

## **Exploring the Seven Domains of a Typical IT Infrastructure**

**Osamudiamen Eweka**

**Cyb-605-Z2 Principles of Cybersecurity**

**Utica University**

## **Introduction**

The lab work involves exploring the seven domains of a typical IT infrastructure and understanding fundamental concepts of information systems security. The lab provides a hands-on demonstration of various tasks, including reviewing basic security controls on a Windows workstation, exploring devices on the LAN segment, connecting to a router-firewall device, and examining network perimeter. The lab also includes research-based exercises to identify threats and security controls in the User Domain, as well as recommend additional security controls for different technical domains of an IT infrastructure. The lab aims to enhance understanding of common command-line utilities, remote connections to network devices, and identification of common network devices and server roles. Overall, the lab work offers a comprehensive learning experience in IT infrastructure and information systems security.

## **Objective**

The objective of this lab is to explore and understand the seven domains of a typical IT infrastructure, including the workstation, LAN, LAN-to-WAN, WAN, remote access, and system/application domains. This involves using common command-line utilities, remote connections, and network devices to gather relevant system information and identify common server roles and network devices. Additionally, the lab aims to provide hands-on experience in applying security controls and measures to protect the IT infrastructure, as well as conducting independent, unguided work to address real-world security challenges and threats.

## Lab Setup

### Lab Environment Details

***The tools and systems used in the lab include:*** vWorkstation (Windows: Server 2022), Switch01 (Linux: Debian 11), FileServer01 (FreeBSD), pfSense-office (FreeBSD), pfSense-dc (FreeBSD), DomainController01 (Windows: Server 2019), WebServer01 (Linux: Ubuntu 20), RemoteWindows01 (Windows: Server 2019), AttackLinux01 (Linux: Kali)

**The required software and utilities for completing the lab include:** PuTTY, Ping, Open vSwitch, TrueNAS, pfSense, Traceroute, Nslookup, OpenVPN, OWASP Juice Shop.

These tools and systems are used to explore and analyze various aspects of a typical IT infrastructure, including network connectivity, security controls, and server roles. They are utilized to gather relevant system information, remotely connect to network devices, and identify common network devices and server roles.

## Section 1: Hands-On Demonstration

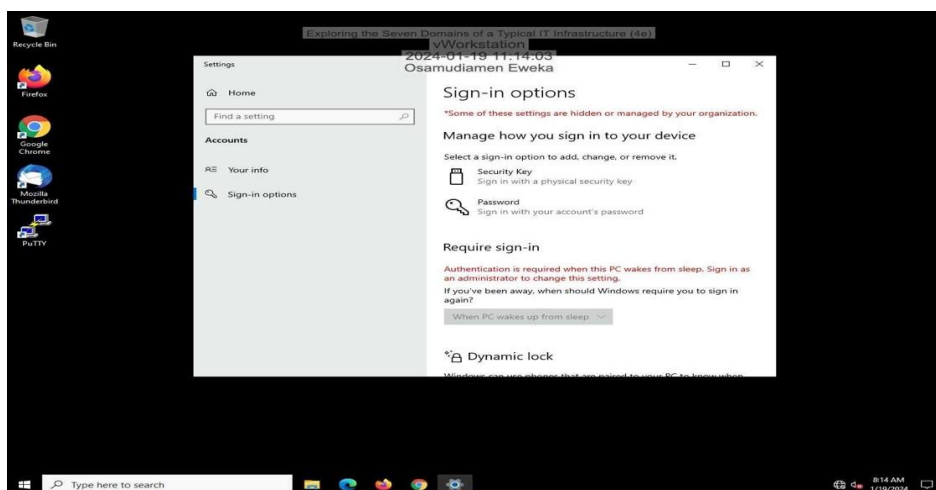
### Part 1:

#### *Explore the Workstation Domain*

In the subsequent steps, participants are tasked with assuming the role of a desktop support engineer operating within the fictional Secure Labs on Demand organization. The scenario envisions that the engineer has recently concluded the update of an older employee workstation to the latest version of Windows. Upon reaching the vWorkstation log-in page, participants are instructed to click on "Other user." Subsequently, they should input the following credentials and press Enter to log in as the workstation's primary user: (User: adodson, Password: P@ssw0rd!) This step ensures access to the workstation and facilitates the validation of security controls within the Workstation Domain. The screenshot in Figure 1 (Eweka,2024) below shows the Sign-in options for Alice's account.

**Figure 1:**

*Sign-in options for Alice's account.*

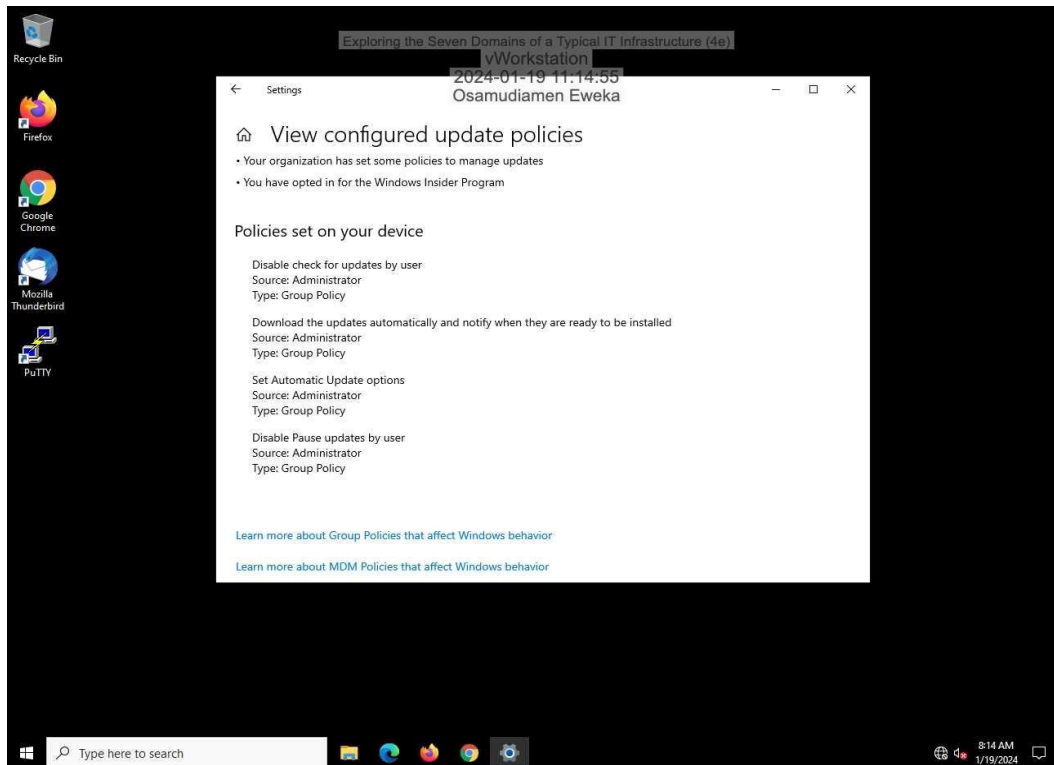


In the ensuing steps, participants are directed to scrutinize the Windows Update settings to verify the automatic reception of system software updates by the vWorkstation. Given the relentless pursuit of new attack methods by malicious entities, it remains imperative to ascertain that each system, in this case, the vWorkstation, is consistently fortified with the latest security updates. Recognizing the inevitability of evolving threats, Microsoft enables administrators to institute policies ensuring the regular infusion of security patches into systems, thus alleviating the burden from individual users.

The adoption of policies for automatic updates stands as one of the paramount security practices within the Workstation Domain. Participants will encounter a comprehensive list of updated policies configured on Alice Dodson's workstation. These policies collectively establish a standardized approach to update management across all devices within an organization. Importantly, they serve as a deterrent against inadvertent or deliberate user interference with the critical update process. Figure 2 (Eweka, 2024) below highlights the View configured update policies page.

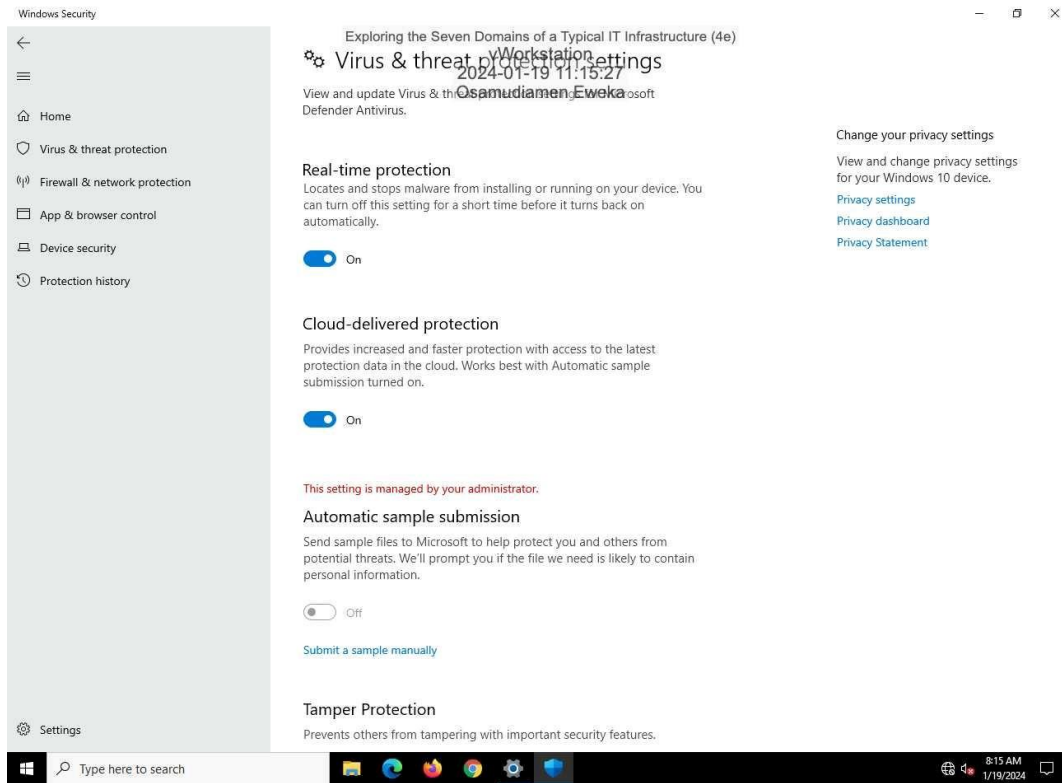
**Figure 2:**

*View the configured update policies page.*



Next downloading and installing operating system and software updates is only one part of a comprehensive security strategy. Patching software with the latest security updates goes a long way toward reducing the number of known software vulnerabilities, but these efforts must be accompanied by real-time monitoring to detect suspicious activity. Figure 3 (Eweka,2024) highlights the Virus & Threat Protection Settings.

**Figure 3:**  
*Virus & Threat Protection Settings.*



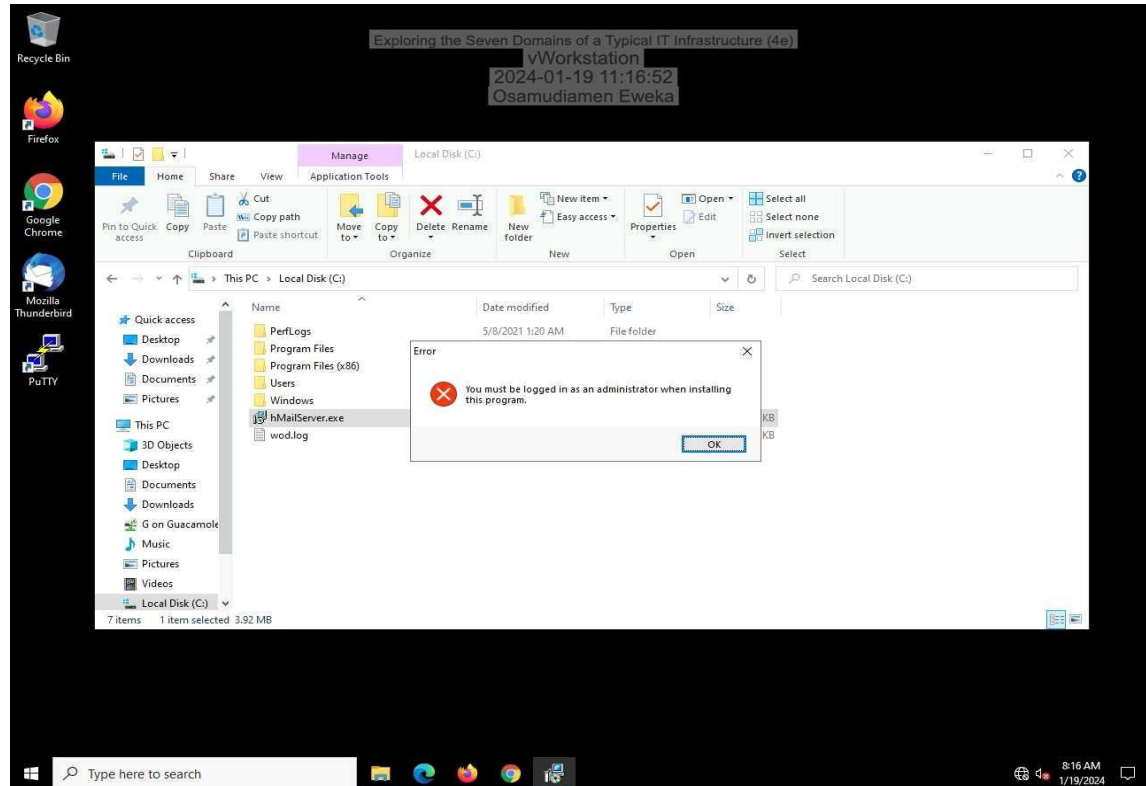
In the subsequent steps, participants are directed to endeavor the installation of a new application, aiming to confirm the adequacy of permissions assigned to Alice's account. An anticipated outcome of this action is the display of an error message indicating the necessity of being logged in as an administrator to proceed with the program installation Figure 4 (Eweka, 2024) shows this error message. Despite the potential inconvenience for certain users, it is crucial to recognize that the imposition of this policy serves as a fundamental security control. This measure effectively limits standard users from independently installing software without the requisite administrator approval. The significance lies in its role as a critical safeguard, preventing malicious actors from deploying tools that may pose a threat to the integrity of the



system. This security control aligns with established best practices within the Workstation Domain, highlighting the paramount importance of restricting user permissions to bolster overall system security.

