D412 TASK 1 SUBMISSION

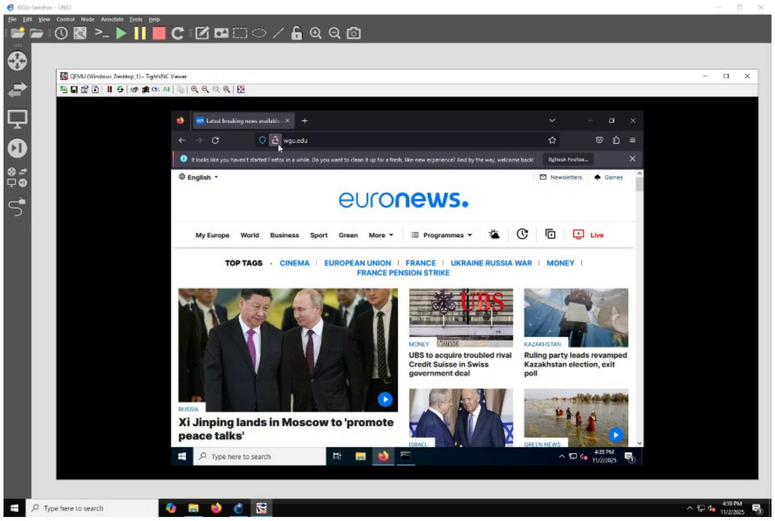
Name: Ismael G. Ibarra
Student ID: 011559560

Helpdesk Ticket 1:

Scenario: There are multiple reports of employees located in the USER_Net subnet who cannot get to www.wgu.edu, and 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 acts as the DNS Server for the organization.

Objective (Identify and Resolve): Troubleshoot to identify the problem and take necessary steps to fix the problem.

A. Using the information in the scenario for helpdesk ticket 1, do the following:
1. Provide screenshot(s) of the identified problem <u>and</u> the resolution. Screenshot(s) must be clear, with a full view of the screen, and include the date and time.



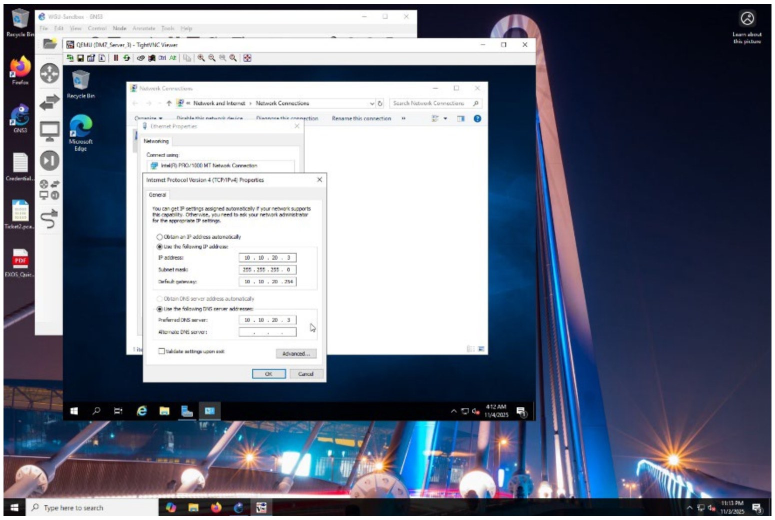
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Xi Jinping lands in Moscow to 'promote peace talks'

UBS to acquire troubled rival Credit Suisse in Swiss government deal

Ruling party leads revamped Kazakhstan election, exit poll

Identified Problem Screenshot – On Windows_Desktop_1, I pulled up the Mozilla web browser and visited www.wgu.edu. I was redirected to euronews website.
Time Stamp 4:39 pm 11/2/2025



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

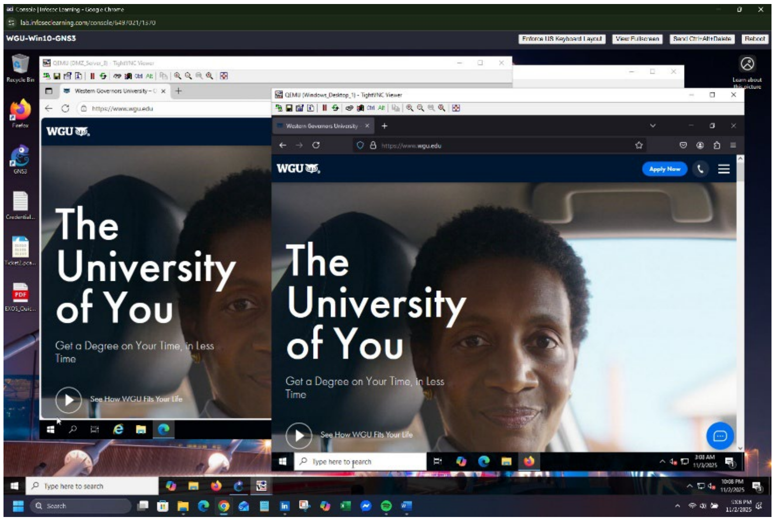
○ Obtain an IP address automatically
● Use the following IP address:
IP address: 10 . 10 . 20 . 3
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 10 . 20 . 254

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 10 . 10 . 20 . 3
Alternate DNS server: . . .

□ Validate settings upon exit

Network Connections
Network and Internet > Network Connections
Ethernet Properties
Networking
Connect using:
Intel(R) PRO/1000 MT Network Connection
Advanced...
OK
Cancel

Changed the preferred DNS server address to the DNS server IP address.
Time Stamp: 11:13 pm 11/3/2025



WGU-Win10-GNS3
QEMU (DMZ_Server_3) - TightVNC Viewer
QEMU (Windows_Desktop_1) - TightVNC Viewer
https://www.wgu.edu
WGU
The University of You
Get a Degree on Your Time, in Less Time
See How WGU Fits Your Life
Apply Now

DNS server issue resolved. I was able to navigate to www.wgu.edu on both DMZ_server_3 and Windows_Desktop_1 devices.
Time Stamp 10:08 pm 11/2/2025

2. **Create a root cause analysis write-up by doing the following:**
   a. **List the tool(s) used to identify the problem.**
      1. Command Prompt (ping, ipconfig /flushdns, ipconfig /all
      2. Windows Settings (Updates and Defender)
      3. Windows Server Manager
      4. Windows Control Panel

   b. **Explain why the tool(s) was (were) chosen to troubleshoot the problem.**
      b1. Command Prompt -

      ping – From the Windows_Desktop_1 workstation, I used the ping command to verify that DNS resolution is functioning. This test verifies whether a domain name resolves correctly to an IP address and confirms basic connectivity to the destination, helping to identify potential DNS or network issues.

      ipconfig /flushdns – From the Windows_Desktop_1 workstation, I used the ipconfig /flushdns command to clear the local DNS cache. Stale or incorrect DNS entries can prevent proper domain name resolution, and flushing the cache ensures the system requests fresh DNS information from the server.

ipconfig /all – From the Windows_Desktop_1 workstation, I used the ipconfig/all command to verify IP addresses, DNS servers, MAC addresses, and DHCP status. This command provides a detailed view of the system's network configuration, helping identify misconfigurations or connectivity issues that could affect DNS resolution.

b2. Windows Settings – On both Windows_Desktop_1 and DMZ_Server_3, I used Windows Update to install the latest security and quality patches, ensuring the systems were protected against known vulnerabilities that could affect DNS or network performance. After updating, I used Windows Defender to perform complete system scans on both machines to detect and remove any malicious software that might have been interfering with network connectivity or DNS resolution. These tools were chosen to eliminate potential security threats and ensure the systems were operating with the most up-to-date protections.

b3. Windows Server Manager – On the DMZ_Server_3 device, I used Windows Server Manager to review installed updates and examine update logs, as it provides centralized visibility into system changes, allowing me to identify whether recent updates have introduced errors or suspicious activity that could be affecting DNS or network functionality.

b4. Windows Control Panel – On the DMZ_Server_3 device, I used the Control Panel to verify that the Ethernet properties were correctly configured, as it allows direct access to adapter settings such as IP configuration and DNS assignment, facilitating the diagnosis and resolution of network connectivity and DNS resolution issues.

