Student: Udo Udo Williams	Email: raggg12@gmail.com

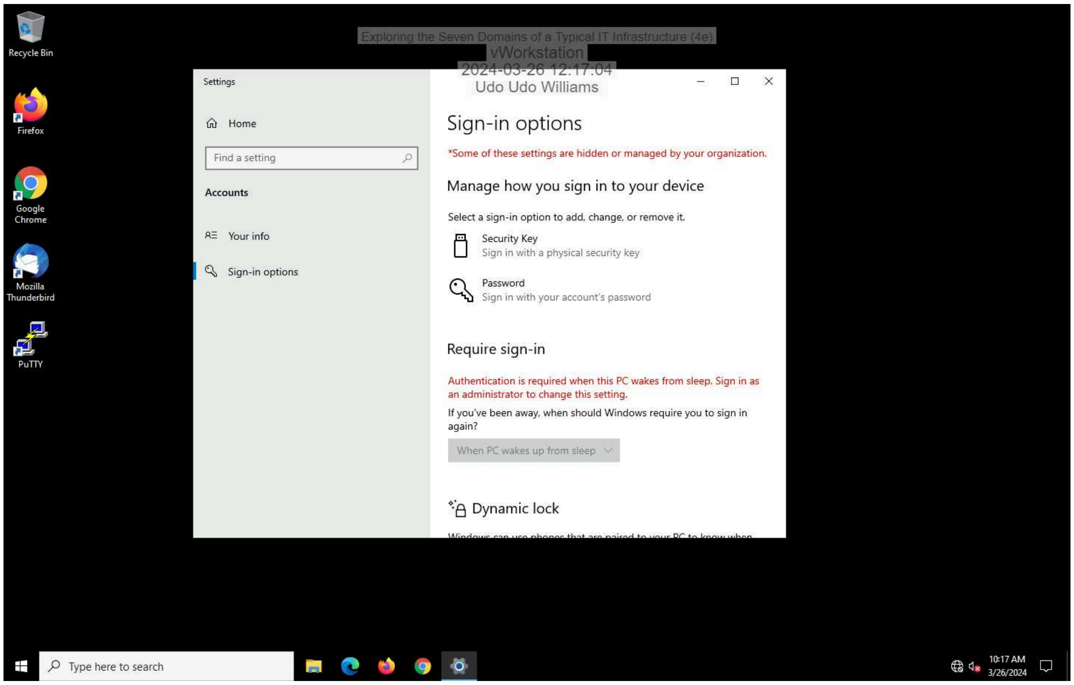
Time on Task: 21 hours, 24 minutes	Progress: 100%

Report Generated: Tuesday, March 26, 2024 at 5:09 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**.



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 12:17:04
Udo Udo Williams

Sign-in options

*Some of these settings are hidden or managed by your organization.

Manage how you sign in to your device

Select a sign-in option to add, change, or remove it.

Security Key
Sign in with a physical security key

Password
Sign in with your account's password

Require sign-in

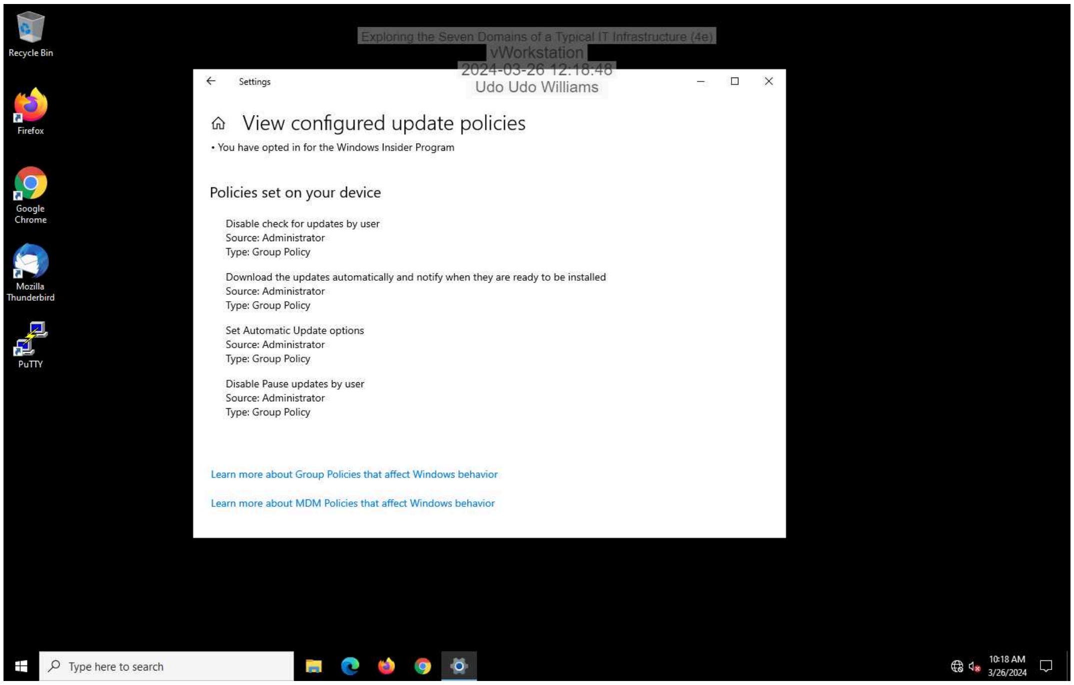
Authentication is required when this PC wakes from sleep. Sign in as an administrator to change this setting.

If you've been away, when should Windows require you to sign in again?

When PC wakes up from sleep

Dynamic lock

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 12:18:48
Udo Udo Williams

View configured update policies

• You have opted in for the Windows Insider Program

Policies set on your device

Disable check for updates by user
Source: Administrator
Type: Group Policy

Download the updates automatically and notify when they are ready to be installed
Source: Administrator
Type: Group Policy

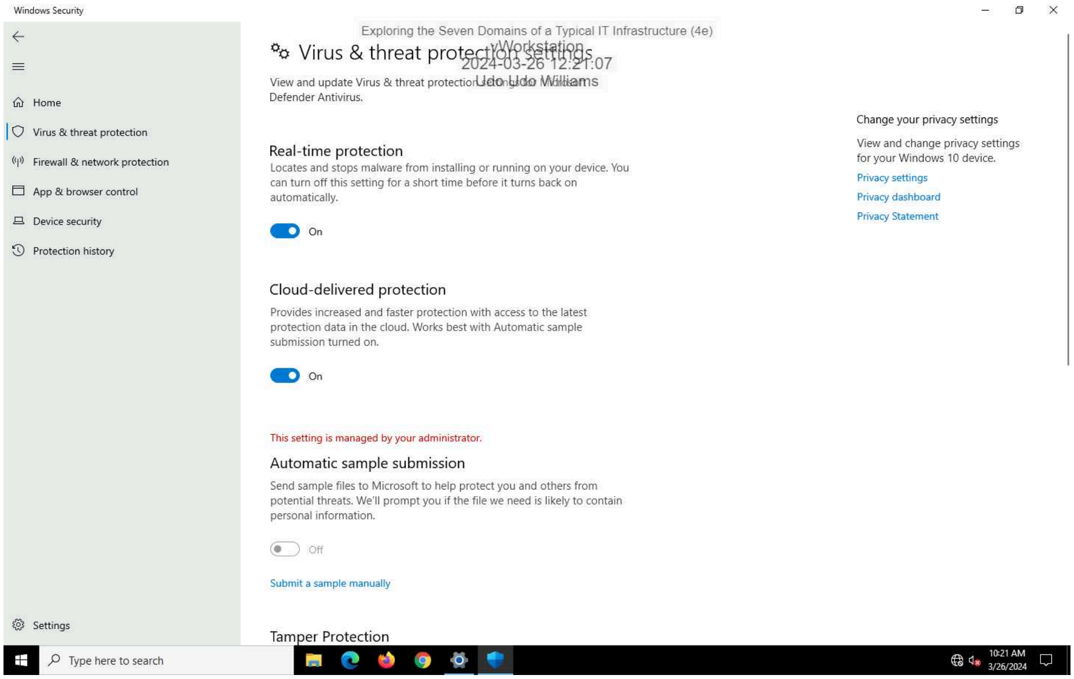
Set Automatic Update options
Source: Administrator
Type: Group Policy

Disable Pause updates by user
Source: Administrator
Type: Group Policy

Learn more about Group Policies that affect Windows behavior

Learn more about MDM Policies that affect Windows behavior

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 12:21:07
Udo Udo Williams

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.
On

Cloud-delivered protection
Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.
On

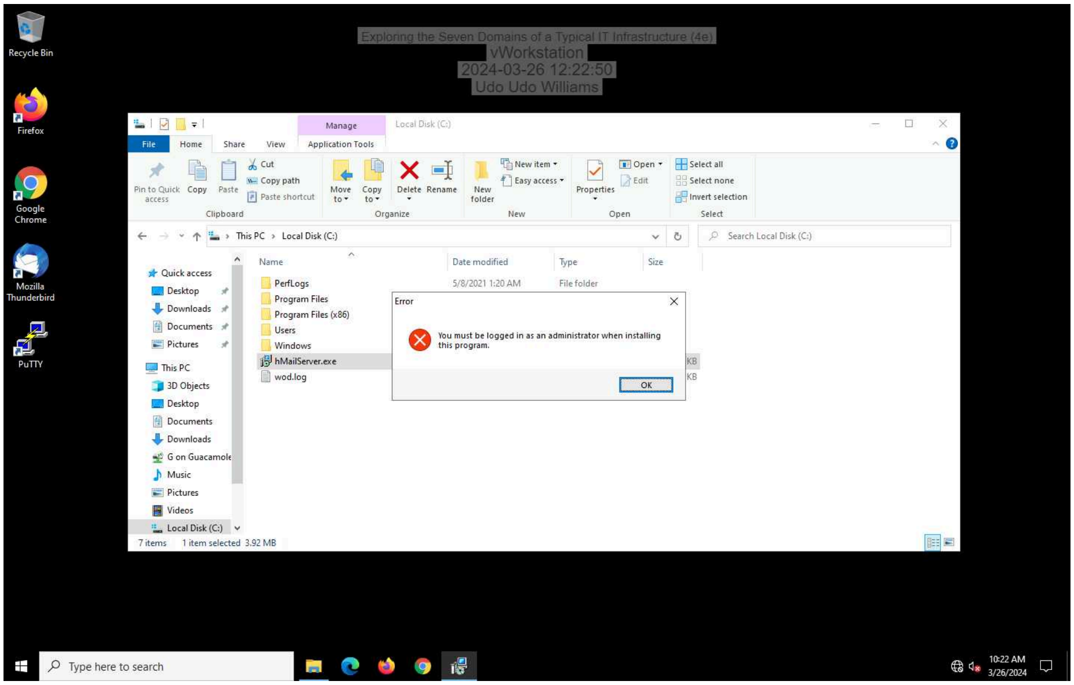
This setting is managed by your administrator.
Automatic sample submission
Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.
Off

Submit a sample manually

Tamper Protection

Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 12:22:50
Udo Udo Williams

Name	Date modified	Type	Size
PerfLogs	5/8/2021 1:20 AM	File folder	
Program Files			
Program Files (x86)			
Users			
Windows			
hMailServer.exe			KB
wod.log			KB

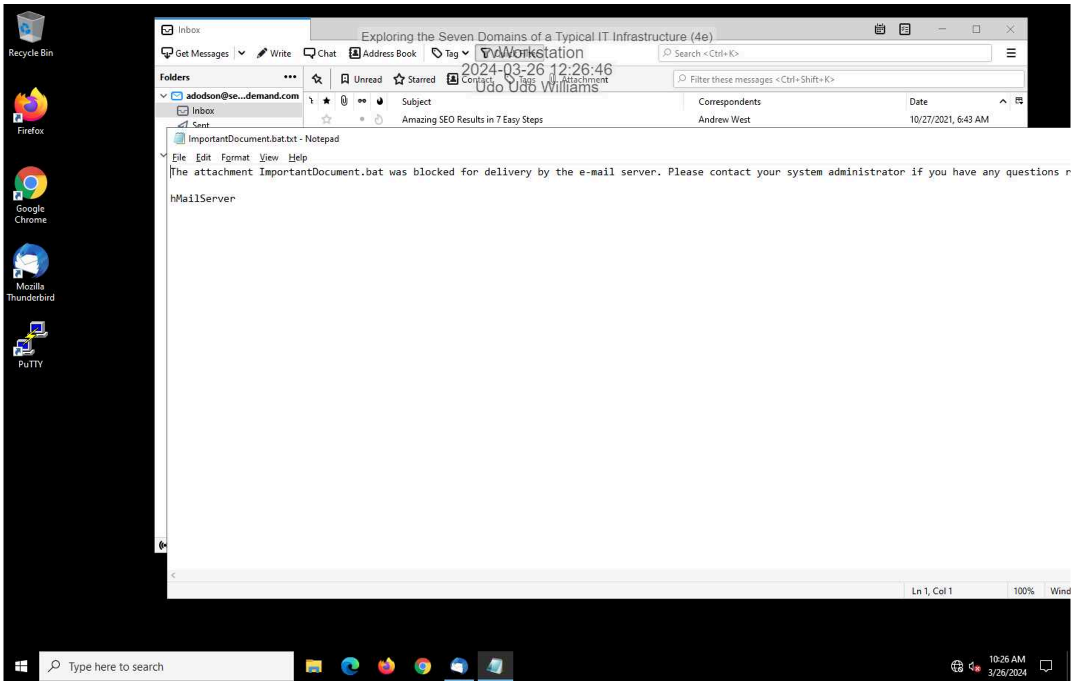
7 items 1 item selected 3.92 MB

Error

You must be logged in as an administrator when installing this program.

