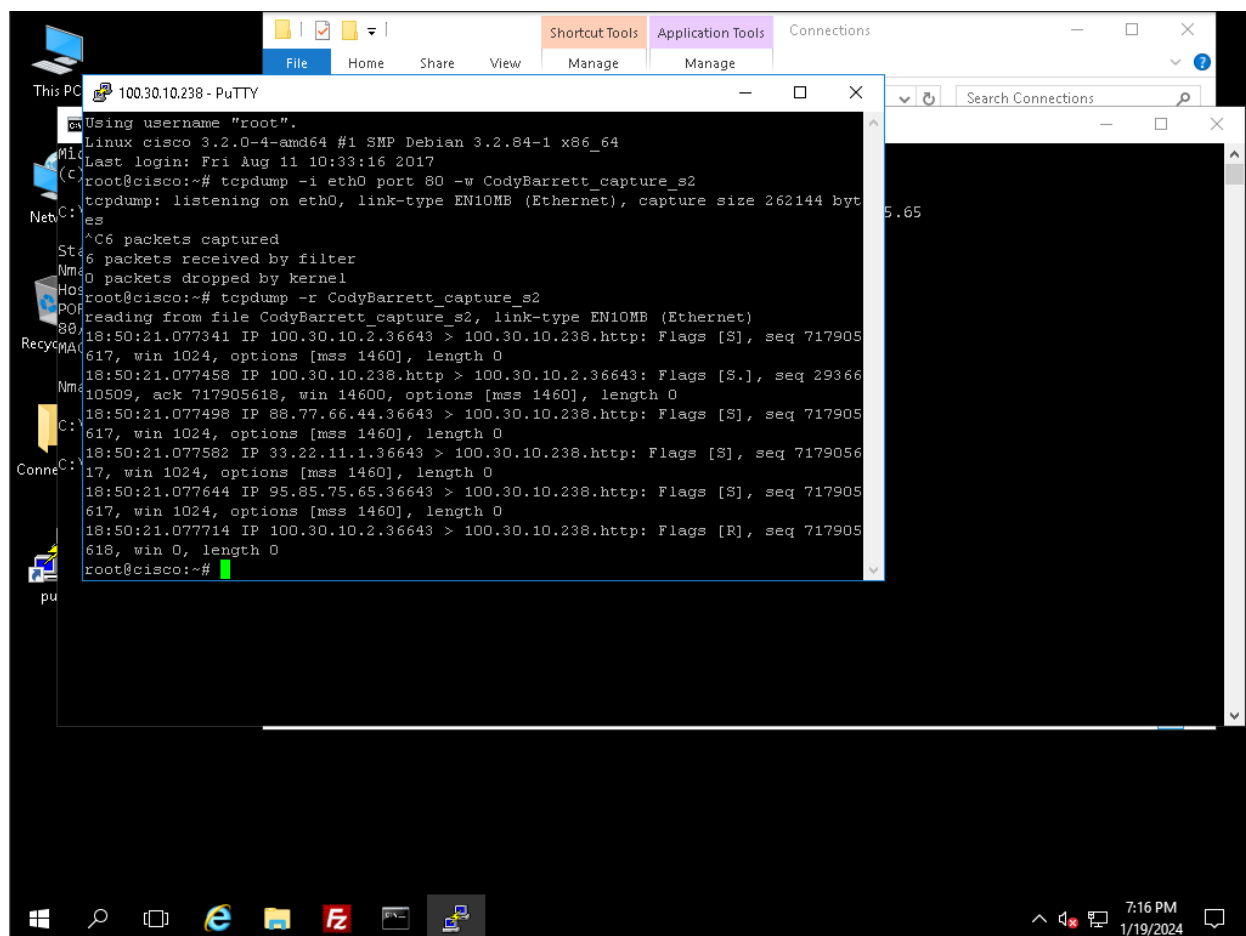


Ctrl+C is used to stop the tcpdump capture in the PuTTY CMD window.



```
100.30.10.238 - PuTTY
Using username "root".
Linux cisco 3.2.0-4-amd64 #1 SMP Debian 3.2.84-1 x86_64
Last login: Fri Aug 11 10:33:16 2017
root@cisco:~# tcpdump -i eth0 port 80 -w CodyBarrett_capture_s2
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C6 packets captured
6 packets received by filter
0 packets dropped by kernel
root@cisco:~# tcpdump -r CodyBarrett_capture_s2
reading from file CodyBarrett_capture_s2, link-type EN10MB (Ethernet)
```

To read the capture file, the command “tcpdump -r CodyBarrett\_capture\_s2” is used.



```
100.30.10.238 - PuTTY
Using username "root".
Linux cisco 3.2.0-4-amd64 #1 SMP Debian 3.2.84-1 x86_64
Last login: Fri Aug 11 10:33:16 2017
root@cisco:~# tcpdump -i eth0 port 80 -w CodyBarrett_capture_s2
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C6 packets captured
6 packets received by filter
0 packets dropped by kernel
root@cisco:~# tcpdump -r CodyBarrett_capture_s2
reading from file CodyBarrett_capture_s2, link-type EN10MB (Ethernet)
18:50:21.077341 IP 100.30.10.2.36643 > 100.30.10.238.http: Flags [S], seq 717905
617, win 1024, options [mss 1460], length 0
18:50:21.077458 IP 100.30.10.238.http > 100.30.10.2.36643: Flags [S.], seq 29366
10509, ack 717905618, win 14600, options [mss 1460], length 0
18:50:21.077498 IP 88.77.66.44.36643 > 100.30.10.238.http: Flags [S], seq 717905
617, win 1024, options [mss 1460], length 0
18:50:21.077582 IP 33.22.11.1.36643 > 100.30.10.238.http: Flags [S], seq 7179056
17, win 1024, options [mss 1460], length 0
18:50:21.077644 IP 95.85.75.65.36643 > 100.30.10.238.http: Flags [S], seq 717905
617, win 1024, options [mss 1460], length 0
18:50:21.077714 IP 100.30.10.2.36643 > 100.30.10.238.http: Flags [R], seq 717905
618, win 0, length 0
root@cisco:~#
```

Note the decoy IP addresses in the contents of the capture in the above screenshot.

The screenshot shows a Windows desktop environment. In the background, a File Explorer window is open, displaying the 'Connections' folder. In the foreground, an 'Administrator: Command Prompt' window is open, showing the output of an Nmap scan performed on the IP address 100.16.16.50. The scan results indicate that the host is up and running Microsoft Windows 2003. The Command Prompt window also shows the discovered open ports and the MAC address of the host.

```

Administrator: Command Prompt
Discovered open port 22/tcp on 100.16.16.50
Discovered open port 139/tcp on 100.16.16.50
Discovered open port 1027/tcp on 100.16.16.50
Completed SYN Stealth Scan at 19:40, 1.16s 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:AB:EC:7A (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=254 (Good luck!)
IP ID Sequence Generation: Incremental

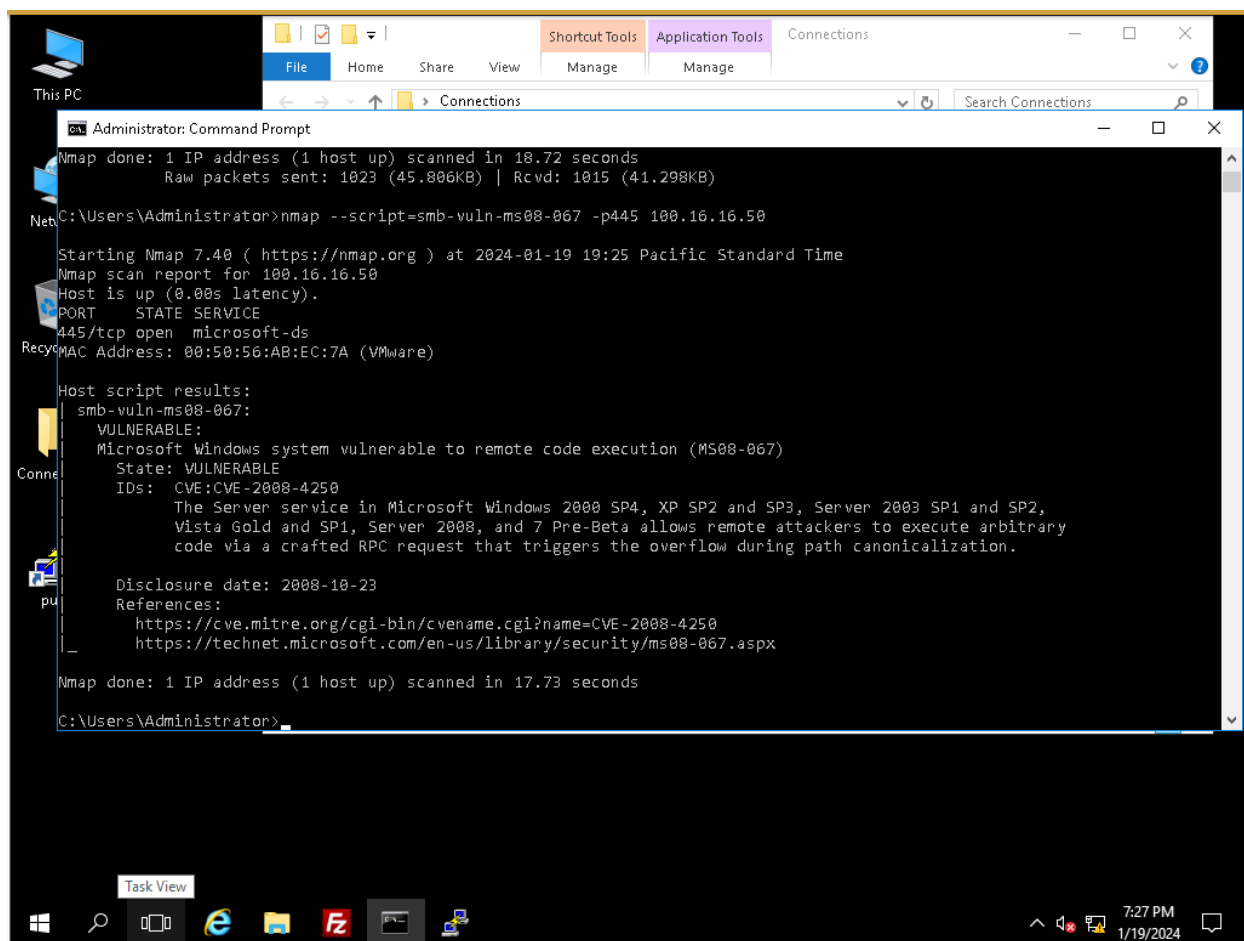
Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.47 seconds
Raw packets sent: 1098 (49.010KB) | Rcvd: 1017 (41.246KB)

C:\Users\Administrator>

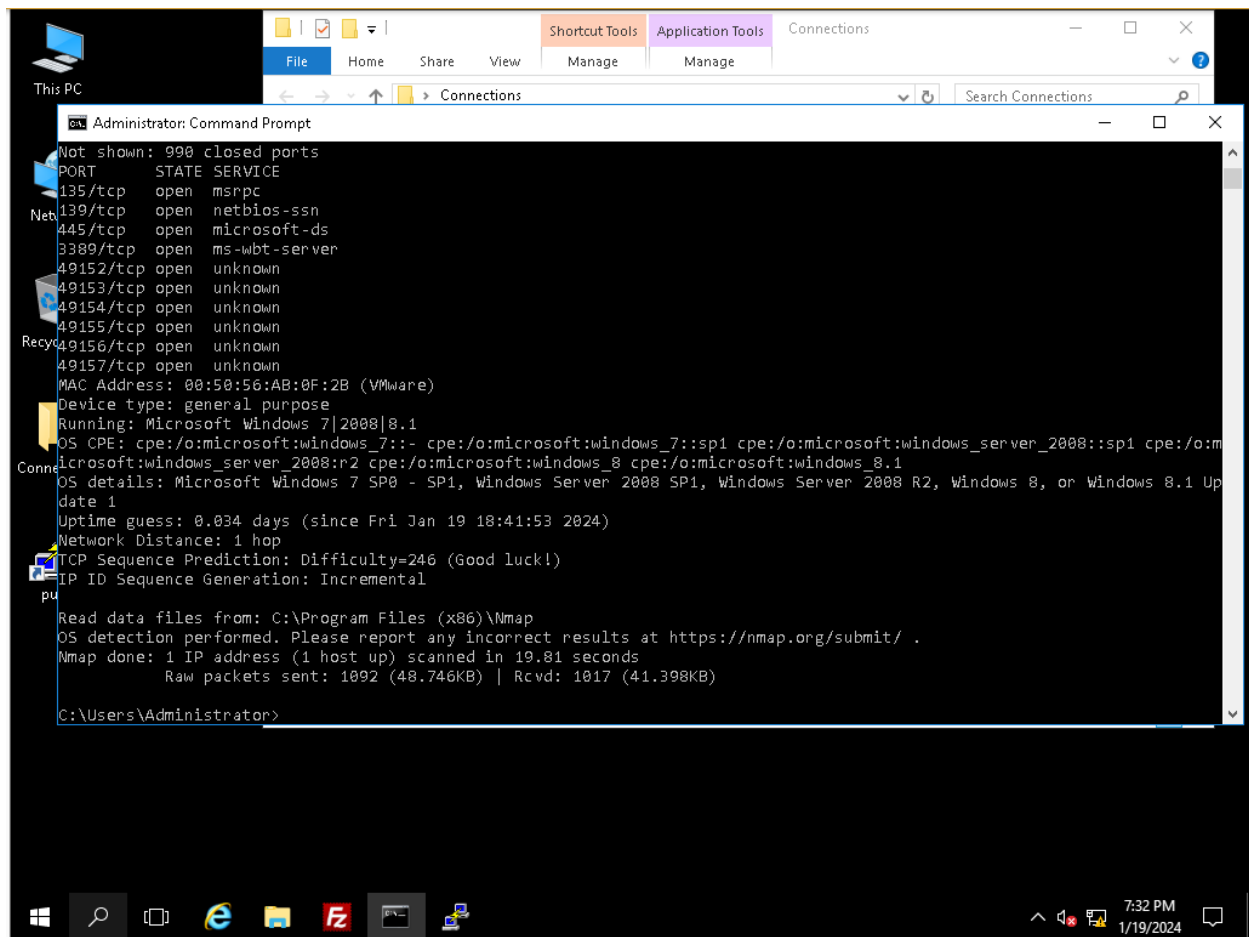
```

To detect the operating system of the target system the command “nmap -O -v 100.16.16.50” is used. Note that the operating system is Microsoft Windows 2003 based on the above screenshot.