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

I began by using the web browser on Windows_Desktop_1 to access www.wgu.edu, but instead of reaching the intended site, I was unexpectedly redirected to an Euronews website. This behavior strongly suggested a DNS resolution issue or possible misconfiguration.

To confirm, I used the ping command to test domain name resolution and verify basic connectivity. This helped determine whether the system could translate domain names into IP addresses. I then ran ipconfig /flushdns to clear any stale or incorrect DNS entries that might have been causing resolution errors. Following that, I used ipconfig /all to inspect the system's IP configuration, DNS server assignments, MAC address, and DHCP status—ensuring that the workstation was configured correctly for network communication.

To rule out security-related causes, I ran Windows Update on both Windows_Desktop_1 and DMZ_Server_3 to apply the latest security fixes, followed by a full system scan using Windows Defender to eliminate any malicious software that could interfere with DNS or network services.

On the DMZ_Server_3 device, I used Windows Server Manager to review recent updates and examine update logs for errors or suspicious activity. I also accessed and configured the DNS Manager, where I discovered that the zone settings had not been appropriately configured.

Finally, I used the Control Panel on DMZ_Server_3 to verify that the Ethernet properties were correctly set, confirming that IP and DNS settings were aligned with the intended network configuration. The preferred DNS server was incorrectly assigned. I believe this misconfiguration was the root cause of the DNS resolution failure and the unexpected redirection. After correcting the zone settings and updating the preferred DNS server, name resolution began functioning as expected.

To verify the resolution, I used the web browser on both Windows_Desktop_1 and DMZ_Server_3 to revisit www.wgu.edu and confirmed that the site loaded correctly without any redirection, indicating that DNS functionality had been restored.

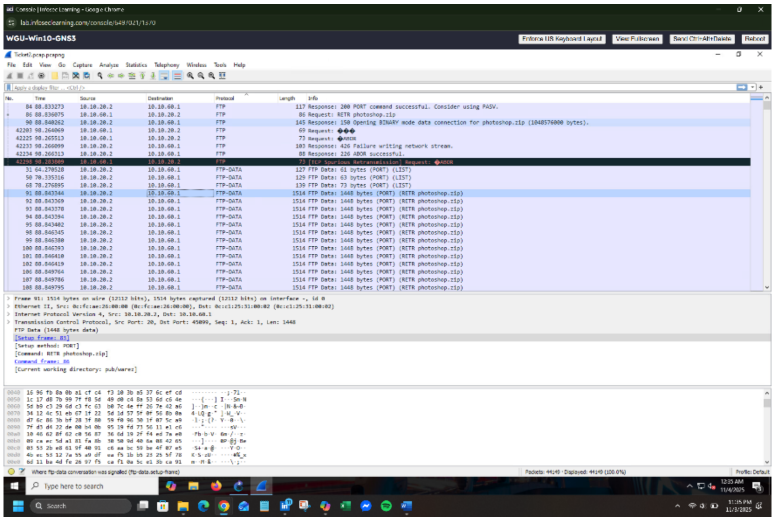
Helpdesk Ticket 2:

Scenario: A complaint has been received 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've asked you to identify where the FTP site is being hosted.

Objective (Identify and Recommend Resolution): Analyze the PCAP file on the Host desktop (minimize GNS3 and look on the desktop for the file) and report back the IP address of the server and what files were observed being accessed.

B. Using the information in the scenario for helpdesk ticket 2, do the following:

1. Provide a screenshot of the identified problem. The screenshot must be clear, with a full view of the screen, and include the date and time.


Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/549/021/1570
WGU-Win10-GNS3
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Ticket2.pcap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
Search
12:35 AM
11/4/2025
11:35 PM
11/3/2025

```
No.    Time       Source       Destination  Protocol  Length Info
   84 88.833273   10.10.20.2   10.10.60.1   FTP         117 Response: 200 PORT command successful. Consider using PASV.
   86 88.836075   10.10.60.1   10.10.20.2   FTP          86 Request: RETR photoshop.zip
   90 88.840262   10.10.20.2   10.10.60.1   FTP         145 Response: 150 Opening BINARY mode data connection for photoshop.zip (1048576000 bytes).
42203 98.264069   10.10.60.1   10.10.20.2   FTP          69 Request: ���
42225 98.265513   10.10.60.1   10.10.20.2   FTP          73 Request: �ABOR
42233 98.266099   10.10.20.2   10.10.60.1   FTP         103 Response: 426 Failure writing network stream.
42234 98.266313   10.10.20.2   10.10.60.1   FTP          88 Response: 226 ABOR successful.
42298 98.283809   10.10.60.1   10.10.20.2   FTP          73 [TCP Spurious Retransmission] Request: �ABOR
   31 64.270528   10.10.20.2   10.10.60.1   FTP-DATA    127 FTP Data: 61 bytes (PORT) (LIST)
   50 70.335316   10.10.20.2   10.10.60.1   FTP-DATA    129 FTP Data: 63 bytes (PORT) (LIST)
   68 78.276895   10.10.20.2   10.10.60.1   FTP-DATA    139 FTP Data: 73 bytes (PORT) (LIST)
   91 88.843344   10.10.20.2   10.10.60.1   FTP-DATA   1514 FTP Data: 1448 bytes (PORT) (RETR photoshop.zip)
   92 88.843369   10.10.20.2   10.10.60.1   FTP-DATA   1514 FTP Data: 1448 bytes (PORT) (RETR photoshop.zip)
   93 88.843378   10.10.20.2   10.10.60.1   FTP-DATA   1514 FTP Data: 1448 bytes (PORT) (RETR photoshop.zip)
   94 88.843394   10.10.20.2   10.10.60.1   FTP-DATA   1514 FTP Data: 1448 bytes (PORT) (RETR photoshop.zip)
   95 88.843402   10.10.20.2   10.10.60.1   FTP-DATA   1514 FTP Data: 1448 bytes (PORT) (RETR photoshop.zip)
   98 88.846345   10.10.20.2   10.10.60.1   FTP-DATA   1514 FTP Data: 1448 bytes (PORT) (RETR photoshop.zip)
   99 88.846380   10.10.20.2   10.10.60.1   FTP-DATA   1514 FTP Data: 1448 bytes (PORT) (RETR photoshop.zip)
  100 88.846393   10.10.20.2   10.10.60.1   FTP-DATA   1514 FTP Data: 1448 bytes (PORT) (RETR photoshop.zip)
  101 88.846410   10.10.20.2   10.10.60.1   FTP-DATA   1514 FTP Data: 1448 bytes (PORT) (RETR photoshop.zip)
  102 88.846419   10.10.20.2   10.10.60.1   FTP-DATA   1514 FTP Data: 1448 bytes (PORT) (RETR photoshop.zip)
  106 88.849764   10.10.20.2   10.10.60.1   FTP-DATA   1514 FTP Data: 1448 bytes (PORT) (RETR photoshop.zip)
  107 88.849786   10.10.20.2   10.10.60.1   FTP-DATA   1514 FTP Data: 1448 bytes (PORT) (RETR photoshop.zip)
  108 88.849795   10.10.20.2   10.10.60.1   FTP-DATA   1514 FTP Data: 1448 bytes (PORT) (RETR photoshop.zip)
```

```
> Frame 91: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface -, id 0
> Ethernet II, Src: 0c:fc:ae:26:00:00 (0c:fc:ae:26:00:00), Dst: 0c:c1:25:31:00:02 (0c:c1:25:31:00:02)
> Internet Protocol Version 4, Src: 10.10.20.2, Dst: 10.10.60.1
> Transmission Control Protocol, Src Port: 20, Dst Port: 45099, Seq: 1, Ack: 1, Len: 1448
  FTP Data (1448 bytes data)
  [Setup frame: 85]
  [Setup method: PORT]
  [Command: RETR photoshop.zip]
  Command frame: 86
  [Current working directory: pub/warez]
```