OK

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



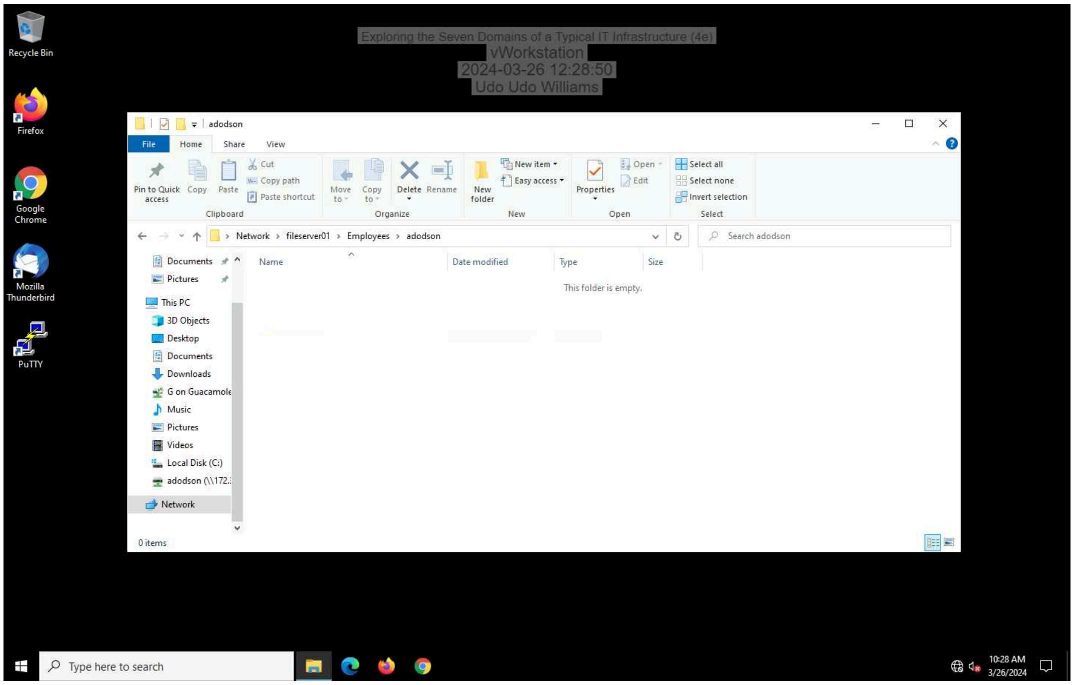
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 12:26:46
Udo Udo Williams

Subject	Correspondents	Date
Amazing SEO Results in 7 Easy Steps	Andrew West	10/27/2021, 6:43 AM

ImportantDocument.bat.txt - Notepad

```
The attachment ImportantDocument.bat was blocked for delivery by the e-mail server. Please contact your system administrator if you have any questions r

hMailServer
```

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 12:28:50
Udo Udo Williams

adodson

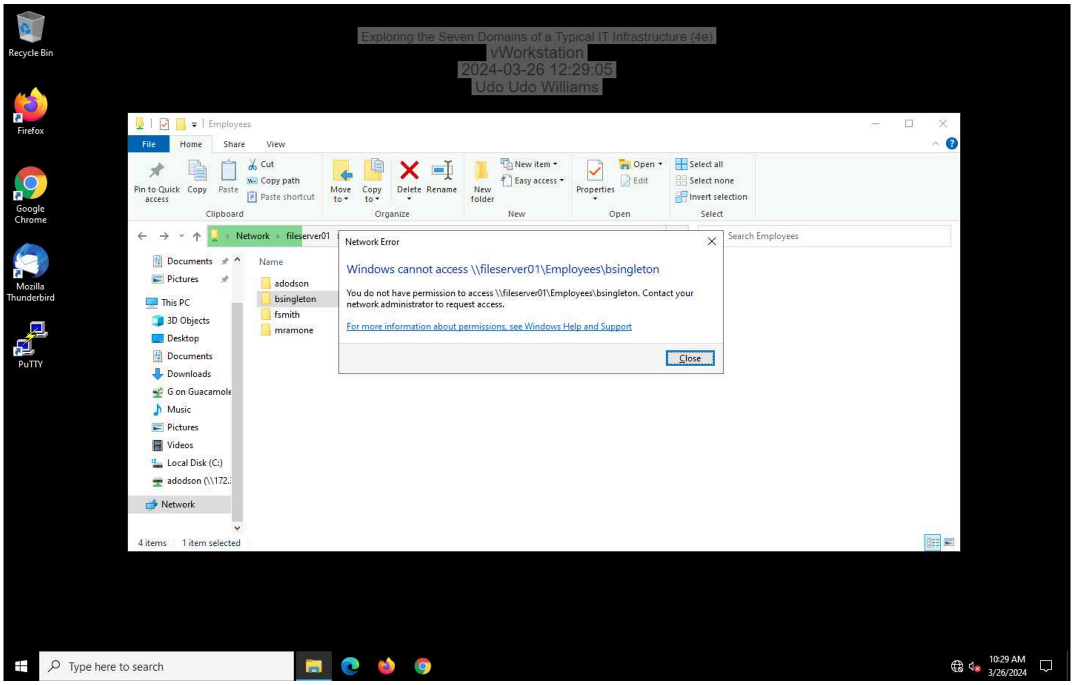
Network › fileserver01 › Employees › adodson

Name | Date modified | Type | Size

This folder is empty.

0 items

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 12:29:05
Udo Udo Williams

Employees

Network › fileserver01

Name

adodson
bsingleton
fsmith
mramone

Network Error

Windows cannot access \\fileserver01\Employees\bsingleton

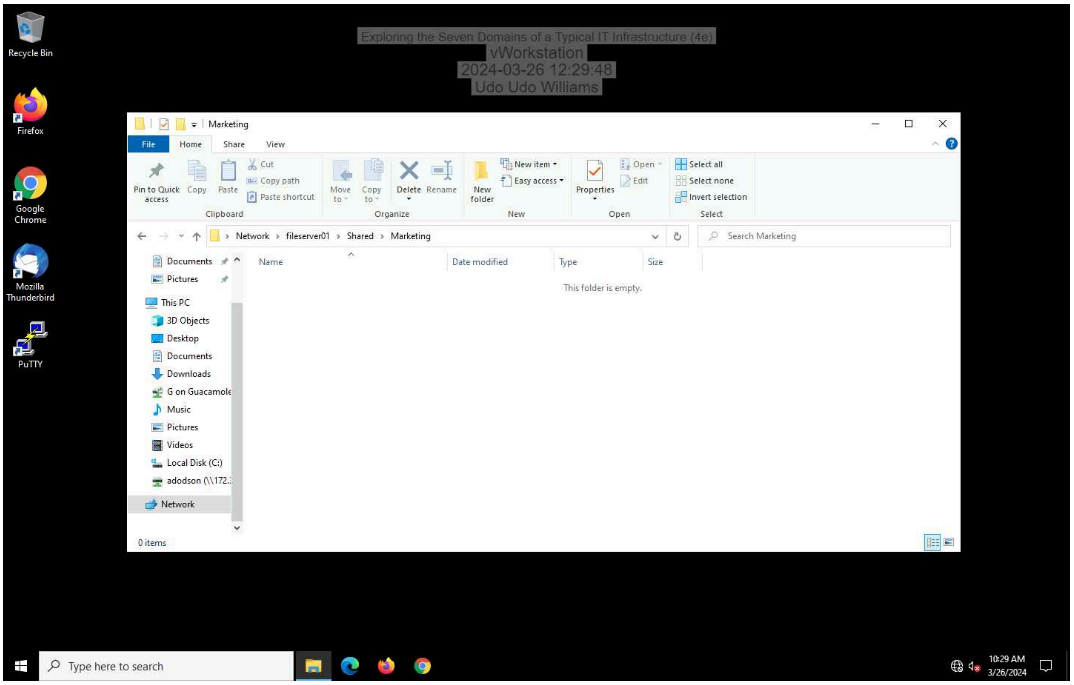
You do not have permission to access \\fileserver01\Employees\bsingleton. Contact your network administrator to request access.

For more information about permissions, see Windows Help and Support

Close

4 items 1 item selected

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



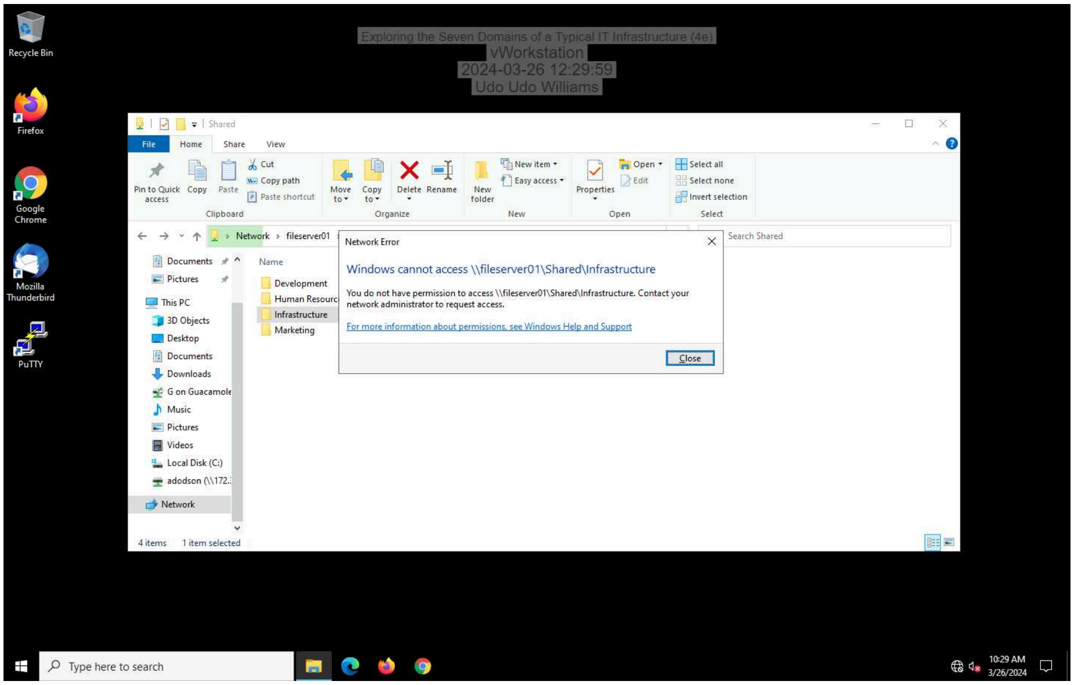
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 12:29:48
Udo Udo Williams

Network › fileserver01 › Shared › Marketing

This folder is empty.

