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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

Student:	Email:
Brandon Trinkle	btrinkle52@gmail.com

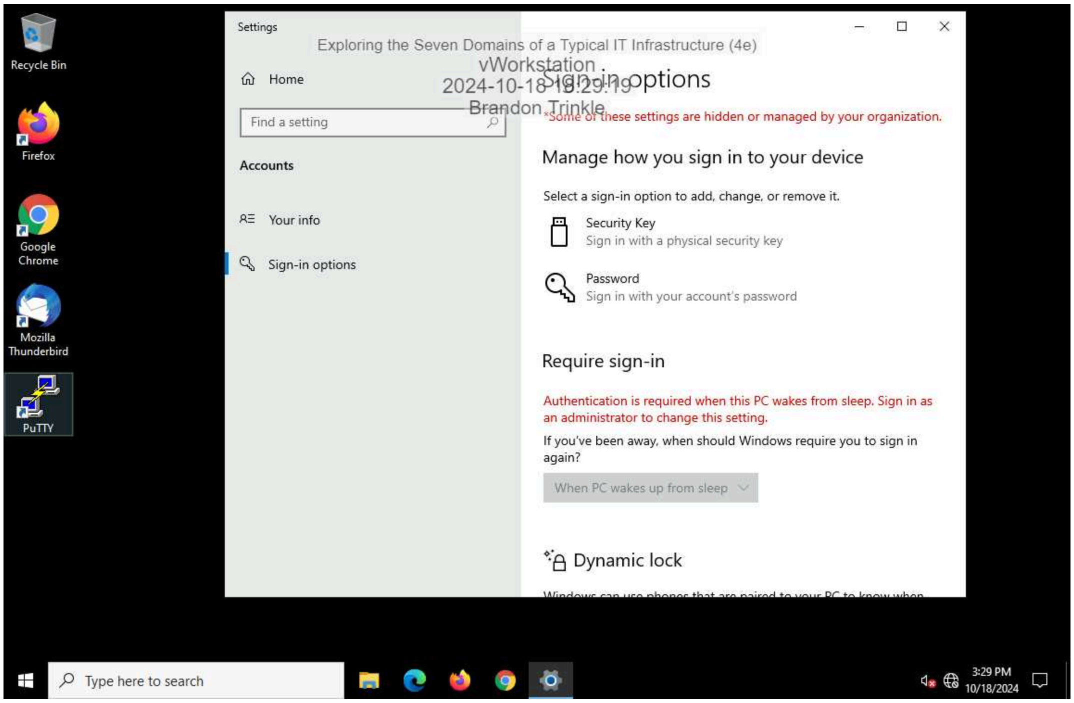
Time on Task:	Progress:
4 hours, 10 minutes	100%

Report Generated: Friday, October 18, 2024 at 7:04 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
2024-10-18 18:29:19
Brandon Trinkle

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.

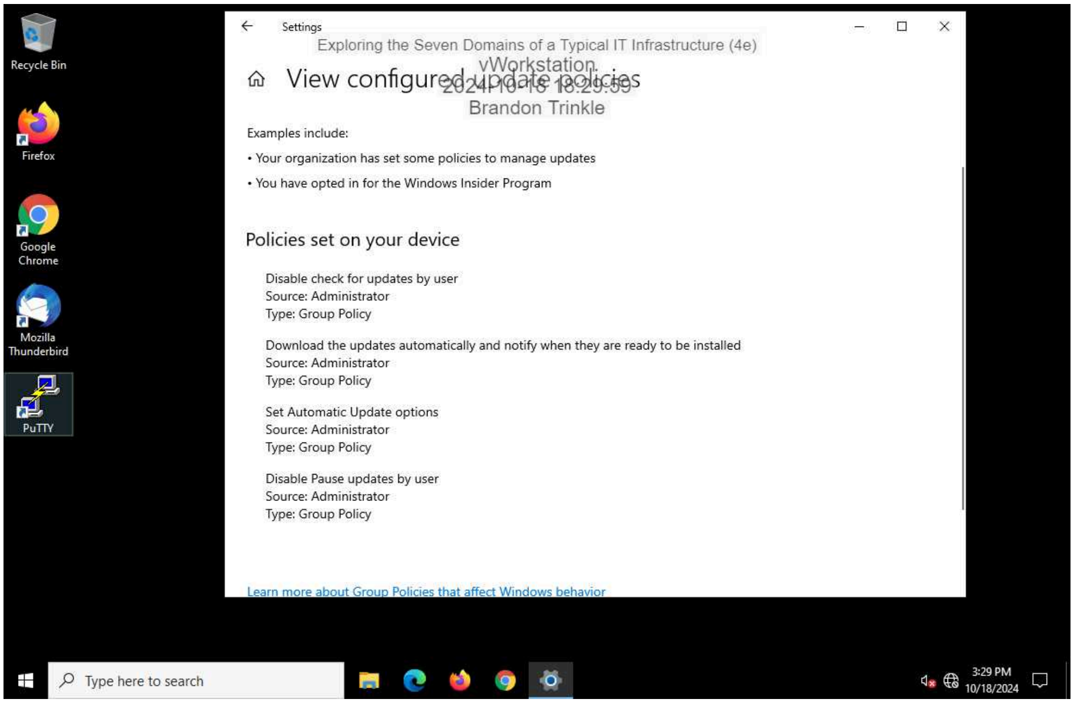
If you've been away, when should Windows require you to sign in again?

When PC wakes up from sleep

Dynamic lock

Windows can use phones that are paired to your PC to know when

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



Settings

Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:29:59
Brandon Trinkle

View configured update policies

Examples include:

- Your organization has set some policies to manage updates
- 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

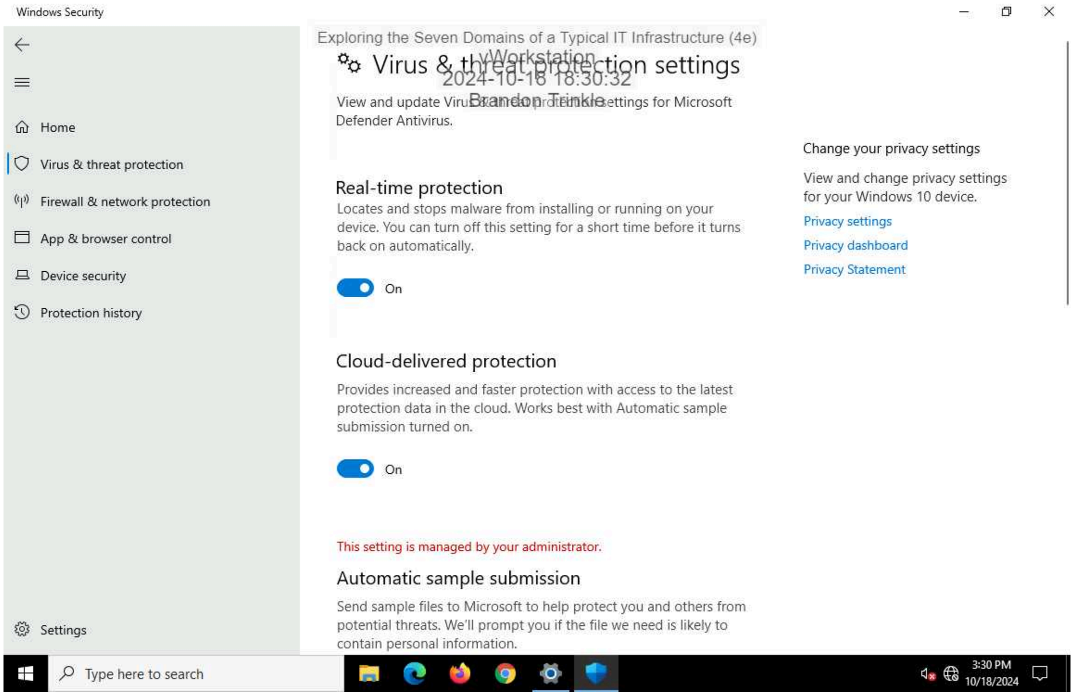
Download the updates automatically and notify when they are ready to be installed
Source: Administrator
Type: Group Policy

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

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



Windows Security

Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:30:32
Brandon Trinkle

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

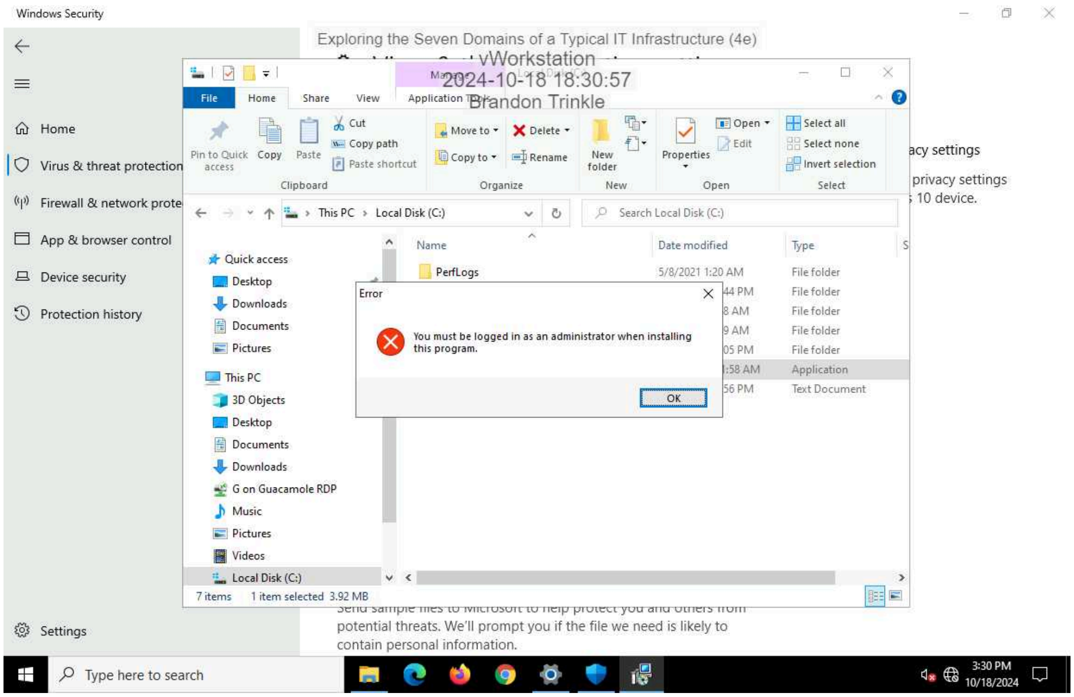
Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

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
2024-10-18 18:30:57
Brandon Trinkle