**Figure 4:**

*security warning from attempting to run an executable file.*

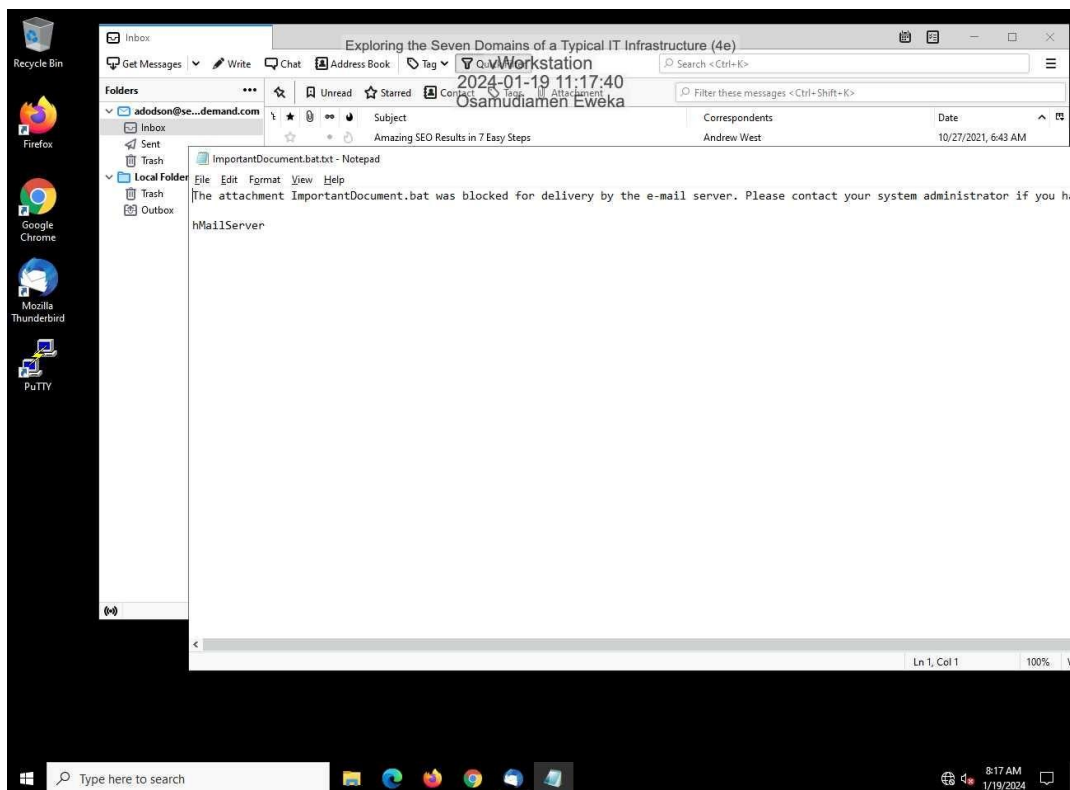


In the forthcoming steps, participants will assess the efficiency of the organization's email security solution by scrutinizing Alice's email account. Previous testing involved intentionally sending test emails to evaluate the system's handling of incoming messages. A pivotal focus is placed on the "EXTERNAL EMAIL: CAUTION" warning, indicating external message origins. This warning is crucial for uncovering potential targeted phishing attempts, particularly if internal-looking emails bear this cautionary label, implying a possible impersonation effort. Participants are instructed to proceed by clicking "OK" when prompted.

An additional point of attention involves the "Important Document" attachment, seemingly a .bat file disguised as a .txt extension as shown in figure 5 (Eweka, 2024). Typically, .bat files carry malicious commands, but in this simulation, the email security service appears to have effectively blocked the .bat file, substituting it with a benign text file. This not only serves as a warning but also acts as a protective measure against potential cyber threats. As participants navigate the email account inspection, these details underscore the critical role of robust email security in countering evolving cyber threats and safeguarding organizational integrity.

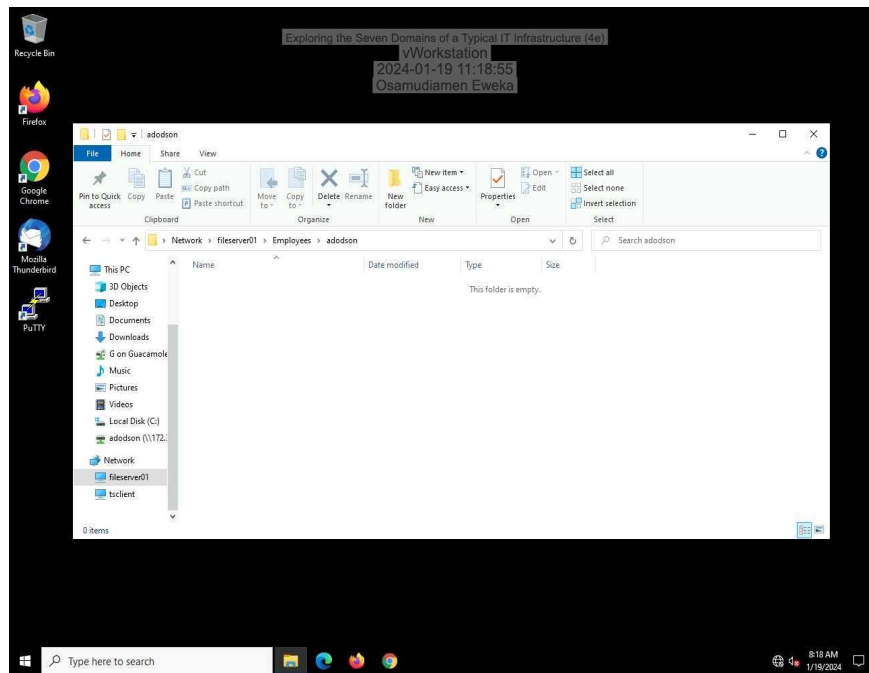
**Figure 5:**

*The blocked attachment messages.*

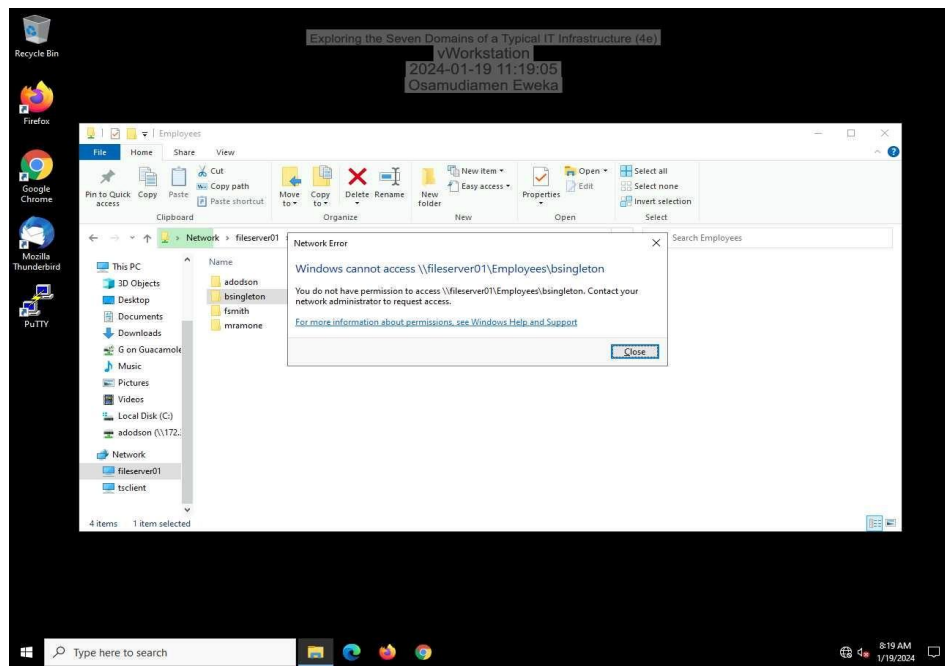


**Figure 6**

*Successful connection to the adodson user folder.*

**Figure 7**

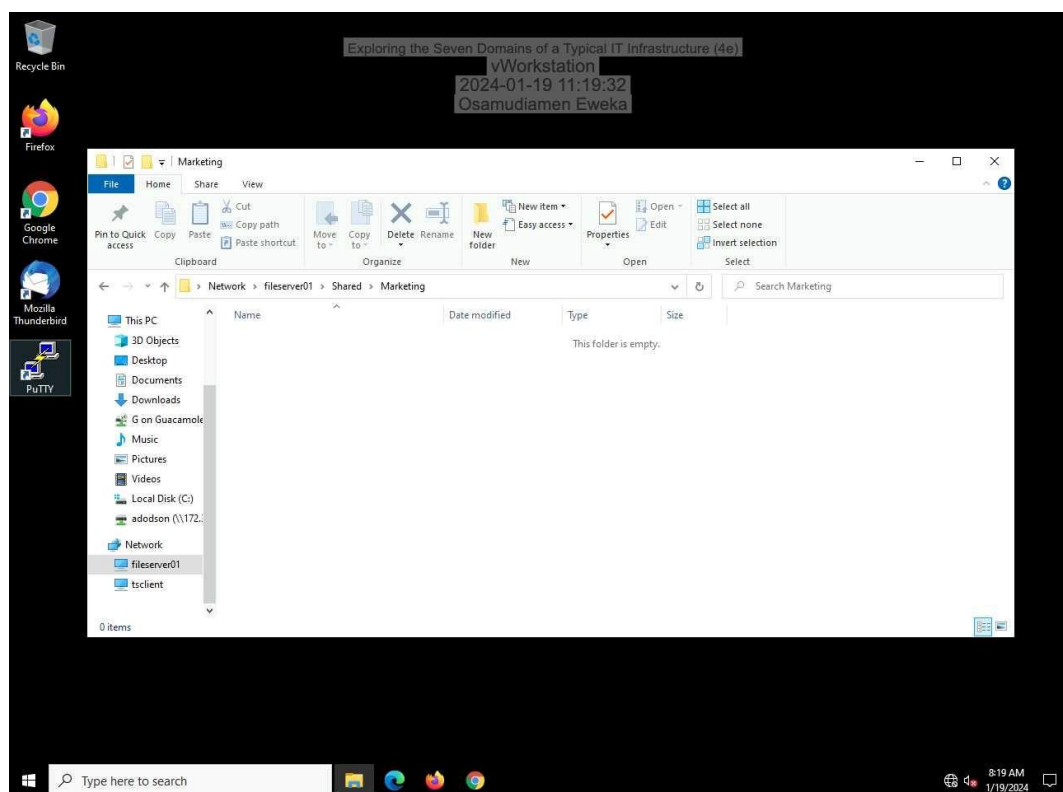
*Shows a failed connection to another user folder.*



In the above Figure 6 & Figure 7 (Eweka, 2024) in the final check, participants will confirm the accurate permissions assigned to Alice's account on Secure Labs on Demand's shared file server. Specifically, it's crucial to ensure that Alice, as a marketing department member, only has access to her private folder and the Marketing team's shared folder. The file server structure includes individual user folders and a globally shared folder for each department, with permissions precisely configured to limit access to designated folders. This ensures strict adherence to the principle of least privilege, granting users access only to the resources essential to their roles.

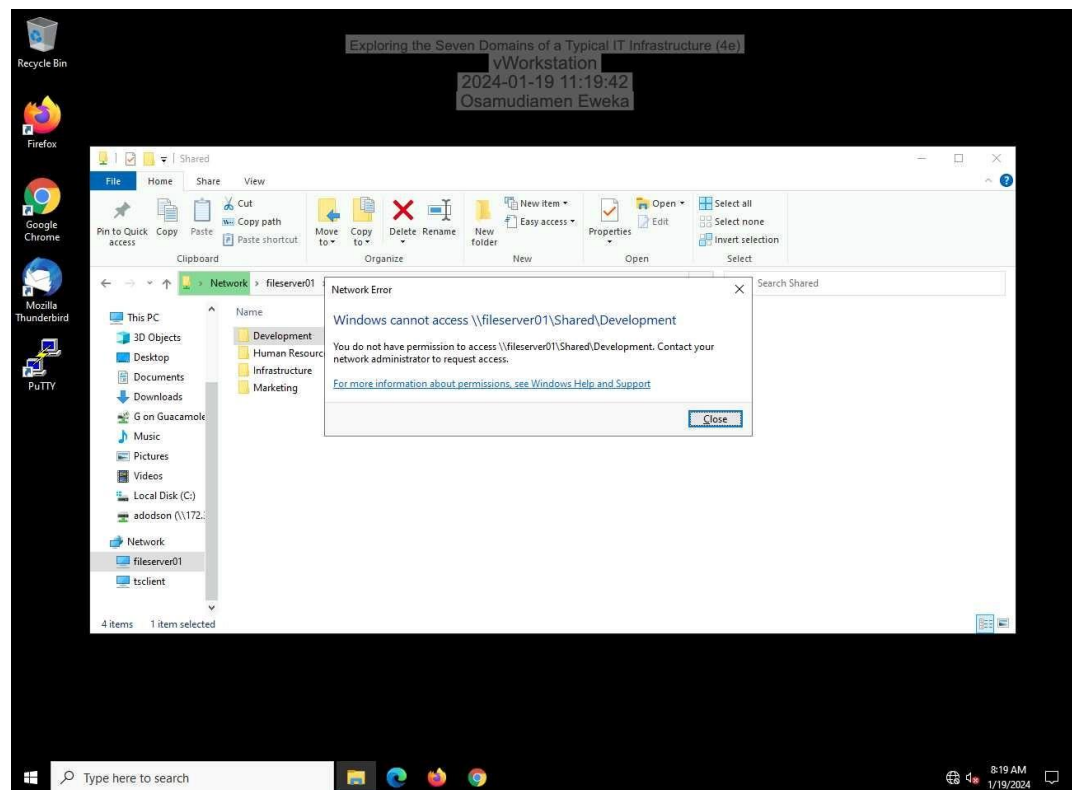
## Figure 8

*Shows a successful connection to the Marketing shared folder.*



**Figure 9**

*Shows a failed connection to another shared folder.*



Figures 8 and 9 (Eweka, 2024) In the current configuration above show, that all authorized users have access to the Shared folder. However, user access is restricted to folders linked with their respective departments. As Alice Dodson is affiliated with the Marketing department, her account should solely have access to the Marketing folder and no others. This setup ensures precise access control, aligning with departmental boundaries and security best practices.

## Section 1: Hands-On Demonstration

### Part 2:

#### *Explore the LAN Domain*

In this segment of the lab, the focus is on exploring the LAN Domain within the virtual environment. The local area network (LAN) Domain, along with the LAN-to-WAN Domain, A wide-area network (WAN) Domain, and Remote Access Domain, primarily deals with networking and network security. To delve into the LAN Domain, a brief review of foundational networking concepts outlined in the Open Systems Interconnection (OSI) Reference Model is recommended.

A Local Area Network (LAN) is essentially a collection of computers connected through a shared medium, such as wires, fiber-optic cables, or radio waves. Typically, LANs are structured based on organizational functions or departments (Kim & Solomon, 2021). In the current configuration, authorized users have access to the Shared folder, but their access is specifically confined to folders associated with their respective departments. For example, as Alice Dodson belongs to the Marketing department, her account is tailored to access only the Marketing folder, exemplifying a precise access control approach that aligns with departmental delineations and adheres to security best practices.

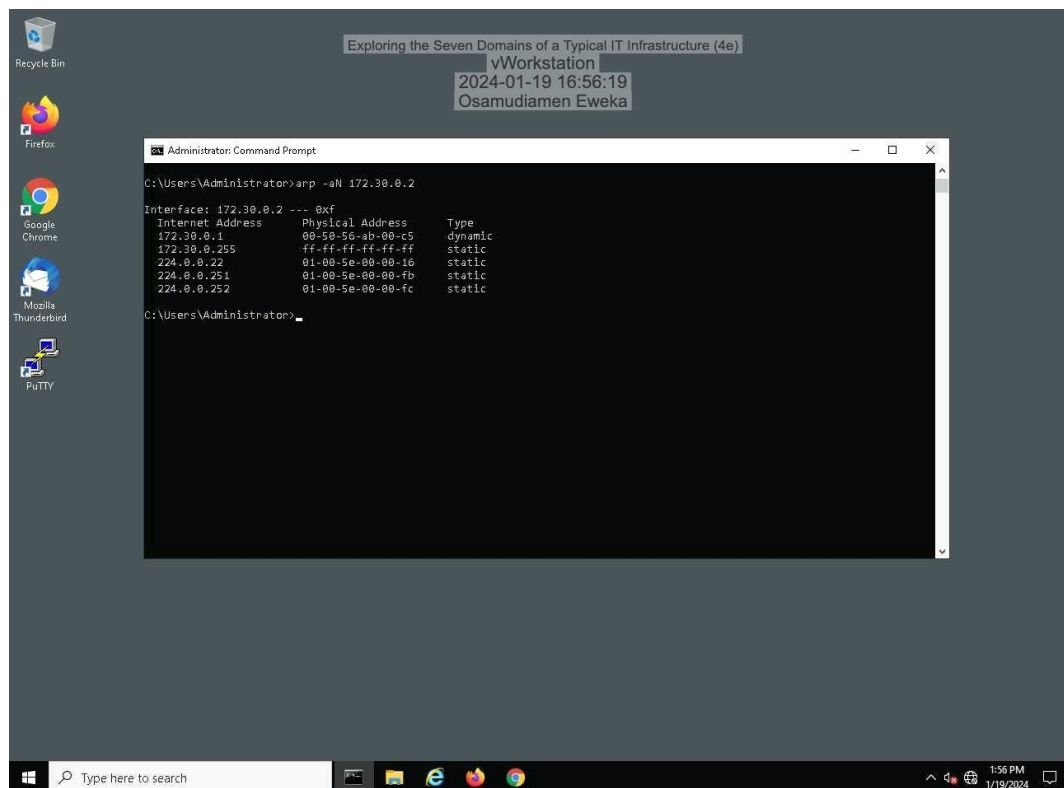
For the rest of the lab, participants have designated the role of a security engineer at the fictional Secure Labs on Domain organization. The task at hand involves acquainting oneself with the organization's network and critical systems. Subsequent steps will entail gathering information regarding the vWorkstation's network configuration, validating connectivity with other devices on the Local Area Network (LAN), and establishing remote connections to two of

these devices. This multifaceted exploration aims to enhance understanding and proficiency in managing network configurations and remote connections within the organization's infrastructure.