0 items

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 12:29:59
Udo Udo Williams

Network › fileserver01

Network Error

Windows cannot access \\fileserver01\Shared\Infrastructure

You do not have permission to access \\fileserver01\Shared\Infrastructure. Contact your network administrator to request access.

For more information about permissions, see Windows Help and Support

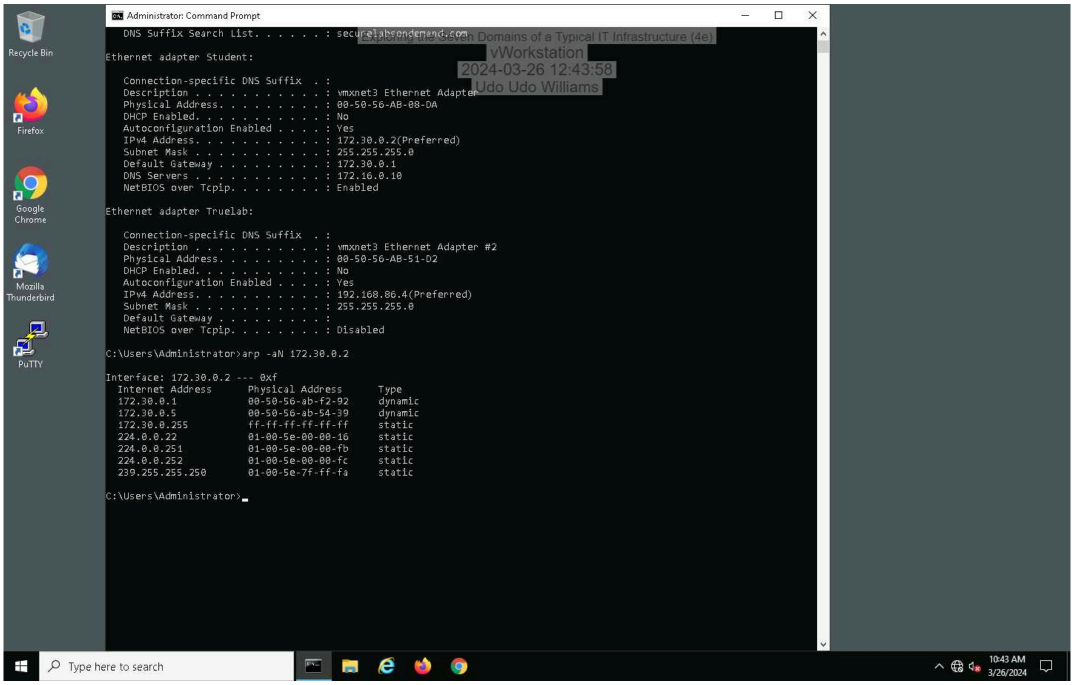
Close

Development
Human Resourc
Infrastructure
Marketing

4 items 1 item selected

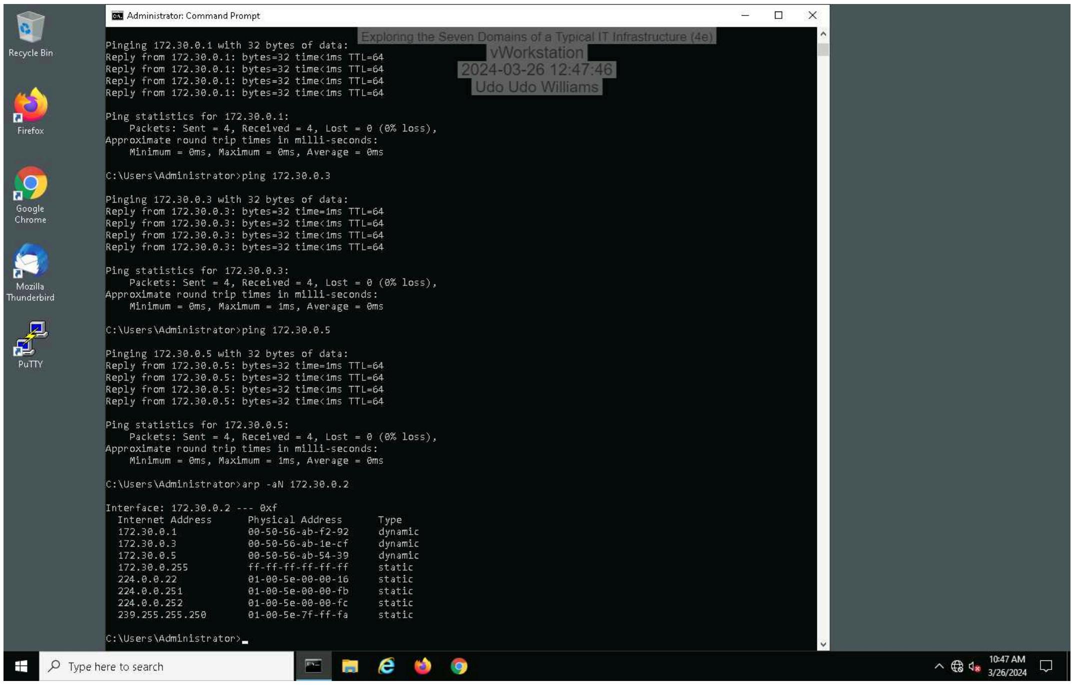
Part 2: Explore the LAN Domain

5. **Make a screen capture** showing the **vWorkstation’s original ARP table**.



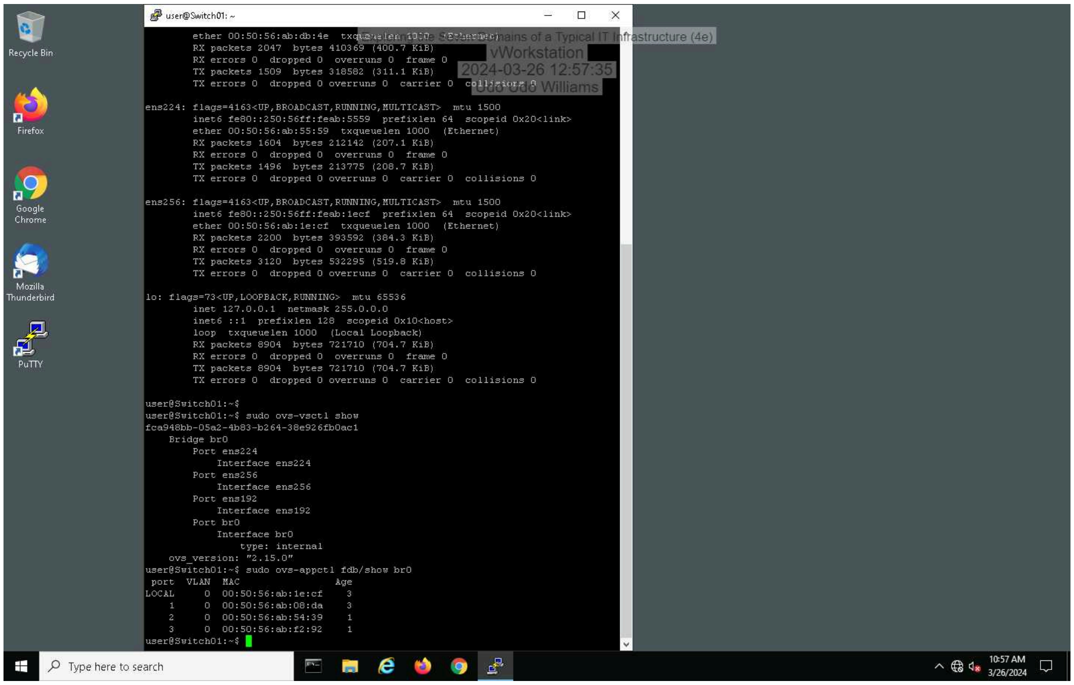
```
   DNS Suffix Search List. . . . . . : securelabsondemand.com

Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-AB-08-DA
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 172.30.0.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.30.0.1
   DNS Servers . . . . . . . . . . . : 172.16.0.10
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Truelab:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #2
   Physical Address. . . . . . . . . : 00-50-56-AB-51-D2
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.86.4(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   NetBIOS over Tcpip. . . . . . . . : Disabled

C:\Users\Administrator>arp -aN 172.30.0.2

Interface: 172.30.0.2 --- 0xf
  Internet Address      Physical Address      Type
  172.30.0.1            00-50-56-ab-f2-92     dynamic
  172.30.0.5            00-50-56-ab-54-39     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.**



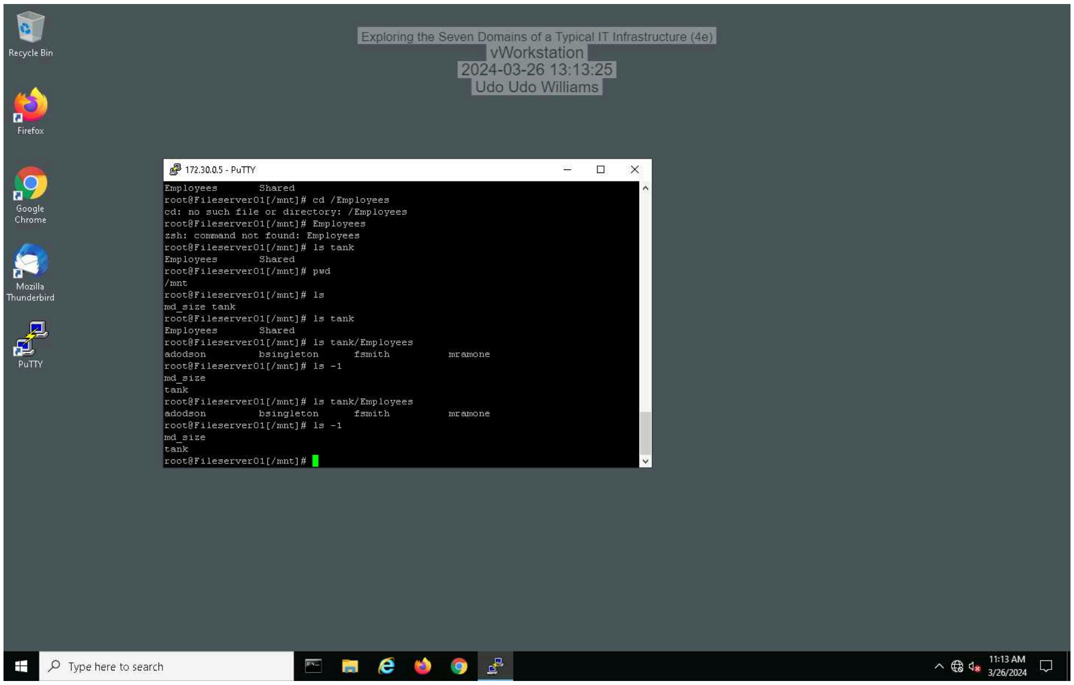
```
Pinging 172.30.0.1 with 32 bytes of data:
Reply from 172.30.0.1: bytes=32 time<1ms TTL=64
Reply from 172.30.0.1: bytes=32 time<1ms TTL=64
Reply from 172.30.0.1: bytes=32 time<1ms TTL=64
Reply from 172.30.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 172.30.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping 172.30.0.3

Pinging 172.30.0.3 with 32 bytes of data:
Reply from 172.30.0.3: bytes=32 time=1ms TTL=64
Reply from 172.30.0.3: bytes=32 time<1ms TTL=64
Reply from 172.30.0.3: bytes=32 time<1ms TTL=64
Reply from 172.30.0.3: bytes=32 time<1ms TTL=64

Ping statistics for 172.30.0.3:
    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>ping 172.30.0.5

Pinging 172.30.0.5 with 32 bytes of data:
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
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 -aN 172.30.0.2