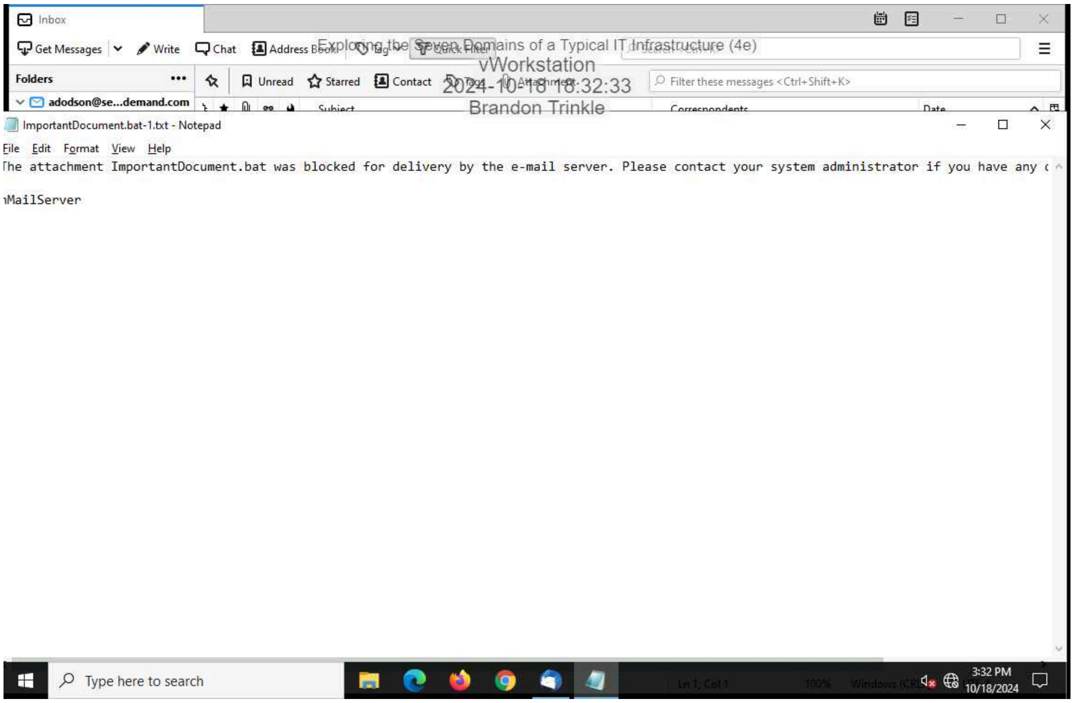
Error

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

OK

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.