Transition to the workstation log-in screen, where participants are instructed to enter the password "P@ssw0rd!" to log in as the local Administrator. Following successful log-in, proceed to the workstation taskbar and click on the Command Prompt icon to initiate a new Command Prompt window. Alternatively, participants can use the shortcut "Win + R" keys on the keyboard, followed by typing "cmd" to achieve the same outcome. These actions set the stage for further exploration and command-line interactions in the lab environment. At the command prompt, type `ipconfig /all` and press Enter to display the vWorkstation's network interfaces. As shown in Figure 10 (Eweka, 2024).

**Figure 10**

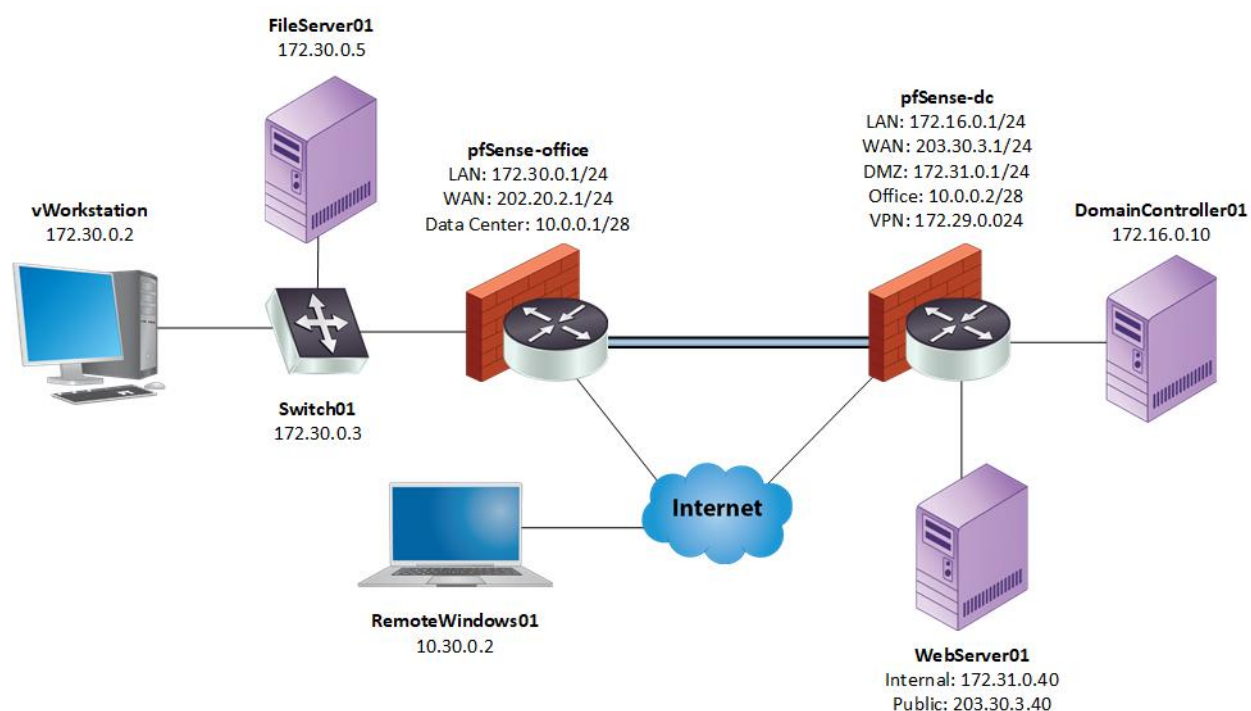
*vWorkstation's original Address Resolution Protocol (ARP) table.*



Examine the command output, where participants should observe two distinct Ethernet adapter results for the vWorkstation, reflecting its two network interface cards. In the context of this lab, the primary focus is on the student interface, the sole interface of interest. This interface serves as the communication conduit with the network illustrated in the topology diagram provided below for your convenience in Figure 11 (Kim, 2021). Understanding and identifying the student interface are crucial steps for subsequent tasks aligned with the lab objectives.

**Figure 11**

*Network topology diagram.*



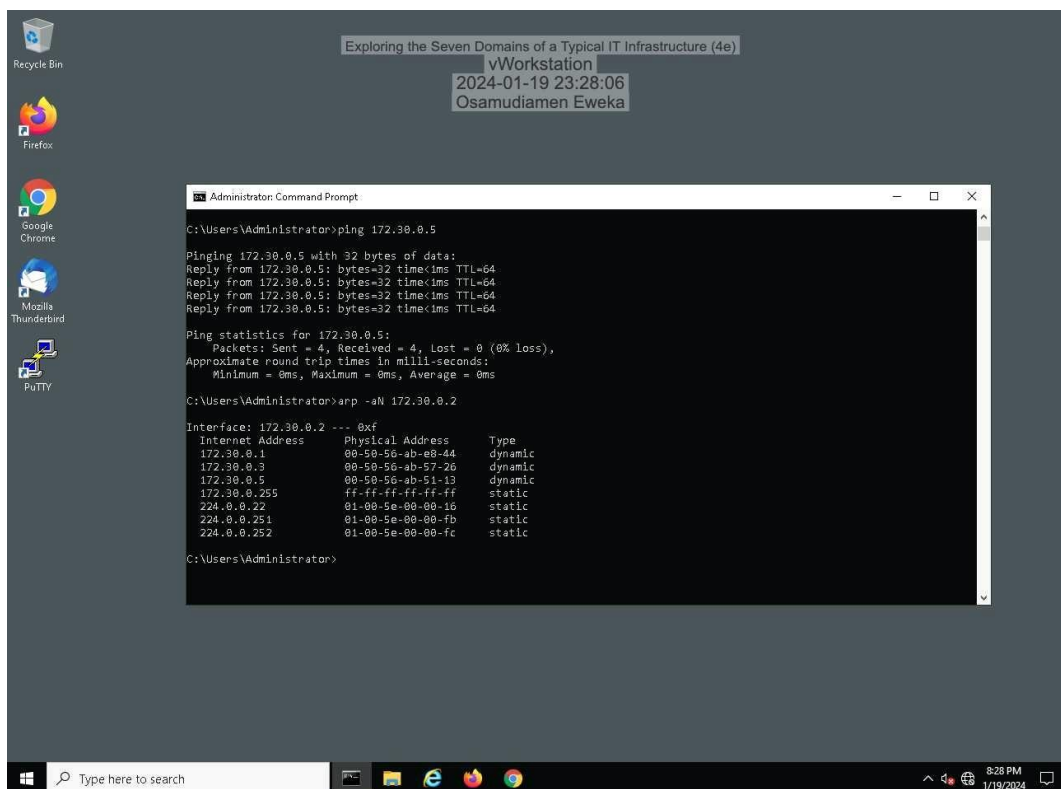
In the subsequent steps, participants are directed to review the Address Resolution Protocol (ARP) table linked to the Student Network Interface Card (NIC). This activity involves examining the ARP table, a critical component for mapping IP addresses to corresponding MAC addresses within the network. This information is vital for understanding the network's current state and facilitating effective communication between devices.



At the command prompt, type `arp -aN 172.30.0.2` and press Enter to display the ARP table for the Student NIC. Figure 12 (Eweka, 2024) shows this action

**Figure 12**

*vWorkstation's updated ARP table.*



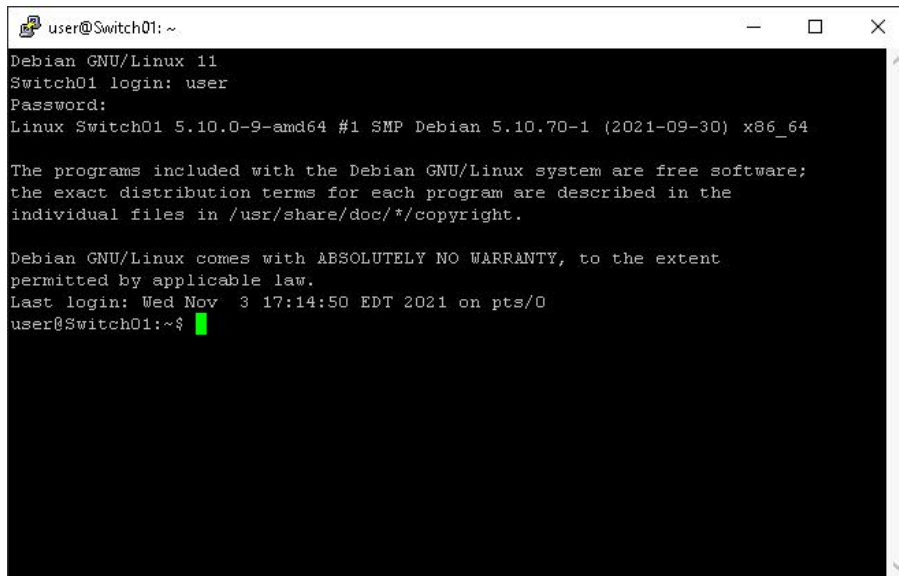
In the upcoming steps, participants are instructed to initiate a remote shell connection to the Switch01 device and scrutinize its networking configuration. To accomplish this, navigate to the vWorkstation desktop and double-click the PuTTY icon, opening the PuTTY configuration window. This step sets the stage for accessing and evaluating the networking parameters of the Switch01 device in the lab environment.

In the next steps, participants are instructed to open a remote shell connection to the Switch01 device by double-clicking the PuTTY icon on the workstation desktop. In the PuTTY configuration window, they should enter "172.30.0.3" as the Host Name and choose the Telnet

protocol. Upon being prompted, users should input the credentials –(Username: user, Password: password).

**Figure 13**

*Log in prompt*

A terminal window titled 'user@Switch01: ~' with standard window controls. The terminal output shows the login sequence for a user on a Debian GNU/Linux 11 system. The prompt 'Switch01 login: user' is followed by a password prompt. After authentication, the system displays the kernel version 'Linux Switch01 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86\_64', a disclaimer about the software being free, and the last login time 'Wed Nov 3 17:14:50 EDT 2021 on pts/0'. The prompt returns to 'user@Switch01:~\$' with a green cursor.

```
user@Switch01: ~  
Debian GNU/Linux 11  
Switch01 login: user  
Password:  
Linux Switch01 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Wed Nov 3 17:14:50 EDT 2021 on pts/0  
user@Switch01:~$
```

Press enter to authenticate the Telnet session. This process enables them to review the networking configuration of the Switch01 device. As shown in Figures 14,15 & 16 (Kim, 2021)

**Figure 14**

*Network interfaces on Switch01.*

```

user@Switch01:~$ sudo ifconfig
[sudo] password for user:
br0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.30.0.3 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fe80::250:56ff:feab:3534 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:ab:35:34 txqueuelen 1000 (Ethernet)
    RX packets 239 bytes 22510 (21.9 KiB)
    RX errors 0 dropped 45 overruns 0 frame 0
    TX packets 103 bytes 8796 (8.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::250:56ff:feab:3534 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:ab:35:34 txqueuelen 1000 (Ethernet)
    RX packets 751 bytes 112690 (110.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 627 bytes 113032 (110.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::250:56ff:feab:c707 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:ab:c7:07 txqueuelen 1000 (Ethernet)
    RX packets 1091 bytes 138431 (135.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 943 bytes 125240 (122.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens256: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::250:56ff:feab:ef9d prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:ab:ef:9d txqueuelen 1000 (Ethernet)
    RX packets 1237 bytes 200388 (195.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1814 bytes 252409 (246.4 KiB)
    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 5142 bytes 417034 (407.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5142 bytes 417034 (407.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

user@Switch01:~$

```

In the following steps, participants were prompted to utilize Open vSwitch for displaying interfaces in its configuration database. At the command prompt, they are instructed to type "sudo ovs-vsctl show" and press Enter. If prompted, participants should enter the password to authorize privilege escalation. you should see ens192, ens224, and ens256. In figure 14 (Kim, 2021).

**Figure 15***Open vSwitch configuration database*

```

user@Switch01:~$ sudo ovs-vsctl show
[sudo] password for user:
fca948bb-05a2-4b83-b264-38e926fb0ac1
    Bridge br0
        Port ens224
            Interface ens224
        Port ens256
            Interface ens256
        Port ens192
            Interface ens192
        Port br0
            Interface br0
                type: internal
    ovs_version: "2.15.0"
user@Switch01:~$

```

At the command prompt, type `sudo ovs-appctl fdb/show br0` and press Enter to display the Open vSwitch forwarding table. If prompted, type password to authorize your privilege escalation. Figure 16 (Kim, 2021) shows the result of this action

**Figure 16***Open vSwitch forwarding table*

```

user@Switch01:~$ sudo ovs-appctl fdb/show br0
port  VLAN  MAC                Age
  3      0  00:50:56:ab:8d:29   22
  1      0  00:50:56:ab:55:98    4
LOCAL    0  00:50:56:ab:1f:4d    4
  2      0  00:50:56:ab:99:fb    3
user@Switch01:~$

```

Much like the ARP table on the vWorkstation, the forwarding table is used to map Switch01's ports to the MAC addresses of the devices connected to them in Figure 17 (Eweka, 2024)

**Figure 17**

*Switch01 forwarding table.*

```

user@Switch01:~$ sudo ovs-vsctl show
TX errors 0 dropped 0 overruns 0 carrier 0
Bridge br0
  Port ens224
    Interface ens224
  Port ens256
    Interface ens256
  Port ens192
    Interface ens192
  Port br0
    Interface br0
    type: internal
  ovs_version: "2.15.0"
user@Switch01:~$ sudo ovs-appctl
ovs-appctl: at least one non-option argument is required (use --help for help)
user@Switch01:~$ sudo ovs-appctl fdb/show br0
port  VLAN  MAC           Age
1      0    00:50:56:ab:17:ff      2
LOCAL  0    00:50:56:ab:57:26      2
3      0    00:50:56:ab:e8:44      0
2      0    00:50:56:ab:51:13      0
user@Switch01:~$

```

Similar to the ARP table on the vWorkstation, the forwarding table on Switch01 serves the purpose of mapping its ports to the respective MAC addresses of the connected devices. This table provides essential information for efficiently directing network traffic, ensuring accurate and swift communication within the network infrastructure.

Next participants can conclude their exploration of the LAN by connecting to the file server and collecting fundamental information. They are instructed to repeat steps that yielded Figure 13 (Eweka 2024) using the following details from the (Jones & Bartlett, 2021) lab guide.

Host Name or IP address: 172.30.0.5

Connection Type: SSH

User: root

Password: password (Num. 16)

This process enables participants to establish a connection to the file server, facilitating the retrieval of essential data and enhancing their understanding of the network environment.

Upon logging in to the file server, participants may observe a banner identifying its operating system as FreeBSD. To proceed, they are directed to the command prompt, where they should type "pwd" and press Enter. This command displays the current directory, providing insights into the file server's file structure and aiding in the exploration of its operating environment. In the next steps, you will use several common Unix commands to gather more information about the file serve At the command prompt, type pwd and press Enter to display the current directory. Figure 18 (Kim, 2021).

### Figure 18

*Pwd output*

```
root@Fileserver01[~]# pwd
/root
root@Fileserver01[~]#
```

At the command prompt, type whoami and press Enter to display the current user account to confirm the current user. Next at the command prompt, type whoami and press Enter to display the current user account. The /mnt directory is commonly used as a mount point in

UNIX-like operating systems., At the command prompt, type `ls -l` and press Enter to list the contents of current directory. As shown below in figure 19 (Kim, 2021).

