Troubleshooting Network Issues

Network engineers are tasked with analyzing and troubleshooting customer issues related to navigating the company's network.

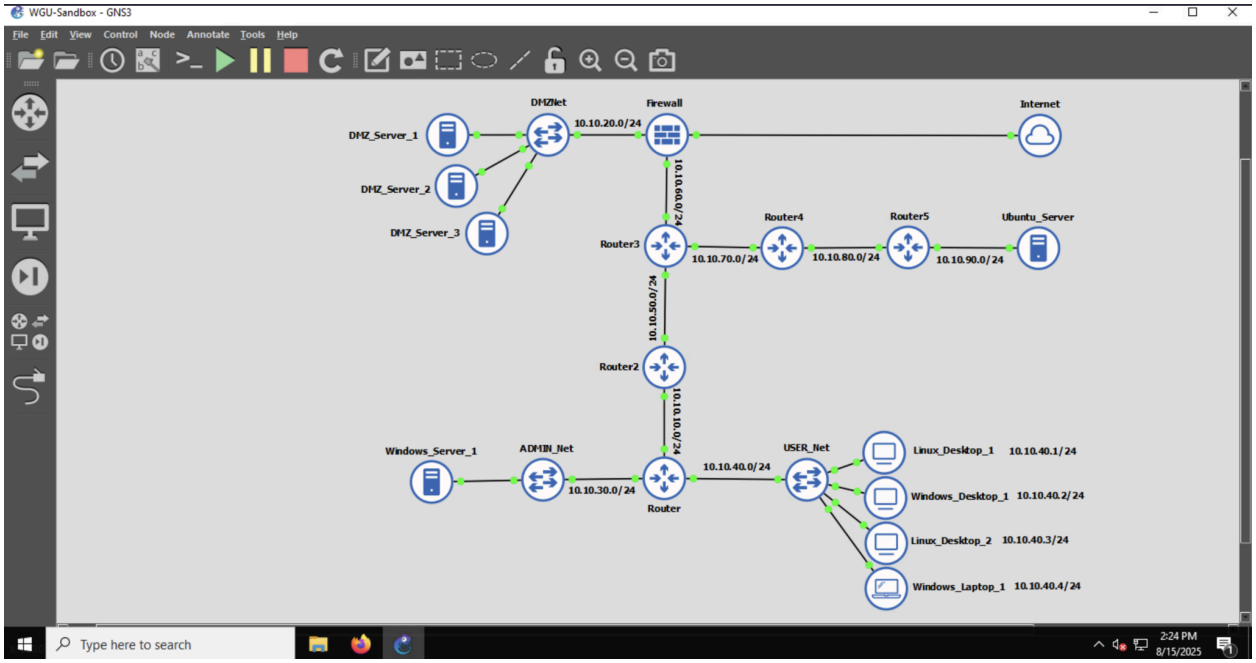

Figure: Network topology of the company

Help Desk Ticket 1

There are multiple reports of employees located in the USER_Net subnet who are unable to access www.wgu.edu, and the issue appears to be affecting the entire organization. They are being redirected to a suspicious site. A help desk technician states that the server team recently installed updates to DMZ_Server_3, which serves as the organization's DNS server. The resolution must be organization-wide.

Screenshots

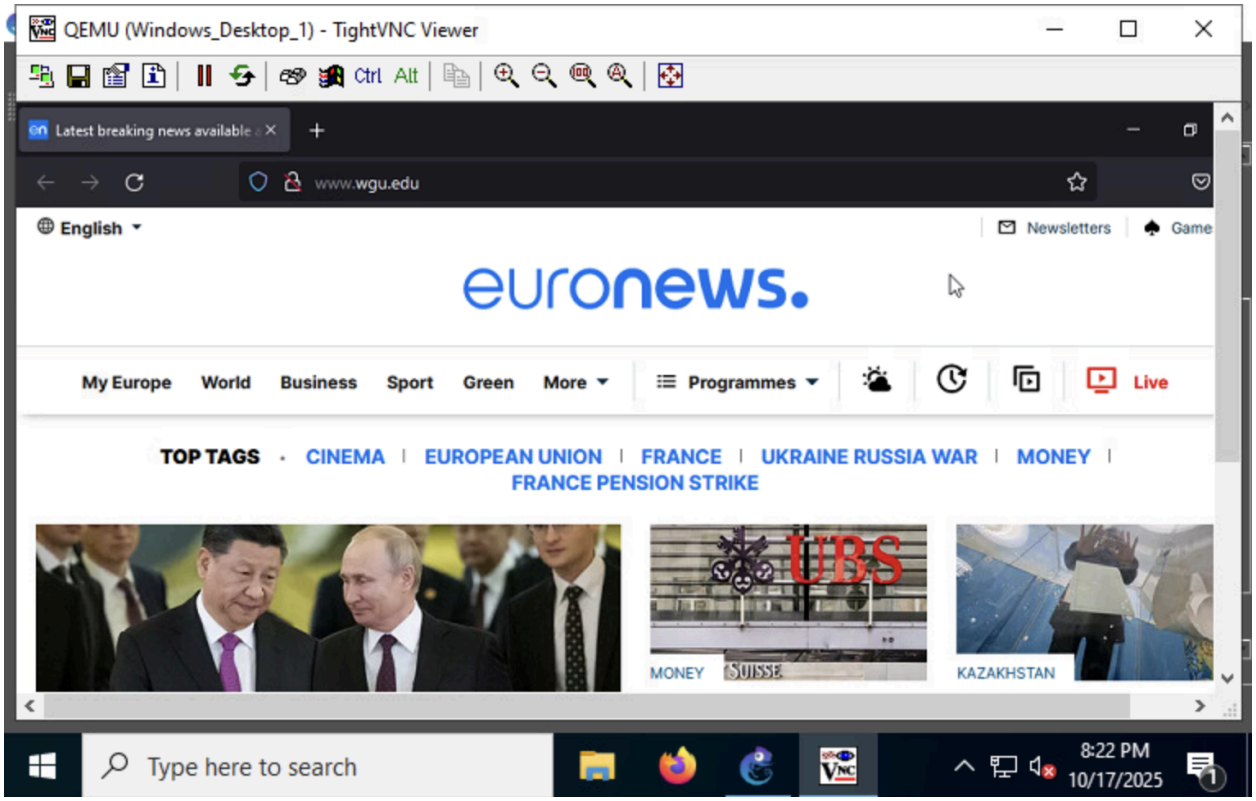

Figure 1.1: Image showing the website redirection to euronews on one of the devices (Windows_Desktop_1) on the USER_Net subnet

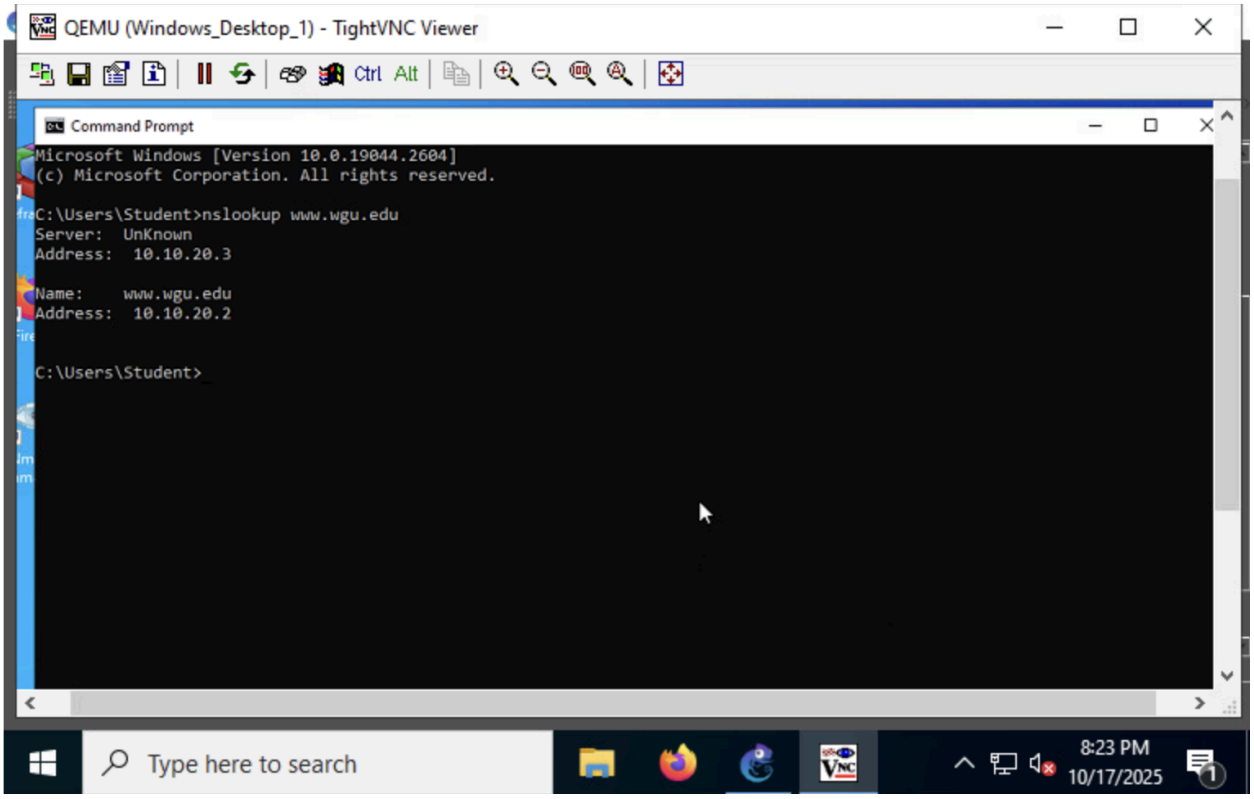

Figure 1.2: Image showing the result of the nslookup command on one of the devices (Windows_Desktop_1) that is redirected to the suspicious website