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

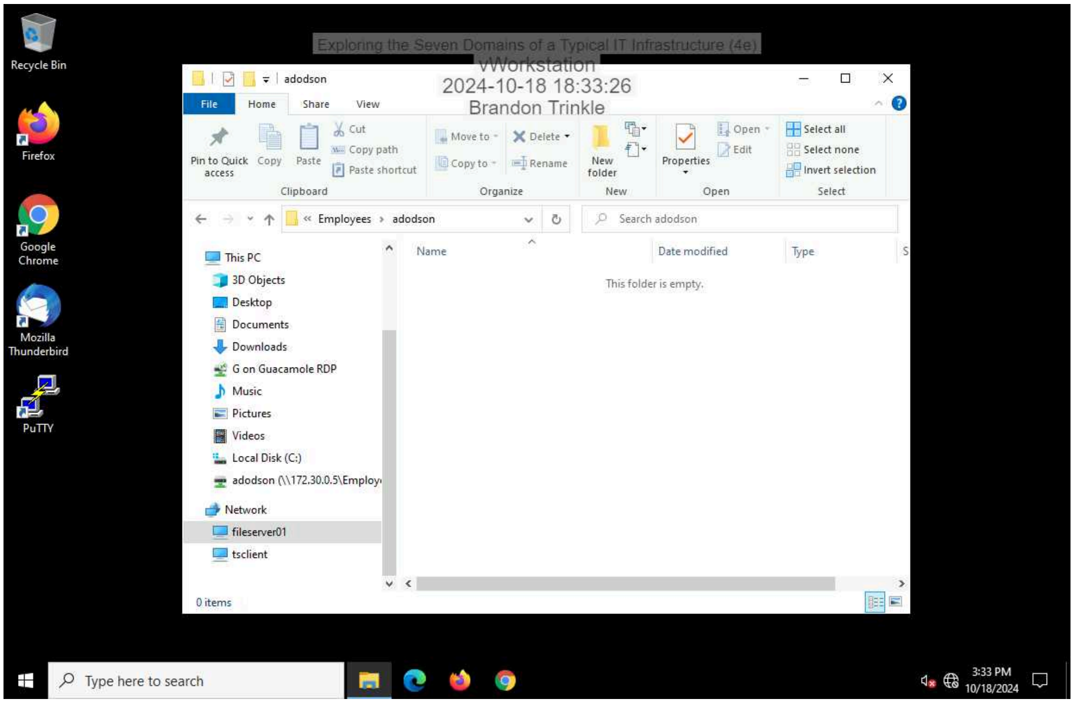


Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:32:33
Brandon Trinkle

ImportantDocument.bat-1.txt - Notepad

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

MailServer
```

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



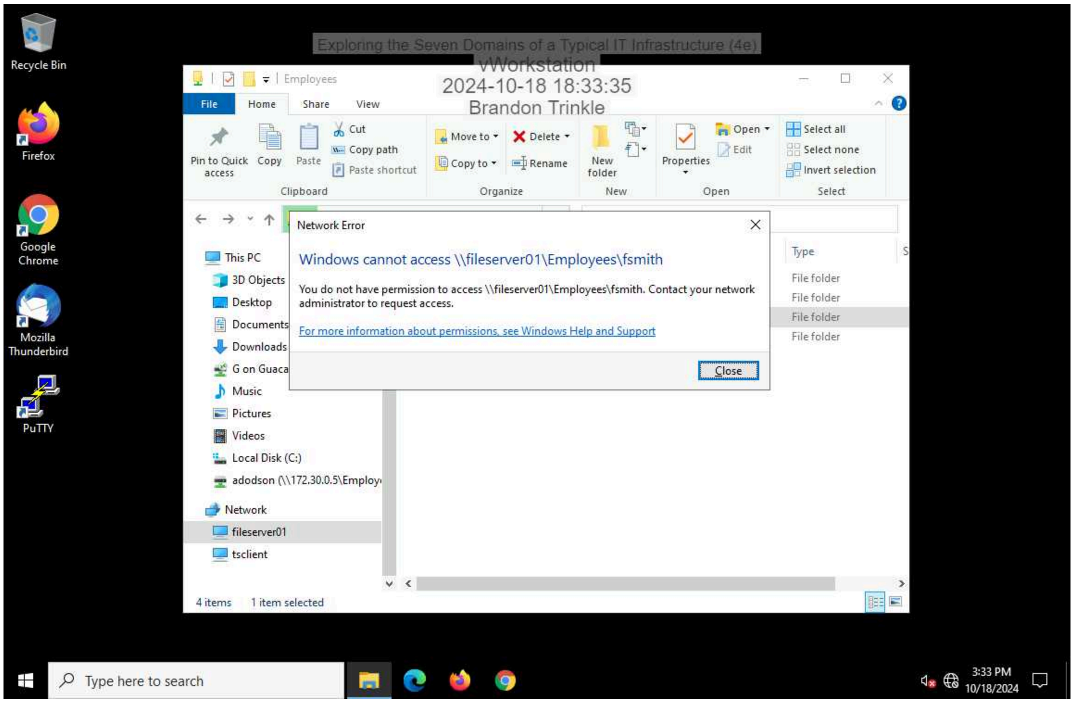
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:33:26
Brandon Trinkle

Employees › adodson

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
2024-10-18 18:33:35
Brandon Trinkle

Network Error

Windows cannot access \\fileserver01\Employees\fsmith

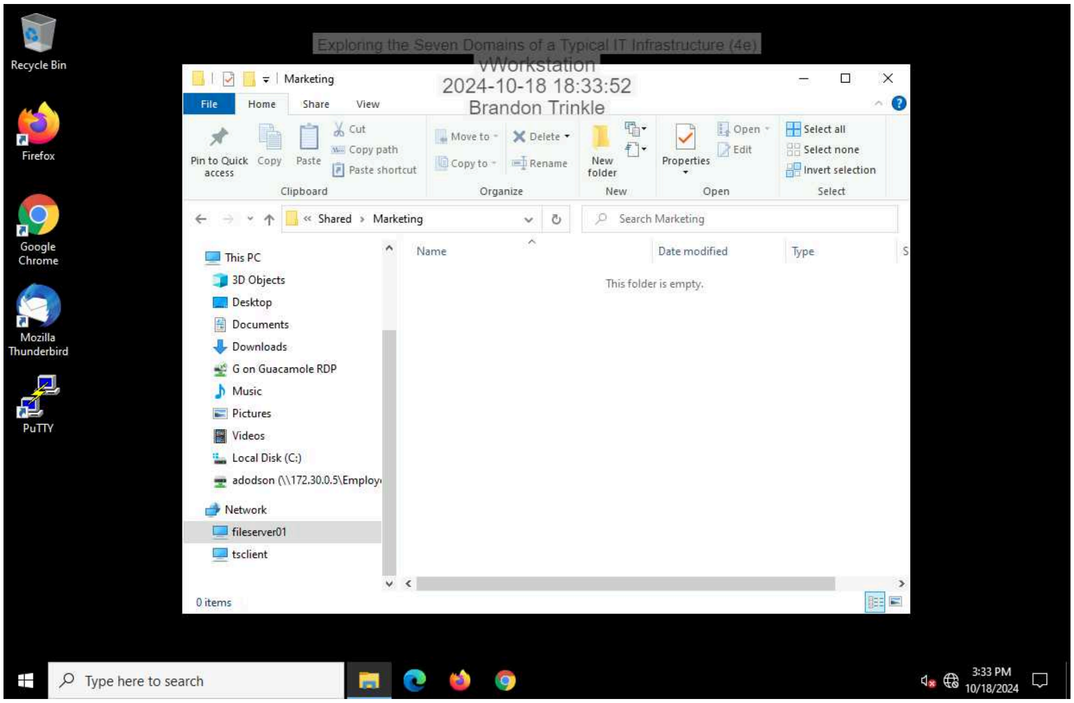
You do not have permission to access \\fileserver01\Employees\fsmith. Contact your network administrator to request access.

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**.



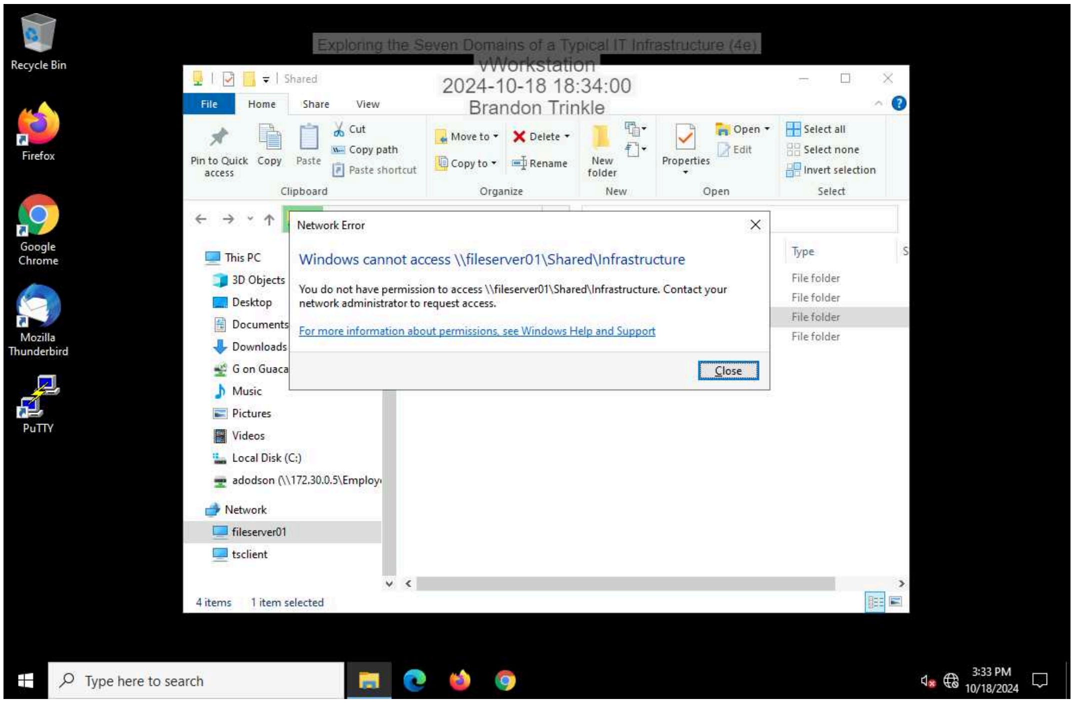
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:33:52
Brandon Trinkle

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
2024-10-18 18:34:00
Brandon Trinkle

Network Error

Windows cannot access \\fileserver01\Shared\Infrastructure

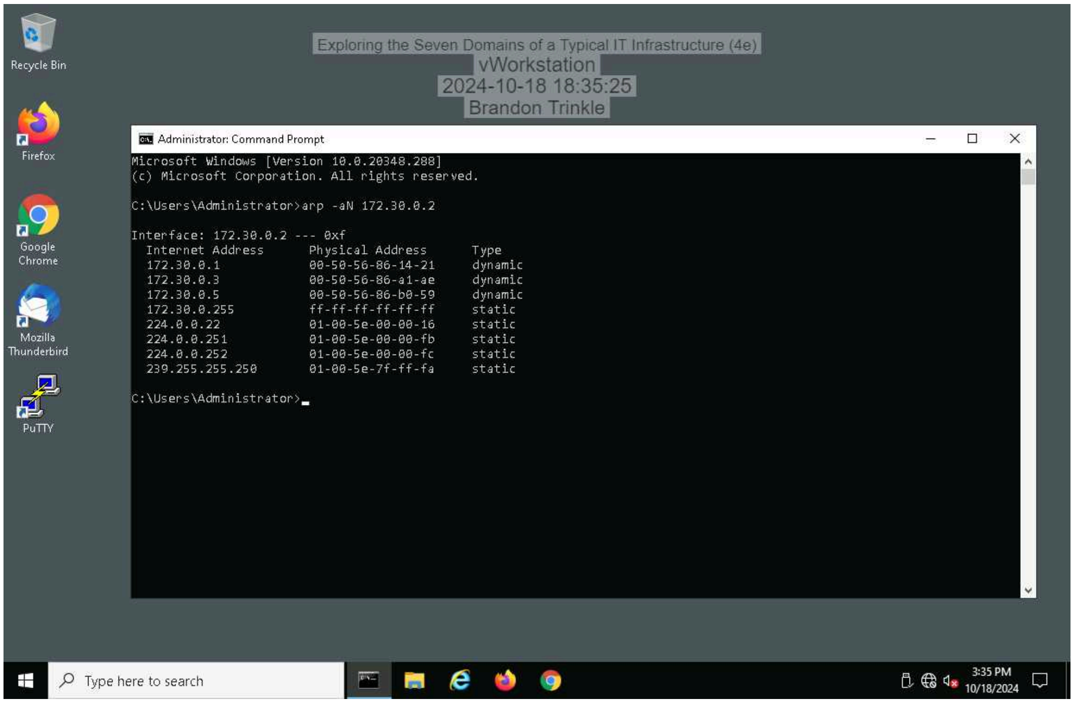
You do not have permission to access \\fileserver01\Shared\Infrastructure. Contact your network administrator to request access.

For more information about permissions, see Windows Help and Support

4 items 1 item selected

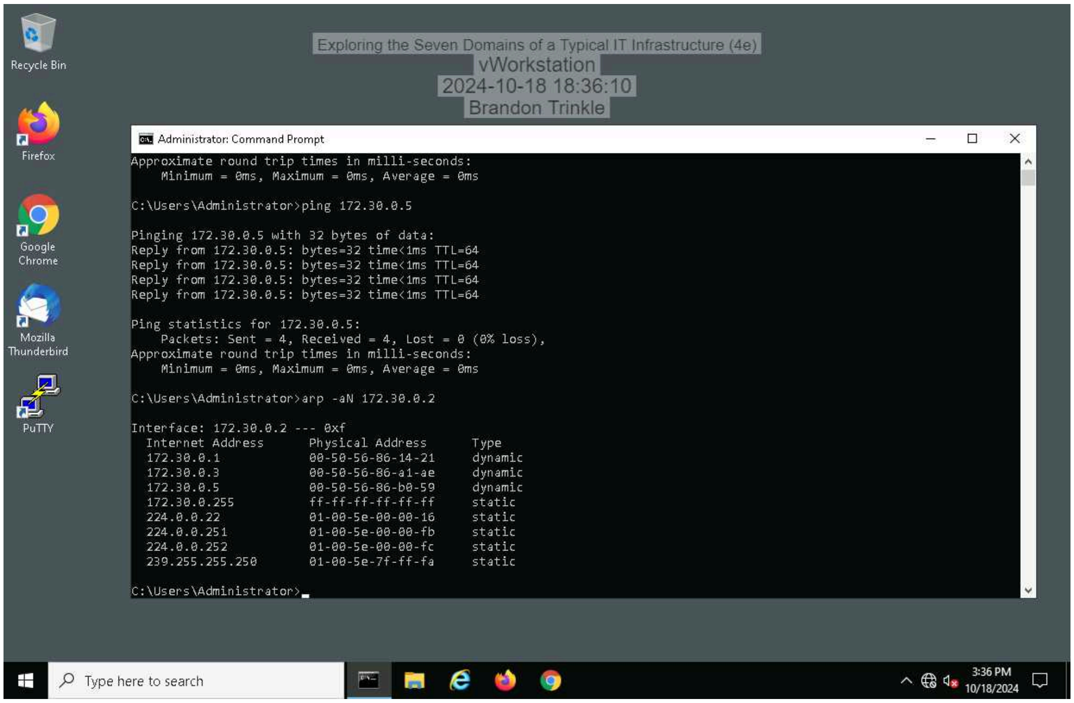
Part 2: Explore the LAN Domain

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



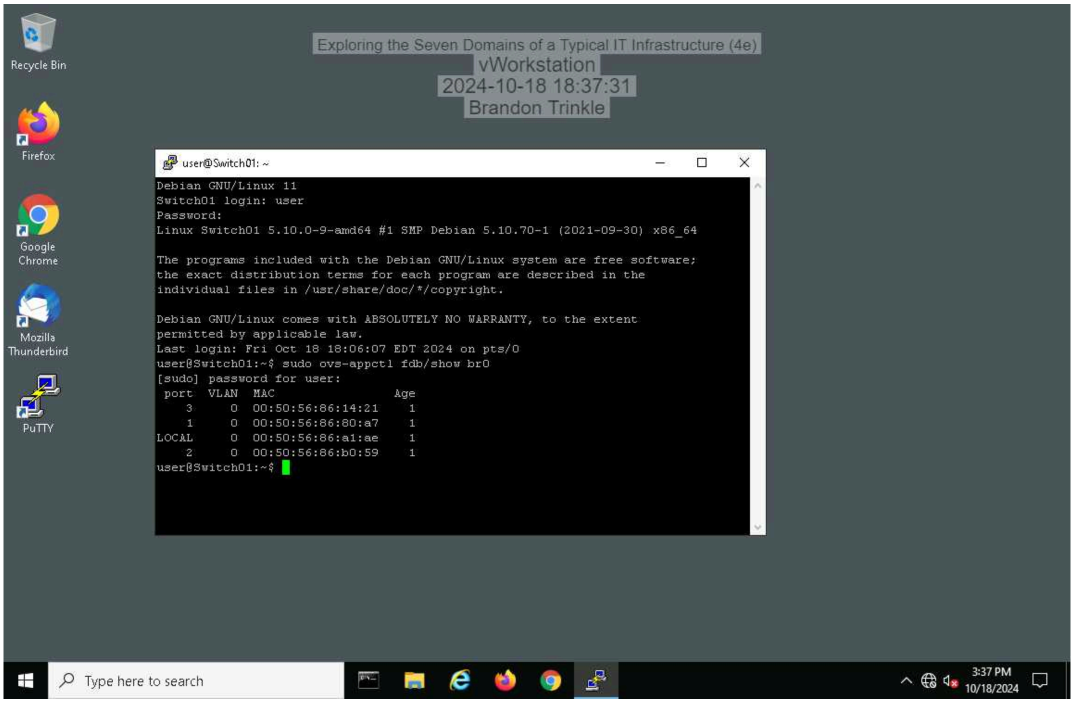
```
Microsoft Windows [Version 10.0.20348.288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>arp -aN 172.30.0.2

Interface: 172.30.0.2 --- 0xf
  Internet Address      Physical Address      Type
  172.30.0.1            00-50-56-86-14-21     dynamic
  172.30.0.3            00-50-56-86-a1-ae     dynamic
  172.30.0.5            00-50-56-86-b0-59     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.**



```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, 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 = 0ms, 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            00-50-56-86-14-21     dynamic
  172.30.0.3            00-50-56-86-a1-ae     dynamic
  172.30.0.5            00-50-56-86-b0-59     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>
```

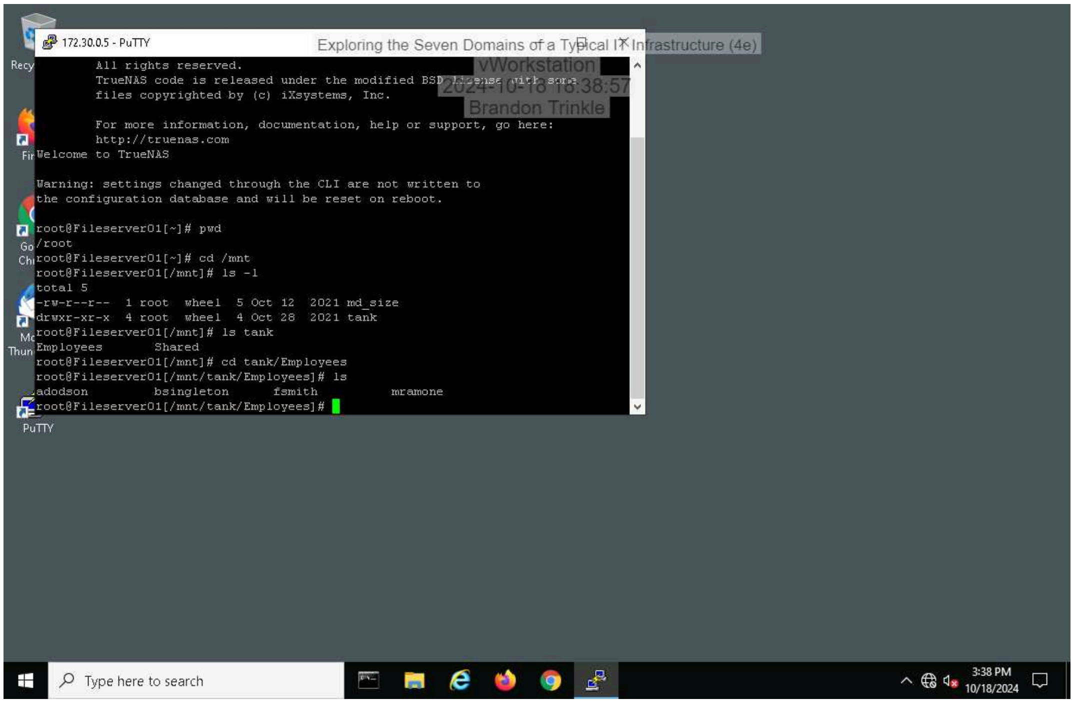
20. **Make a screen capture** showing the **Switch01 forwarding table**.


Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:37:31
Brandon Trinkle

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: Fri Oct 18 18:06:07 EDT 2024 on pts/0
user@Switch01:~$ sudo ovs-appctl fdb/show br0
[sudo] password for user:
 port  VLAN  MAC                Age
    3     0  00:50:56:86:14:21    1
    1     0  00:50:56:86:80:a7    1
LOCAL     0  00:50:56:86:a1:ae    1
    2     0  00:50:56:86:b0:59    1
user@Switch01:~$
```

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

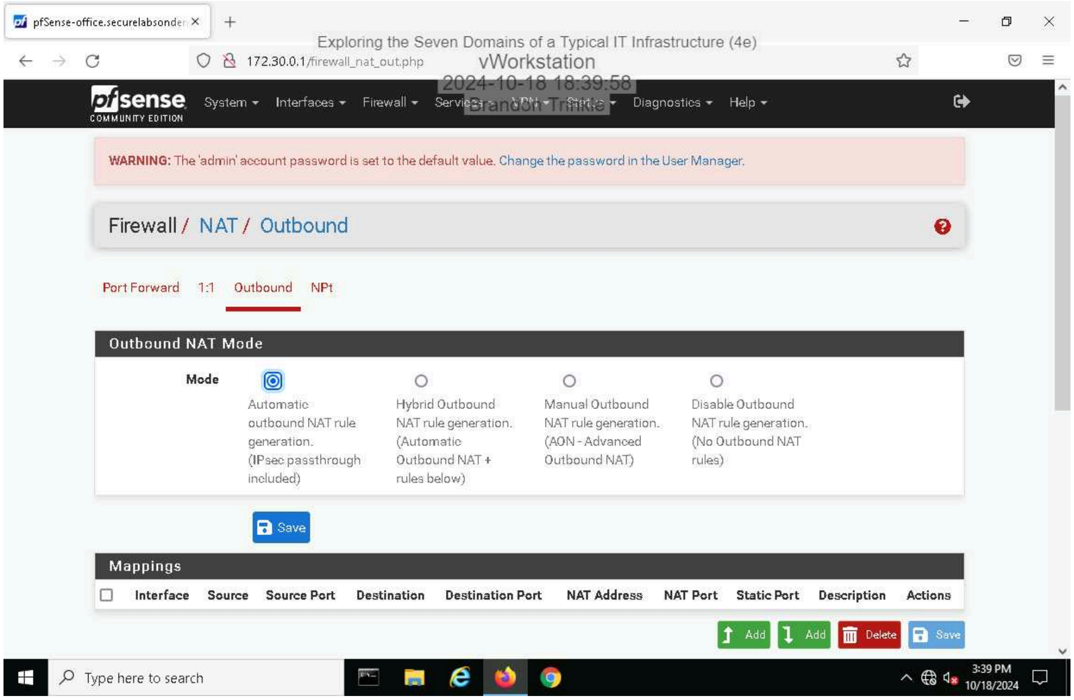

Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:38:57
Brandon Trinkle

172.30.0.5 - PuTTY

```
        All rights reserved.
        TrueNAS code is released under the modified BSD license with some
        files copyrighted by (c) iXsystems, Inc.

        For more information, documentation, help or support, go here:
        http://truenas.com
Welcome to TrueNAS

Warning: settings changed through the CLI are not written to
the configuration database and will be reset on reboot.

root@Fileserver01[~]# pwd
/root
root@Fileserver01[~]# cd /mnt
root@Fileserver01[/mnt]# ls -l
total 5
-rw-r--r--  1 root  wheel  5 Oct 12  2021 md_size
drwxr-xr-x  4 root  wheel  4 Oct 28  2021 tank
root@Fileserver01[/mnt]# ls tank
Employees       Shared
root@Fileserver01[/mnt]# cd tank/Employees
root@Fileserver01[/mnt/tank/Employees]# ls
adodson         bsingleton      fsmith          mramone
root@Fileserver01[/mnt/tank/Employees]#
```

Part 3: Explore the LAN-to-WAN Domain

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:39:58
Brandon Trinkle

172.30.0.1/firewall_nat_out.php

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

Firewall / NAT / Outbound

Port Forward · 1:1 · Outbound · NPt

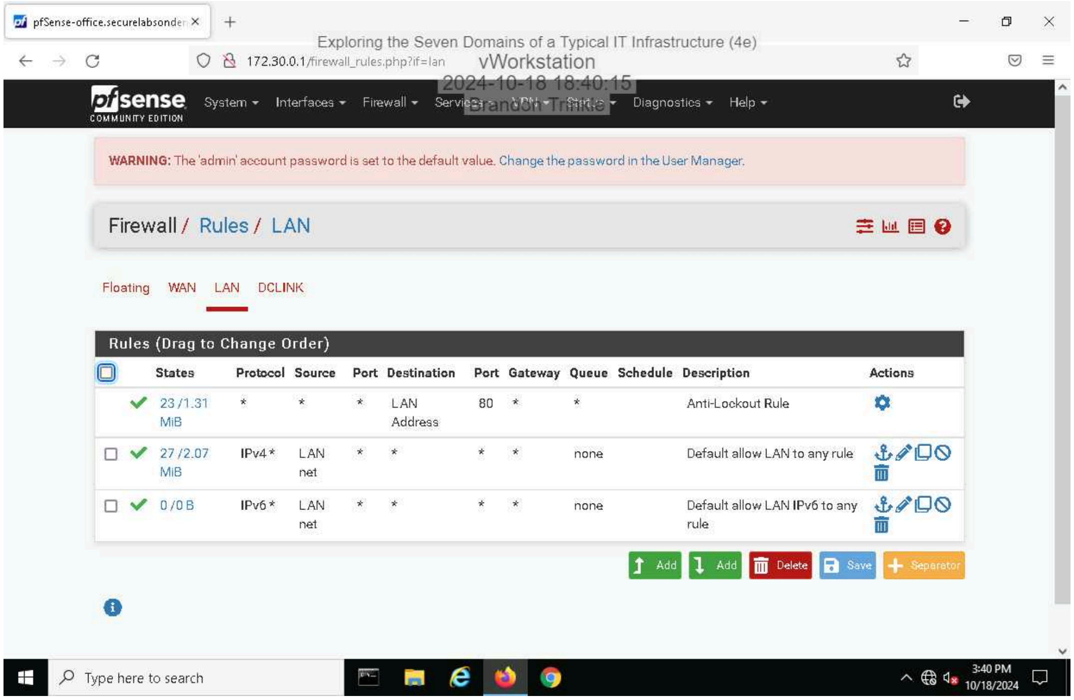
Outbound NAT Mode

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)

Mappings

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

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:40:15
Brandon Trinkle

172.30.0.1/firewall_rules.php?if=lan

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

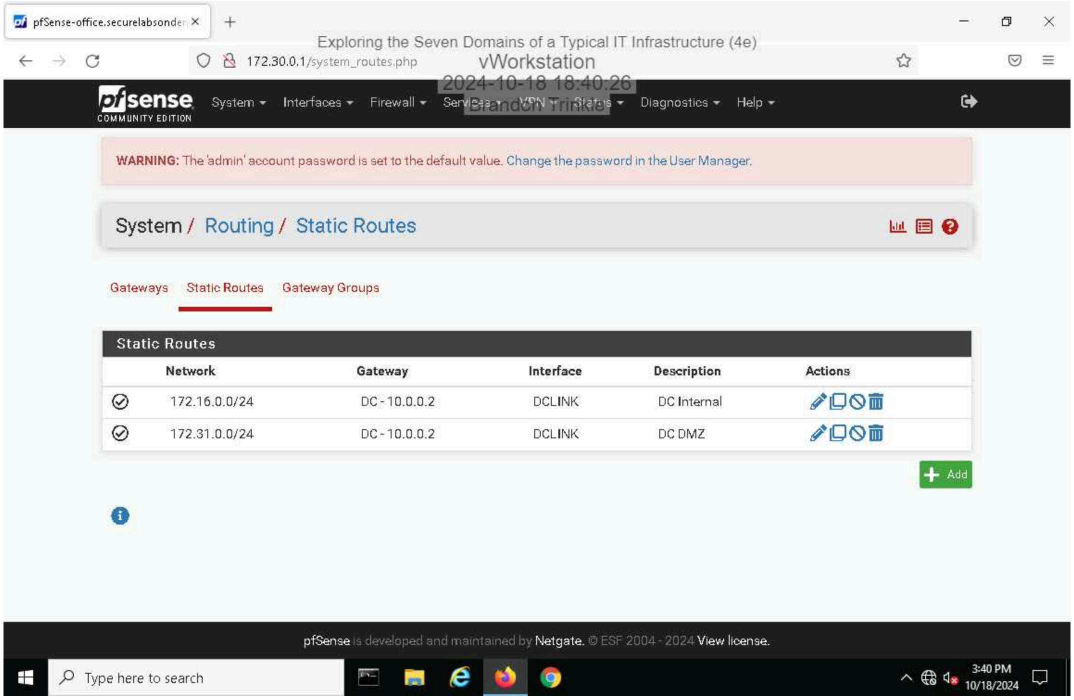
Firewall / Rules / LAN

Floating · WAN · LAN · DCLINK

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	23 /1.31 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
□	✓	27 /2.07 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:40:26
Brandon Trinkle

172.30.0.1/system_routes.php

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

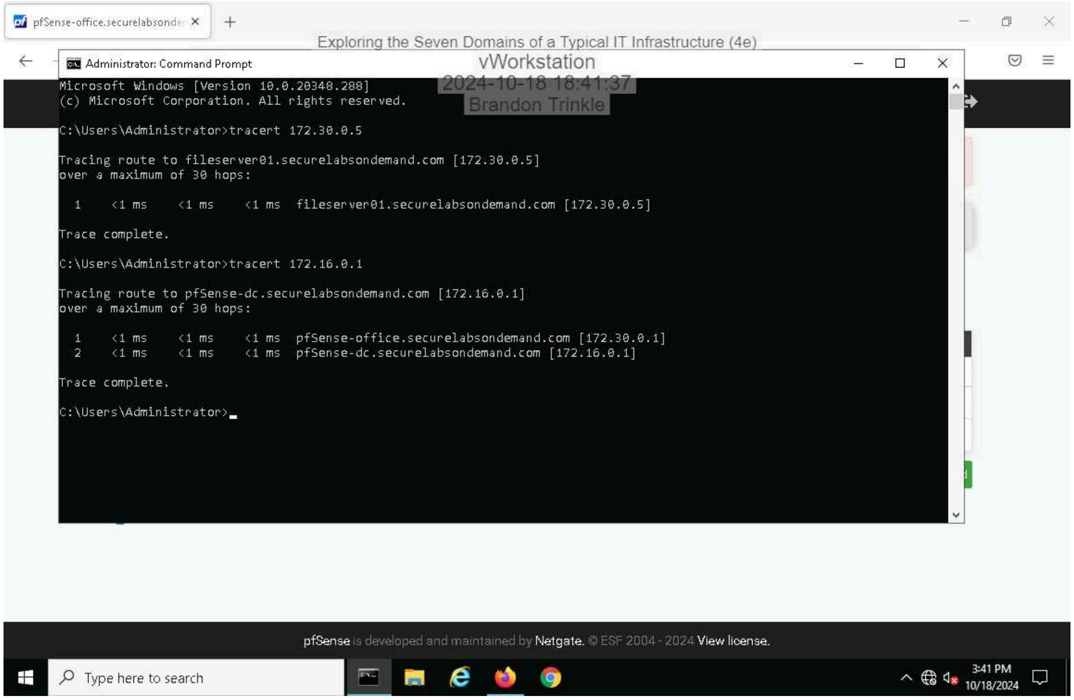
System / Routing / Static Routes

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**.



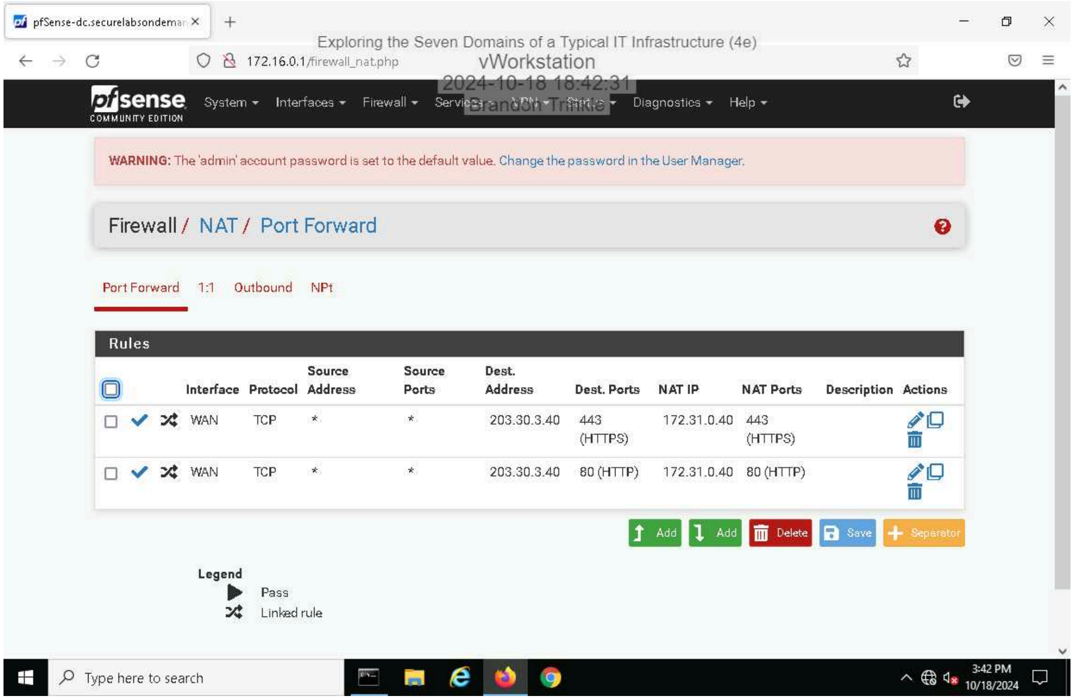
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:41:37
Brandon Trinkle

Administrator: Command Prompt

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

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**.



pfSense-dc.securelabsondemar ×
172.16.0.1/firewall_nat.php
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:42:31
Brandon Trinkle
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.

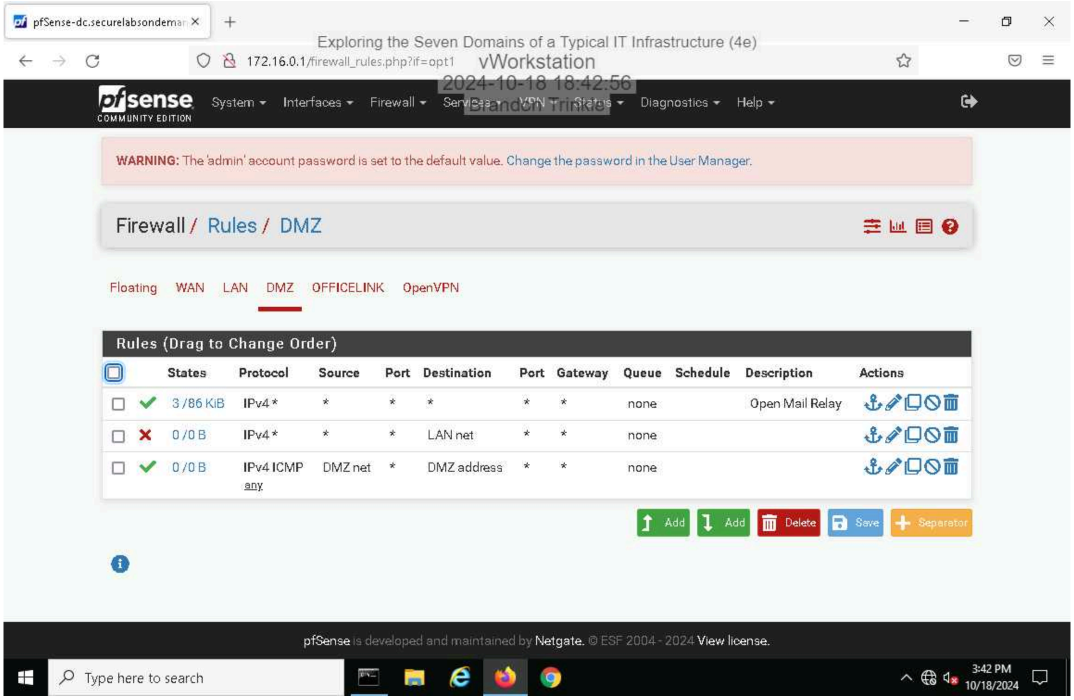
Firewall / NAT / Port Forward

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

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



pfSense-dc.securelabsondemar ×
172.16.0.1/firewall_rules.php?if=opt1
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:42:56
Brandon Trinkle
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 / DMZ

Rules (Drag to Change Order)

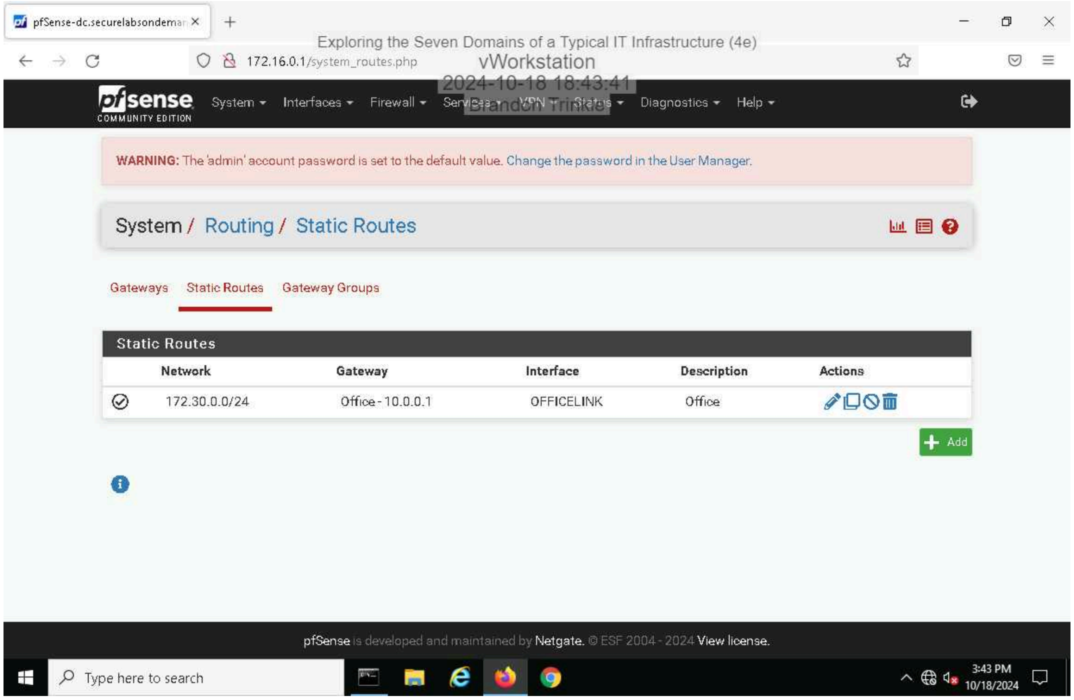
□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	3 /86 KiB	IPv4 *	*	*	*	*	*	none		Open Mail Relay	
□	✗	0 /0 B	IPv4 *	*	*	LAN net	*	*	none			
□	✓	0 /0 B	IPv4 ICMP any	DMZ net	*	DMZ address	*	*	none			

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**.



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:43:41
Brandon Trinkle

172.16.0.1/system_routes.php

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

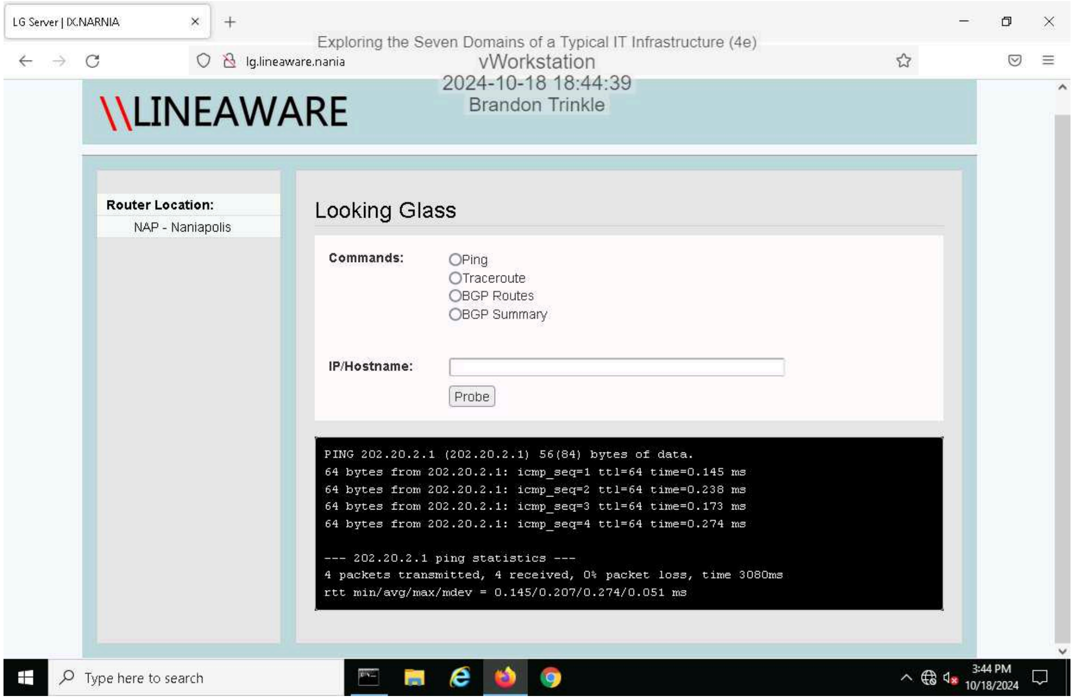
System / Routing / Static Routes

Static Routes

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

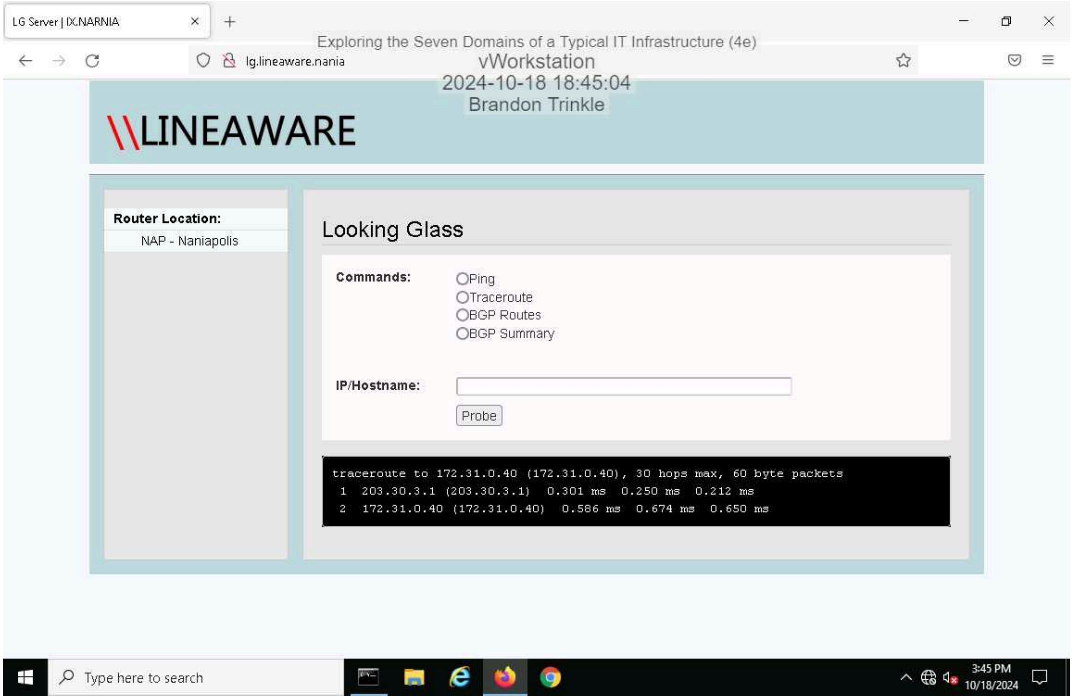
pfSense-dc.securelabsondeman
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Gateways
Static Routes
Gateway Groups
Add
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Type here to search
3:43 PM
10/18/2024

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