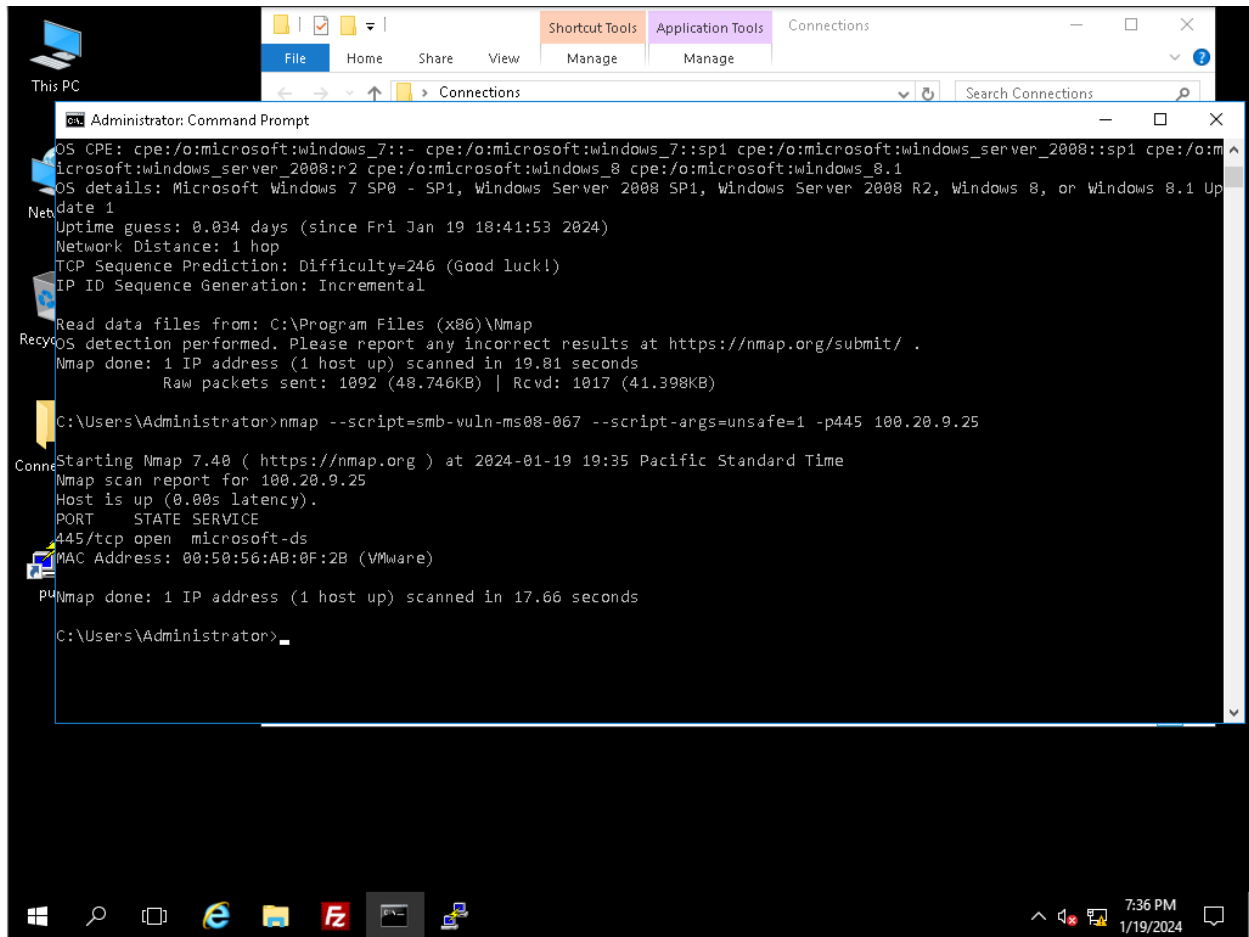




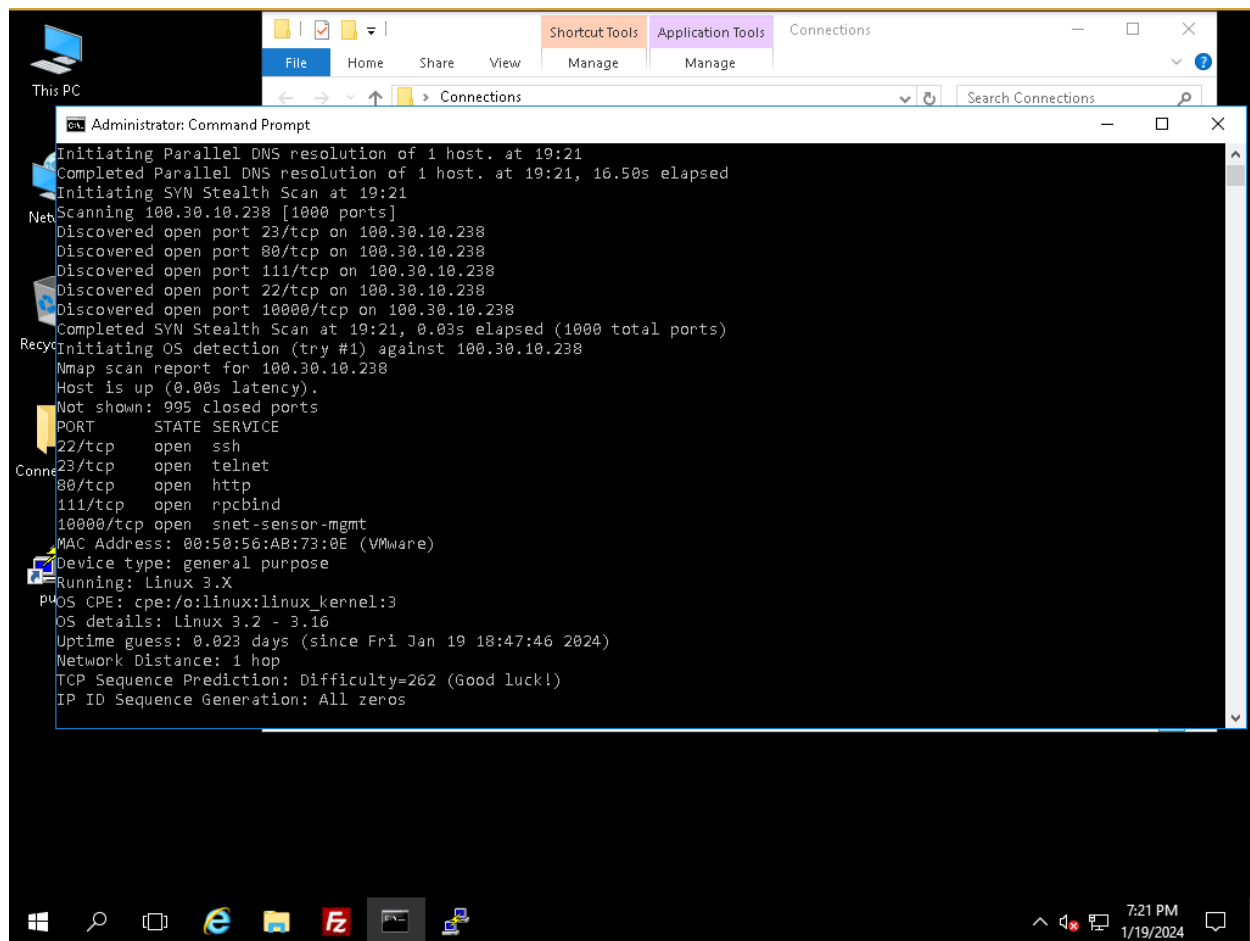
The command “`nmap --script=smb-vuln-ms08-067 -p445 100.16.16.50`” is used to use nmap to run a script file named `smb-vuln-ms08-067` to check port 445 for a vulnerability for an exploit titled MS08-067.



To find the operating system of TargetWindows04 the command “nmap -O -v 100.20.9.25” is used. The operating system is listed as Windows 7|2008|8.1



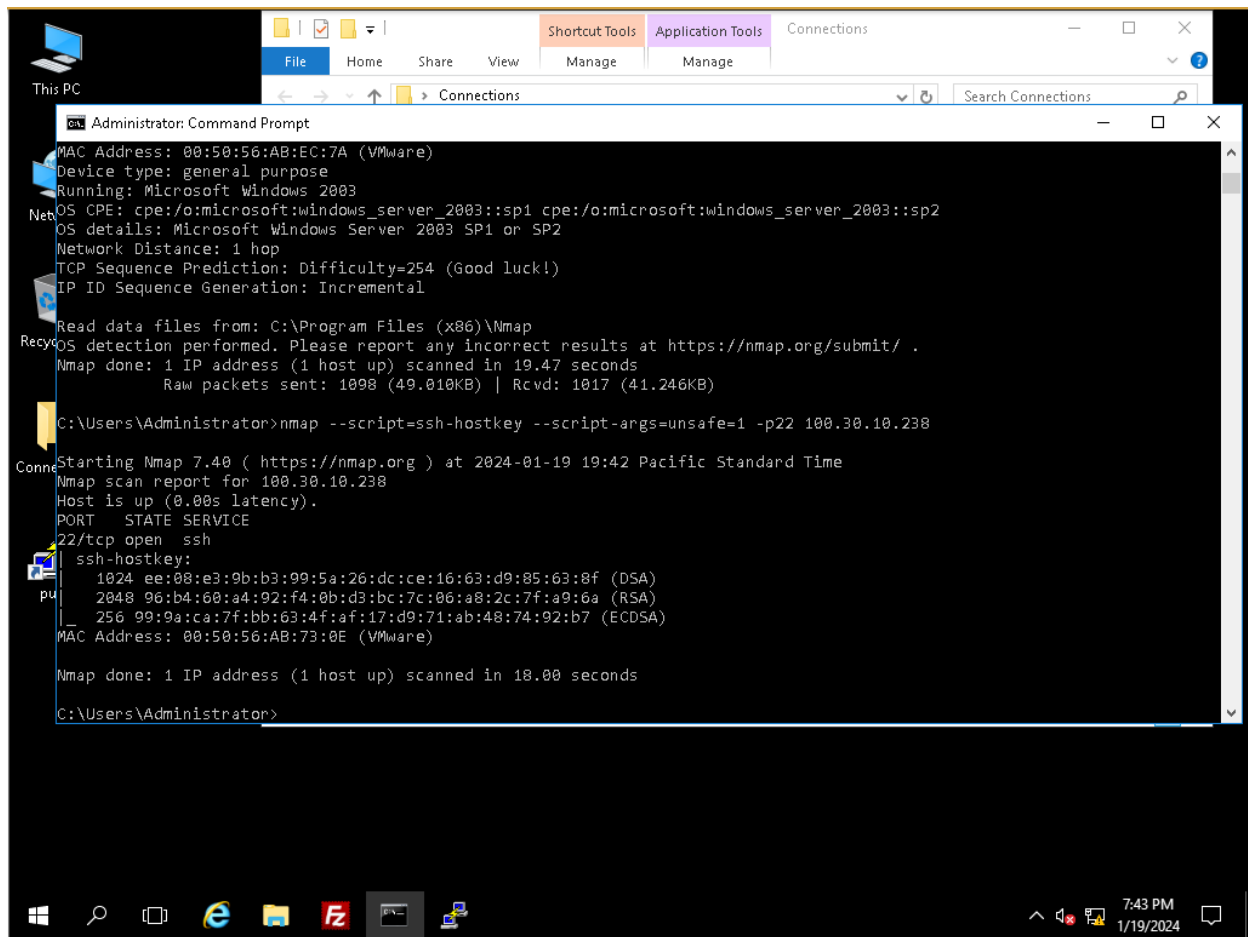
To run a similar SMB vulnerability check on port 445 for MS08-067 on TargetWindows04, the command “`nmap --script=smb-vuln-ms08-067 --script-args=unsafe=1 -p445 100.20.9.25`” This adds the argument to the script to add the unsafe flag.