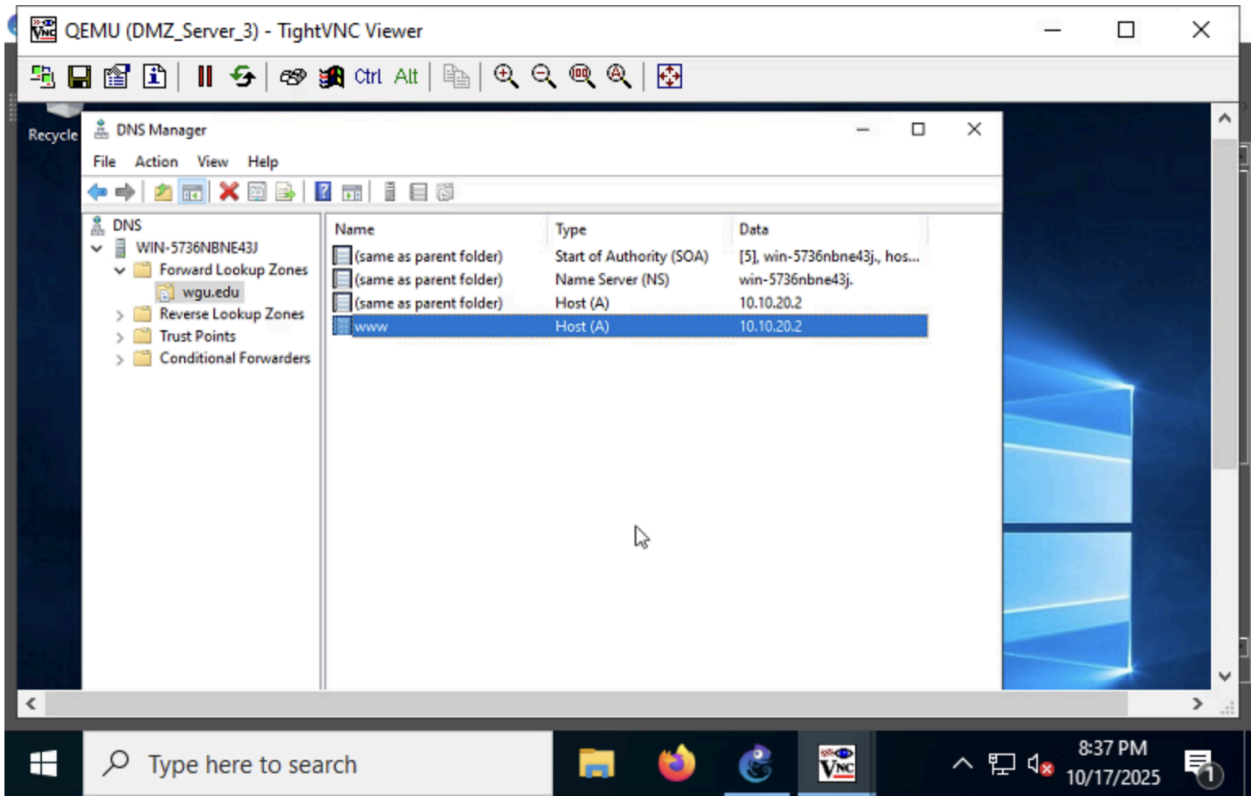

Figure 1.3: Image showing the DNS cached record on the DMZ_Server_3

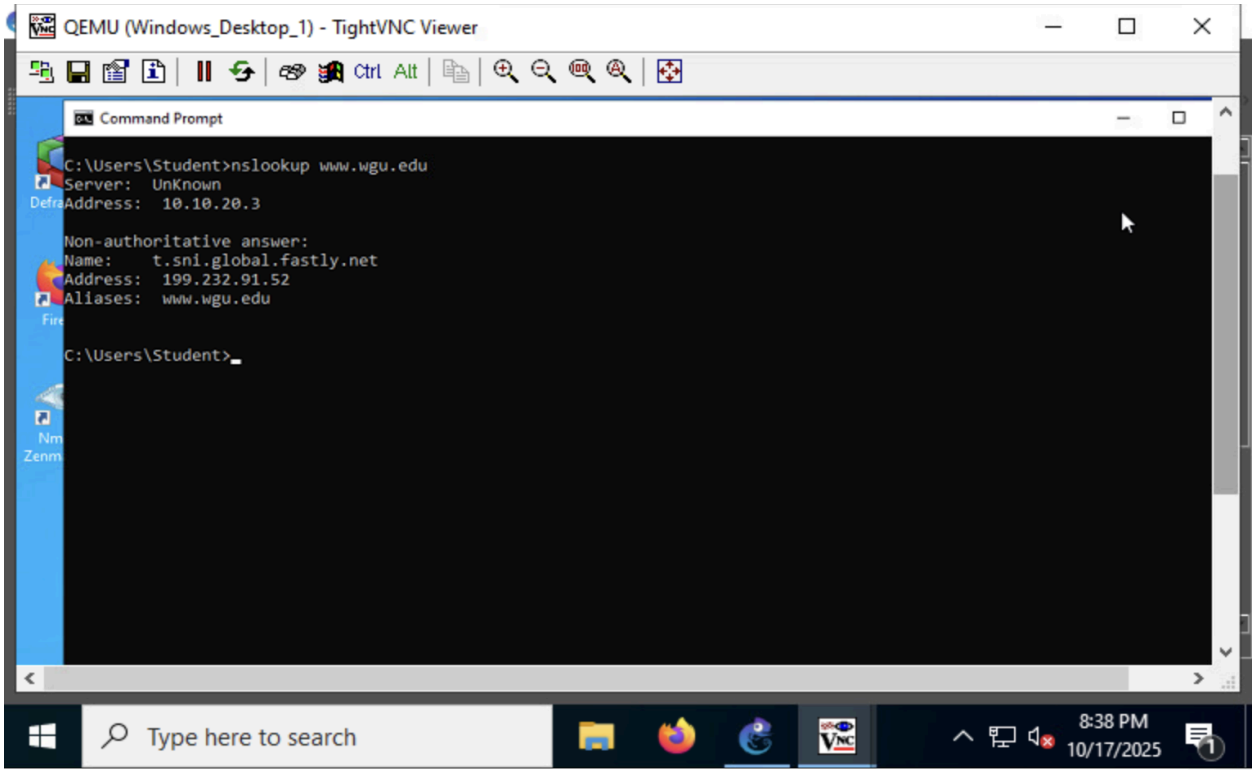

Figure 1.4: Image showing the result of the nslookup command of the website on one of the affected devices (Windows_Desktop_1) that was previously redirected to a different website

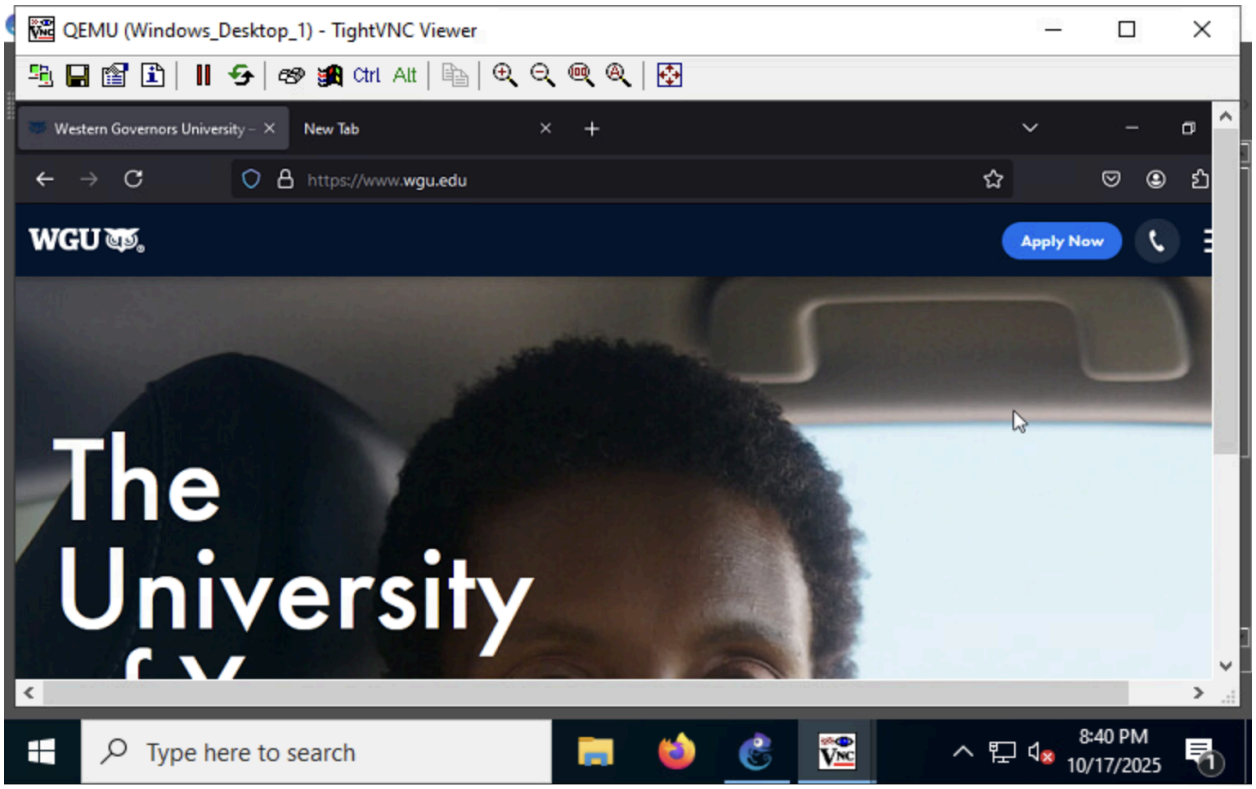

*Figure 1.5:*Image showing the access to the www.wgu.edu website on the Windows_Desktop_1

Root cause analysis

. a. List the tool(s) used to identify the problem.

- nslookup
- DNS manager

b. Explain why the tool(s) was (were) chosen to troubleshoot the problem.

- nslookup (to retrieve the domain information of the WGU website, such as the domain name, the retrieved IP address, and the DNS records)
- DNS manager (GUI tool used to manage DNS records)

c. Explain the steps of the troubleshooting process that were used to identify the problem and a resolution to solve the problem.

Problem identification

Users from the USERNet subnet were redirected to a different website when they accessed the www.wgu.edu after updating the DNS server, DMZ_Server_3. This is highly suggestive of misconfiguration of the DNS record during the server update. DNS records are crucial for accessing the internet, as they map human-readable domain names to IP addresses. They can be manually configured and cached on local devices.

The redirection to the suspicious site was verified by using one of the devices within the subnet from the USER _Net and accessing the website, 'www.wgu.edu'. It was found that the link caused redirection to a website titled "Euronews." (Figure 1.1)

The redirection, instead of failing to connect to the website, indicated that it was indeed an issue with the DNS record. The probable causes are;

- server-side DNS issue: misconfiguration during the DNS server update (highly possible)

- tampering of the host file (the mapping of the IP and the domain name) on the device

From the host device, the nslookup command is run on the WGU website to retrieve the website's information. It turned out that the website is mapped to the IP address of 10.10.20.2, which was retrieved from 10.10.20.3 (DMZ_Server_3, the server with the recent update) (Figure 1.2). It clarifies the possible misconfiguration of the local DMZ server 3.

Problem Resolution

On DMZ_Server_3, the DNS record and cache were inspected using DNS Manager (dnsmgmt.msc). Under the forward lookup zone, it was found that there were cache entries of wgu.edu mapping to the IPv4 address 10.10.20.2, which caused the redirection to that IP address instead of the actual WGU website. (Figure 1.3)

The cache entry for wgu.edu, which pointed to the incorrect IP address, was deleted, and then the DNS record was rechecked on the CLI of Windows_Desktop_1. This time, the domain was mapped to the actual IP address of the website, 199.232.91.52. (Figure 1.4)

For confirmation, the WGU website was accessed through the browser, which directed the user to the correct website. (Figure 1.5)

Help Desk Ticket 2

A complaint came in that a certain organization is hosting an illegal FTP site to download copyrighted software. The security team has provided a PCAP file capturing all FTP traffic on the network. They have asked you to identify where the FTP site is being hosted.

Screenshots

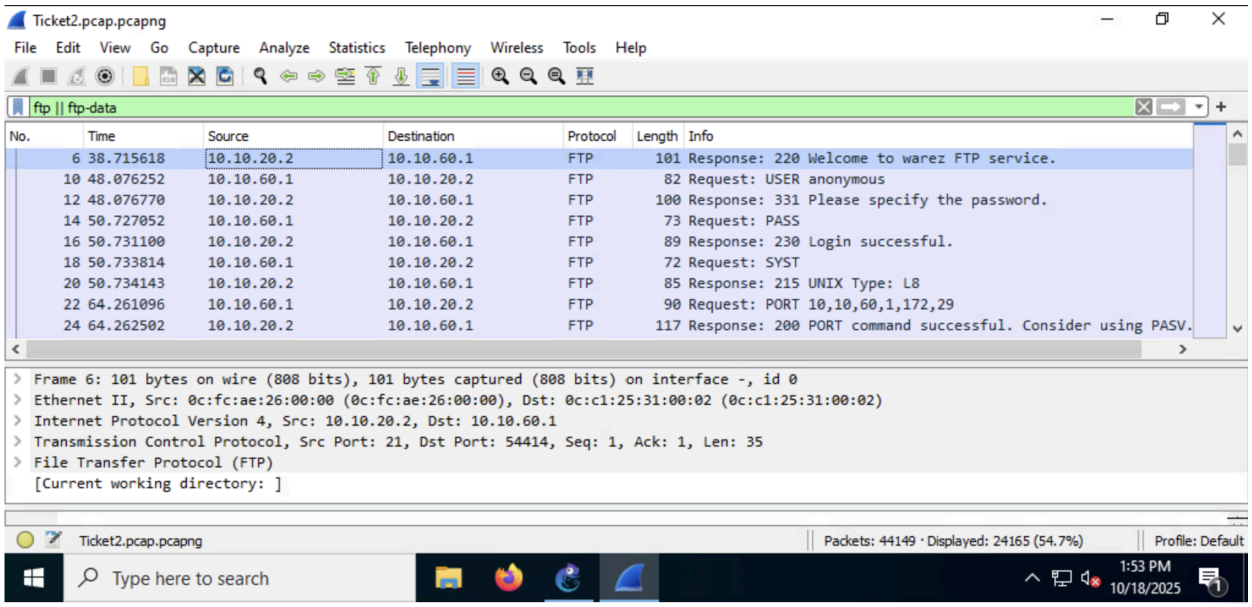

Figure 2.1: result of the traffic that used the FTP protocol in the .pcap file

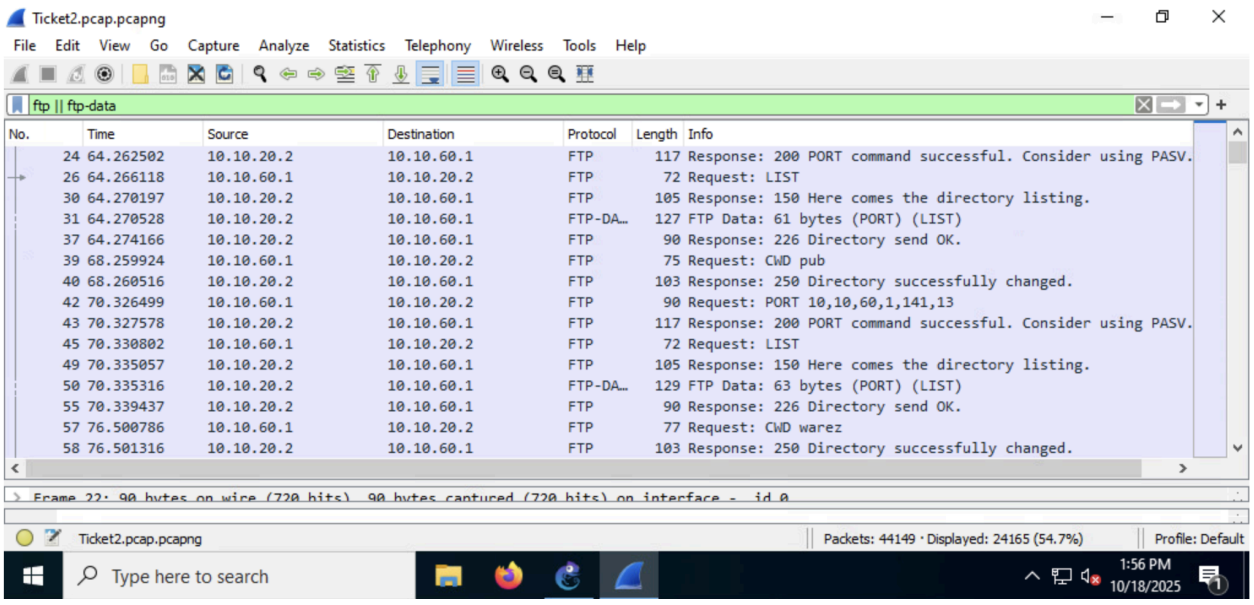

Figure 2.2: result of the traffic that used the FTP protocol in the .pcap file

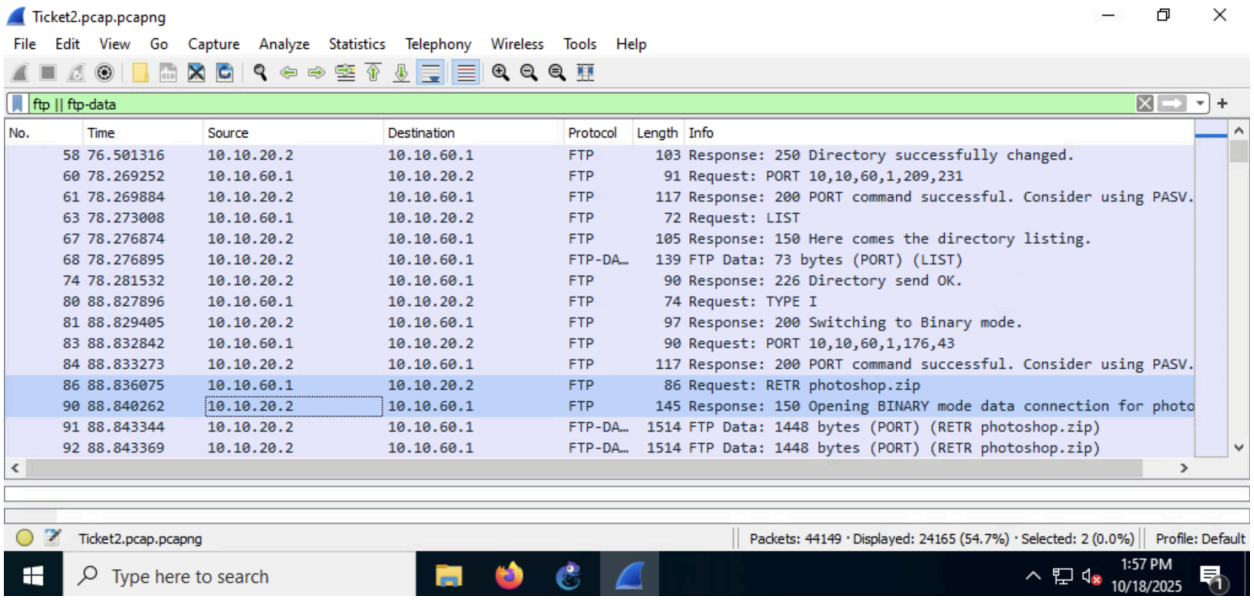

Figure 2.3: result of the traffic that used the FTP protocol in the .pcap file

Root cause analysis

a. List the tool(s) that you used to identify the problem.