Figure 19

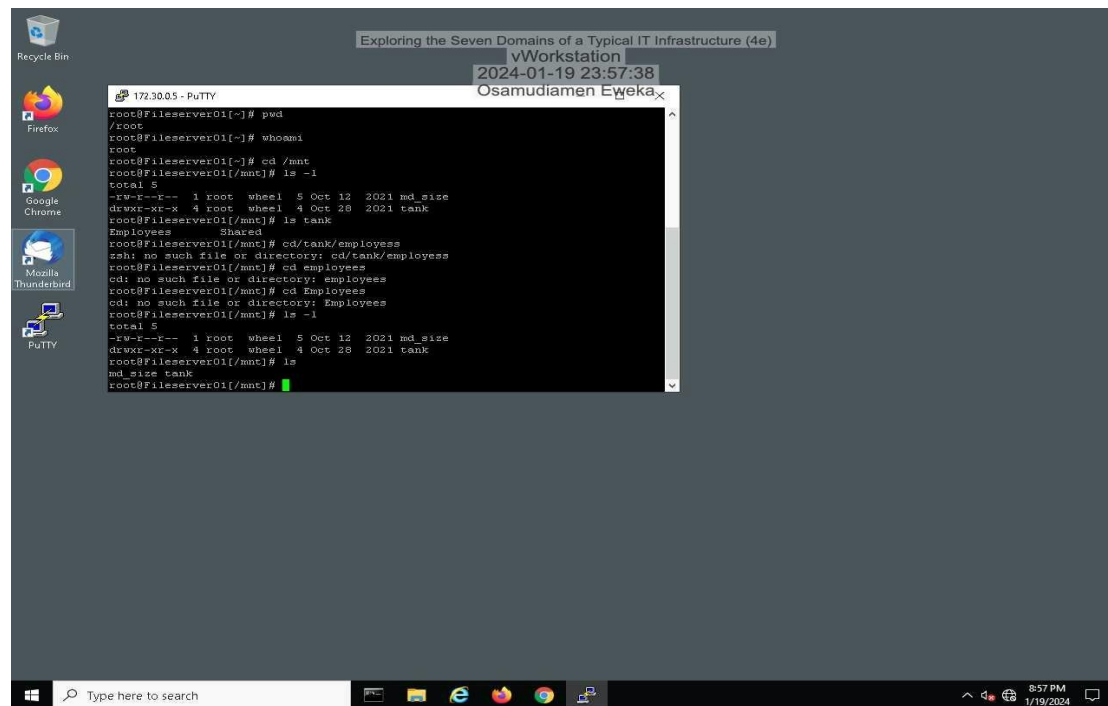
*Ls -l output.*

```
root@Fileserver01[/mnt]# ls -l
total 1
-rw-r--r--  1 root  wheel  5 Oct 12 10:19 md_size
drwxr-xr-x  4 root  wheel  4 Oct 28 09:10 tank
root@Fileserver01[/mnt]#
```

Participants are directed to input the command "`ls tank`" at the command prompt and press Enter. This action will list the contents of the "tank" directory. Participants are to switch to the specified directory using the command "`cd tank/Employees`". Subsequently, input "`ls`" at the command prompt to list the contents of the current directory, now set to "tank/Employees."

Figure 20

*Directory. contents of the Employees directory.*



## Section 1: Hands-On Demonstration

### Part 3

#### *Explore the LAN-to-WAN Domain*

In this lab section, participants are prompted to broaden their exploration of the network, with routing functions managed by the open-source pfSense firewall/router software distribution. The subsequent steps involve accessing the local pfSense firewall/router, which caters to the Secure Labs on Demand office, via the pfSense webGUI. During this exploration, participants will engage with key functionalities of the pfSense application, encompassing routing, Network Address Translation (NAT), and packet filtering.

To access the pfSense webGUI, participants are instructed to click the Firefox icon on the vWorkstation taskbar, opening a new browser window. In the Firefox navigation bar, they should type “http://172.30.0.1” and press Enter. This action establishes a connection to the webGUI for the pfSense-office device, facilitating exploration and interaction with its features. At the pfSense log-in screen, type the following credentials and press Enter to log in to the pfSense webGUI. (User: admin Password: pfsense) Participants are directed to review the NAT table for the pfSense-office appliance as the next step in their exploration. This involves examining and understanding the Network Address Translation (NAT) configurations, a crucial aspect of the pfSense firewall/router setup.

To access the NAT settings on pfSense, participants are instructed to follow these steps:

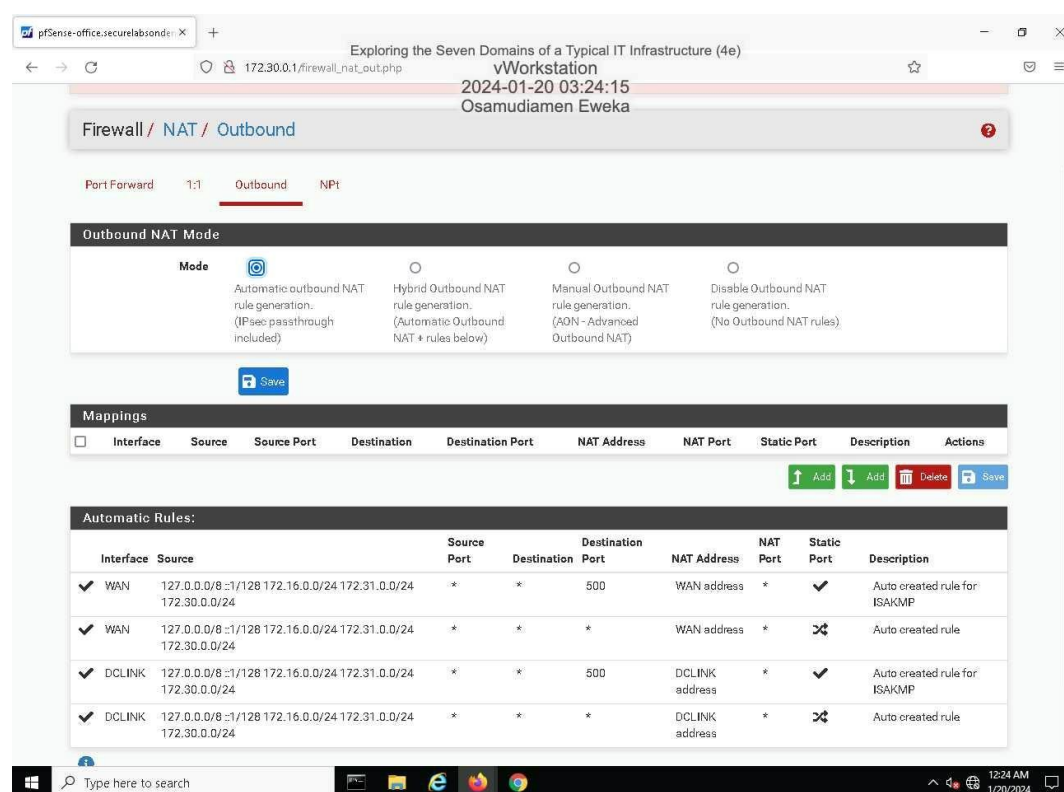
- On the pfSense menu bar, click the "Firewall" menu.
- From the dropdown menu, select "NAT" to open the NAT settings.
- Within the NAT settings, click the "Outbound" tab to access the Outbound NAT configurations.



These steps guide participants through the navigation within the pfSense interface to review and potentially modify the Outbound NAT settings shown in Figure 21 (Eweka, 2024).

**Figure 21**

*Outbound NAT settings.*

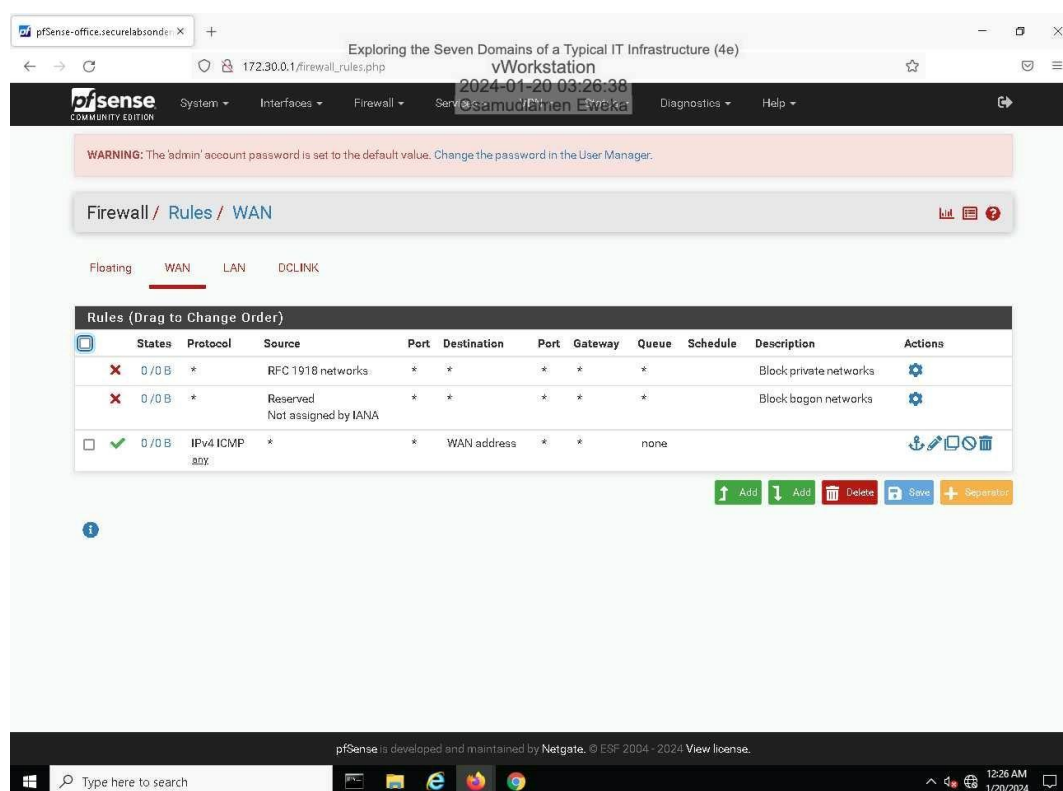


Upon accessing the pfSense Firewall Rules page, participants will be directed to the default view, which is the WAN Rules table. This table governs traffic on the WAN interface, with the initial rule automatically generated by pfSense. This rule is designed to block any traffic originating from a source IP address reserved exclusively for private (internal) networks, as defined by the IETF and IANA in RFC 1918. This precautionary measure helps identify potential IP spoofing attacks.

For a detailed view of the rules governing the LAN interface, participants are instructed to click on the "LAN" tab on the WAN Rules page. This action will display the rules table specifically tailored for the LAN interface, providing insights into the configured security measures for local network traffic. Figure 22 (Eweka, 2024)

**Figure 22**

*Permissive LAN rules.*



For the upcoming steps, participants are guided to explore the Routing configuration on pfSense by following these instructions:

- On the pfSense menu bar, click the "System" menu.
- From the dropdown menu, select "Routing" to open the Routing page.

- Upon accessing the Routing configuration, the default landing page is the "Gateways" tab. Participants are then directed to click on the "Static Routes" tab to open the Static Routes page.

**Figure 23**

*Static routes page*

System / Routing / Static Routes

Gateways

Static Routes

Gateway Groups

Static Routes

	Network	Gateway	Interface
✓	172.16.0.0/24	DC - 10.0.0.2	DCLINK
✓	172.31.0.0/24	DC - 10.0.0.2	DCLINK

This sequence of actions leads participants through the navigation within the pfSense interface, facilitating the exploration of routing configurations with a specific focus on the Static Routes settings. As seen above in Figure 23 (Kim, 2021).

On the Static Routes page of pfSense, participants will observe specific entries outlining routing configurations:

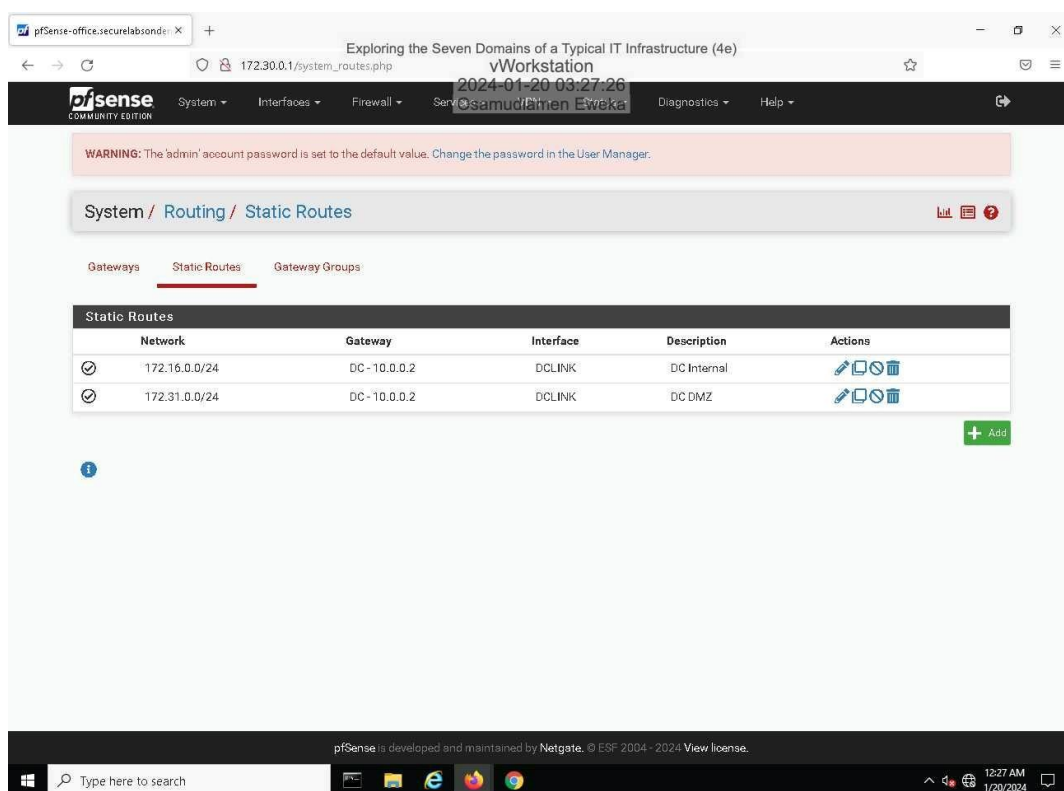
- The first entry designates that all traffic destined for the 172.16.0.x network (representing the private LAN at the data center) should pass through the DC 10.0.0.2 gateway.

- The second entry dictates that all traffic directed to the 172.31.0.x network (representing the Demilitarized Zone, another network segment at the data center) should also pass through the DC 10.0.0.2 gateway.