Interface: 172.30.0.2 --- 0xf
  Internet Address      Physical Address      Type
  172.30.0.1            00-50-56-ab-f2-92     dynamic
  172.30.0.3            00-50-56-ab-1e-cf     dynamic
  172.30.0.5            00-50-56-ab-54-39     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**.



```
        ether 00:50:56:ab:db:4e  txqueuelen 1000  (Ethernet)
        RX packets 2047  bytes 410369 (400.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1509  bytes 318582 (311.1 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:5559  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:ab:55:59  txqueuelen 1000  (Ethernet)
        RX packets 1604  bytes 212142 (207.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1496  bytes 213775 (208.7 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:1ecf  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:ab:1e:cf  txqueuelen 1000  (Ethernet)
        RX packets 2200  bytes 393592 (384.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3120  bytes 532295 (519.8 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 8904  bytes 721710 (704.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8904  bytes 721710 (704.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

user@Switch01:~$
user@Switch01:~$ sudo ovs-vsctl show
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:~$ sudo ovs-appctl fdb/show br0
 port  VLAN  MAC                Age
LOCAL     0  00:50:56:ab:1e:cf    3
    1     0  00:50:56:ab:08:da    3
    2     0  00:50:56:ab:54:39    1
    3     0  00:50:56:ab:f2:92    1
user@Switch01:~$
```

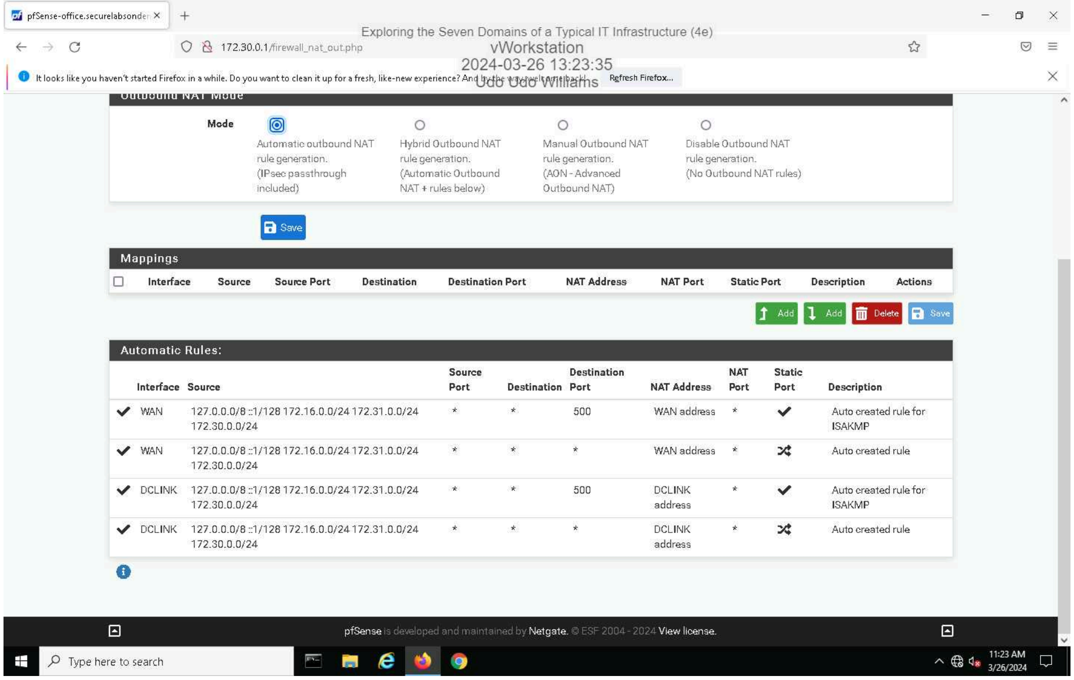
30. **Make a screen capture** showing the **contents of the Employees directory**.



```
Employees       Shared
root@Fileserver01[/mnt]# cd /Employees
cd: no such file or directory: /Employees
root@Fileserver01[/mnt]# Employees
zsh: command not found: Employees
root@Fileserver01[/mnt]# ls tank
Employees       Shared
root@Fileserver01[/mnt]# pwd
/mnt
root@Fileserver01[/mnt]# ls
md_size tank
root@Fileserver01[/mnt]# ls tank
Employees       Shared
root@Fileserver01[/mnt]# ls tank/Employees
adodson         bsingleton      fsmith          mramone
root@Fileserver01[/mnt]# ls -1
md_size
tank
root@Fileserver01[/mnt]# ls tank/Employees
adodson         bsingleton      fsmith          mramone
root@Fileserver01[/mnt]# ls -1
md_size
tank
root@Fileserver01[/mnt]#
```

Part 3: Explore the LAN-to-WAN Domain

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



pfSense-office.securelabsonder ✕

172.30.0.1/firewall_nat_out.php

Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 13:23:35
Udo Udo Williams

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! Refresh Firefox...

Outbound NAT Mode

Mode

● Automatic outbound NAT rule generation. (IPsec passthrough included)
○ Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
○ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
○ Disable Outbound NAT rule generation. (No Outbound NAT rules)

Save

Mappings

□	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions

Add Add Delete Save

Automatic Rules:

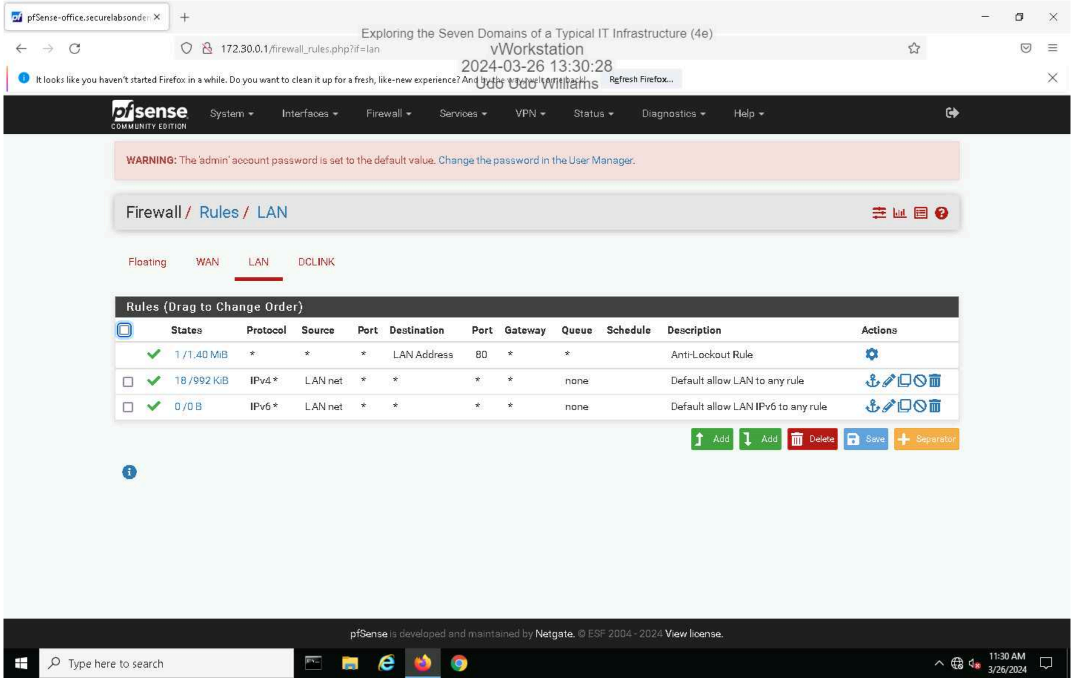
	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓	WAN	127.0.0.0/8 ::1/128 172.16.0.0/24 172.31.0.0/24 172.30.0.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓	WAN	127.0.0.0/8 ::1/128 172.16.0.0/24 172.31.0.0/24 172.30.0.0/24	*	*	*	WAN address	*	🔀	Auto created rule
✓	DCLINK	127.0.0.0/8 ::1/128 172.16.0.0/24 172.31.0.0/24 172.30.0.0/24	*	*	500	DCLINK address	*	✓	Auto created rule for ISAKMP
✓	DCLINK	127.0.0.0/8 ::1/128 172.16.0.0/24 172.31.0.0/24 172.30.0.0/24	*	*	*	DCLINK address	*	🔀	Auto created rule

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

Type here to search

11:23 AM
3/26/2024

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



pfSense-office.securelabsonder ✕

172.30.0.1/firewall_rules.php?if=lan

Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 13:30:28
Udo Udo Williams

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! Refresh Firefox...

pfsense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

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

Firewall / Rules / LAN

Floating WAN LAN DCLINK

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1 /1.40 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
□	✓	18 /992 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

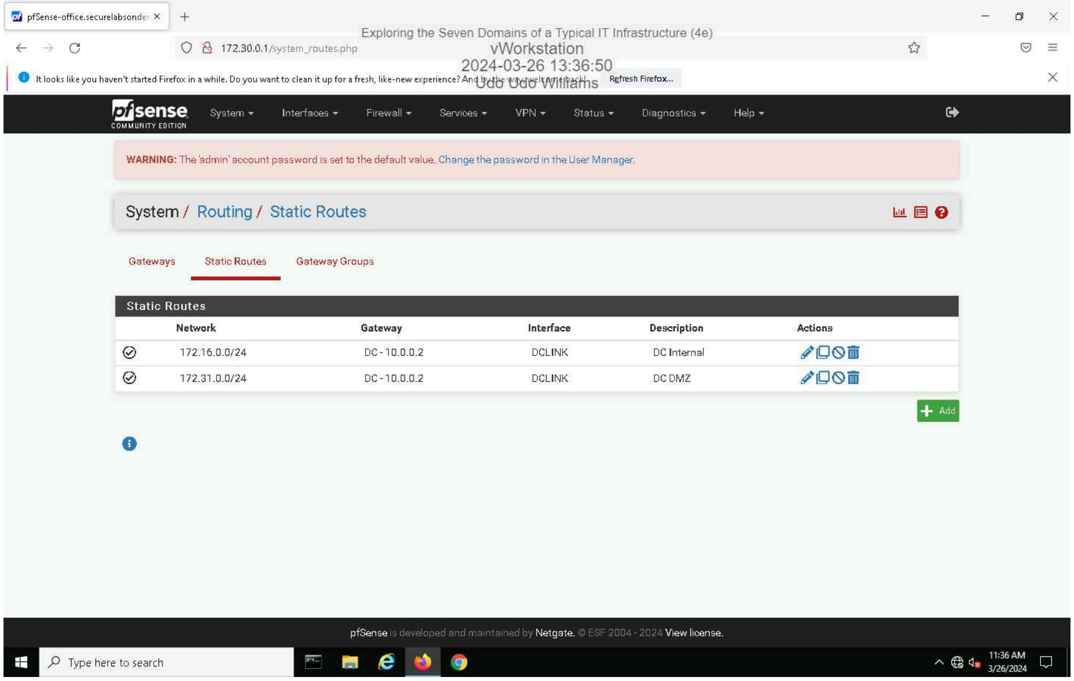
Add Add Delete Save Separator

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

Type here to search

11:30 AM
3/26/2024

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



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!