```
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=0.145 ms
64 bytes from 202.20.2.1: icmp_seq=2 ttl=64 time=0.238 ms
64 bytes from 202.20.2.1: icmp_seq=3 ttl=64 time=0.173 ms
64 bytes from 202.20.2.1: icmp_seq=4 ttl=64 time=0.274 ms

--- 202.20.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3080ms
rtt min/avg/max/mdev = 0.145/0.207/0.274/0.051 ms
```

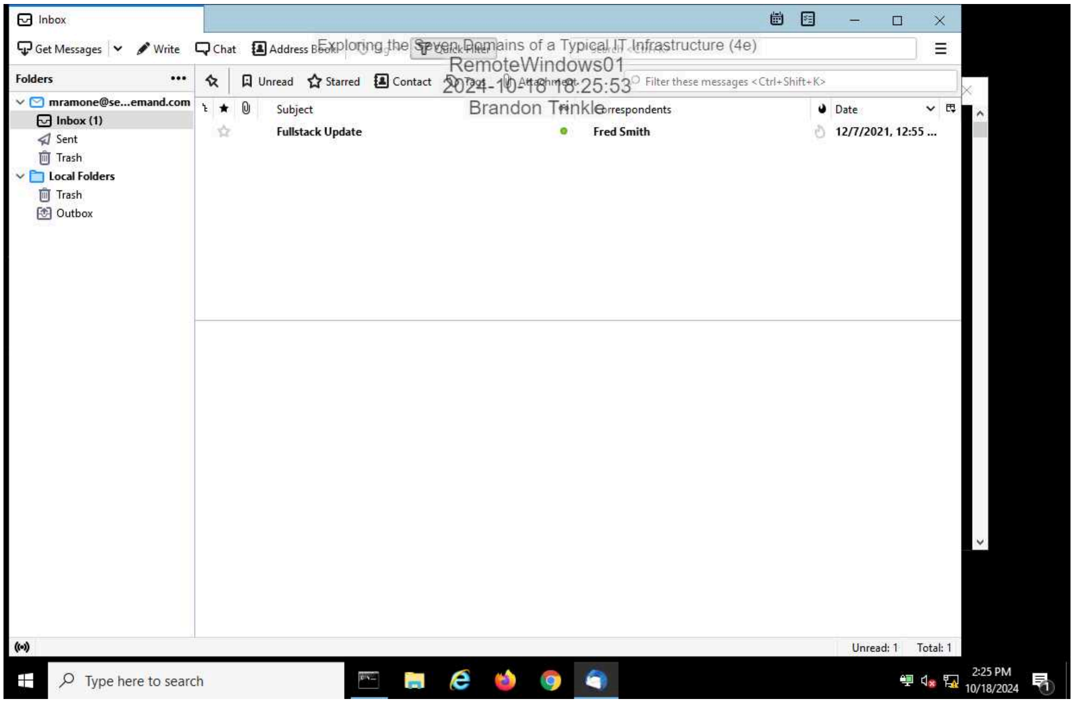
12. **Make a screen capture** showing the **traceroute to the file server**.



```
traceroute to 172.31.0.40 (172.31.0.40), 30 hops max, 60 byte packets
 1  203.30.3.1 (203.30.3.1)  0.301 ms  0.250 ms  0.212 ms
 2  172.31.0.40 (172.31.0.40)  0.586 ms  0.674 ms  0.650 ms
```

Part 2: Explore the Remote Access Domain

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



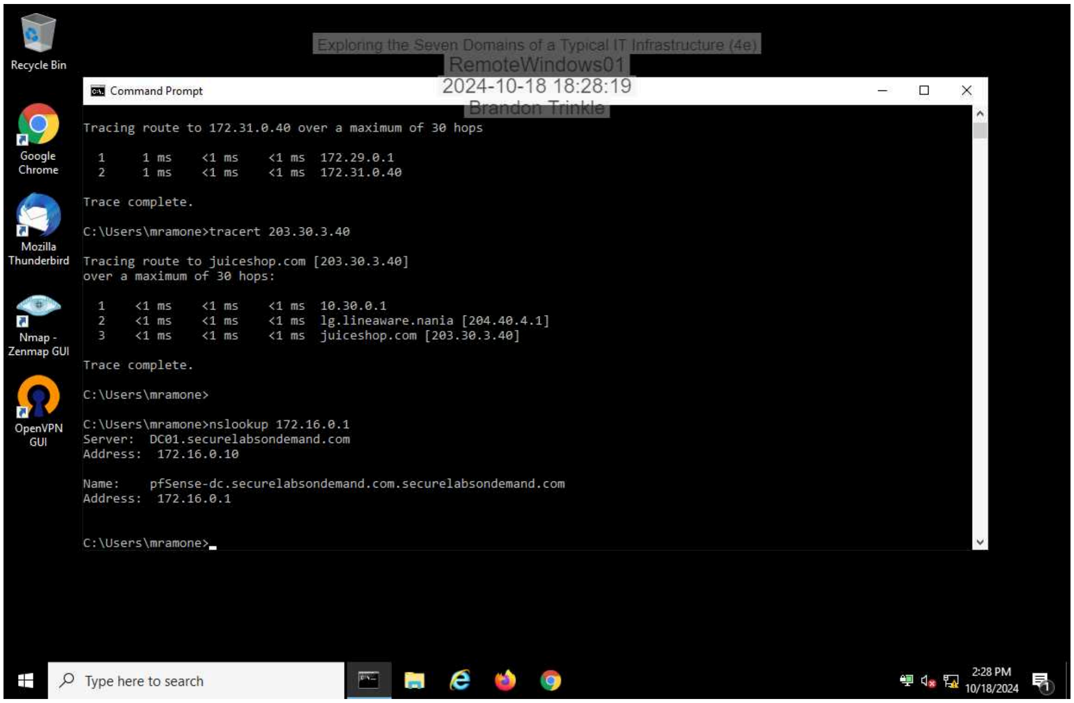
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
RemoteWindows01
2024-10-18 18:25:53
Brandon Trinkle

Subject	Correspondents	Date
Fullstack Update	Fred Smith	12/7/2021, 12:55 ...

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

this is a split tunnel

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

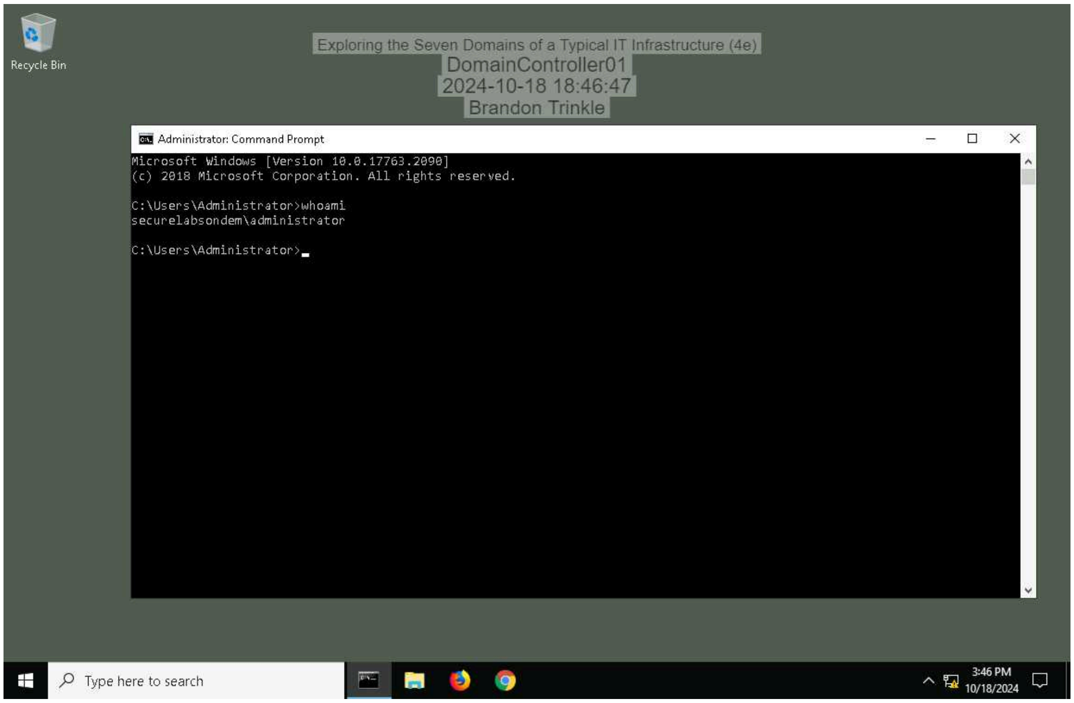


Exploring the Seven Domains of a Typical IT Infrastructure (4e)
RemoteWindows01
2024-10-18 18:28:19
Brandon Trinkle

```
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>

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**.

