

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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

Student:

John Monteiro

Email:

jmonteiro48@bristolcc.edu

Time on Task:

8 hours, 58 minutes

Progress:

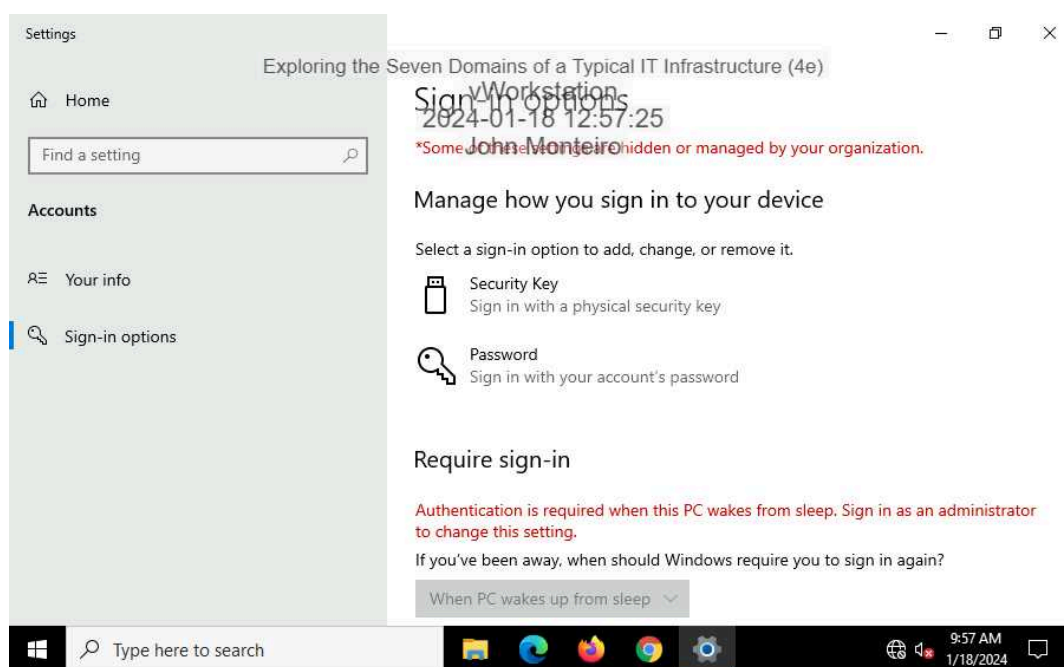
100%

Report Generated: Friday, January 19, 2024 at 1:09 PM

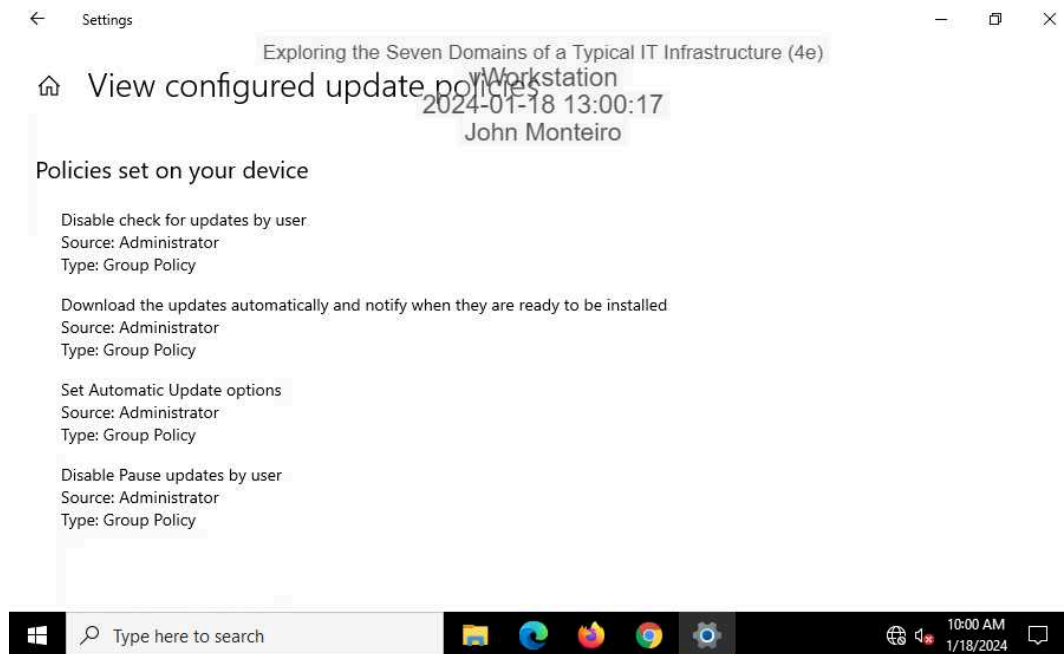
## Section 1: Hands-On Demonstration

### Part 1: Explore the Workstation Domain

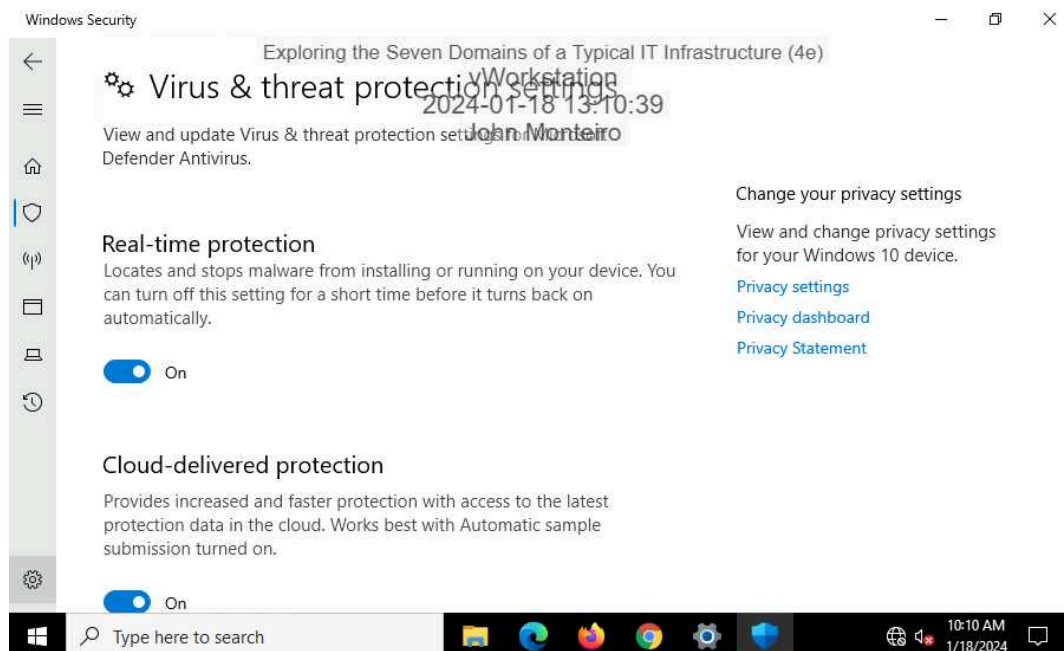
4. Make screen capture showing the **Sign-in options** for Alice's account.



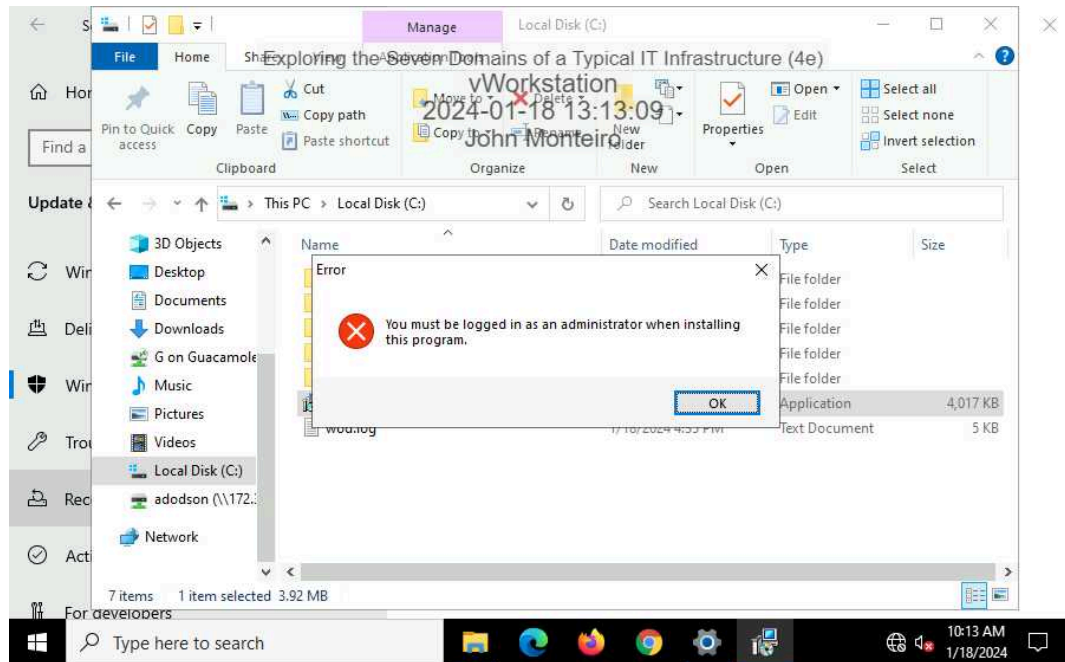
### 7. Make a screen capture showing the **View configured update policies** page.