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

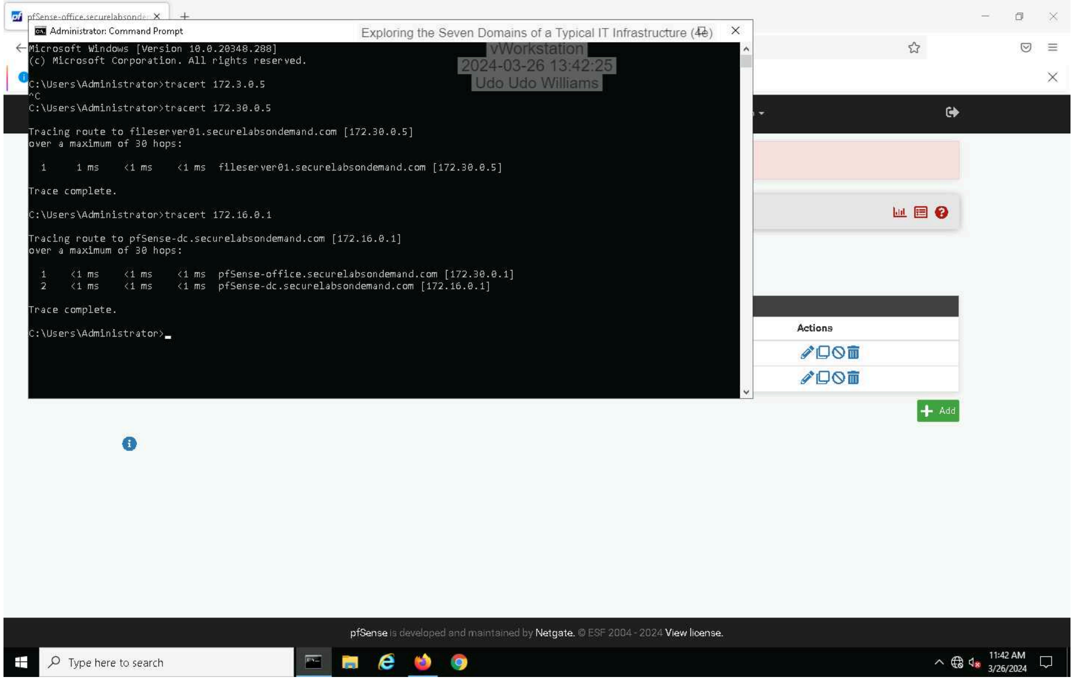
System / Routing / Static Routes

Static Routes

	Network	Gateway	Interface	Description	Actions
✓	172.16.0.0/24	DC - 10.0.0.2	DCLINK	DC Internal	
✓	172.31.0.0/24	DC - 10.0.0.2	DCLINK	DC DMZ	

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

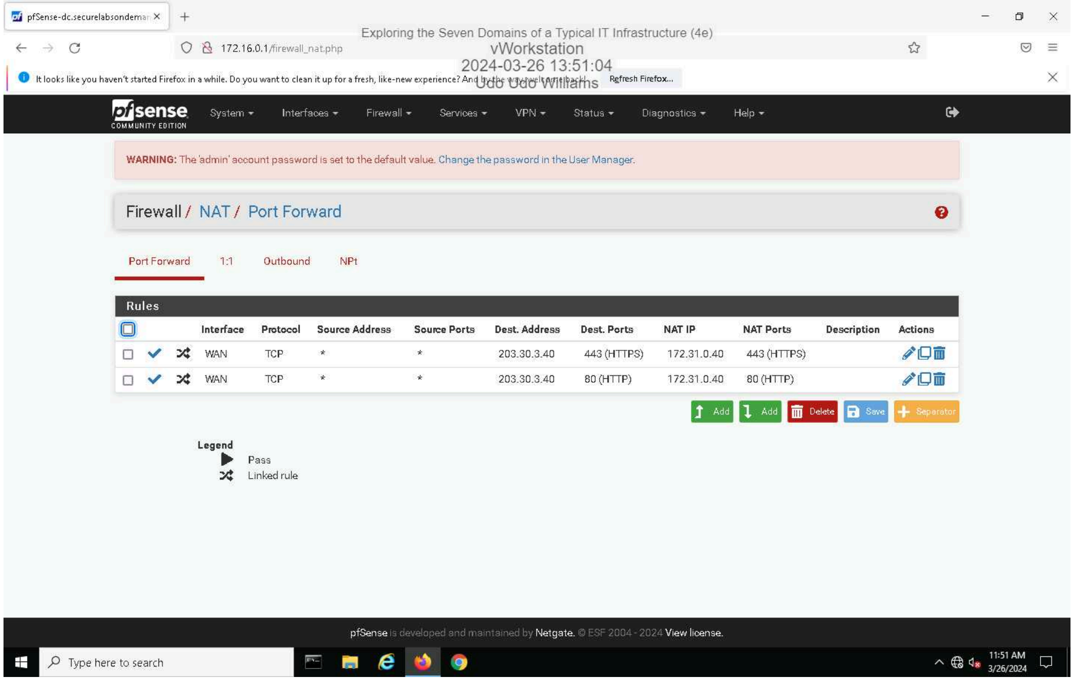
16. **Make a screen capture** showing the **result of your tracert to the pfsense-dc appliance**.


pfSense-office.securelabsonde
Administrator: Command Prompt
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 13:42:25
Udo Udo Williams
Actions
Add
Type here to search
11:42 AM
3/26/2024

```
Microsoft Windows [Version 10.0.20348.288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>tracert 172.3.0.5
^C
C:\Users\Administrator>tracert 172.30.0.5

Tracing route to fileserver01.securelabsondemand.com [172.30.0.5]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  fileserver01.securelabsondemand.com [172.30.0.5]

Trace complete.

C:\Users\Administrator>tracert 172.16.0.1

Tracing route to pfSense-dc.securelabsondemand.com [172.16.0.1]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  pfSense-office.securelabsondemand.com [172.30.0.1]
  2    <1 ms    <1 ms    <1 ms  pfSense-dc.securelabsondemand.com [172.16.0.1]

Trace complete.

C:\Users\Administrator>
```

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

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 13:51:04
Udo Udo Williams

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!

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

Firewall / NAT / Port Forward

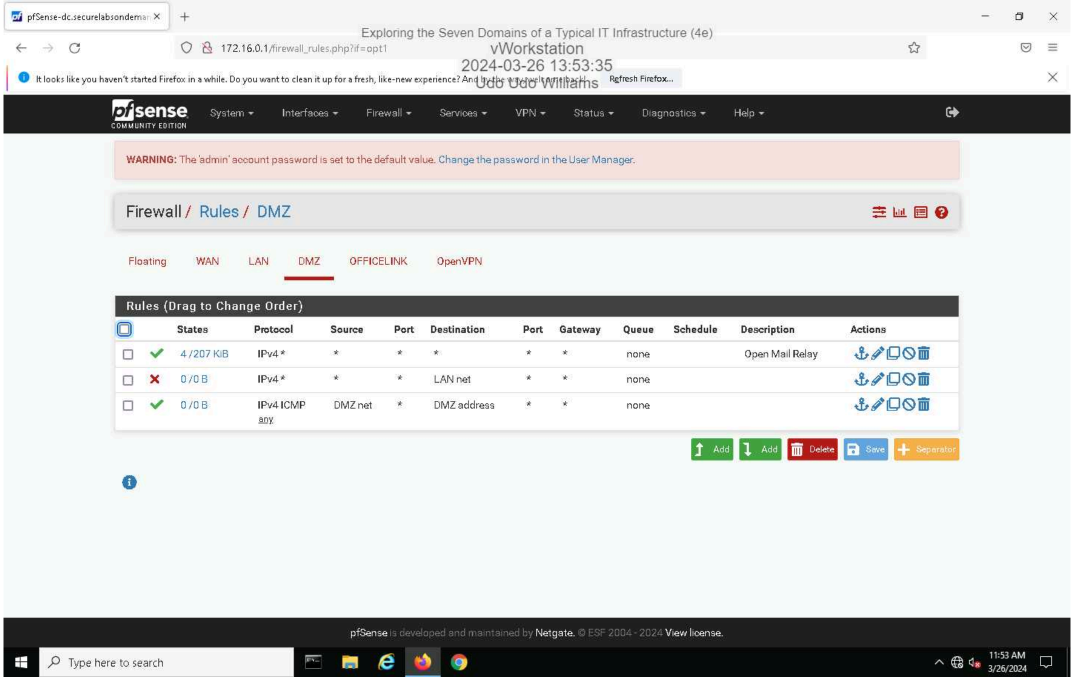
Rules

□			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓	⤮	WAN	TCP	*	*	203.30.3.40	443 (HTTPS)	172.31.0.40	443 (HTTPS)		
□	✓	⤮	WAN	TCP	*	*	203.30.3.40	80 (HTTP)	172.31.0.40	80 (HTTP)		

Legend
▶ Pass
⤮ Linked rule

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

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 13:53:35
Udo Udo Williams

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!

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

Firewall / Rules / DMZ

Rules (Drag to Change Order)

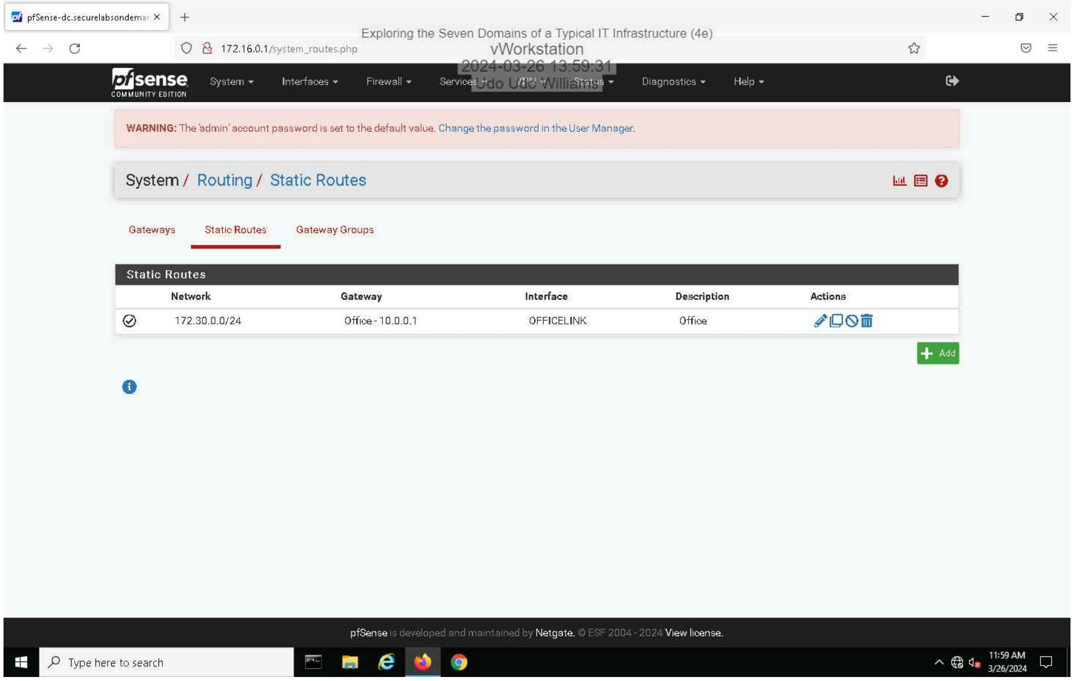
□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	4 /207 KiB	IPv4 *	*	*	*	*	*	none		Open Mail Relay	
□	✗	0 /0 B	IPv4 *	*	*	LAN net	*	*	none			
□	✓	0 /0 B	IPv4 ICMP any	DMZ net	*	DMZ address	*	*	none			

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

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**.



pfSense-dc.securelabsondeman
172.16.0.1/system_routes.php
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 13:59:31
Udo Udo Williams
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