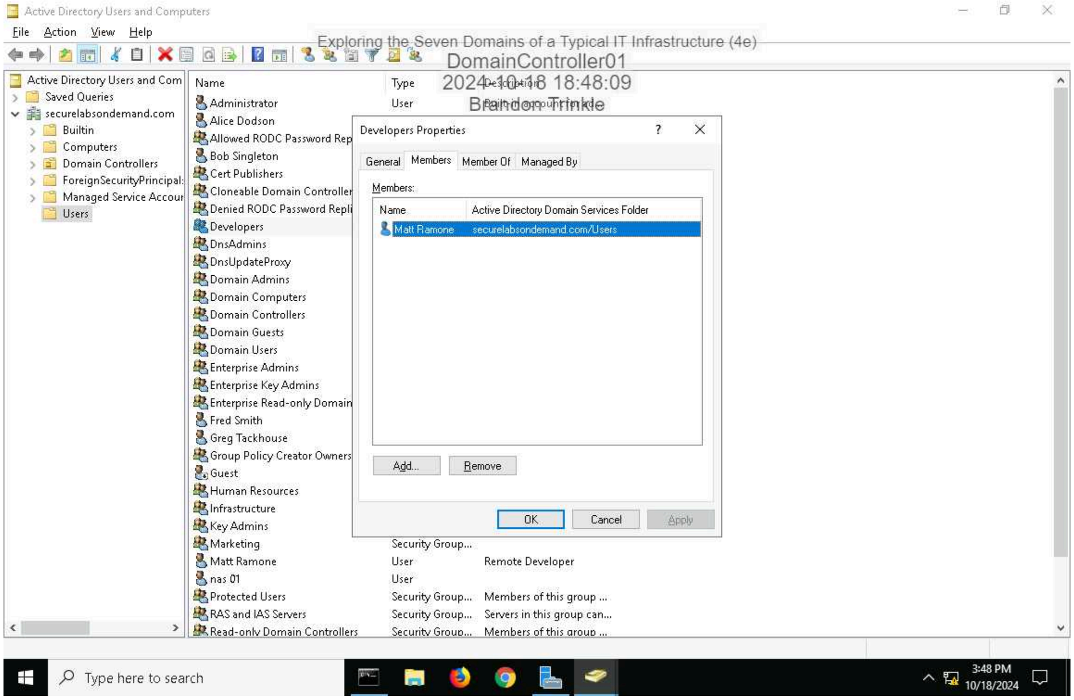


Exploring the Seven Domains of a Typical IT Infrastructure (4e)
DomainController01
2024-10-18 18:46:47
Brandon Trinkle

Administrator: Command Prompt

```
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**.



Active Directory Users and Computers

Exploring the Seven Domains of a Typical IT Infrastructure (4e)
DomainController01
2024-10-18 18:48:09
Brandon Trinkle

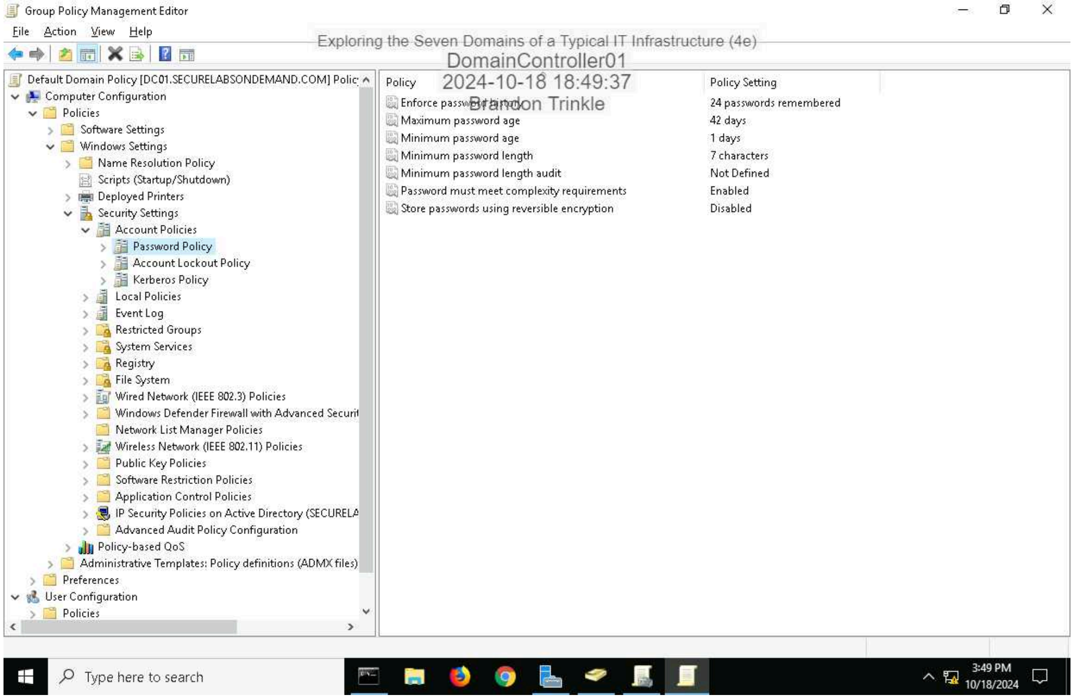
Name	Type	Description
Administrator	User	Built-in account for ad...
Alice Dodson		
Allowed RODC Password Rep		
Bob Singleton		
Cert Publishers		
Cloneable Domain Controller		
Denied RODC Password Repli		
Developers		
DnsAdmins		
DnsUpdateProxy		
Domain Admins		
Domain Computers		
Domain Controllers		
Domain Guests		
Domain Users		
Enterprise Admins		
Enterprise Key Admins		
Enterprise Read-only Domain		
Fred Smith		
Greg Tackhouse		
Group Policy Creator Owners		
Guest		
Human Resources		
Infrastructure		
Key Admins		
Marketing	Security Group...	
Matt Ramone	User	Remote Developer
nas 01	User	
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group can...
Read-only Domain Controllers	Security Group...	Members of this group ...

Developers Properties

Members:

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

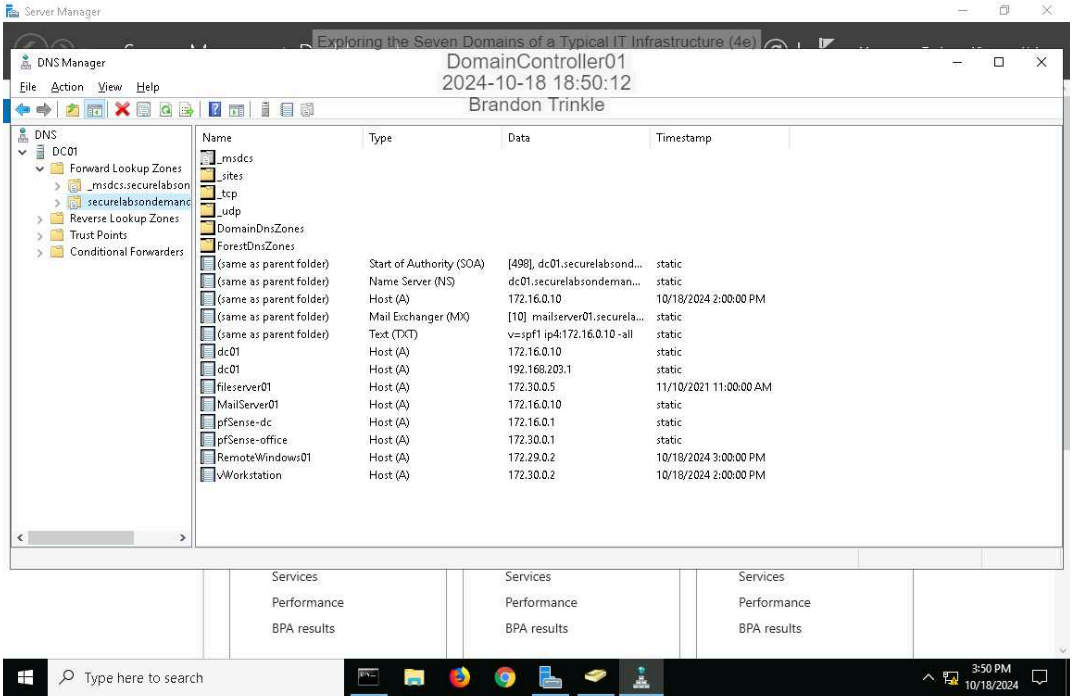
16. **Make a screen capture** showing the **password policy settings in the Group Policy Management Console**.


Group Policy Management Editor
File
Action
View
Help
Default Domain Policy [DC01.SECURELABSONDEMAND.COM] Polic
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Securit
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (SECURELA
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files)
Preferences
User Configuration
Policies
Type here to search
3:49 PM
10/18/2024

Exploring the Seven Domains of a Typical IT Infrastructure (4e)
DomainController01
2024-10-18 18:49:37
Brandon Trinkle

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

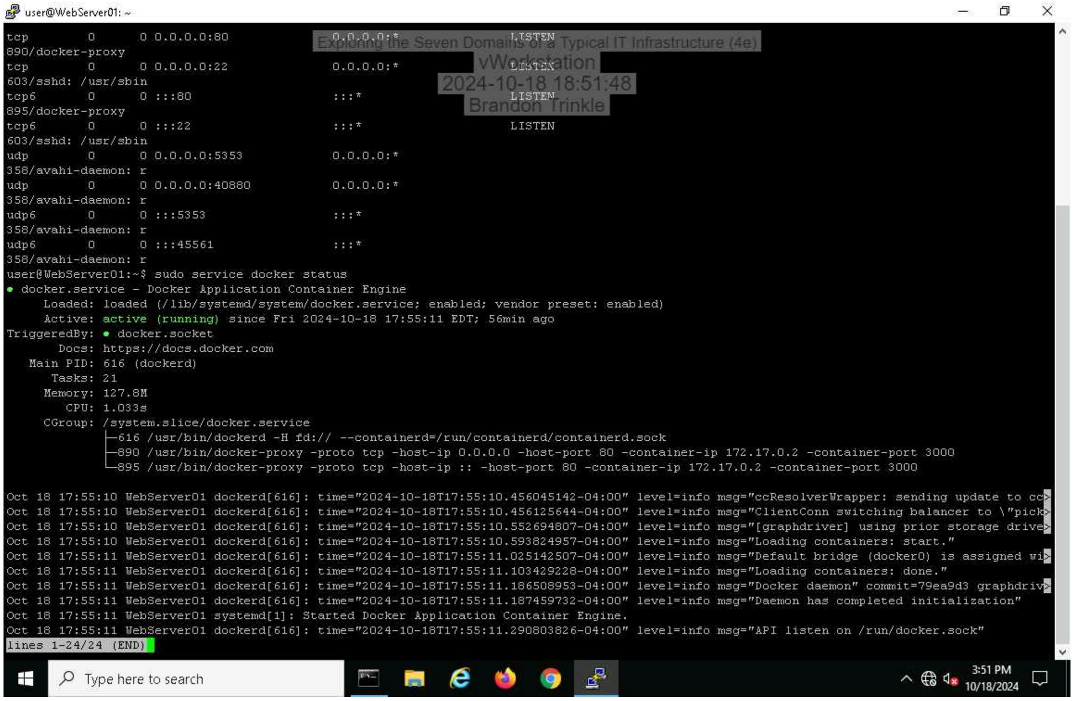
20. **Make a screen capture** showing the **DNS entries**.



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
DomainController01
2024-10-18 18:50:12
Brandon Trinkle

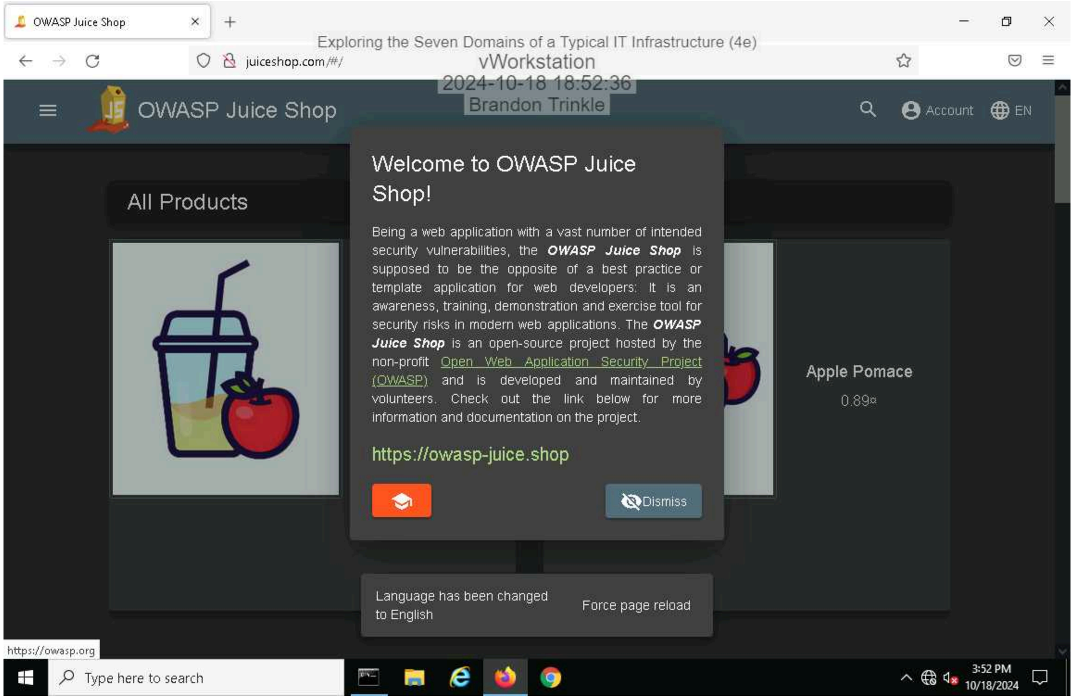
Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[498], dc01.securelabsond...	static
(same as parent folder)	Name Server (NS)	dc01.securelabsondeman...	static
(same as parent folder)	Host (A)	172.16.0.10	10/18/2024 2:00:00 PM
(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)	172.16.0.10	static
dc01	Host (A)	192.168.203.1	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	10/18/2024 3:00:00 PM
vWorkstation	Host (A)	172.30.0.2	10/18/2024 2:00:00 PM

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