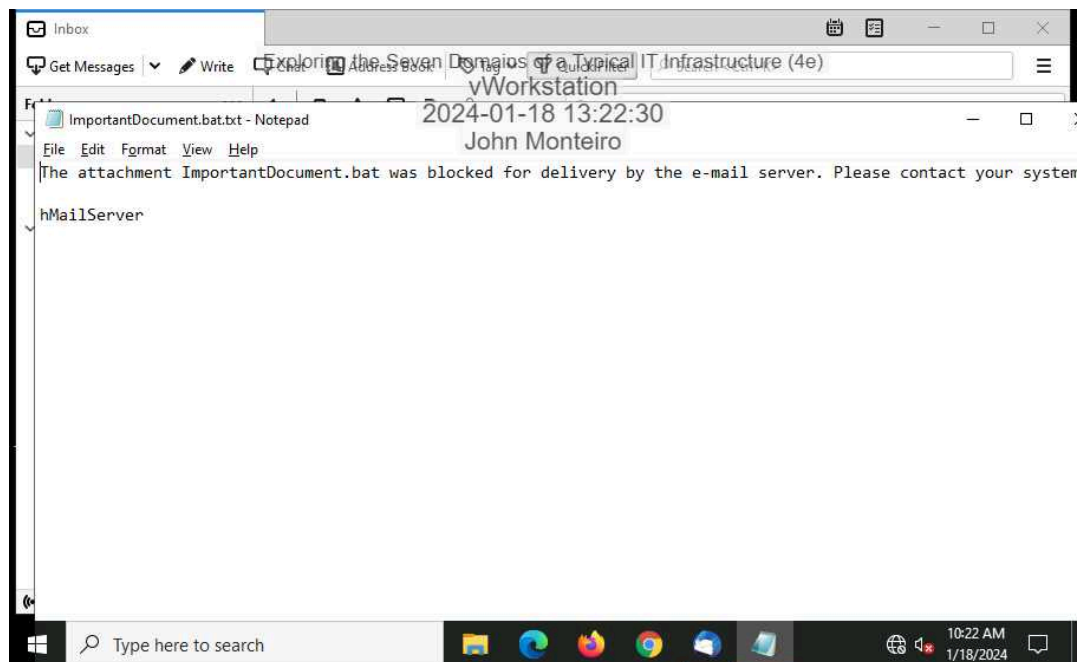
### 14. Make a screen capture showing the **Virus & Threat Protection Settings**.



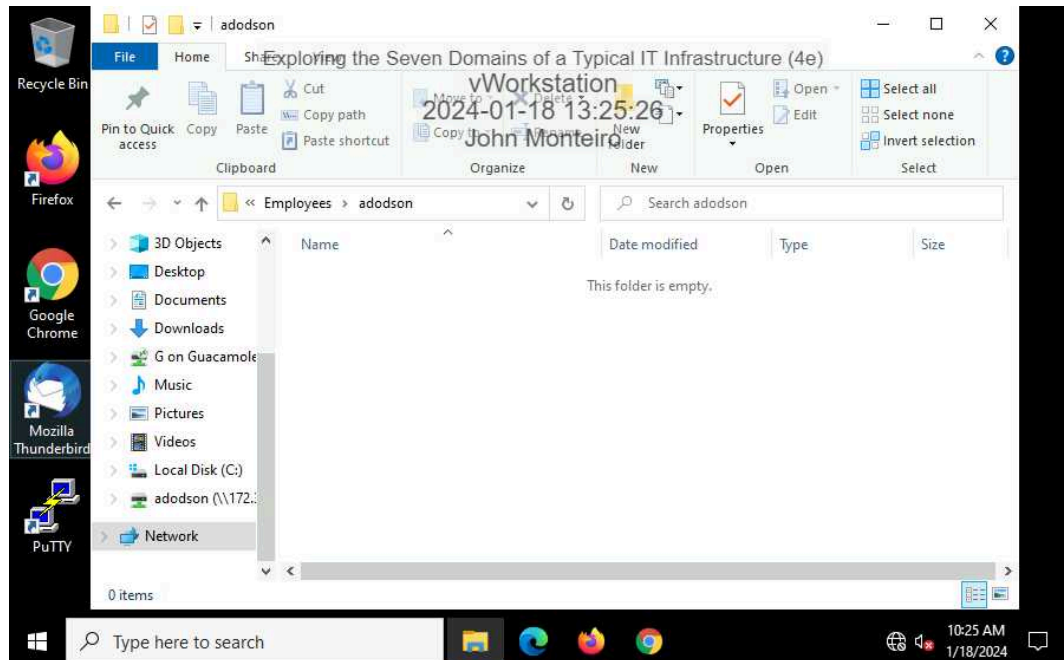
18. **Make a screen capture** showing the **security warning** from attempting to run an **executable file**.



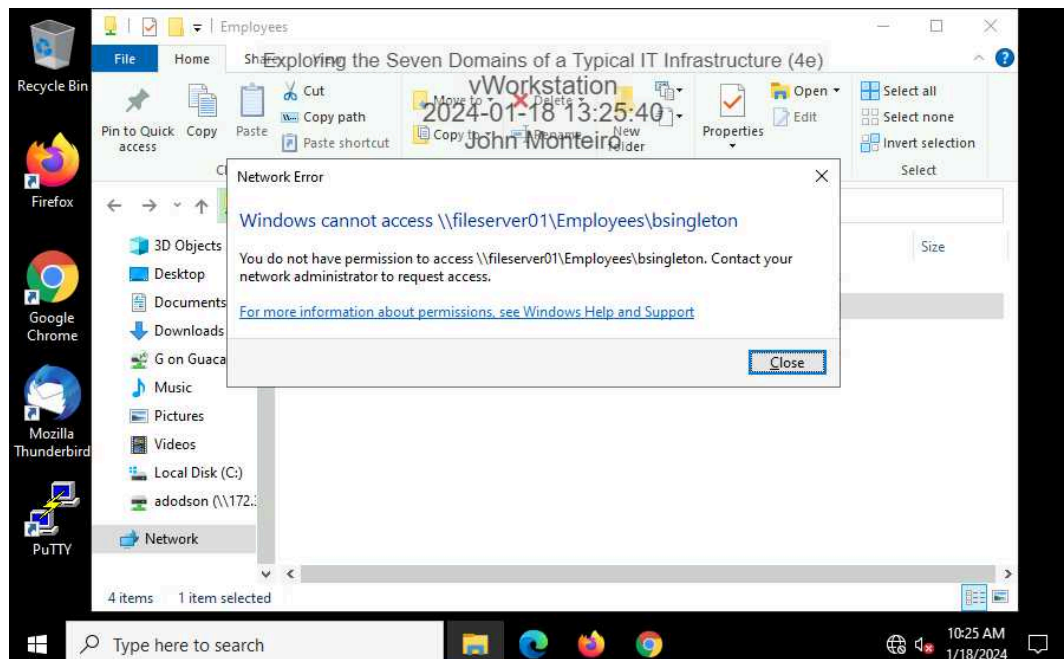
24. **Make a screen capture** showing the **blocked attachment message**.



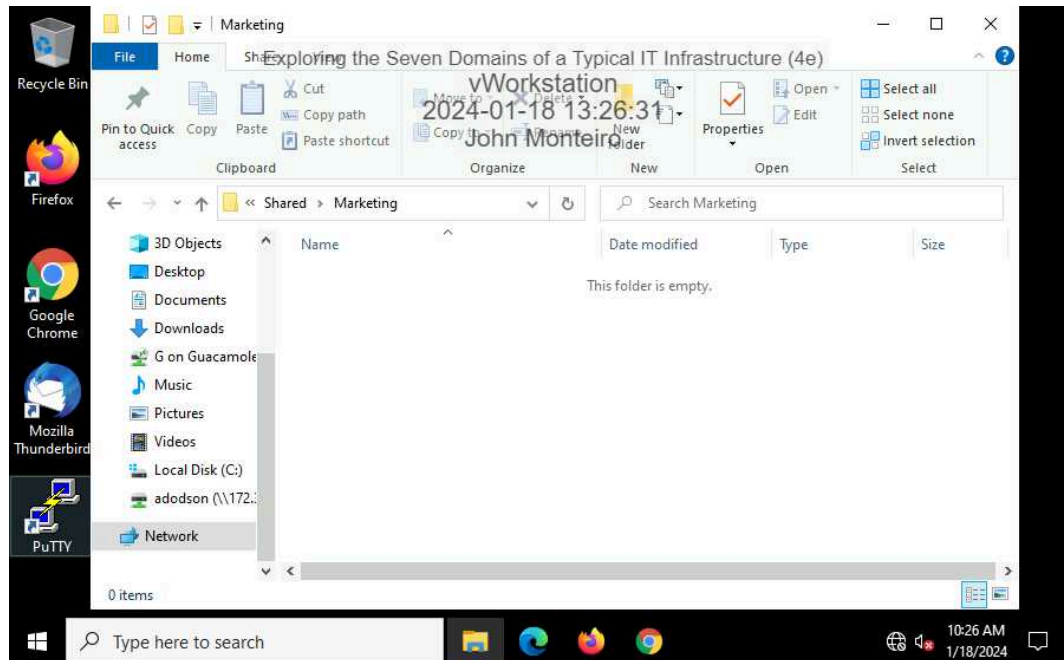
28. Make a screen capture showing a **successful connection to the adodson user folder**.



