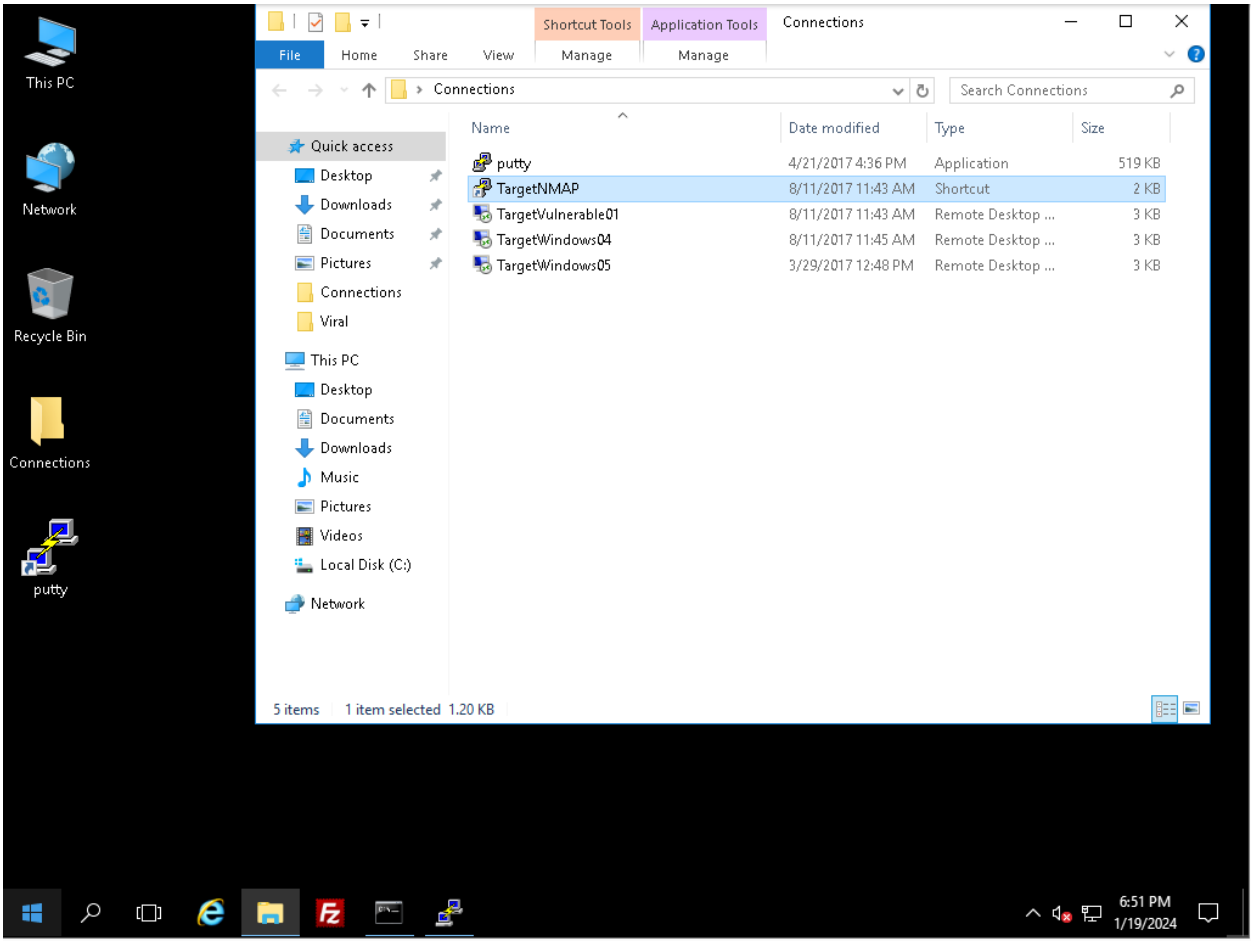
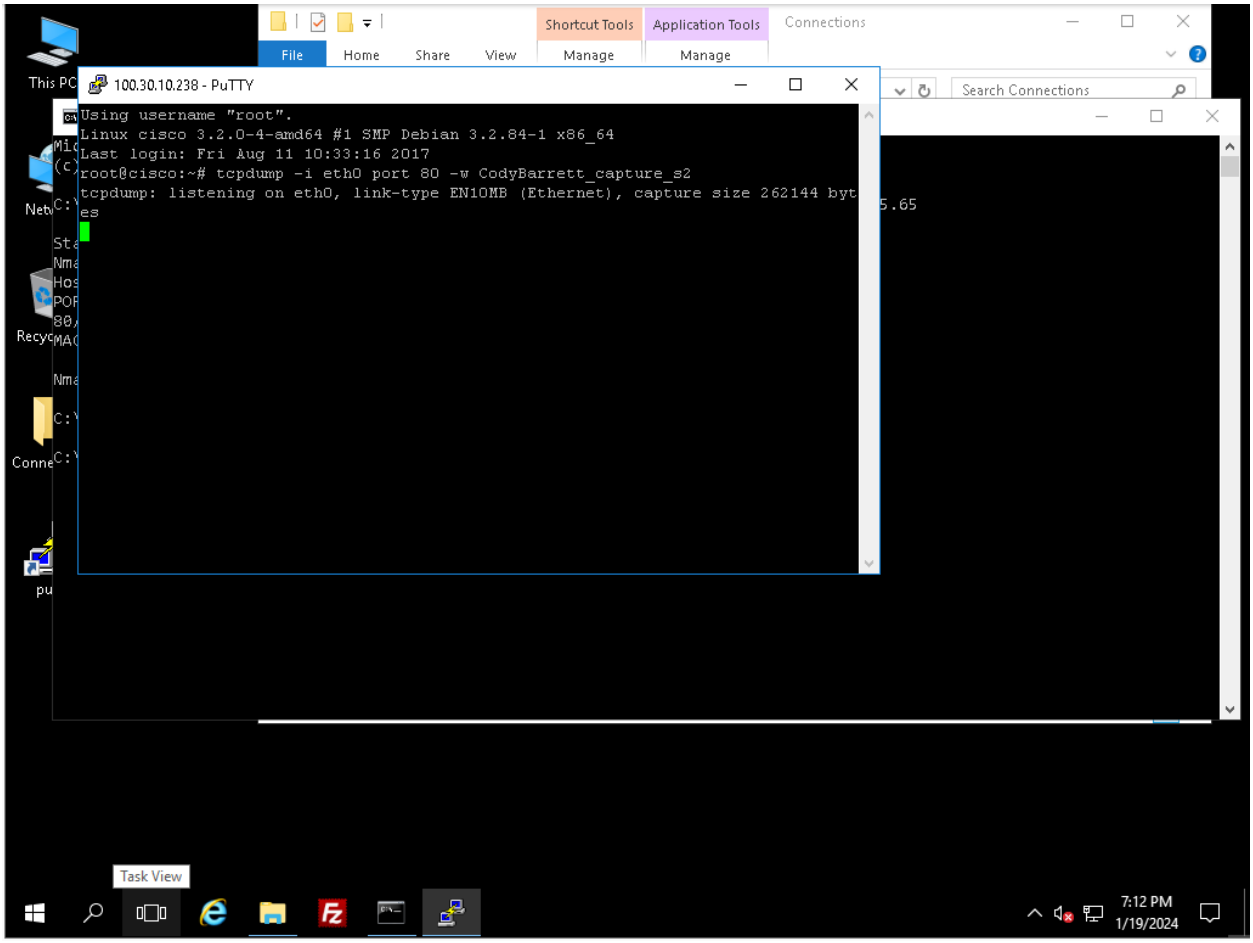
Cody J Barrett

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

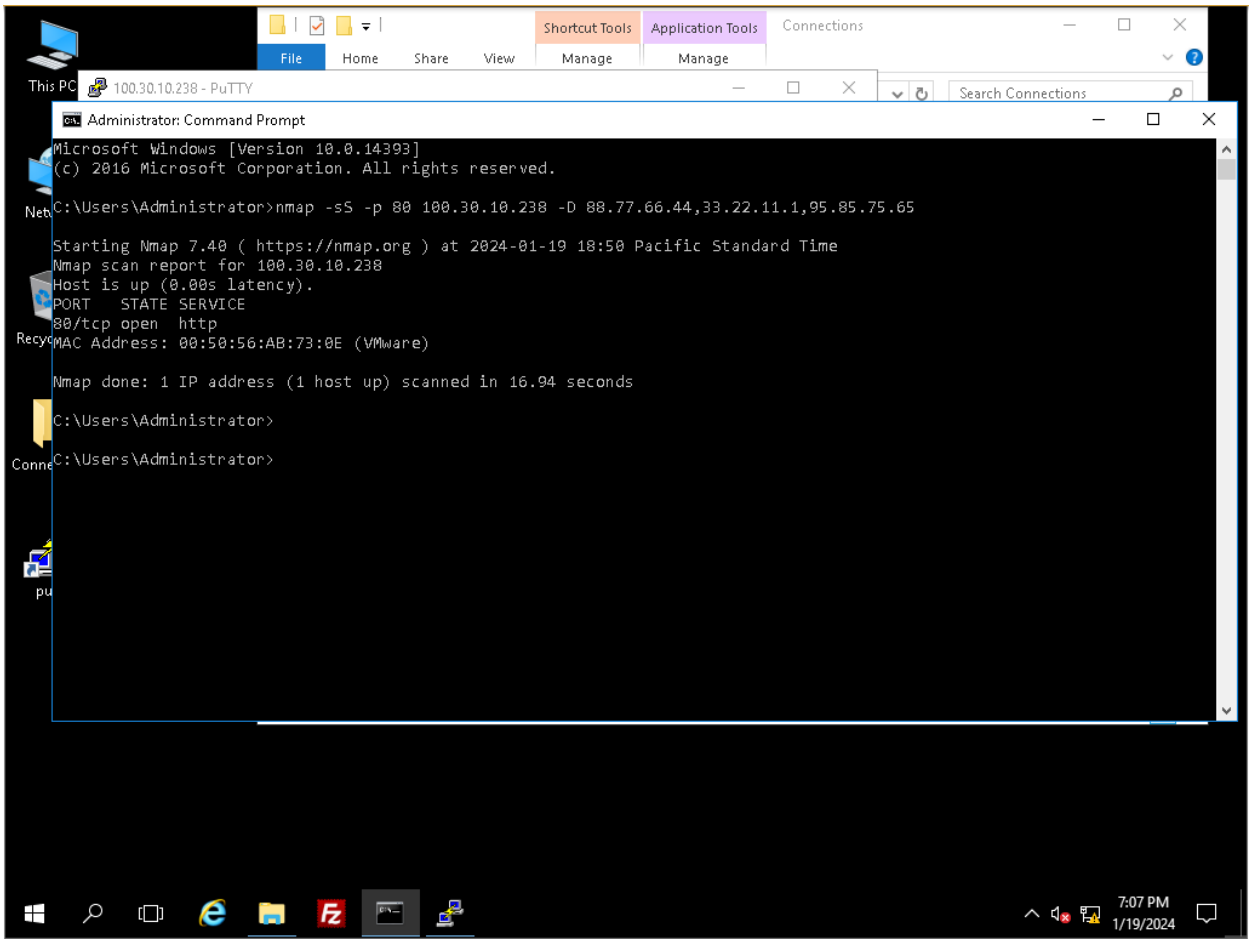
Part 1: Scan the Wide Area Network



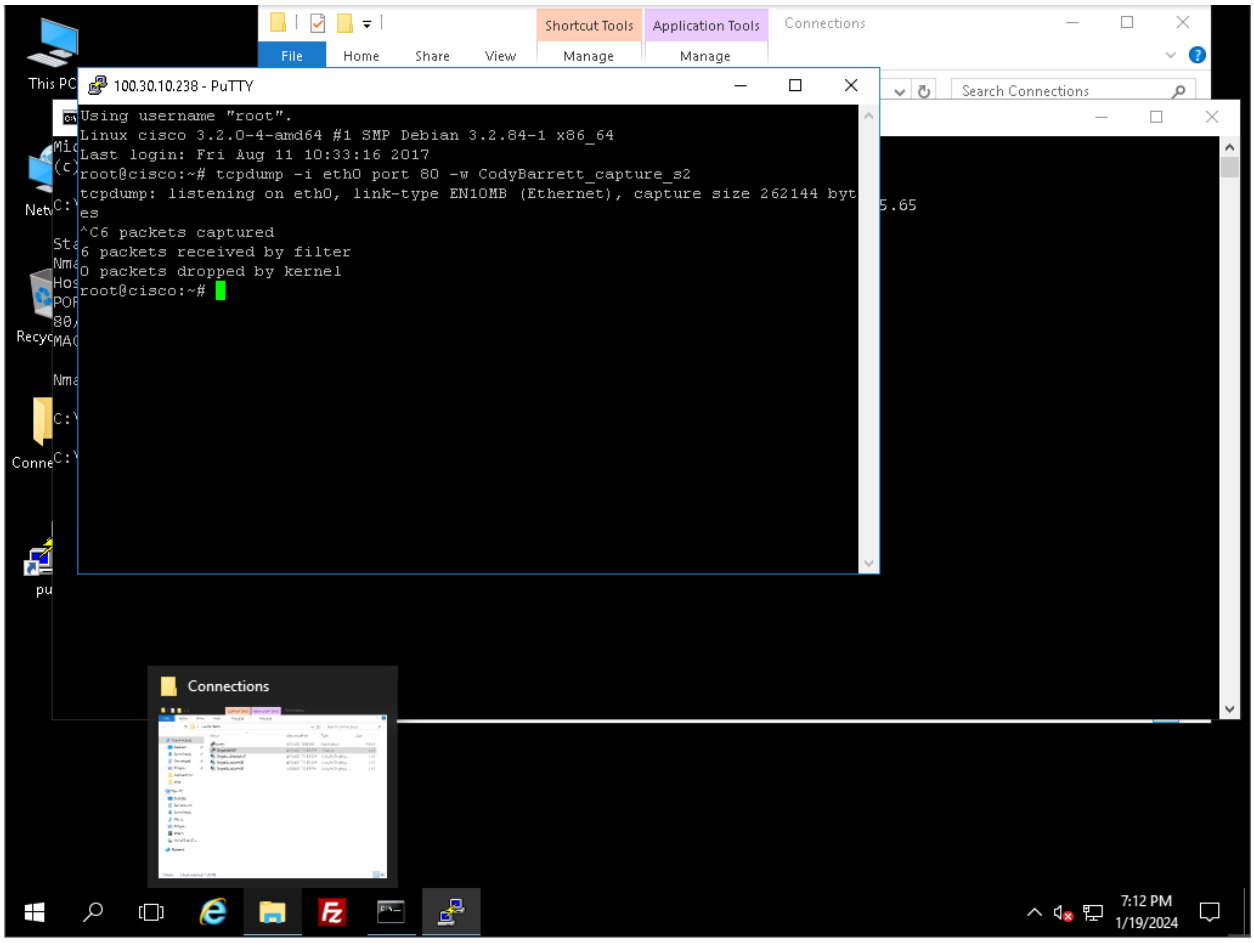
A shortcut is used to start a connection to a target system via PuTTY.



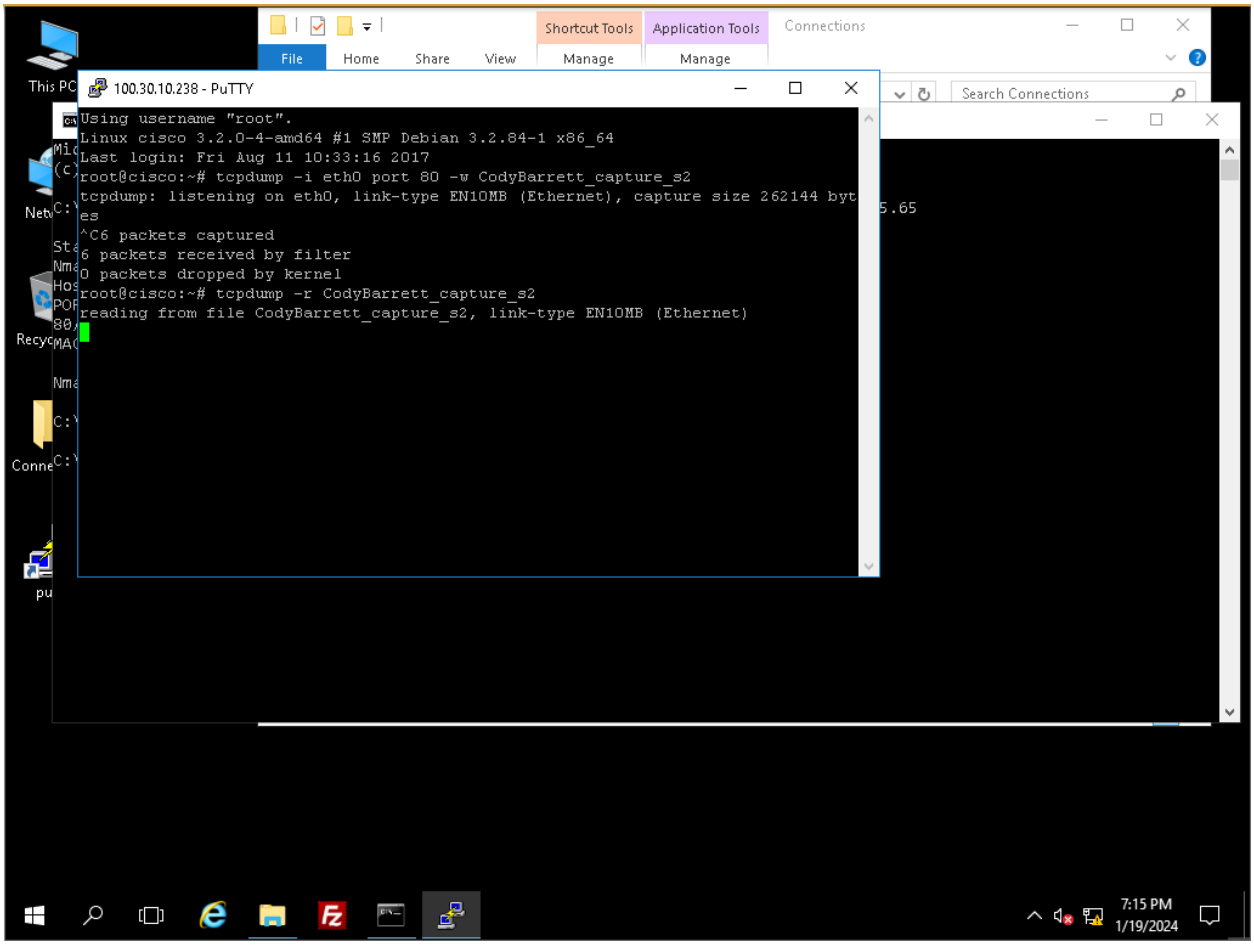
The command “tcpdump -i eth0 port 80 -w CodyBarrett_capture_s2” is used to start capturing network traffic over port 80 to a file named CodyBarrett_capture_s2.



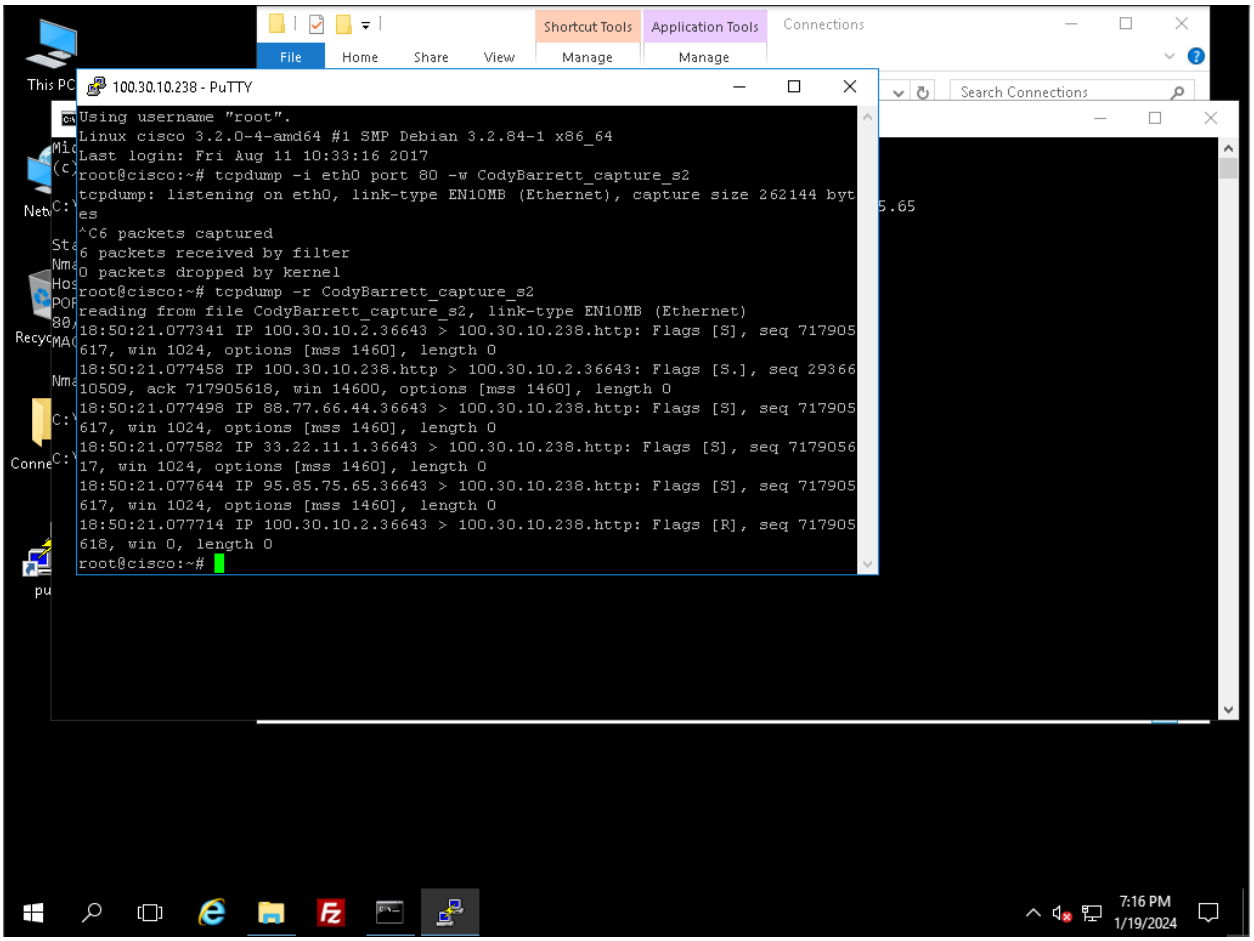
In a CMD window, the command “nmap -sS -p 80 100.30.10.238 -D 88.77.66.44,33.22.11.1,95.85.75.65” is used to start a stealth scan on the system with the IP address of 100.30.10.238. This command also uses 88.77.66.44 33.22.11.1 and 95.85.75.65 as decoy IP addresses.



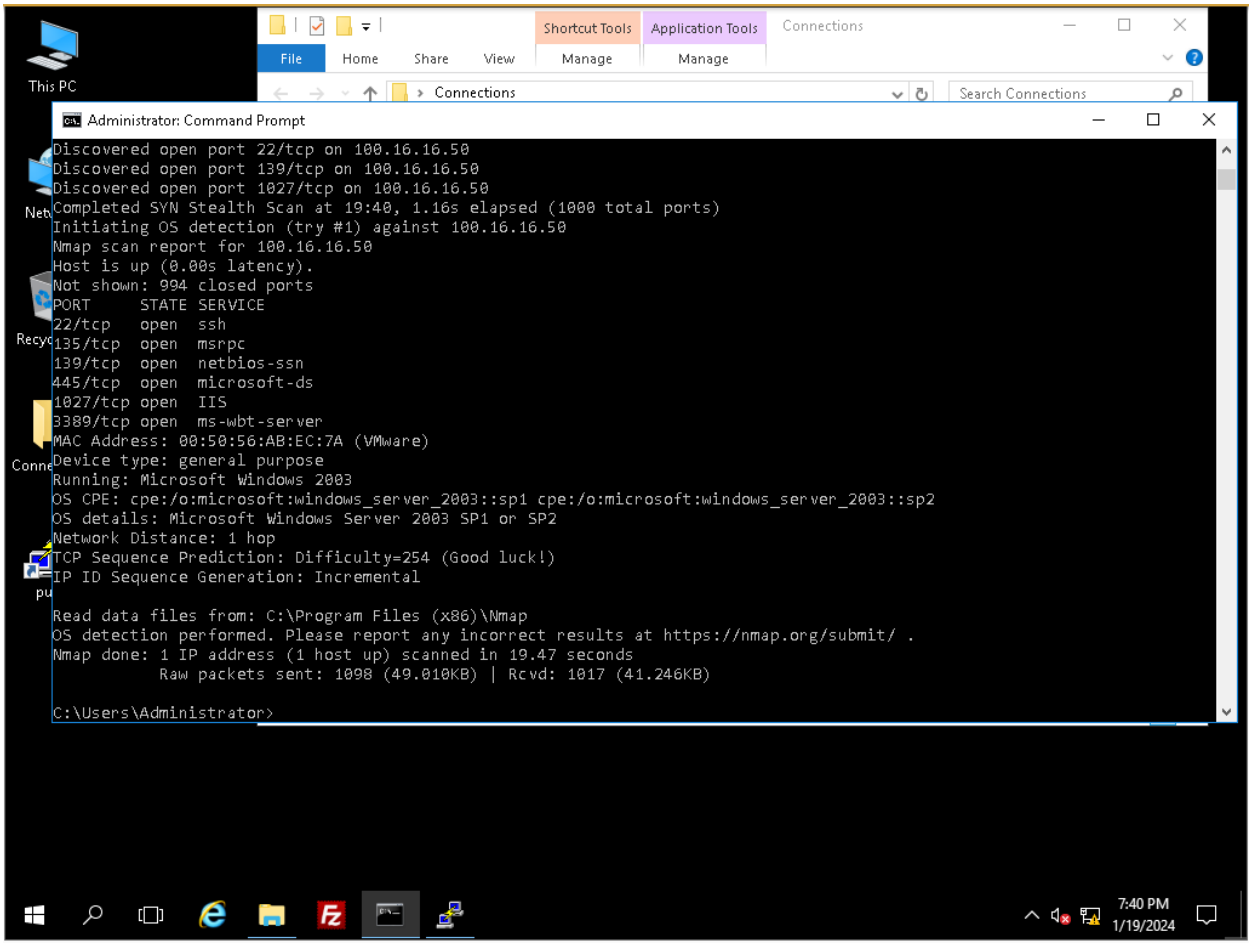
Ctrl+C is used to stop the tcpdump capture in the PuTTY CMD window.



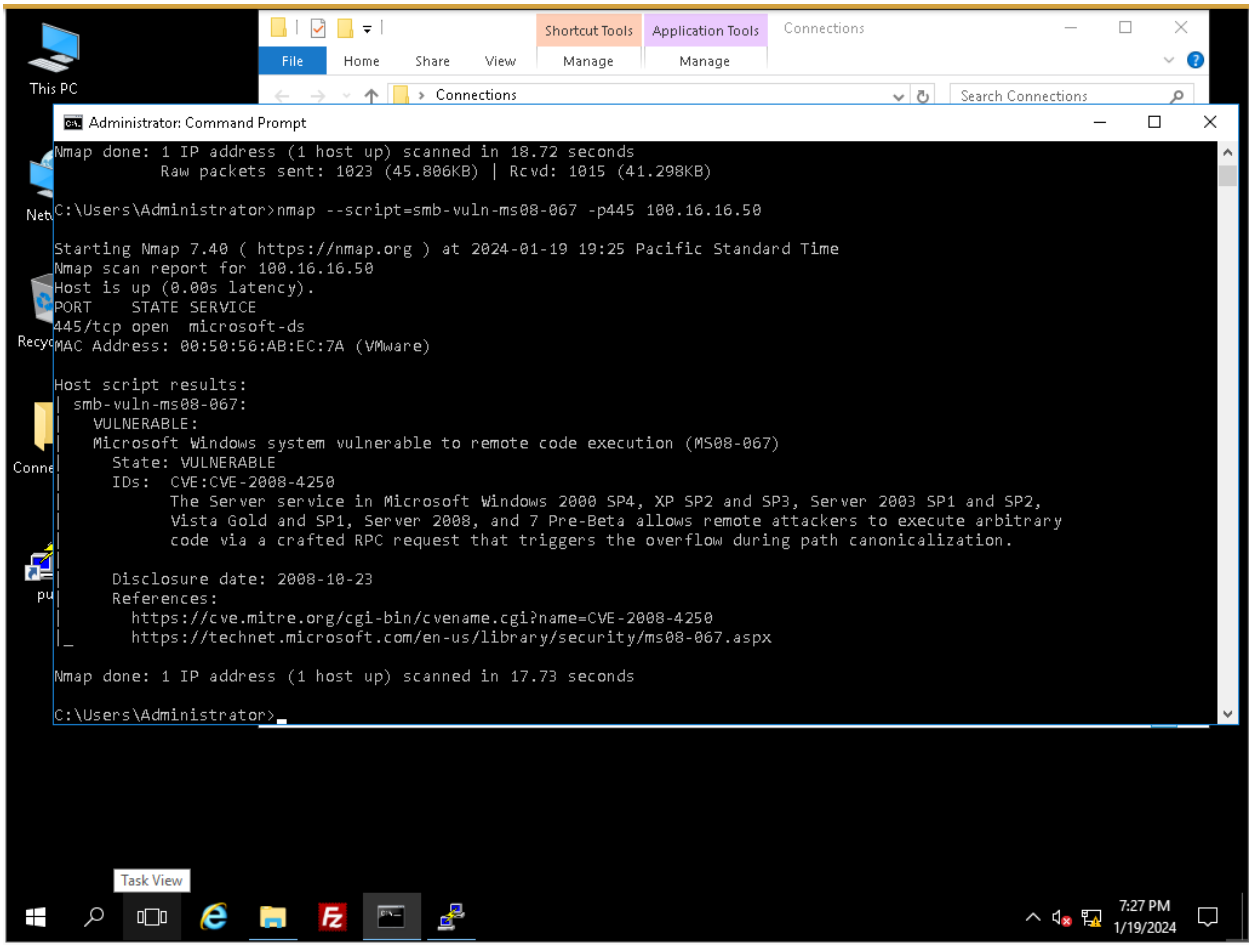
To read the capture file, the command “tcpdump -r CodyBarrett_capture_s2” is used.



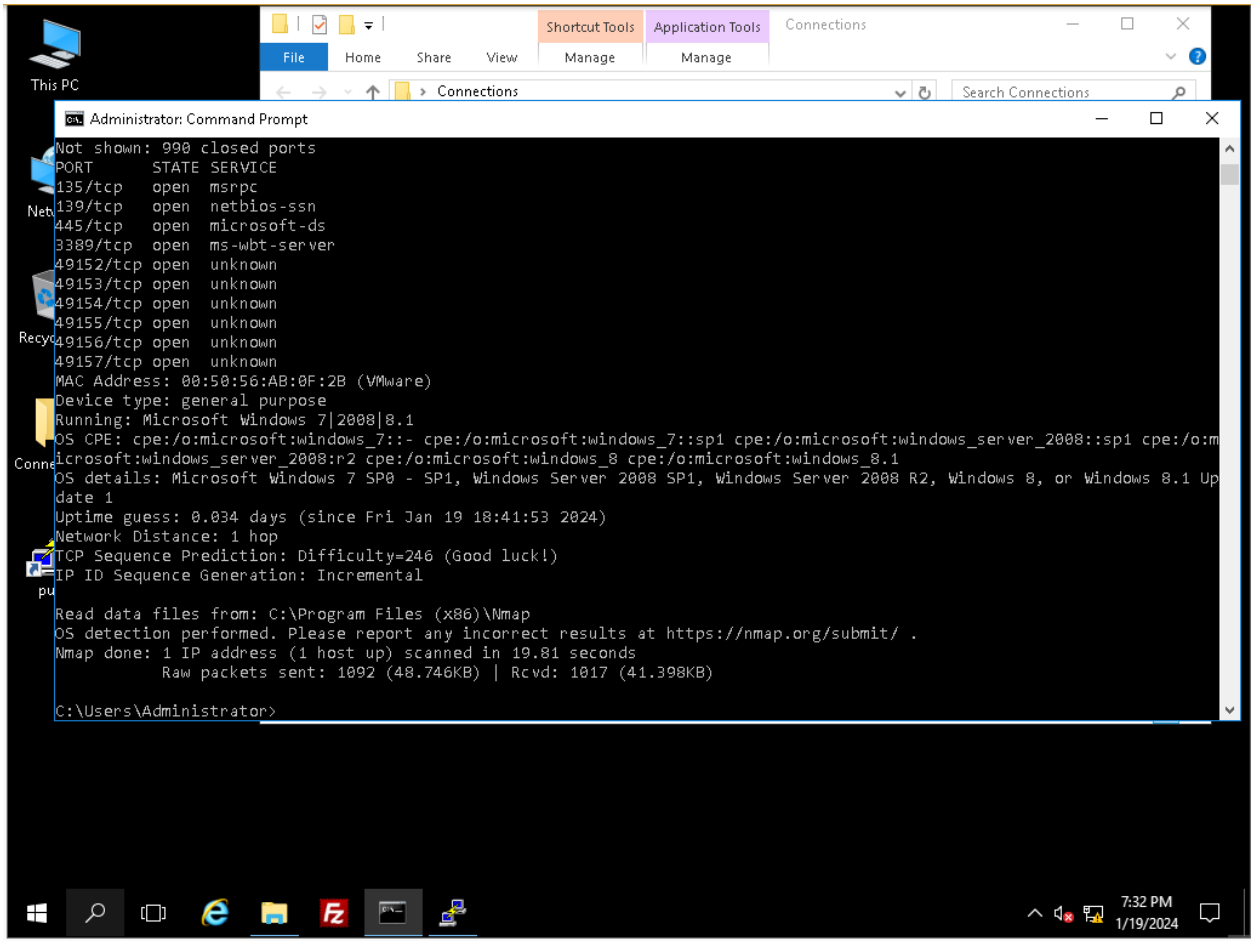
Note the decoy IP addresses in the contents of the capture in the above screenshot.



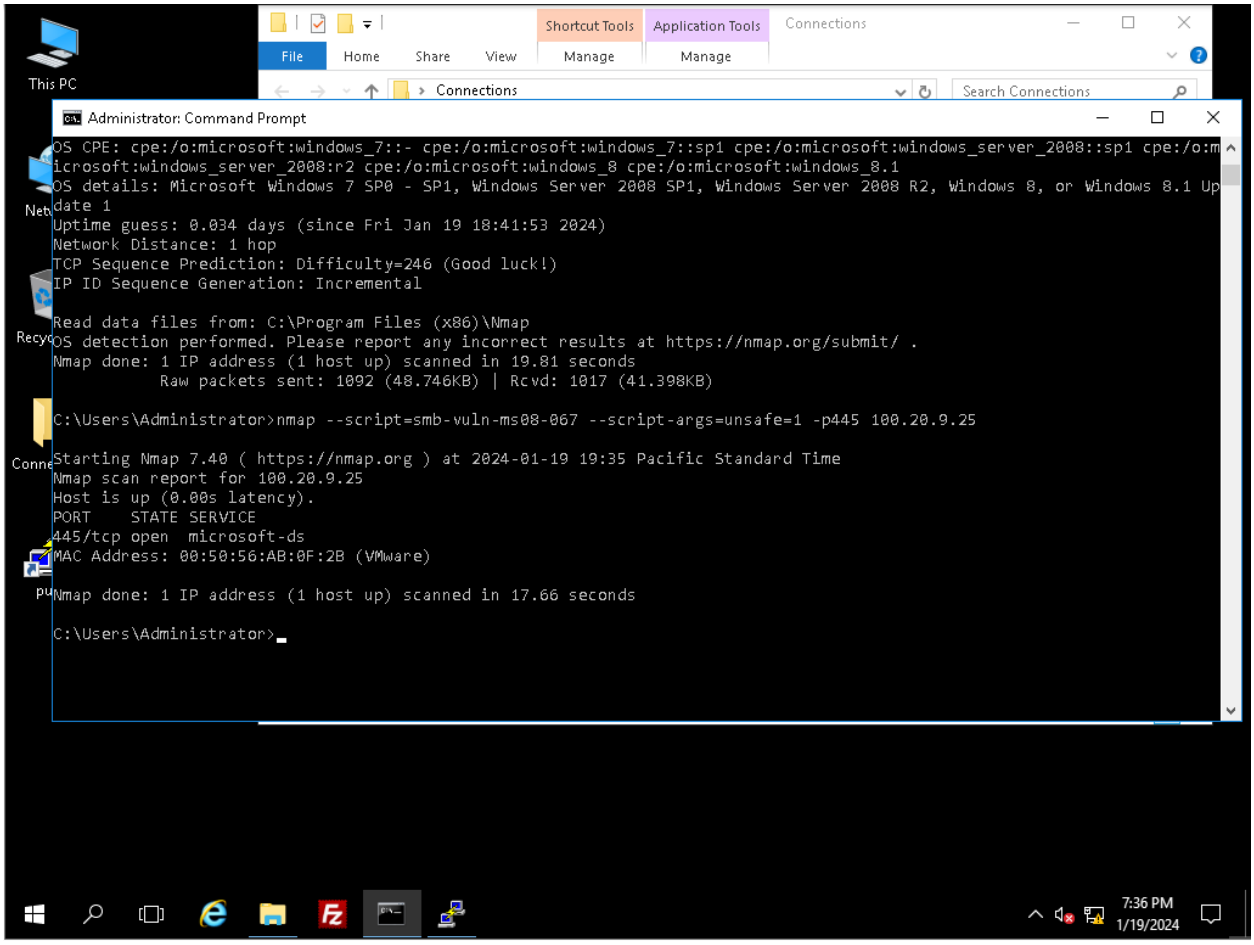
To detect the operating system of the target system the command “nmap -O -v 100.16.16.50” is used. Note that the operating system is Microsoft Windows 2003 based on the above screenshot.



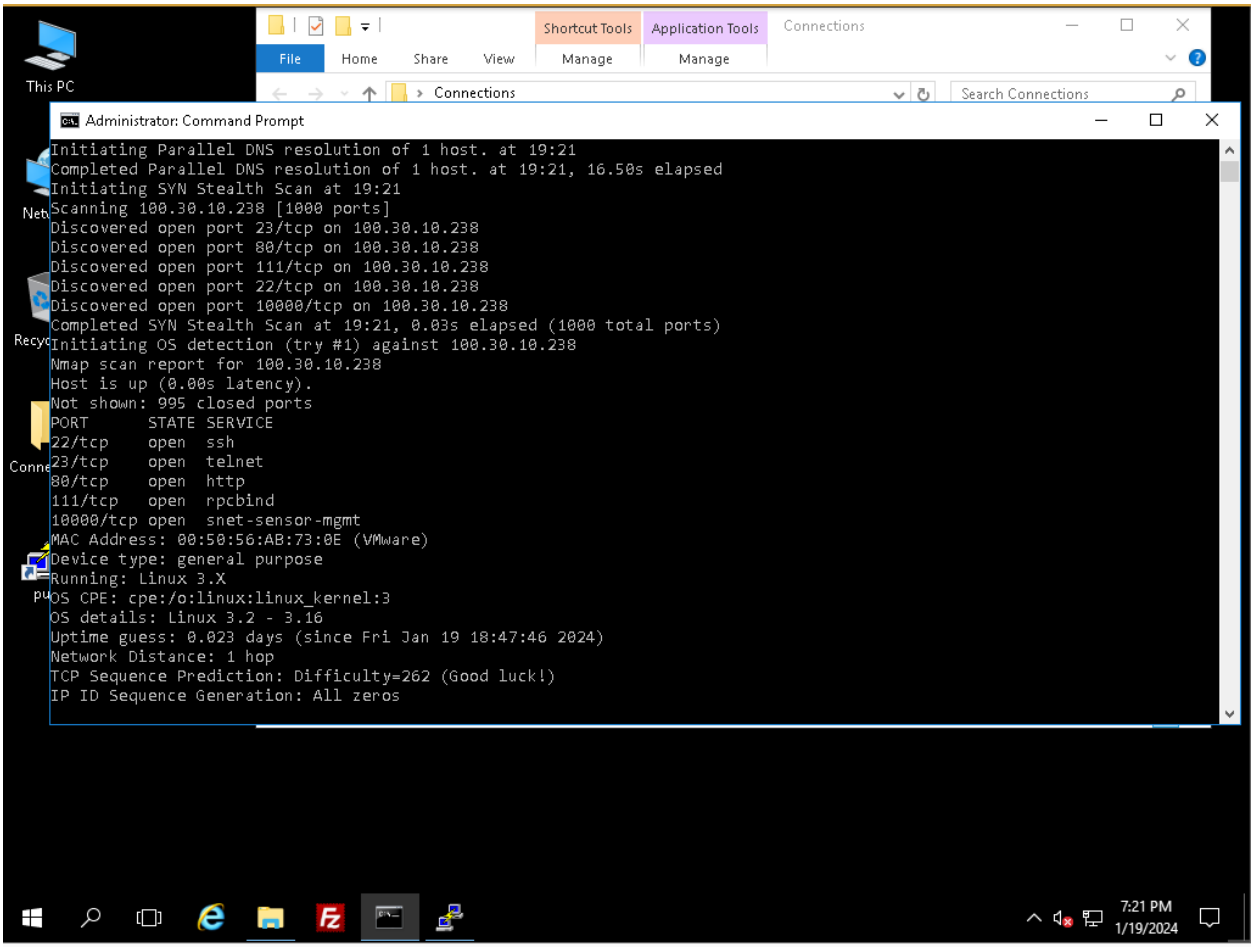
The command “nmap –script=smb-vuln-ms08-067 -p445 100.16.16.50” is used to use nmap to run a script file named smb-vuln-ms08-067 to check port 445 for a vulnerability for an exploit titled MS08-067.



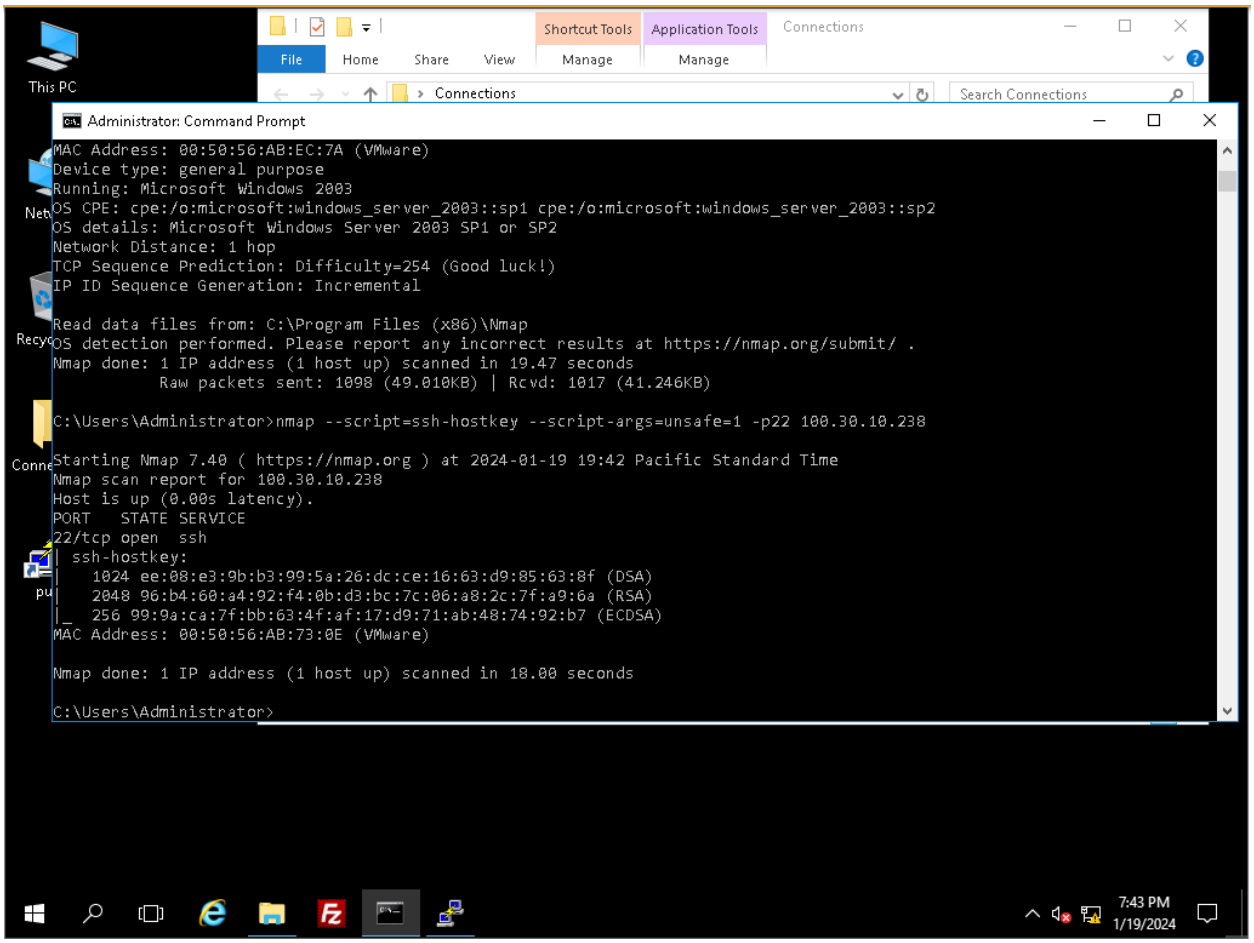
To find the operating system of TargetWindows04 the command “nmap -O -v 100.20.9.25” is used. The operating system is listed as Windows 7|2008|8.1



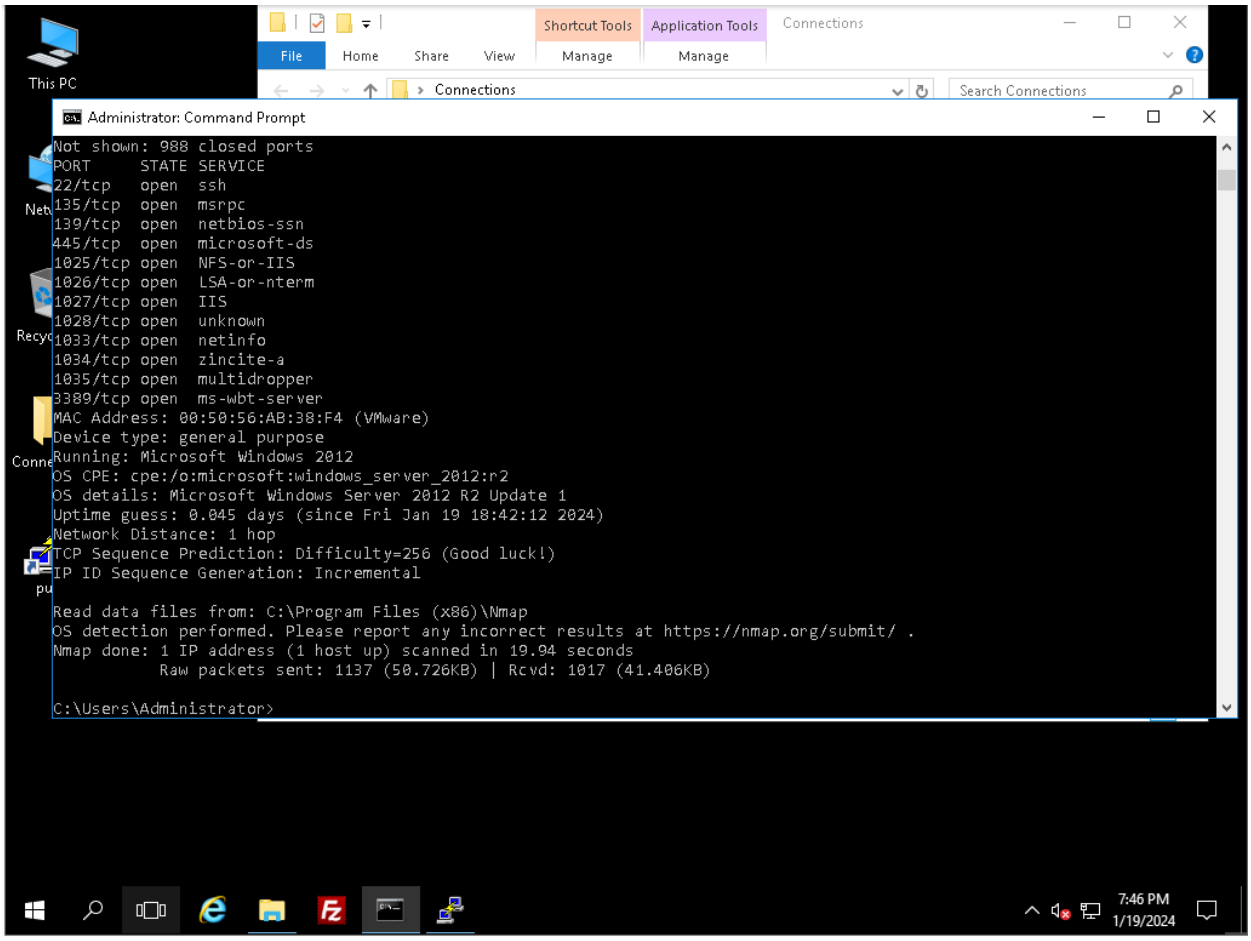
To run a similar SMB vulnerability check on port 445 for MS08-067 on TargetWindows04, the command “nmap –script=smb-vuln-ms08-067 –script-args=unsafe=1 -p445 100.20.9.25” This adds the argument to the script to add the unsafe flag.



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.



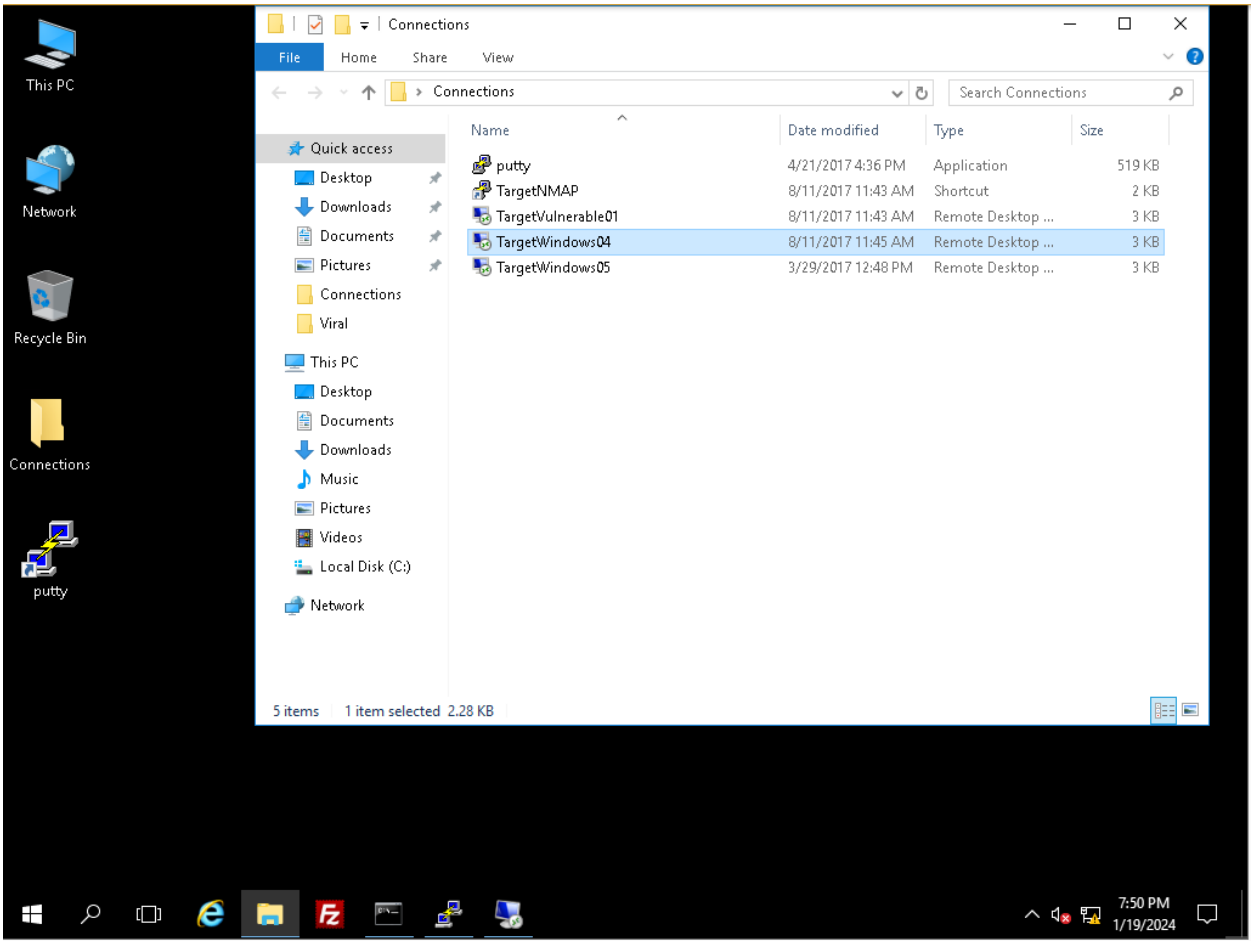
To check for a ssh vulnerability named hostkey on port 22 with an unsafe flag, the script ssh-hostkey is ran with the command “nmap –script=ssh-hostkey –script-args=unsafe=1 -p22 100.30.10.238”



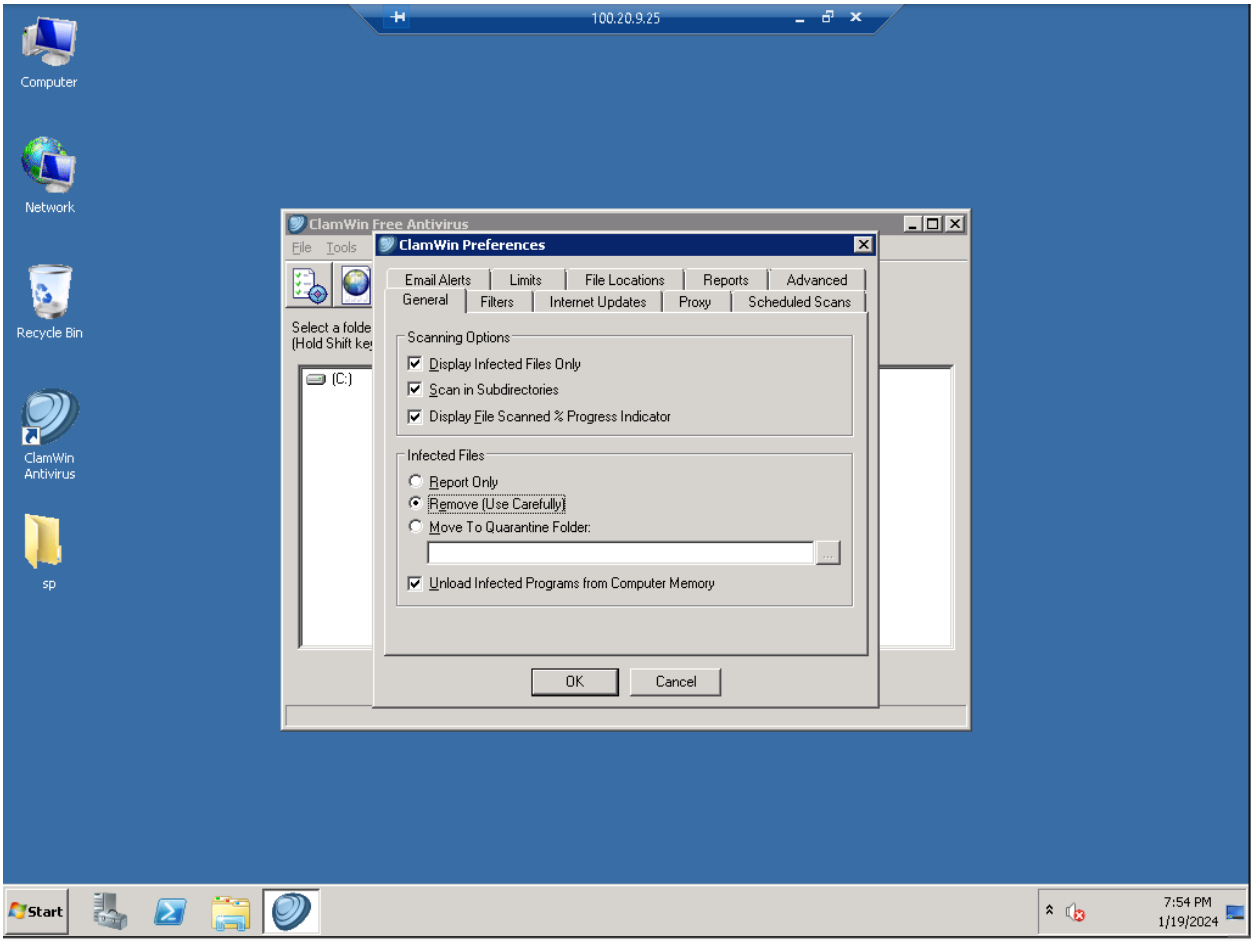
To view TargetWindows05's operating system, the command "nmap -O -v 172.30.0.31" is used.

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

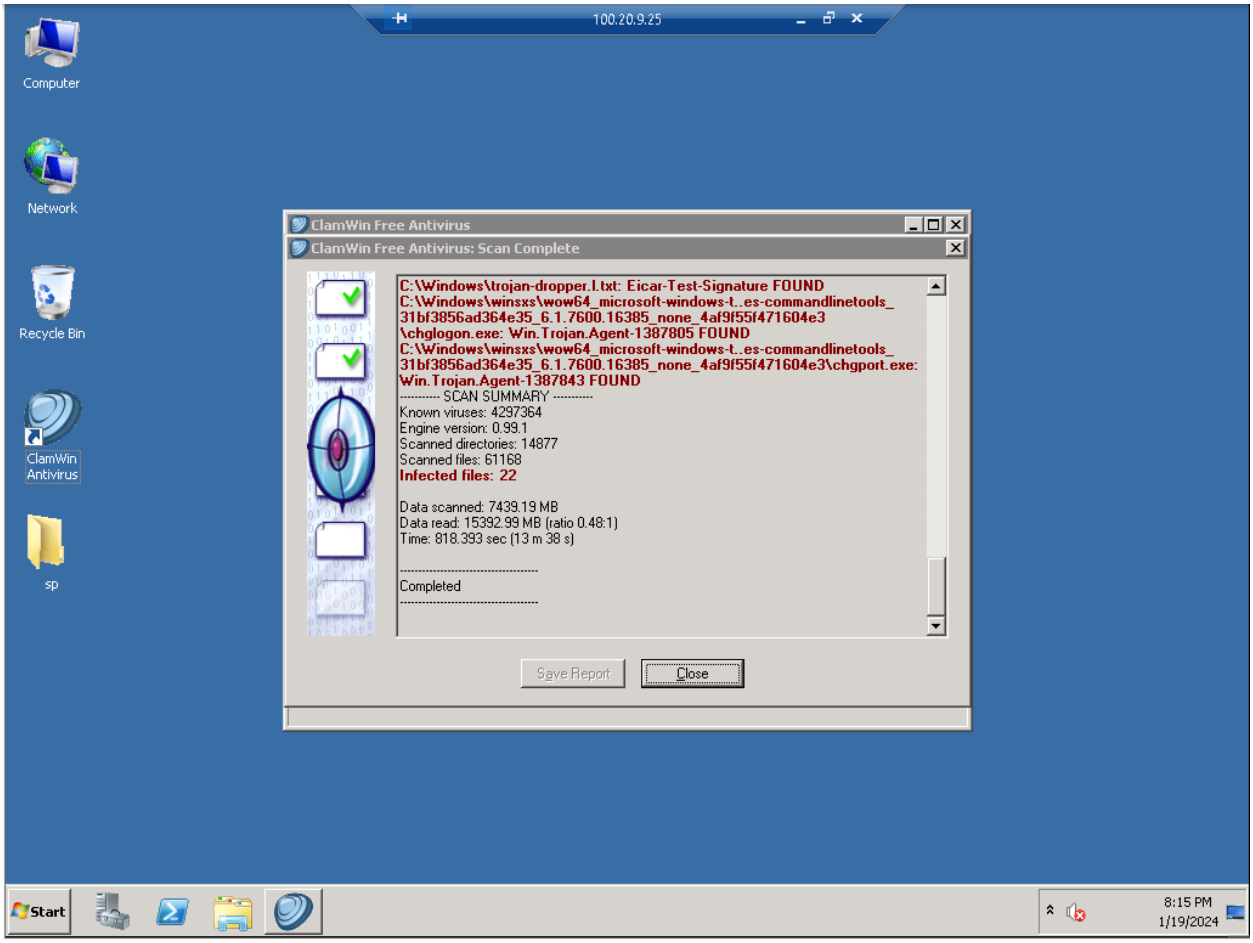
Part 2: Clean Vulnerable Systems



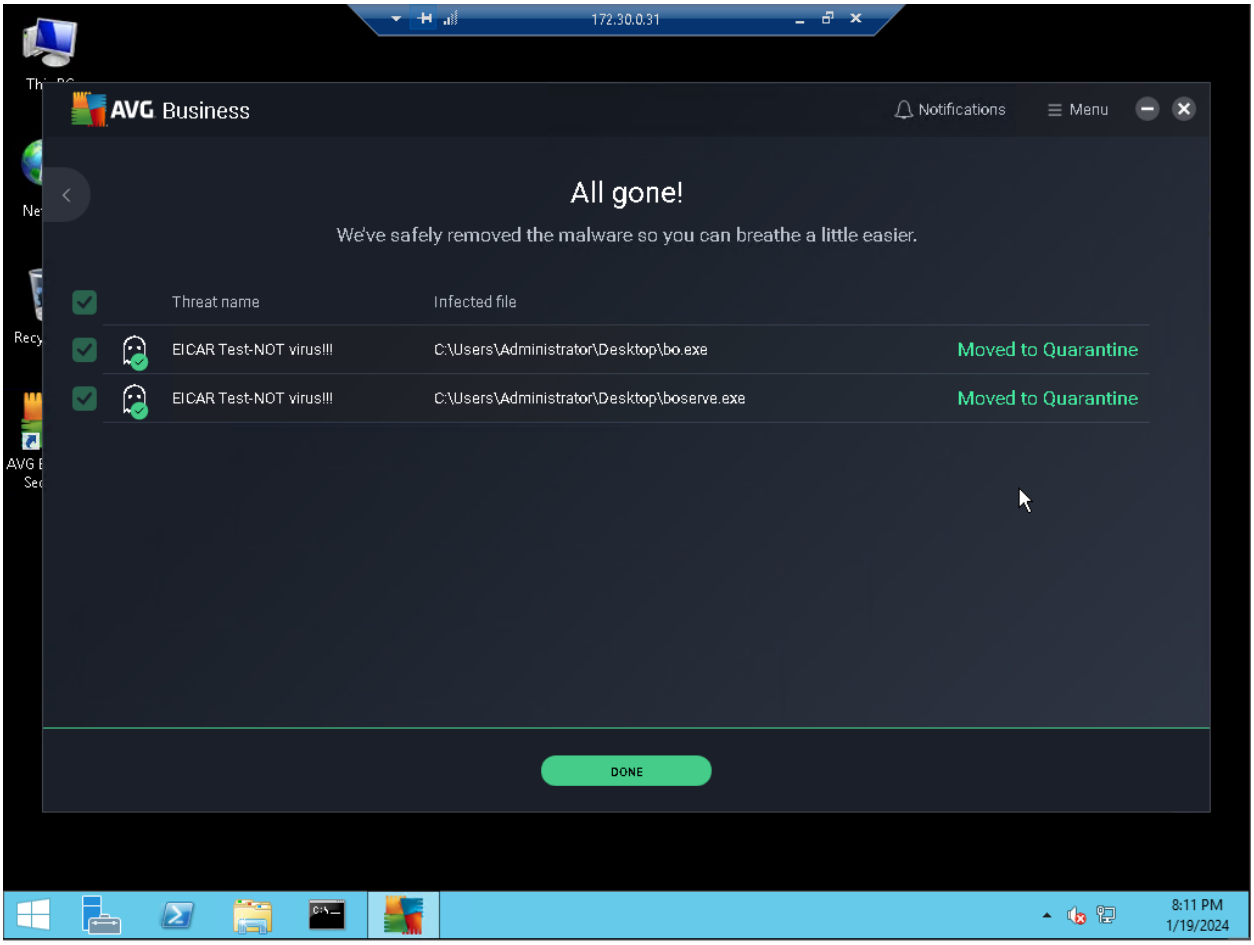
To open a connection to TargetWindows04, double-click the shortcut in the Connections folder.



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

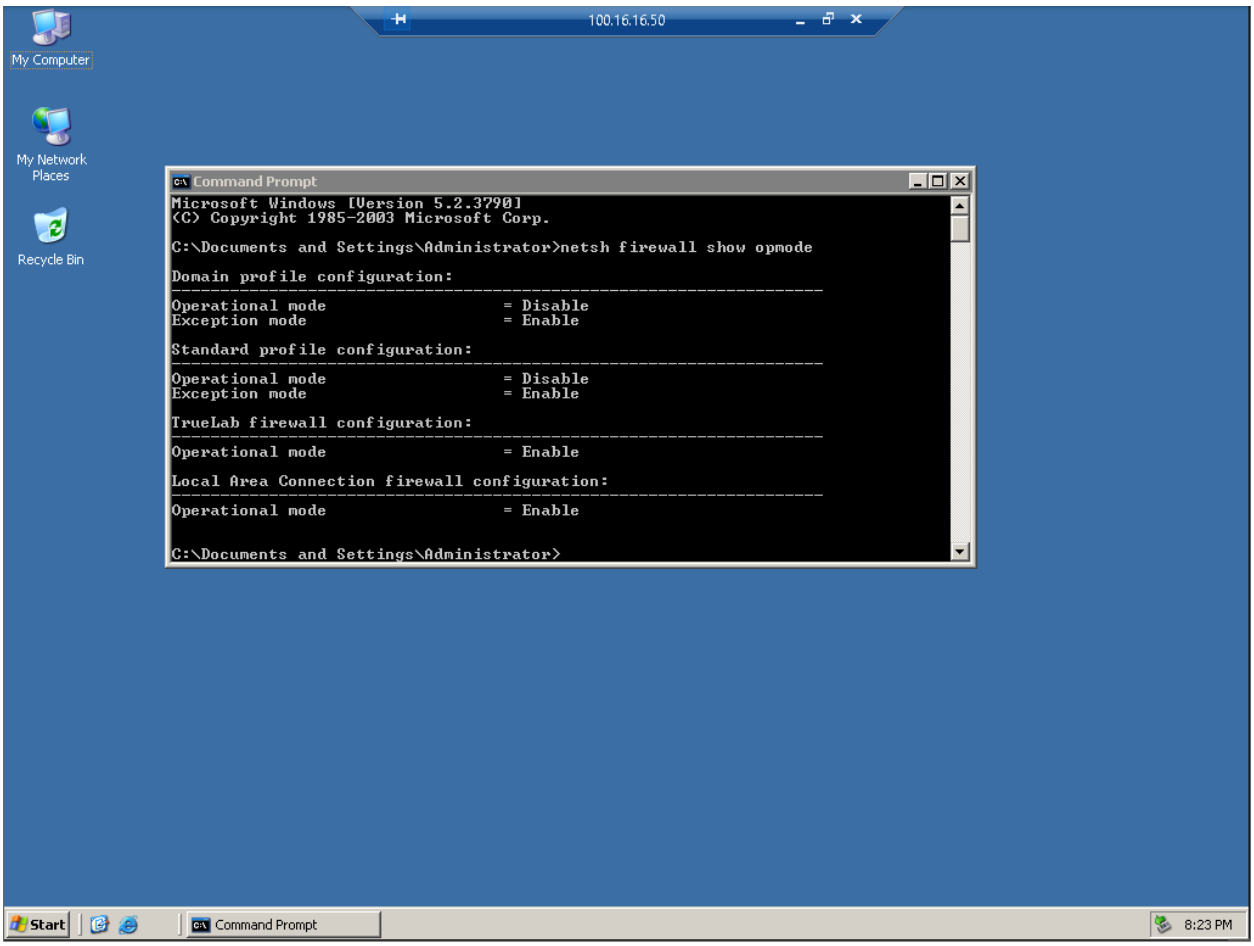


Above are the results of the ClamWin Antivirus scan. This shows that 22 infected files were found and removed.

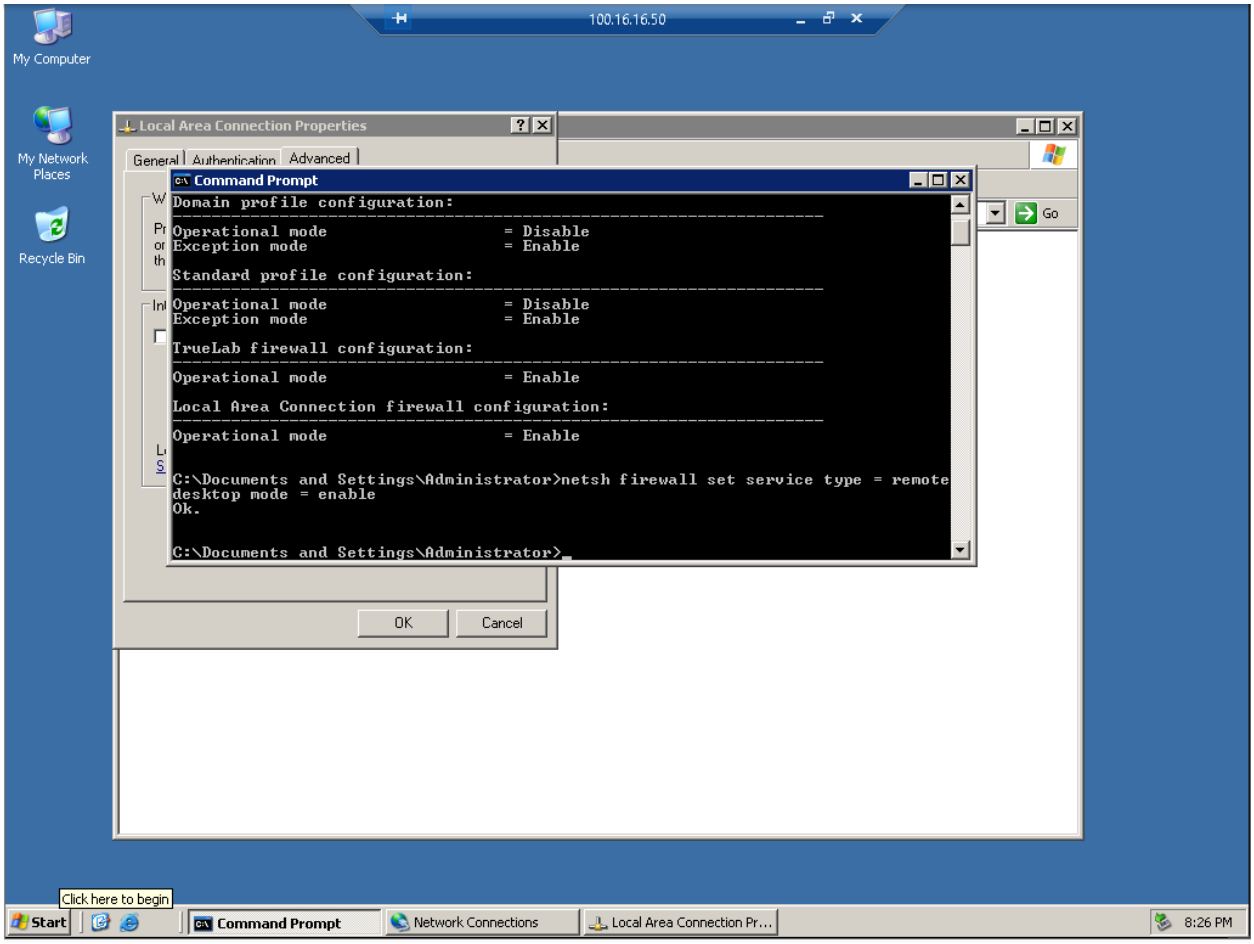


On TargetWindows05 Launch AVG, click the “Turn On” button and perform a scan on the folder C:\Users\Administrator\Desktop. The above are the results of the scan where the threat named “EICAR Test-NOT virus!!!” was found.

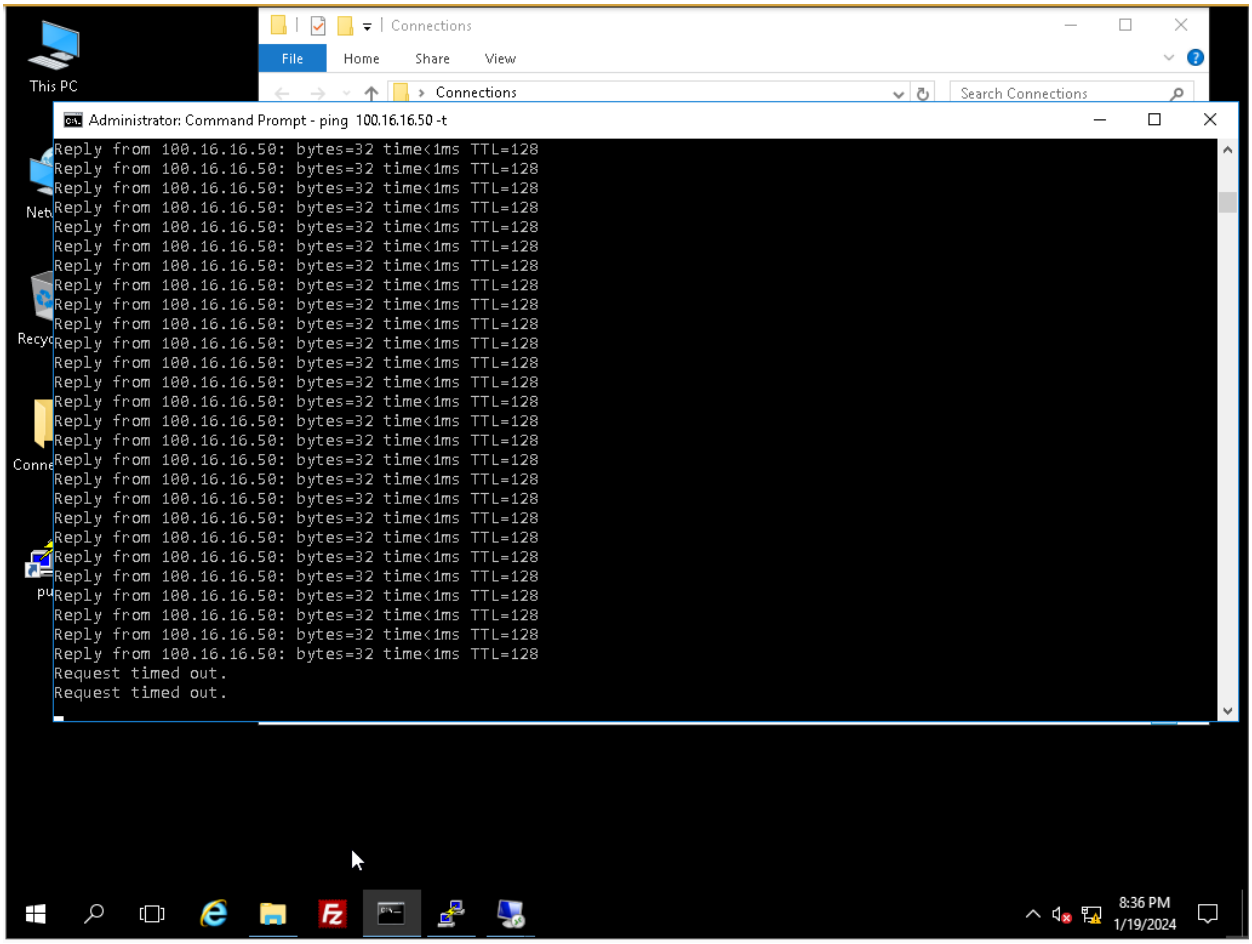
Part 3: Reduce the Attack Surface on the Windows 2003 Server



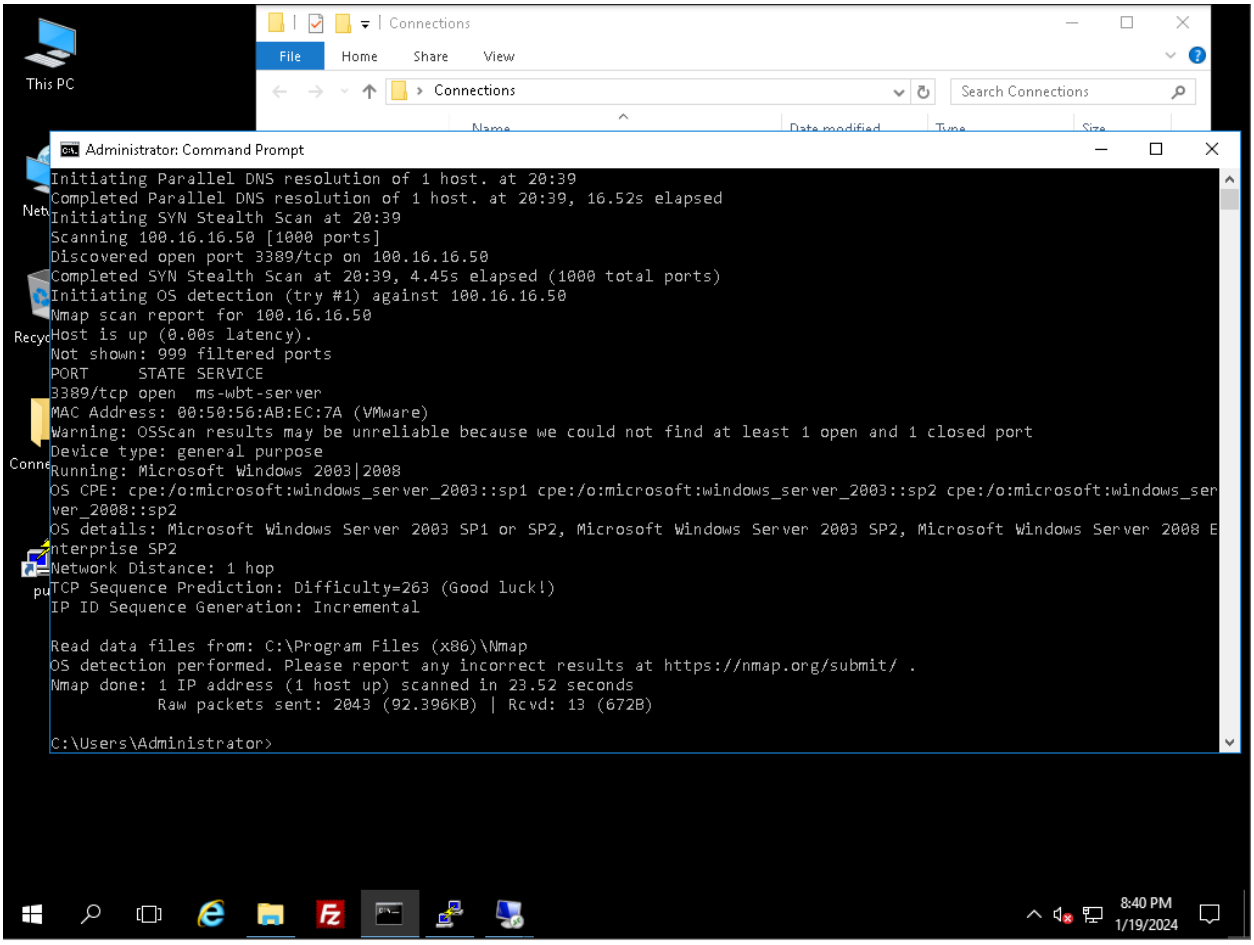
The command “netsh firewall show opmode” is used in CMD on TargetWindows01 to show firewall profile settings.



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.



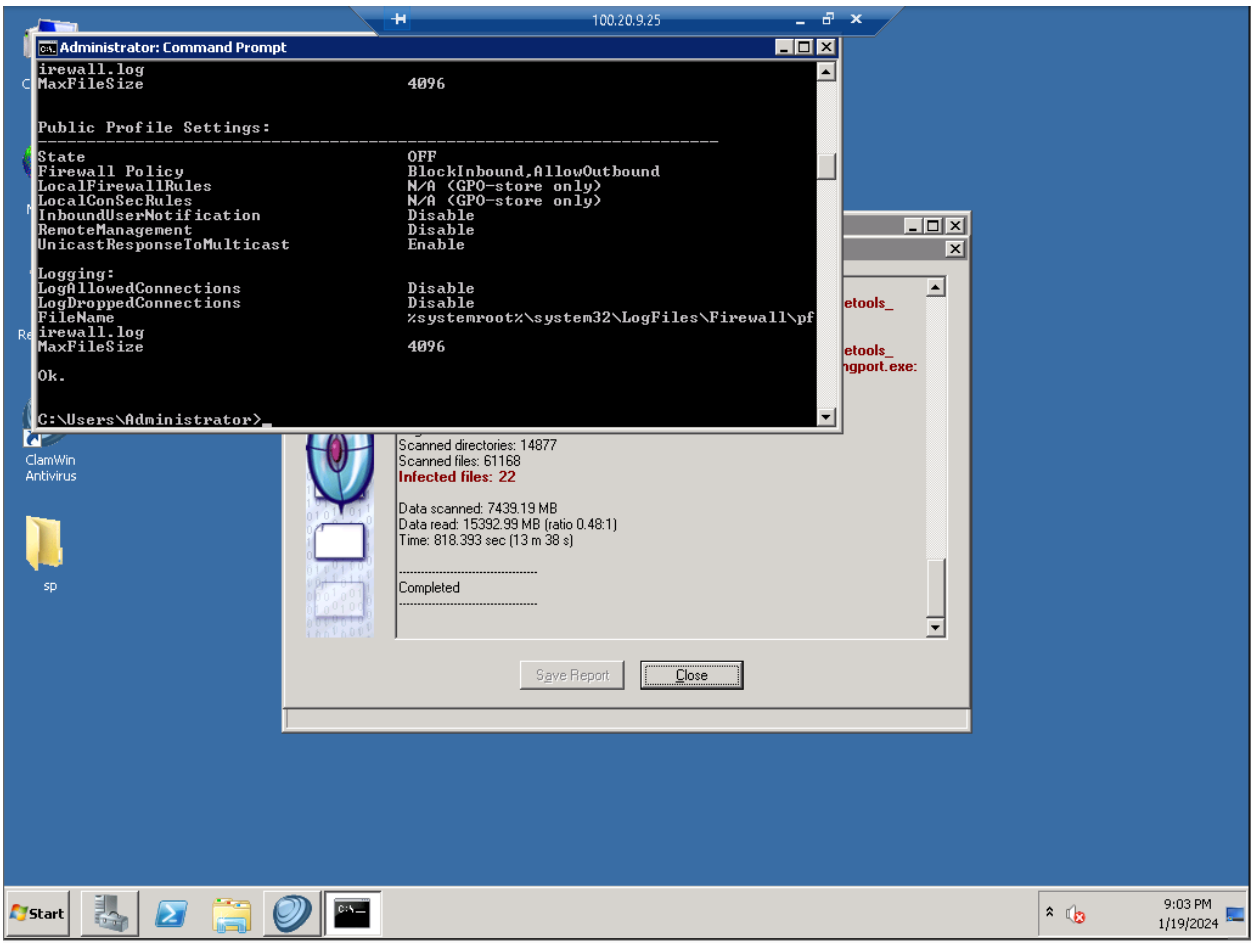
The command “nmap -O -v 100.16.16.50” is used to scan for the operating system of TargetVulnerable01.

Comparison of the two nmap scans.

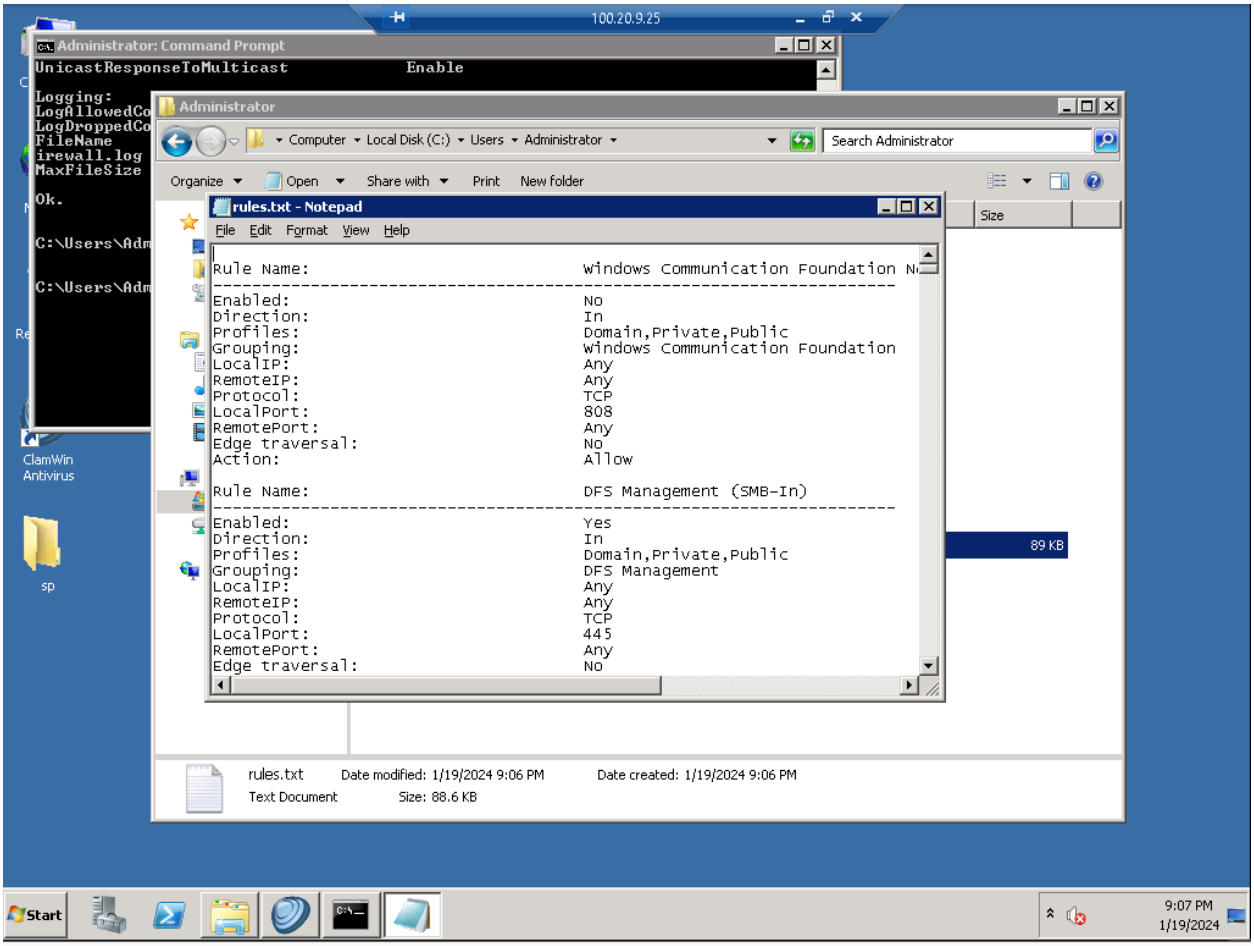
The first Nmap scan of the system 100.16.16.50 was prior to the reduction of attack surface on the system. In the first scan we were able to see that a number of ports are open including 22/ssh, 135/msrpc, 139/netbios-ssn, 445/Microsoft-ds, 1027/IIS, and 3389/ms-wbt-server. Additionally, we were able 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.

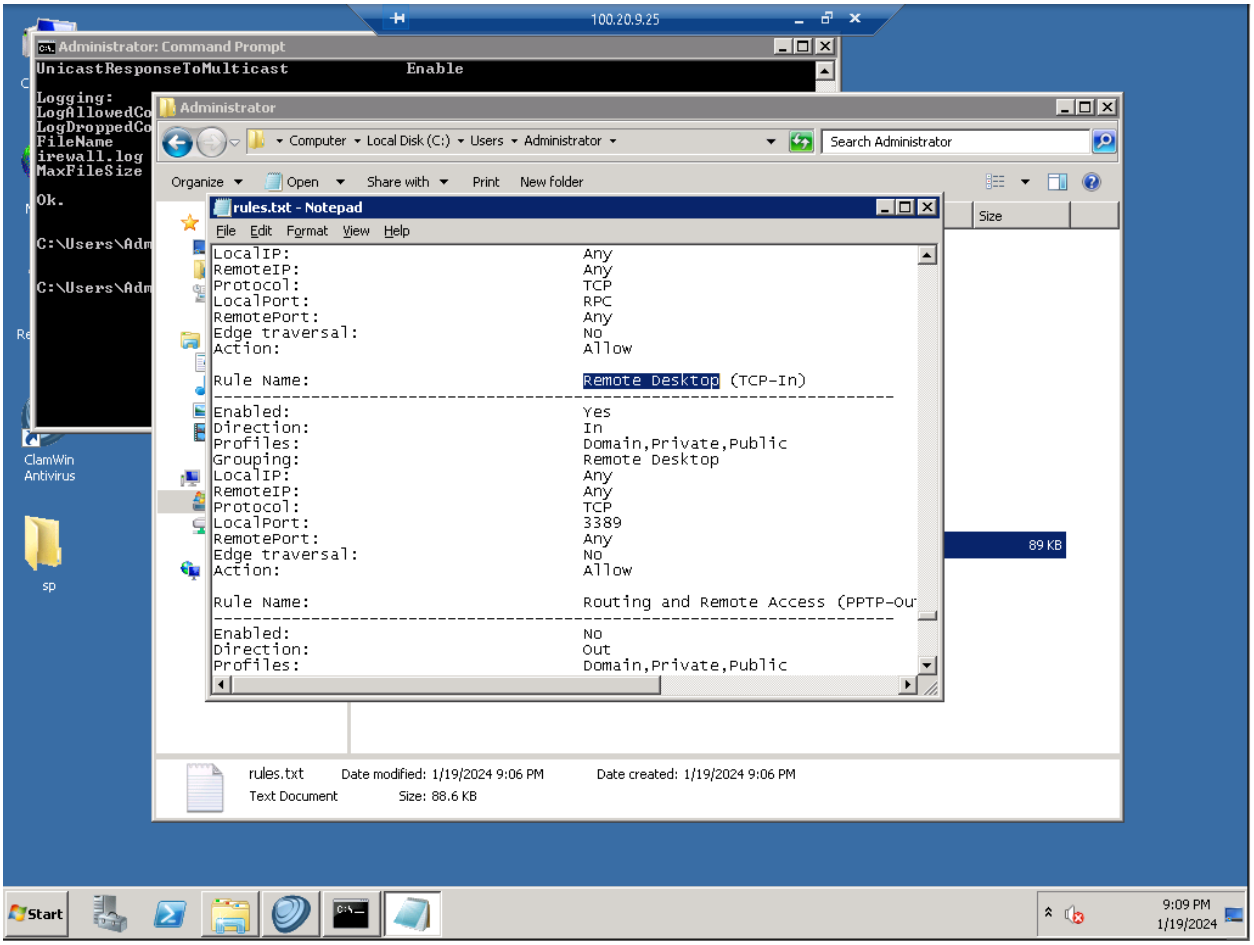
Part 4: Reduce the Attack Surface on the Windows 2008 Server



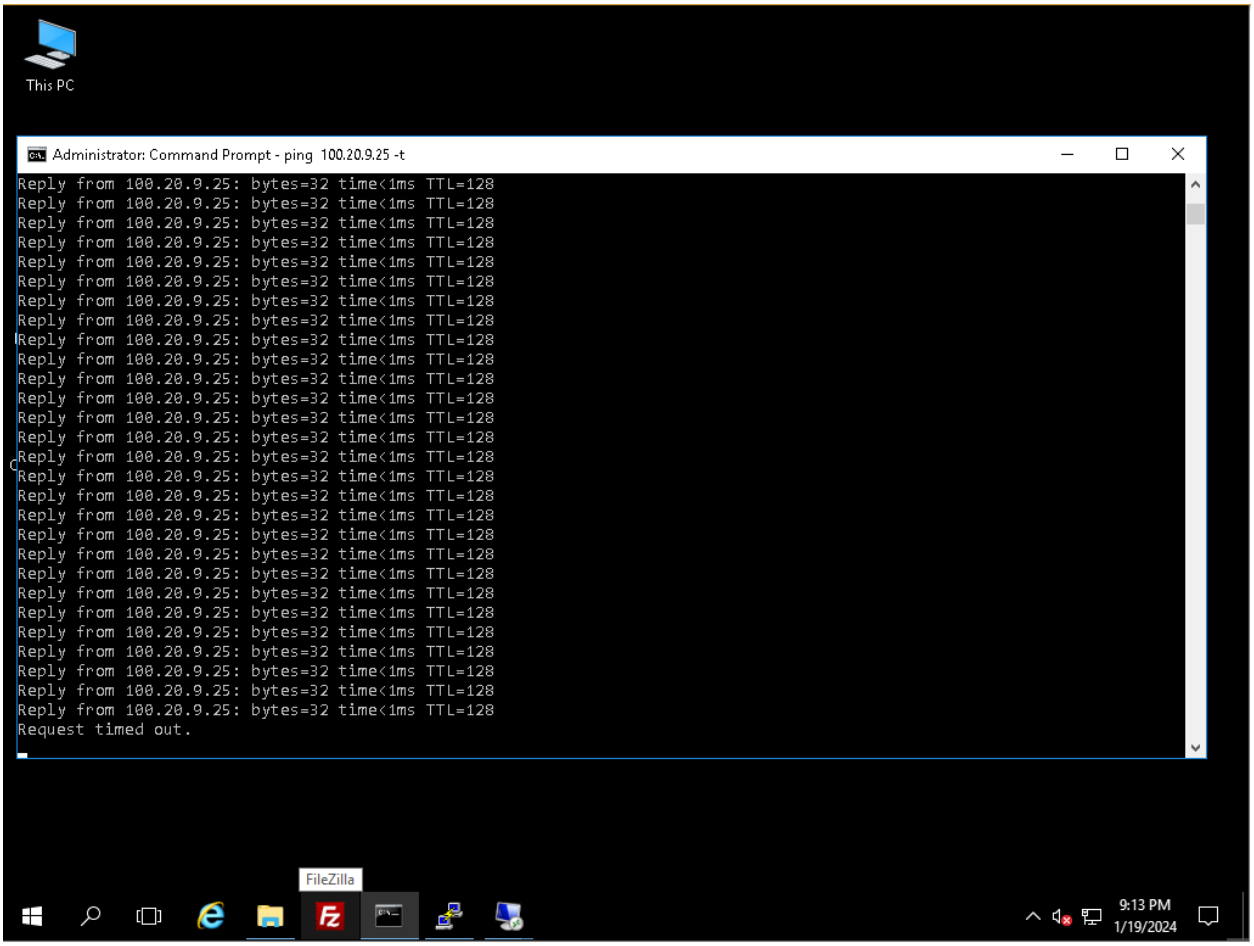
The command “netsh -r WIN-IKTLR0P6DID advfirewall show allprofiles” is used to show the systems firewall profiles.



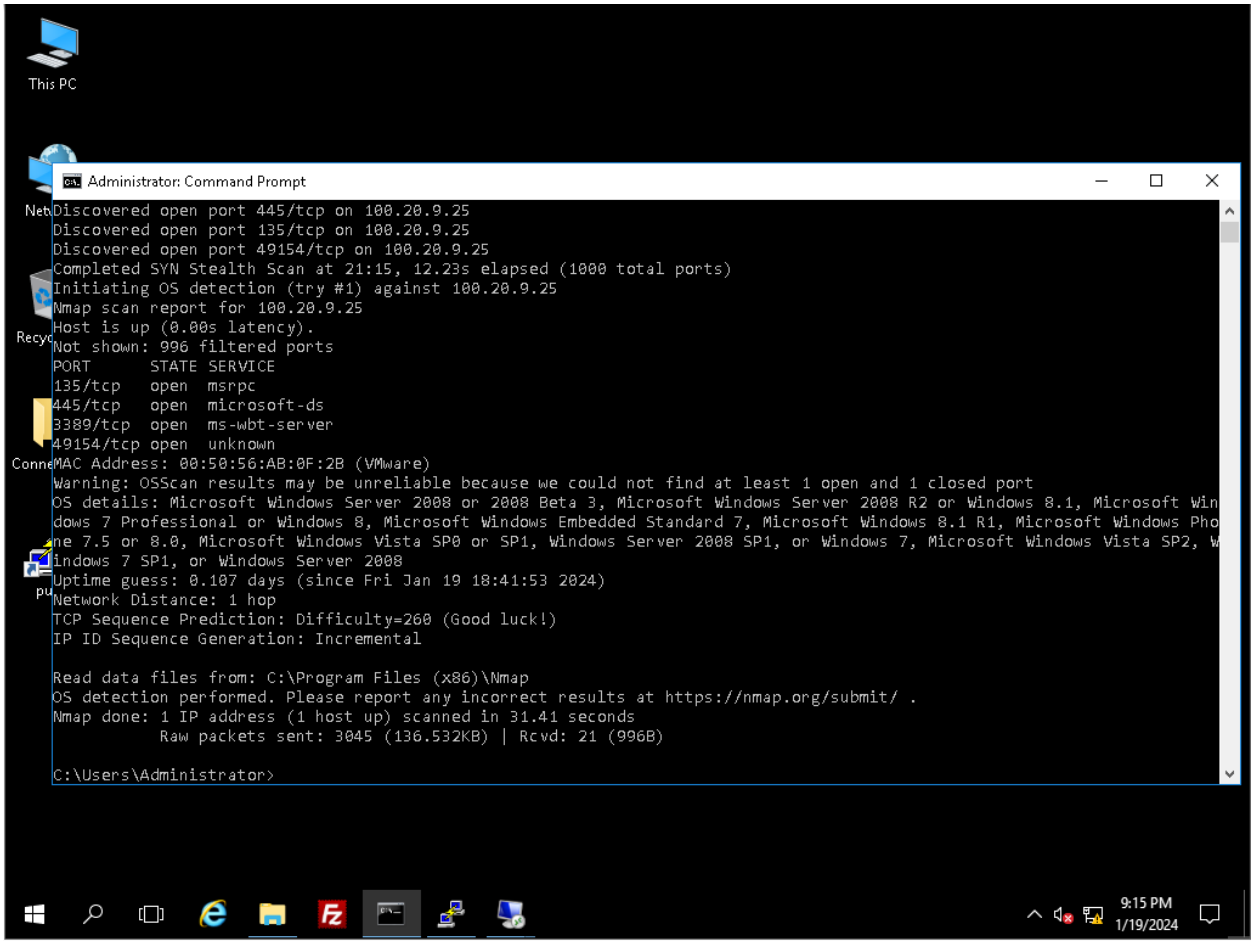
Above are the firewall rules output from the command “netsh advfirewall firewall show rule name=all > rule.txt”



Above is the remote desktop rule.



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



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.

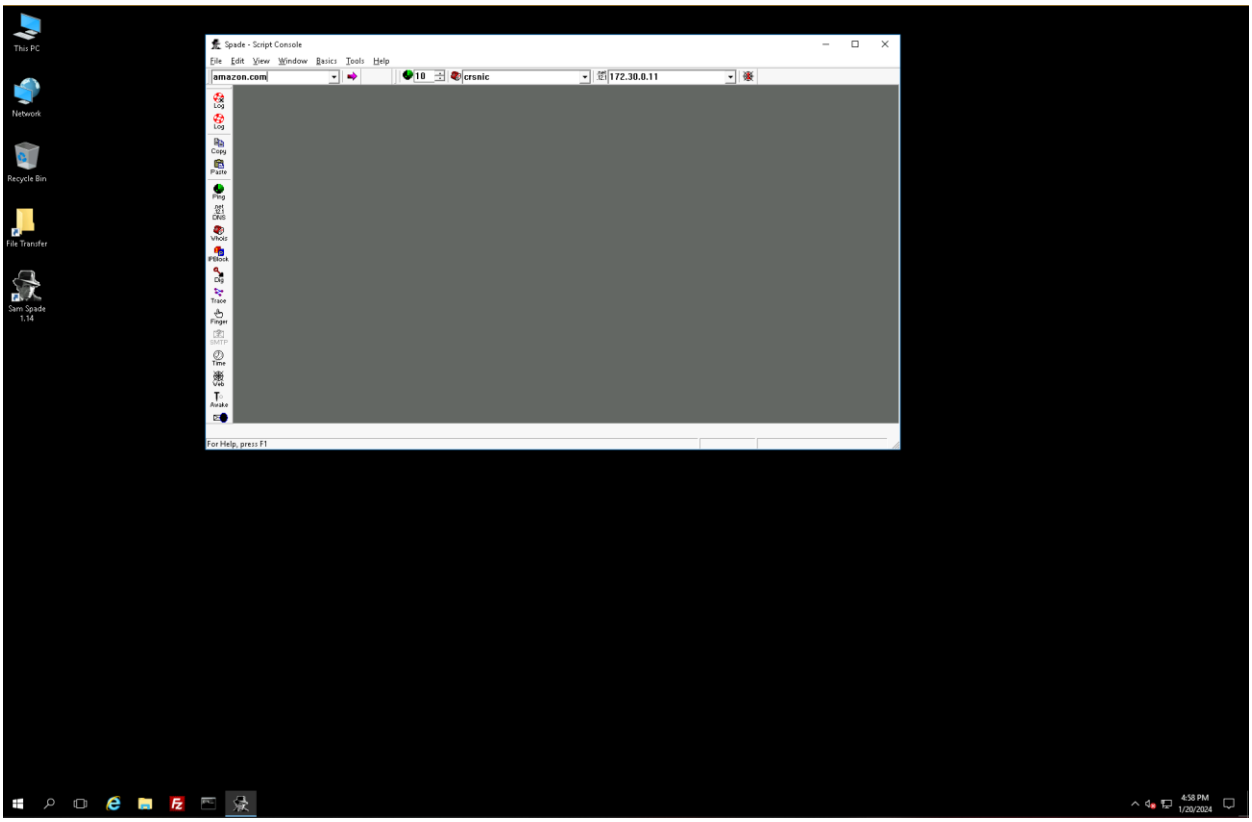
Remediation of a vulnerable system.

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 lates 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

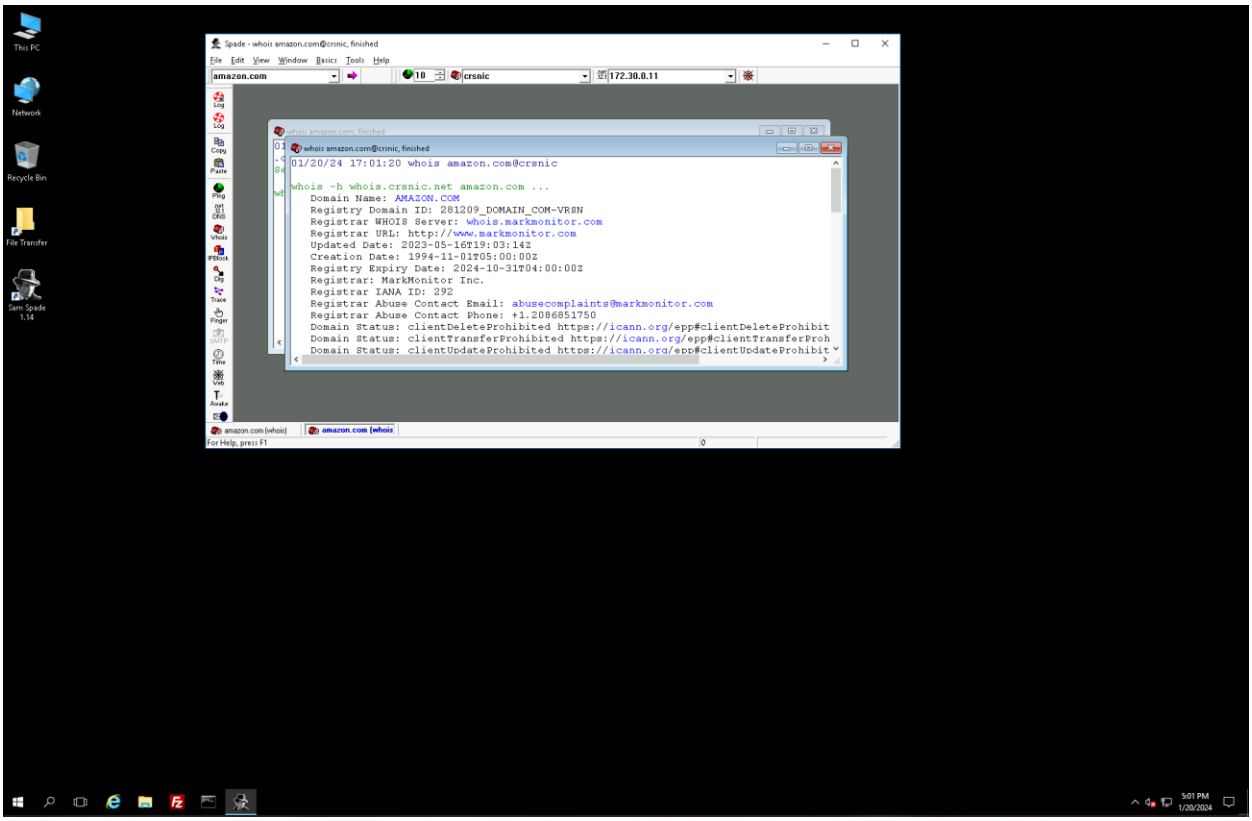
segmentation and VLANs. Another consideration would be to add an IDS (intrusion Detection System) to the network so that attacks can be detected. It is also important to keep all sensitive data backed up in case of loss or breach of integrity.

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

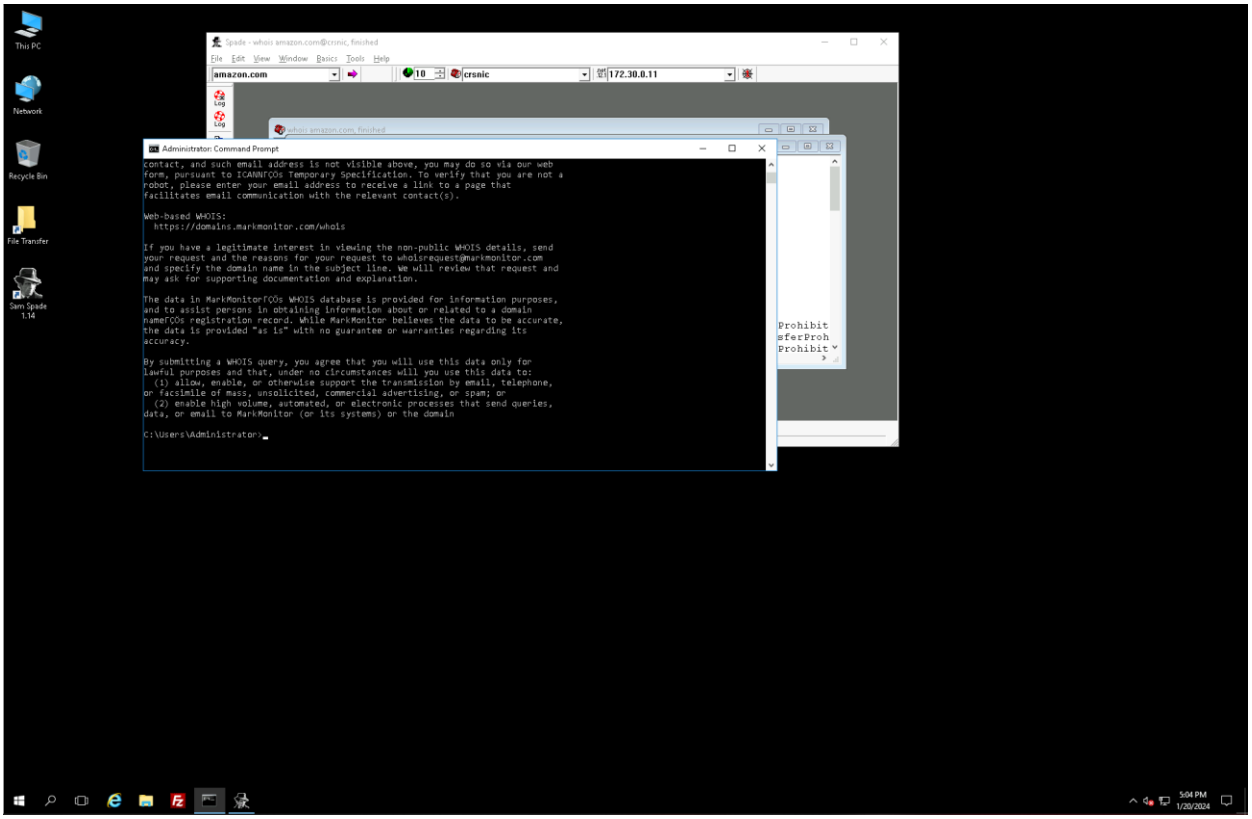
Part 1: Technical Research



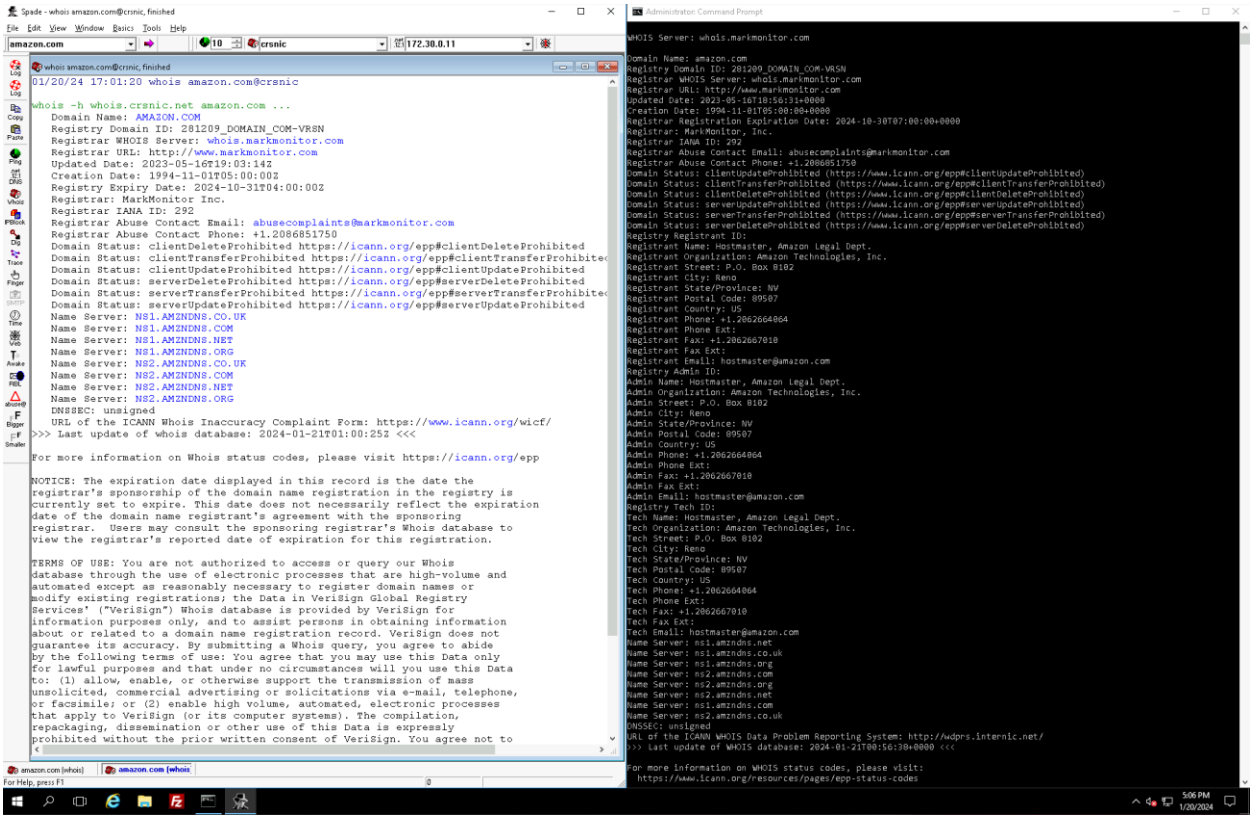
Using the Sam Spade application, the website amazon.com was entered into the search field.



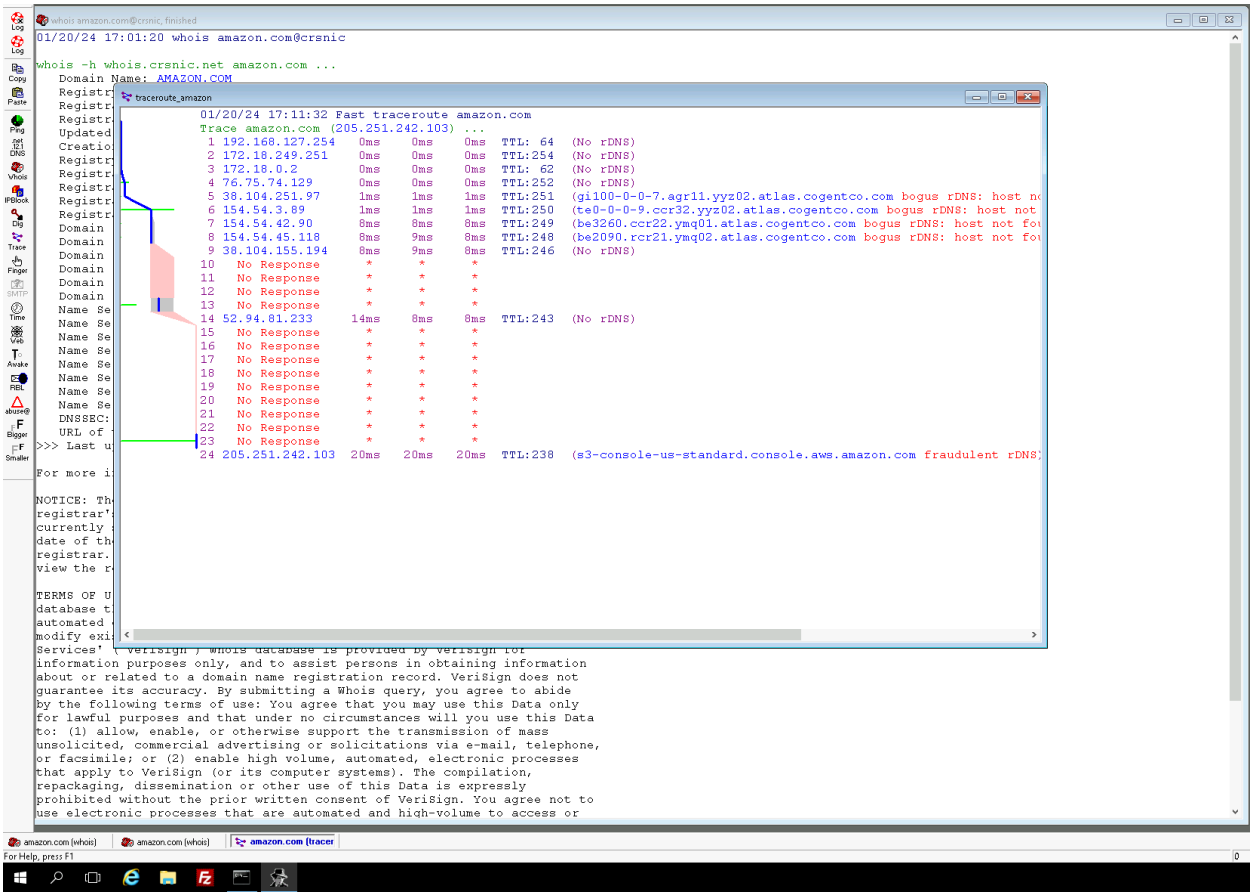
The above screenshot shows the result of selecting Basics > Whois following the search. This shows information about the owner of the domain ‘amazon.com’.



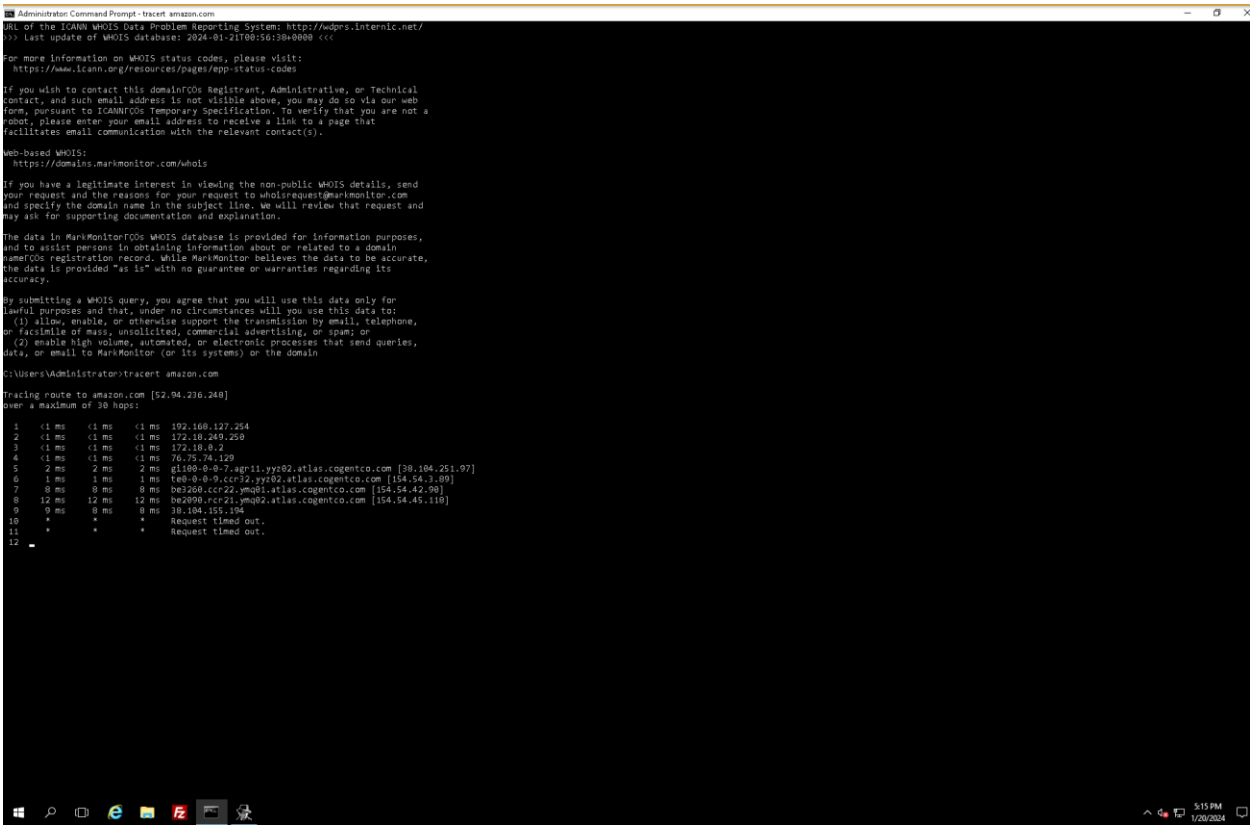
Via CMD the command “whois amazon.com” was entered to find similar information via the command line rather than an external application.



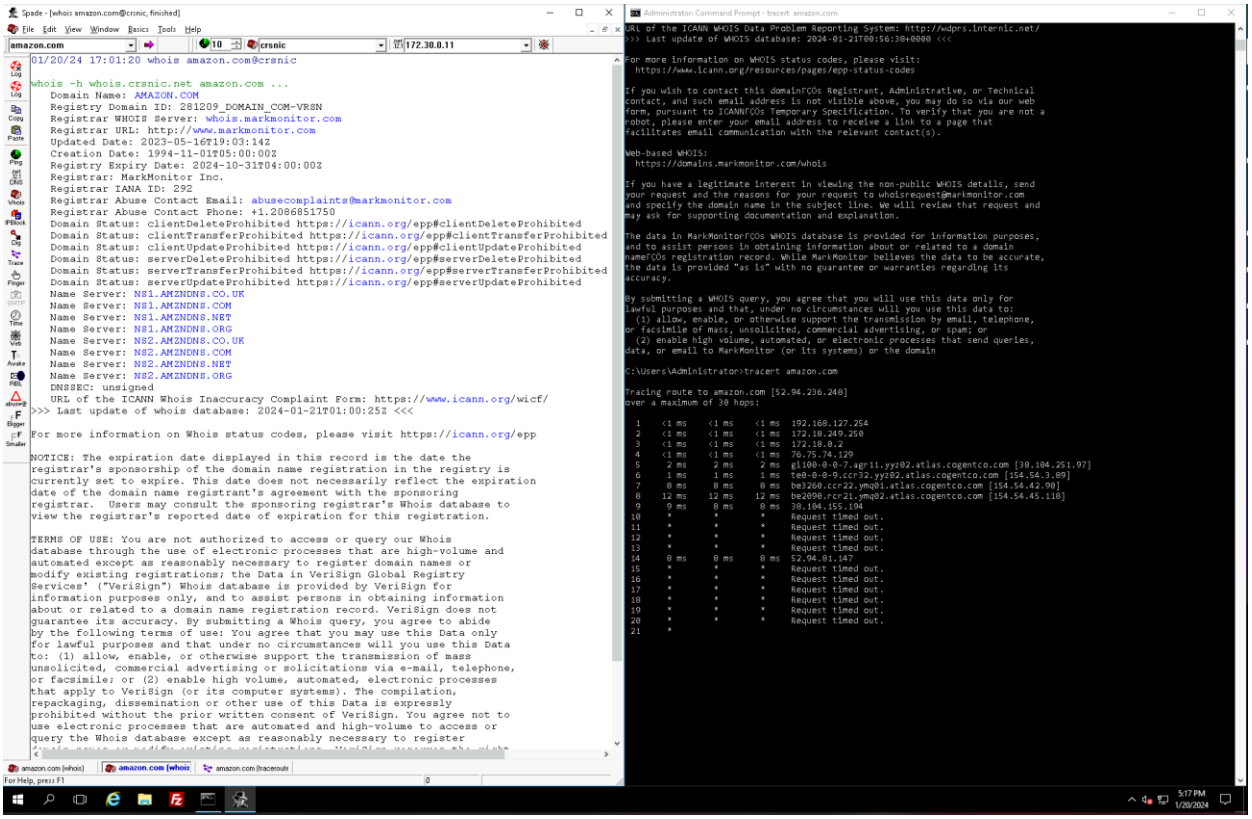
Comparing the information offered by both searches shows similar information, however it seems that using the command line shows more information.



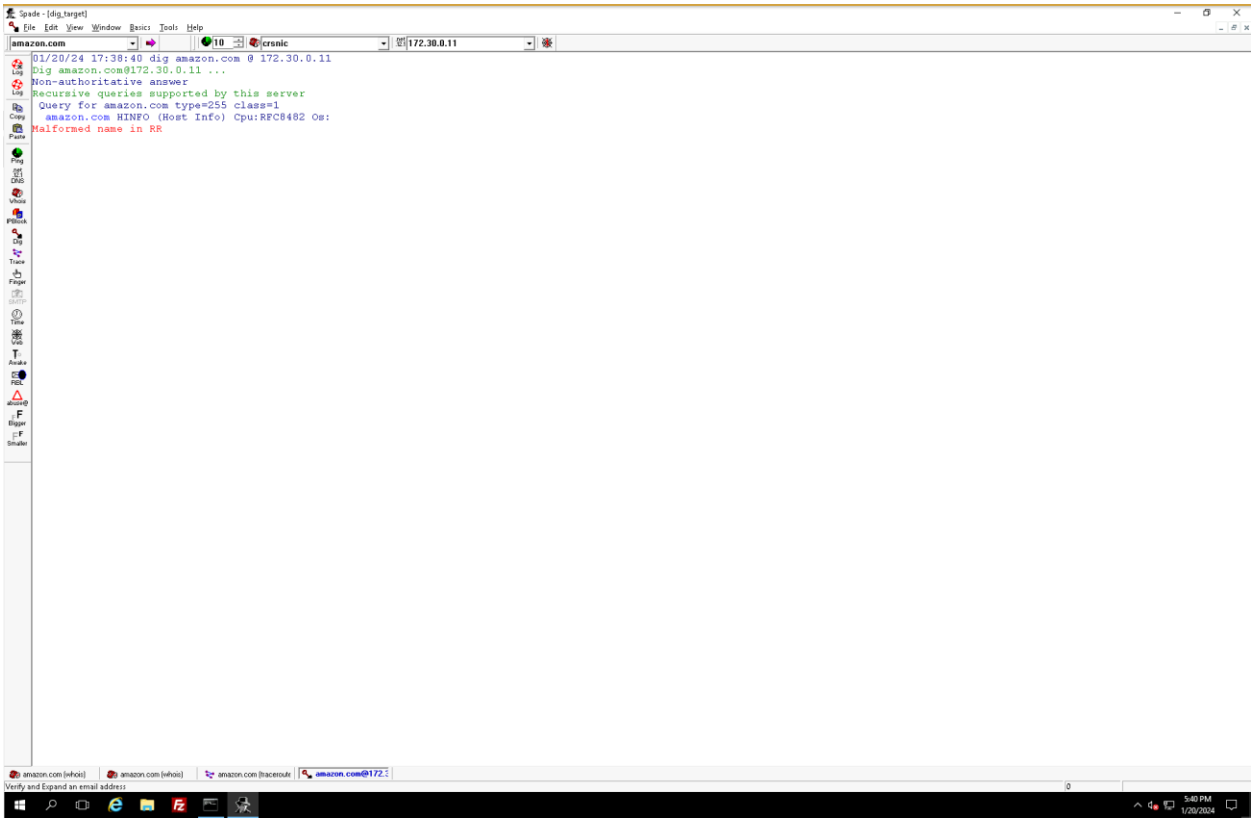
Above is the result of running a traceroute scan on amazon.com via Same Spade. The results were saved to the desktop under traceroute_amazon.



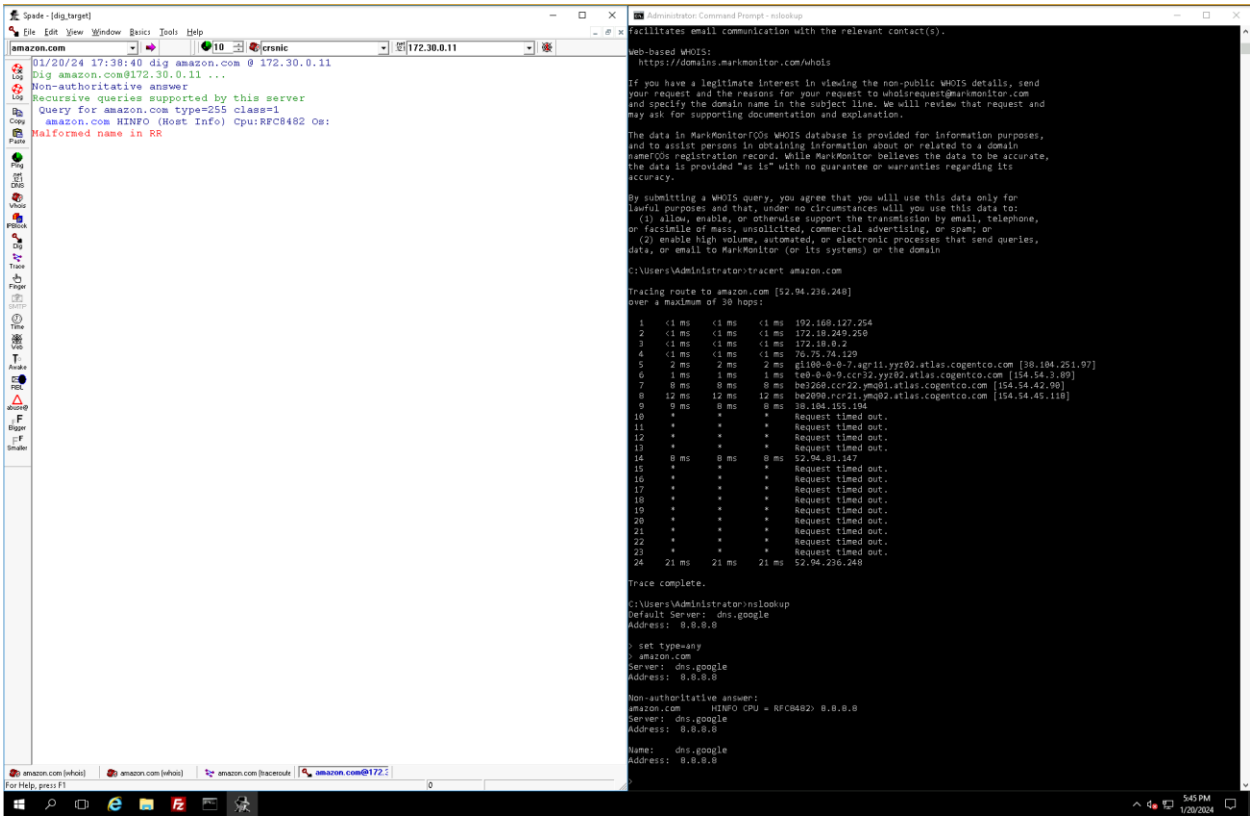
Above is the result of using the command “tracert amazon.com” to gather similar information via CMD.



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



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



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

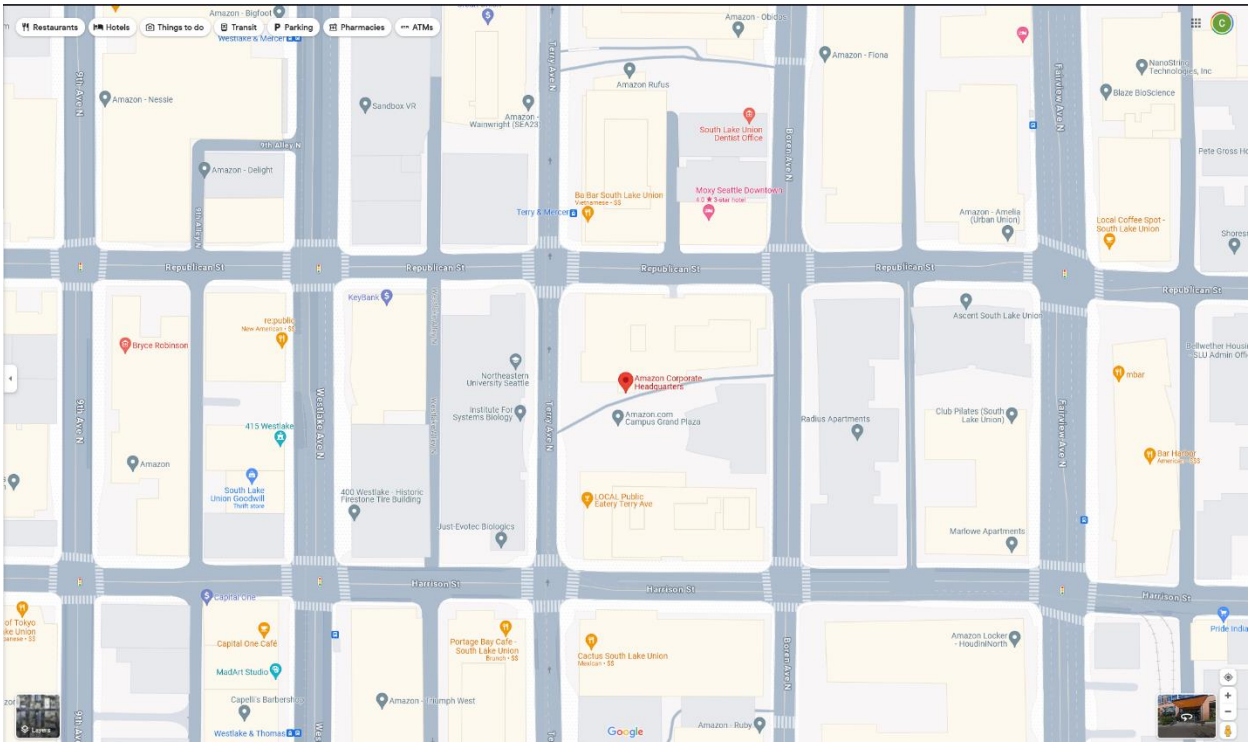
Physical Address: 410 Terry Ave N, Seattle, WA.

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.

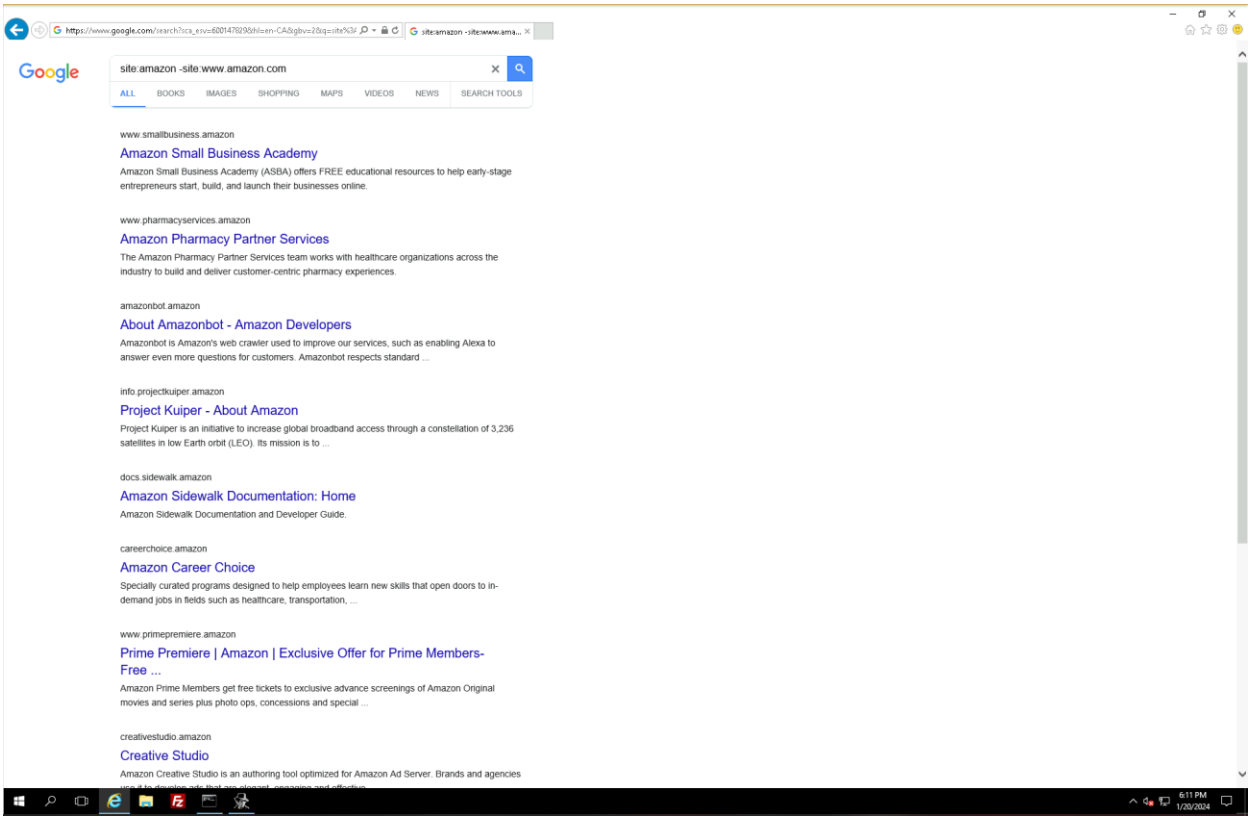
Number of employees: 1.5 million

Business Partners: N/A

Google maps streetview of Amazon headquarters.



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. 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.