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

System / Routing / Static Routes

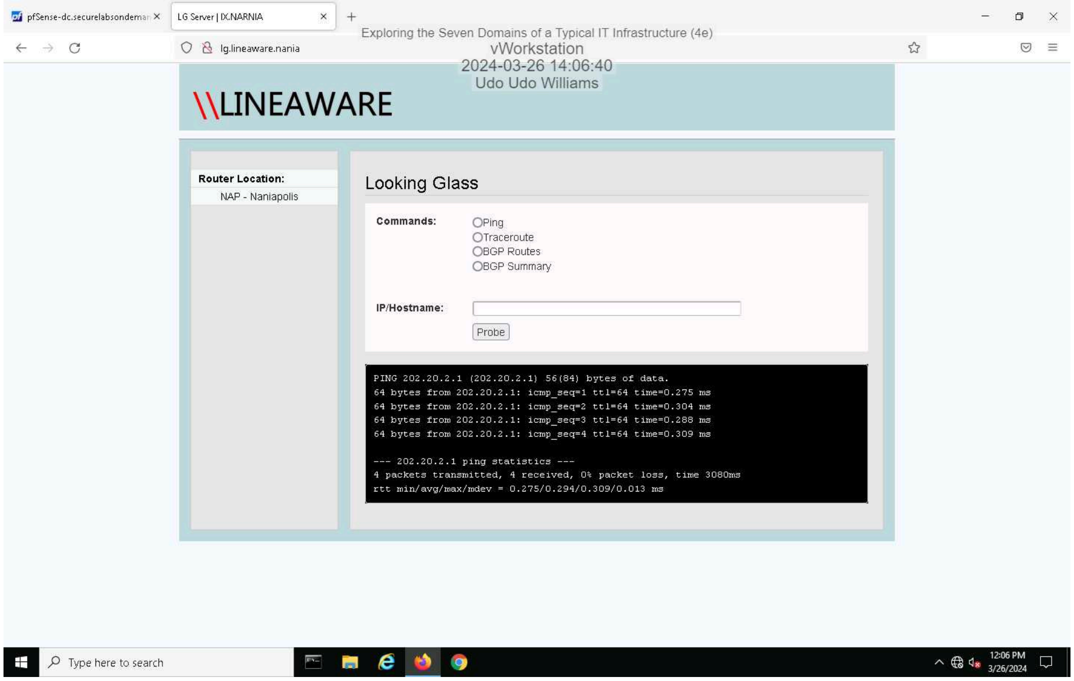
Gateways
Static Routes
Gateway Groups

Static Routes

	Network	Gateway	Interface	Description	Actions
✓	172.30.0.0/24	Office - 10.0.0.1	OFFICELINK	Office	

Add
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Type here to search
11:59 AM
3/26/2024

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



Router Location:
NAP - Naniapolis

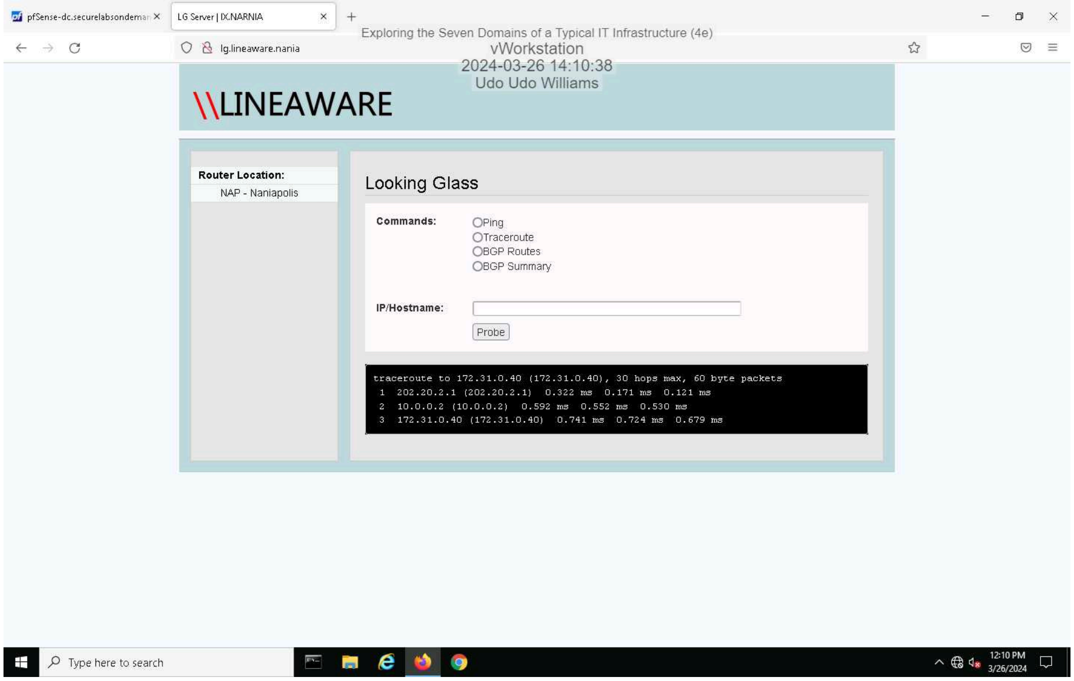
Looking Glass

Commands:
○Ping
○Traceroute
○BGP Routes
○BGP Summary

IP/Hostname:

```
PING 202.20.2.1 (202.20.2.1) 56(84) bytes of data.
64 bytes from 202.20.2.1: icmp_seq=1 ttl=64 time=0.275 ms
64 bytes from 202.20.2.1: icmp_seq=2 ttl=64 time=0.304 ms
64 bytes from 202.20.2.1: icmp_seq=3 ttl=64 time=0.288 ms
64 bytes from 202.20.2.1: icmp_seq=4 ttl=64 time=0.309 ms

--- 202.20.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3080ms
rtt min/avg/max/mdev = 0.275/0.294/0.309/0.013 ms
```

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

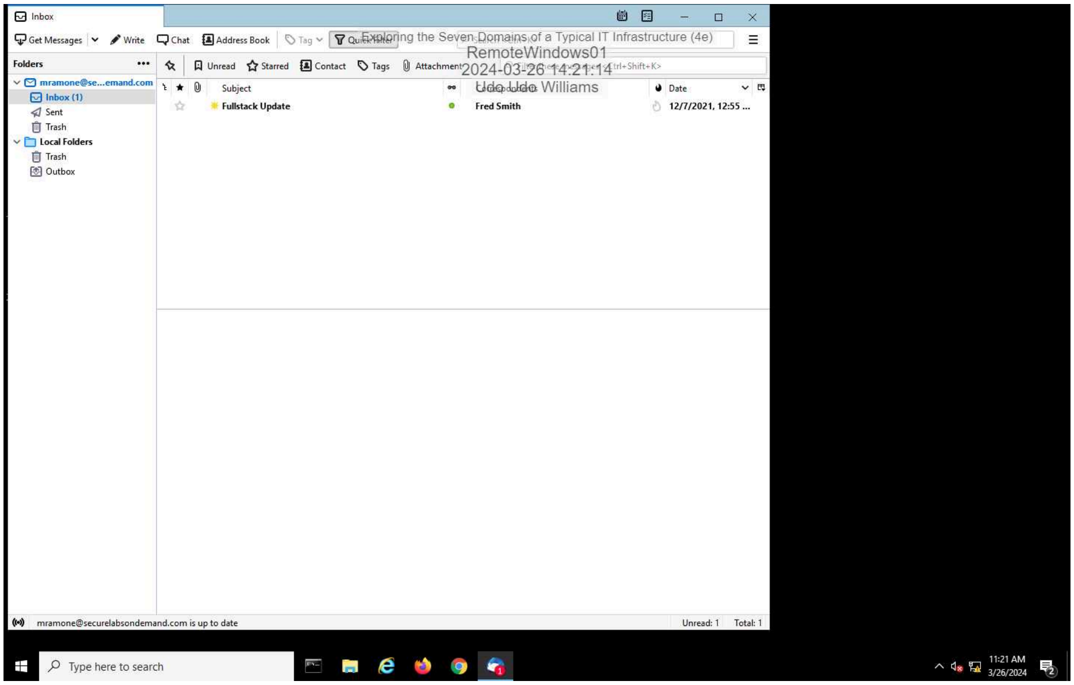


Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-03-26 14:10:38
Udo Udo Williams

```
traceroute to 172.31.0.40 (172.31.0.40), 30 hops max, 60 byte packets
 1  202.20.2.1 (202.20.2.1)  0.322 ms  0.171 ms  0.121 ms
 2  10.0.0.2 (10.0.0.2)  0.592 ms  0.552 ms  0.530 ms
 3  172.31.0.40 (172.31.0.40)  0.741 ms  0.724 ms  0.679 ms
```

Part 2: Explore the Remote Access Domain

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
RemoteWindows01
2024-03-26 14:21:14
Udo Udo Williams

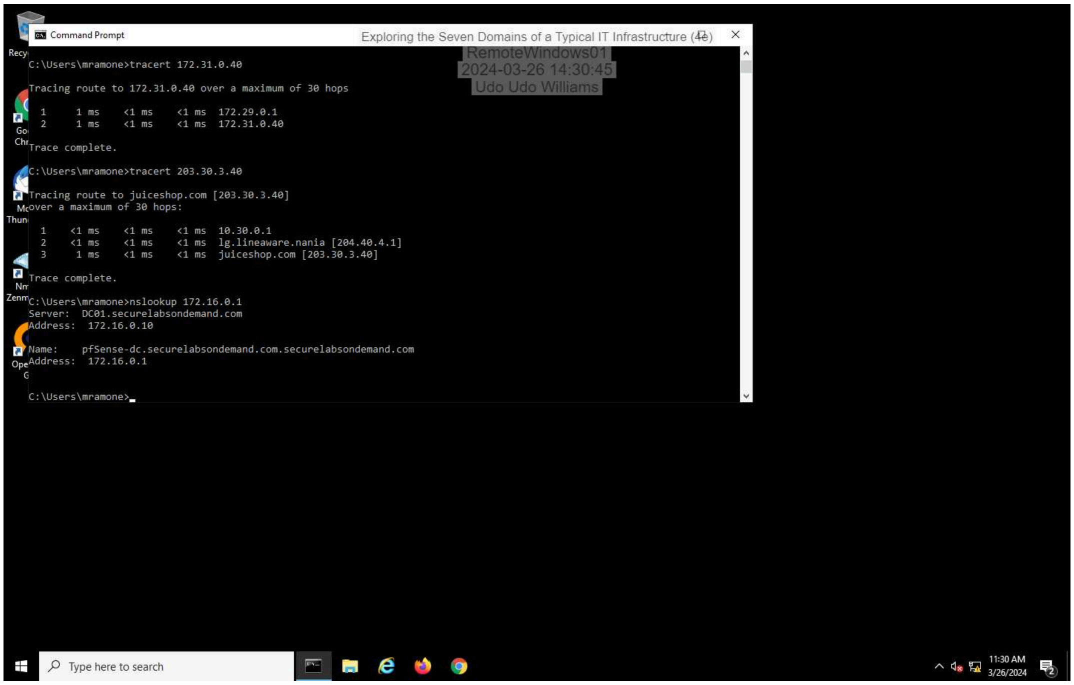
Fullstack Update — Fred Smith — 12/7/2021, 12:55 ...

mramone@securelabsondemand.com is up to date — Unread: 1 — Total: 1

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

split tunnel is enabled

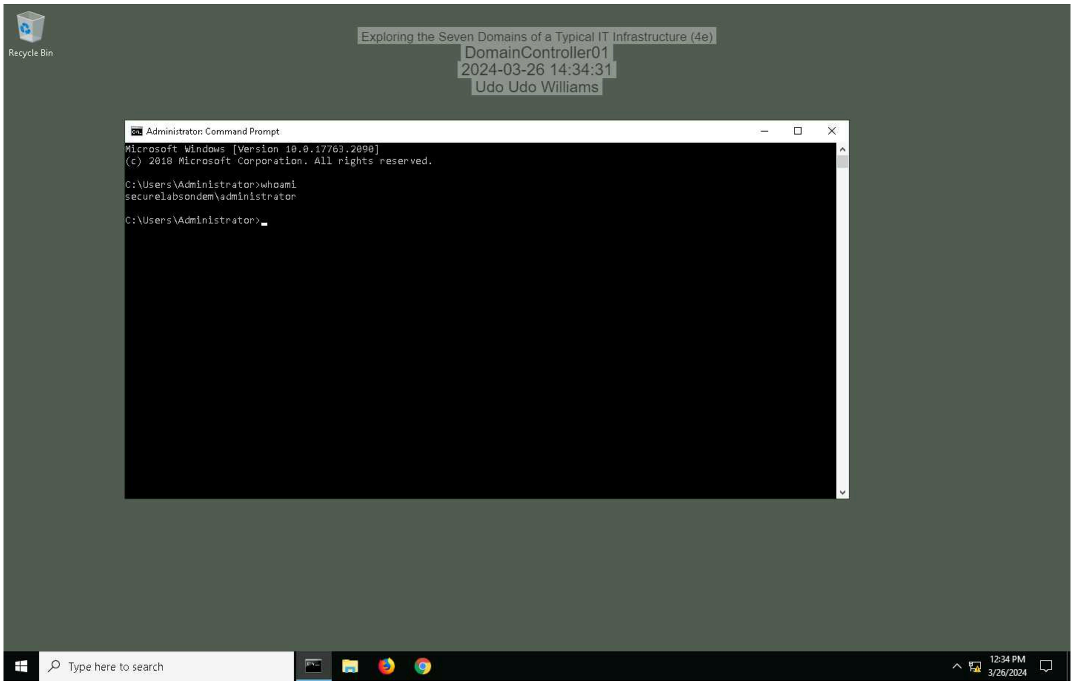
16. **Make a screen capture** showing the **successful reverse DNS lookup for the internal host**.



```
C:\Users\mramone>tracert 172.31.0.40

Tracing route to 172.31.0.40 over a maximum of 30 hops

  1     1 ms    <1 ms    <1 ms  172.29.0.1
  2     1 ms    <1 ms    <1 ms  172.31.0.40

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:

  1    <1 ms    <1 ms    <1 ms  10.30.0.1
  2    <1 ms    <1 ms    <1 ms  lg.lineaware.nania [204.40.4.1]
  3     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>
```