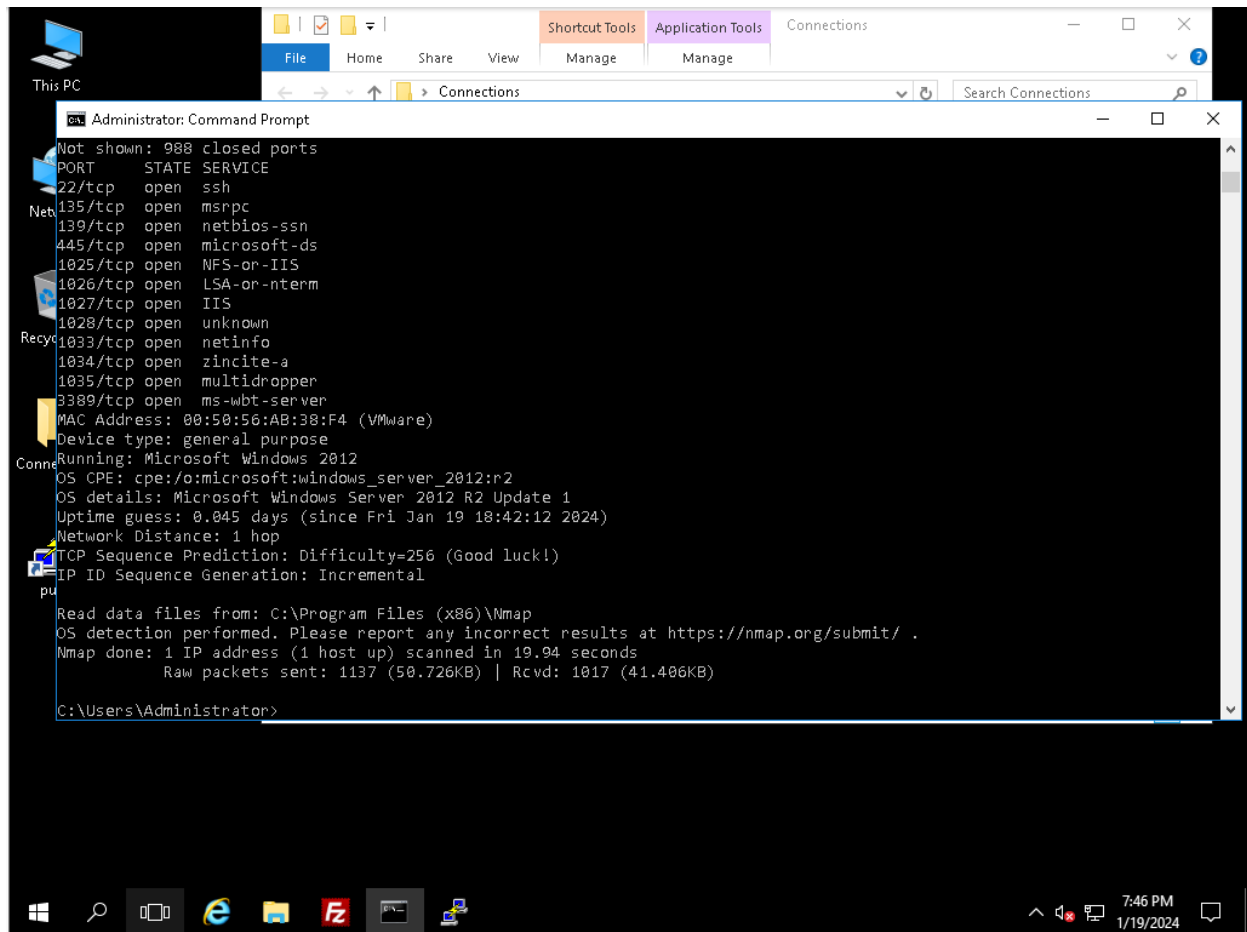
The screenshot shows a Windows desktop environment. In the background, a File Explorer window is open, displaying the 'Connections' folder. In the foreground, an 'Administrator: Command Prompt' window is open, showing the output of an Nmap scan. The scan results indicate that the target system is a Linux 3.X based system.

```
Administrator: Command Prompt
Initiating Parallel DNS resolution of 1 host. at 19:21
Completed Parallel DNS resolution of 1 host. at 19:21, 16.50s elapsed
Initiating SYN Stealth Scan at 19:21
Scanning 100.30.10.238 [1000 ports]
Discovered open port 23/tcp on 100.30.10.238
Discovered open port 80/tcp on 100.30.10.238
Discovered open port 111/tcp on 100.30.10.238
Discovered open port 22/tcp on 100.30.10.238
Discovered open port 10000/tcp on 100.30.10.238
Completed SYN Stealth Scan at 19:21, 0.03s elapsed (1000 total ports)
Initiating OS detection (try #1) against 100.30.10.238
Nmap scan report for 100.30.10.238
Host is up (0.00s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
111/tcp   open  rpcbind
10000/tcp open  snet-sensor-mgmt
MAC Address: 00:50:56:AB:73:0E (VMware)
Device type: general purpose
Running: Linux 3.X
P4OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Uptime guess: 0.023 days (since Fri Jan 19 18:47:46 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
```

To detect the operating system of the target system the command “nmap -O -v 100.30.10.238” is used. Note that the operating system is Linux 3.X based on the above screenshot.



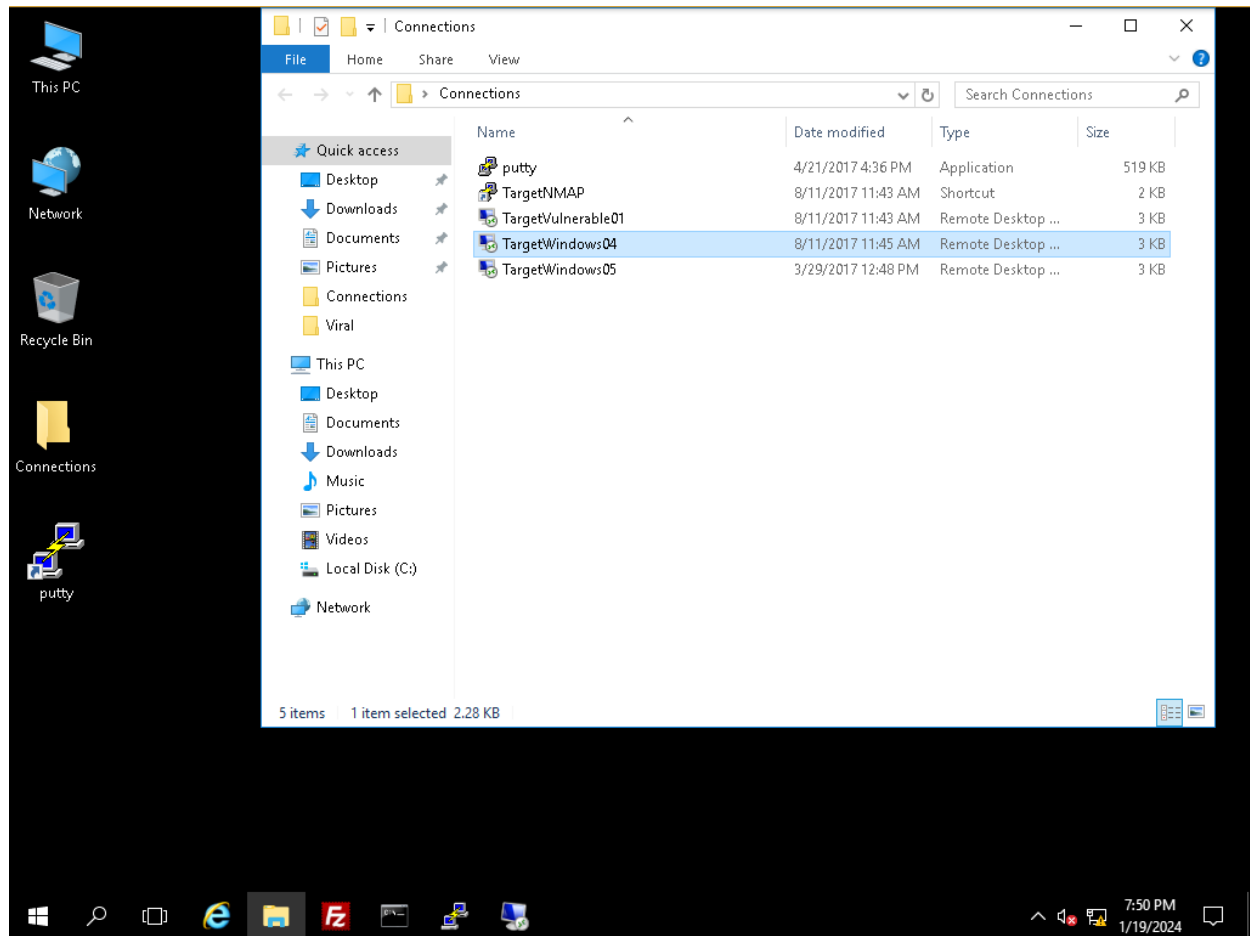
To check for a ssh vulnerability named hostkey on port 22 with an unsafe flag, the script ssh-hostkey is ran with the command “nmap –script=ssh-hostkey –script-args=unsafe=1 -p22 100.30.10.238”



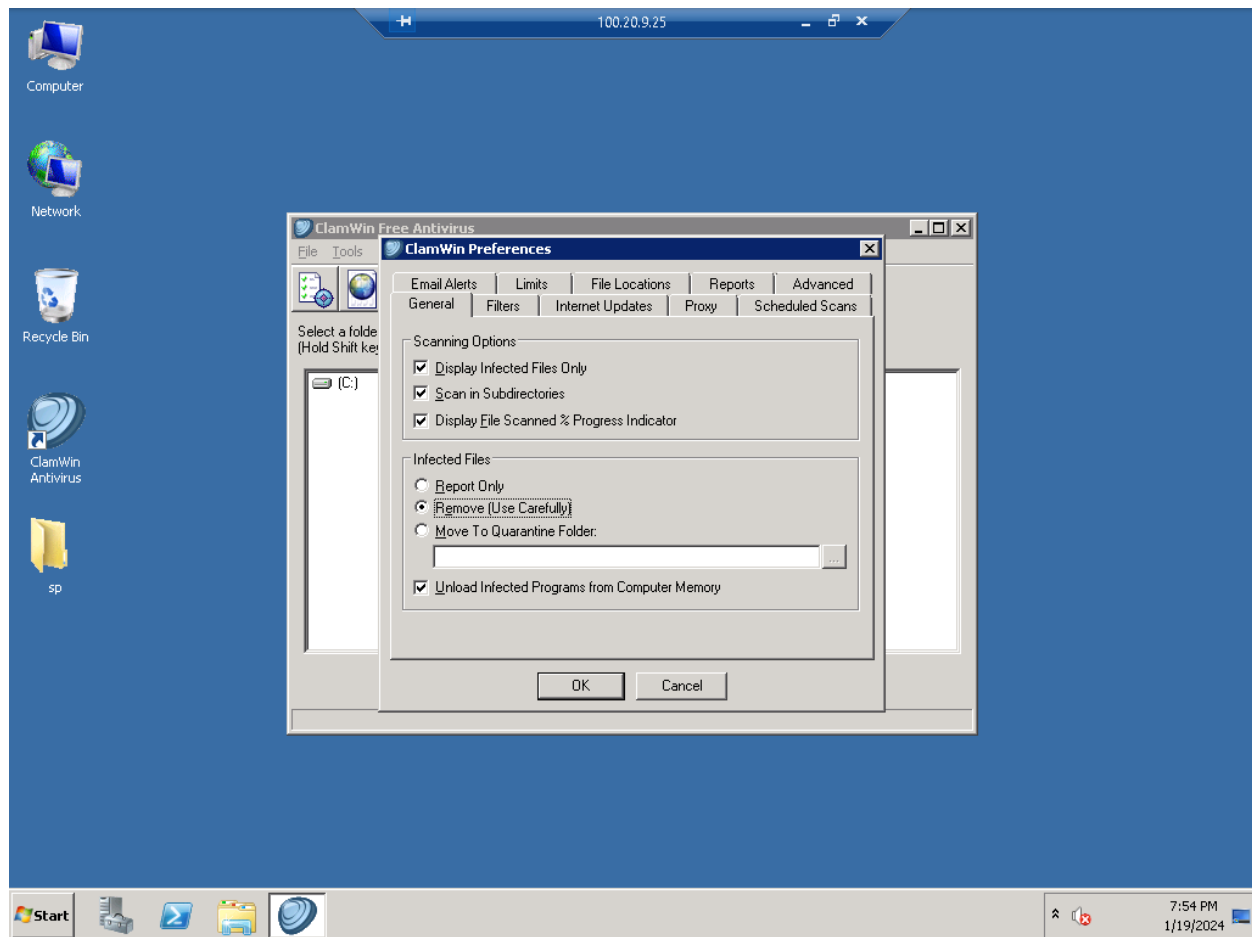
To view TargetWindows05's operating system, the command "nmap -O -v 172.30.0.31" is used.

The scan shows that the OS is Microsoft Windows Server 2012 R2 Update 1.

## Part 2: Clean Vulnerable Systems

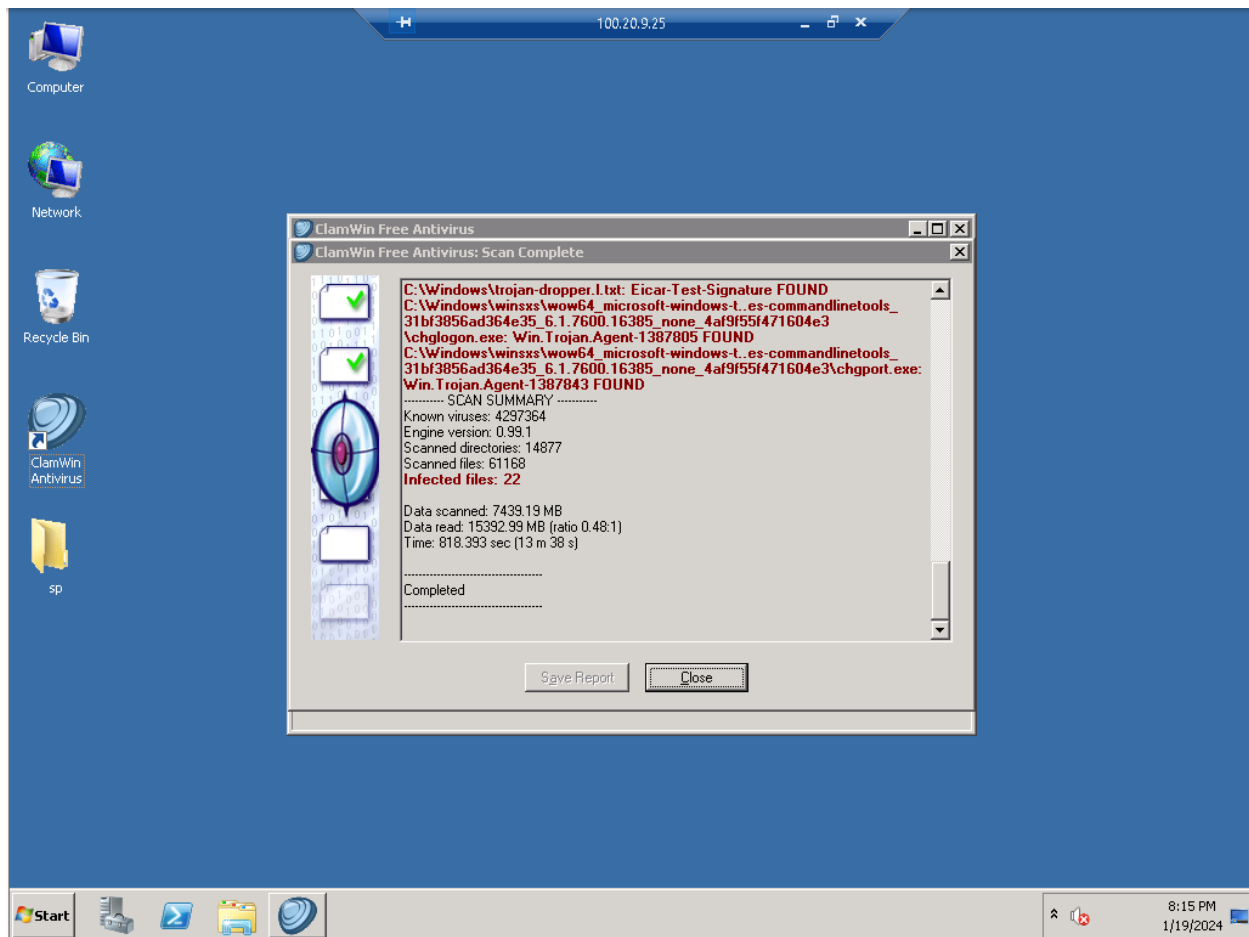


To open a connection to TargetWindows04, double-click the shortcut in the Connections folder.