- Wireshark

b. Explain why you chose the tool(s) to troubleshoot the problem.

- Wireshark (An open source GUI network traffic analyzer used to capture and inspect data packets of each layer, such as traffic flow, protocols used, and source and destination of the data. It is very useful in analyzing and troubleshooting network issues. It can also be used to inspect the pre-captured network .pcap file. From the captured FTP traffic flows, a lot of information can be extracted and point out the hosting illegal server and the requesting client, as well as all the detailed actions performed.) (Wireshark, n.d.)

c. Explain the steps of the troubleshooting process that were used to identify the illegal FTP site and a recommendation to solve the problem. Include the IP address of the illegal FTP site.

Problem identification

The network traffic snapshot, in the form of a .pcap file, was inspected using Wireshark and filtered (using ftp || ftp-data) to examine the traffic that only used FTP sessions. (Figure 2.1)

From lines 6 to 16, it was found that a successful login to the FTP server occurred. The source of the FTP server was 10.10.20.2 (the DMZ_Server_2), where the client accessed the service using the IP address of 10.10.60.1. (Figure 2.1) After logging, it is noted that the client ran the PORT commands on the FTP server, accessed the directories. (Figure 2.2)

"FTP bounce attack takes advantage of the PORT command in FTP, which is designed to forward FTP traffic to another server. An attacker can exploit this vulnerability to bypass firewall restrictions, thereby gaining access to systems that are otherwise blocked by firewall ACLs. Any use of the PORT command in FTP traffic should be investigated to determine if it is malicious." (Poston, 2019)

On lines 86 and 90, it is evident that the client requested the server to download the 'photoshop.zip' folder, where the server authenticated. The following traffic revealed that the zip file was sent to the client. (Figure 2.3)

All of this evidence proved that the company's internal server, 10.10.20.2, was hosting an FTP site.

Recommended problem resolution

First, isolate the server from the network and then disable the FTP service. Verify if the service is authorized to run or was being hosted illegally on that server. Check for any symptoms and signs of a cyberattack or credential leakage. Change the credentials to be safe. Also, examine the client IP address to determine if it is from an internal employee or if it has been spoofed by a malicious actor. Check the 'photoshop.zip' file and contain and remove any suspicious or malicious files, and also check for any backdoor implementations. Disable any unnecessary open ports. Update the operating system regularly and apply patches as soon as they become available. Continue to monitor the traffic and analyze the log file to detect any abnormalities or intrusions.

Help Desk Ticket 3

The host "Ubuntu_Server" cannot get to any of the assigned networks or the internet, which is preventing the server from pulling the required security patches. The resolution must be organization-wide.

Screenshots

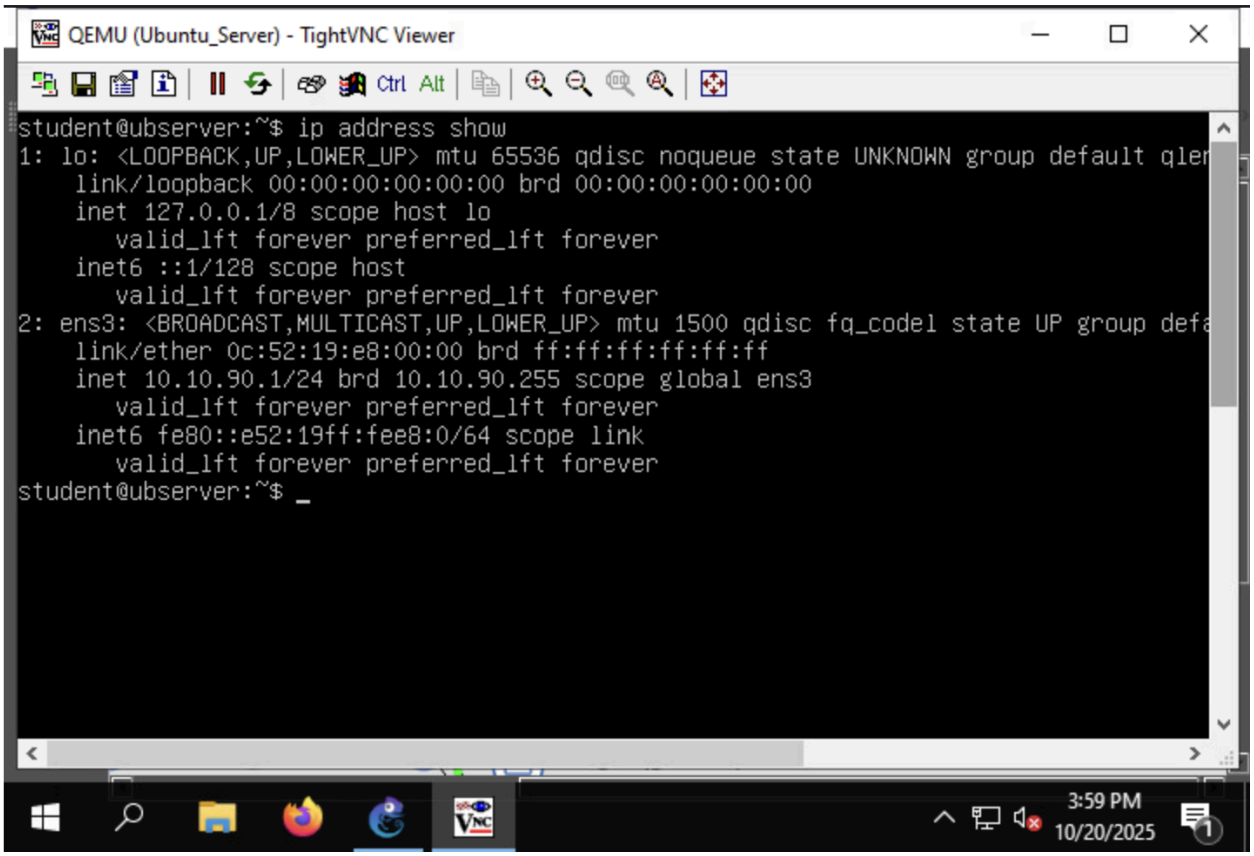

Figure 4.1: Image showing the IP configuration on the interfaces of the Ubuntu Server

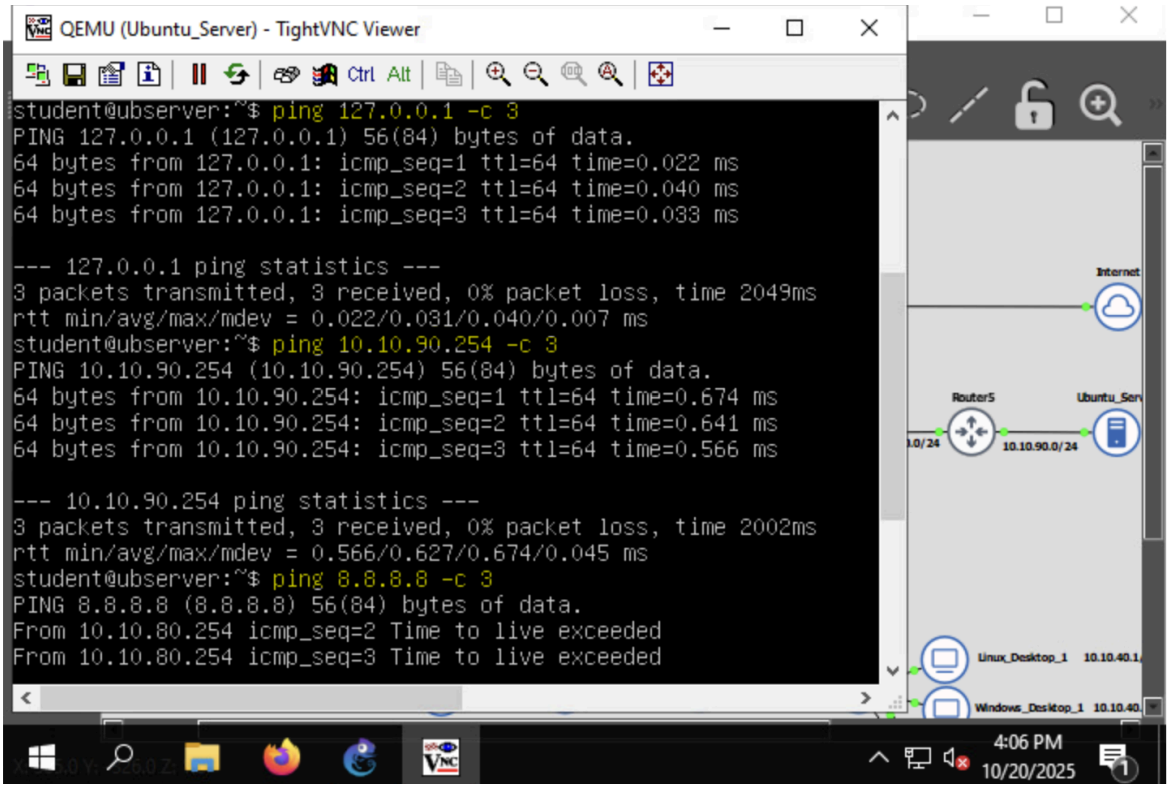

Figure 4.2: Image showing the result of pinging different addresses

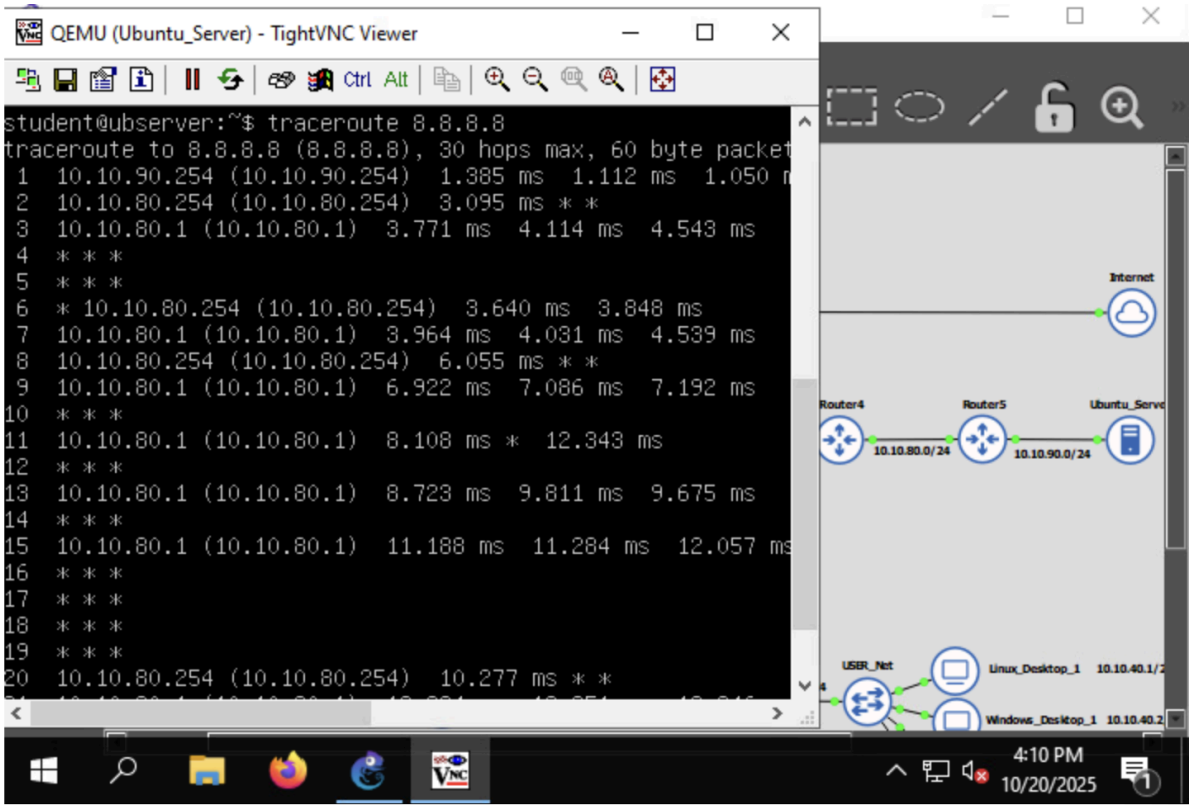

Figure 4.3: Image showing the result of the traceroute command from the server to the Internet