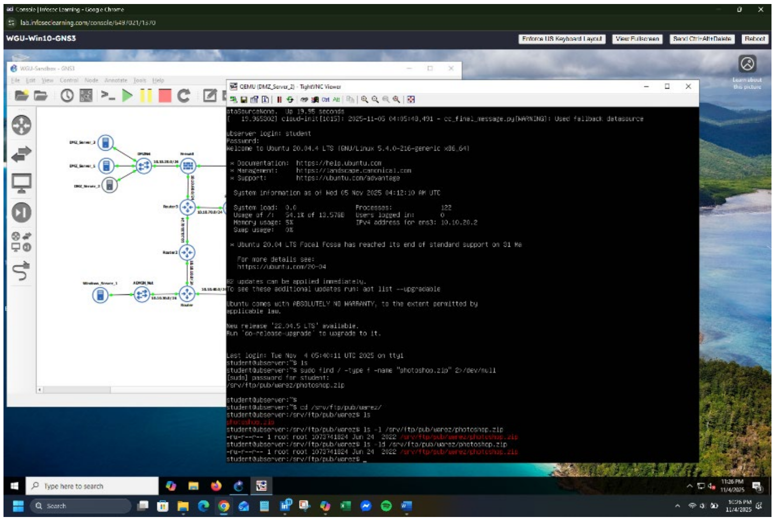
```
0040  16 96 fb 8a 0b a1 cf c4  f3 10 3b a5 37 6c ef cd   ········ ··;·7l··
0050  1c 17 d8 7b 99 7f f8 5d  49 d0 c4 8a 53 6d c6 4e   ···{···] I···Sm·N
0060  5d b9 c3 29 6d c3 fc 63  b0 7c 4e ff 26 7e 42 a6   ]··)m··c ·|N·&~B·
0070  34 12 4c 51 eb 67 1f 22  5d 1d 57 5f 0f 56 8b 0a   4·LQ·g·" ]·W_·V··
0080  d7 6c 86 3b bf 28 3f 80  59 f8 96 30 1f 07 5c a9   ·l·;·(?· Y··0··\·
0090  7f d3 d4 22 de 00 b4 0b  95 19 fd 73 56 11 e1 c6   ···"···· ···sV···
00a0  10 46 62 8f 62 c0 56 87  36 6d 19 2f f4 ed 7a e0   ·Fb·b·V· 6m·/··z·
00b0  09 ca ec 5d a1 81 fa 8b  30 50 9d 40 6a 08 42 65   ···]···· 0P·@j·Be
00c0  03 55 2b e8 61 9f 40 91  c6 aa bc 59 be 4f 07 e5   ·U+·a·@· ···Y·O··
00d0  4b ec 53 12 7a 55 a9 df  ea f5 1b b5 23 25 5f 78   K·S·zU·· ····#%_x
00e0  6d 11 ba 4d fe 26 97 f5  ca f1 0a 5c e1 3b ca 91   m··M·&·· ···\·;··
```

Where ftp-data conversation was signalled (ftp-data.setup-frame)

Packets: 44149 · Displayed: 44149 (100.0%)

Profile: Default

The screenshot displays a PCAP file opened in Wireshark, filtered to show FTP protocol traffic using the ftp display filter. The packet view highlights a RTR photoshop.zip command, indicating an attempt to download a suspicious file. Timestamp: 12:35 AM, 11/4/2025


WGU-Win10-GNS3
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
QEMU (DMZ_Server_2) - TightVNC Viewer

```
ataSourceNone.  Up 19.95 seconds
[   19.965302] cloud-init[1015]: 2025-11-05 04:05:48,491 - cc_final_message.py[WARNING]: Used fallback datasource

ubserver login: student
Password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-216-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed 05 Nov 2025 04:12:10 AM UTC

  System load:  0.0               Processes:             122
  Usage of /:   54.1% of 13.57GB   Users logged in:       0
  Memory usage: 5%                IPv4 address for ens3: 10.10.20.2
  Swap usage:   0%

 * Ubuntu 20.04 LTS Focal Fossa has reached its end of standard support on 31 Ma

   For more details see:
   https://ubuntu.com/20-04

82 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Tue Nov  4 05:40:11 UTC 2025 on tty1
student@ubserver:~$ ls
student@ubserver:~$ sudo find / -type f -name "photoshop.zip" 2>/dev/null
[sudo] password for student:
/srv/ftp/pub/warez/photoshop.zip

student@ubserver:~$
student@ubserver:~$ cd /srv/ftp/pub/warez/
student@ubserver:/srv/ftp/pub/warez$ ls
photoshop.zip
student@ubserver:/srv/ftp/pub/warez$ ls -l /srv/ftp/pub/warez/photoshop.zip
-rw-r--r-- 1 root root 1073741824 Jun 24  2022 /srv/ftp/pub/warez/photoshop.zip
student@ubserver:/srv/ftp/pub/warez$ ls -ld /srv/ftp/pub/warez/photoshop.zip
-rw-r--r-- 1 root root 1073741824 Jun 24  2022 /srv/ftp/pub/warez/photoshop.zip
student@ubserver:/srv/ftp/pub/warez$ _
```

The traffic analysis revealed that the FTP server is hosted on DMZ_Server_2, which corresponds to the IP address 10.10.20.2 identified in the capture. After launching DMZ_Server_2 for investigation, I located the file photoshop.zip in the directory /srv/ftp/pub/warez/. Timestamp: 11:26 PM, 11/4/2025

2. **Create a root cause analysis write-up by doing the following:**
   a. **List the tool(s) used to identify the problem.**
   1. Wireshark
   2. Linux Terminal Command Line Interface (ls, find, cd)

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

I used Wireshark to analyze the provided .pcap file, applying the ftp display filter to isolate FTP traffic. This allowed me to identify the IP address of the suspected FTP server and observe file transfer activity, including the retrieval of the photoshop.zip file.

Once I confirmed the server's IP address, I accessed the corresponding Ubuntu system and used the Linux command-line interface to locate the file and its hosting directory. Specifically, I used tools like 'find', 'ls', and 'cd' to trace the file's path and inspect its contents. This approach provided both network-level and system-level visibility, enabling me to verify the presence of unauthorized software and begin containment procedures.

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.

I began by analyzing the provided .pcap file using Wireshark. I applied the ftp display filter to isolate FTP control traffic, which allowed me to observe login attempts and file transfer commands. One particular command, RETR photoshop.zip, stood out as it indicated an attempt to download a potentially unauthorized file.

By examining the packet details, I identified the destination IP address as 10.10.20.2, which consistently appeared as the FTP server throughout the capture. I correlated this IP with an internal host named DMZ_Server_2, which I then accessed for further investigation.