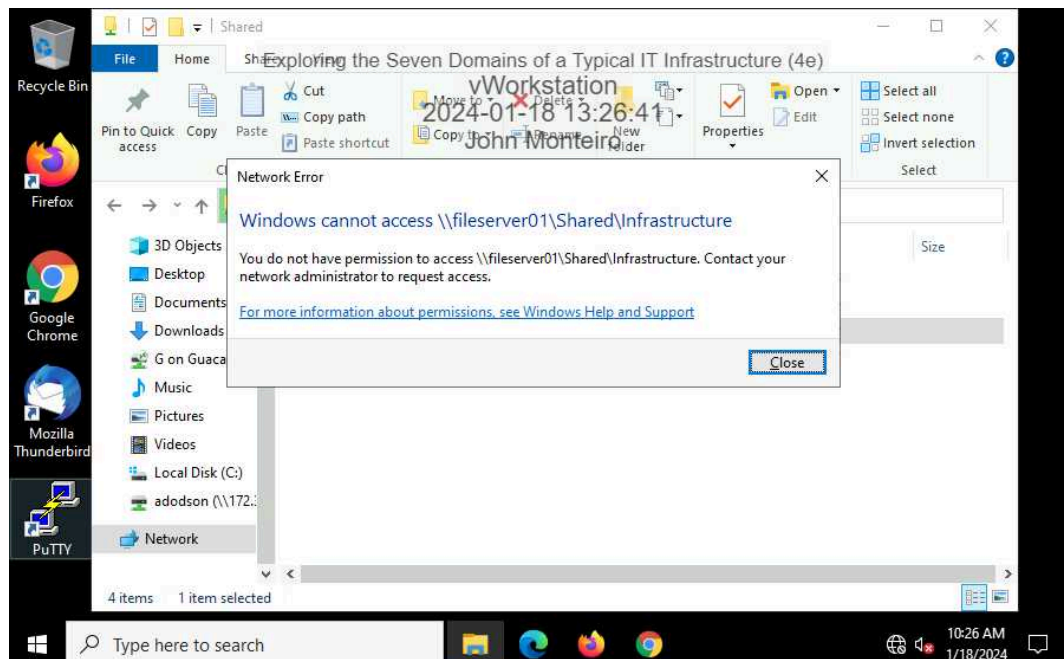
29. Make a screen capture showing a **failed connection to another user folder**.



31. Make a screen capture showing a successful connection to the Marketing shared folder.



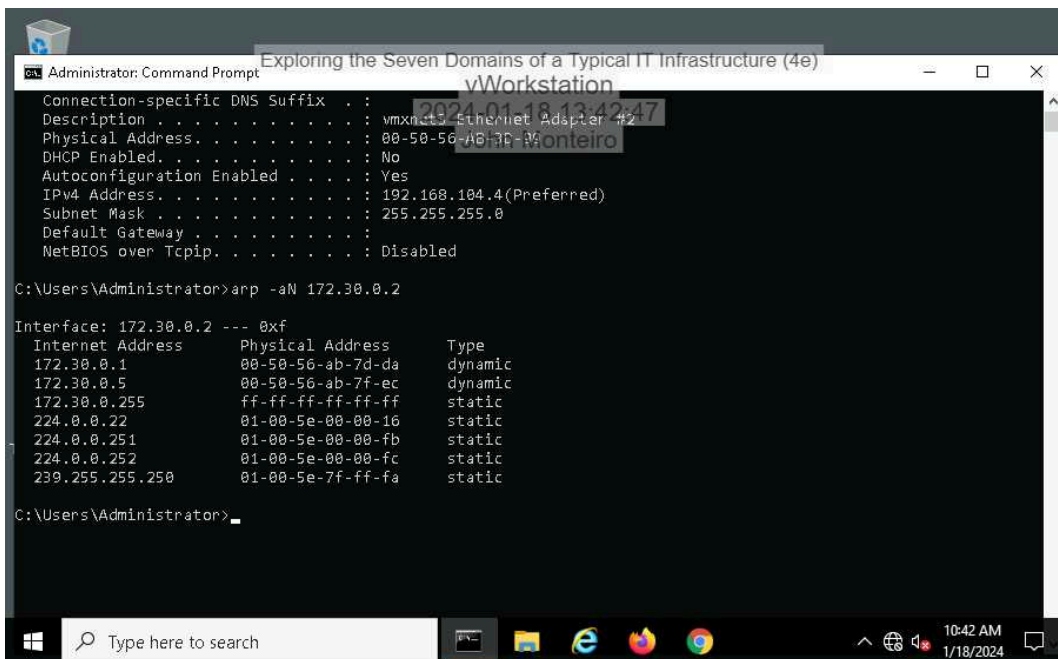
32. Make a screen capture showing a failed connection to another shared folder.



## Part 2: Explore the LAN Domain



### 5. Make a screen capture showing the vWorkstation's original ARP table.



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The window displays the output of the command `arp -a` for the interface 172.30.0.2. The output shows the ARP table for the interface, listing Internet Address, Physical Address, and Type.

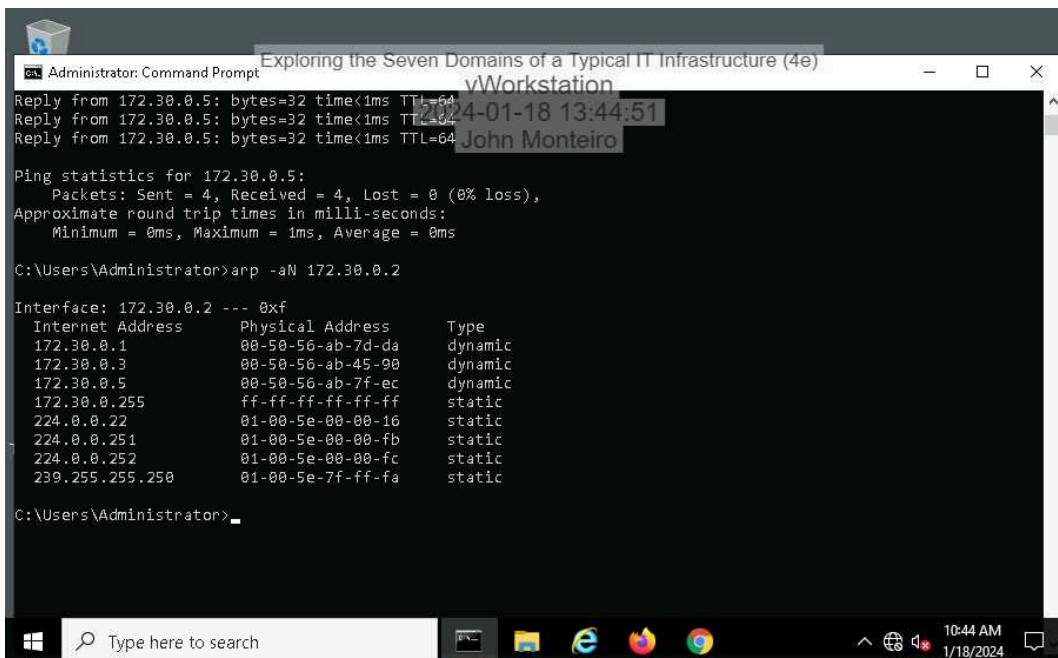
```
Connection-specific DNS Suffix . : 
Description . . . . . : vmxnet3 Ethernet Adapter #2
Physical Address. . . . . : 00-50-56-AB-7D-DA
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.104.4(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 
NetBIOS over Tcpip. . . . . : Disabled

C:\Users\Administrator>arp -a 172.30.0.2

Interface: 172.30.0.2 --- 0xf
Internet Address      Physical Address      Type
172.30.0.1            00-50-56-ab-7d-da     dynamic
172.30.0.5            00-50-56-ab-7f-ec     dynamic
172.30.0.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Users\Administrator>
```