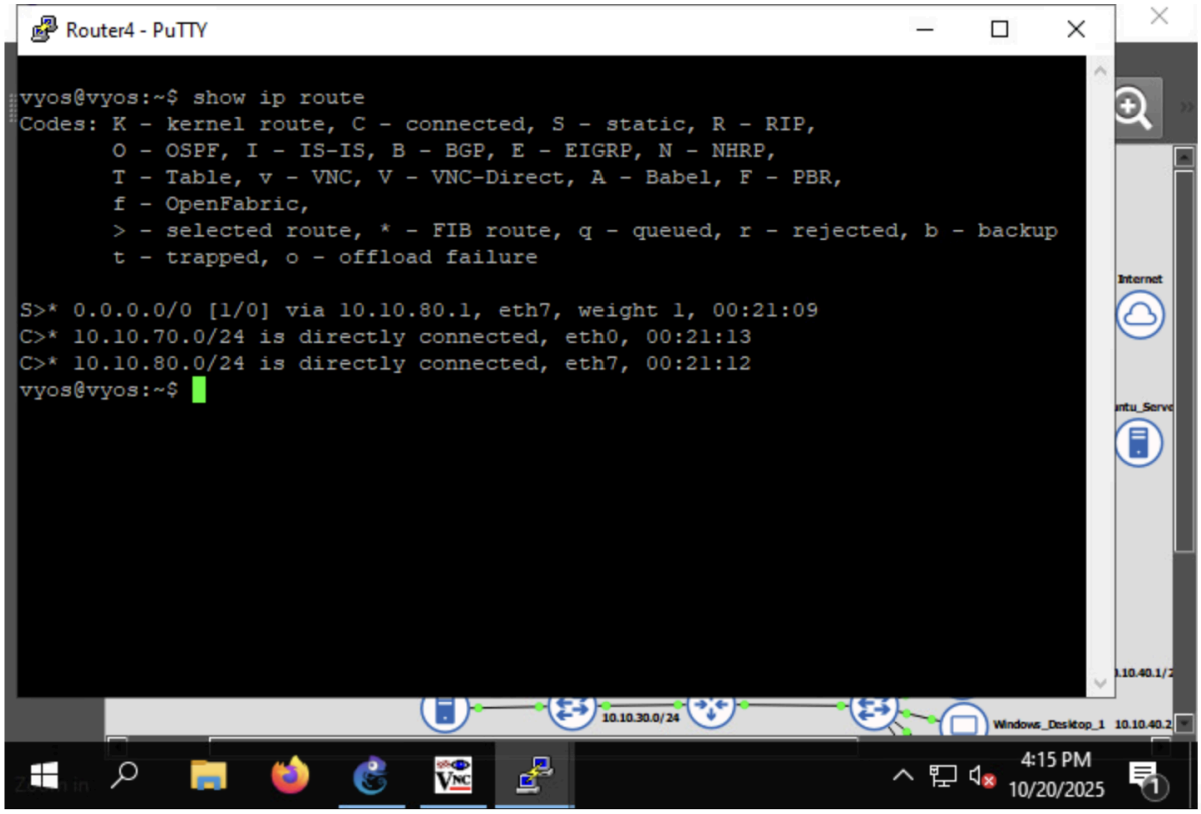

Figure 4.4: Image showing the routing configuration on Router 4

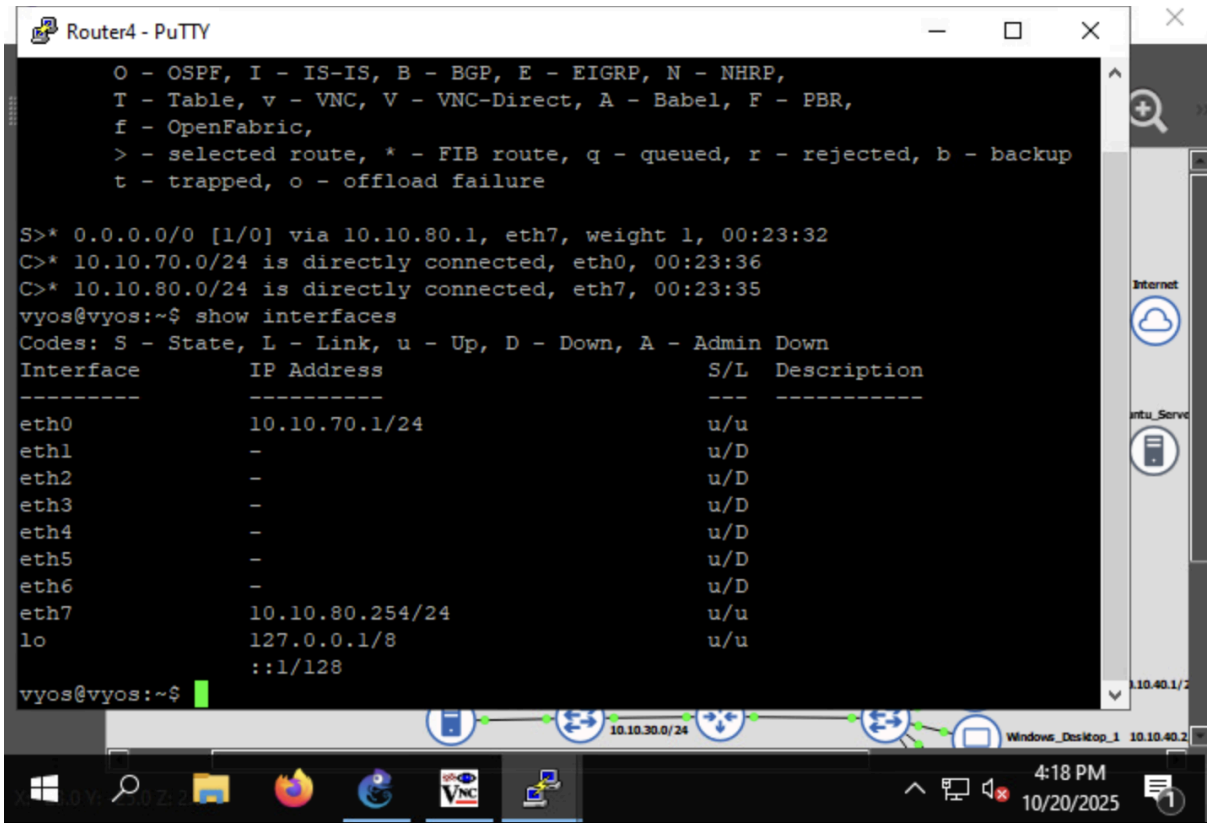

Figure 4.5: Image showing the detailed status of the interfaces on Router4

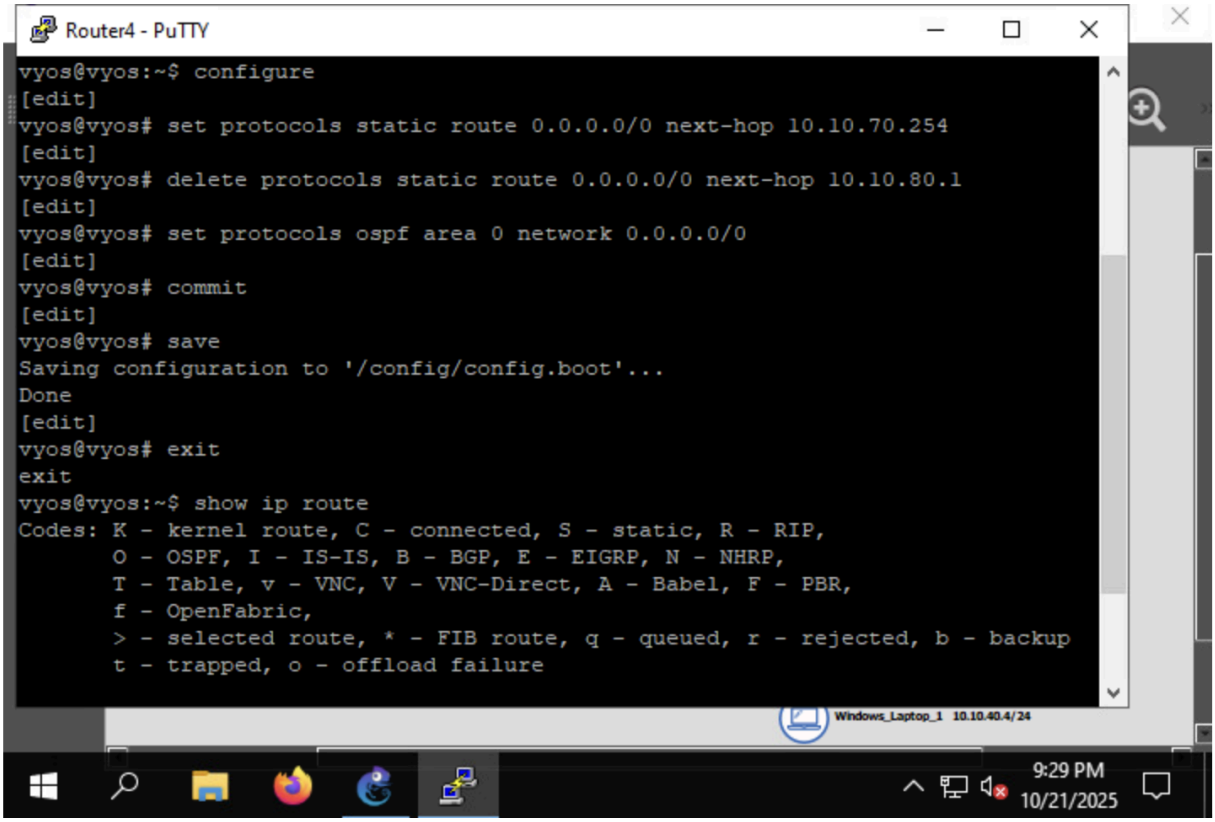

Figure 4.6: Image showing the configuration of routing on Router 4

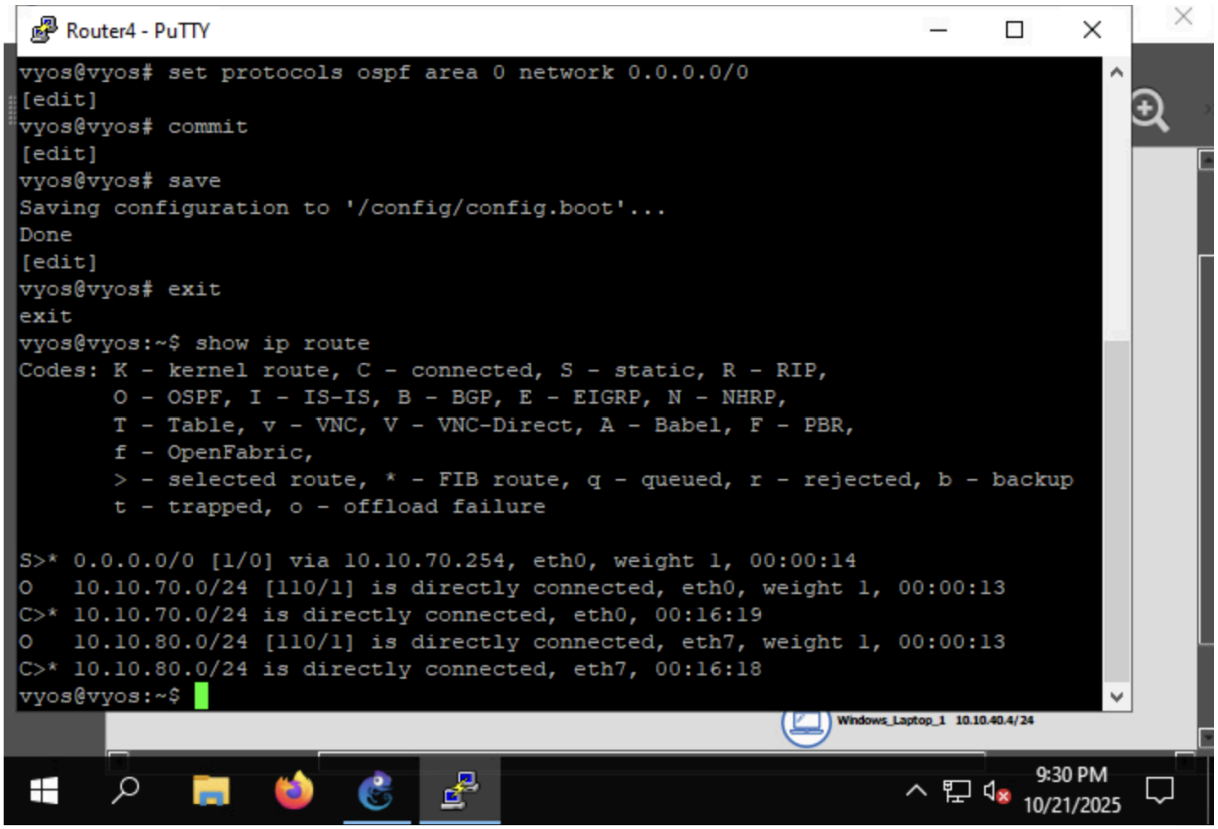

Figure 4.7: Image showing new routing configuration on Router 4

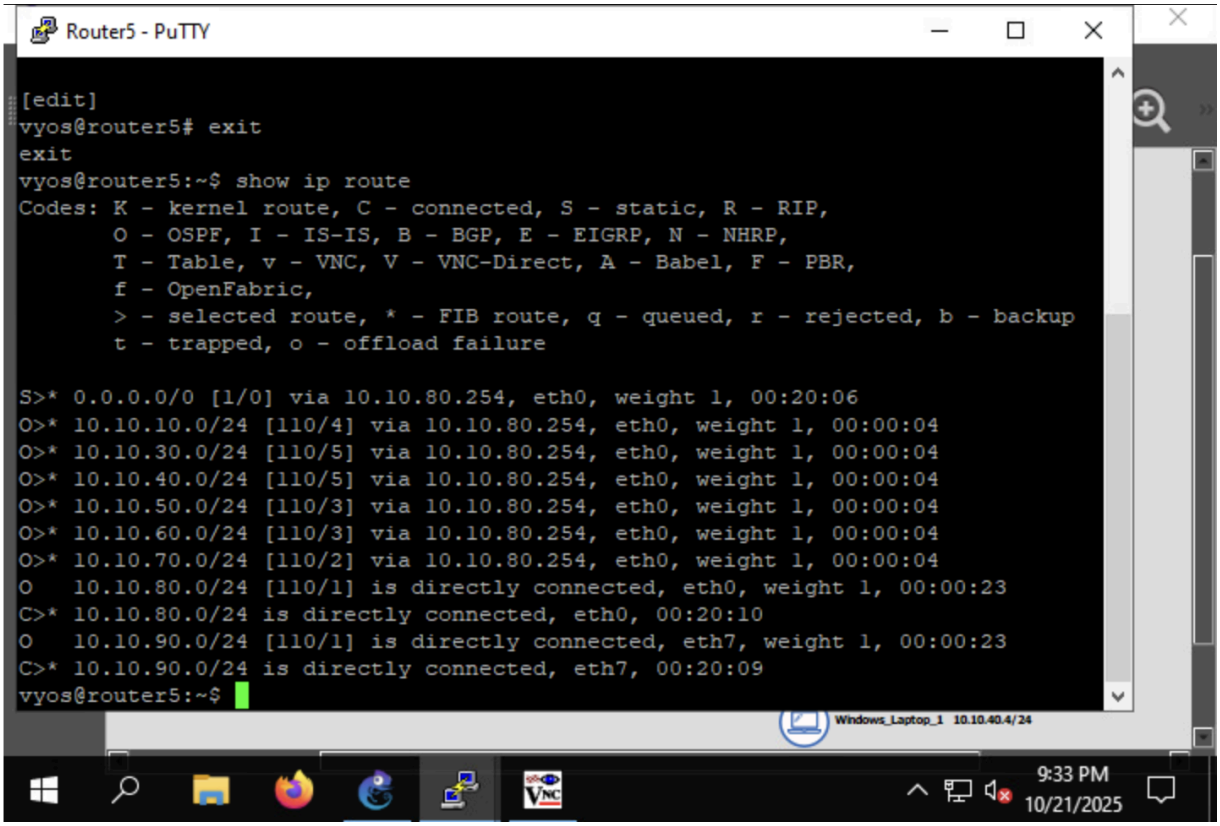

Figure 4.8: Image showing new routing configuration on Router 5

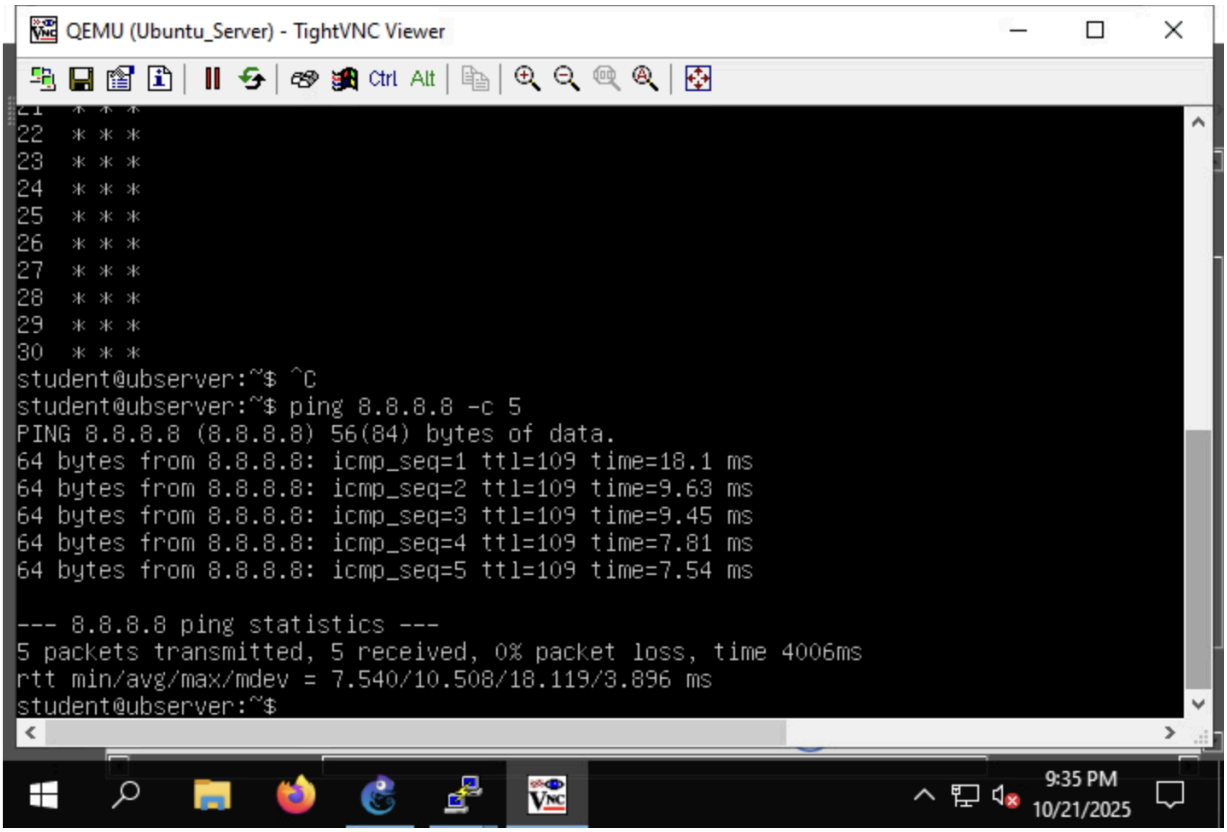

Figure 4.9: Image showing a successful ping to the Internet from the Ubuntu Server

Root cause analysis

2. Create a root cause analysis write-up by doing the following:

a. List the tools that you used to identify the problem.

- traceroute
- ping
- set protocols static route
- delete protocols static route
- set protocols ospf area _ network

b. Explain why you chose them to troubleshoot the problem.

- ping (to test the reachability of the destination, including information such as round-trip time, time to live, packet loss, and success %)
- traceroute (used to view detailed hops of the traffic from the source to the destination, useful in figuring out the location of the issue in routing)
- set protocols static route (used to configure the default route on the router) (VyOS Networks, n.d.)
- delete protocols static route (used to remove the existing static route on the router) (VyOS Networks, n.d.)
- set protocols ospf area _ network (used to configure OSPF on the router) (VyOS Networks, n.d.)

c. Explain the steps of the troubleshooting process that were used to identify the problem and a specific recommendation to solve the problem for the organization.

Problem identification:

Users complained that Ubuntu Server was unable to reach the internet. To exclude each probable cause, it is verified by pinging different IP addresses.

- ping the loopback address (127.0.0.1) - to exclude the NIC/Network driver issue
- ping the gateway IP address (10.10.90.254) - to exclude misconfiguration of gateway IP
- ping the public IP address (8.8.8.8) - to test the reachability to the external network