Using the Linux command-line interface, I searched the server's filesystem and located the file photoshop.zip in the directory /srv/ftp/pub/warez/. This directory contained only that file, suggesting it was intentionally hosted for distribution. I also reviewed the FTP server configuration and confirmed that the service was publicly accessible, posing a security risk.

To resolve the issue and prevent further unauthorized access, I recommend quarantining the FTP server immediately. This includes stopping the FTP service, restricting access to the /srv/ftp directory, and preserving the files and logs for forensic analysis. Only authorized security personnel should have access during the investigation. Additionally, the FTP configuration should be audited and hardened to prevent future misuse.

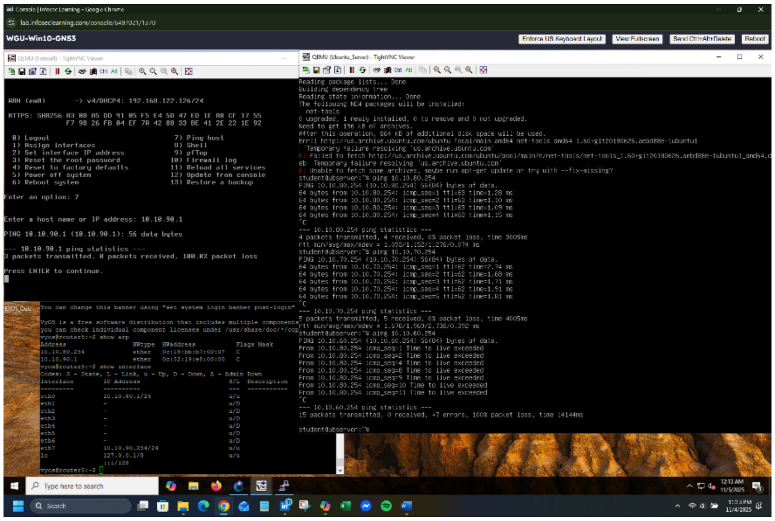
Helpdesk Ticket 3:

Scenario: The host "Ubuntu_Server" can’t get to any of the assigned networks or the internet, which is preventing the server from pulling the required security patches.

Objective (Identify and Recommend Specific Resolution): Identify the issue and report back the possible problem that the server/infrastructure team needs to address to allow network traffic to get to and from this device.

C. Using the information in the scenario for helpdesk ticket 3, do the following:

1. Provide a screenshot or screenshots of the identified problem. The screenshot must be clear, with a full view of the screen, and include the date and time.


Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/649/021/1370
WGU-Win10-GNS3
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
QEMU (Firewall) - TightVNC Viewer
QEMU (Ubuntu_Server) - TightVNC Viewer
Type here to search
Search
12:13 AM
11/5/2025
11:13 PM
11/4/2025

```
 WAN (em0)       -> v4/DHCP4: 192.168.122.126/24

 HTTPS: SHA256 A3 88 A5 DD 91 85 F5 E4 5D 47 ED 1E A8 CF 17 55
               F7 98 26 FB 04 EF 7A 42 88 33 BE 41 2E 22 1E 92

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option: 7


Enter a host name or IP address: 10.10.90.1

PING 10.10.90.1 (10.10.90.1): 56 data bytes

--- 10.10.90.1 ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss

Press ENTER to continue.
```

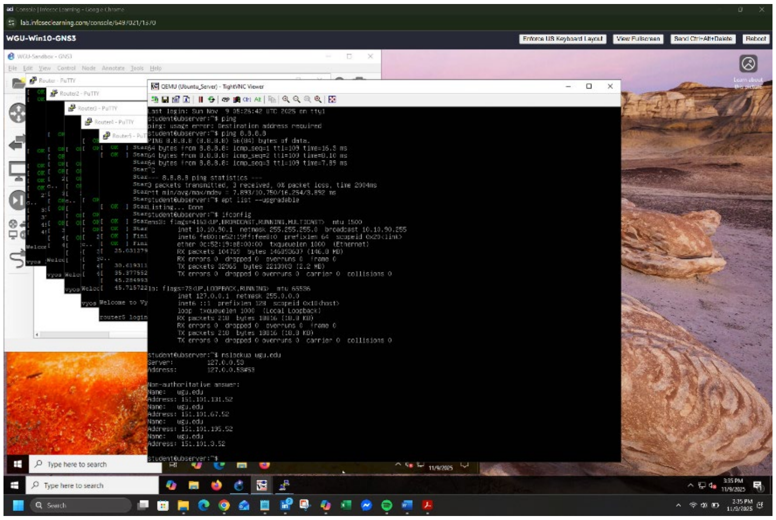
```
You can change this banner using "set system login banner post-login"

VyOS is a free software distribution that includes multiple components
you can check individual component licenses under /usr/share/doc/*/cop
vyos@router5:~$ show arp
Address                  HWtype  HWaddress           Flags Mask
10.10.80.254             ether   0c:18:bb:b7:00:07   C
10.10.90.1               ether   0c:52:19:e8:00:00   C
vyos@router5:~$ show interface
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             10.10.80.1/24                     u/u
eth1             -                                 u/D
eth2             -                                 u/D
eth3             -                                 u/D
eth4             -                                 u/D
eth5             -                                 u/D
eth6             -                                 u/D
eth7             10.10.90.254/24                   u/u
lo               127.0.0.1/8                       u/u
                 ::1/128
vyos@router5:~$
```

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 196 kB of archives.
After this operation, 864 kB of additional disk space will be used.
Err:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1.60+git20180626.aebd88e-1ubuntu1
  Temporary failure resolving 'us.archive.ubuntu.com'
E: Failed to fetch http://us.archive.ubuntu.com/ubuntu/pool/main/n/net-tools/net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.d
eb  Temporary failure resolving 'us.archive.ubuntu.com'
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
student@ubserver:~$ ping 10.10.80.254
PING 10.10.80.254 (10.10.80.254) 56(84) bytes of data.
64 bytes from 10.10.80.254: icmp_seq=1 ttl=63 time=1.28 ms
64 bytes from 10.10.80.254: icmp_seq=2 ttl=63 time=1.10 ms
64 bytes from 10.10.80.254: icmp_seq=3 ttl=63 time=1.09 ms
64 bytes from 10.10.80.254: icmp_seq=4 ttl=63 time=1.15 ms
^C
--- 10.10.80.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.093/1.152/1.276/0.074 ms
student@ubserver:~$ ping 10.10.70.254
PING 10.10.70.254 (10.10.70.254) 56(84) bytes of data.
64 bytes from 10.10.70.254: icmp_seq=1 ttl=62 time=2.74 ms
64 bytes from 10.10.70.254: icmp_seq=2 ttl=62 time=1.68 ms
64 bytes from 10.10.70.254: icmp_seq=3 ttl=62 time=1.71 ms
64 bytes from 10.10.70.254: icmp_seq=4 ttl=62 time=1.91 ms
64 bytes from 10.10.70.254: icmp_seq=5 ttl=62 time=1.81 ms
^C
--- 10.10.70.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 1.670/1.969/2.738/0.392 ms
student@ubserver:~$ ping 10.10.60.254
PING 10.10.60.254 (10.10.60.254) 56(84) bytes of data.
From 10.10.80.254 icmp_seq=1 Time to live exceeded
From 10.10.80.254 icmp_seq=2 Time to live exceeded
From 10.10.80.254 icmp_seq=4 Time to live exceeded
From 10.10.80.254 icmp_seq=8 Time to live exceeded
From 10.10.80.254 icmp_seq=9 Time to live exceeded
From 10.10.80.254 icmp_seq=10 Time to live exceeded
From 10.10.80.254 icmp_seq=11 Time to live exceeded
^C
--- 10.10.60.254 ping statistics ---
15 packets transmitted, 0 received, +7 errors, 100% packet loss, time 14144ms

student@ubserver:~$
```

From the Ubuntu_Server, I ran ifconfig to identify the server's IP address, but network tools were not installed. I tried to install network tools, but I was unable to connect the ping command to the routers in the network traffic. Had good pings until I reached the firewall, where I was unable to ping the device. I attempted to access the firewall from the Ubuntu server side, but I was unable to ping the Ubuntu server. Time Stamp: 12:13 AM 11/5/2025