Part 3: Explore the System/Application Domain

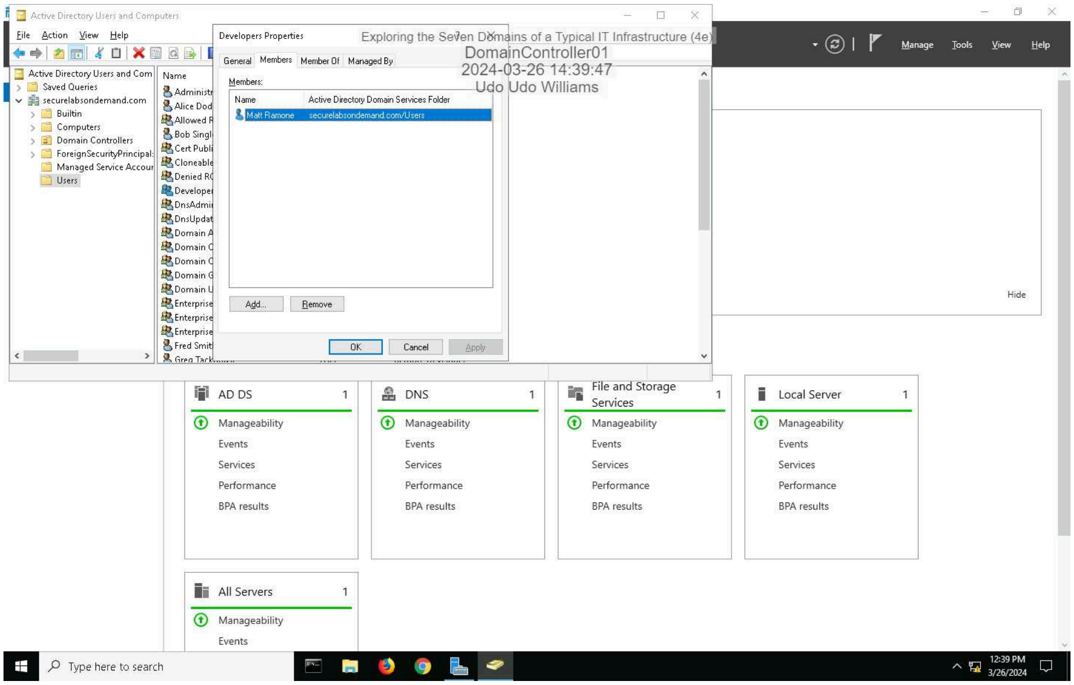
4. **Make a screen capture** showing the **whoami results**.



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
DomainController01
2024-03-26 14:34:31
Udo Udo Williams

```
Microsoft Windows [Version 10.0.17763.2090]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>whoami
securelabsondem\administrator

C:\Users\Administrator>_
```

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

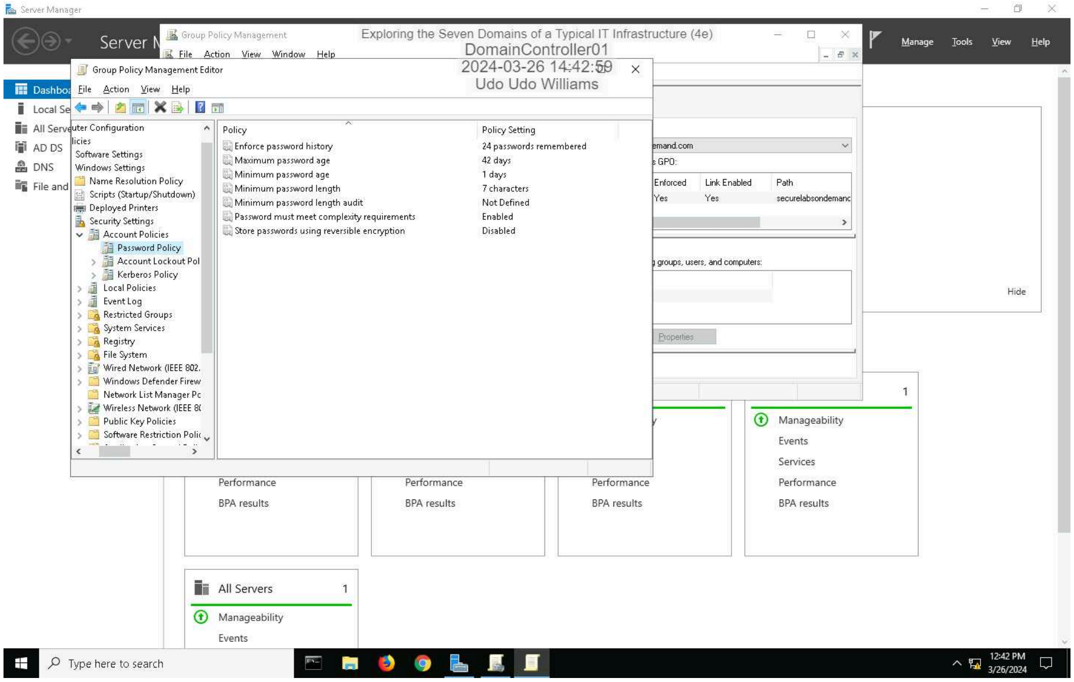


Exploring the Seven Domains of a Typical IT Infrastructure (4e)
DomainController01
2024-03-26 14:39:47
Udo Udo Williams

Members:

Name	Active Directory Domain Services Folder
Matt Ramone	securelabsondemand.com/Users

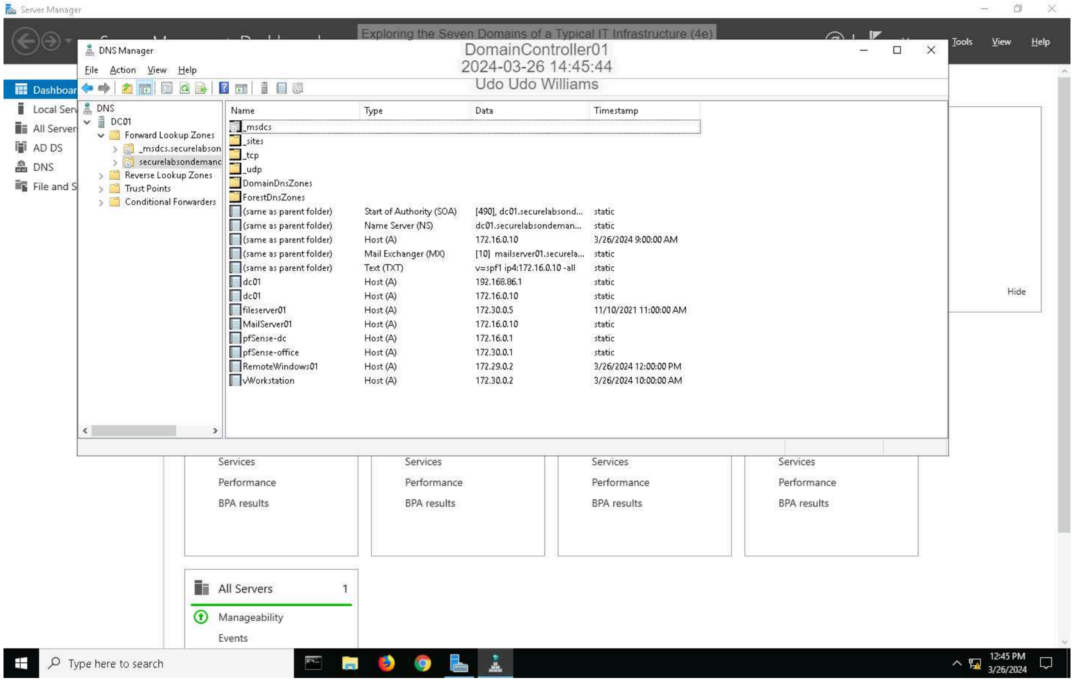
16. **Make a screen capture** showing the **password policy settings in the Group Policy Management Console**.



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
DomainController01
2024-03-26 14:42:59
Udo Udo Williams

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

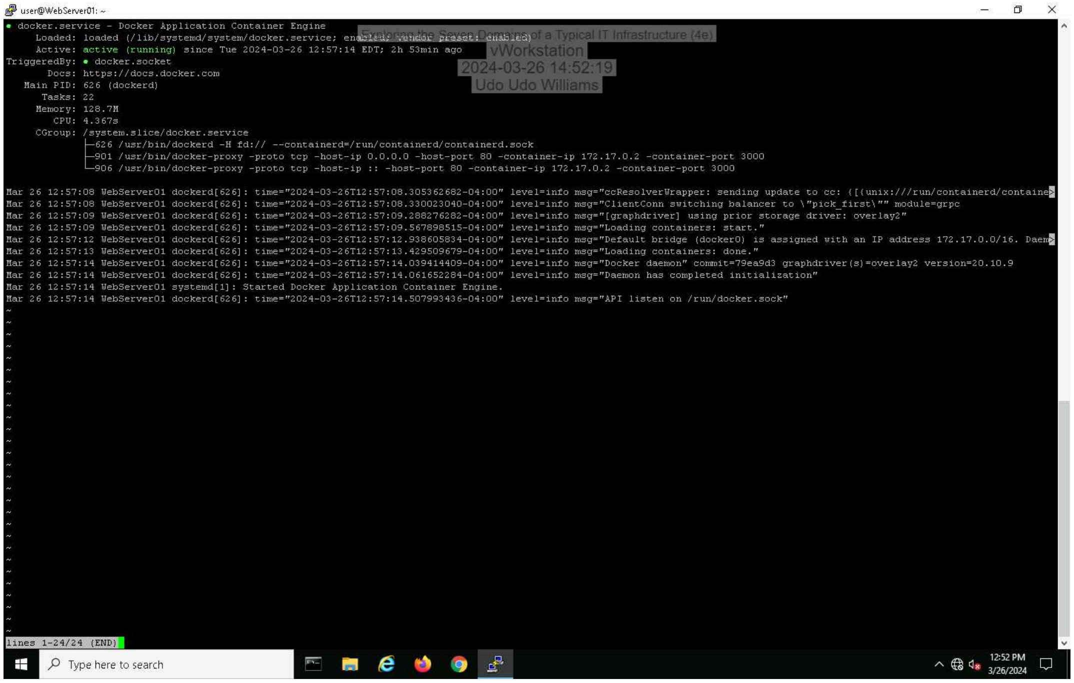
20. **Make a screen capture** showing the **DNS entries**.