Without additional static routes specified, any other outbound traffic will automatically be routed to the default gateway. In this scenario, the default gateway is configured to connect to the WAN, facilitating connectivity to the simulated public Internet. As illustrated in Figure 24 below (Eweka,2024)

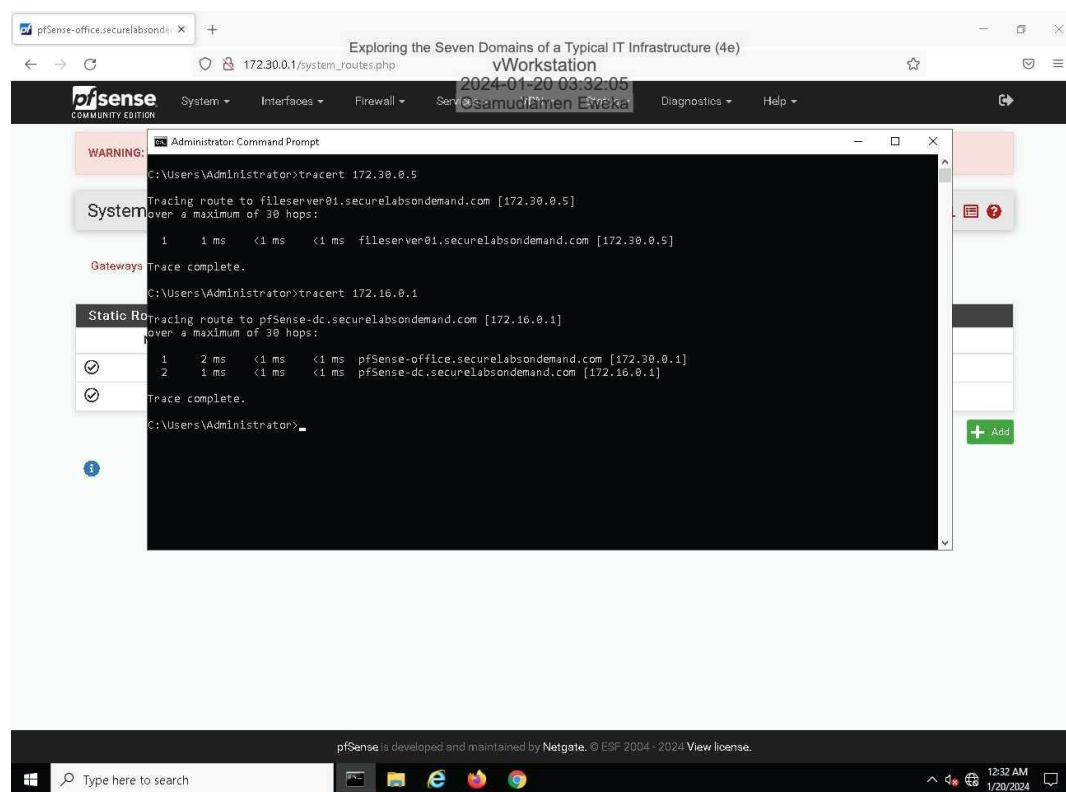
**Figure 24**

*Full view of Static Routes page.*



**Figure 25**

*Tracert to the pfSense-dc appliance.*



To demonstrate the routing functions facilitated by the pfSense firewall/router, participants are instructed to run traceroutes to both a local host on the LAN side and a remote host on the WAN side. Here are the steps:

- On the vWorkstation taskbar, click the "Command Prompt" icon to open a new Command Prompt window.
- At the command prompt, type "tracert 172.30.0.5" and press Enter to trace the path to FileServer01.
  - The expected output should indicate a path with only one hop, as Switch01, connecting vWorkstation and FileServer01, is not counted due to its Layer 2 nature.

- Next, at the command prompt, type "tracert 172.16.0.1" and press Enter to trace the path to the pfSense firewall in the remote data center.

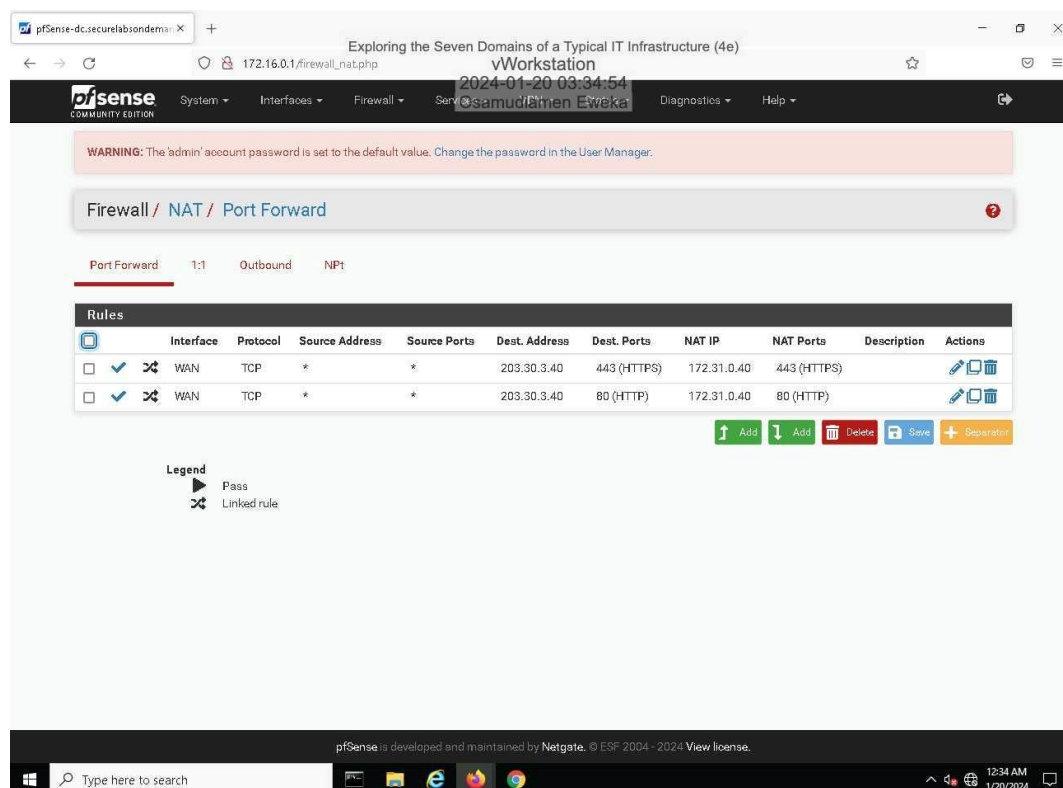
These traceroutes provide insights into the routing capabilities of the pfSense firewall/router in Figure 25 above (Eweka, 2024), showcasing the efficient routing of traffic to both local and remote destinations. Participants can anticipate slightly more intricate results from the traceroute in this specific scenario. Upon running "tracert 172.16.0.1" to trace the path to the pfSense firewall in the remote data center, the output should reveal two hops. The first hop corresponds to the pfsense-office device, and the second hop corresponds to the pfsense-dc device. This outcome illustrates the routing journey through both pfSense devices in the network infrastructure.

In this section, participants are prompted to inspect the pfSense dashboard's interfaces table, revealing four interfaces: LAN, WAN, OFFICELINK, and DMZ. The DMZ serves as a segregated network for public-facing resources like WebServer01. The subsequent steps involve reviewing NAT configuration and firewall rules for WebServer01:

- Navigate to "Firewall" and select "Virtual IPs" to access the Virtual IPs page.
- Then, go to "Firewall," select "NAT," and open the NAT Port Forwarding page.
- Two rules redirect traffic to the 203.30.3.40 VIP on ports 443 and 80 to the private IP 172.31.0.40 on the corresponding ports as seen in Figure 26 (Eweka, 2024)

## Figure 26

*Port Forward rules for the web server.*



In the evaluation of firewall rules about WebServer01 access, participants are directed to the WAN Rules page, where they should click the "DMZ" tab to inspect the rules for the DMZ interface. Within the DMZ rules table, the significance lies in the second rule, serving as a paramount security measure by expressly blocking all traffic directed to the LAN interface. This rule plays a crucial role in preventing direct communication between the DMZ and LAN interfaces, thereby enhancing the overall security posture, and safeguarding the internal network from potential threats shown in figure 27 (Eweka,2024).

**Figure 27**

*DMZ firewall rules.*

Exploring the Seven Domains of a Typical IT Infrastructure (4e)

172.16.0.1/firewall\_rules.php?if=opt1

2024-01-20 03:35:33

Osamudiamen Eweka













2024-01-20 03:35:33






WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / DMZ

Floating WAN LAN **DMZ** OFFICELINK OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 6 / 41 KIB	IPv4 *	*	*	*	*	*	none		Open Mail Relay	   
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 *	*	*	LAN net	*	*	none			   
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 ICMP	DMZ net	*	DMZ address	*	*	none			   

 Add  Add  Delete  Save  Separator

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

Type here to search

12:35 AM 1/20/2024



## Section 2: Applied Learning

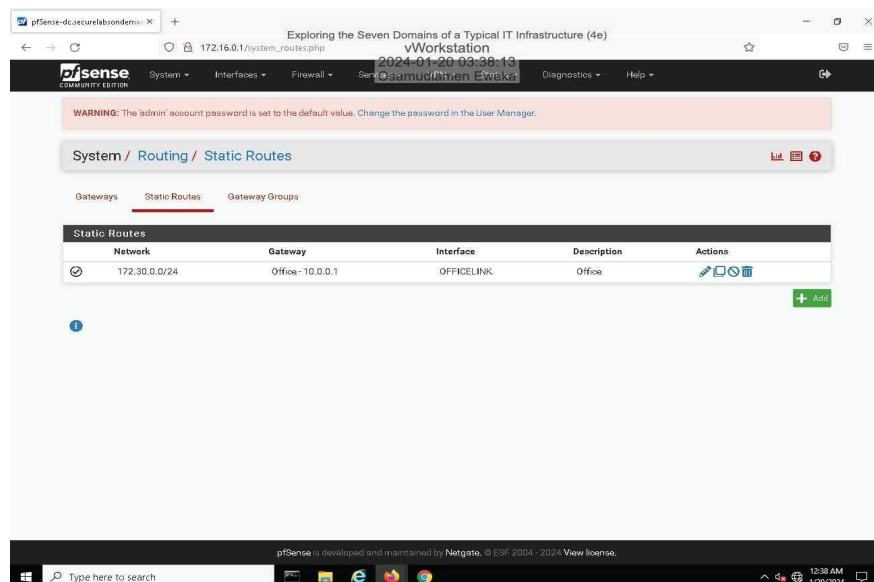
### Part 1:

#### *Explore the WAN Domain*

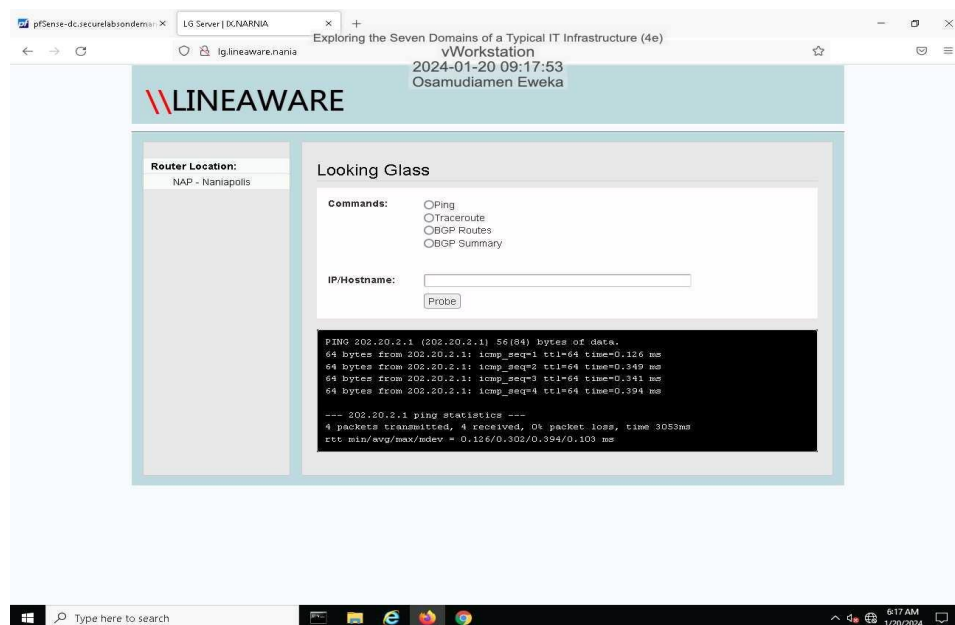
In this lab segment, the exploration focuses on the WAN Domain, extending over the WAN interfaces on an organization's routers and covering a broad geographical area. The term WAN, denoting a Wide Area Network, encompasses networks with extensive geographic reach. Building on the previous section utilizing the pfSense WebGUI for LAN-to-WAN functions, participants are directed to return to the pfSense WebGUI for further examination. Specifically, they will scrutinize routes between Secure Labs on Demand's remote sites and their connection to the simulated public Internet. The steps involve opening the Firefox application from the vWorkstation taskbar, navigating to <http://172.16.0.1>, and logging in with the provided credentials (Username: admin, Password: pfsense). Within the pfSense WebGUI, participants should then access System > Routing to view the Gateways list and navigate to the Static Routes tab to review the static routing table. Notably, a single static route is defined, stipulating that all traffic destined for the 172.30.0.0/24 network should be forwarded to the OFFICELINK upstream gateway. For all other traffic, pfSense will use the default gateway defined on the Gateways page, which in this case is the WANGW gateway. The performed action is expected to mirror the configuration illustrated in Figure 28, as depicted in the reference source (Eweka, 2024).

**Figure 28**

*Static route for the point-to-point connection.*

**Figure 29**

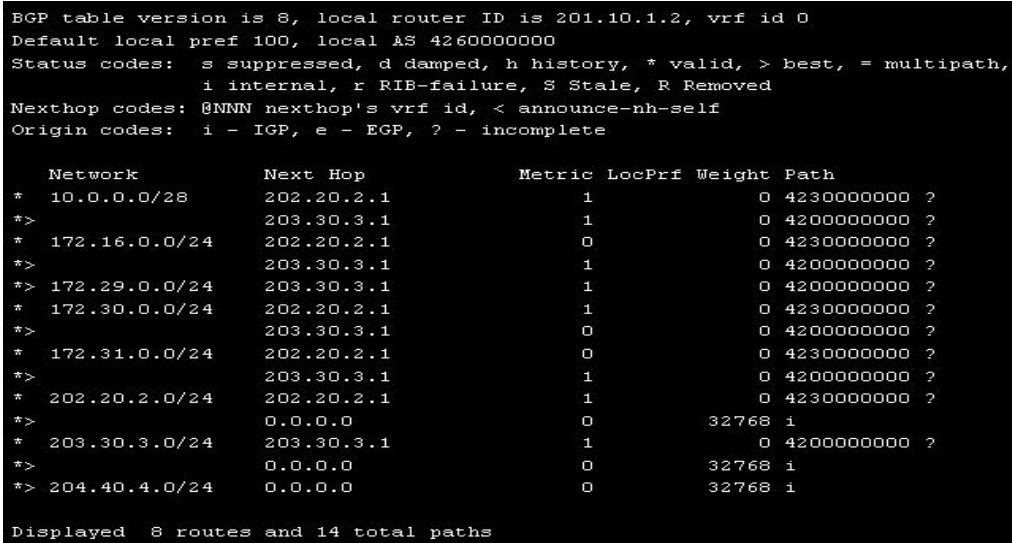
*Make a screen capture showing the BPG neighbor ping results.*



As displayed in Figure 29 (Eweka, 2024), individuals will have the opportunity to explore a Looking Glass server, a tool commonly maintained by Internet Service Providers (ISPs) or Network Service Providers (NSPs). This server allows public users to access high-level routing information. By navigating to <http://lg.lineaware.nania> through the Firefox address bar, users will engage with the Looking Glass server within this simulated ISP environment. The interface presents four command options: Ping, Traceroute, BGP Summary, and BGP Route. Opting for the BGP Summary, users can click the Probe button to reveal a summary output, providing insights into messages sent and received (MsgRcvd and MsgSent). The non-zero values in these columns indicate the operational status. Subsequently, users will employ the Ping command to test connectivity with one of the BGP neighbors displayed in the summary. These steps promise an enlightening exploration into the intricate world of network infrastructure, offering a hands-on experience in understanding and verifying routing functionalities. Figure 30 (Kim, 2021) runs the Run the BGP Routes command.

**Figure 30**

### *BGP Routes*



```

BGP table version is 8, local router ID is 201.10.1.2, vrf id 0
Default local pref 100, local AS 4260000000
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete

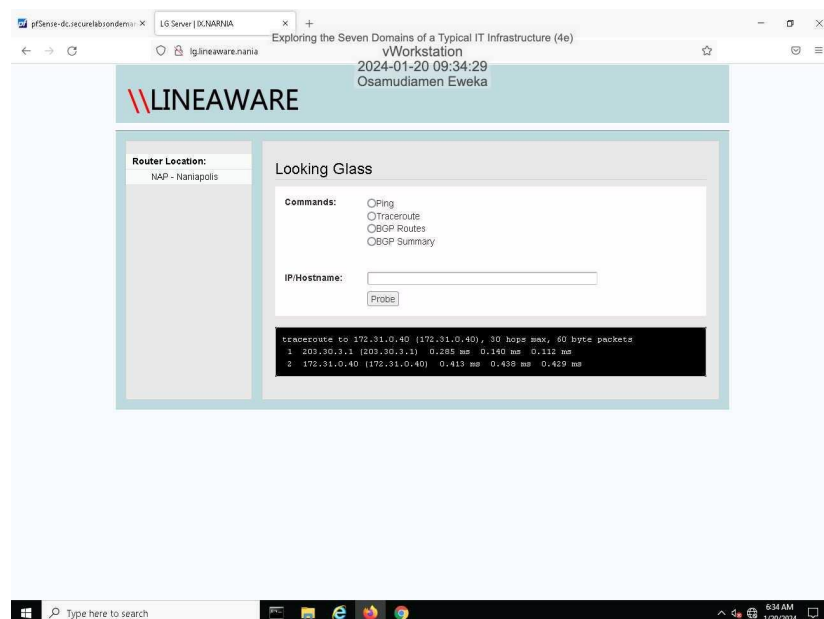
   Network        Next Hop        Metric LocPrf Weight Path
* 10.0.0.0/28     202.20.2.1         1           0 4230000000 ?
*>                203.30.3.1         1           0 4200000000 ?
* 172.16.0.0/24   202.20.2.1         0           0 4230000000 ?
*>                203.30.3.1         1           0 4200000000 ?
*> 172.29.0.0/24   203.30.3.1         1           0 4200000000 ?
* 172.30.0.0/24   202.20.2.1         1           0 4230000000 ?
*>                203.30.3.1         0           0 4200000000 ?
* 172.31.0.0/24   202.20.2.1         0           0 4230000000 ?
*>                203.30.3.1         1           0 4200000000 ?
* 202.20.2.0/24   202.20.2.1         1           0 4230000000 ?
*>                0.0.0.0            0          32768 i
* 203.30.3.0/24   203.30.3.1         1           0 4200000000 ?
*>                0.0.0.0            0          32768 i
*> 204.40.4.0/24   0.0.0.0            0          32768 i

```

table. Displayed 8 routes and 14 total paths

**Figure 31**

*Screen capture of Traceroute to the file server.*



In the ensuing steps in Figure 31 (Eweka, 2024), individuals will verify the current path to the WebServer01 machine (172.31.0.40) within the pfSense-dc DMZ, ensuring alignment with the identified best route in the BGP routing table. By selecting the Traceroute radio button, entering 172.31.0.40 in the IP/Hostname field, and clicking the Probe button, users initiate a traceroute to WebServer01. The ensuing results are expected to confirm that the initial hop to the WebServer01 host corresponds to the same IP address recognized as the optimal route within the BGP routing table. This exercise adds a practical dimension to understanding network routing, illustrating the correlation between the identified best route and the actual traversal path to the designated server.

## Section 2: Applied Learning

### Part 2:

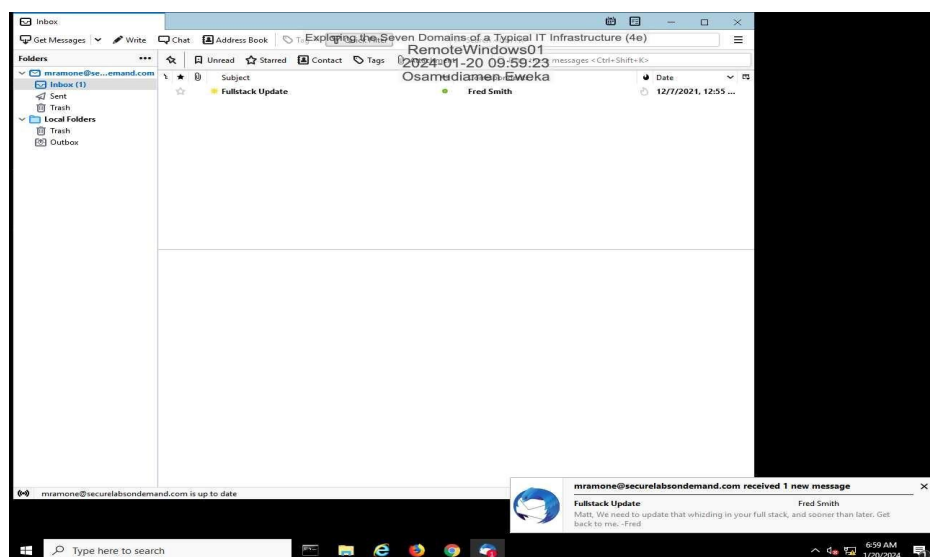
#### *Explore the Remote Access Domain*

In the process the lab focused on setting up and testing various aspects of the IT infrastructure. This included activities such as connecting to the RemoteWindows01 system, using OpenVPN to establish a secure connection to the private company network, and verifying access to the company's internal mail server.

Specifically, the steps involved signing in to the RemoteWindows01 system using the provided credentials, encountering an error message when attempting to connect to the email server using the Thunderbird application, launching the OpenVPN application to establish a secure tunnel to the company's network, logging in to OpenVPN, and then successfully connecting to the email server using Thunderbird. Figure 31 shows the successful connection to the email server.

### Figure 32

*Screen capture of a Successful connection to the email server.*



Throughout this process, the lab demonstrated the importance of secure remote access, the use of VPNs to establish encrypted connections, and the verification of successful access to internal resources such as the email server. These activities are essential for ensuring that remote employees, such as the fictional developer Matt Ramone, can securely access company resources while working from a remote location.

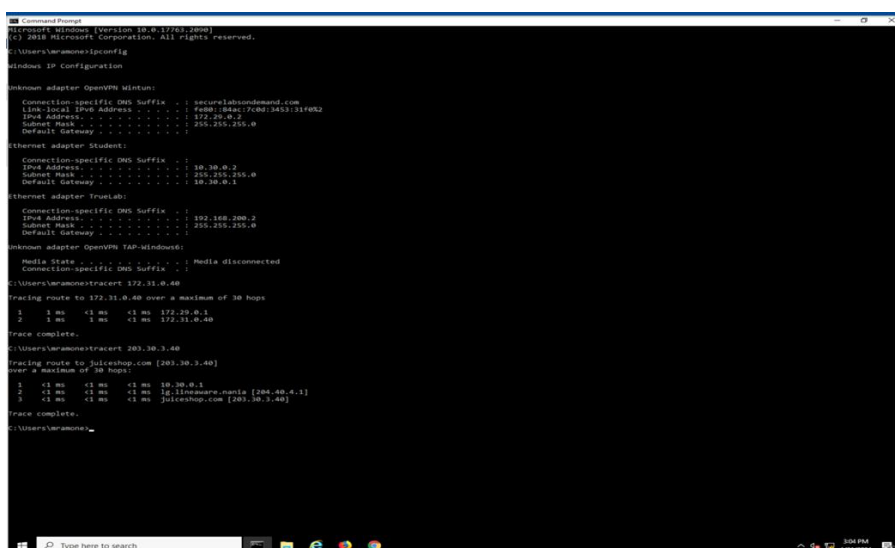
### Question

- **Document** whether the VPN connection is a split tunnel or full tunnel, based on the tracert results.

### Answer/Observations

#### Figure 33

*Execute tracert 172.31.0.40 & execute tracert 172.31.0.40 in cmd*



```

Microsoft Windows [Version 10.0.17134.220]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ramone>ipconfig

Windows IP Configuration

Ethernet adapter OpenVPN Minton:

    Connection-specific DNS Suffix  : .securelabsdemand.com
    Link-local IPv6 Address . . . . . : fe80::b6a7:7c9d:3453:31f0%2
    IPv4 Address. . . . . : 172.29.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.29.0.1

Ethernet adapter Student:

    Connection-specific DNS Suffix  : .
    IPv4 Address. . . . . : 10.30.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.30.0.1

Ethernet adapter TrueLab:

    Connection-specific DNS Suffix  : .
    IPv4 Address. . . . . : 192.168.200.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Bluetooth adapter OpenVPN TAP-windows8:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  : .

C:\Users\ramone>tracert 172.31.0.40

Tracing route to 172.31.0.40 over a maximum of 30 hops:
  0  1 ms  <1 ms  <1 ms  172.29.0.1
  1  1 ms  1 ms  1 ms  172.31.0.40
Trace complete.

C:\Users\ramone>tracert 203.30.3.40

Tracing route to juiceshop.com [203.30.3.40]
over a maximum of 30 hops:
  0  <1 ms  <1 ms  <1 ms  10.30.0.1
  1  <1 ms  <1 ms  <1 ms  10.30.0.2
  2  <1 ms  <1 ms  <1 ms  192.168.200.2
  3  <1 ms  <1 ms  <1 ms  203.30.3.40
Trace complete.

C:\Users\ramone>

```

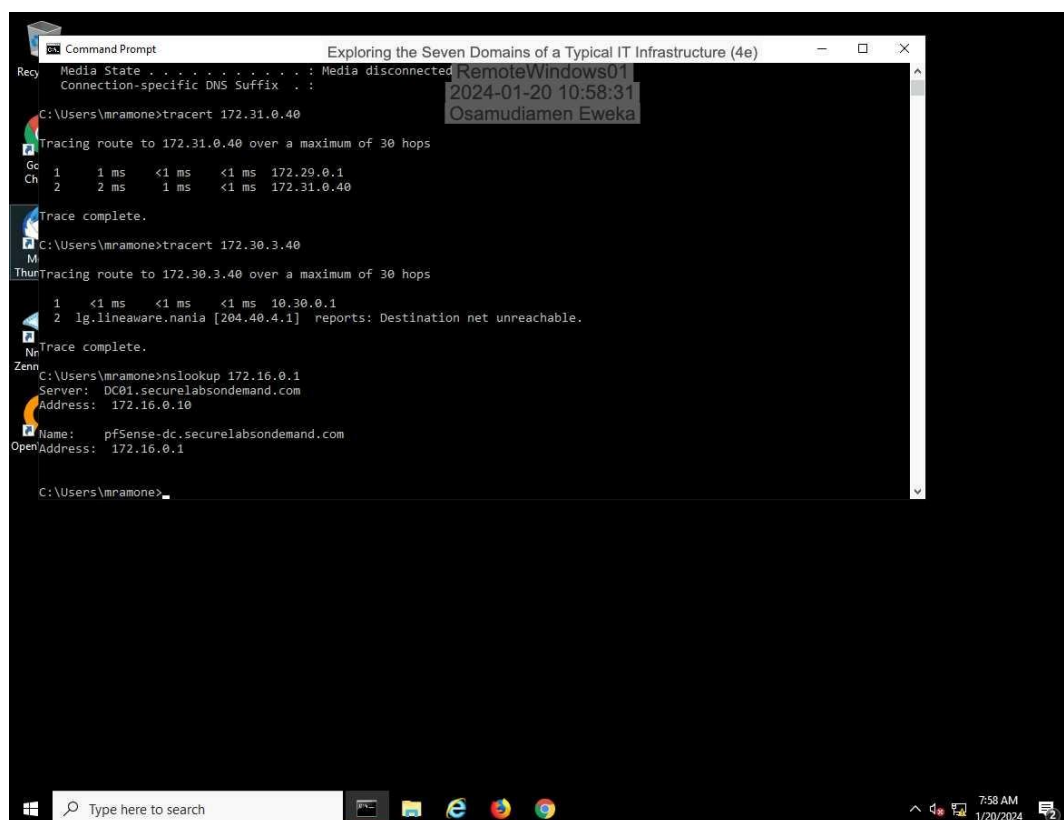
Image reference (Eweka,2024), screenshot of this procedure to answer the question above.

## Summary:

- The VPN connection appears to be a split tunnel configuration.
- Split tunneling means that only specific traffic is routed through the VPN, while other traffic goes directly to the internet.
- In this case, traffic to the internal network (172.31.0.40) goes through the VPN tunnel, while internet-bound traffic (juiceshop.com) takes a direct route without passing through the VPN.

**Figure 34**

*Screen shot of the Successful reverse DNS lookup for the internal host.*



In the final step of this lab segment, participants confirmed the successful propagation of the internal DNS server to a remote host by conducting a reverse DNS lookup. This involved executing the command "nslookup 172.16.0.1" at the command prompt. The expected outcome was a successful reverse DNS lookup for 172.16.0.1, affirming that RemoteWindows01 had successfully accessed the DNS server for the Secure Labs on Demand network. Any failure in this lookup would indicate an inability to locate the private network host at the specified IP address.

Additionally, the process involved tracing the path to the FileServer01 device and the pfSense firewall located in the remote data center. The tracert command was used to determine the number of hops required to reach these devices. The results revealed that the path to the FileServer01 device took only one hop, indicating a direct connection without the need for additional routing through other devices. However, the tracert to the pfSense firewall located in the remote data center showed two hops: one for the pfsense-office device and one for the pfsense-dc device. This indicated the path the network traffic took to reach the remote data center, Shown in Figure 34 above (Eweka, 2024).



## Section 2: Applied Learning

### Part 3:

#### *Explore the System/Application Domain*

In the process from section 2 part 3 Explore the System/Application Domain number 1 to 4, the user would have explored the critical systems and applications that support and provide various services for the organization. This would have included examining several key systems such as a domain controller, web server, and file server. The user would have navigated through the Windows operating system to access the Command Prompt, execute commands such as `whoami` to display information about the current user account, and change the working directory to gather more information about the file server.

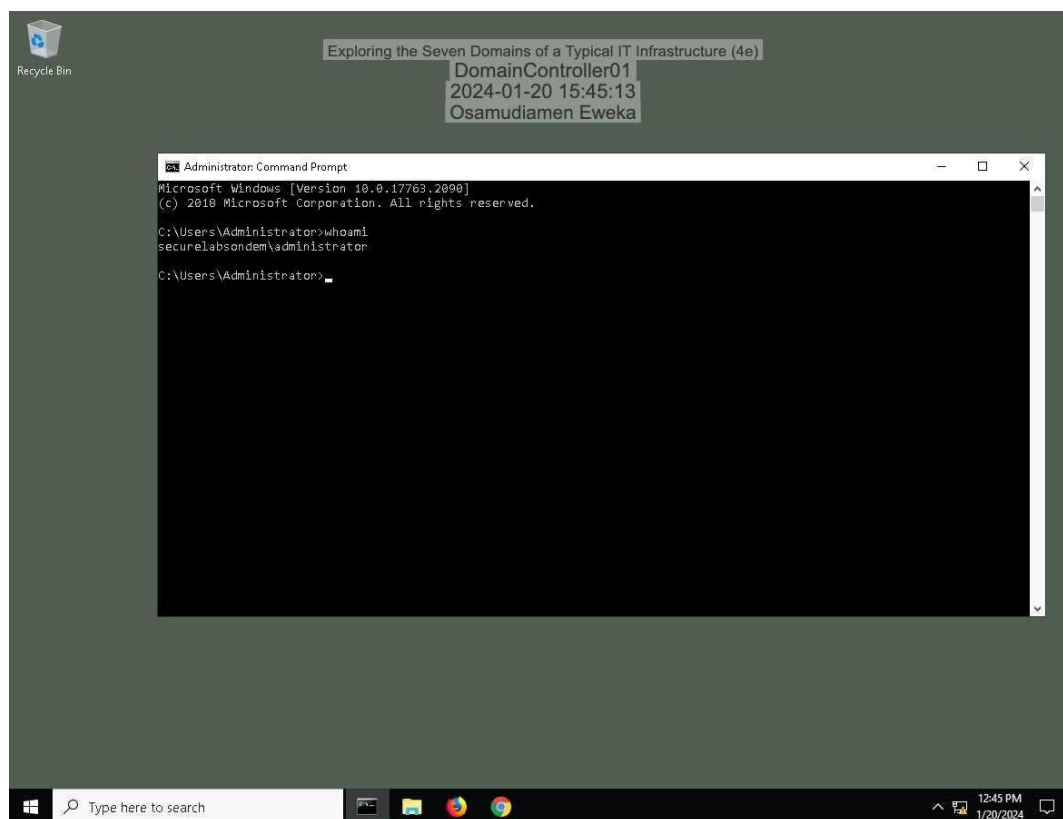
The user would have also used common Unix commands to gather information about the file server, such as displaying the current directory with the `pwd` command, listing the contents of the current directory with the `ls -l` command, and confirming the current user with the `whoami` command.

To fulfill the requirement of making a screen capture showing the `whoami` results, the user would have captured the output of the `whoami` command, which displays the current user account information in the Command Prompt window, this screen capture is illustrated below in Figure 35 (Eweka, 2024).

Overall, this process would have involved navigating through the systems and using command-line utilities to gather relevant system information in the System/Application Domain.

**Figure 35**

*Make a screen capture showing thewhoami results.*



In the process from section 2 part 3 Explore the System/Application Domain, the following steps were completed (Kim & Solomon, 2021).:

6. On the Windows Update page, the View Policies link was clicked to open the View configured update policies page.
7. The View configured update policies page displayed a list of update policies that have been set on Alice Dodson's account.
8. The Members tab of the Developers group in the Active Directory Users and Groups console was opened to review the list of users within this group.

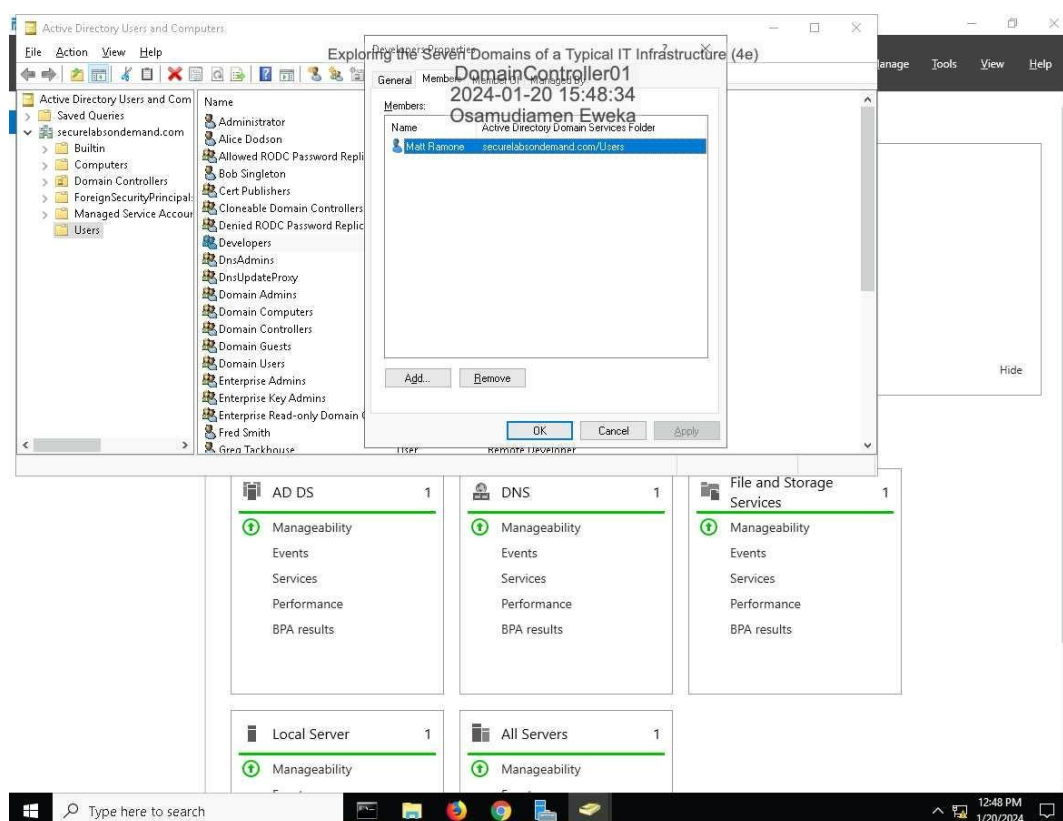
9. Within the Users folder, the Developers group was double-clicked to open the Developers Properties dialog box, then the Members tab was clicked to review the list of users within this group.

10. A screen capture was made showing the members of the Developers AD group. As shown in Figure 36 (Eweka, 2024)

During these steps, the security policies and group memberships for the Developers group were reviewed in the Active Directory Users and Computers tool, which is part of the Active Directory Domain Services role. The review of these settings is important for managing access control and ensuring proper security measures within the System/Application Domain.

**Figure 36**

*Make a screen capture showing the members of the Developers AD group.*

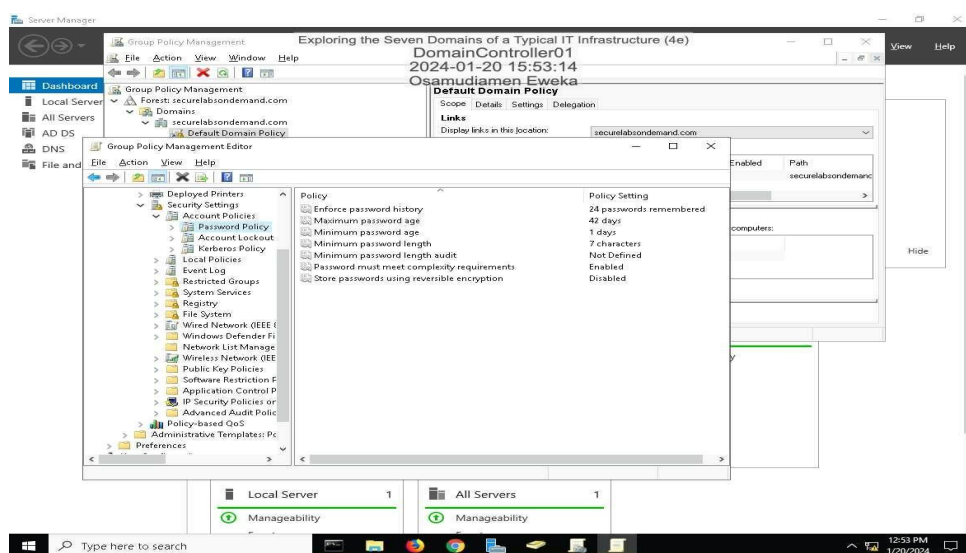


Next in the process, the user navigated to the Group Policy Management Console and accessed the password policy settings. They opened the Group Policy Management Editor and navigated to Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy. From there, they were able to define different aspects of the default password policy for the Secure Labs on Demand domain, including minimum password length, minimum password age, and password complexity.

After making the necessary configurations, they closed the Group Policy Management Editor and Console. Finally, they made a screen capture showing the password policy settings in the Group Policy Management Console illustrated in Figure 37 (Eweka, 2024), to document the changes and ensure that the password policy was correctly configured according to the organization's security requirements.

**Figure 37**

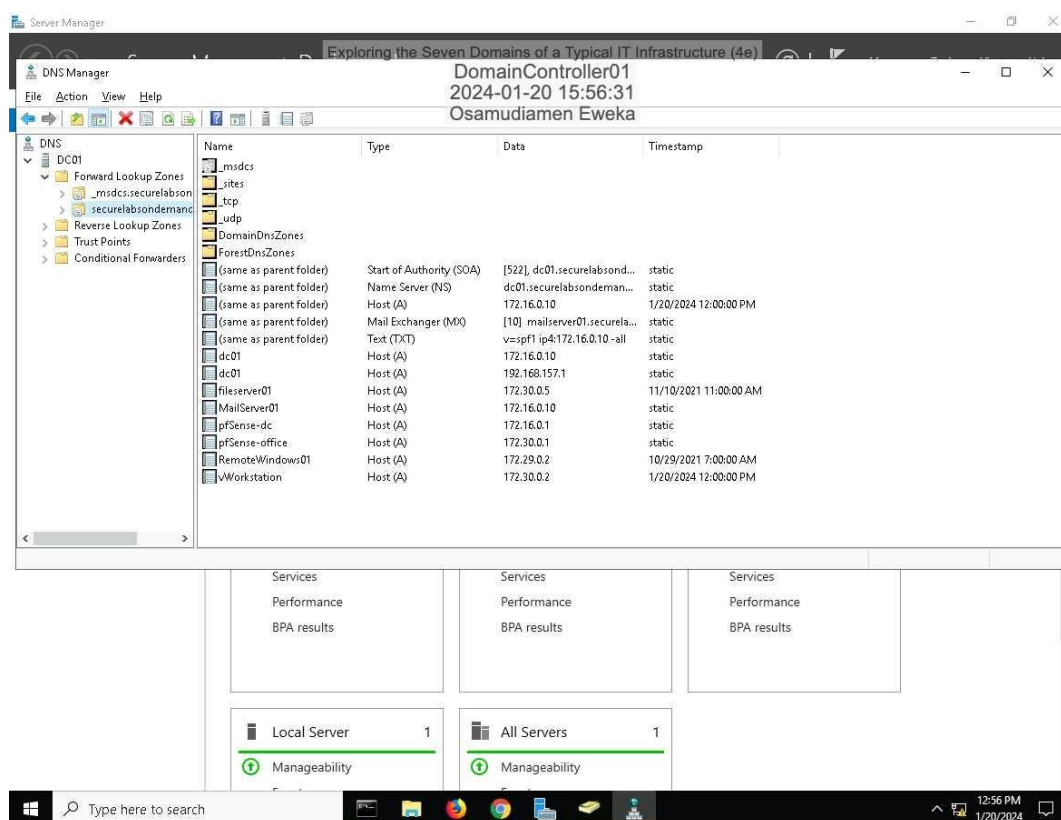
*Make a screen capture showing the password policy settings in the Group Policy Management Console.*



Subsequently, in the next step, we made a screen capture showing the DNS entries shown in Figure 38 (Eweka 2024), which displayed the DNS records associated with a specific web address “securelabsondemand.com” within the domain. This information is crucial for understanding the network infrastructure and ensuring proper connectivity and data management within the System/Application Domain.

**Figure 38**

*Make a screen capture showing the DNS entries.*



In this next process, the user accessed the Linux computer running the web server by navigating to the lab view toolbar and selecting vWorkstation from the Virtual Machine menu, and using PuTTY. When prompted, log in using this credentials: (User: user, Password: password). They then executed the command "sudo netstat -tulpn" to view open connections on

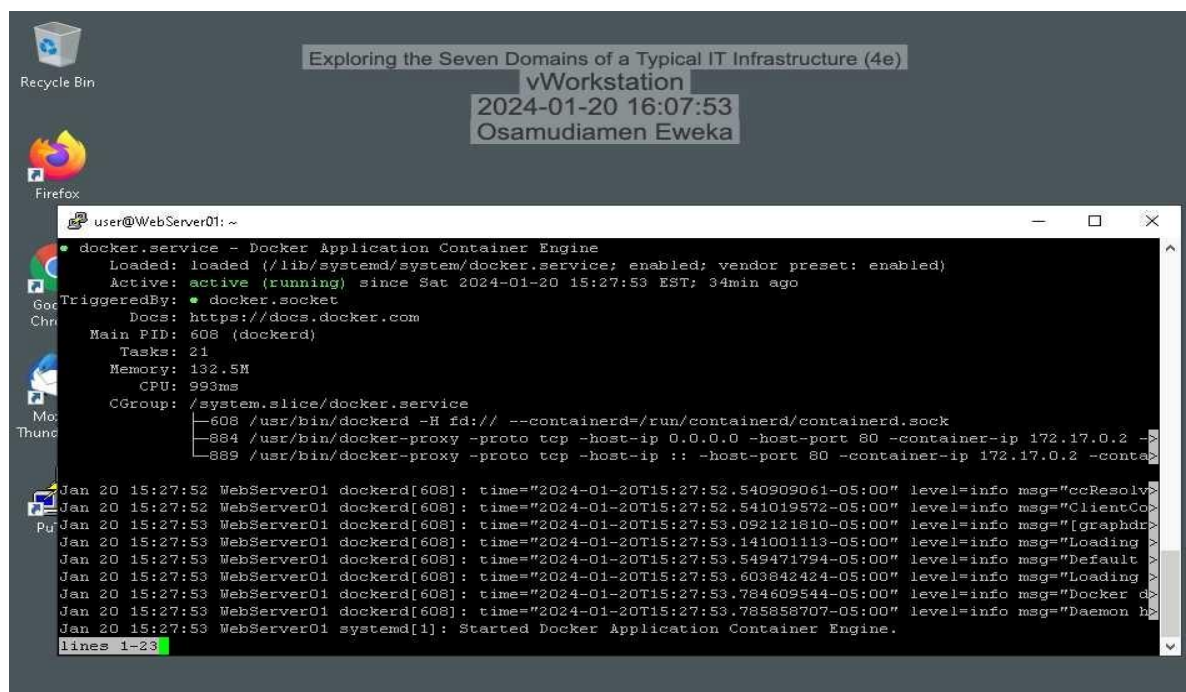
the WebServer01 system. This command displayed various statistics about the computer's network status, including ports that are listening for connections, established connections, and the services associated with those connections. The output of the command showed a service titled "docker-proxy" running on port 80, indicating that the web server software is actually running on a Docker container atop the WebServer01 Linux system. The addition of the word "proxy" suggested that connections were being redirected to another container, perhaps on a different port.

After that, the user executed the command "sudo service docker status" to check the status of the Docker container. The output showed that port 80 on the host was being redirected to IP address 172.17.0.2 and port 3000 on the container, indicating a typical configuration for a container running on a host system, wherein the host and container both have their own set of TCP ports, which requires a mapping to ensure traffic flows from one to the other.

Finally, in Figure 39 below the user made a screen capture showing the Docker service status to document the status of the Docker container (Eweka,2024).

**Figure 39**

*Make a screen capture showing the Docker service status.*

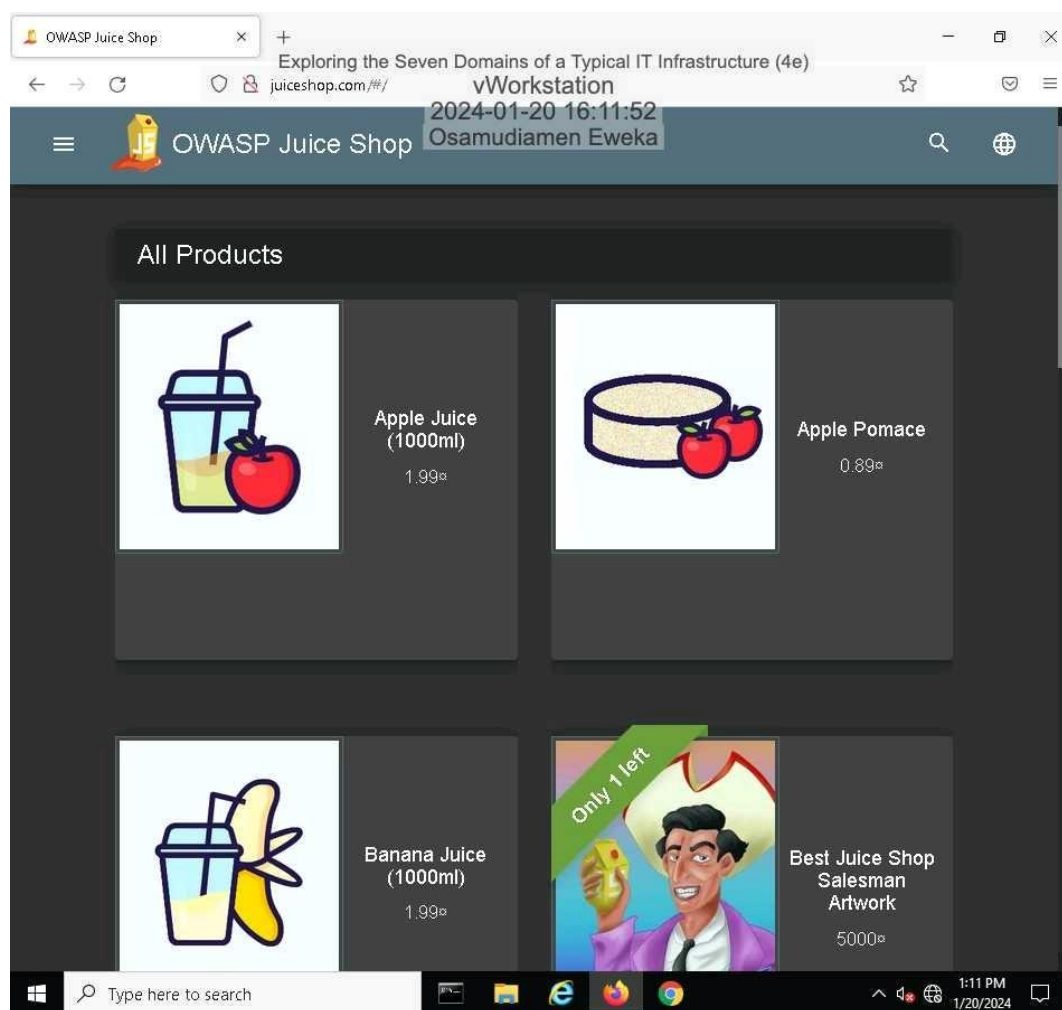


Next In section 2, part three of Explore the System/Application Domain, the user was instructed to open the Firefox browser on the vWorkstation and navigate to [juiceshop.com](https://juiceshop.com) to access the website being hosted on the web server. The Juice Shop is an open-source web application developed by the Open Web Application Security Project (OWASP) to demonstrate common web application vulnerabilities, OWASP Juice Shop is probably the most modern and sophisticated insecure web application! It can be used in security training, awareness demos, CTFs and as a guinea pig for security tools! Juice Shop encompasses vulnerabilities from the entire OWASP Top Ten (OWASP, 2021), along with many other security flaws found in real-world applications! (OWASP, n.d.). The user was then asked to make a screen capture showing the [juiceshop.com](https://juiceshop.com) web page as seen in Figure 40 below (Eweka, 2024).