### 10. Make a screen capture showing the vWorkstation's updated ARP table.



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The window displays the output of the command `arp -a` for the interface 172.30.0.2. The output shows the ARP table for the interface, listing Internet Address, Physical Address, and Type. The table is updated compared to the previous screenshot, showing new physical addresses for 172.30.0.1 and 172.30.0.3.

```
Reply from 172.30.0.5: bytes=32 time<1ms TTL=64
Reply from 172.30.0.5: bytes=32 time<1ms TTL=64
Reply from 172.30.0.5: bytes=32 time<1ms TTL=64

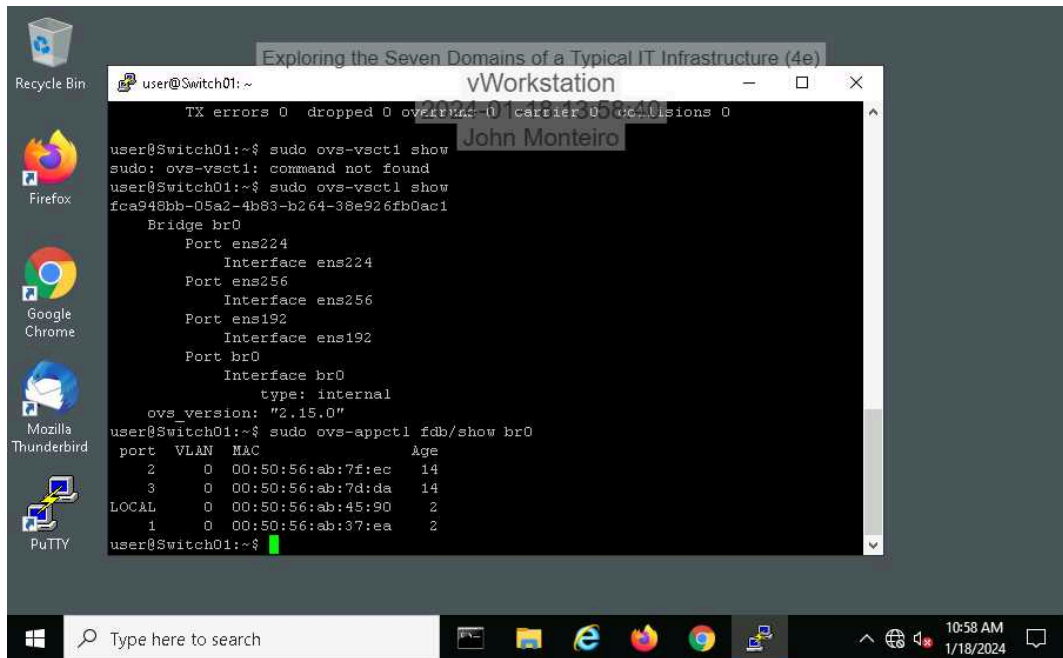
Ping statistics for 172.30.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>arp -a 172.30.0.2

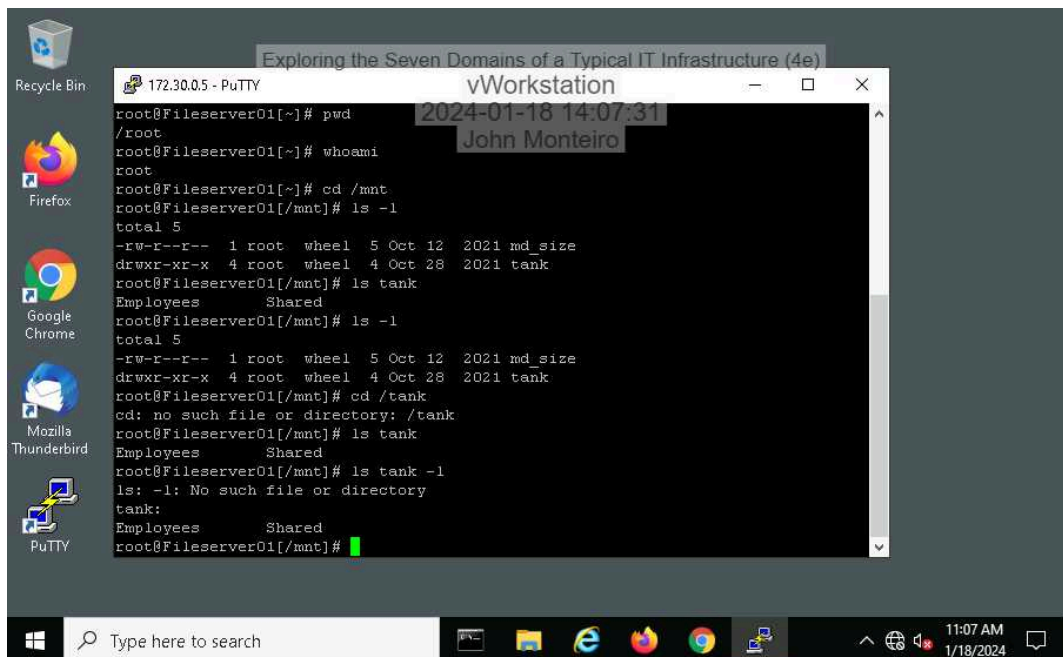
Interface: 172.30.0.2 --- 0xf
Internet Address      Physical Address      Type
172.30.0.1            00-50-56-ab-7d-da     dynamic
172.30.0.3            00-50-56-ab-45-90     dynamic
172.30.0.5            00-50-56-ab-7f-ec     dynamic
172.30.0.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Users\Administrator>
```