```
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
890/docker-proxy
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
603/sshd: /usr/sbin
tcp6       0      0 :::80                   :::*                    LISTEN
895/docker-proxy
tcp6       0      0 :::22                   :::*                    LISTEN
603/sshd: /usr/sbin
udp        0      0 0.0.0.0:5353            0.0.0.0:*
358/avahi-daemon: r
udp        0      0 0.0.0.0:40880           0.0.0.0:*
358/avahi-daemon: r
udp6       0      0 :::5353                 :::*
358/avahi-daemon: r
udp6       0      0 :::45561                :::*
358/avahi-daemon: r
user@WebServer01:~$ sudo service docker status
● docker.service - Docker Application Container Engine
     Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2024-10-18 17:55:11 EDT; 56min ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 616 (dockerd)
      Tasks: 21
     Memory: 127.8M
        CPU: 1.033s
     CGroup: /system.slice/docker.service
             ├─616 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
             ├─890 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 80 -container-ip 172.17.0.2 -container-port 3000
             └─895 /usr/bin/docker-proxy -proto tcp -host-ip :: -host-port 80 -container-ip 172.17.0.2 -container-port 3000

Oct 18 17:55:10 WebServer01 dockerd[616]: time="2024-10-18T17:55:10.456045142-04:00" level=info msg="ccResolverWrapper: sending update to cc>
Oct 18 17:55:10 WebServer01 dockerd[616]: time="2024-10-18T17:55:10.456125644-04:00" level=info msg="ClientConn switching balancer to \"pick>
Oct 18 17:55:10 WebServer01 dockerd[616]: time="2024-10-18T17:55:10.552694807-04:00" level=info msg="[graphdriver] using prior storage drive>
Oct 18 17:55:10 WebServer01 dockerd[616]: time="2024-10-18T17:55:10.593824957-04:00" level=info msg="Loading containers: start."
Oct 18 17:55:11 WebServer01 dockerd[616]: time="2024-10-18T17:55:11.025142507-04:00" level=info msg="Default bridge (docker0) is assigned wi>
Oct 18 17:55:11 WebServer01 dockerd[616]: time="2024-10-18T17:55:11.103429228-04:00" level=info msg="Loading containers: done."
Oct 18 17:55:11 WebServer01 dockerd[616]: time="2024-10-18T17:55:11.186508953-04:00" level=info msg="Docker daemon" commit=79ea9d3 graphdriv>
Oct 18 17:55:11 WebServer01 dockerd[616]: time="2024-10-18T17:55:11.187459732-04:00" level=info msg="Daemon has completed initialization"
Oct 18 17:55:11 WebServer01 systemd[1]: Started Docker Application Container Engine.
Oct 18 17:55:11 WebServer01 dockerd[616]: time="2024-10-18T17:55:11.290803826-04:00" 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**.



Welcome to OWASP Juice Shop!

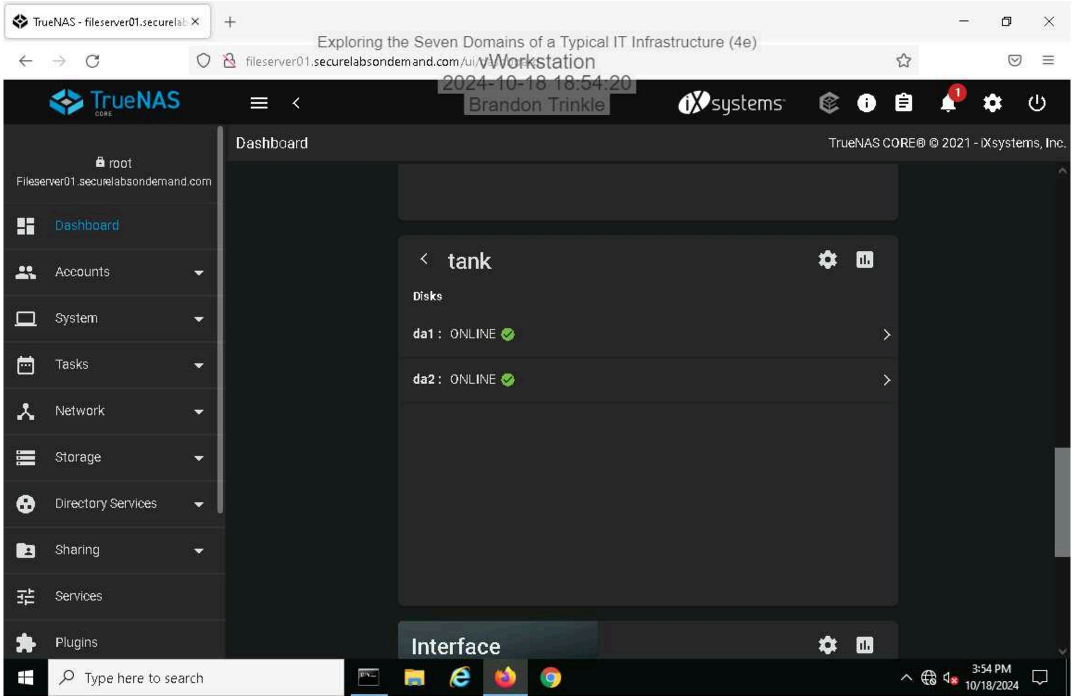
Being a web application with a vast number of intended security vulnerabilities, the ***OWASP Juice Shop*** is supposed to be the opposite of a best practice or template application for web developers: It is an awareness, training, demonstration and exercise tool for security risks in modern web applications. The ***OWASP Juice Shop*** is an open-source project hosted by the non-profit Open Web Application Security Project (OWASP) and is developed and maintained by volunteers. Check out the link below for more information and documentation on the project.

https://owasp-juice.shop

Language has been changed to English

Force page reload

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


Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-10-18 18:54:20
Brandon Trinkle

fileserver01.securelabsondemand.com/ui/

root
Fileserver01.securelabsondemand.com

tank
Disks
da1 : ONLINE
da2 : ONLINE

TrueNAS CORE® © 2021 - iXsystems, Inc.

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 effective security controls to protect the User Domain are Multi-Factor Authentication (MFA) and Security Awareness Training. MFA requires users to provide two or more verification factors to gain access to a system, such as something they know (password), something they have (security token), or something they are (fingerprint or facial recognition). This method adds an extra layer of security beyond passwords, making it significantly harder for attackers to access systems even if a password is compromised (Microsoft Security). Meanwhile, regular Security Awareness Training educates users on recognizing and avoiding common security threats, such as phishing, and encourages adherence to best practices, thereby reducing human error and minimizing risks. Educating users helps them avoid falling victim to attacks that exploit human vulnerabilities, such as social engineering (SANS Institute). By implementing both controls, organizations can better protect the User Domain from vulnerabilities and enhance overall security.

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.

To strengthen the security of the Juice Shop’s IT infrastructure across various domains, several security controls can be recommended. In the Workstation Domain, implementing an Endpoint Detection and Response (EDR) solution can monitor real-time activity on workstations to detect and respond to threats like malware, providing enhanced protection for employee devices. For the LAN Domain, Network Access Control (NAC) should be used to ensure that only authorized and compliant devices can access the internal network, reducing the risk of compromised devices being connected. In the LAN-to-WAN Domain, deploying a Unified Threat Management (UTM) solution can provide comprehensive security by integrating firewall, intrusion prevention, and antivirus functionalities into a single platform, protecting the network boundary. For the WAN Domain, implementing a Virtual Private Network (VPN) is essential to secure data transmitted between remote users and the company's network, encrypting the connection to prevent unauthorized access. In the Remote Access Domain, Multi-Factor Authentication (MFA) should be utilized to add an additional layer of security by requiring users to authenticate using multiple factors, thereby reducing the likelihood of compromised credentials leading to unauthorized access. Finally, in the System/Application Domain, a Web Application Firewall (WAF) is necessary to protect web applications from common vulnerabilities like SQL injection and cross-site scripting (XSS), ensuring that internet-facing applications remain secure. These security controls together will provide comprehensive protection across the Juice Shop’s IT infrastructure.