The user successfully accessed the juiceshop.com website and captured a screenshot of the web page, which would have included the content and layout of the Juice Shop application as hosted on the web server. This exercise aimed to provide hands-on experience in interacting with a web application and understanding common web application vulnerabilities, as well as the importance of securing web servers and applications.

**Figure 40**

*Make a screen capture showing the juiceshop.com web page.*





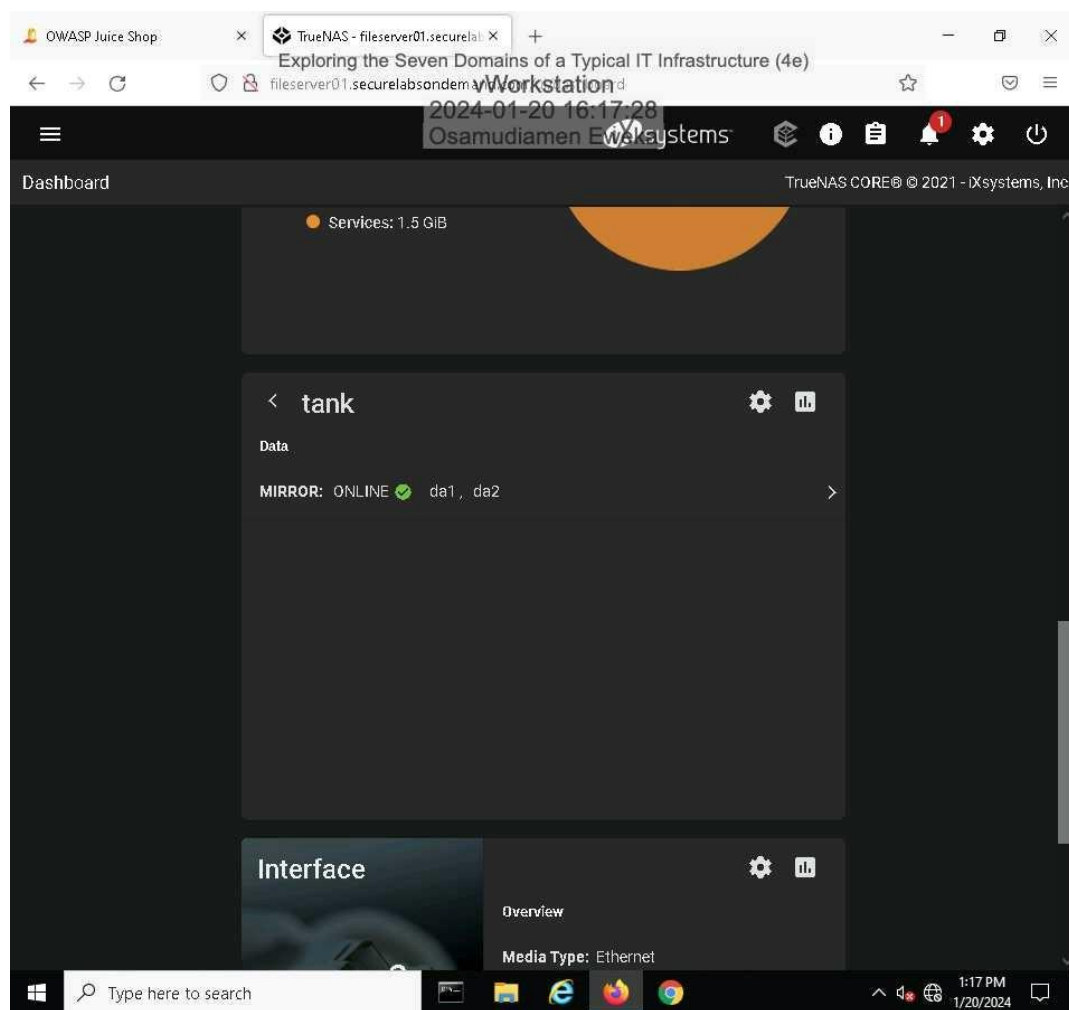
Next, the participant/user accessed the file server's web GUI using the Firefox address bar and logged in with the provided credentials. They were greeted by the TrueNAS dashboard, which displayed important details about the NAS configuration and its status. Within the Pool tile, they saw two data disks associated with the Tank pool, which is a virtual device (or vdev).

After logging in, they closed the Get Started dialog box and clicked on the Data row in the Pool/tank tile to display the disks in the tank volume. They made a screen capture showing the disks in the tank volume, which revealed that the two disks (da1 and da2) were organized in a mirrored configuration to ensure redundancy in case one disk fails. This configuration is important for data security and supports a comprehensive data security strategy by offering redundancy, backup management, generating alerts for unusual behavior, and scanning content for malicious code.

The user also learned that NAS systems like this one can play an important role in supporting data security strategy. They can enable redundancy, and backup management, generate alerts for unusual behavior, and scan content for malicious code. The screen capture they made shows in Figure 41 (Eweka, 2024), the disks in the tank volume, confirming the mirrored configuration for redundancy.

**Figure 41**

*Make a screen capture showing the disks in the tank volume.*



### Section 3: Challenge and Analysis

#### Part 1:

##### *Explore the User Domain*

**Question:** Based on your research, **identify** at least **two compelling threats** to the User Domain and **two effective security controls** used to protect it. Be sure to cite your sources.

**Answer ONE Research on threats to the User Domain:** The User Domain is often considered the weakest link in an organization's security chain. This is because it involves human users who can be unpredictable and make mistakes. Two significant threats to the User Domain include phishing attacks and insider threats. Phishing attacks are when attackers trick users into revealing sensitive information, such as passwords or credit card numbers, by pretending to be a trustworthy entity. Insider threats are risks posed by individuals within the organization, such as employees or contractors, who have access to sensitive information and systems (Eldardiry et al., 2013). These individuals may intentionally or unintentionally cause harm to the organization.

**Answer TWO Research on security controls for the User Domain:** Several security controls can be implemented to protect the User Domain. Two effective controls include user awareness training and access controls. User awareness training involves educating users about the risks and threats they face and how to avoid them. This can significantly reduce the risk of phishing attacks and other user-related threats. Access controls involve limiting the access users have to sensitive information and systems (What Are Security Controls? | IBM, n.d.). This can help prevent insider threats by ensuring that users only have access to the information and systems they need to perform their jobs.

**Summary:** The two compelling threats to the User Domain are phishing attacks and insider threats. The two effective security controls used to protect the User Domain are user awareness training and access controls.

### Section 3: Challenge and Analysis

#### Part 2:

##### *Research Additional Security Controls*

Based on your research, **identify** security controls that could be implemented in the Workstation, LAN, LAN-to-WAN, WAN, Remote Access, and System/Application Domains.

**Recommend** and **explain** one security control for each domain. Be sure to cite your sources.

#### 1. Workstation Domain:

**Security Control:** Endpoint Protection Software

**Explanation:** Implementing robust endpoint protection software on each workstation can help defend against malware, including those delivered through phishing campaigns. This software typically includes antivirus, anti-malware, and other features to detect and prevent malicious activities on individual workstations (Ruotsalainen, 2013).

#### 2. LAN (Local Area Network) Domain:

**Security Control:** Network Segmentation

**Explanation:** Segmenting the LAN into different subnetworks based on functional roles or security requirements helps contain potential security breaches. This reduces the lateral movement of attackers within the network, limiting their impact (Toivakka, 2018).

#### 3. LAN-to-WAN (Wide Area Network) Domain:

**Security Control:** Intrusion Prevention System (IPS)

**Explanation:** Deploying an IPS at the network perimeter helps identify and prevent malicious activities, such as unauthorized access attempts and exploits before they reach the internal network. It adds an extra layer of defense against external threats (Stiawan et al., 2010).

#### 4. **WAN (Wide Area Network) Domain:**

**Security Control:** Virtual Private Network (VPN) for Site-to-Site Connectivity

**Explanation:** Using VPNs for site-to-site connectivity ensures secure communication between geographically dispersed locations. This encryption helps protect data in transit over the WAN, reducing the risk of interception by unauthorized entities (Sholihah et al., 2019).

#### 5. **Remote Access Domain:**

**Security Control:** Multi-Factor Authentication (MFA)

**Explanation:** Enforcing MFA for remote access adds an extra layer of identity verification beyond passwords. This significantly enhances the security posture, making it more challenging for attackers to compromise user accounts even if credentials are stolen.

#### 6. **System/Application Domain:**

**Security Control:** Application Whitelisting

**Explanation:** Implementing application whitelisting allows only approved and known applications to run on systems. This mitigates the risk of unauthorized or malicious software being executed, providing better control over the applications running on servers. (Securing Industrial Automation and Control Systems Using Application Whitelisting, 2014)

## **CONCLUSION**

In this lab, a comprehensive exploration of the seven domains of a typical IT infrastructure was conducted. This included reviewing basic security controls on a Windows workstation, exploring additional devices on the LAN segment, and examining critical functions of the pfSense application such as routing, Network Address Translation (NAT), and packet filtering. Additionally, the lab involved inspecting common server roles in IT infrastructures, such as a domain controller, DNS server, and web server. The use of various command-line utilities, PuTTY for remote connections, and screen captures for documentation were integral parts of the lab work. Overall, the lab provided a hands-on opportunity to gain practical knowledge and skills related to fundamental IT concepts and security controls.

## REFERENCES

- Eldardiry, H., Bart, E., Liu, J., Hanley, J., Price, B., & Brdiczka, O. (2013, May 1). *Multi-Domain Information Fusion for Insider Threat Detection*. IEEE Xplore.  
<https://doi.org/10.1109/SPW.2013.14>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 1). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 2). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 4). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 5). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 6). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 7). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 8). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 9). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 10). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>



- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 12). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 16). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 17). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 21). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 22). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 24). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 25). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 26). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 27). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 28). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 29). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>

- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 31). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 33). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 34). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 35). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 36). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 37). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 38). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Eweka O. (2024). Exploring the Seven Domains of a Typical IT Infrastructure (Figure 41). *Jones and Bartlett Learning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>
- Kim, D. (2021). *Fundamentals Of Information Systems Security + Cloud Labs*. Jones & Bartlett Learning Lab1 Exploring the Seven Domains of a Typical IT Infrastructure (Figure 11) <https://jbl-lti.hatsize.com/startlab>
- Kim, D. (2021). *Fundamentals Of Information Systems Security + Cloud Labs*. Jones & Bartlett Learning Lab1 Exploring the Seven Domains of a Typical IT Infrastructure (Figure 13) <https://jbl-lti.hatsize.com/startlab>

Kim, D. (2021). *Fundamentals Of Information Systems Security + Cloud Labs*. Jones & Bartlett  
Learning Lab1 Exploring the Seven Domains of a Typical IT Infrastructure (Figure 14)

<https://jbl-lti.hatsize.com/startlab>

Kim, D. (2021). *Fundamentals Of Information Systems Security + Cloud Labs*. Jones & Bartlett  
Learning Lab1 Exploring the Seven Domains of a Typical IT Infrastructure (Figure 15)

<https://jbl-lti.hatsize.com/startlab>

Kim, D. (2021). *Fundamentals Of Information Systems Security + Cloud Labs*. Jones & Bartlett  
Learning Lab1 Exploring the Seven Domains of a Typical IT Infrastructure (Figure 16)

<https://jbl-lti.hatsize.com/startlab>

Kim, D. (2021). *Fundamentals Of Information Systems Security + Cloud Labs*. Jones & Bartlett  
Learning Lab1 Exploring the Seven Domains of a Typical IT Infrastructure (Figure 18)

<https://jbl-lti.hatsize.com/startlab>

Kim, D. (2021). *Fundamentals Of Information Systems Security + Cloud Labs*. Jones & Bartlett  
Learning Lab1 Exploring the Seven Domains of a Typical IT Infrastructure (Figure 19)

<https://jbl-lti.hatsize.com/startlab>

Kim, D. (2021). *Fundamentals Of Information Systems Security + Cloud Labs*. Jones & Bartlett  
Learning Lab1 Exploring the Seven Domains of a Typical IT Infrastructure (Figure 20)

<https://jbl-lti.hatsize.com/startlab>

Kim, D. (2021). *Fundamentals Of Information Systems Security + Cloud Labs*. Jones & Bartlett  
Learning Lab1 Exploring the Seven Domains of a Typical IT Infrastructure (Figure 23)

<https://jbl-lti.hatsize.com/startlab>

Kim, D. (2021). *Fundamentals Of Information Systems Security + Cloud Labs*. Jones & Bartlett

Learning Lab1 Exploring the Seven Domains of a Typical IT Infrastructure (Figure 30)

<https://jbl-lti.hatsize.com/startlab>

OWASP. (2021). *OWASP Top Ten*. Owasp.org; OWASP.

<https://owasp.org/www-project-top-ten/>

OWASP. (n.d.). *Juice Shop - Insecure Web Application for Training* | OWASP. Owasp.org.

<https://owasp.org/www-project-juice-shop/>

Ruotsalainen, P. (2013). *ENDPOINT PROTECTION SECURITY SYSTEM FOR AN*

*ENTERPRISE*. Wwv.theseus.fi. <https://www.theseus.fi/handle/10024/62932>

*Securing industrial automation and control systems using application whitelisting* | IEEE

*Conference Publication* | IEEE Xplore. (n.d.). Ieeexplore.ieee.org. Retrieved February 6,

2024, from <https://ieeexplore.ieee.org/abstract/document/7005242>

Sholihah, W., Rizaldi, T., & Novianty, I. (2019). Information and communication system

technology with VPN site-to-site IPsec. *Journal of Physics*, 1193, 012012.

<https://doi.org/10.1088/1742-6596/1193/1/012012>

Stiawan, D., Abdullah, A. H., & Yazid Idris, Mohd. (2010, June 1). *The trends of Intrusion*

*Prevention System network*. IEEE Xplore. <https://doi.org/10.1109/ICETC.2010.5529697>

Toivakka, J. (2018). *Network segmentation*. Wwv.theseus.fi.

<https://www.theseus.fi/handle/10024/158766>

*What are Security Controls?* | IBM. (n.d.). Wwv.ibm.com.

[https://www.ibm.com/topics/security-](https://www.ibm.com/topics/security-controls#:~:text=Digital%20security%20controls%20include%20such)

[controls#:~:text=Digital%20security%20controls%20include%20such](https://www.ibm.com/topics/security-controls#:~:text=Digital%20security%20controls%20include%20such)