### 20. Make a screen capture showing the Switch01 forwarding table.

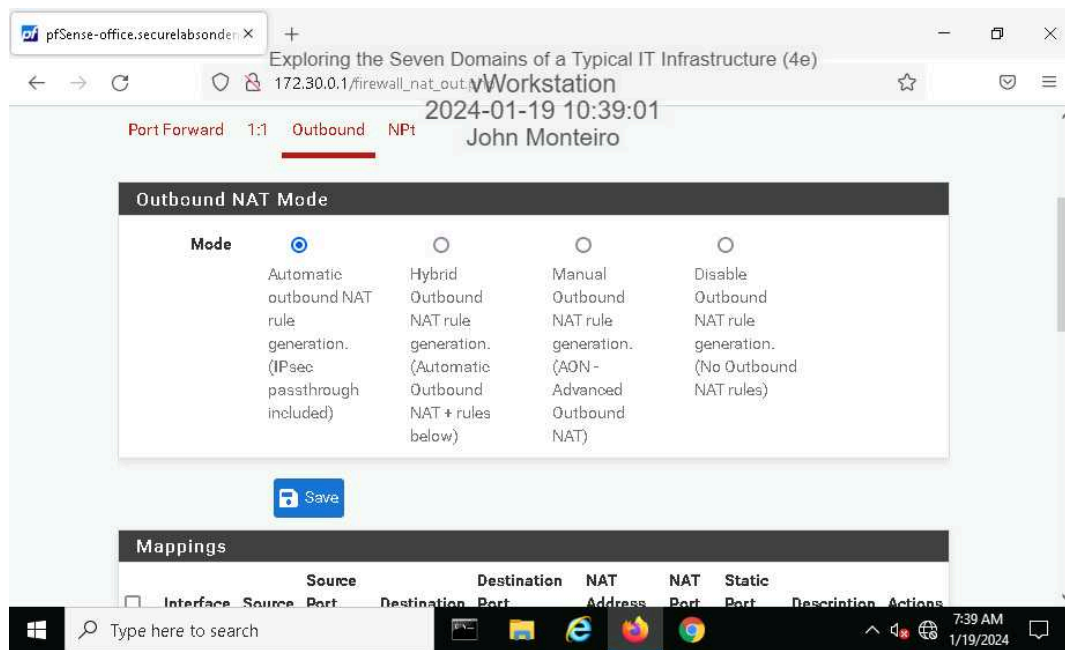


### 30. Make a screen capture showing the contents of the Employees directory.

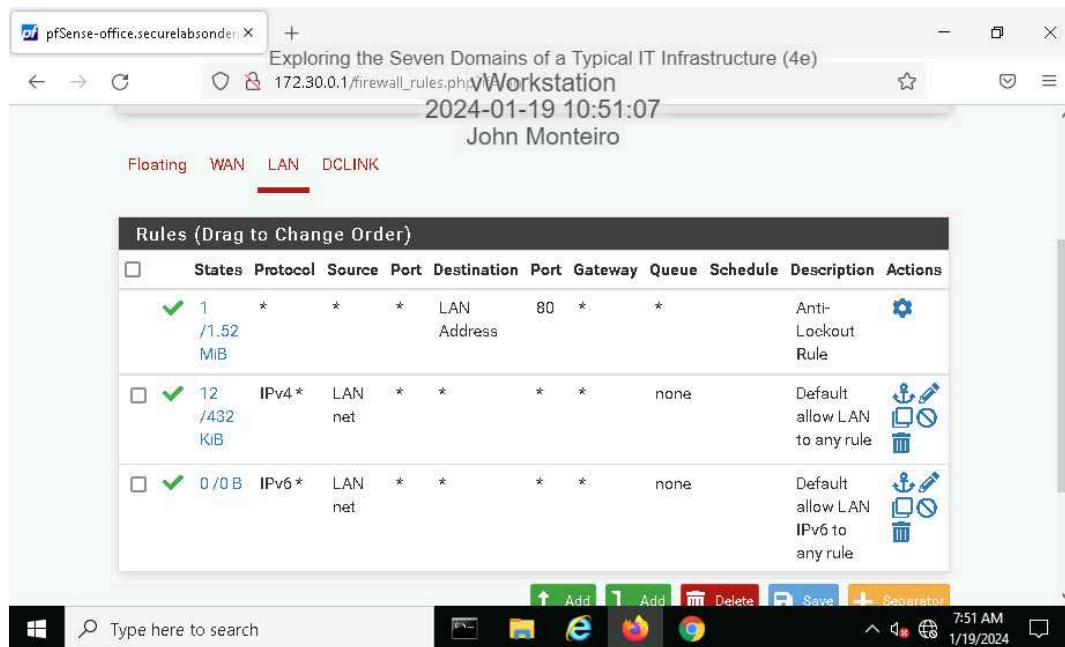


## Part 3: Explore the LAN-to-WAN Domain

### 6. Make a screen capture showing the Outbound NAT settings.

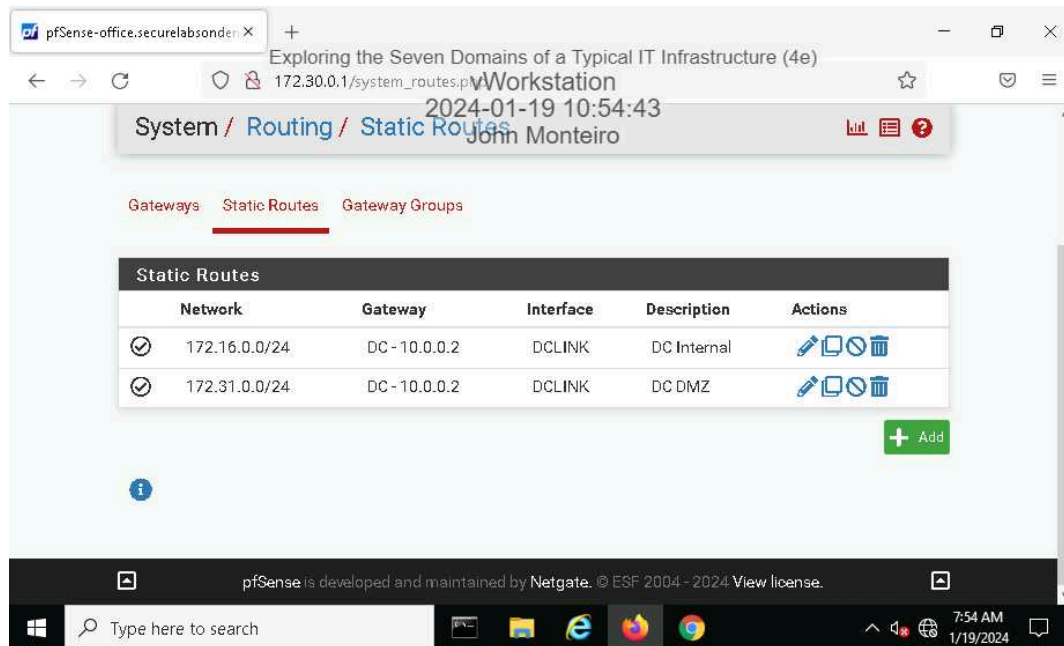


### 9. Make a screen capture showing the permissive LAN rules.

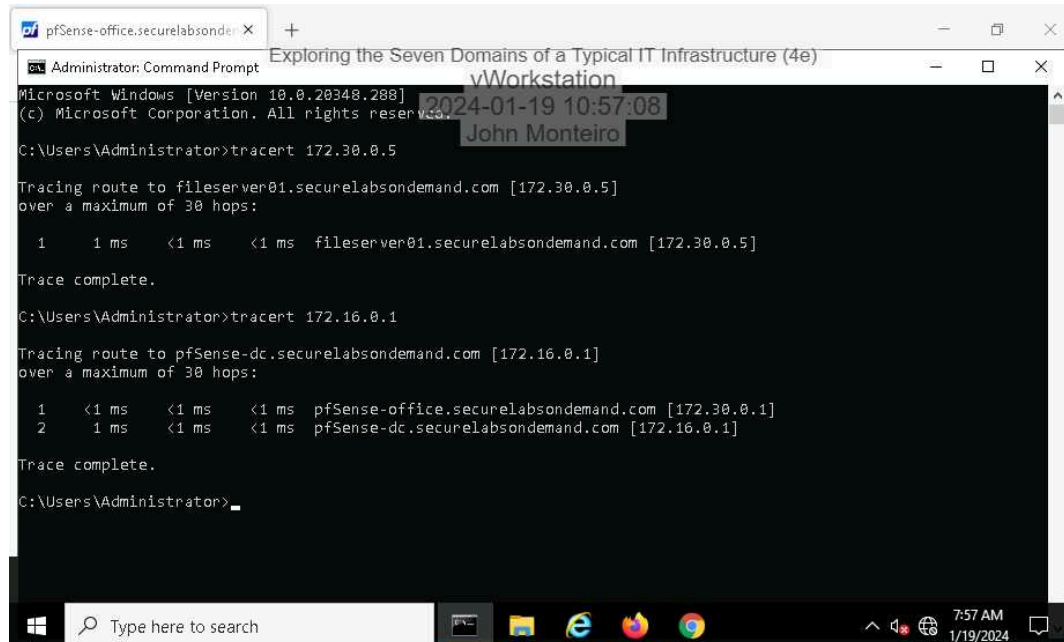




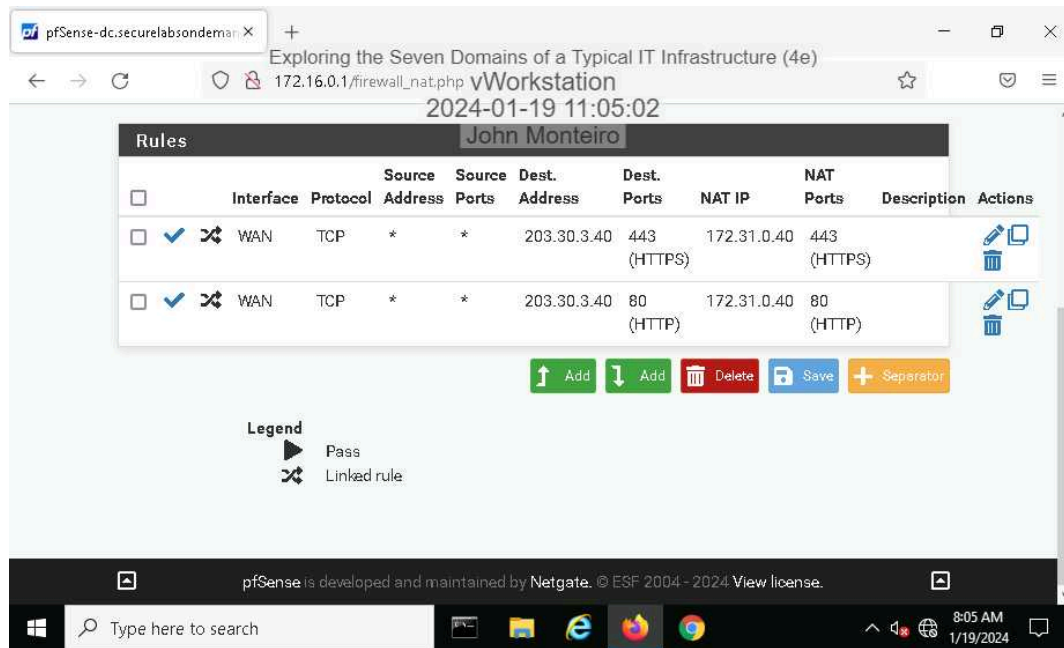
### 12. Make a screen capture showing the **Static Routes** page.



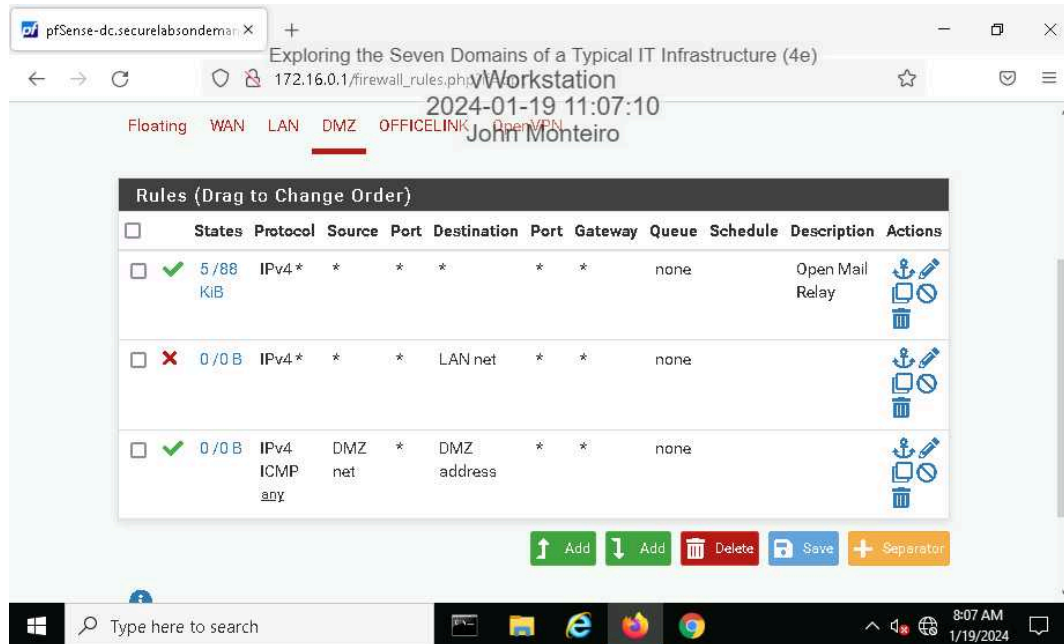
### 16. Make a screen capture showing the result of your tracert to the pfsense-dc appliance.



22. Make a screen capture showing the **Port Forward** rules for the web server.



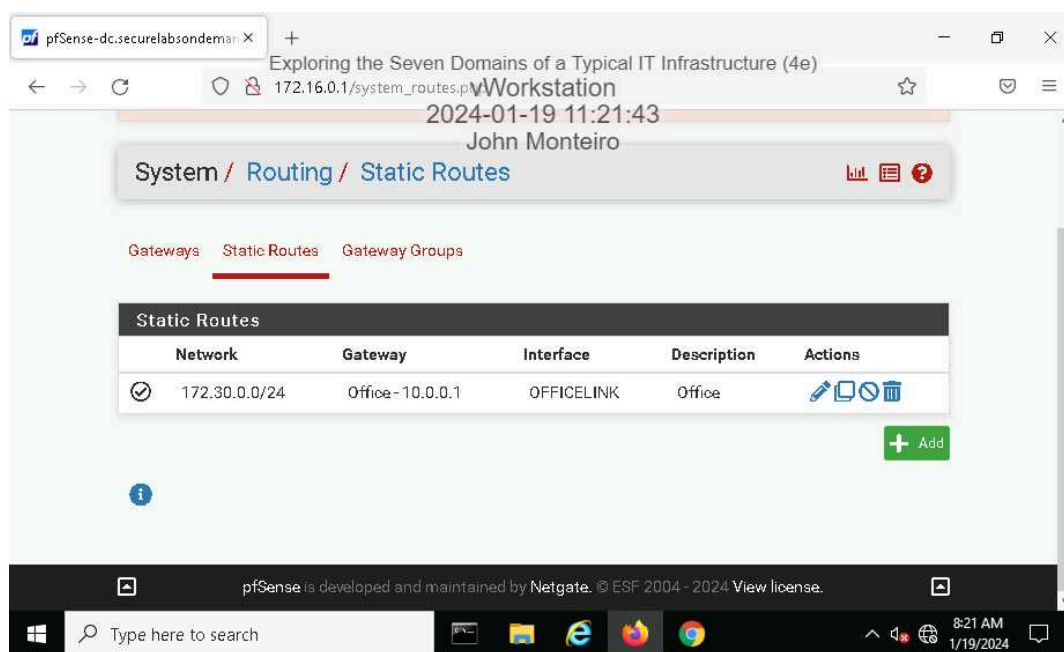
25. Make a screen capture showing the **DMZ** firewall rules.