```
Last login: Sun Nov  9 05:26:42 UTC 2025 on tty1
student@ubserver:~$ ping
ping: usage error: Destination address required
student@ubserver:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=16.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=109 time=8.10 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=109 time=7.89 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 7.893/10.750/16.254/3.892 ms
student@ubserver:~$ apt list --upgradable
Listing... Done
student@ubserver:~$ ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.90.1  netmask 255.255.255.0  broadcast 10.10.90.255
        inet6 fe80::e52:19ff:fee8:0  prefixlen 64  scopeid 0x20<link>
        ether 0c:52:19:e8:00:00  txqueuelen 1000  (Ethernet)
        RX packets 104769  bytes 146893637 (146.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32965  bytes 2213003 (2.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 218  bytes 18816 (18.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 218  bytes 18816 (18.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

student@ubserver:~$ nslookup wgu.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   wgu.edu
Address: 151.101.131.52
Name:   wgu.edu
Address: 151.101.67.52
Name:   wgu.edu
Address: 151.101.195.52
Name:   wgu.edu
Address: 151.101.3.52

student@ubserver:~$
```

From the Ubuntu_Server, connectivity was verified using ping 8.8.8.8 and nslookup wgu.edu, confirming successful internet access and DNS resolution through the internal DNS server and fallback to Google DNS. Time Stamp: 3:35 pm 11/9/2025

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

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

   1. Linux command line interface (ping, traceroute, nslookup, ifconfig, net-tools)

   2. Vyos command line interface (show ip route, show interfaces, show protocols static route, show protocols ospf, configure, set protocols static route, set protocols ospf area, commit, and save)

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

   I initially attempted to run ‘ifconfig’ to verify interface status and IP assignments, but discovered that ‘net-tools’ was not installed. This led me to install the package using ‘sudo apt install net-tools’, which then enabled access to legacy tools like ‘ifconfig’, ‘netstat’, and ‘route’. I used ‘ping’ and ‘traceroute’ to determine how far packets were traveling before being dropped. These tools helped me identify that the routing path broke down between Router 5 and Router 4.

   On the VyOS routers, I used commands such as ‘show ip route’, show interfaces’, and ‘show protocols’ to inspect routing tables and OSPF configurations. I then used ‘configure’, ‘set protocols static route’, and ‘set protocols ospf are’ to correct routing paths and ensure proper next-hop logic. The ‘commit’ and ‘save’ commands finalized and preserved the changes.

   Back on Ubuntu_Server, I verified connectivity by pinging external IPs like 8.8.8.8 and confirmed DNS resolution using nslookup wgu.edu. These tests validated both internet access and proper DNS configuration.

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

   I initiated a verification test on Ubuntu_Server on the command line interface. I initially used ‘ifconfig’ to verify the IP setting on the device, but quickly noticed that the command was unavailable and required net-tools to be installed to use it. I used the ‘ping 10.10.80.1’ command to reach Router5 as shown on the topology. Had a good connection to Router5, but when I tried to ping Router4, I was unsuccessful. I ran ‘traceroute 192.168.122.126’, which is the IP address for the firewall. I noticed the packets were stuck on router5 and making to router4. Initially, I thought it would be a firewall issue, but after checking the routes, it appeared to be a routing issue with routers 4 and 5. Router3 seemed to be routing correctly, as I was able to connect with Windows_Desktop_1 in the previous scenario.

   Since Router1, Router2, and Router3 had a good route, I ran the 'show protocols' command on those routers to see how they were configured. They all had a static route 0.0.0.0/0 next-hop 10.10.xx.254 and OSPF area 0.0.0.0 network 0.0.0.0/0 configuration. I then matched those configurations to Router4 and Router5, and changed the next-hop third octet to 10.10.80.254 for Router5 and 10.10.70.254. Although I missed typed Router4, I set it to 10.10.70.1 by accident. Because of that mistake, I thought the connection was hung up on the firewall, so I checked the firewall settings. The firewall settings appeared to be quite liberal, allowing any traffic to pass through. So, I went back to Ubuntu_Server and ran a traceroute command to see where the connection stopped and discovered it wasn’t going past Router5. So I checked the protocols on Router4 and discovered that it was configured with 10.10.70.1 instead of 0f 10.10.70.254. After that one change, I went back to the Ubuntu_Server to check the connection. It went all the way through the firewall, ‘ping 192.168.122.126’. I ran a ping to 8.8.8.8, the Google DNS server, and had a good connection. I ran ‘sudo apt-get net-tools’ to get the commands like ifconfig through the Ubuntu applications server. The command executed successfully after being downloaded and installed via net-tools. I ran ‘nslookup wgu.edu” to see if it would resolve the domain name with an IP address, and it sure did.

After resolving the issue, I recommend starting at the point where the problem occurred and verifying the resolution to ensure it is effective. Then check the routing configurations. If routing configurations are correct but connectivity issues persist, I recommend checking the firewall rules and settings to determine if the connection is being blocked at that point. Also, when changing configurations, double-check your settings before proceeding; this will prevent you from wasting time searching for something that was left unchecked.

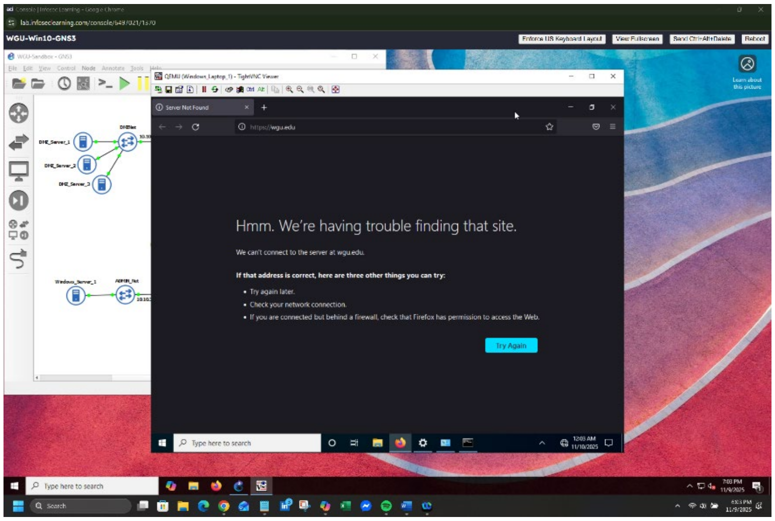
Helpdesk Ticket 4:

Scenario: 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.

Objective (Identify and Resolve): Examine the laptop and network diagram to determine the root cause and fix the issue so the laptop can use and access network resources.

D. Using the information in the scenario for helpdesk ticket 4, do the following:

1. Provide screenshots of the identified problem and the resolution. Screenshots must be clear, with a full view of the screen, and include the date and time.



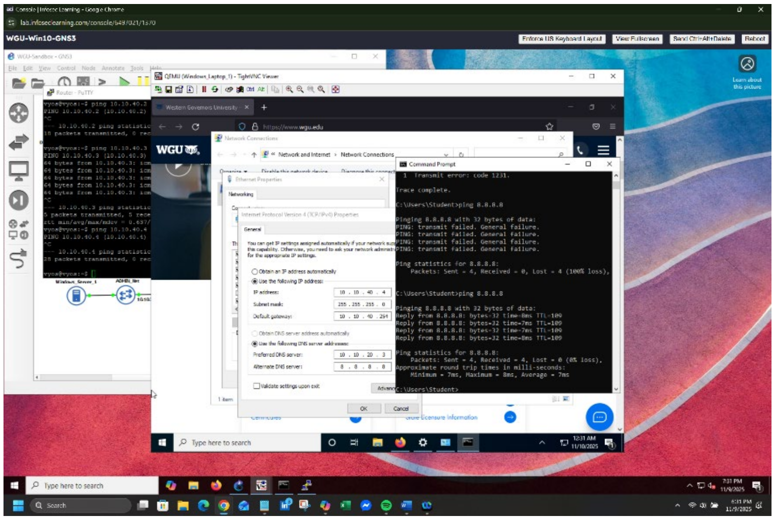
Hmm. We’re having trouble finding that site.

We can’t connect to the server at wgu.edu.

If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

Verified connection by opening a web browser, and unable to connect to wgu.edu
Time Stamp 6:03 pm 11/9/2025



```
vyos@vyos:~$ ping 10.10.40.2
PING 10.10.40.2 (10.10.40.2)
^C
--- 10.10.40.2 ping statistic
10 packets transmitted, 0 rec

vyos@vyos:~$ ping 10.10.40.3
PING 10.10.40.3 (10.10.40.3)
64 bytes from 10.10.40.3: icm
64 bytes from 10.10.40.3: icm
64 bytes from 10.10.40.3: icm
64 bytes from 10.10.40.3: icm
64 bytes from 10.10.40.3: icm
^C
--- 10.10.40.3 ping statistic
5 packets transmitted, 5 rece
rtt min/avg/max/mdev = 0.637/
vyos@vyos:~$ ping 10.10.40.4
PING 10.10.40.4 (10.10.40.4)
^C
--- 10.10.40.4 ping statistic
28 packets transmitted, 0 rec

vyos@vyos:~$
```

Internet Protocol Version 4 (TCP/IPv4) Properties

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 10 . 10 . 40 . 4
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 10 . 40 . 254

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 10 . 10 . 20 . 3
Alternate DNS server: 8 . 8 . 8 . 8

☐ Validate settings upon exit

```
  1  Transmit error: code 1231.

Trace complete.

C:\Users\Student>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),


C:\Users\Student>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=8ms TTL=109
Reply from 8.8.8.8: bytes=32 time=7ms TTL=109
Reply from 8.8.8.8: bytes=32 time=7ms TTL=109
Reply from 8.8.8.8: bytes=32 time=8ms TTL=109

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 8ms, Average = 7ms

C:\Users\Student>
```

I resolved the issue by updating IPv4 properties. Ping 8.8.8.8 and used a web browser to verify the connection to wgu.edu.

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

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

1. Vyos Command line interface (show interface)
2. Windows command prompt (ping, nslookup)
3. Windows Settings (Ethernet Properties, Internet Protocol Version 4 (TCP/IPv4) Properties)

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

To troubleshoot the connectivity issue on Windows_Laptop_1, I accessed the VyOS Router1 command line interface. I used the ‘show interface’ command to identify the IP address assigned to the router interface that connects directly to the laptop. This step was essential to determine the correct default gateway that should be configured on the laptop’s network settings.

On the Windows_Laptop_1 device I opened the Command Prompt. I used the command ping to test basic connectivity and verify whether the laptop could reach external IP addresses. I also ran ‘nslookup wgu.edu’ to check if DNS resolution was functioning correctly. These tools helped confirm whether the issue was related to IP configuration or DNS.

After identifying that the laptop had a self-assigned IP address and no default gateway, I opened the Ethernet adapter settings through the Windows Settings menu. I navigated to the Internet Protocol Version 4 (TCP/IPv4) properties and manually configured the network settings. I assigned a valid static IP address, subnet mask, default gateway (based on the VyOS interface IP), and DNS server addresses.

These tools were chosen because they provided direct visibility into both the router’s configuration and the laptop’s network state, allowing me to isolate and resolve the issue efficiently.

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

I began the troubleshooting process at the user’s device, Windows_Laptop_1, by checking its ability to connect to the internet. I opened a web browser and attempted to access wgu.edu, but the page failed to load, confirming a connectivity issue. To gather more information, I launched the Command Prompt and ran ‘ipconfig /all’. The output revealed that the laptop had a self-assigned IP address of ‘169.254.0.1’ and no default gateway—indicating it was unable to obtain a valid IP configuration from the network.

To determine the correct default gateway for the laptop, I accessed VyOS Router1 and used the ‘show interface’ command. This allowed me to identify the IP address assigned to the router interface connected to Windows_Laptop_1, which was 10.10.40.254.

With this information, I returned to the laptop and navigated to Windows Settings → Network & Internet → Ethernet → Change Adapter Options → Ethernet Properties. I selected Internet Protocol Version 4 (TCP/IPv4) and opened its properties. I manually configured the following settings:

- IP Address: 10.10.40.4
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.10.40.254
- Preferred DNS Server: 10.10.20.3
- Alternate DNS Server: 8.8.8.8.

After applying these changes, the laptop immediately connected to the network. I verified connectivity by successfully pinging 8.8.8.8 and running nslookup wgu.edu, which returned a valid IP address. Finally, I reopened the browser and confirmed that wgu.edu loaded without issue, indicating that both internet access and DNS resolution were functioning correctly.

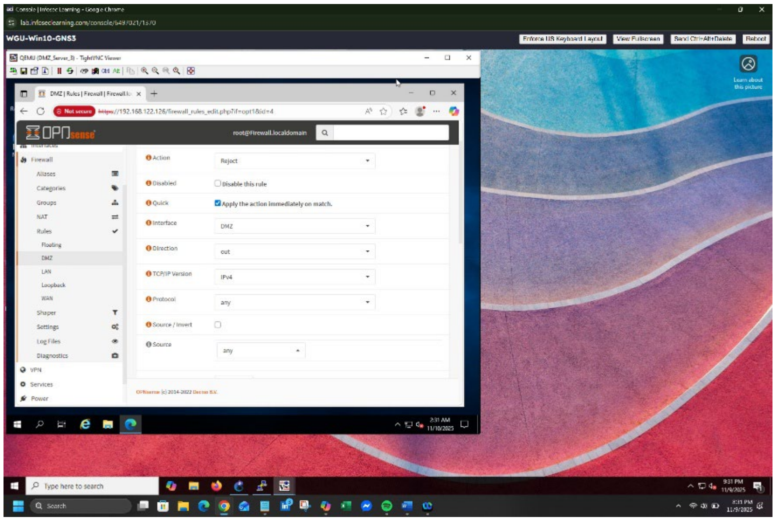
Helpdesk Ticket 5:

Scenario: 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.

Objective (Identify and Resolve): Examine the host and firewall to determine the root cause of the issue and make changes to provide a resolution.

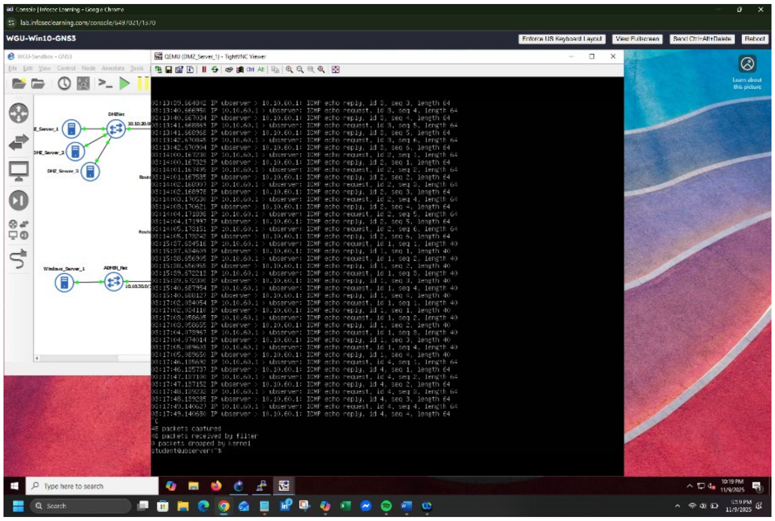
E. Using the information in the scenario for helpdesk ticket 5, do the following:

1. Provide screenshots of the identified problem and the resolution. Screenshots must be clear, with a full view of the screen, and include the date and time.


Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/549/021/1570
WGU-Win10-GNS3
QEMU (DMZ_Server_3) - TightVNC Viewer
DMZ | Rules | Firewall | Firewall.lo
Not secure
https://192.168.122.126/firewall_rules_edit.php?if=opt1&id=4
OPNsense
root@Firewall.localdomain
Firewall
Aliases
Categories
Groups
NAT
Rules
Floating
DMZ
LAN
Loopback
WAN
Shaper
Settings
Log Files
Diagnostics
VPN
Services
Power
OPNsense (c) 2014-2022 Deciso B.V.
2:31 AM
11/10/2025
Type here to search
9:31 PM
11/9/2025
Search

Action: Reject
Disabled: ☐ Disable this rule
Quick: ☑ Apply the action immediately on match.
Interface: DMZ
Direction: out
TCP/IP Version: IPv4
Protocol: any
Source / Invert: ☐
Source: any

Checked Firewall Rules DMZ. It appears that the person working on the ticket set the action to reject instead of allowing.
Time Stamp: 9:31 PM 11/9/2025