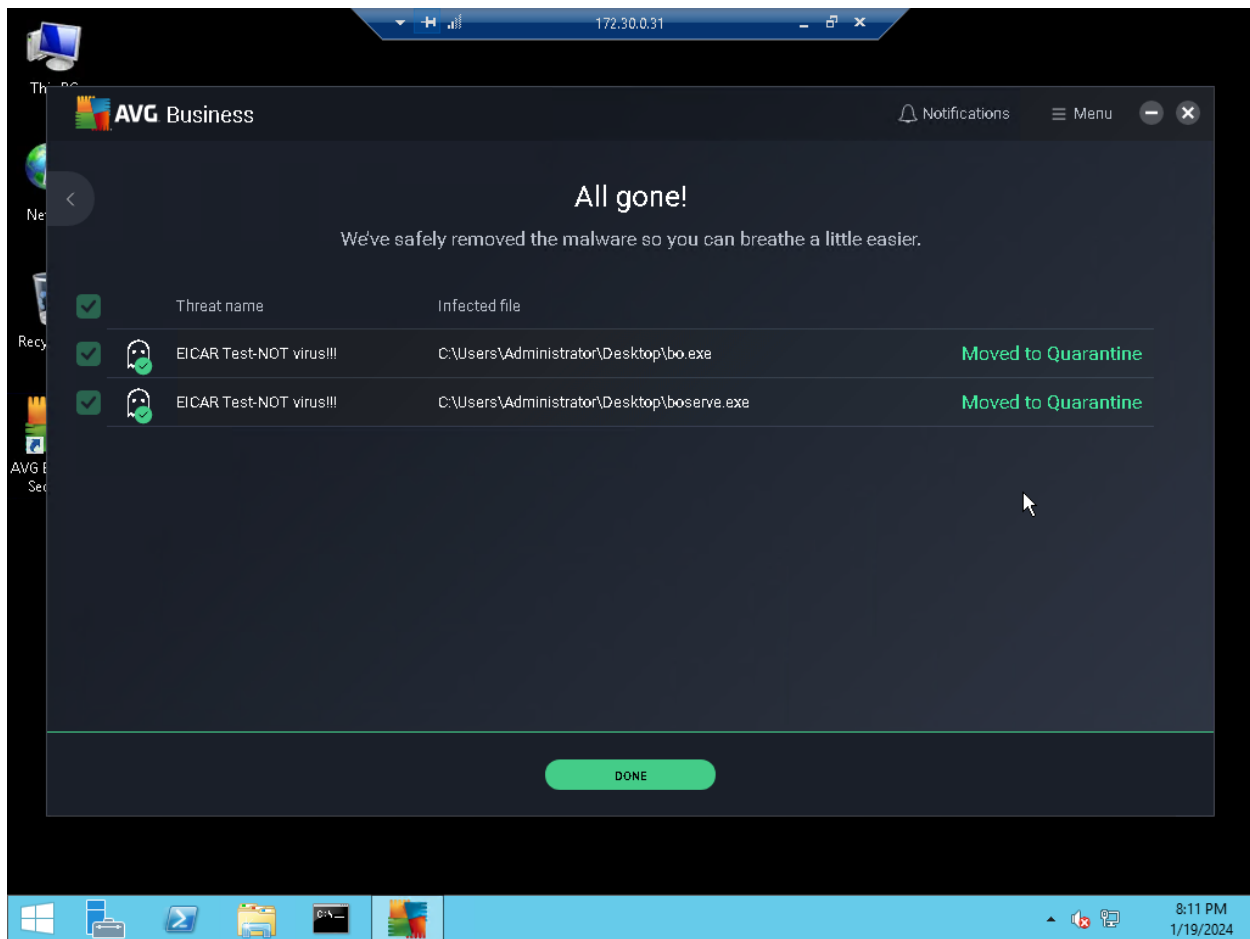


In ClamWin Antivirus select “Remove (Use Carefully)” under Tools > Preferences and click “OK”. Then click scan to scan the :C drive.



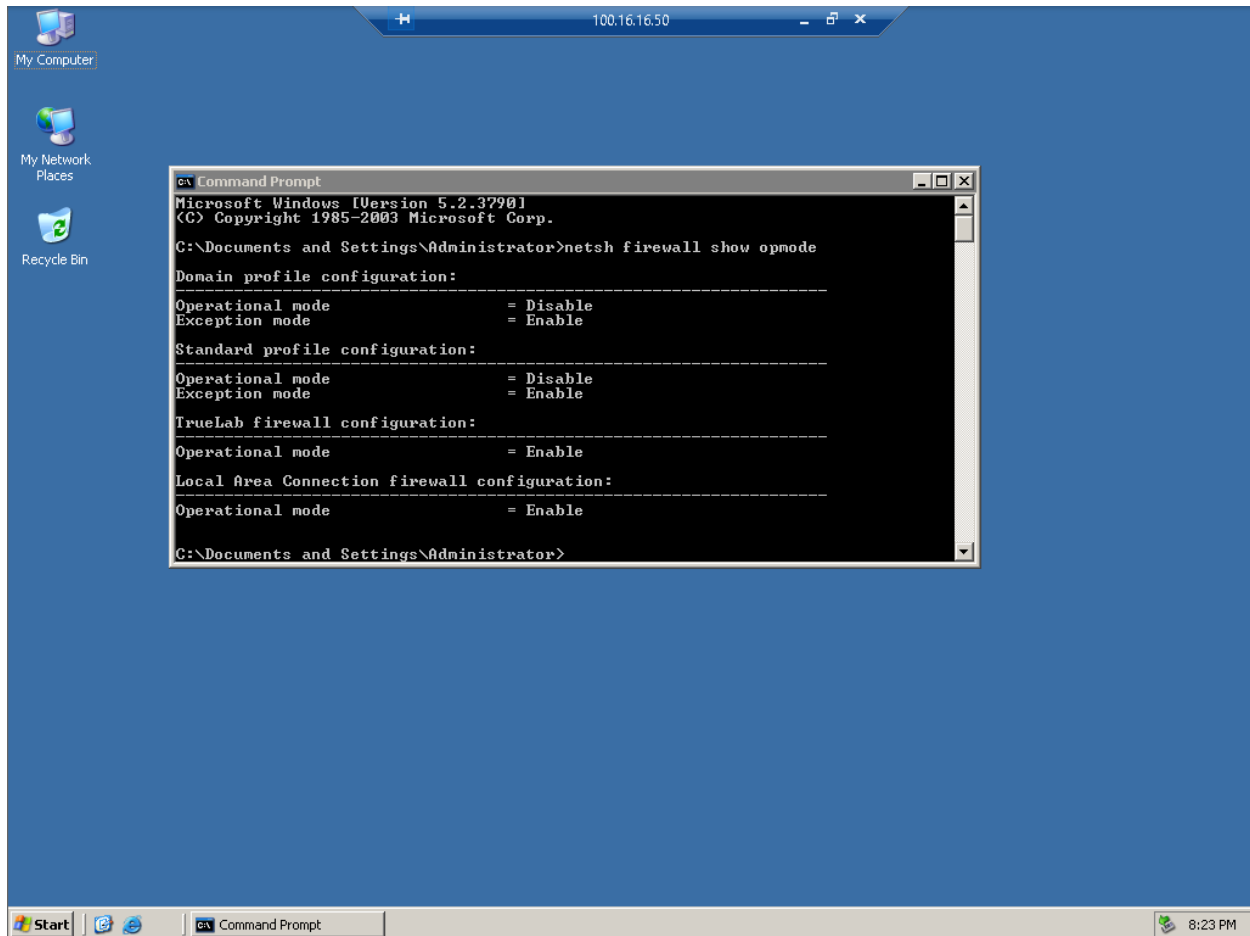


Above are the results of the ClamWin Antivirus scan. This shows that 22 infected files were found and removed.

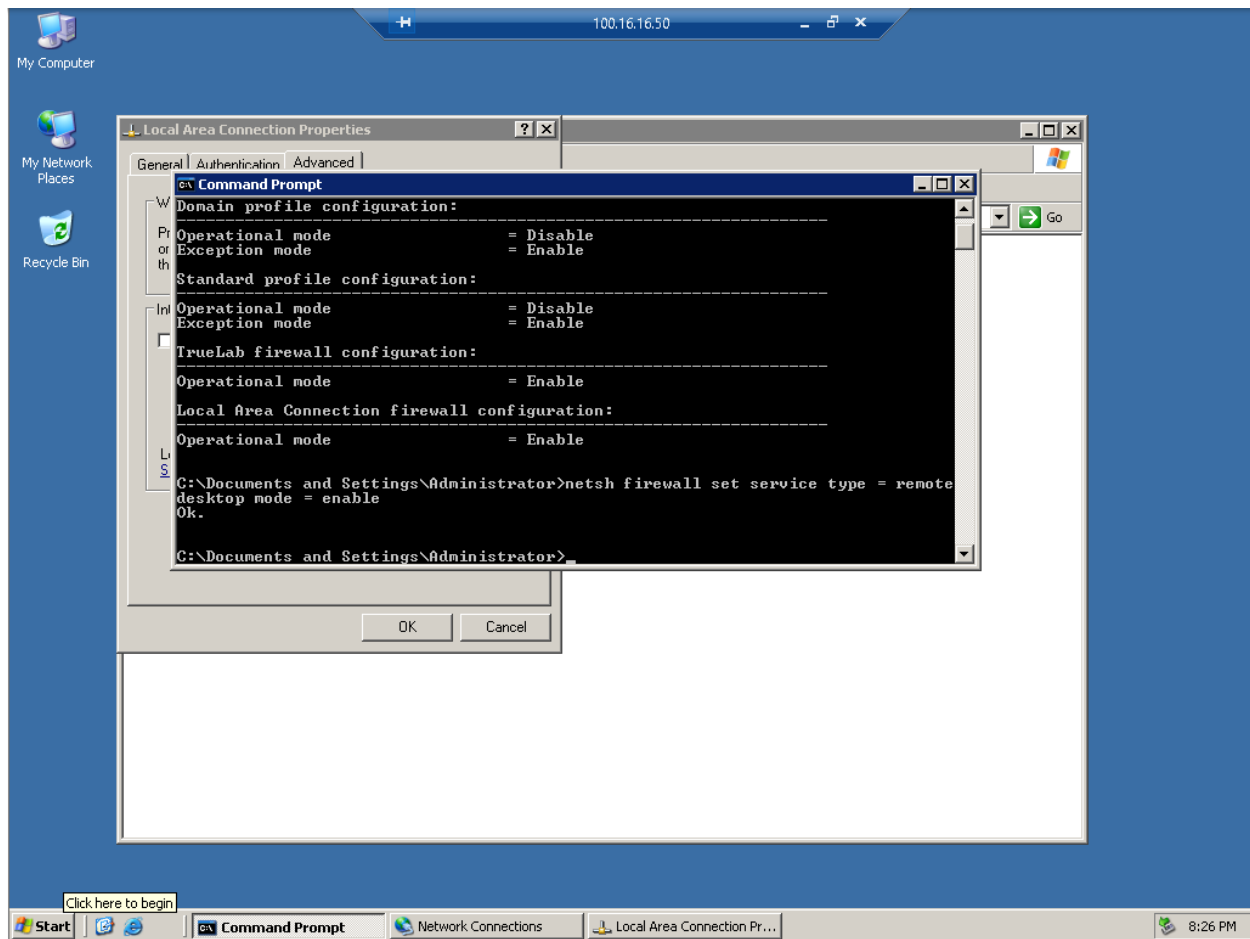


On TargetWindows05 Launch AVG, click the “Turn On” button and perform a scan on the folder C:\Users\Administrator\Desktop. The above are the results of the scan where the threat named “EICAR Test-NOT virus!!!” was found.

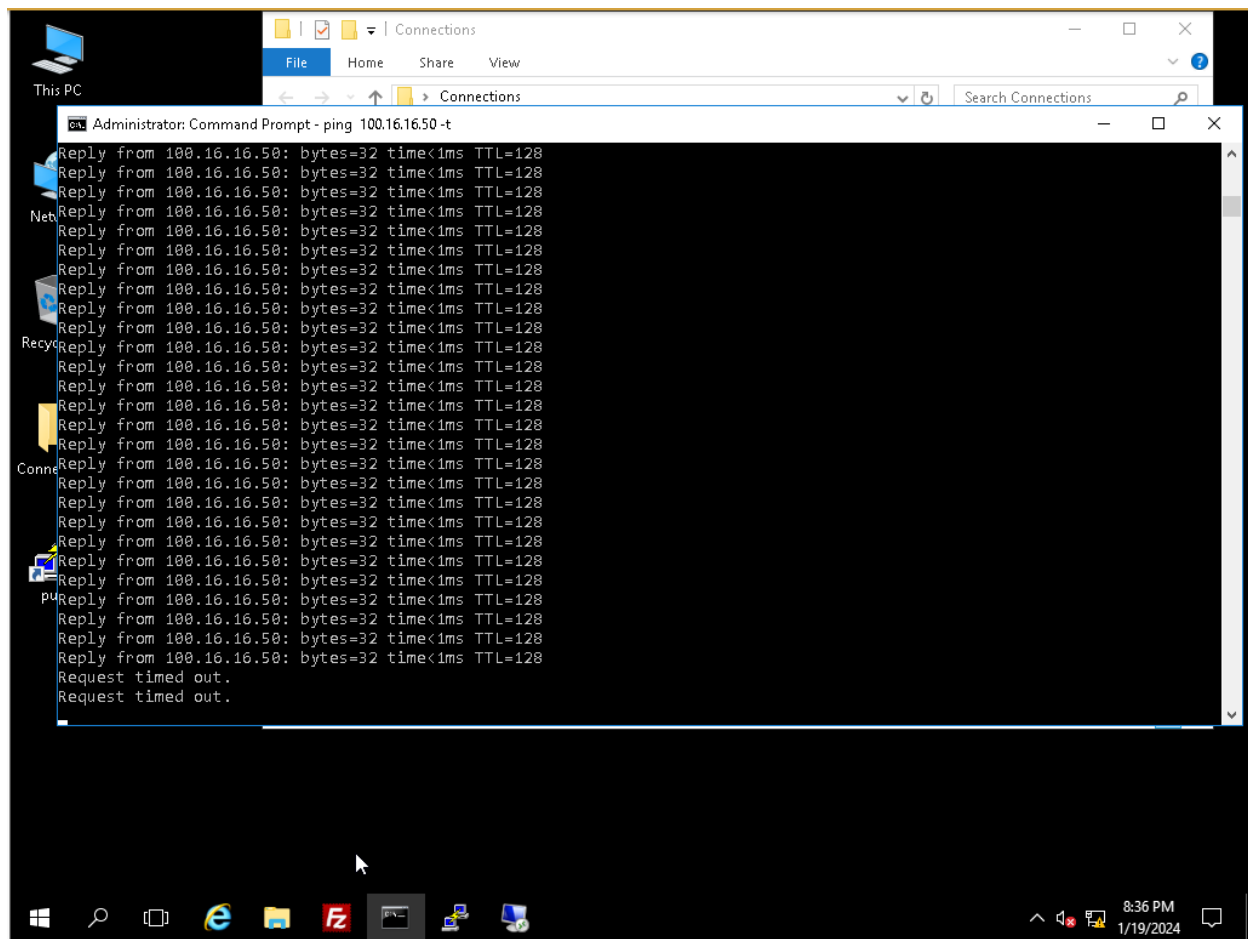
### Part 3: Reduce the Attack Surface on the Windows 2003 Server