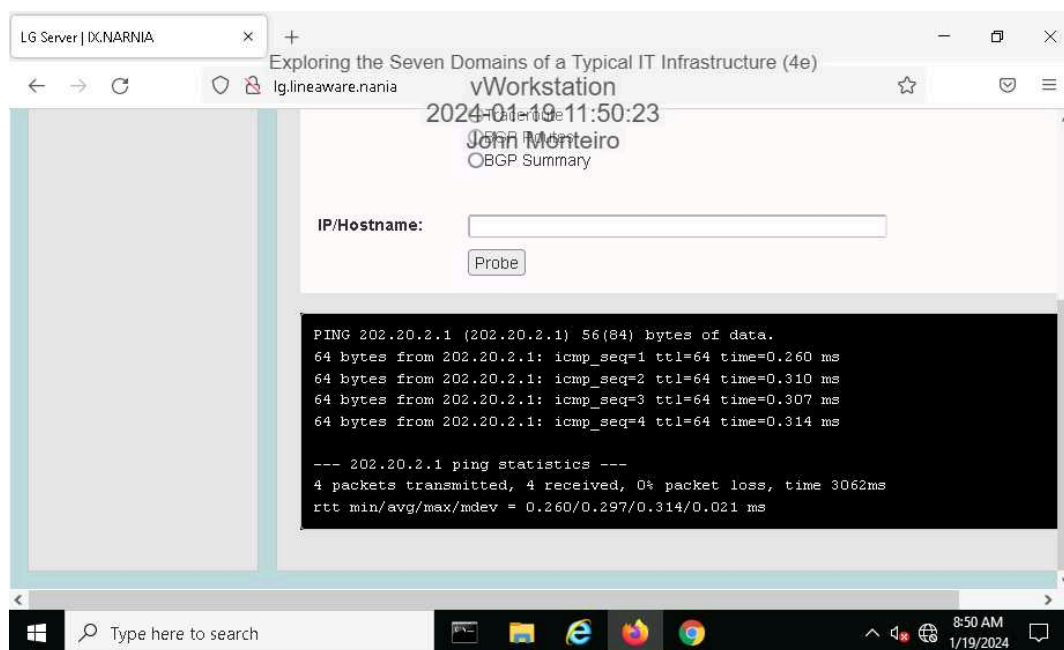
### Section 2: Applied Learning

#### Part 1: Explore the WAN Domain

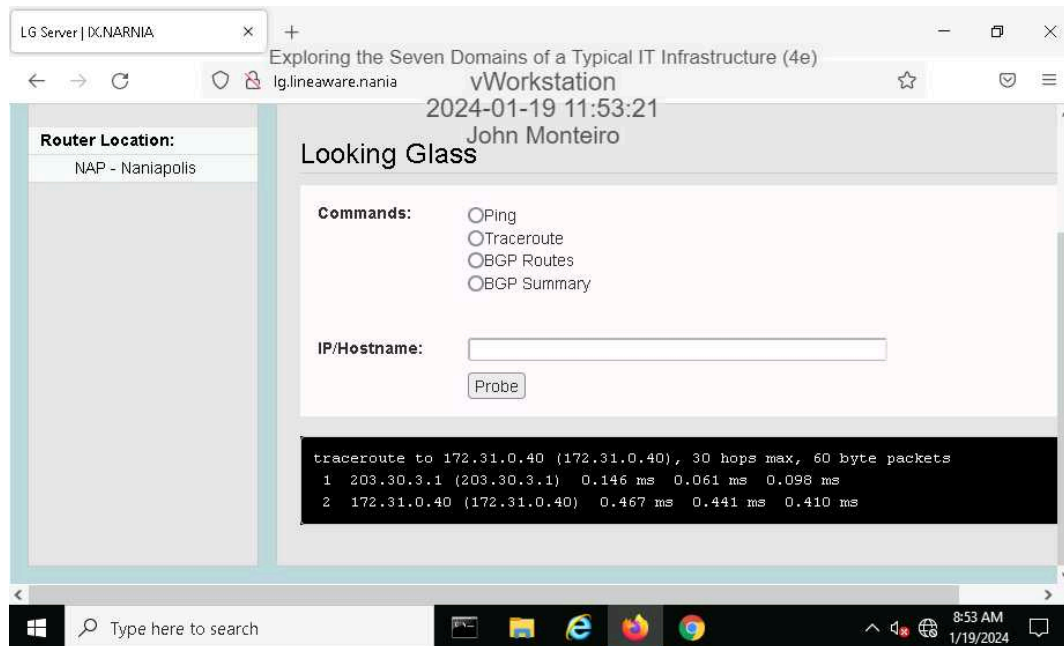
5. Make a screen capture showing the **static route** for the point-to-point connection.



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

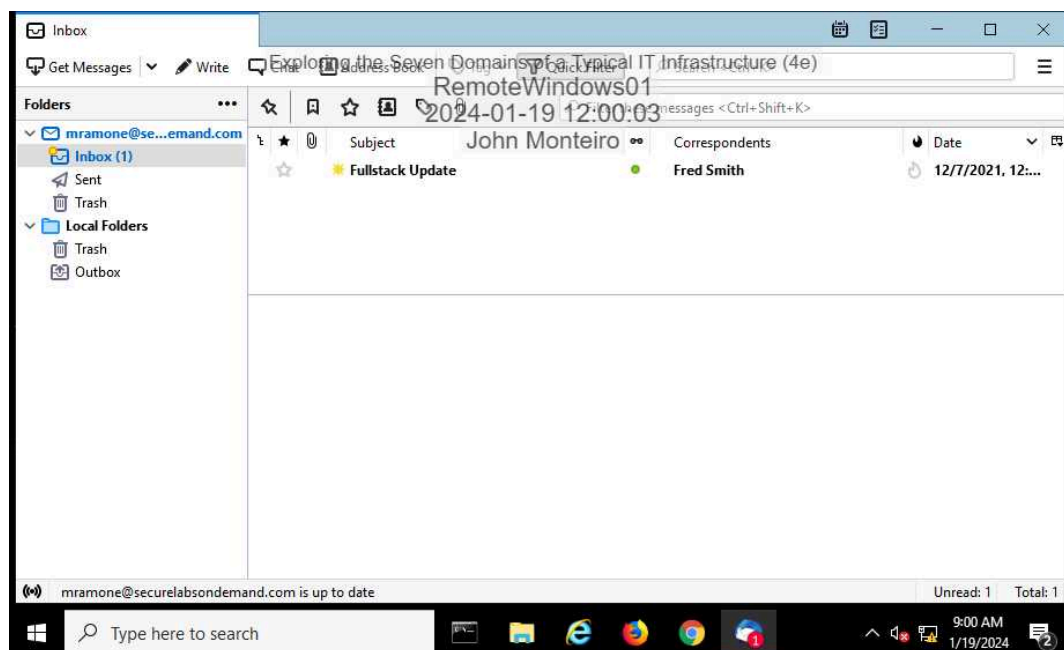


### 12. Make a screen capture showing the **traceroute** to the file server.



## Part 2: Explore the Remote Access Domain

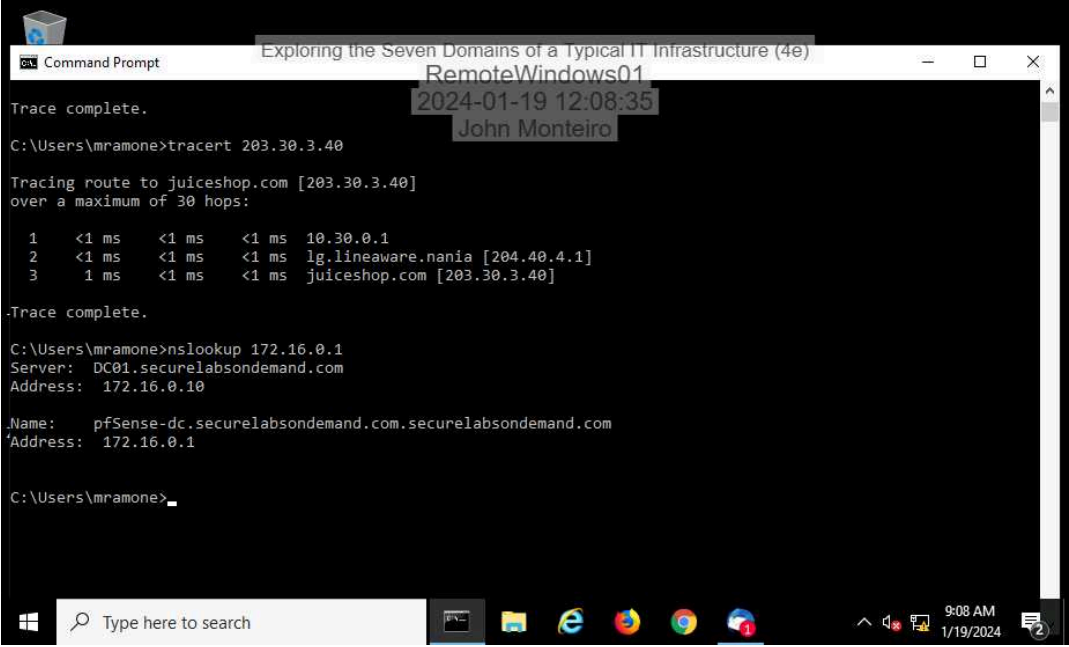
### 9. Make a screen capture showing the **successful connection** to the email server.



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

both split and full tunnel in use

16. **Make a screen capture** showing the **successful reverse DNS lookup** for the internal host.