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
DomainController01
2024-03-26 14:45:44
Udo Udo Williams

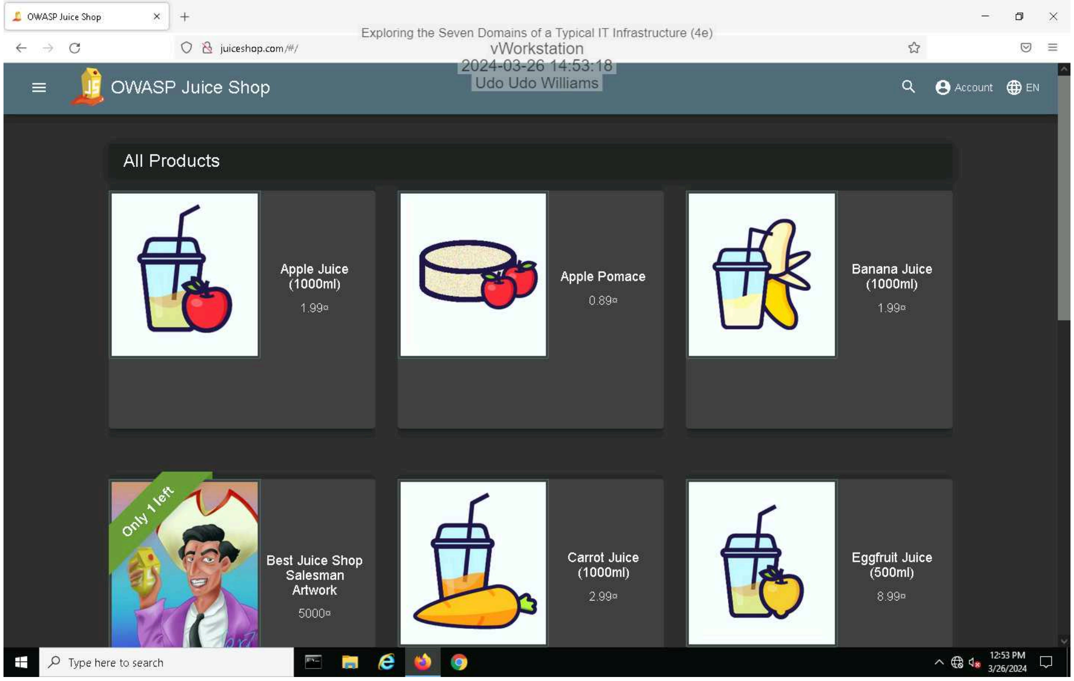
Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[490], dc01.securelabsond...	static
(same as parent folder)	Name Server (NS)	dc01.securelabsondeman...	static
(same as parent folder)	Host (A)	172.16.0.10	3/26/2024 9:00:00 AM
(same as parent folder)	Mail Exchanger (MX)	[10] mailserver01.securela...	static
(same as parent folder)	Text (TXT)	v=spf1 ip4:172.16.0.10 -all	static
dc01	Host (A)	192.168.86.1	static
dc01	Host (A)	172.16.0.10	static
fileserver01	Host (A)	172.30.0.5	11/10/2021 11:00:00 AM
MailServer01	Host (A)	172.16.0.10	static
pfSense-dc	Host (A)	172.16.0.1	static
pfSense-office	Host (A)	172.30.0.1	static
RemoteWindows01	Host (A)	172.29.0.2	3/26/2024 12:00:00 PM
vWorkstation	Host (A)	172.30.0.2	3/26/2024 10:00:00 AM

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

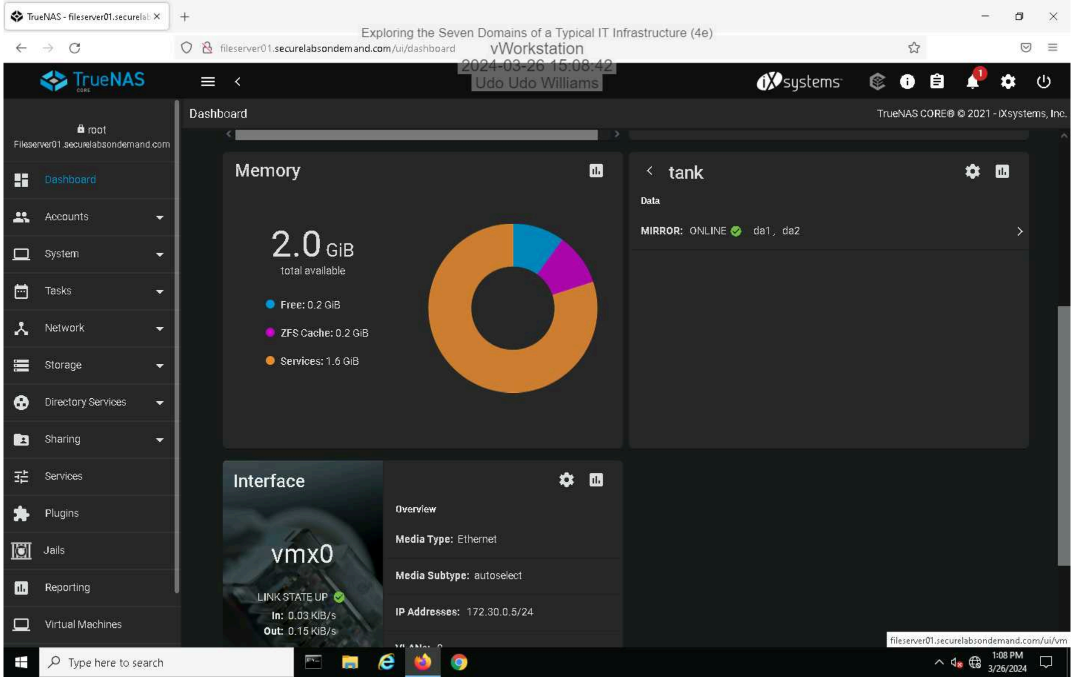


```
user@WebServer01: ~
● docker.service - Docker Application Container Engine
     Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2024-03-26 12:57:14 EDT; 2h 53min ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 626 (dockerd)
      Tasks: 22
     Memory: 128.7M
        CPU: 4.367s
     CGroup: /system.slice/docker.service
             ├─626 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
             ├─901 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 80 -container-ip 172.17.0.2 -container-port 3000
             └─906 /usr/bin/docker-proxy -proto tcp -host-ip :: -host-port 80 -container-ip 172.17.0.2 -container-port 3000

Mar 26 12:57:08 WebServer01 dockerd[626]: time="2024-03-26T12:57:08.305362682-04:00" level=info msg="ccResolverWrapper: sending update to cc: {[{unix:///run/containerd/containe>
Mar 26 12:57:08 WebServer01 dockerd[626]: time="2024-03-26T12:57:08.330023040-04:00" level=info msg="ClientConn switching balancer to \"pick_first\"" module=grpc
Mar 26 12:57:09 WebServer01 dockerd[626]: time="2024-03-26T12:57:09.288276282-04:00" level=info msg="[graphdriver] using prior storage driver: overlay2"
Mar 26 12:57:09 WebServer01 dockerd[626]: time="2024-03-26T12:57:09.567898515-04:00" level=info msg="Loading containers: start."
Mar 26 12:57:12 WebServer01 dockerd[626]: time="2024-03-26T12:57:12.938605834-04:00" level=info msg="Default bridge (docker0) is assigned with an IP address 172.17.0.0/16. Daem>
Mar 26 12:57:13 WebServer01 dockerd[626]: time="2024-03-26T12:57:13.429509679-04:00" level=info msg="Loading containers: done."
Mar 26 12:57:14 WebServer01 dockerd[626]: time="2024-03-26T12:57:14.039414409-04:00" level=info msg="Docker daemon" commit=79ea9d3 graphdriver(s)=overlay2 version=20.10.9
Mar 26 12:57:14 WebServer01 dockerd[626]: time="2024-03-26T12:57:14.061652284-04:00" level=info msg="Daemon has completed initialization"
Mar 26 12:57:14 WebServer01 systemd[1]: Started Docker Application Container Engine.
Mar 26 12:57:14 WebServer01 dockerd[626]: time="2024-03-26T12:57:14.507993436-04:00" level=info msg="API listen on /run/docker.sock"
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
lines 1-24/24 (END)
```

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



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


TrueNAS - fileserver01.securelab
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
fileserver01.securelabsondemand.com/ui/dashboard
vWorkstation
2024-03-26 15:08:42
Udo Udo Williams
TrueNAS CORE
iXsystems
root
Fileserver01.securelabsondemand.com
Dashboard
Accounts
System
Tasks
Network
Storage
Directory Services
Sharing
Services
Plugins
Jails
Reporting
Virtual Machines
Dashboard
TrueNAS CORE® © 2021 - iXsystems, Inc.
fileserver01.securelabsondemand.com/ui/vm
Type here to search
1:08 PM
3/26/2024

Memory

2.0 GiB
total available

● Free: 0.2 GiB
● ZFS Cache: 0.2 GiB
● Services: 1.6 GiB

tank

Data

MIRROR: ONLINE ✓ da1 , da2

Interface

vmx0

LINK STATE UP ✓
In: 0.03 KiB/s
Out: 0.15 KiB/s

Overview

Media Type: Ethernet

Media Subtype: autoselect

IP Addresses: 172.30.0.5/24

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 are phishing attacks and insider threats. Phishing attacks involve malicious actors attempting to deceive users into disclosing sensitive information or installing malware by posing as legitimate entities. Insider threats involve employees or contractors intentionally or unintentionally compromising security by abusing their access privileges or mishandling sensitive data. To protect the User Domain against phishing attacks, organizations can implement email filtering and spam detection systems to identify and block suspicious emails. Additionally, security awareness training educates users about the dangers of phishing and teaches them how to recognize and report suspicious emails, reducing the likelihood of falling victim to such attacks. To mitigate insider threats, organizations can implement role-based access controls (RBAC) to limit users' access to only the resources and information necessary to perform their job functions. Additionally, user activity monitoring solutions can detect and alert on unusual or suspicious behavior, enabling organizations to proactively identify and respond to potential insider threats before they escalate.
Divyaaradhya. (2018, January 15). What are Three Risks and Threats of the User Domain? [Blog post]. Retrieved from http://www.divyaaradhya.com/2018/01/15/what-are-three-risks-and-threats-of-the-user-domain/
Bolster. (n.d.). Domain Security Risks. Retrieved from https://bolster.ai/blog/domain-security-risks
TechTarget. (n.d.). Top 10 types of information security threats for IT teams. Retrieved from https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams

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.

Here are the recommendations I would propose for the six domains.
Workstation Domain: Anitvirus and Anti Malware Endpoint protection software, such as antivirus and anti-malware solutions, can be implemented on workstations to detect and prevent various types of malware infections. LAN Domain: Network Access Control (NAC) solutions enforce security policies on devices attempting to connect to the local area network (LAN). NAC systems authenticate users and devices, assess their compliance. By implementing NAC, organizations can ensure that only authorized and properly configured devices gain access to the LAN, reducing the risk of unauthorized access and network breaches.LAN-to-WAN Domain: Next-Generation Firewalls NGFWs inspect network traffic at the application layer, allowing organizations to enforce granular security policies based on application type, user identity, and content. These firewalls can detect and block malicious activities, such as intrusions, malware downloads, and data exfiltration attempts, at the boundary between the LAN and the wide area network.WAN Domain: Encryption VPNs encrypt data transmitted between remote locations and central network resources, protecting it from interception or eavesdropping by unauthorized parties. Remote Access Domain: Multi-Factor Authentication adds an extra layer of security to remote access solutions by requiring users to verify their identities using multiple factors, such as passwords, biometrics, and one-time codes. System/Application Domain: Application Whitelisting By defining a list of approved applications and blocking all others from running, organizations can prevent the execution of malicious or unauthorized software, including malware and potentially unwanted programs. To begin building a strong domain network infrastructure, these basic additions can be made to harden the security posture of the 6 domains.
Allied Telesis. (n.d.). Solutions: LAN/WAN Protection. Retrieved from
https://www.alliedtelesis.com/us/en/solution-guide/solutions-lan-wan-protection
Scientific Research Publishing. (n.d.). Paper Information. Retrieved from
https://www.scirp.org/journal/paperinformation?paperid=80763