```
03:13:39.664842 IP ubserver > 10.10.60.1: ICMP echo reply, id 3, seq 3, length 64
03:13:40.666950 IP 10.10.60.1 > ubserver: ICMP echo request, id 3, seq 4, length 64
03:13:40.667034 IP ubserver > 10.10.60.1: ICMP echo reply, id 3, seq 4, length 64
03:13:41.668869 IP 10.10.60.1 > ubserver: ICMP echo request, id 3, seq 5, length 64
03:13:41.668968 IP ubserver > 10.10.60.1: ICMP echo reply, id 3, seq 5, length 64
03:13:42.670845 IP 10.10.60.1 > ubserver: ICMP echo request, id 3, seq 6, length 64
03:13:42.670904 IP ubserver > 10.10.60.1: ICMP echo reply, id 3, seq 6, length 64
03:14:00.167230 IP 10.10.60.1 > ubserver: ICMP echo request, id 2, seq 1, length 64
03:14:00.167329 IP ubserver > 10.10.60.1: ICMP echo reply, id 2, seq 1, length 64
03:14:01.167495 IP 10.10.60.1 > ubserver: ICMP echo request, id 2, seq 2, length 64
03:14:01.167585 IP ubserver > 10.10.60.1: ICMP echo reply, id 2, seq 2, length 64
03:14:02.168907 IP 10.10.60.1 > ubserver: ICMP echo request, id 2, seq 3, length 64
03:14:02.168978 IP ubserver > 10.10.60.1: ICMP echo reply, id 2, seq 3, length 64
03:14:03.170530 IP 10.10.60.1 > ubserver: ICMP echo request, id 2, seq 4, length 64
03:14:03.170621 IP ubserver > 10.10.60.1: ICMP echo reply, id 2, seq 4, length 64
03:14:04.171898 IP 10.10.60.1 > ubserver: ICMP echo request, id 2, seq 5, length 64
03:14:04.171997 IP ubserver > 10.10.60.1: ICMP echo reply, id 2, seq 5, length 64
03:14:05.173151 IP 10.10.60.1 > ubserver: ICMP echo request, id 2, seq 6, length 64
03:14:05.173242 IP ubserver > 10.10.60.1: ICMP echo reply, id 2, seq 6, length 64
03:15:37.634516 IP 10.10.60.1 > ubserver: ICMP echo request, id 1, seq 1, length 40
03:15:37.634609 IP ubserver > 10.10.60.1: ICMP echo reply, id 1, seq 1, length 40
03:15:38.656905 IP 10.10.60.1 > ubserver: ICMP echo request, id 1, seq 2, length 40
03:15:38.656955 IP ubserver > 10.10.60.1: ICMP echo reply, id 1, seq 2, length 40
03:15:39.672213 IP 10.10.60.1 > ubserver: ICMP echo request, id 1, seq 3, length 40
03:15:39.672300 IP ubserver > 10.10.60.1: ICMP echo reply, id 1, seq 3, length 40
03:15:40.687954 IP 10.10.60.1 > ubserver: ICMP echo request, id 1, seq 4, length 40
03:15:40.688127 IP ubserver > 10.10.60.1: ICMP echo reply, id 1, seq 4, length 40
03:17:02.034054 IP 10.10.60.1 > ubserver: ICMP echo request, id 1, seq 1, length 40
03:17:02.034110 IP ubserver > 10.10.60.1: ICMP echo reply, id 1, seq 1, length 40
03:17:03.058605 IP 10.10.60.1 > ubserver: ICMP echo request, id 1, seq 2, length 40
03:17:03.058655 IP ubserver > 10.10.60.1: ICMP echo reply, id 1, seq 2, length 40
03:17:04.073967 IP 10.10.60.1 > ubserver: ICMP echo request, id 1, seq 3, length 40
03:17:04.074014 IP ubserver > 10.10.60.1: ICMP echo reply, id 1, seq 3, length 40
03:17:05.089603 IP 10.10.60.1 > ubserver: ICMP echo request, id 1, seq 4, length 40
03:17:05.089650 IP ubserver > 10.10.60.1: ICMP echo reply, id 1, seq 4, length 40
03:17:46.135692 IP 10.10.60.1 > ubserver: ICMP echo request, id 4, seq 1, length 64
03:17:46.135737 IP ubserver > 10.10.60.1: ICMP echo reply, id 4, seq 1, length 64
03:17:47.137100 IP 10.10.60.1 > ubserver: ICMP echo request, id 4, seq 2, length 64
03:17:47.137152 IP ubserver > 10.10.60.1: ICMP echo reply, id 4, seq 2, length 64
03:17:48.139232 IP 10.10.60.1 > ubserver: ICMP echo request, id 4, seq 3, length 64
03:17:48.139285 IP ubserver > 10.10.60.1: ICMP echo reply, id 4, seq 3, length 64
03:17:49.140627 IP 10.10.60.1 > ubserver: ICMP echo request, id 4, seq 4, length 64
03:17:49.140680 IP ubserver > 10.10.60.1: ICMP echo reply, id 4, seq 4, length 64
^C
48 packets captured
48 packets received by filter
0 packets dropped by kernel
student@ubserver:~$
```

Log showing devices outside its network connecting to DMZ_Server_1 using the ‘sudo tcpdump -i ens3 icmp’ command.
Time Stamp: 10:19 pm 11/9/2025

2. **Provide a root cause analysis write-up by doing the following:**
   a. **List the tool(s) used to identify the problem.**

1. Web Browser
2. OPNsense Firewall Graphical User Interface (GUI)
3. Linux command line interface (ping, ifconfig, tcpdump)
4. Windows command prompt (ping)

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

I used the web browser to open the OPNsense Firewall GUI. In the firewall GUI, navigate to the Firewall, Rules, and DMZ tabs. At that window, I can verify DMZ rules that have been applied.

I used the Linux command line interface to verify the connection and the Ethernet interface. ‘ping’ to confirm the connection from outside the network devices. ‘ifconfig’ to identify the Ethernet interface on DMZ_Server_1. ‘tcpdump’ to verify and record that other devices outside the network are connecting to DMZ_Server_1.

I used the Windows command prompt ‘ping’ command to verify the connection of the outside device to DMZ_Server_1.

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

I began by signing into the OPNsense Firewall GUI on a web browser with the 192.168.122.126 address. I navigated to the Firewall, Rules, and DMZ tabs to find the rules. It appears that a rule was set up to allow connections to DMZ_Server_1 from devices outside its network. But it was configured with a reject instead of a pass. All I had to do was change the status from 'reject' to 'pass' to allow traffic.

To prove that devices connected to DMZ_Server_1 (10.10.20.0/24 subnet) are identified, I identified its Ethernet interface so I can run the ‘tcpdump’ command to record connections from outside devices. I ran ‘sudo tcpdump -i ens3 icmp’ to start recording other devices connecting to it. Then I went to other devices, including Ubuntu_Server (10.10.90.0/24 subnet) and Windows_Laptop_1 (10.10.40.0/24 subnet), and ran ‘ping 10.10.20.1’ (the DMZ_Server_1 IP address) on each device. After receiving positive pings, I returned to DMZ_Server_1 to capture a snapshot of the connection notifications—verifying the connection from outside networks to DMZ_Server_1.

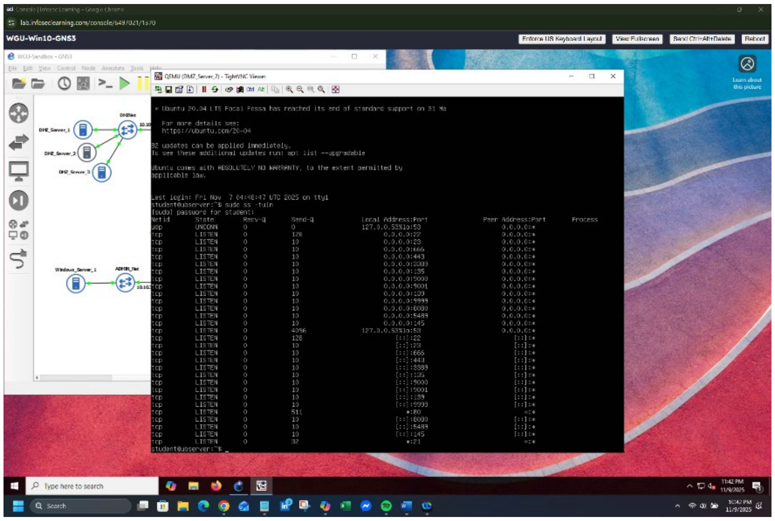
Helpdesk Ticket 6:

Scenario: Your local cyber security team is requesting to know what ports are open on DMZ_Server2 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.

Objective (Identify and Recommend Resolution): Use network assessment tools to scan the device and report back any services that are not in the approved services list above to the security team.

F. Using the information in the scenario for helpdesk ticket 6, do the following:

1. Provide screenshots of the identified problem and the resolution. Screenshots must be clear, with a full view of the screen, and include the date and time.



```
* Ubuntu 20.04 LTS Focal Fossa has reached its end of standard support on 31 Ma

  For more details see:
  https://ubuntu.com/20-04

82 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


Last login: Fri Nov  7 04:48:47 UTC 2025 on tty1
student@ubserver:~$ sudo ss -tuln
[sudo] password for student:
Netid      State      Recv-Q     Send-Q          Local Address:Port          Peer Address:Port      Process
udp        UNCONN     0          0               127.0.0.53%lo:53                 0.0.0.0:*
tcp        LISTEN     0          128                   0.0.0.0:22                 0.0.0.0:*
tcp        LISTEN     0          10                    0.0.0.0:23                 0.0.0.0:*
tcp        LISTEN     0          10                    0.0.0.0:666                0.0.0.0:*
tcp        LISTEN     0          10                    0.0.0.0:443                0.0.0.0:*
tcp        LISTEN     0          10                    0.0.0.0:3389               0.0.0.0:*
tcp        LISTEN     0          10                    0.0.0.0:135                0.0.0.0:*
tcp        LISTEN     0          10                    0.0.0.0:9000               0.0.0.0:*
tcp        LISTEN     0          10                    0.0.0.0:9001               0.0.0.0:*
tcp        LISTEN     0          10                    0.0.0.0:139                0.0.0.0:*
tcp        LISTEN     0          10                    0.0.0.0:9999               0.0.0.0:*
tcp        LISTEN     0          10                    0.0.0.0:8080               0.0.0.0:*
tcp        LISTEN     0          10                    0.0.0.0:5489               0.0.0.0:*
tcp        LISTEN     0          10                    0.0.0.0:145                0.0.0.0:*
tcp        LISTEN     0          4096            127.0.0.53%lo:53                 0.0.0.0:*
tcp        LISTEN     0          128                      [::]:22                    [::]:*
tcp        LISTEN     0          10                       [::]:23                    [::]:*
tcp        LISTEN     0          10                       [::]:666                   [::]:*
tcp        LISTEN     0          10                       [::]:443                   [::]:*
tcp        LISTEN     0          10                       [::]:3389                  [::]:*
tcp        LISTEN     0          10                       [::]:135                   [::]:*
tcp        LISTEN     0          10                       [::]:9000                  [::]:*
tcp        LISTEN     0          10                       [::]:9001                  [::]:*
tcp        LISTEN     0          10                       [::]:139                   [::]:*
tcp        LISTEN     0          10                       [::]:9999                  [::]:*
tcp        LISTEN     0          511                         *:80                       *:*
tcp        LISTEN     0          10                       [::]:8080                  [::]:*
tcp        LISTEN     0          10                       [::]:5489                  [::]:*
tcp        LISTEN     0          10                       [::]:145                   [::]:*
tcp        LISTEN     0          32                          *:21                       *:*
student@ubserver:~$ _
```

On DMZ_Server_2, I ran the command sudo ss -tuln to display the open ports on that device.
Time Stamp 11:42 pm 11/9/2025

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

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

1. Linux command line interface (ss -tuln and lsof -I -P | grep LISTEN)

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

I choose to run ‘ss -tuln’ to provide a snapshot of all TCP and UDP ports currently in the LISTEN state. I then ran ‘lsof -I -P | grep LISTEN’ to correlate ports with the services responsible and map each open port to its corresponding process, user, and protocol.

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.

On the DMZ_Server_2, I ran ss -tuln and ‘lsof -I -P | grep LISTEN’ commands on the command line interface and determined that the following not permitted ports/services were running:

- Port 23 / Telnet
- Port 53 / DNS
- Port 666 / IRC-based backdoor

- Port 80 / HTTP
- Port 443 / HTTPS
- Port 145 / UACC
- Port 5489 / VMware
- Port 9000 / Docker
- Port 9001 / ETL
- Port 9999 / potential backdoor

Recommend report findings to the security team and discuss the way forward to align with the security team's policy.