The screenshot shows a Windows Command Prompt window titled "Command Prompt" with the following text:

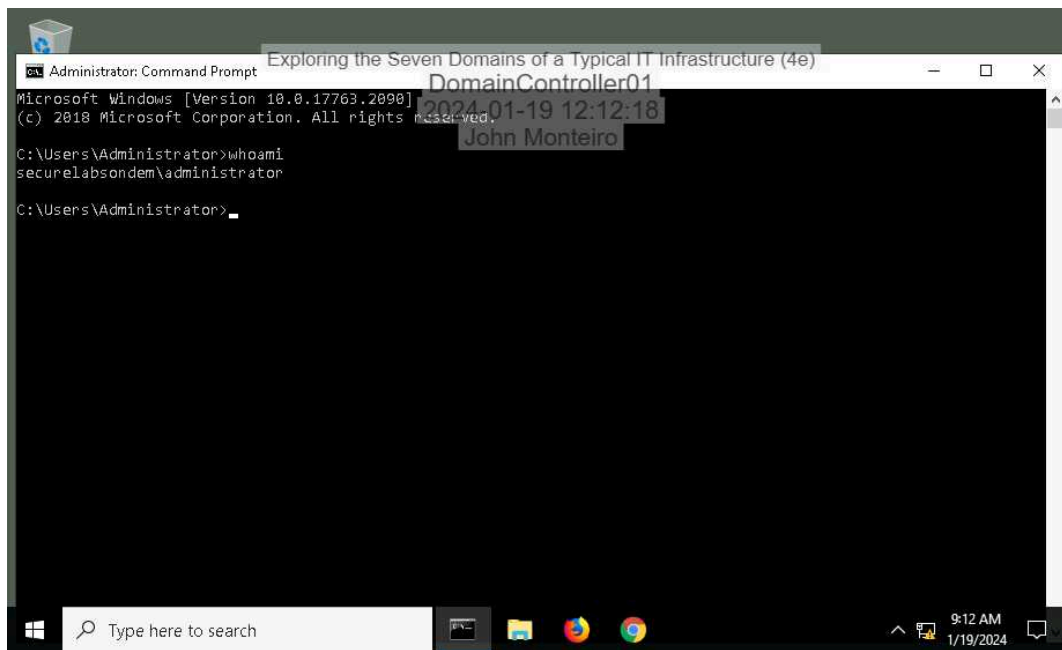
```
Trace complete.  
C:\Users\mramone>tracert 203.30.3.40  
  
Tracing route to juiceshop.com [203.30.3.40]  
over a maximum of 30 hops:  
  0  <1 ms  <1 ms  <1 ms  10.30.0.1  
  1  <1 ms  <1 ms  <1 ms  lg.lineaware.nania [204.40.4.1]  
  2  1 ms   <1 ms  <1 ms  juiceshop.com [203.30.3.40]  
  
Trace complete.  
  
C:\Users\mramone>nslookup 172.16.0.1  
Server: DC01.securelabsondemand.com  
Address: 172.16.0.10  
  
.Name:   pfSense-dc.securelabsondemand.com.securelabsondemand.com  
Address: 172.16.0.1  
  
C:\Users\mramone>
```

Overlaid on the screenshot is a semi-transparent box containing the text: "RemoteWindows01", "2024-01-19 12:08:35", and "John Monteiro". The Windows taskbar at the bottom shows the search bar, task view button, and several application icons. The system clock in the bottom right corner displays "9:08 AM 1/19/2024".

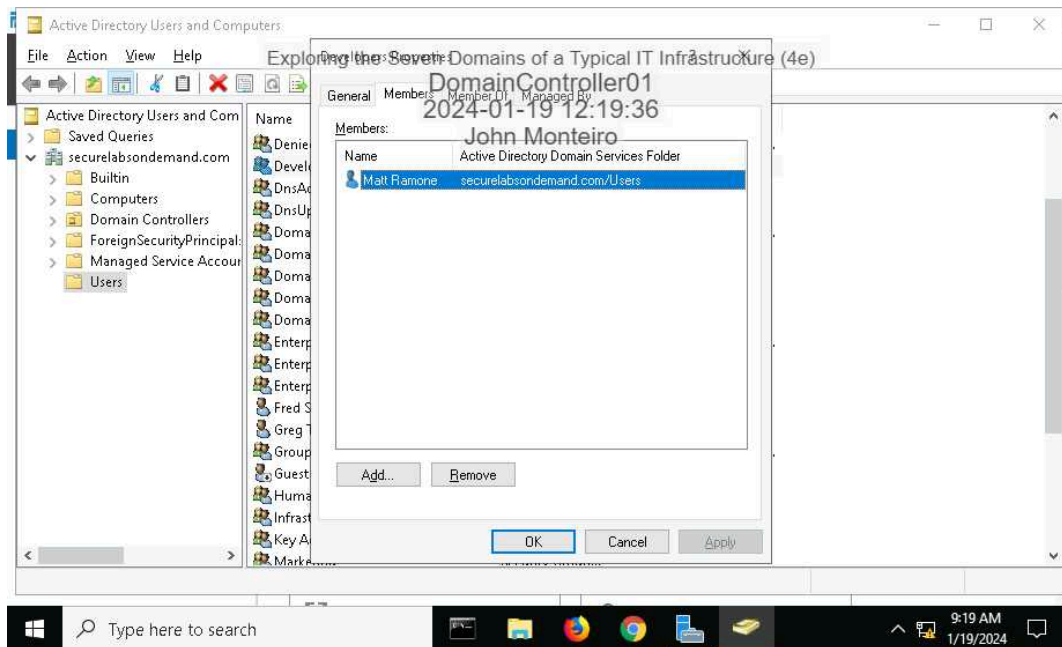
### Part 3: Explore the System/Application Domain



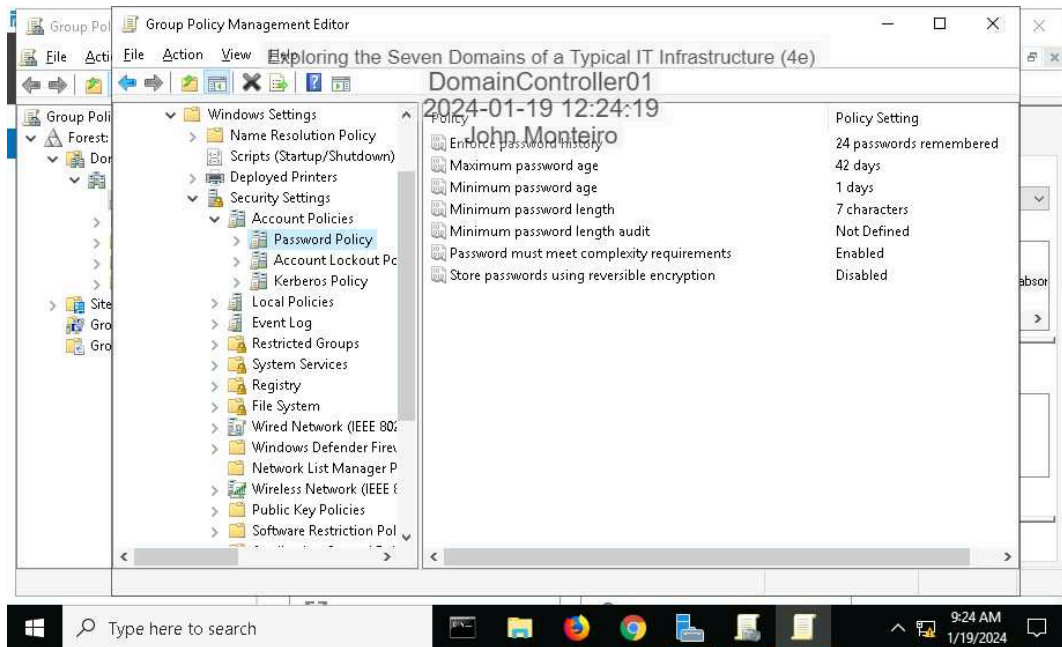
4. Make a screen capture showing the **whoami** results.



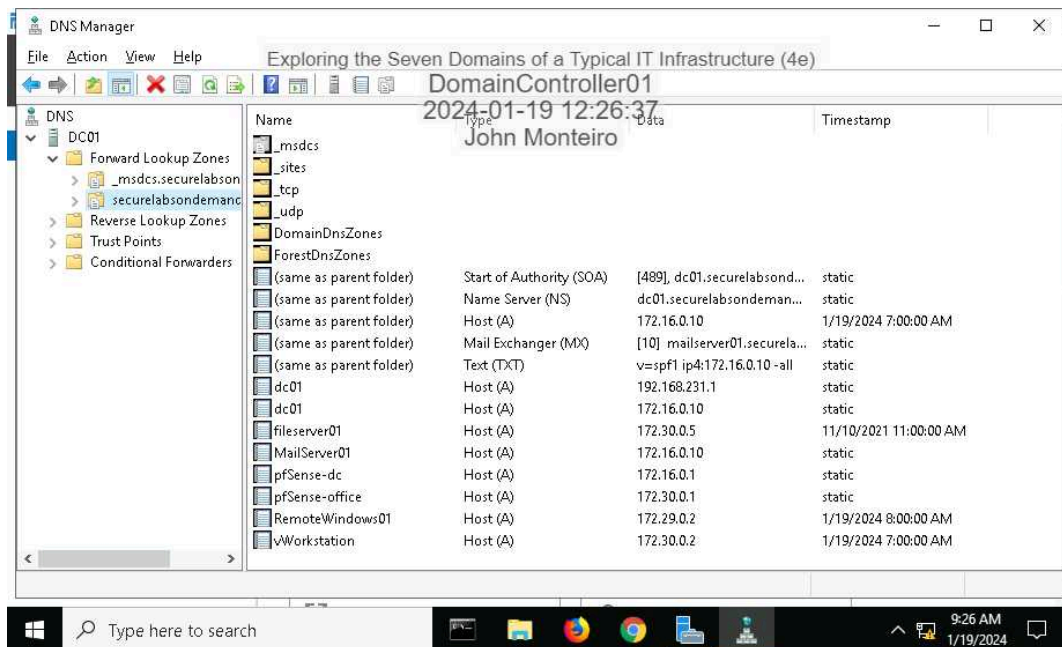
10. Make a screen capture showing the members of the Developers AD group.