From the test, it was found that the server could reach the default gateway, but could not access the internet. (Figure 3.2) To pinpoint the exact location of the issue, the traceroute command was used to view each hop along the traffic path. The output shows that a loop was forming between Router 5 (10.10.80.1) and Router 4 (10.10.80.254), where the issue could lie in Router 4, with sending traffic back to Router 5 instead of forwarding it to Router 3. (Figure 4.3)

Problem resolution:

The routing table on Router 4 was accessed, and it was noted that the default route is pointing back to Router 5's IP address, which is 10.10.80.1, resulting in a loop. (Figure 4.4) A new default route was configured to forward traffic to 10.10.70.254 (Router 3's interface), and

the old existing route that pointed back to Router 5 was removed. (Figure 4.6) During the analysis of the network issue, it was also noted that both routers, 5 and 4, were missing OSPF configuration. Thus, OSPF was configured on both routers in area 0 to coordinate with other routers in the corporate network. (Figure 4.6-8)

After the configurations were completed on the routers, a ping was sent to the public IP address from the Ubuntu Server, and this time, the ping was successful.

Recommendation:

To maintain consistency and prevent configuration drift, it is recommended to maintain a standard configuration practice and provide proper documentation of all configurations made on each device, along with log file inspection. For effective and efficient management, it is highly recommended to utilize network automation tools such as Ansible, Puppet, or Chef, which are particularly useful for configuration management.

Help Desk Ticket 4

A user complains that he cannot access the internet or network resources on his company laptop (Windows_Laptop_1) when it is connected via an Ethernet cable to the office network.

Screenshots

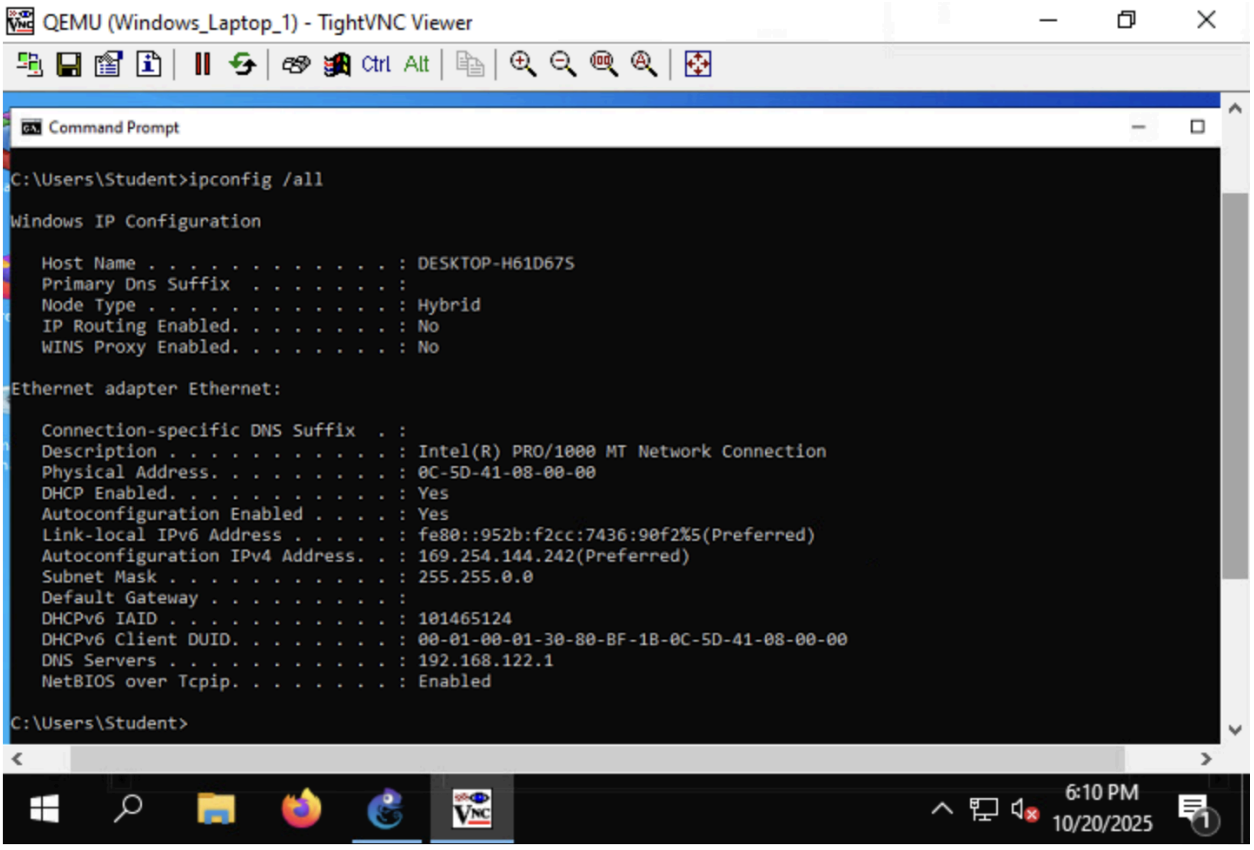

Figure 4.1: Missing default gateway on Windows_Laptop_1

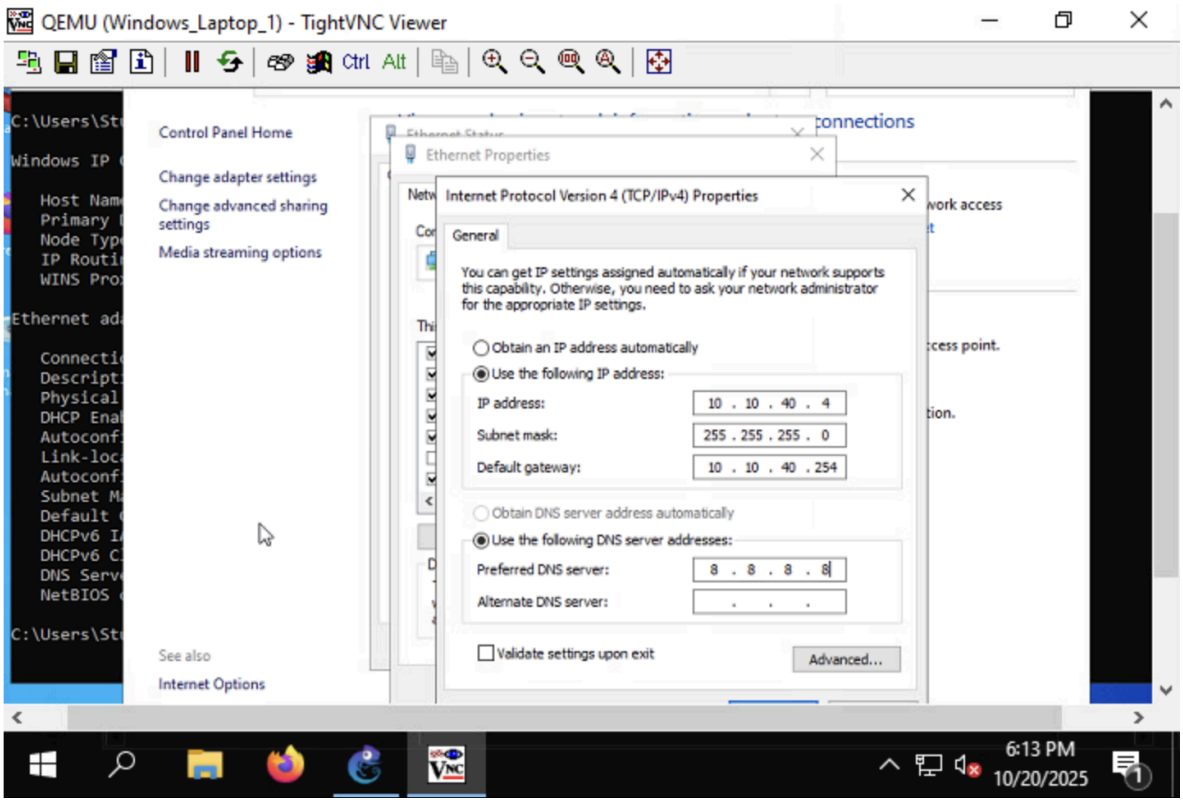

Figure 4.2: Image showing the manual configuration of IPv4 properties on Windows_Laptop_1

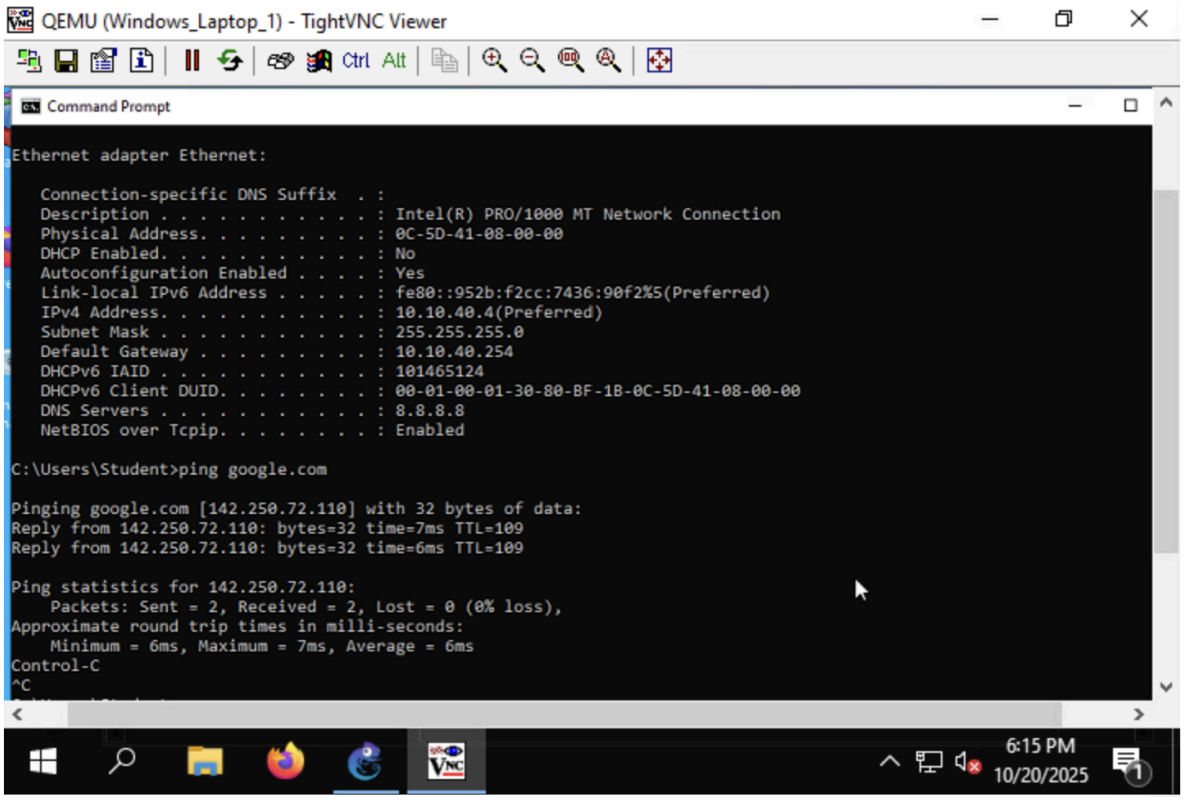

Figure 4.3: Image showing the successful ping to google.com

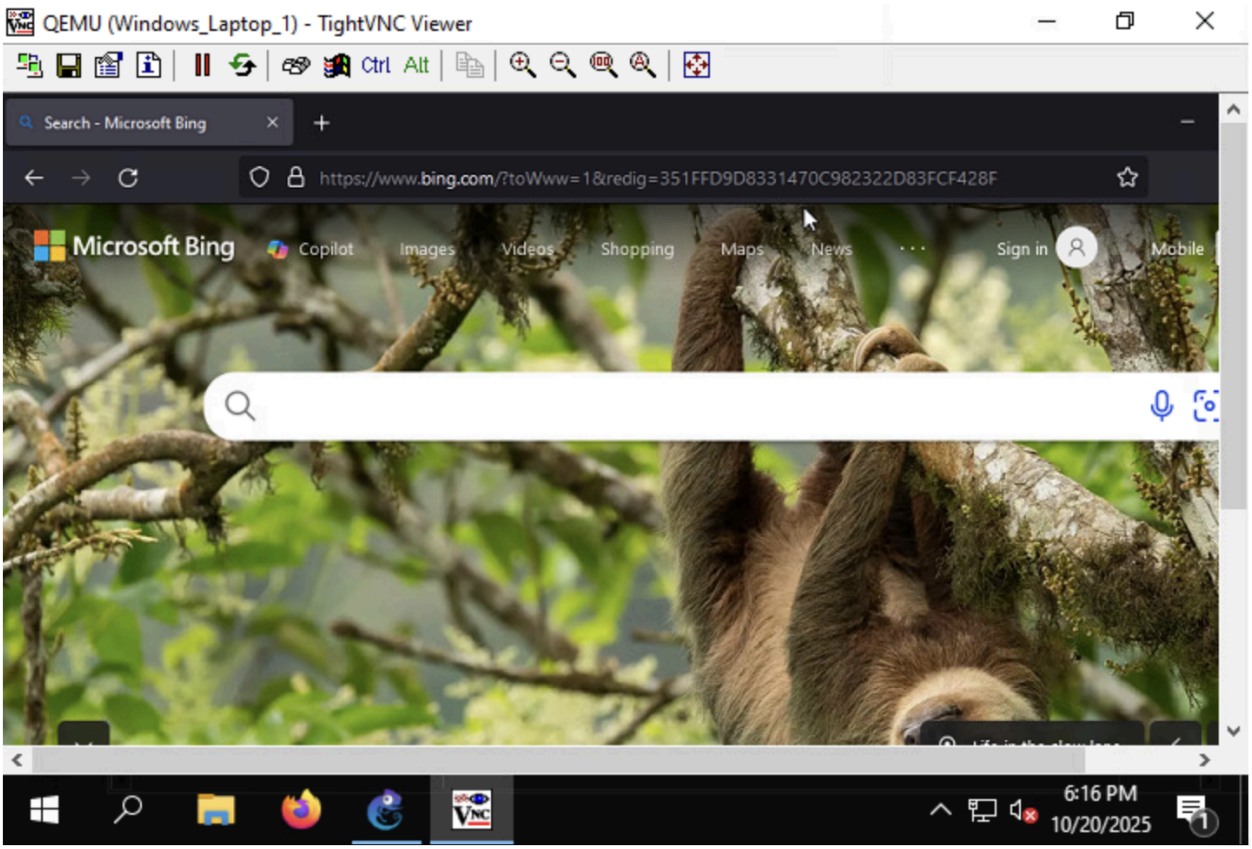

Figure 4.4: Image showing the successful network connection to the internet

Root cause analysis

a. List the tool(s) used to identify the problem.

- ipconfig
- ping
- Control Panel

b. Explain why you chose the tool(s) to troubleshoot the problem.

- ipconfig /all (Used to view the network properties of the device, such as IP address, subnet mask, gateway IP, DNS, DHCP, MAC address, etc.)
- ping (To test the reachability between the source and the destination, and information such as time to live, round-trip time, percent of packets received and lost, etc.)
- Control Panel (A collection of tools used to manage and configure various aspects of the system on the device, easily accessible and configurable.) In this case, the network and sharing center is used to troubleshoot the network connection status of the device.

c. Explain the steps of the troubleshooting process that were used to identify the problem and the resolution to solve the problem.

Problem identification

The Windows laptop user complained of being unable to access the internet or network resources. This is verified by the failure to access a website from the browser and the failure to ping the external network.

Possible causes include physical connection issues (such as cable or port issues), DHCP or IP address misconfiguration, and network adapter issues.

Problem resolution

The Ethernet cable was ensured to be connected to the interface, and the network adapter status was verified to be enabled and connected.

The ipconfig /all command was run on the CLI to check the network configurations on the laptop, such as IP address, subnet mask, gateway IP, DHCP, and DNS. It was discovered that the gateway IP address was missing, which was the reason the device was unable to access the internet outside the network. Additionally, it was noted that the device's IPv4 address was 169.254.144.242, indicating an APIPA (Automatic Private IP Addressing) address. The absence of the gateway IP address on the device resulted in an inability to reach the DHCP server and retrieve a dynamic IP address. (Figure 4.1)

From the control panel, the device was manually configured and assigned an IP address of 10.10.40.4/24 with the gateway IP of 10.10.40.254 (of Router 1), and the DNS server was set to Google’s server for convenience. (Figure 4.2)

It was pinged to a website to verify that the device had internet access and could properly connect to the internet and access the website, as shown in Figures 4.3 and 4.4.

Help Desk Ticket 5

A coworker states that she worked on a ticket to allow access through the firewall to DMZ_Server_1. There is now no access to the server from any device outside its network.

Screenshots

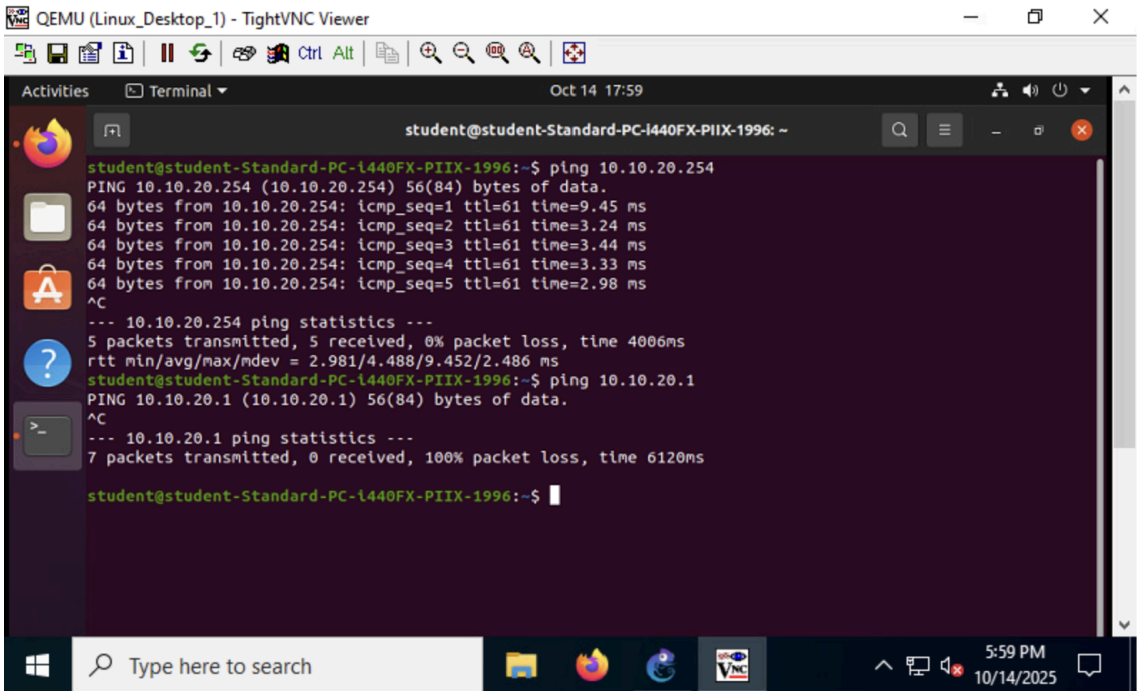

Figure 5.1: image showing the ping result of one of the DMZ servers and its gateway

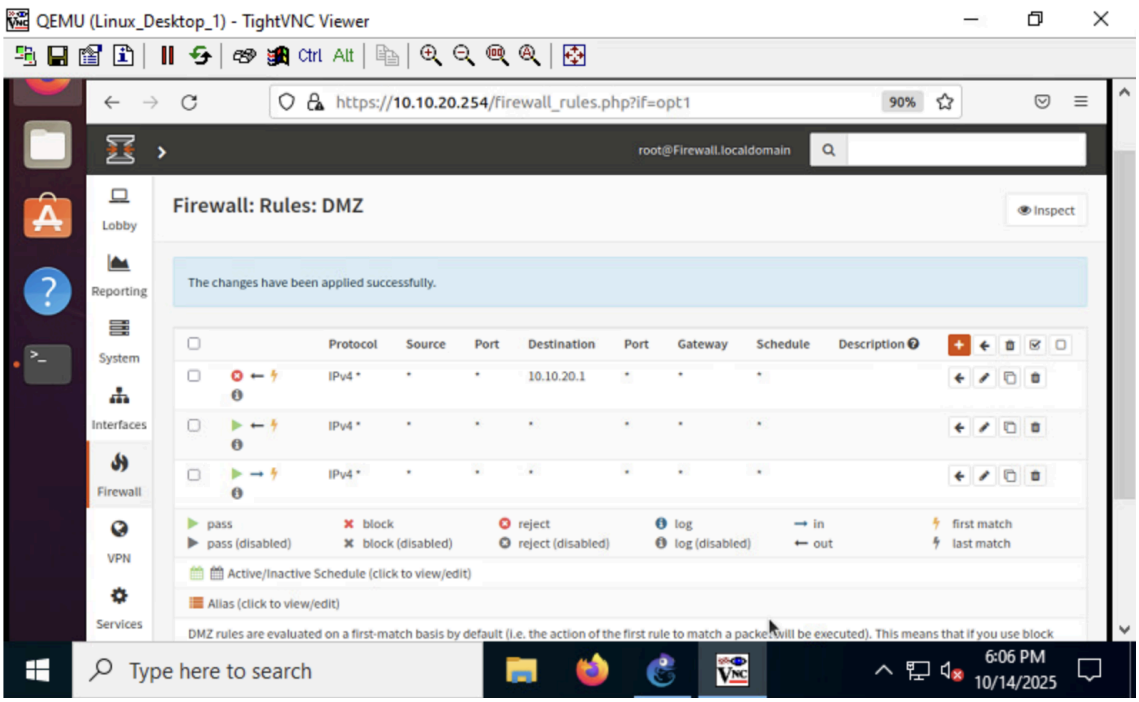

Figure 5.2: image showing the current firewall rules configuration for the DMZNet subnet

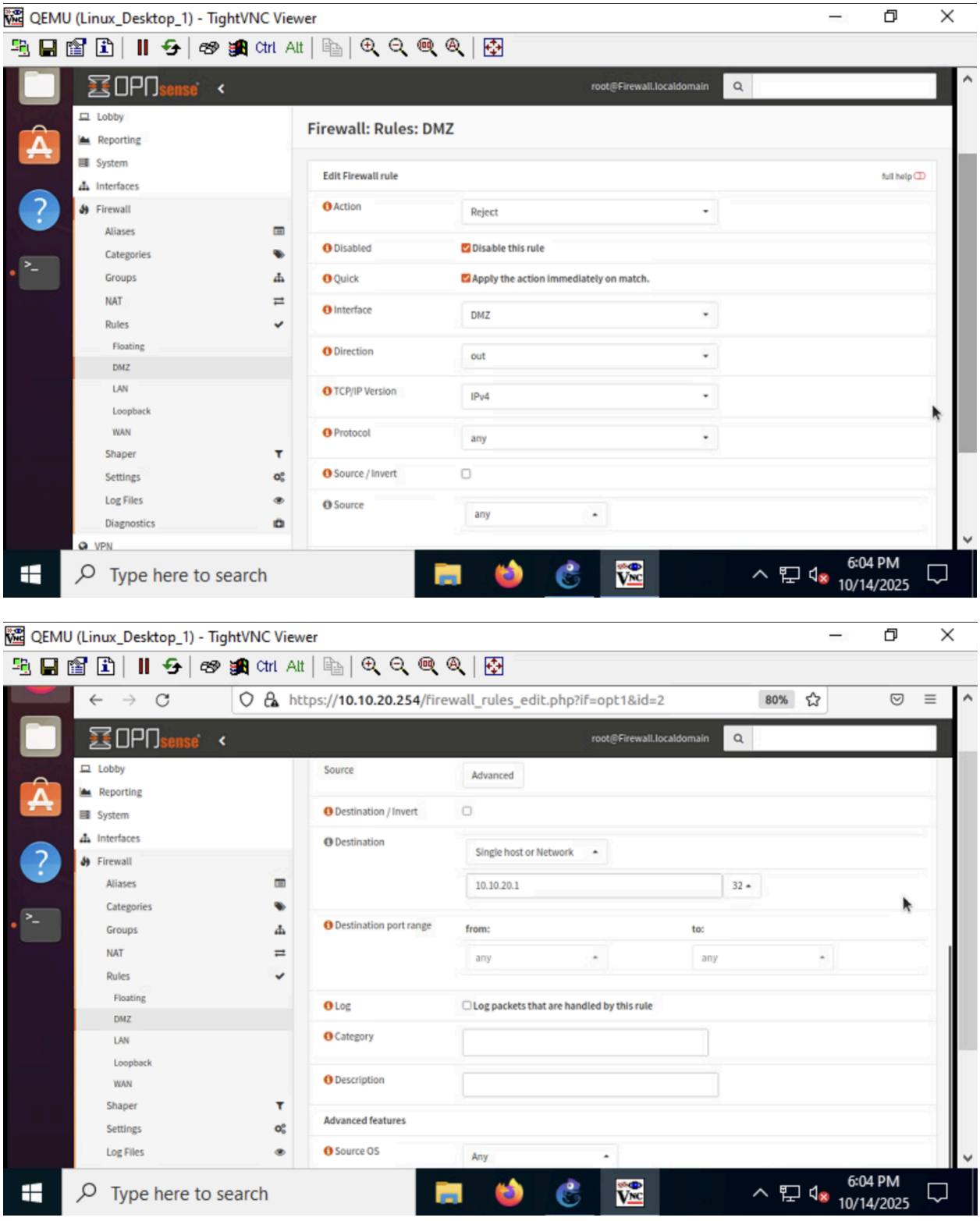

Figure 5.3: images showing the configuration of the first rule

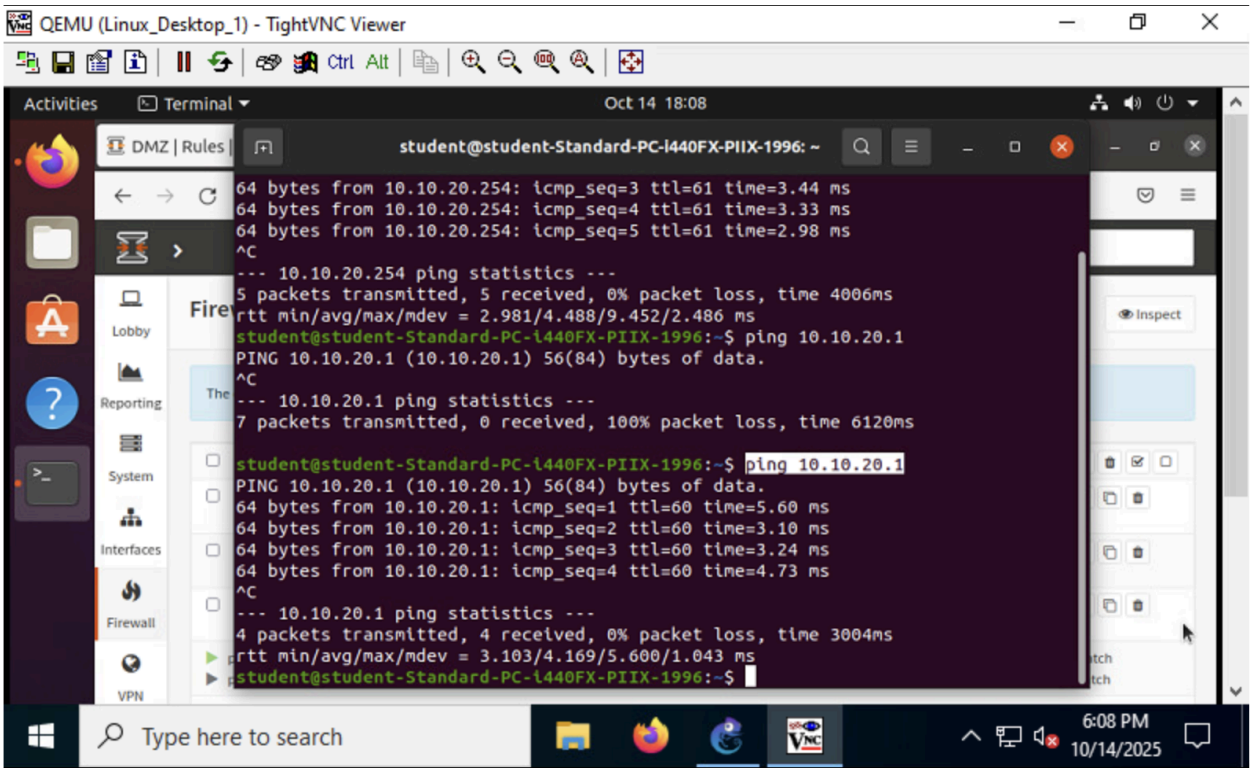

Figure 5.4: image showing the successful ping result to the DMZ server

Root cause analysis

a. List the tool(s) used to identify the problem.

- ping
- OPNsense firewall

b. Explain why you chose the tool(s) to troubleshoot the problem.

- ping (A network troubleshooting tool used to test the reachability of the data from the source to the destination, recording time to live, round-trip time, and packet loss. It is used to test if the packets generated from the PC could reach the destination, the firewall and DMZ_Server_1.) (Jimenez, 2022)
- OPNsense firewall (GUI tool used to configure the firewall rules, simpler than accessing the firewall from CLI)

c. Explain the steps of the troubleshooting process that were used to identify the problem and the resolution to solve the problem.

Problem identification:

It was tested first by pinging the gateway of the subnet, the firewall (10.10.20.254), and it was successful. However, when pinging one of the servers, the packets were 100% lost, indicating an issue with connectivity beyond the firewall. (Figure 5.1)

The probable causes are;

- firewall misconfiguration leading to the dropping of the packets

- physical connection breakage between the router and the servers (usually only the server with the breakage is affected)

Testing the theory and problem resolution:

The firewall was accessed from the browser of one of the workstations through its GUI interface using its IP address, 10.10.20.254. The firewall ACL rules are shown in Figure 5.2, and each rule was analyzed in detail.

It was found that the first rule caused the firewall to drop any IPv4 packets intended for 10.10.20.1 (the IP address of the DMZ_Server_1), which was the cause of the inability to reach the DMZ Server 1. The rule was disabled so that packets destined for the Server would not be dropped.

After disabling the first configuration, it was tested by pinging one of the servers, and this time, the ping was successful.

Help Desk Ticket 6

Your local cybersecurity team is requesting information on the open ports on DMZ_Server_2 to identify services that may be running outside of the permitted services. Permitted services are 22/ssh, 135/msrpc, 3389/ms-wbt-server, and 8080/http-proxy.

Screenshots

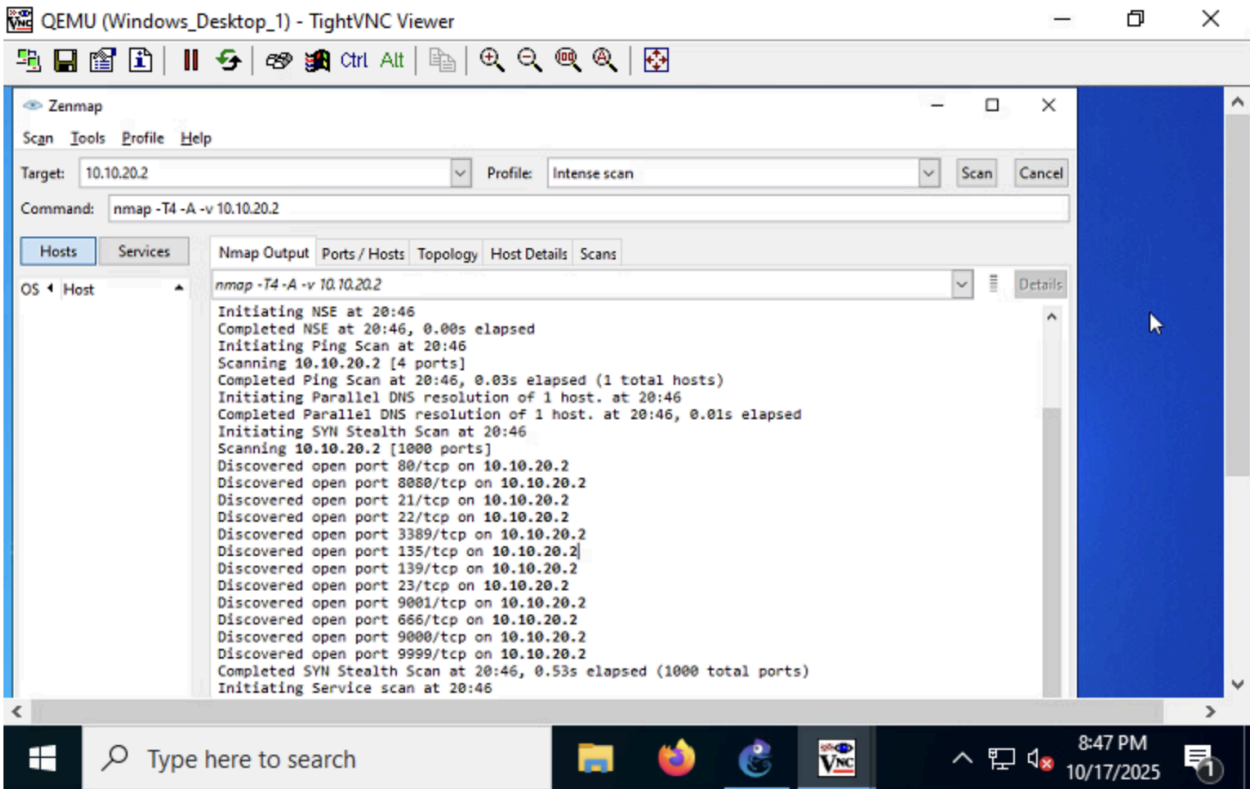

Figure 6.1: Image showing the list of opened ports on DMZ_Server_2 (10.10.20.2)

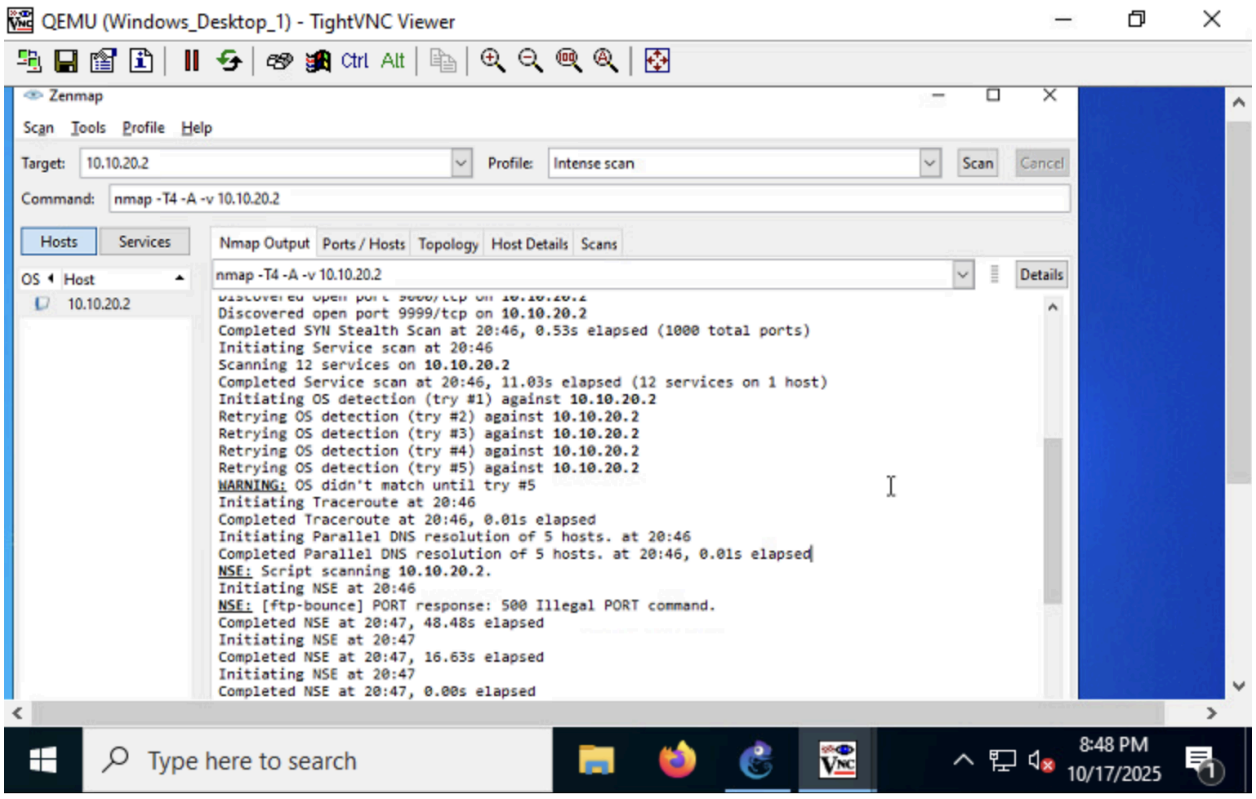

Figure 6.2: Image showing the rest of the scanning against DMZ_Server_2

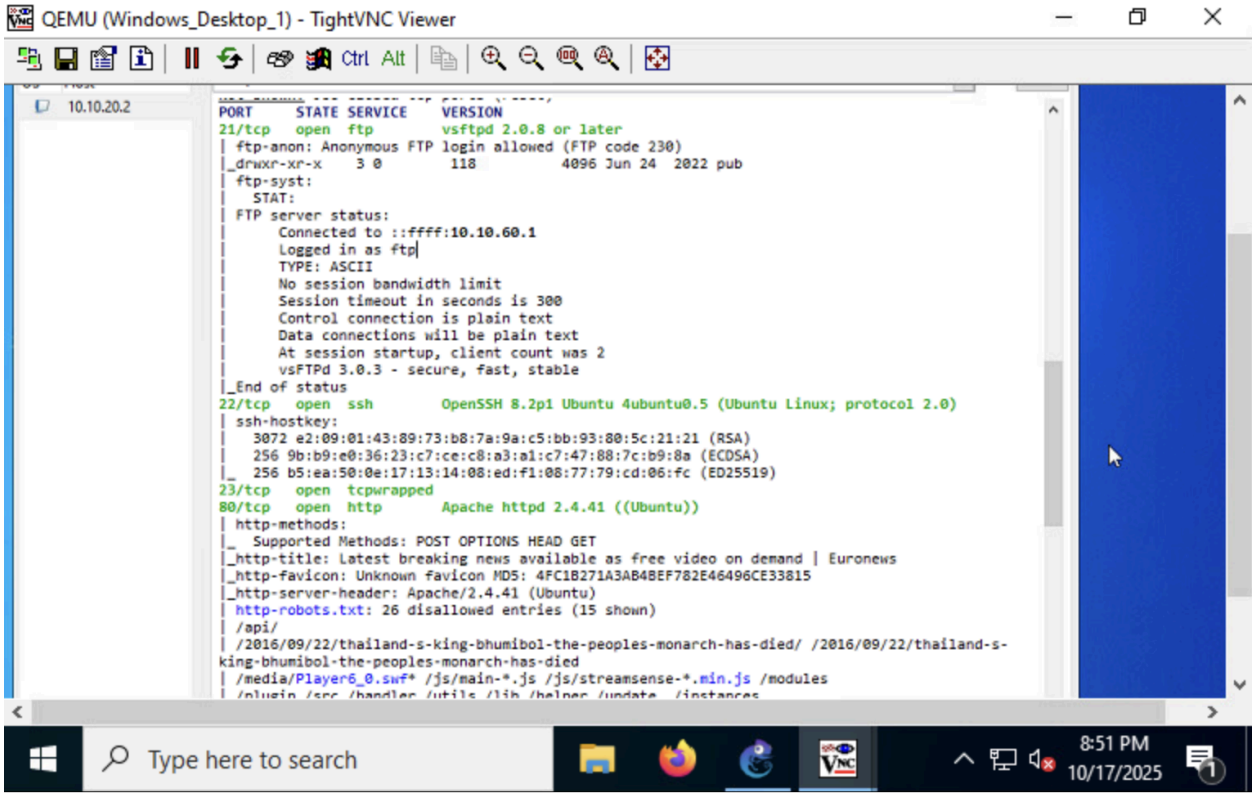

Figure 6.3: Image showing the detailed result of the scan for open ports against DMZ_Server_2

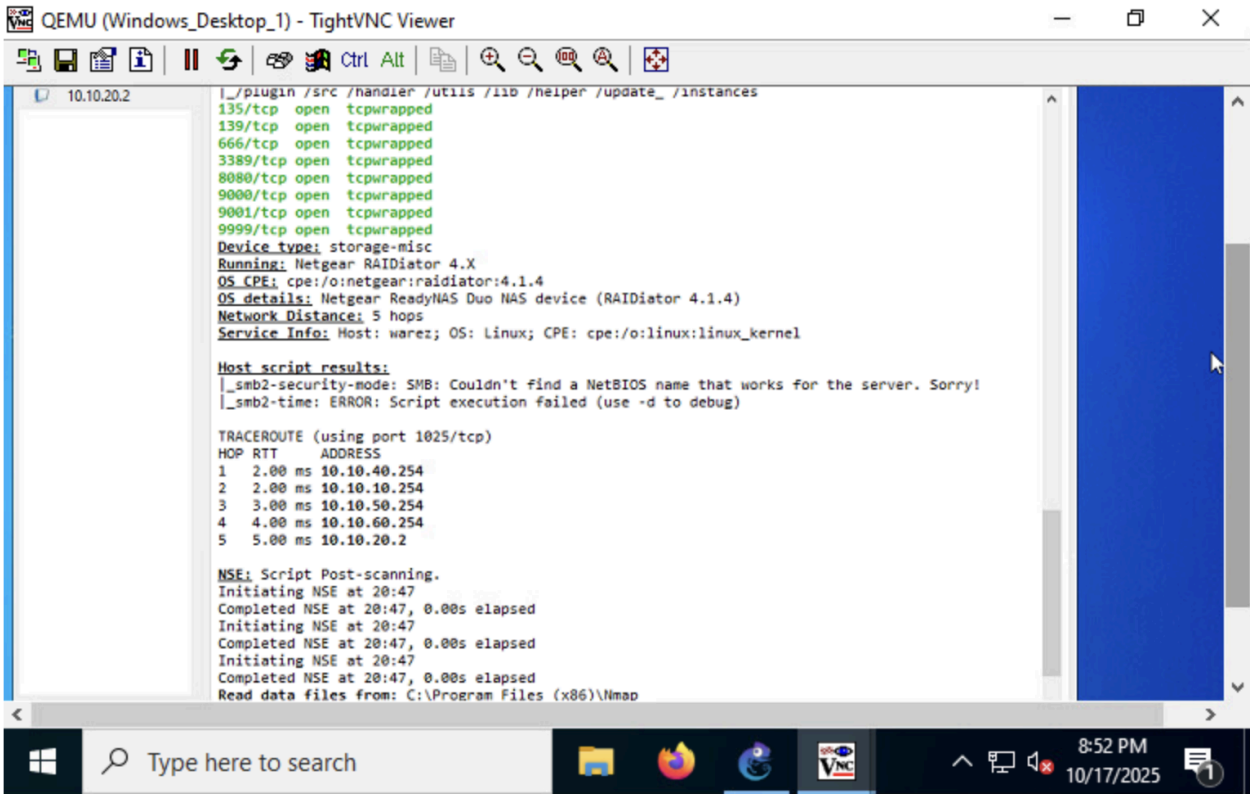

Figure 6.4: Image showing the port scan result on DMZ_Server_2

Root cause analysis

a. List the tool(s) used to identify the problem.

- Zenmap (Nmap.org, n.d.)

b. Explain why you chose the tool(s) to troubleshoot the problem.

- Zenmap is a cross-platform, open-source GUI version of Nmap, a network scanning tool that scans open ports against a host. It is useful for security auditing and network exploration. (Lyon, 2008) Zenmap provides the same function, but in the form of a graphical interface and user user-friendly.

c. Explain the steps of the troubleshooting process that were used to identify the problem and a recommendation to solve the problem. Include a complete list of unauthorized open ports.

Troubleshooting

The DMZ_Server_2 (10.10.20.2) is scanned with the Zenmap utility using one of the end devices, Windows_Desktop_1. An intense scan performs a comprehensive exploration and analysis of a targeted host by scanning all TCP ports, performing OS and version detection, reconnaissance of open ports and their services, as well as gathering network device details. (Figure 6.1)

It is noted that the scan identified 500 illegal ‘port’ commands (Figure 6.2), which require further attention and network analysis, and monitoring.

The list of unpermitted open ports is as follows;

- port 80 (HTTP, insecure version of HTTPS, ‘GET’ used against Apache server, Figure 6.3)
- port 21 (FTP, File Transfer Protocol - Anonymous FTP login allowed, Figure 6.3)
- port 23 (Telnet, insecure)
- port 139 (NetBios)
- port 666 (Doom multiplayer gaming protocol used in the first online person shooter game, but it became more widely known for its use for malware communication like Trojans and backdoor implantation, data exfiltration due to its symbolic number, and remote-controlling of wireless devices) (PentestPad, n.d.)
- port 3389 (RDP, Remote Desktop Protocol)
- port 9000 (used for different purposes in developing and handling internal services of the website, for code analysis, as well as to test the environments. However, it is vulnerable as it could expose the code to the threat actor, authentication bypass, and remote execution of the code.) (PentestPad, n.d.)
- Port 9001 (primarily used as the default unencrypted relay port for Tor, the onion router anonymity protocol) poses a security risk due to its lack of encryption and could be used conversely for traffic analysis. It is also known to be used for Windows HTTPAPI/2.0, PHP-CGI, Milestone XProtect, and Dell NMC.) (WhatPortIs, n.d.)
- port 9999 (commonly used by IoT devices, in debug consoles, or custom development tools for command/control or testing purposes. It serves vulnerability as it could expose the debugging interfaces, command injection to IoT devices, and amplify DDoS attacks.) (PentestPad, n.d.)

A detailed packet analysis should be performed, and all unused ports should be closed. Only the secure, encrypted version should be used.

References

Jimenez, J. (2022, October 4). *Understand the Ping and Traceroute Commands*. Cisco. Retrieved October 14, 2025, from https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12778-ping-traceroute.html

Lyon, G. (2008). *Nmap Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure.com, LLC.

Nmap.org. (n.d.). *Zenmap - Official cross-platform Nmap Security Scanner GUI*. Nmap. https://nmap.org/zenmap/

PentestPad. (n.d.). *Port 666 – DOOM (Doom Game Protocol)*. https://www.pentestpad.com/port-exploit/port-666-doom-doom-game-protocol

PentestPad. (n.d.). *Port 9000 – Dev Tools (Development Tools Protocol)*. https://www.pentestpad.com/port-exploit/port-9000-dev-tools-development-tools-protocol

PentestPad. (n.d.). *Port 9999 – Debug Servers / IoT Interfaces / Custom Apps*. https://www.pentestpad.com/port-exploit/port-9999-debug-servers-iot-interfaces-custom-apps

Poston, H. (2019, December 5). *FTP Bounce Attack*. Network traffic analysis for IR: FTP protocol with Wireshark. https://www.infosecinstitute.com/resources/incident-response-resources/network-traffic-analysis-for-ir-ftp-protocol-with-wireshark/

Stewart, J. M., & Kinsey, D. (2020). *Network Security, Firewalls, and VPNs*. Jones & Bartlett Learning, LLC.

VyOS Networks. (n.d.). *OSPFv2 (IPv4)*. OSPF.

https://docs.vyos.io/en/1.4/configuration/protocols/ospf.html

VyOS Networks. (n.d.). *Static Routes*. Static.

https://docs.vyos.io/en/1.4/configuration/protocols/static.html

WhatPortIs. (n.d.). *Port 9001*. https://www.whatportis.com/ports/9001_tor-network-default

Wireshark.org. (n.d.). *1.1. What is Wireshark?* Chapter 1. Introduction.

https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html