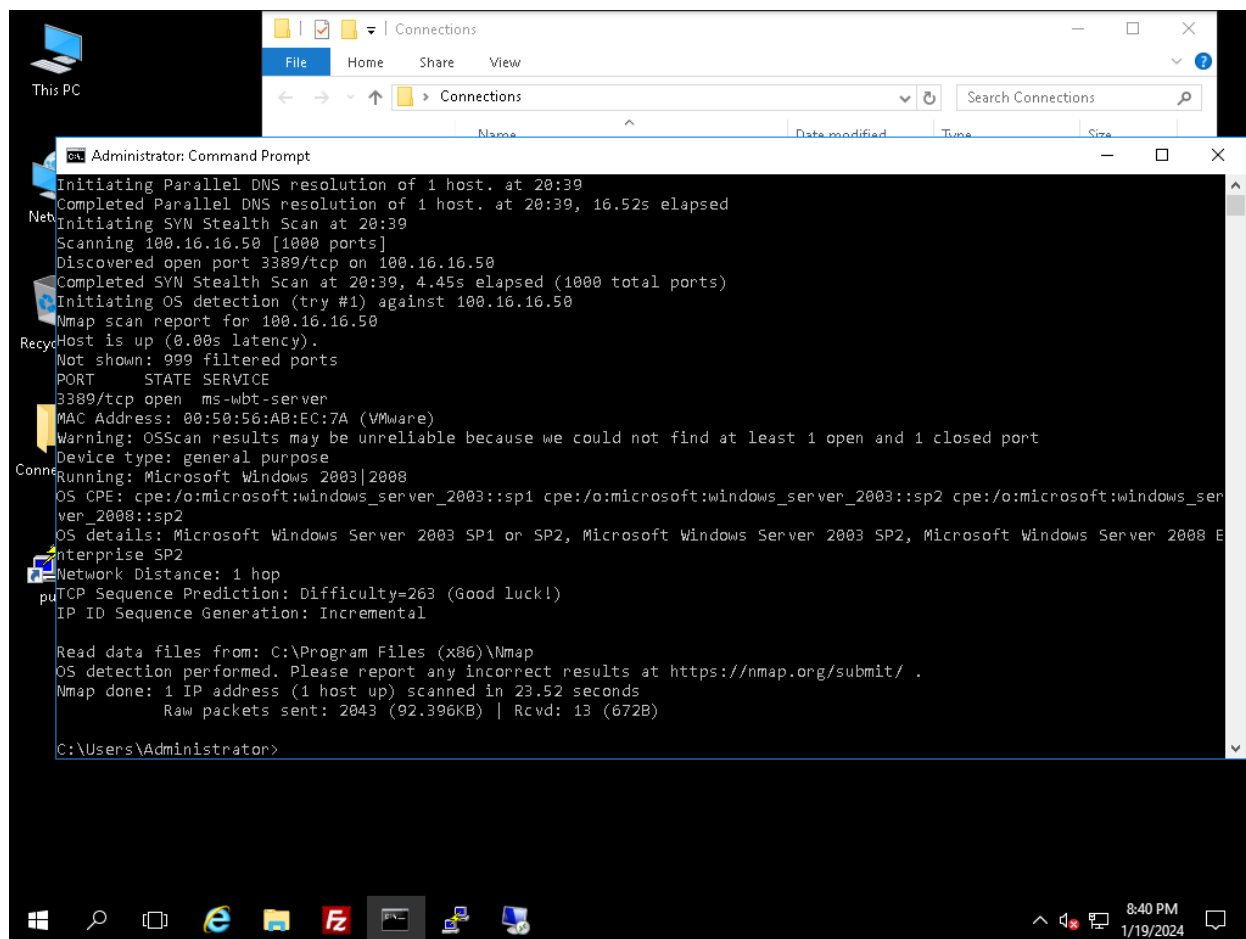
The command “netsh firewall show opmode” is used in CMD on TargetWindows01 to show firewall profile settings.



To allow Remote Desktop to travel through the firewall use the command “netsh firewall set service type = remotedesktop mode = enable” and then to continuously ping TargetVulnerable01 from the vWorkstation system use the command “ping 100.16.16.50 -t”



After enabling firewall rules, the request from vWorkstation pinging TargetVulnerable01 has timed out.



The command “nmap -O -v 100.16.16.50” is used to scan for the operating system of TargetVulnerable01.

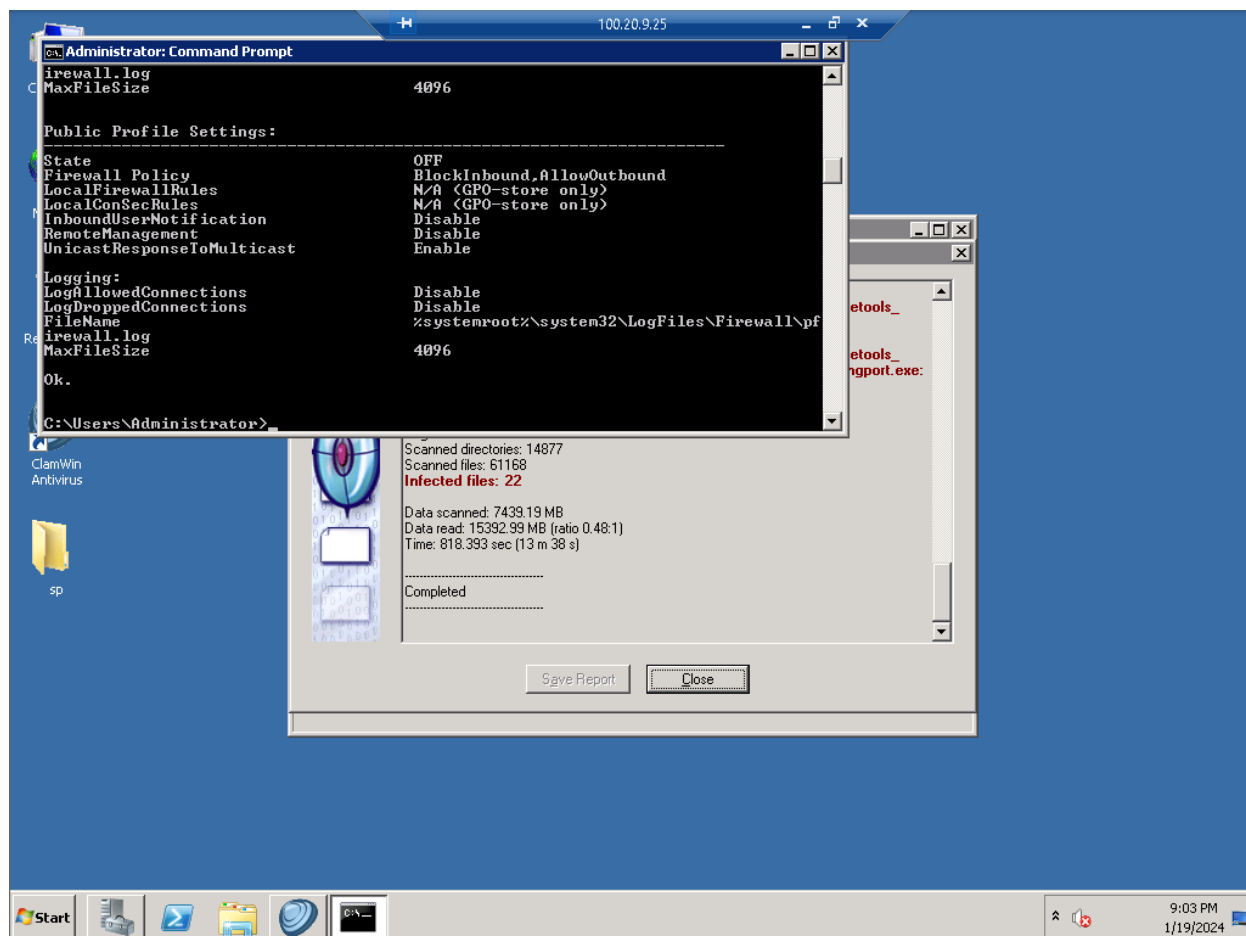
Comparison of the two nmap scans.

The first Nmap scan of the system 100.16.16.50 was prior to the reduction of attack surface on the system. In the first scan we were able to see that a number of ports are open including 22/ssh, 135/msrpc, 139/netbios-ssn, 445/Microsoft-ds, 1027/IIS, and 3389/ms-wbt-server. Additionally, we were able to see that the OS was Microsoft Windows 2003 SP1 or SP2. In the second Nmap scan we saw that the only open port remaining was 389/ms-wbt-server. This shows that the steps taken to reduce the attack surface via the firewall were effective in removing access to the

previously opened ports by vWorkstation. This likely explains the differences behind the scans.

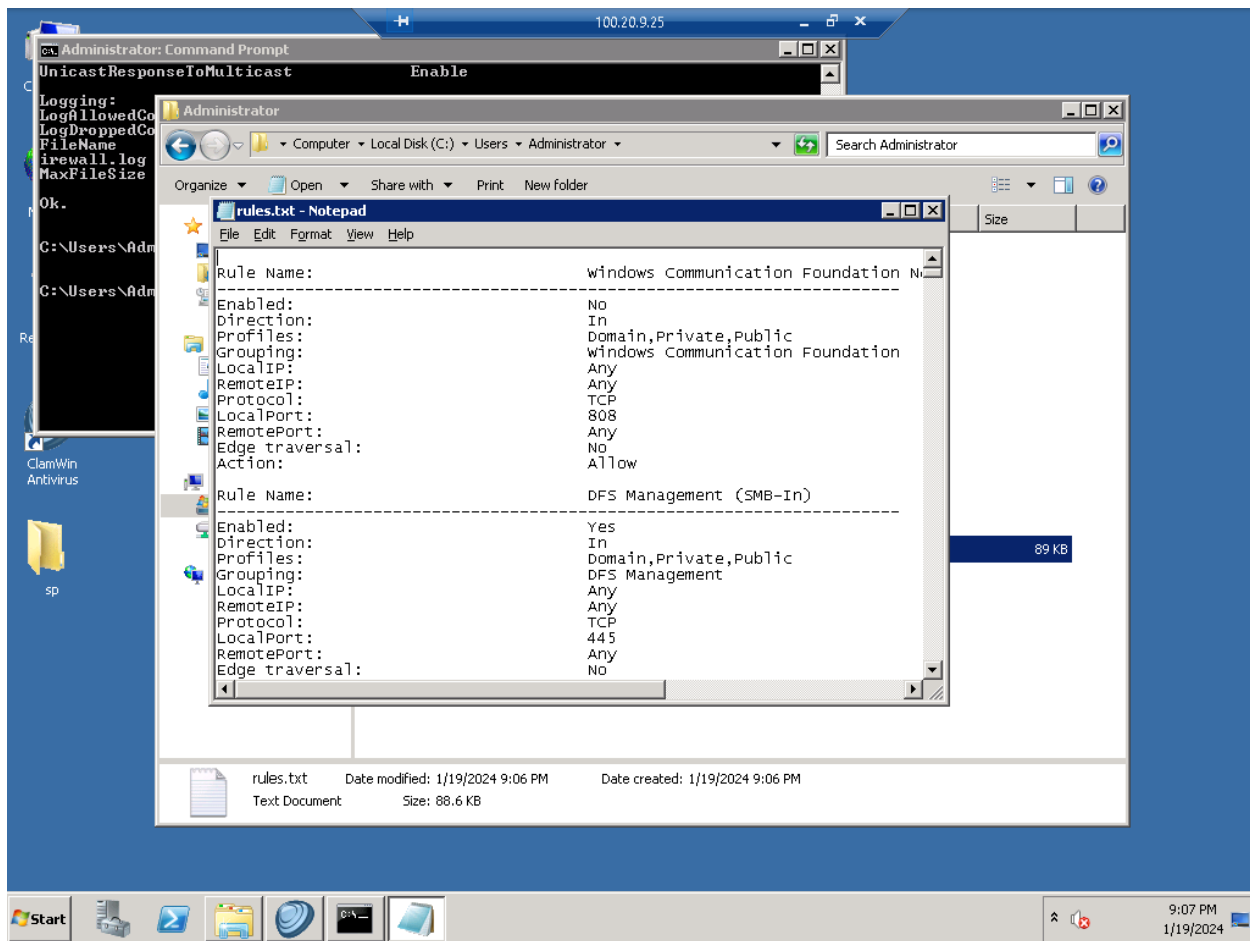
We also see in the second scan that the OS details changed to say “Microsoft Windows Server 2003 SP1 or SP2, Microsoft Windows Server 2003 SP2, Microsoft Windows Server 2008 Enterprise SP2”. This change could be due to the way that Nmap gathers and reports information due to the now inaccessible ports.

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

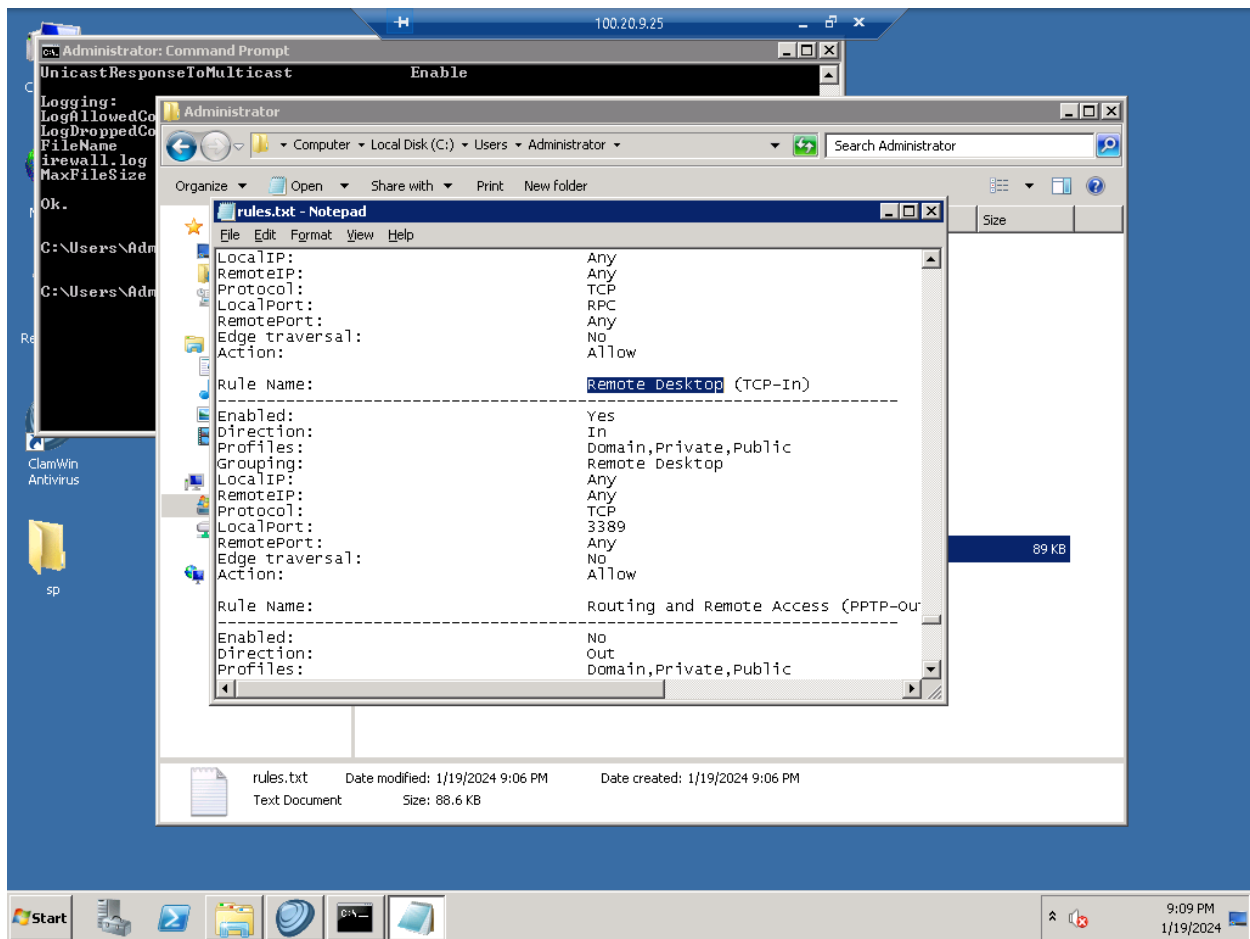


The command “`netsh -r WIN-IKTLR0P6DID advfirewall show allprofiles`” is used to show the systems firewall profiles.

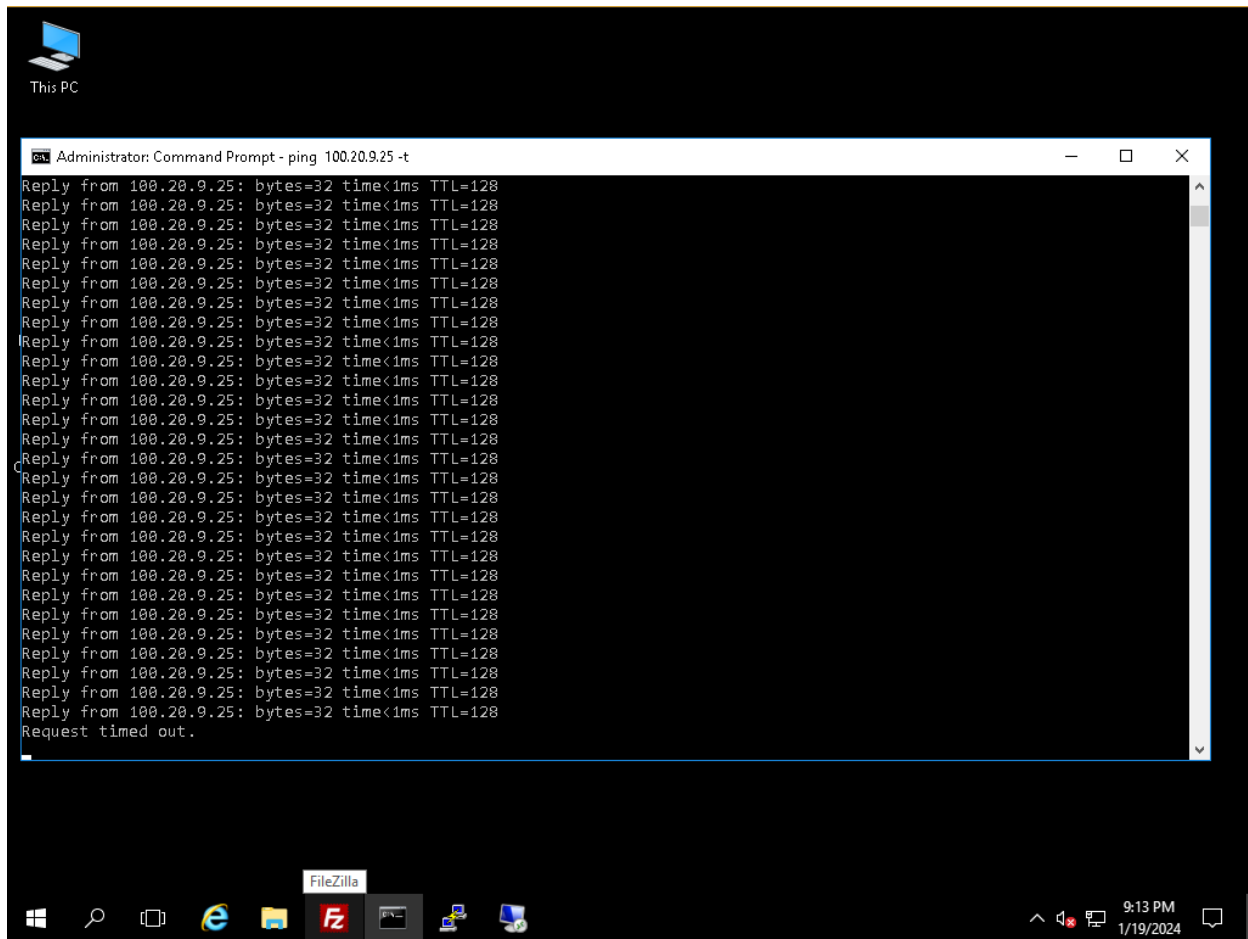




Above are the firewall rules output from the command “netsh advfirewall firewall show rule name=all > rule.txt”



Above is the remote desktop rule.



The above screenshot shows the ping being interrupted from vWorkstation to TargetWindows04 after blocking ICMP V4 on TargetWindows04.

```

Administrator: Command Prompt
Net
Discovered open port 445/tcp on 100.20.9.25
Discovered open port 135/tcp on 100.20.9.25
Discovered open port 49154/tcp on 100.20.9.25
Completed SYN Stealth Scan at 21:15, 12.23s elapsed (1000 total ports)
Initiating OS detection (try #1) against 100.20.9.25
Nmap scan report for 100.20.9.25
Host is up (0.00s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49154/tcp open  unknown
Connection: 00:50:56:AB:0F:2B (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Win
dows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 R1, Microsoft Windows Pho
ne 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, W
indows 7 SP1, or Windows Server 2008
Uptime guess: 0.107 days (since Fri Jan 19 18:41:53 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (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 31.41 seconds
Raw packets sent: 3045 (136.532KB) | Rcvd: 21 (996B)

C:\Users\Administrator>

```

Above is the new Nmap scan results with the Reduced Attack Surface on the Windows 2008 Server.

Comparison of the two nmap scans.

In the first Nmap scan for system 100.20.9.25 there are a larger number of open ports. The ports listed in the scan are 135/msrpc, 139/netbios-ssn, 445/Microsoft-ds, 3389/ms-wbt-server, 49152/unknown, 49153/unknown, 49154/unknown, 49155/unknown, 49156/unknown, and 49157/unknown. After reducing the attack surface, the only unknown port that remains open is 49154/unknown. The other ports with known services are all still open other than 139/netbios-ssn. It seems that blocking ICMP V4 disabled access to the previous ports via the firewall.

Another difference amongst the scans is in the first Nmap scan, the OS details are listed as “Microsoft Windows 7 SP0 – SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1”, but in the second scan the OS details are “Microsoft Windows Server 2008 or 2008 Beta3, Microsoft Windows server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 R1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1 or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008”. This shows that there are many more possible options for what the OS could be. This makes it considerably harder to find which exploits this system is vulnerable to.

Remediation of a vulnerable system.

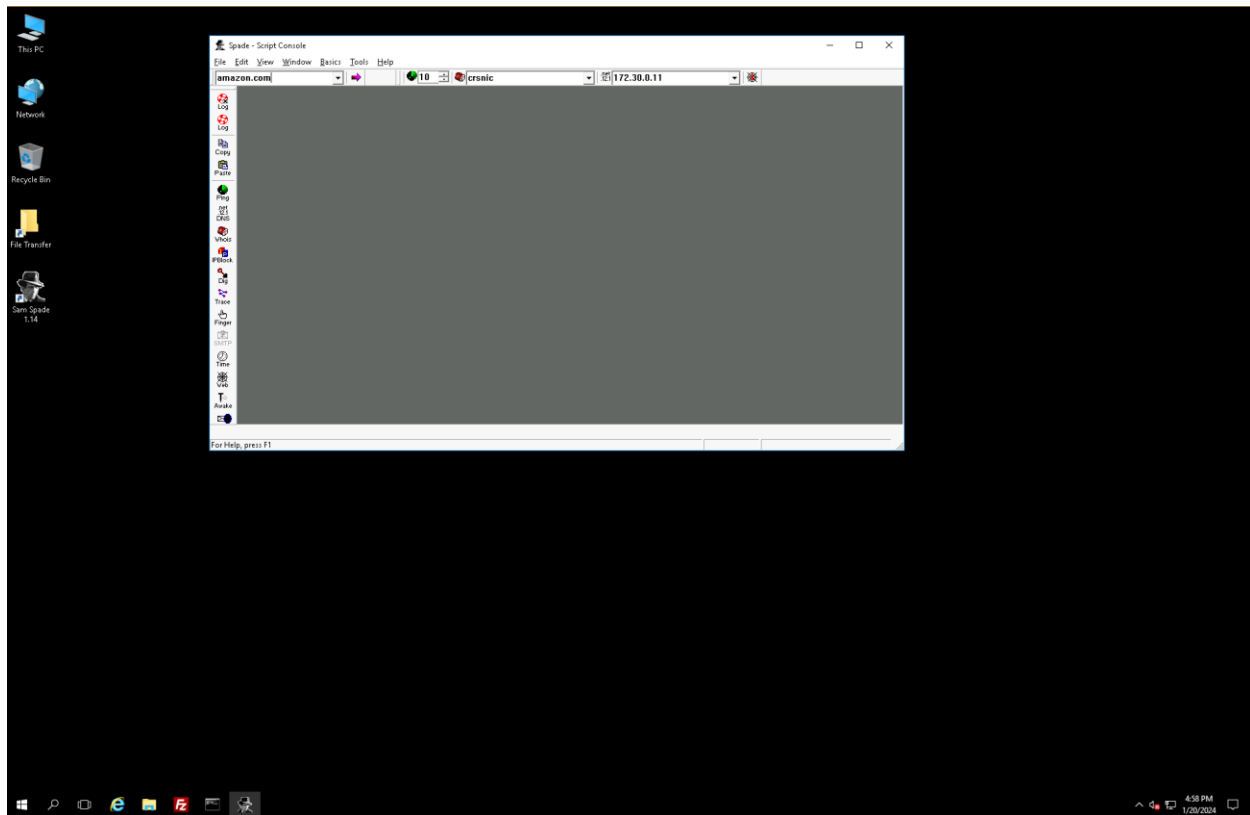
To remediate a vulnerable system the first step is to run a scan for viruses using antivirus software. This will find and remove any malware found on the system. Next is to update to the most recent security patch. The following step is to disable any unnecessary services and disable any unnecessary ports so that they cannot be used by attackers to access the machine. Next is to restrict access to users so that only necessary access is held by user accounts. Lastly, access controls should be implemented for all files and directories. In this lab the remediation steps that were followed were to scan for malware with an antivirus, and to disable unnecessary services. Some additional considerations could be to create a regular patch management system in order to stay up to date with the latest security patches. Additionally, the network could be segmented in order to harden the network. This can be done in a number of ways including physical

segmentation and VLANs. Another consideration would be to add an IDS (intrusion Detection System) to the network so that attacks can be detected. It is also important to keep all sensitive data backed up in case of loss or breach of integrity.



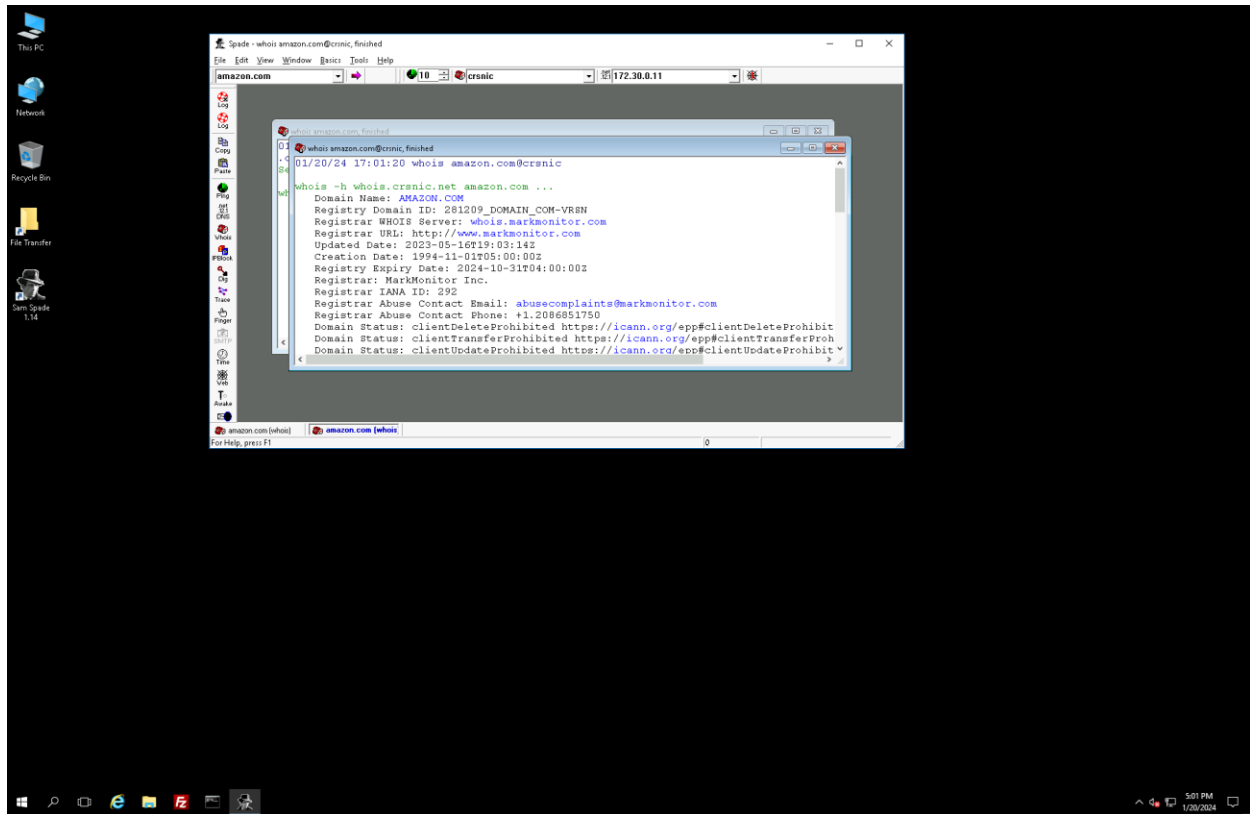
## Lab 2: Data Gathering and Footprinting on a Targeted Web Site

### Part 1: Technical Research

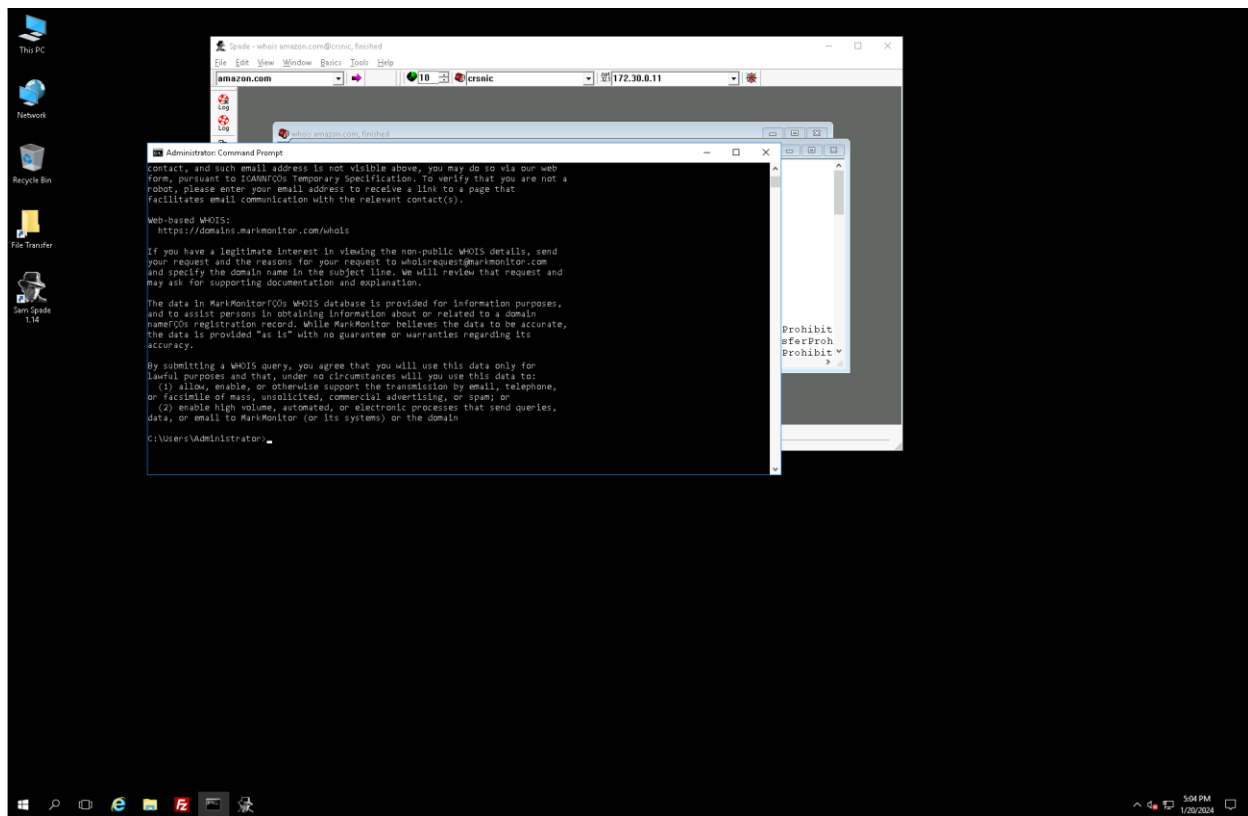


Using the Sam Spade application, the website amazon.com was entered into the search field.





The above screenshot shows the result of selecting Basics > Whois following the search. This shows information about the owner of the domain ‘amazon.com’.



Via CMD the command “whois amazon.com” was entered to find similar information via the command line rather than an external application.

```

Spade - whois amazon.com@crnic, finished
amazon.com - 172.30.0.11
whois -h whois.crnic.net amazon.com ...
Domain Name: AMAZON.COM
Registry Domain ID: 281209 DOMAIN COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2025-05-16T19:03:14Z
Creation Date: 1994-11-01T05:00:00Z
Registry Expiry Date: 2024-10-31T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.AMZNDNS.CO.UK
Name Server: NS1.AMZNDNS.COM
Name Server: NS1.AMZNDNS.NET
Name Server: NS1.AMZNDNS.ORG
Name Server: NS2.AMZNDNS.CO.UK
Name Server: NS2.AMZNDNS.COM
Name Server: NS2.AMZNDNS.NET
Name Server: NS2.AMZNDNS.ORG
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-01-21T01:00:25Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' (VeriSign) Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
<<<

amazon.com@crnic:~$ whois amazon.com
Domain Name: amazon.com
Registry Domain ID: 281209 DOMAIN COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2025-05-16T19:03:14Z
Creation Date: 1994-11-01T05:00:00Z
Registry Expiry Date: 2024-10-31T04:00:00Z
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Registry Registrant ID:
Registrant Name: Hostmaster, Amazon Legal Dept.
Registrant Organization: Amazon Technologies, Inc.
Registrant Street: P.O. Box 8102
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89507
Registrant Country: US
Registrant Phone: +1.2082664804
Registrant Fax: +1.2082667018
Registrant Fax Ext:
Registrant Email: hostmaster@amazon.com
Registry Admin ID:
Admin Name: Hostmaster, Amazon Legal Dept.
Admin Organization: Amazon Technologies, Inc.
Admin Street: P.O. Box 8102
Admin City: Reno
Admin State/Province: NV
Admin Postal Code: 89507
Admin Country: US
Admin Phone: +1.2082664804
Admin Phone Ext:
Admin Fax: +1.2082667018
Admin Fax Ext:
Admin Email: hostmaster@amazon.com
Registry Tech ID:
Tech Name: Hostmaster, Amazon Legal Dept.
Tech Organization: Amazon Technologies, Inc.
Tech Street: P.O. Box 8102
Tech City: Reno
Tech State/Province: NV
Tech Postal Code: 89507
Tech Country: US
Tech Phone: +1.2082664804
Tech Phone Ext:
Tech Fax: +1.2082667018
Tech Fax Ext:
Tech Email: hostmaster@amazon.com
Name Server: ns1.amzndns.net
Name Server: ns1.amzndns.org
Name Server: ns2.amzndns.com
Name Server: ns2.amzndns.org
Name Server: ns2.amzndns.net
Name Server: ns1.amzndns.com
Name Server: ns2.amzndns.co.uk
DNSSEC: unsigned
URL of the ICANN Whois Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-01-21T00:56:30+0000 <<<

For more information on WHOIS status codes, please visit:
https://www.icann.org/resources/pages/epp-status-codes
  
```

Comparing the information offered by both searches shows similar information, however it seems that using the command line shows more information.

Above is the result of running a traceroute scan on amazon.com via Same Spade. The results were saved to the desktop under traceroute\_amazon.

```

Administrator Command Prompt - tracert amazon.com
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-01-21T00:56:38+0000 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain's registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN's Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
  https://domains.markmonitor.com/whois

If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name's registration record, while MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.

By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
(1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
(2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain

C:\Users\Administrator>tracert amazon.com

Tracing route to amazon.com [52.94.236.248]
over a maximum of 30 hops:
  0  <1 ms <1 ms <1 ms 192.168.127.254
  1  <1 ms <1 ms <1 ms 172.18.249.250
  2  <1 ms <1 ms <1 ms 172.18.0.2
  3  <1 ms <1 ms <1 ms 76.75.74.129
  4  <1 ms <1 ms <1 ms g1100-0-0-7-aggr1.yy202.atlas.cogentco.com [38.104.251.07]
  5  <1 ms <1 ms <1 ms te0-0-0-9.ccr32.yy202.atlas.cogentco.com [154.54.3.09]
  6  <1 ms <1 ms <1 ms be3268.ccr22.ymq01.atlas.cogentco.com [154.54.42.98]
  7  <1 ms <1 ms <1 ms be2080.ccr21.ymq02.atlas.cogentco.com [154.54.45.110]
  8  <1 ms <1 ms <1 ms 38.104.155.194
  9  * * * Request timed out.
 10  * * * Request timed out.
 11  * * * Request timed out.
 12  *

```

Above is the result of using the command “tracert amazon.com” to gather similar information via CMD.

The screenshot shows a Windows desktop with two windows open. The left window, titled "Spade - [whois amazon.com@cnic, finished]", displays the results of a WHOIS query for "amazon.com". The right window, titled "Administration Command Prompt - tracert amazon.com", shows the output of a traceroute command to "amazon.com".

**WHOIS Data for amazon.com:**

```

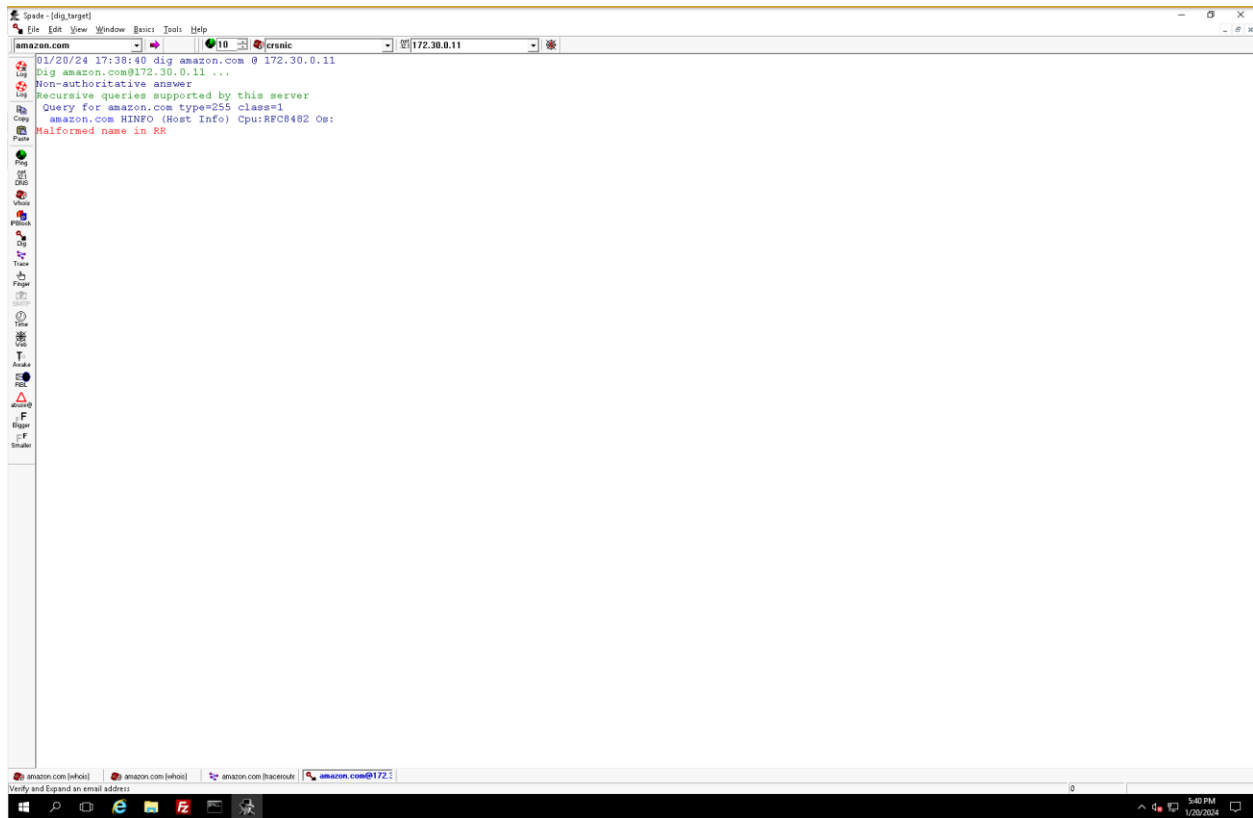
Domain Name: AMAZON.COM
Registry Domain ID: 281209 DOMAIN_COM-VRIN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-05-16T19:03:14Z
Creation Date: 1994-11-01T05:00:00Z
Registry Expiry Date: 2024-10-31T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.AMZ2DNS.CO.UK
Name Server: NS1.AMZ2DNS.COM
Name Server: NS1.AMZ2DNS.NET
Name Server: NS1.AMZ2DNS.ORG
Name Server: NS2.AMZ2DNS.CO.UK
Name Server: NS2.AMZ2DNS.COM
Name Server: NS2.AMZ2DNS.NET
Name Server: NS2.AMZ2DNS.ORG
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-01-21T01:00:25Z <<<

```

**Traceroute to amazon.com [52.94.236.248] over a maximum of 30 hops:**

Hop	Router	IP Address	Time (ms)
1		192.168.172.254	<1 ms
2		172.18.249.258	<1 ms
3		172.18.0.2	<1 ms
4		76.75.74.120	<1 ms
5		g1100-0-0-7.aggr11.yy02.atlas.cogentco.com [30.104.251.97]	2 ms
6		te0-0-0-9.ccr32.yy02.atlas.cogentco.com [154.54.3.89]	1 ms
7		be2260.ccr22.yw01.atlas.cogentco.com [154.54.42.90]	8 ms
8		be2090.ccr21.yw02.atlas.cogentco.com [154.54.45.118]	12 ms
9		38.104.155.194	8 ms
10			Request timed out.
11			Request timed out.
12			Request timed out.
13			Request timed out.
14			Request timed out.
15			Request timed out.
16			Request timed out.
17			Request timed out.
18			Request timed out.
19			Request timed out.
20			Request timed out.
21			Request timed out.

The above results show the comparison between using CMD or Sam Spade to perform a traceroute. The information is extremely similar to one another.



```
Spade - [dig.target]
File Edit View Window Basics Tools Help
amazon.com 10 cronic 172.30.0.11
01/20/24 17:38:40 dig amazon.com @ 172.30.0.11
dig amazon.com@172.30.0.11 ...
Non-authoritative answer
Recursive queries supported by this server
Query for amazon.com type=255 class=1
amazon.com HINFO (Host Info) Cpu:RFC8482 Os:
Malformed name in RR
```

Above are the results of performing a Domain Internet Groper DNS query by using Basics > Dig in the toolbar. The results have been saved to the desktop under dig\_amazon

The screenshot displays two windows side-by-side on a Windows desktop. The left window, titled 'Spade - [dig.target]', shows the output of a 'dig amazon.com' command. The output includes a header with the date and time, the command executed, and a 'Non-authoritative answer' section. The 'amazon.com HINFO (Host Info)' section shows 'Cpu:RFC8482 Os:'. The right window, titled 'Administrator Command Prompt - nslookup', shows the output of an 'nslookup' command. It displays a 'web-based WHOIS' link, a disclaimer about the data's accuracy, and a 'Tracing route to amazon.com' section. The trace shows a path from the user's machine to amazon.com, with various IP addresses and response times. The final output shows 'Trace complete.' and 'Default Server: dns.google'.

```

Spade - [dig.target]
amazon.com
01/20/24 17:38:40 dig amazon.com @ 172.30.0.11
Dig amazon.com@172.30.0.11 ...
Non-authoritative answer
Recursive queries supported by this server
Query for amazon.com type=255 class=1
amazon.com HINFO (Host Info) Cpu:RFC8482 Os:
Malformed name in RR

Administrator Command Prompt - nslookup
Facilitates email communication with the relevant contact(s).
web-based WHOIS:
https://domains.markmonitor.com/whois
If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.
The data in MarkMonitor's WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name's registration record. While MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.
By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
(1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
(2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain
C:\Users\Administrator>tracert amazon.com
Tracing route to amazon.com [52.94.236.248]
over a maximum of 30 hops:
 0  0 ms  0 ms  0 ms  192.168.127.254
 1  1 ms  1 ms  1 ms  172.18.249.250
 2  1 ms  1 ms  1 ms  172.18.0.2
 3  1 ms  1 ms  1 ms  70.72.74.129
 4  1 ms  1 ms  1 ms  gl108-0-0-7.agr11.yyz02.atlas.cogentco.com [38.104.251.97]
 5  2 ms  2 ms  2 ms  tco-0-0-0-crs22.yyz02.atlas.cogentco.com [154.54.3.89]
 6  1 ms  1 ms  1 ms  be208-crs22.yyz02.atlas.cogentco.com [154.54.42.98]
 7  8 ms  8 ms  8 ms  be208-rtr21.yyz02.atlas.cogentco.com [154.54.45.118]
 8  12 ms  12 ms  12 ms  38.104.155.104
 9  9 ms  9 ms  9 ms  Request timed out.
10  * * * Request timed out.
11  * * * Request timed out.
12  * * * Request timed out.
13  * * * Request timed out.
14  8 ms  8 ms  8 ms  52.94.81.147
15  * * * Request timed out.
16  * * * Request timed out.
17  * * * Request timed out.
18  * * * Request timed out.
19  * * * Request timed out.
20  * * * Request timed out.
21  * * * Request timed out.
22  * * * Request timed out.
23  * * * Request timed out.
24  21 ms  21 ms  21 ms  52.94.236.248
Trace complete.
C:\Users\Administrator>nslookup
Default Server: dns.google
Address: 8.8.8.8
> set type=any
> amazon.com
Server: dns.google
Address: 8.8.8.8
Non-authoritative answer:
amazon.com HINFO Cpu = RFC8482 8.8.8.8
Server: dns.google
Address: 8.8.8.8
Name: dns.google
Address: 8.8.8.8

```

Comparing the data from the dig search to using nslookup in CMD, we see that the data is quite different. The data from Sam Spade seems accurate, while the data in the cmd is flawed.



**Part 2: Public Domain Research**

Name of Target organization: Amazon.com, Inc

Domain name and extension: amazon.com

URLs for the e-commerce website and any social networking sites: <https://www.amazon.com/>,  
<https://www.facebook.com/Amazon/>, <https://twitter.com/amazon>,  
<https://www.instagram.com/amazon/>, <https://www.linkedin.com/company/amazon>,  
<https://www.youtube.com/user/amazon>

Physical Address: 410 Terry Ave N, Seattle, WA.

Names of officers: Jeff Bezos - Founder and Executive Chairman, Andy Jassy - CEO, Brian T.

Olsavsky - Senior Vice President and Chief Financial Officer, Dave Clark - CEO, Worldwide

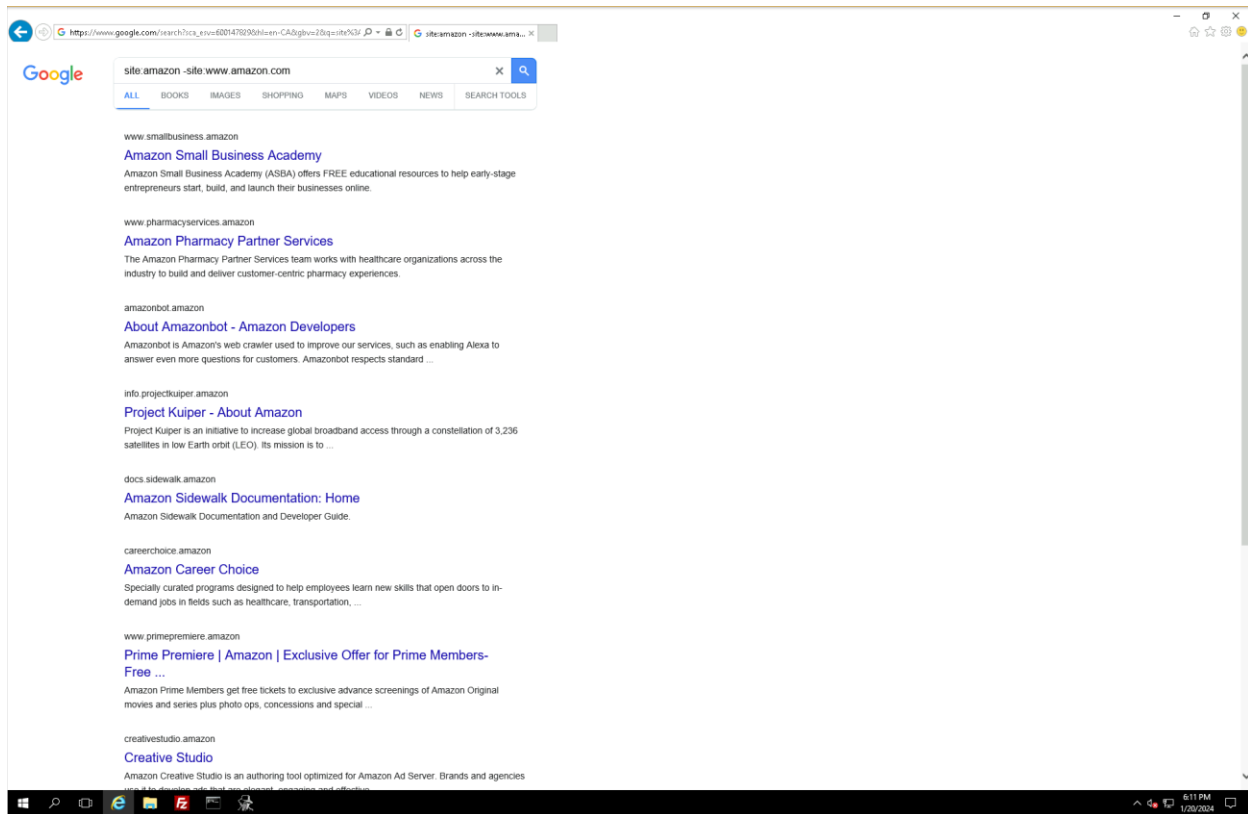
Consumer, David Zapolsky - General Counsel, Beth Galetti - Senior Vice President, Human

Resources, Tom Taylor - Senior Vice President, Amazon Web Services, Shelley Reynolds - Vice President, Worldwide Controller and Principal Accounting Officer.

Number of employees: 1.5 million

Business Partners: N/A

Google maps Amazon headquarters location.



Above are the results of using the command “site:amazon -site:www.amazon.com” on google.

### Part 3: Research Report

In Parts 1 and 2 of this lab we worked through how an attacker can use publicly available information to gather valuable information that can be exploited. Whois was used to find information about the owner of a domain. Traceroute/tracert was used to find information about the route that packets travel to get from the domain to the host. DIG as well as Nslookup were used to find DNS related information about the target domain. Google search was used to find additional information such as social media sites, physical addresses, names of officers and number of employees. Throughout this lab a number of tools and techniques were used for research including Sam Spade, CMD, Whois, traceroute/tracert, DIG, Nslookup, and google search. With these tools and techniques we were able to find out that amazon.com is registered to <http://www.markmonitor.com> and was created on 1994-11-01. We were able to find information about how many hops it takes to reach amazon.com. We were also able to find DNS information including class and type for the domain. Class being 1 and type being 255. The following research was found during the public domain portion of research. The target organization is Amazon.com, Inc. The domain name and extension associated with the organization's website is amazon.com. The e-commerce website can be accessed at <https://www.amazon.com/>. Additionally, Amazon has an active presence on various social networking sites, including Facebook (<https://www.facebook.com/Amazon/>), Twitter (<https://twitter.com/amazon>), Instagram (<https://www.instagram.com/amazon/>), LinkedIn (<https://www.linkedin.com/company/amazon>), and YouTube (<https://www.youtube.com/user/amazon>). The physical address of Amazon.com, Inc. is located at 410 Terry Ave N, Seattle, WA. The notable officers of Amazon.com, Inc. include Jeff Bezos - Founder and Executive Chairman, Andy Jassy - CEO, Brian T. Olsavsky - Senior Vice President

and Chief Financial Officer, Dave Clark - CEO, Worldwide Consumer, David Zapolsky - General Counsel, Beth Galetti - Senior Vice President, Human Resources, Tom Taylor - Senior Vice President, Amazon Web Services, Shelley Reynolds - Vice President, Worldwide Controller and Principal Accounting Officer. Amazon.com, Inc. has approximately 1.5 million employees. Unfortunately, specific information about their business partners was not available in this research. Additional research that I would like to have to learn more about amazon would include knowledge of their IT infrastructure, security practices, and potential vulnerabilities.

### **What is the difference between running a Sam Spade investigation versus searching DNS records?**

Utilizing the application Sam Spade and searching DNS records via the command line offer similar results, but there are advantages to using Sam Spade. One aspect where Sam Spade shines is its ability to provide a more comprehensive view with a broader range of information. In addition to retrieving DNS records, Sam Spade offers functionalities such as WHOIS searches and traceroutes. This allows for a more thorough and holistic analysis of the target domain. Another benefit of Sam Spade is its user-friendly experience. With a graphical interface, users can easily navigate through the application without needing to rely on specific command line commands. This accessibility makes it a more convenient option for those who prefer a more intuitive tool. The convenience of Sam Spade extends to its ability to perform various searches within the same application. Users can switch between DNS record lookups, traceroute investigations, and Whois inquiries, saving time and effort compared to using the command line.

### **Which method might let the target organization know you are looking at them?**

A method that might let the target organization know you are looking at them is tracert/traceroute due to an Intrusion Detection System or IDS. An IDS works by monitoring the traffic through a network for any activity that could indicate an attack. Performing a network scan or using tracert/traceroute could trigger the IDS and raise an alarm. This could prompt the organization's security team to investigate the report further. This could allow them to log and report any host IP addresses. Similarly, an organization could monitor DNS queries if they own the DNS server. This could also trigger the IDS if deemed suspicious.

### **What will the result of the search in Google® tell you? “site:amazon - site:www.amazon.com”**

The google search “site:amazon -site:www.amazon.com” results in URL's that contain the word Amazon but are not the specific website [www.amazon.com](http://www.amazon.com). This type of query is known as google dorking and allows for better search capability. This search discovers web pages that are related to Amazon but excludes the primary website. This results in web pages that can include subdomains, services, or other documents related to Amazon. These include <https://www.pharmacyservices.amazon/> - Amazon's pharmacy service, <https://www.smallbusiness.amazon/> - Amazon's small business academy, <https://amazonbot.amazon/> - Amazon's amazonbot site, and many other URL's. Exploring these URLs can offer a deeper understanding of some of amazon's offerings or inner workings.