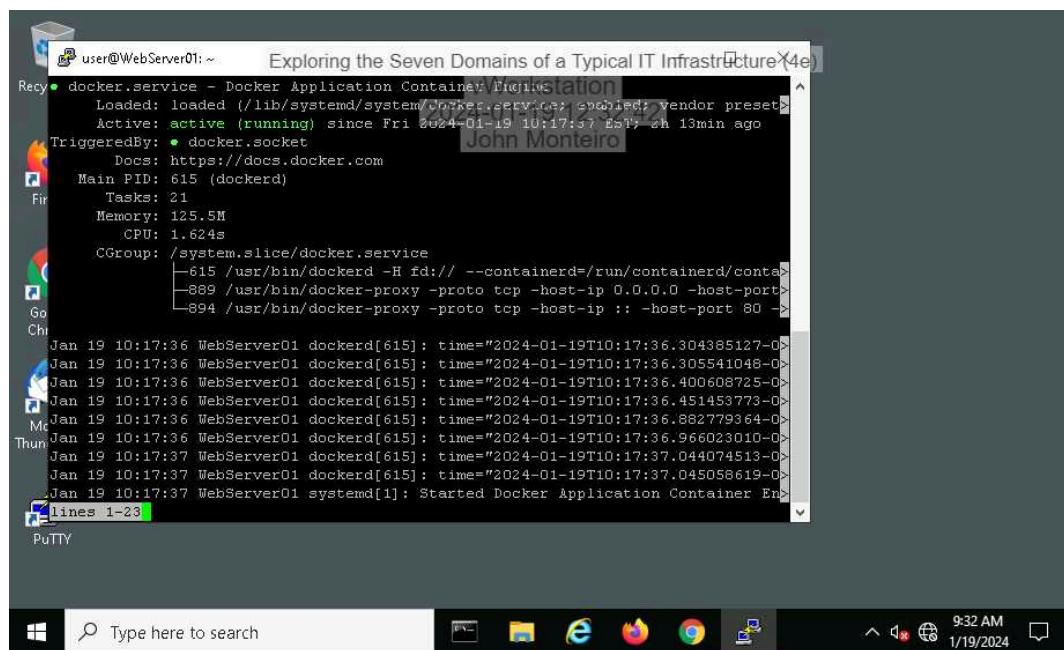
16. **Make a screen capture** showing the **password policy settings in the Group Policy Management Console.**



20. **Make a screen capture** showing the **DNS entries.**

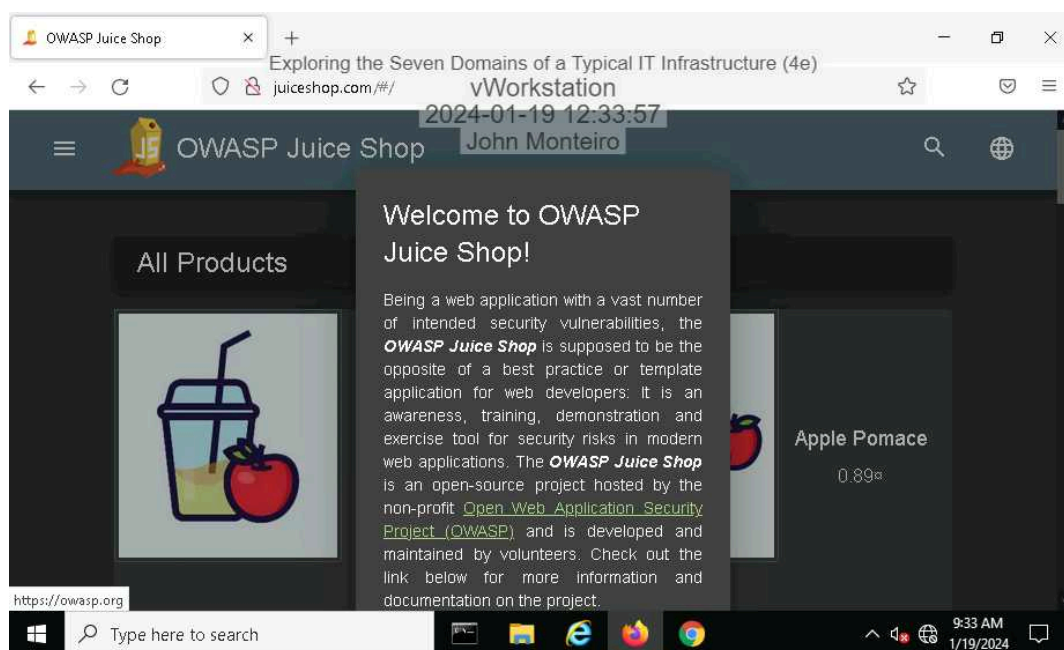


### 28. Make a screen capture showing the Docker service status.



```
user@WebServer01: ~  
docker.service - Docker Application Container Engine  
Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: enabled)  
Active: active (running) since Fri 2024-01-19 10:17:37 EST; 2h 13min ago  
TriggeredBy: ● docker.socket  
Docs: https://docs.docker.com  
Main PID: 615 (dockerd)  
Tasks: 21  
Memory: 125.5M  
CPU: 1.624s  
CGroup: /system.slice/docker.service  
└─615 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock  
└─889 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 80  
└─894 /usr/bin/docker-proxy -proto tcp -host-ip :: -host-port 80  
Jan 19 10:17:36 WebServer01 dockerd[615]: time="2024-01-19T10:17:36.304385127-0500" level=info msg="Starting  
Jan 19 10:17:36 WebServer01 dockerd[615]: time="2024-01-19T10:17:36.305541048-0500" level=info msg="API  
Jan 19 10:17:36 WebServer01 dockerd[615]: time="2024-01-19T10:17:36.400608725-0500" level=info msg="API  
Jan 19 10:17:36 WebServer01 dockerd[615]: time="2024-01-19T10:17:36.451453773-0500" level=info msg="API  
Jan 19 10:17:36 WebServer01 dockerd[615]: time="2024-01-19T10:17:36.882779364-0500" level=info msg="API  
Jan 19 10:17:36 WebServer01 dockerd[615]: time="2024-01-19T10:17:36.966023010-0500" level=info msg="API  
Jan 19 10:17:37 WebServer01 dockerd[615]: time="2024-01-19T10:17:37.044074513-0500" level=info msg="API  
Jan 19 10:17:37 WebServer01 dockerd[615]: time="2024-01-19T10:17:37.045058619-0500" level=info msg="API  
Jan 19 10:17:37 WebServer01 systemd[1]: Started Docker Application Container Engine.  
lines 1-23  
PuTTY
```

### 31. Make a screen capture showing the juiceshop.com web page.

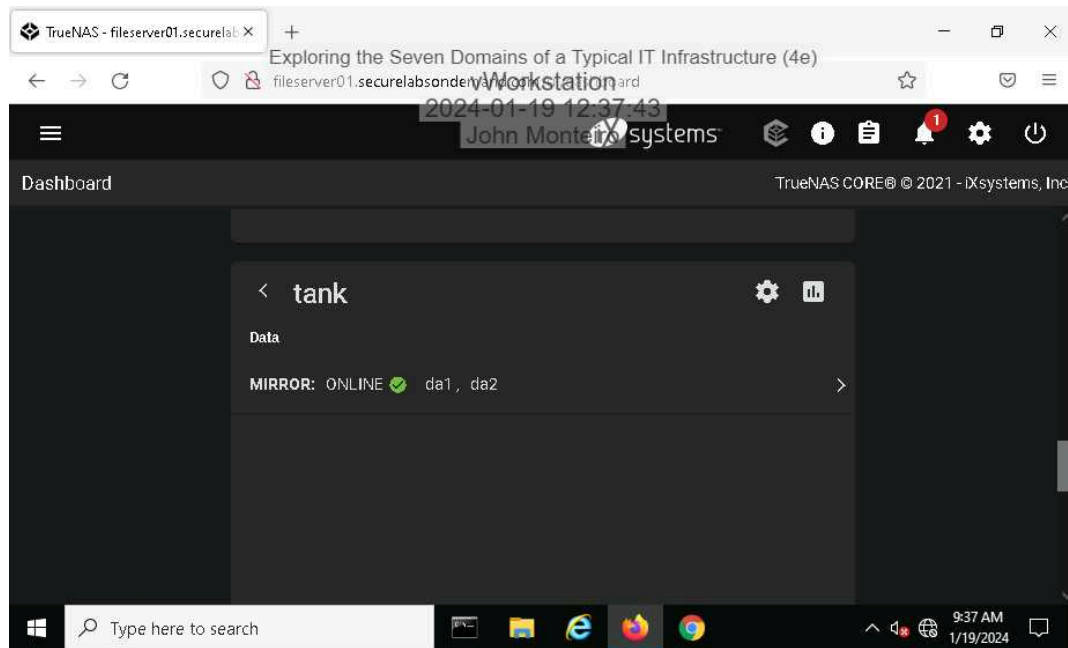


## Exploring the Seven Domains of a Typical IT Infrastructure (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

---

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



### Section 3: Challenge and Analysis

#### Part 1: Explore the User Domain

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.

Two compelling threats to the User Domain that I found in my research are Susceptibility to Social Engineering & Unlocked Domains. To protect the User Domain two controls include Registry Locks & Use of Updated Antivirus Software.

Sources: [What are three risks and threats of the user domain? – Divya Aradhya](#)  
[How to protect your organization's domain from security threats | TechRepublic](#)

1. **Susceptibility to Social Engineering:** Users are vulnerable to being socially engineered into letting malware and threat actors into the system. Phishing, vishing, whaling, pharming, spoofing, and impersonation are various ways a user could fall victim to hackers
2. **Unlocked Domains:** Unlocked domains are susceptible to malicious tactics that can lead to unauthorized DNS changes and domain name hijacking

To protect the User Domain, effective security controls are crucial. Two such controls include:

1. **Registry Locks:** Registry locks prevent domain name hijacking and unauthorized changes to the DNS
2. **Use of Updated Antivirus Software:** Updated antivirus software can inspect encrypted traffic for hidden malware and phishing attempts

#### Part 2: Research Additional Security Controls



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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

---

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.

Some recommendations I found were the following:

