Student:	Email:
Kanchan Chopde	hq0656@wayne.edu

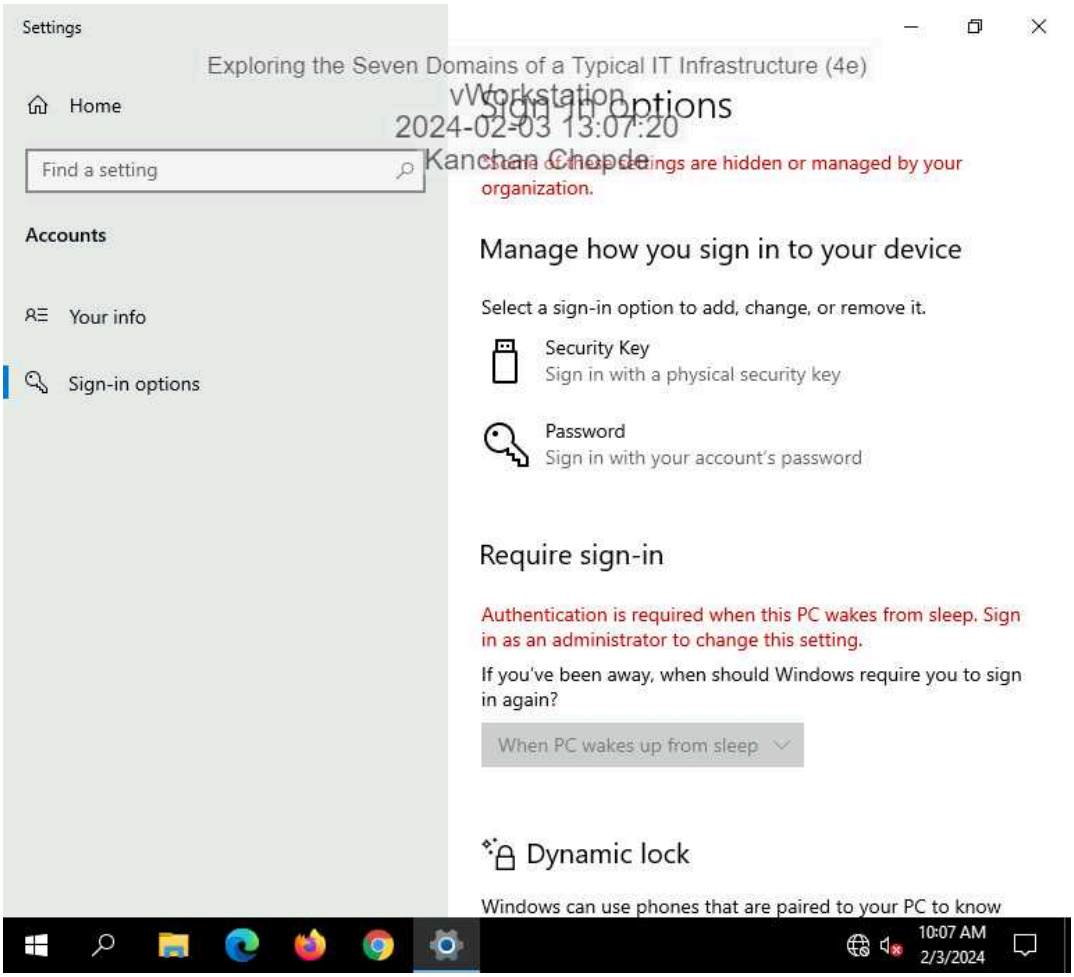
Time on Task:	Progress:
4 hours, 32 minutes	100%

Report Generated: Saturday, February 3, 2024 at 8:16 PM

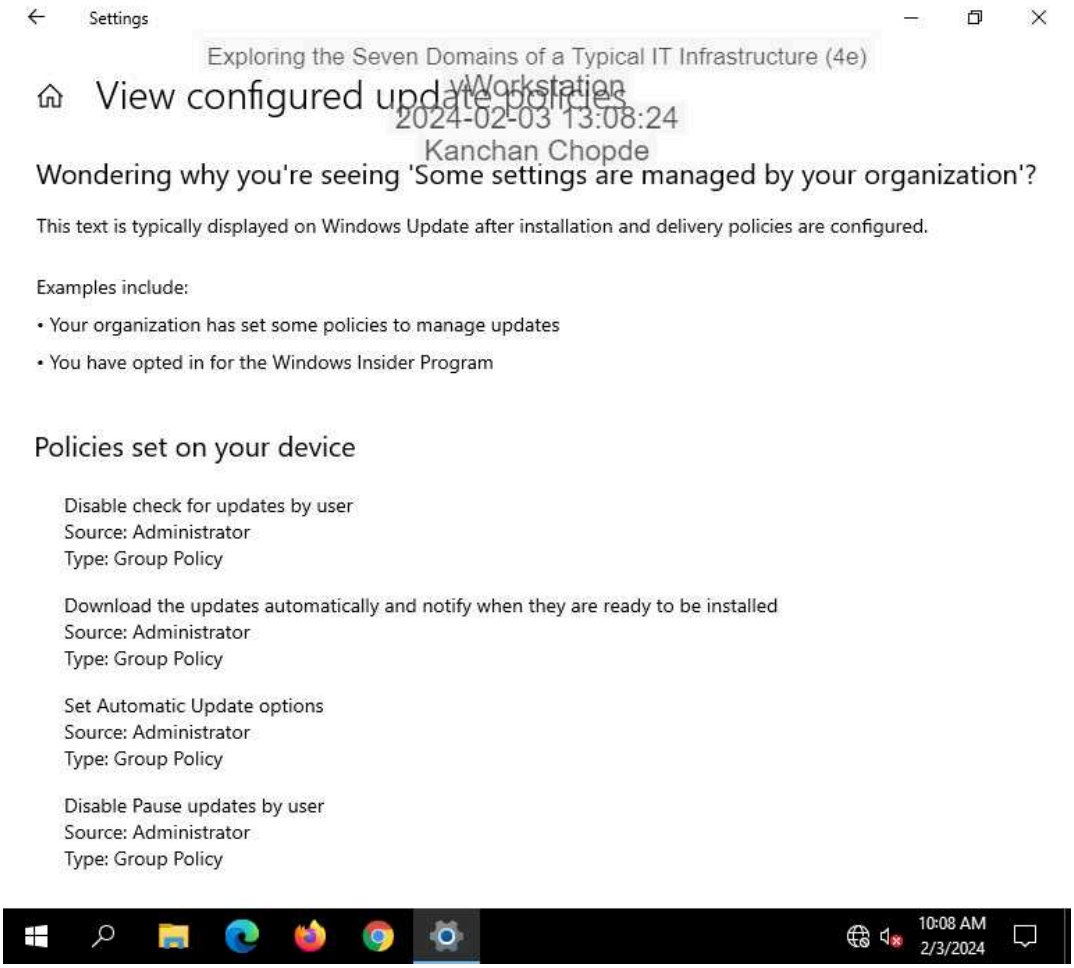
Section 1: Hands-On Demonstration

Part 1: Explore the Workstation Domain

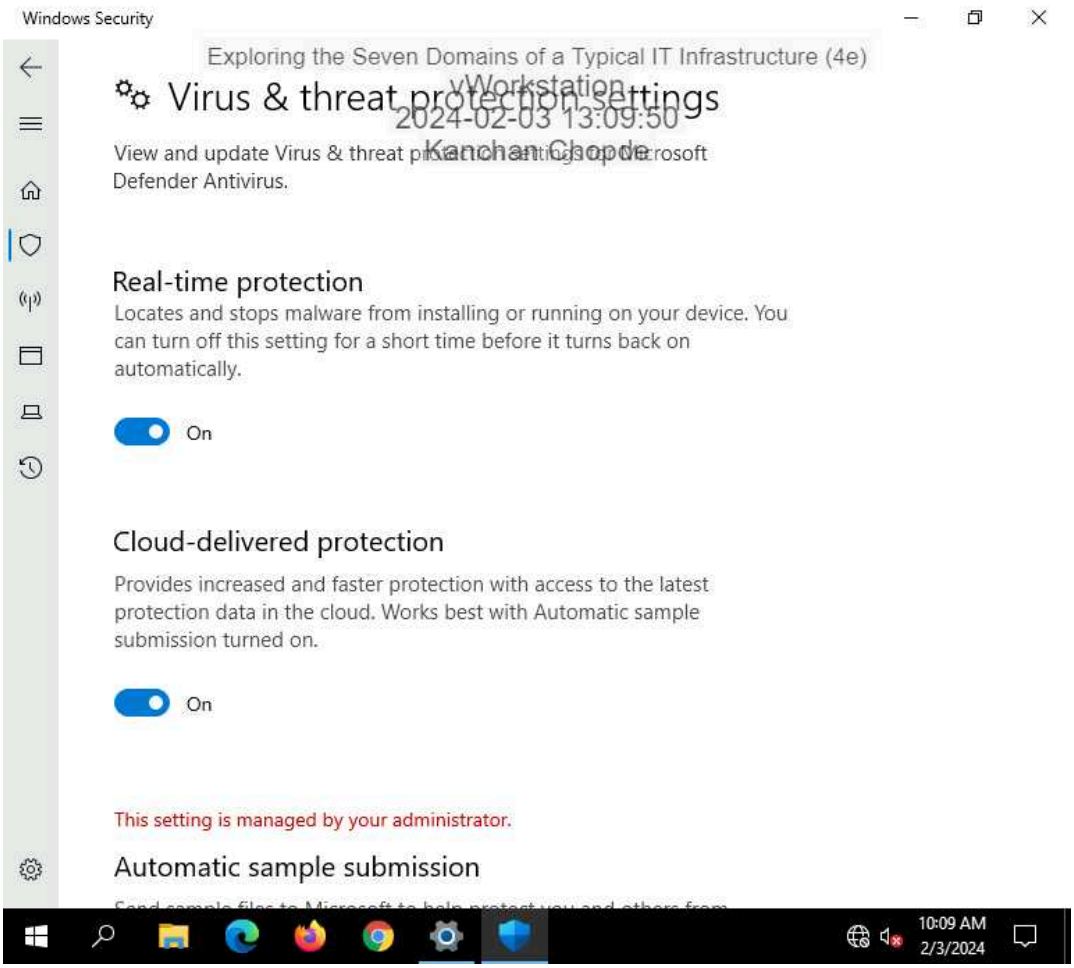
4. **Make screen capture** showing the **Sign-in options for Alice's account**.



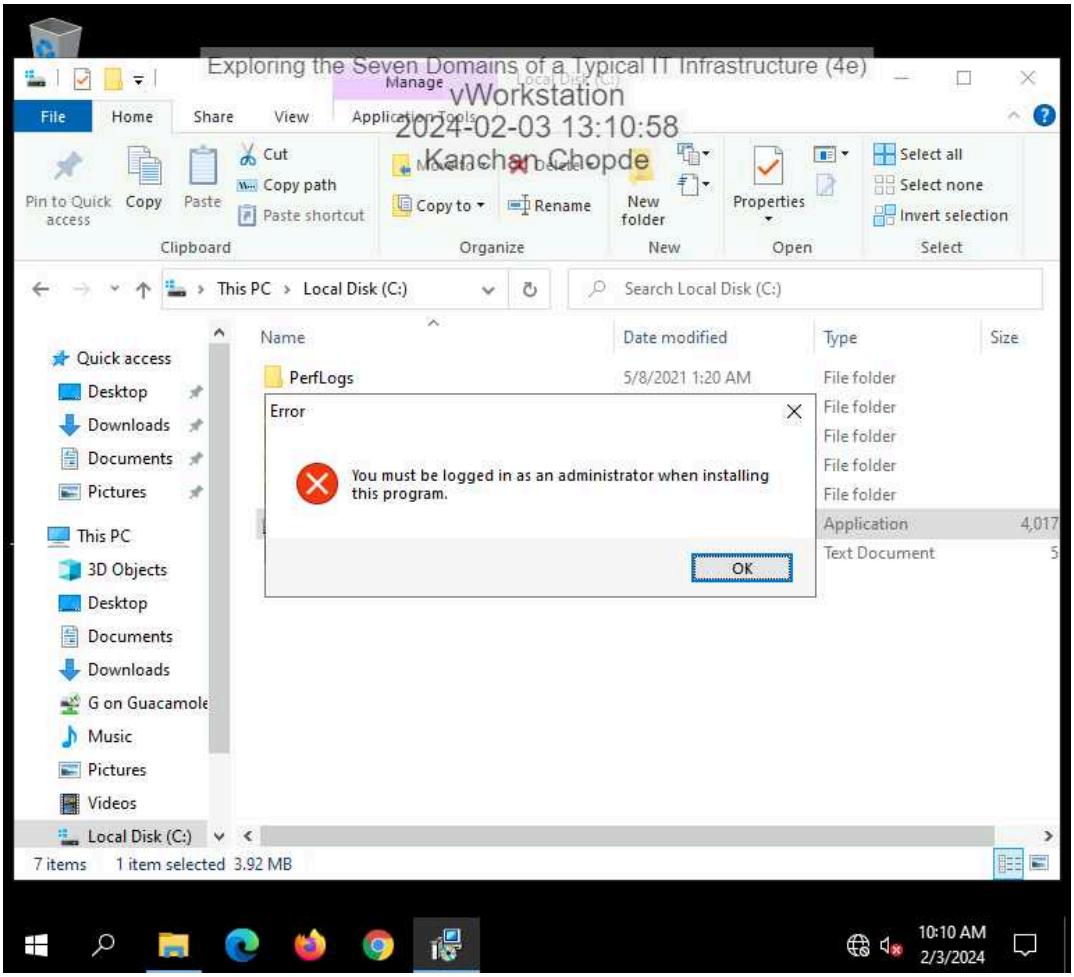
7. **Make a screen capture** showing the **View configured update policies page**.



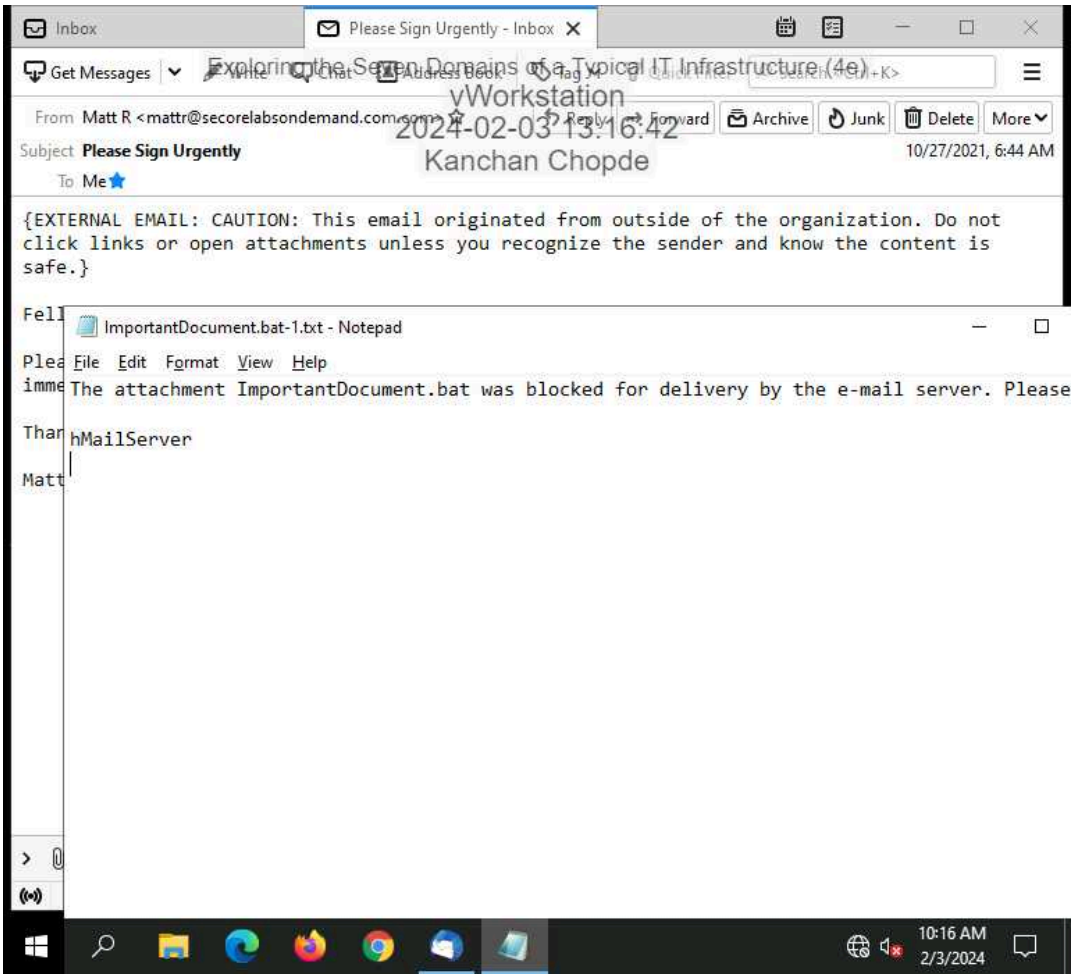
14. **Make a screen capture** showing the **Virus & Threat Protection Settings**.



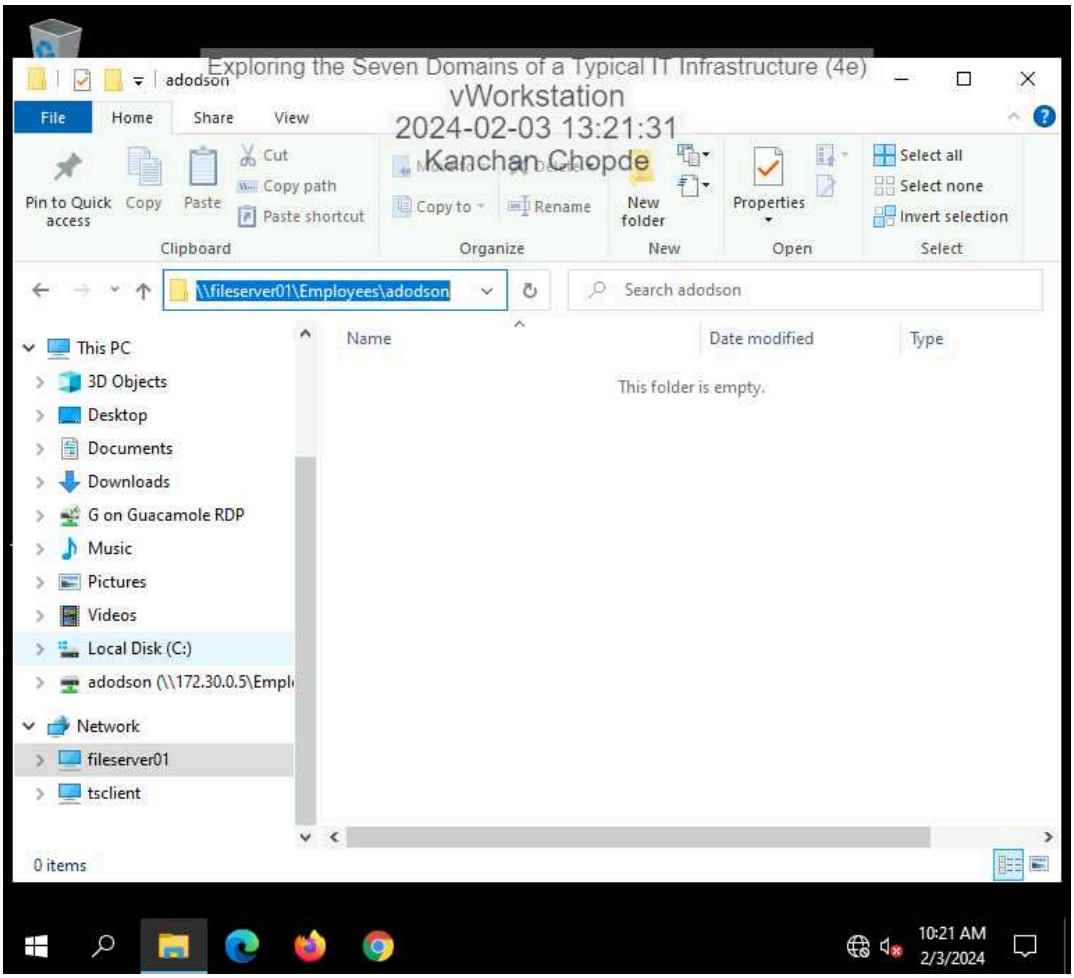
18. **Make a screen capture** showing the **security warning from attempting to run an executable file**.



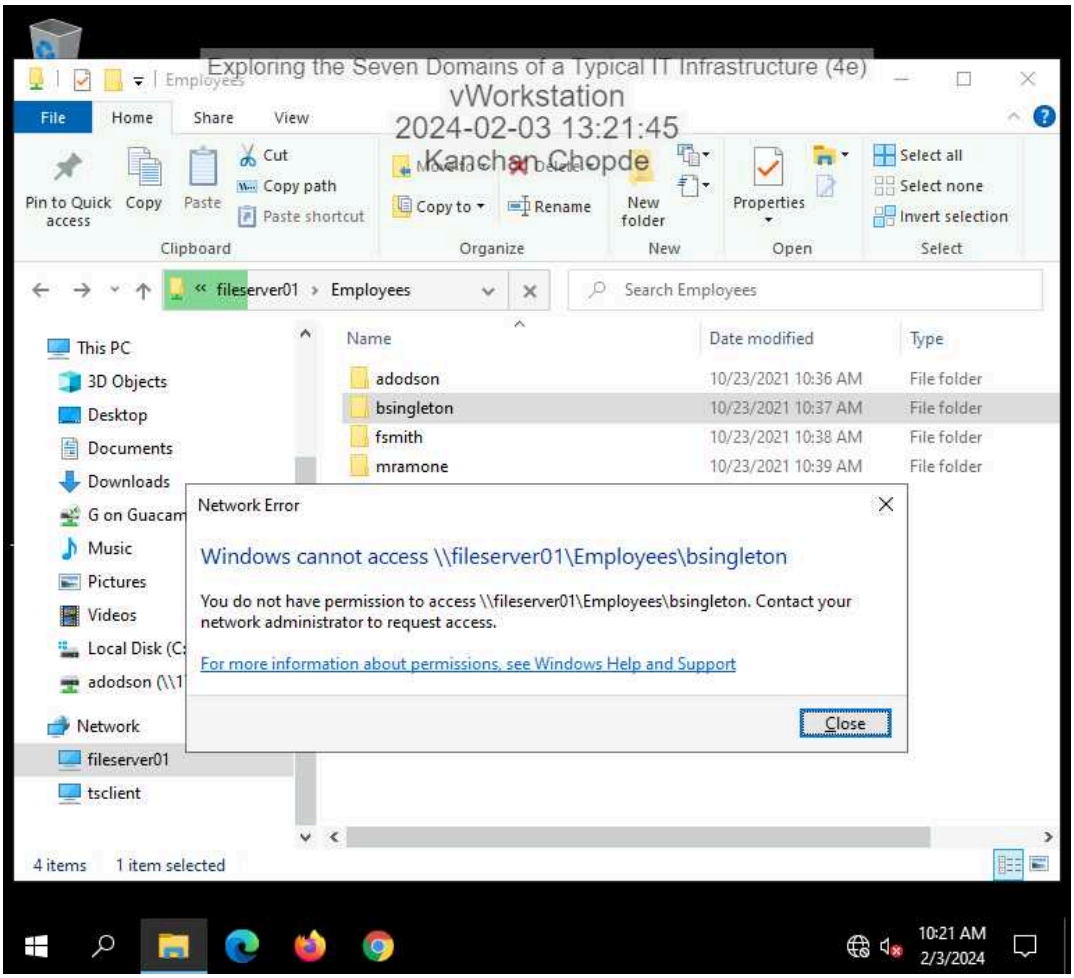
24. **Make a screen capture** showing the **blocked attachment message**.



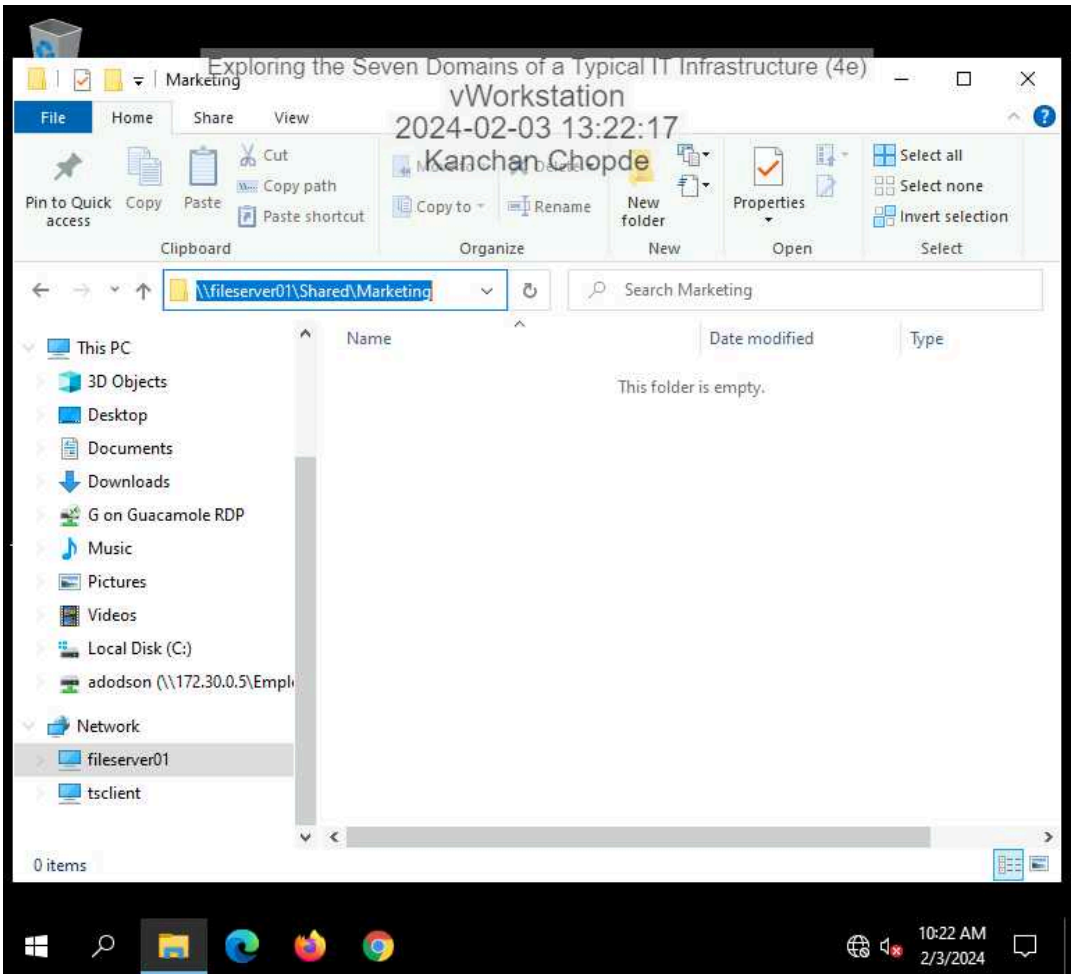
28. **Make a screen capture** showing a **successful connection to the adodson user folder**.



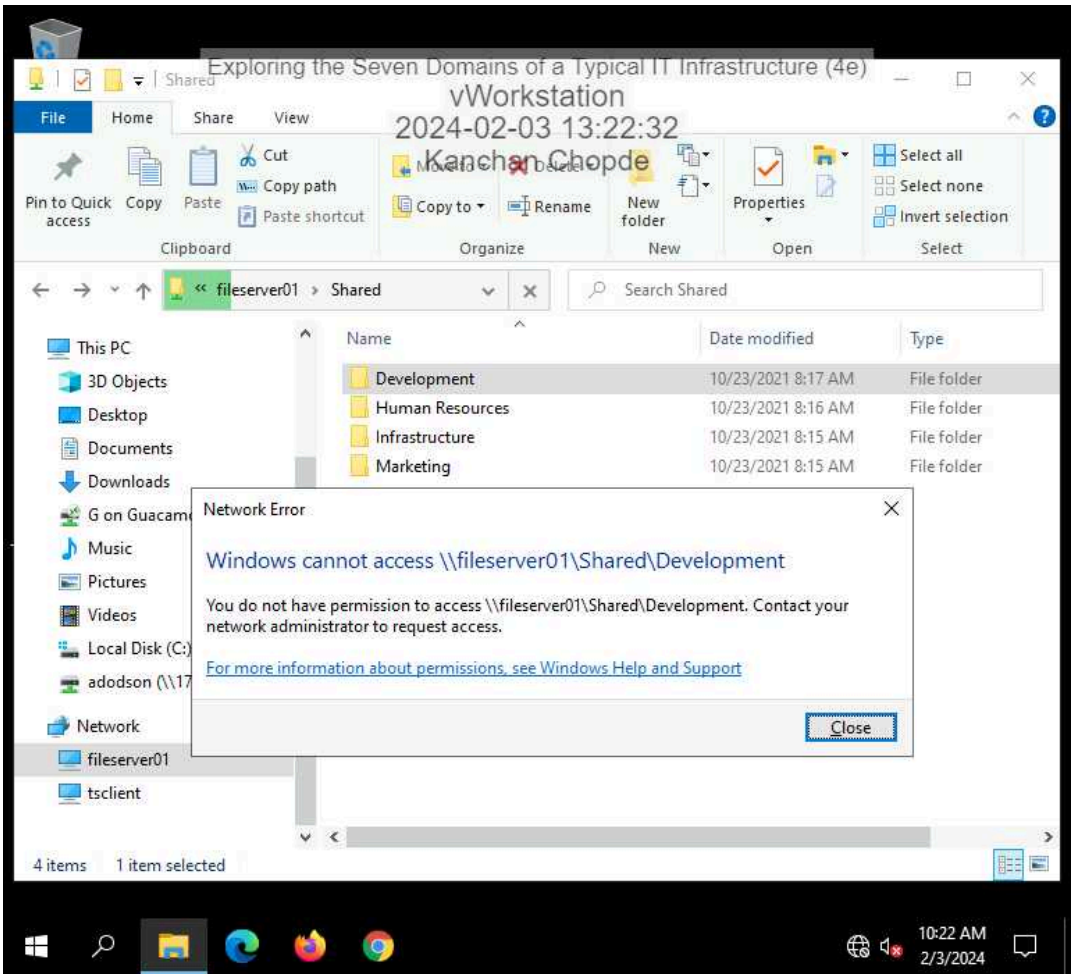
29. **Make a screen capture** showing a **failed connection to another user folder**.



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

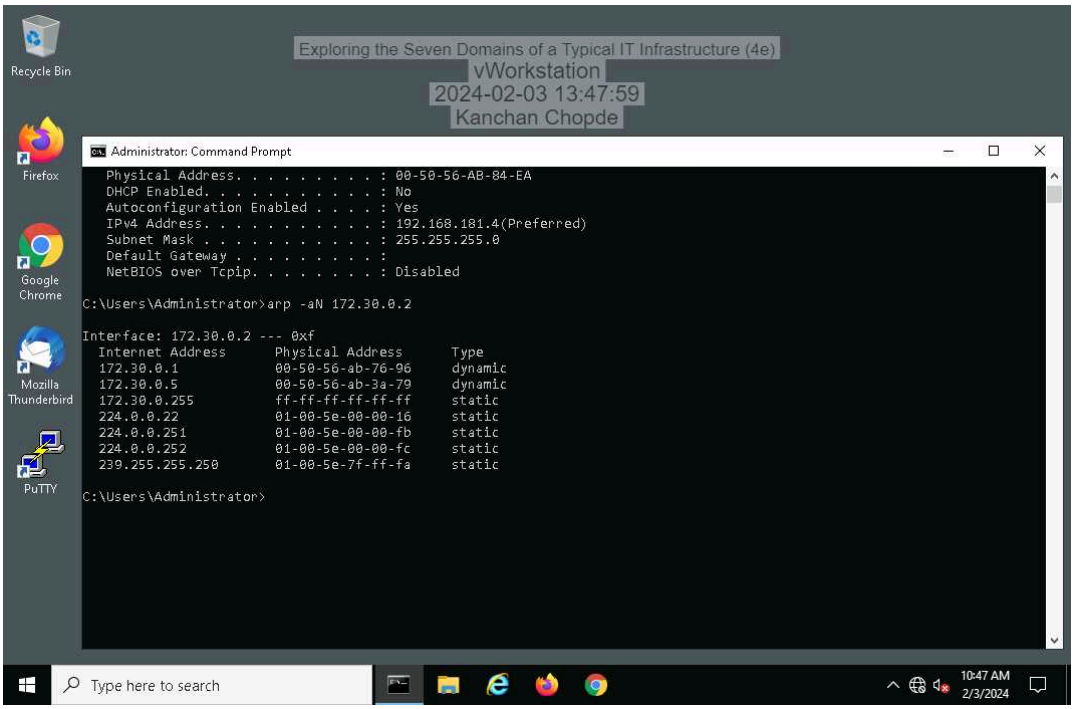


32. **Make a screen capture** showing a **failed connection to another shared folder**.

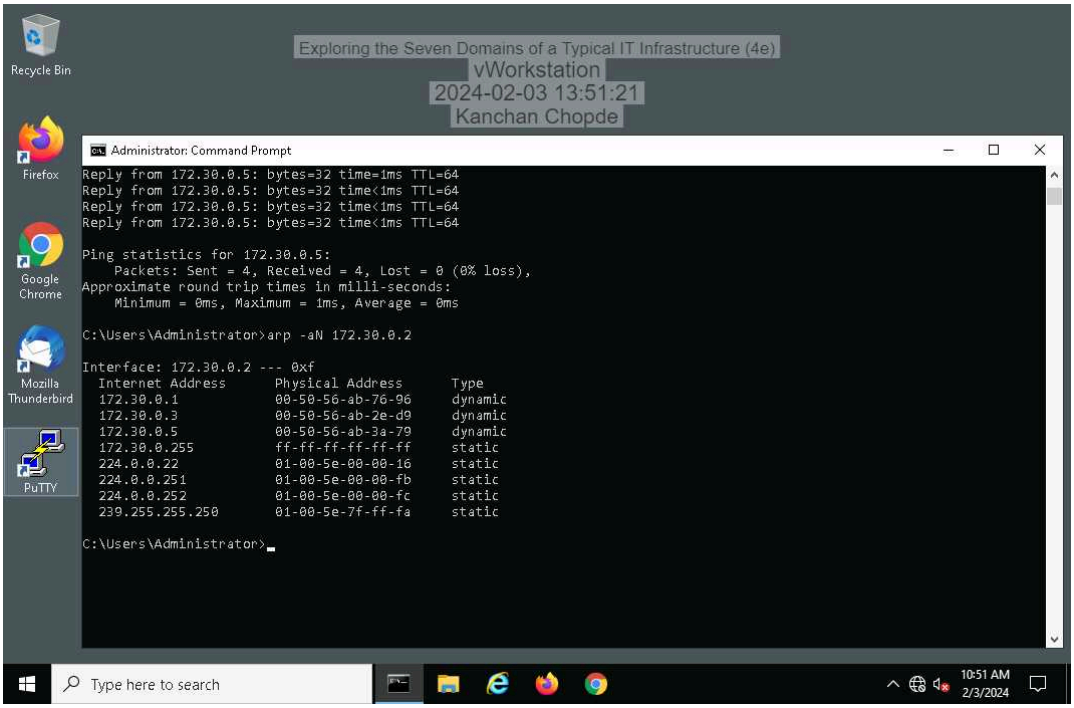


Part 2: Explore the LAN Domain

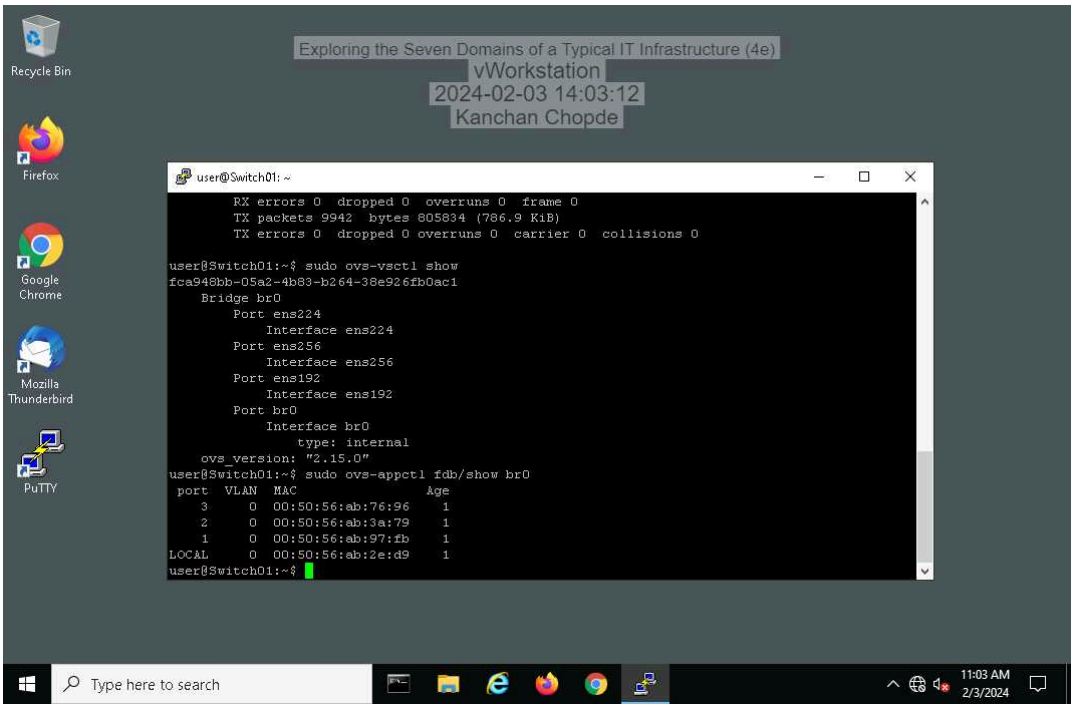
5. **Make a screen capture** showing the **vWorkstation's original ARP table**.



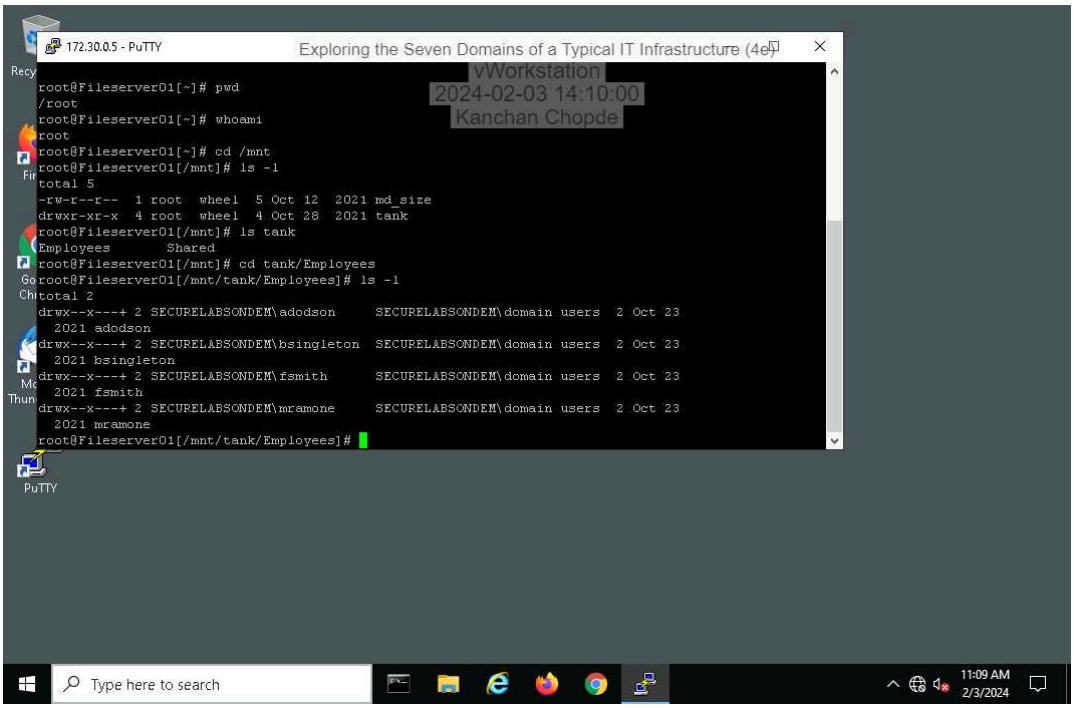
10. **Make a screen capture** showing the **vWorkstation's updated ARP table.**



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

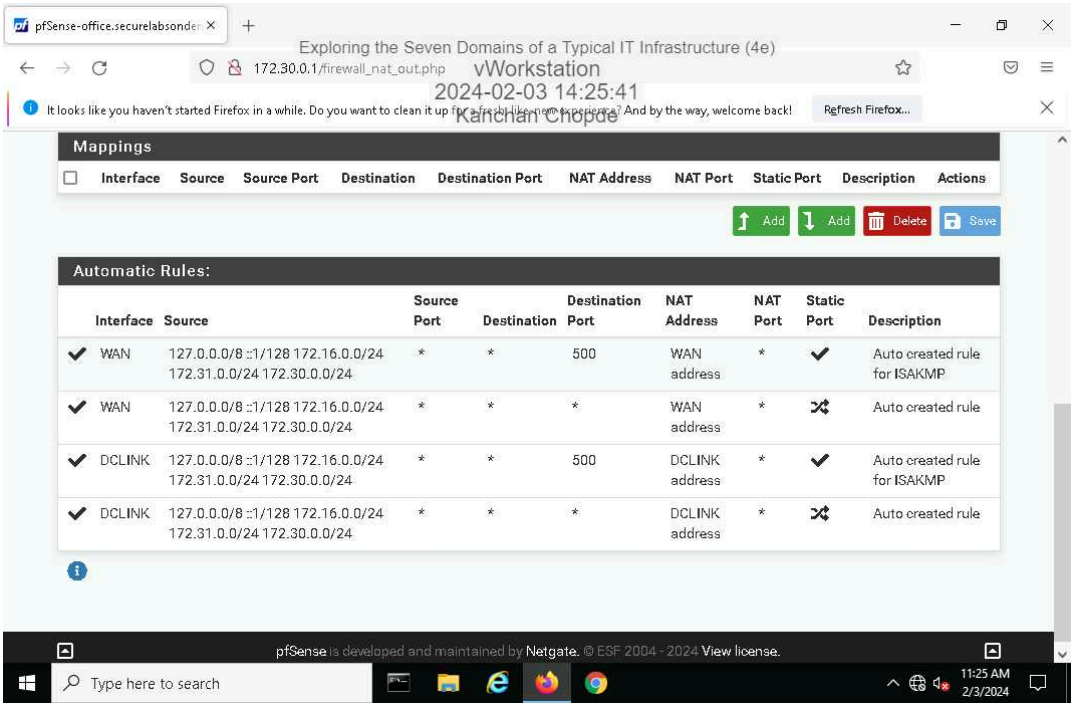


30. **Make a screen capture** showing the **contents of the Employees directory**.

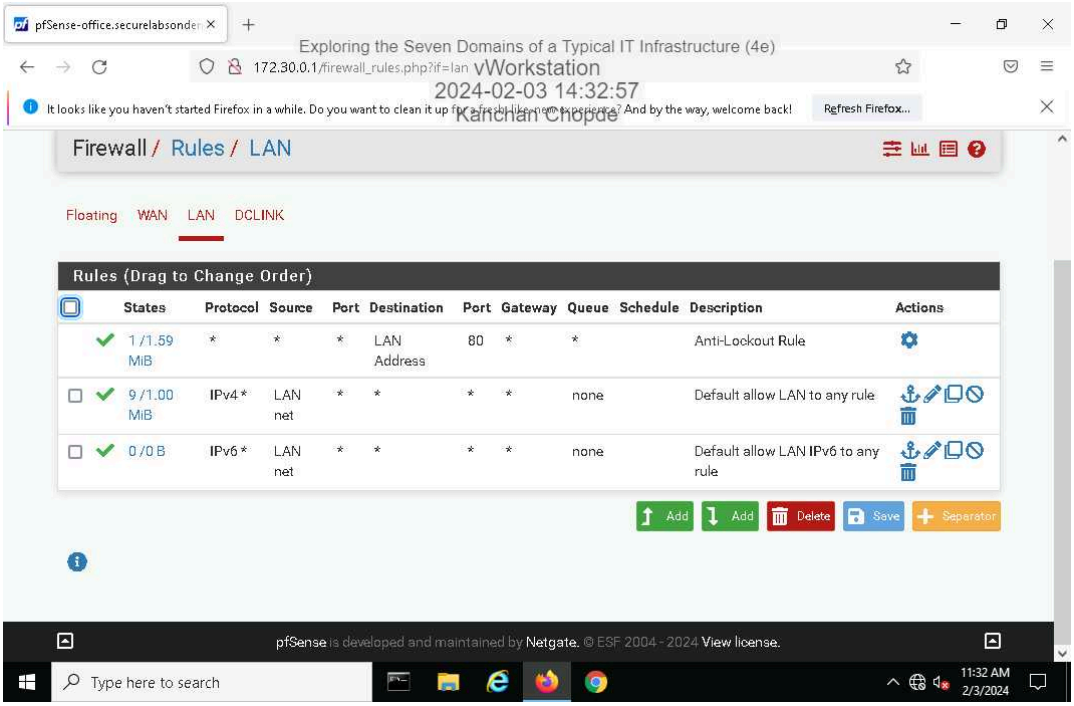


Part 3: Explore the LAN-to-WAN Domain

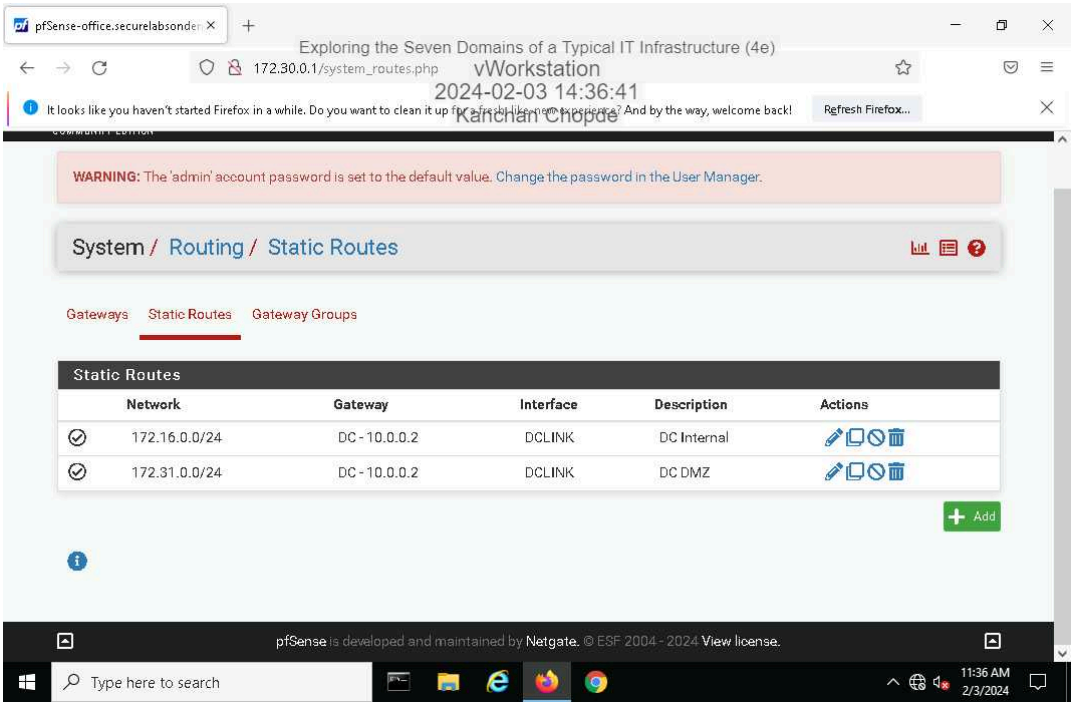
6. **Make a screen capture** showing the **Outbound NAT settings**.



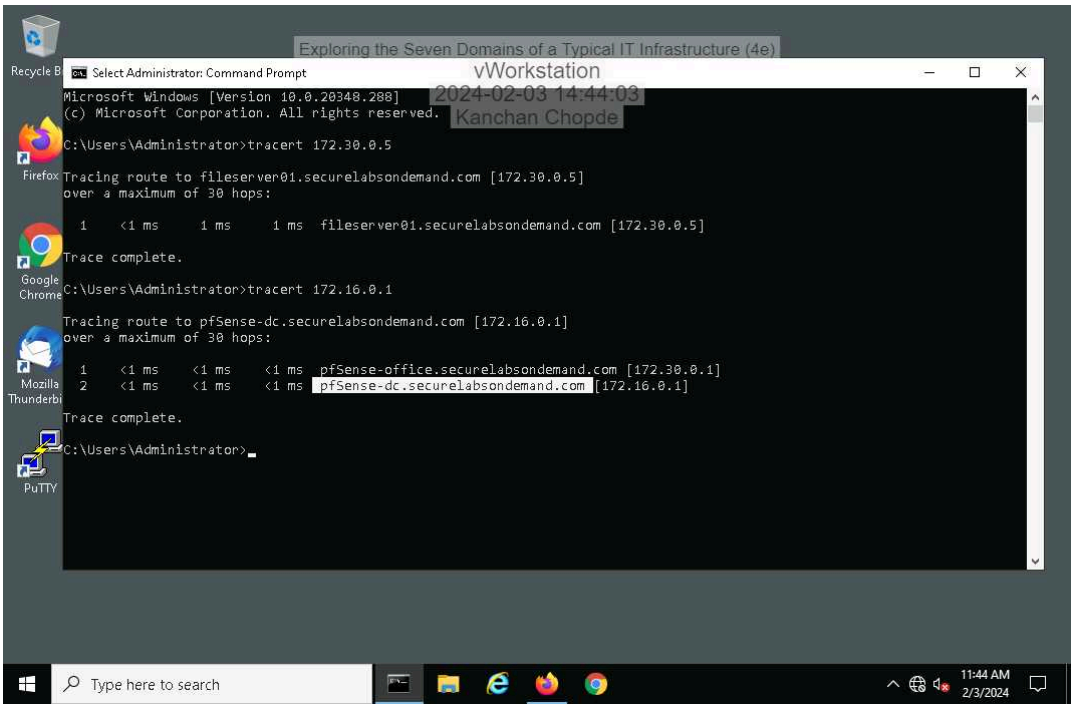
9. **Make a screen capture** showing the **permissive LAN rules**.



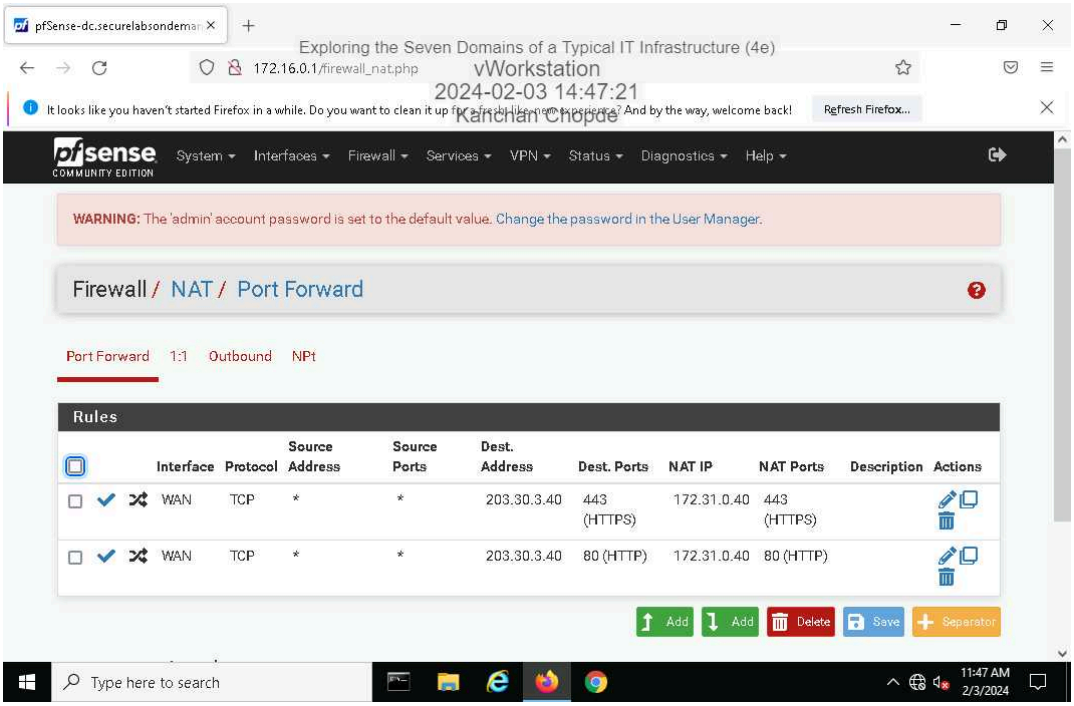
12. **Make a screen capture** showing the **Static Routes page**.



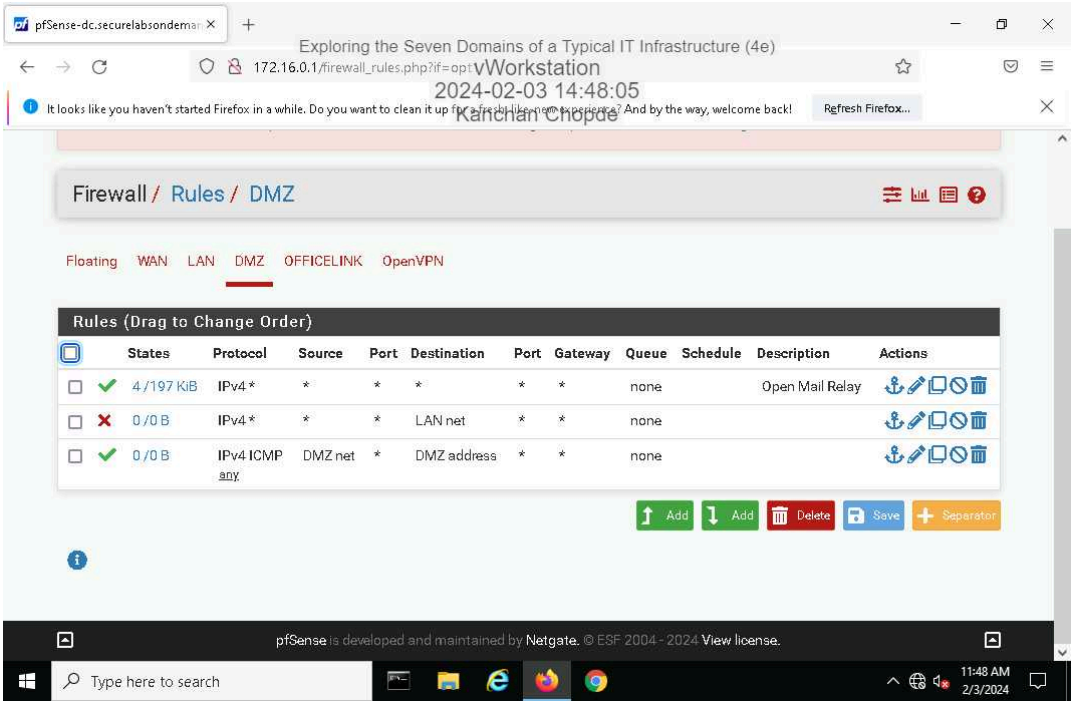
16. **Make a screen capture** showing the **result of your tracert to the pfsense-dc appliance**.



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



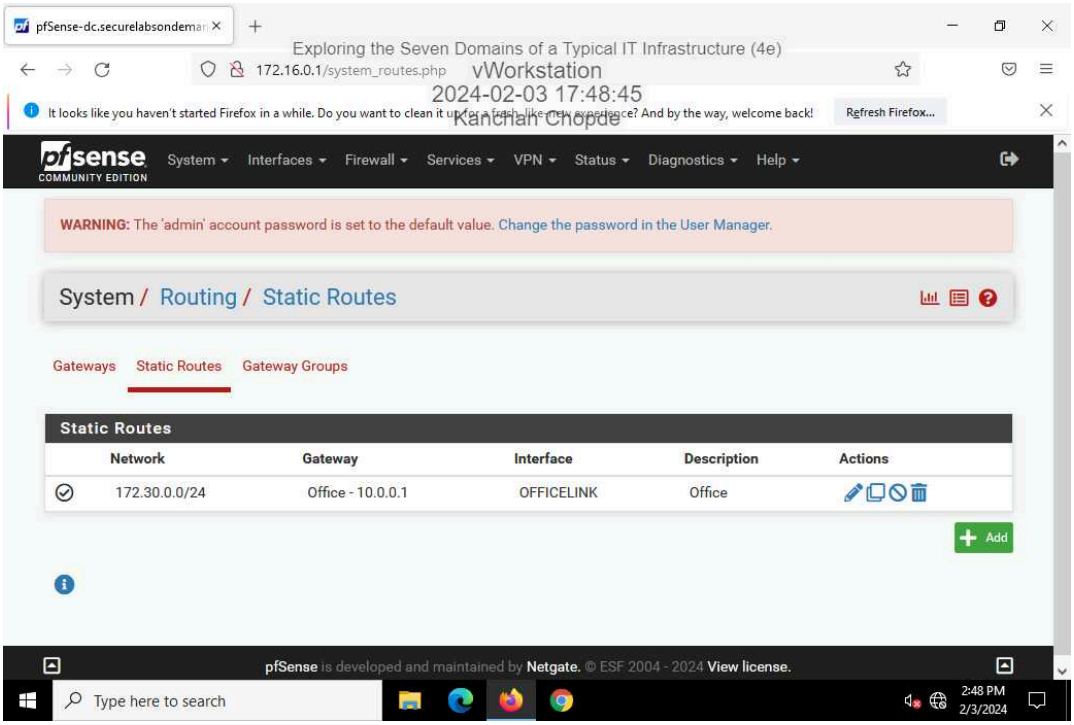
25. **Make a screen capture** showing the **DMZ firewall rules**.



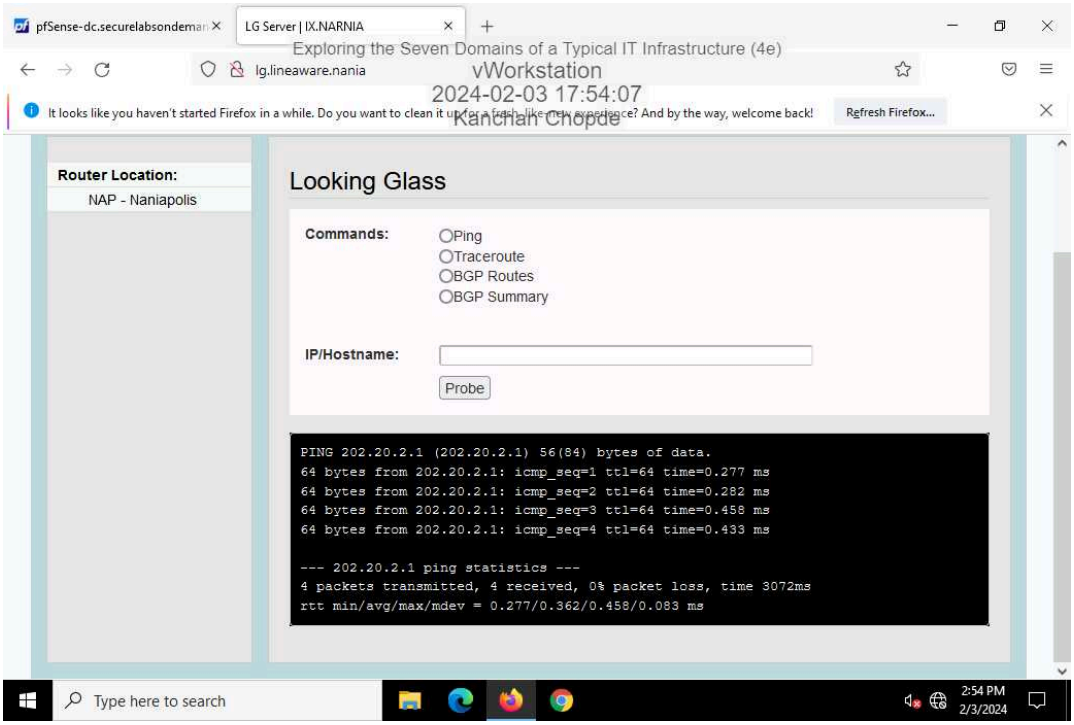
Section 2: Applied Learning

Part 1: Explore the WAN Domain

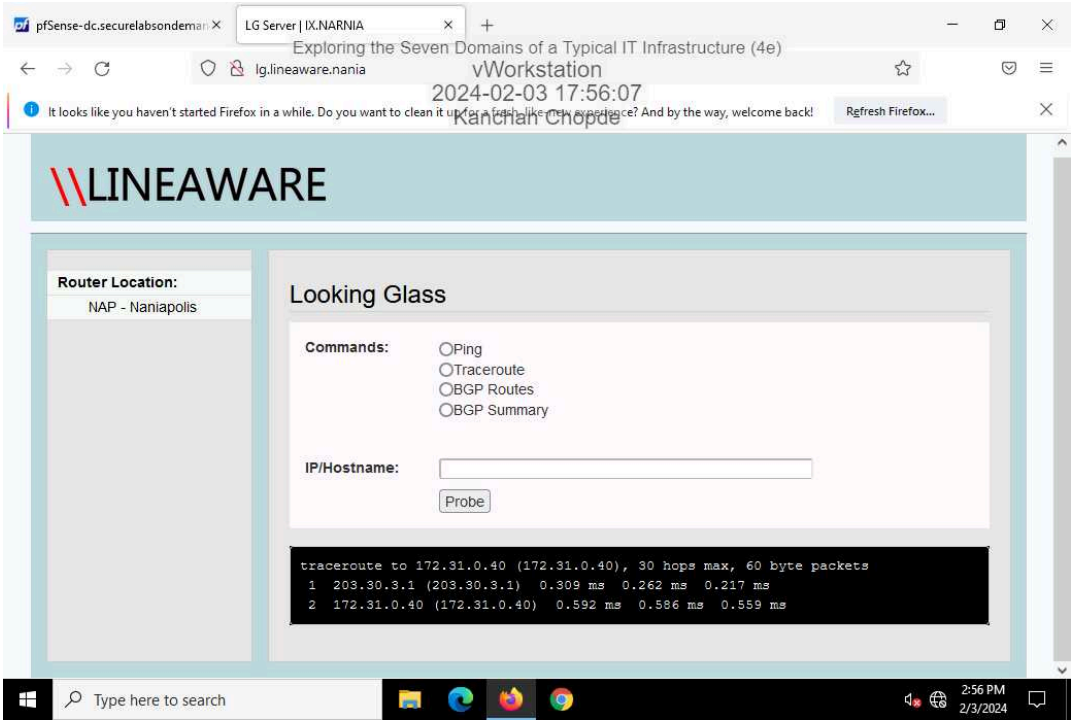
5. **Make a screen capture** showing the **static route for the point-to-point connection**.



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

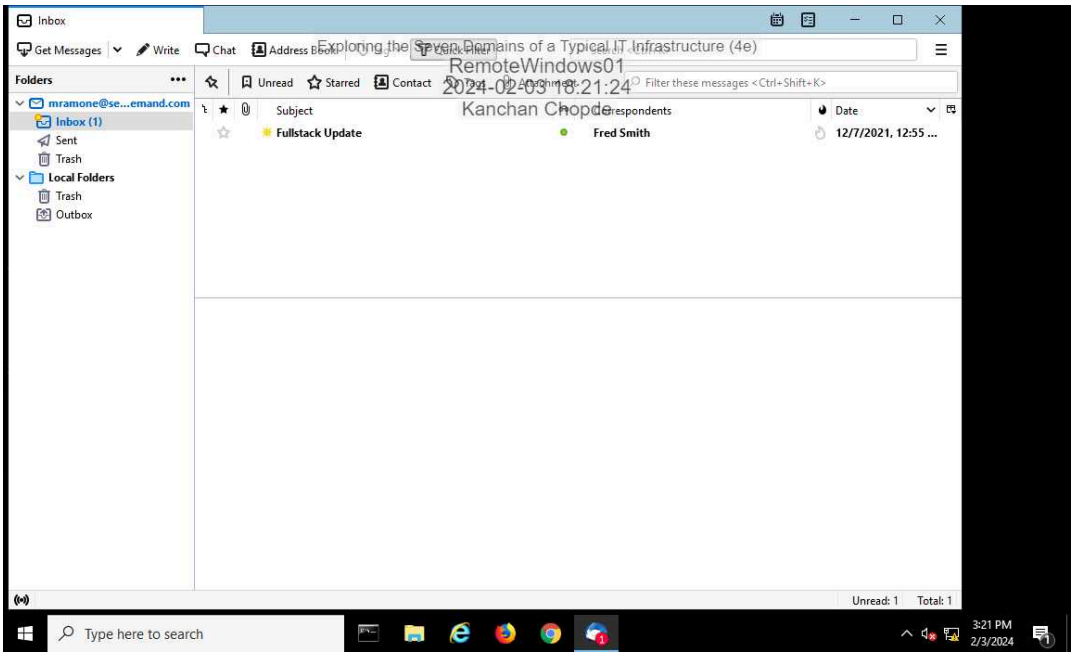


12. **Make a screen capture** showing the **traceroute to the file server**.



Part 2: Explore the Remote Access Domain

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

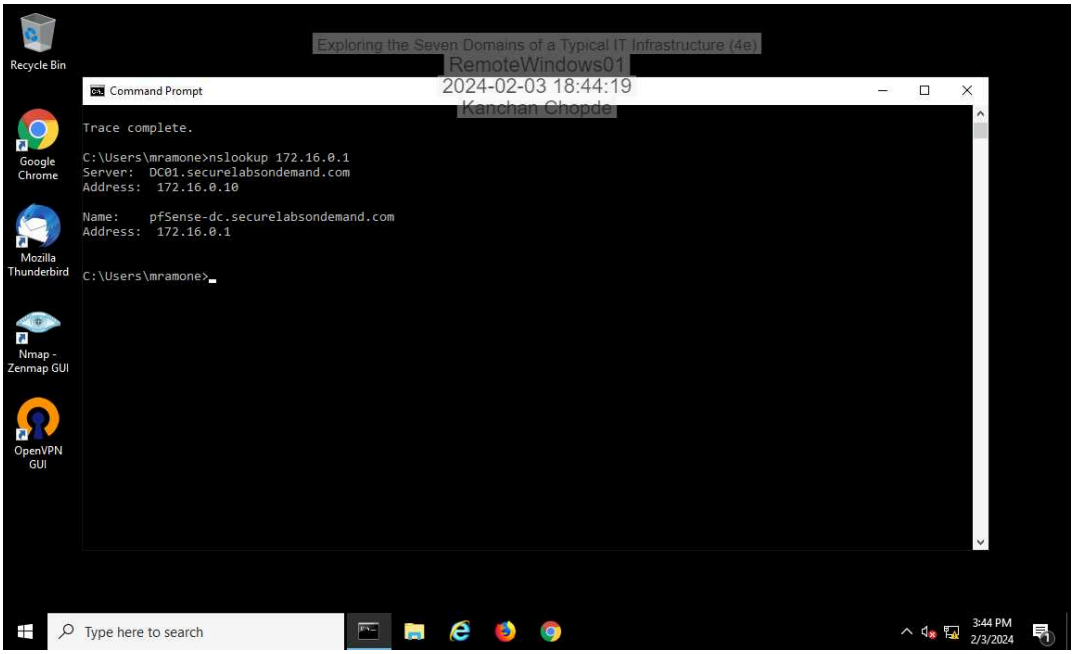


14. **Document** whether the VPN connection is split tunnel or full tunnel, based on the tracert results.

tracert 172.31.0.40 is full tunnel VPN connection as 1st hop is gateway for 172.29.0.1 network.In case of full tunnel, all traffic is routed through VPN.

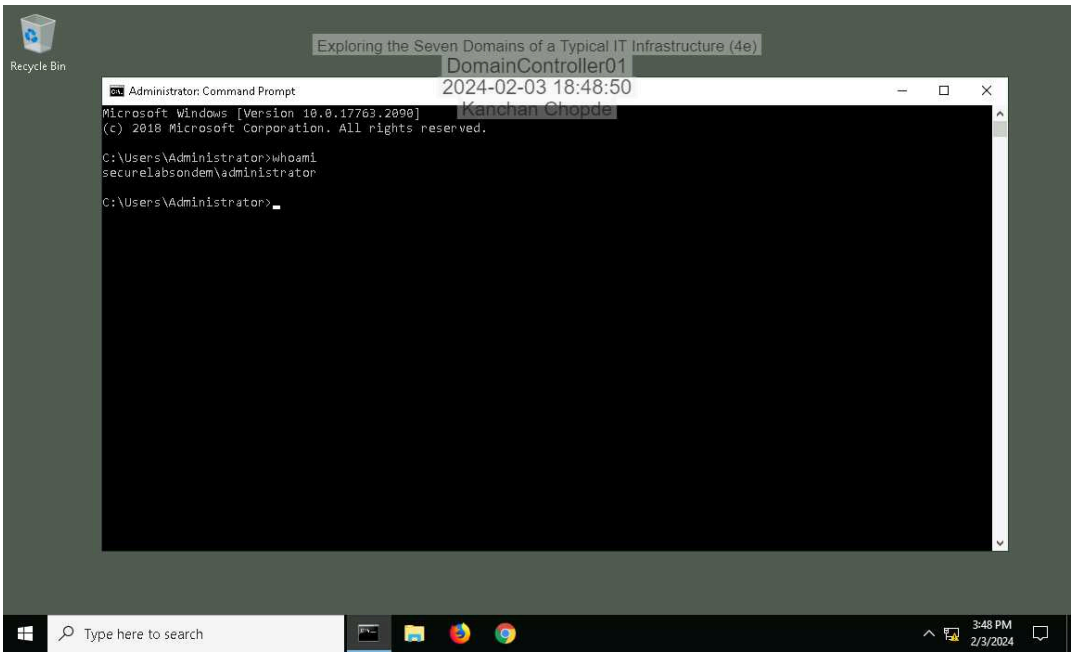
tracert 203.30.3.40 is split tunnel VPN connection as its 1st hop is gateway for 10.30.0.1 network. Traffic is allowed to split some through VPN and some by local network.

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

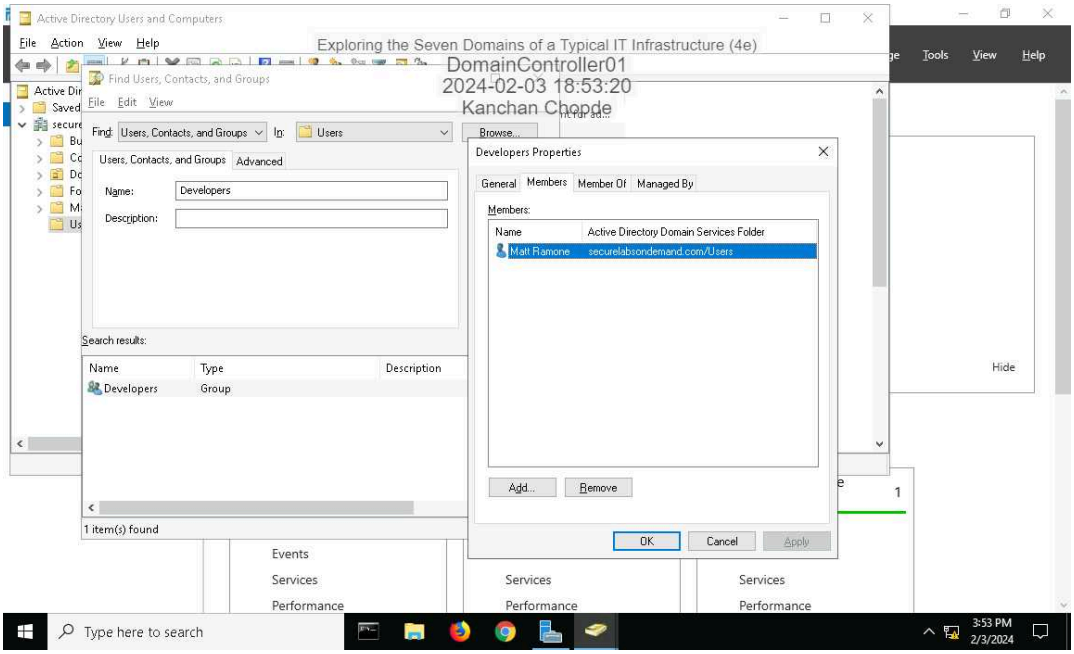


Part 3: Explore the System/Application Domain

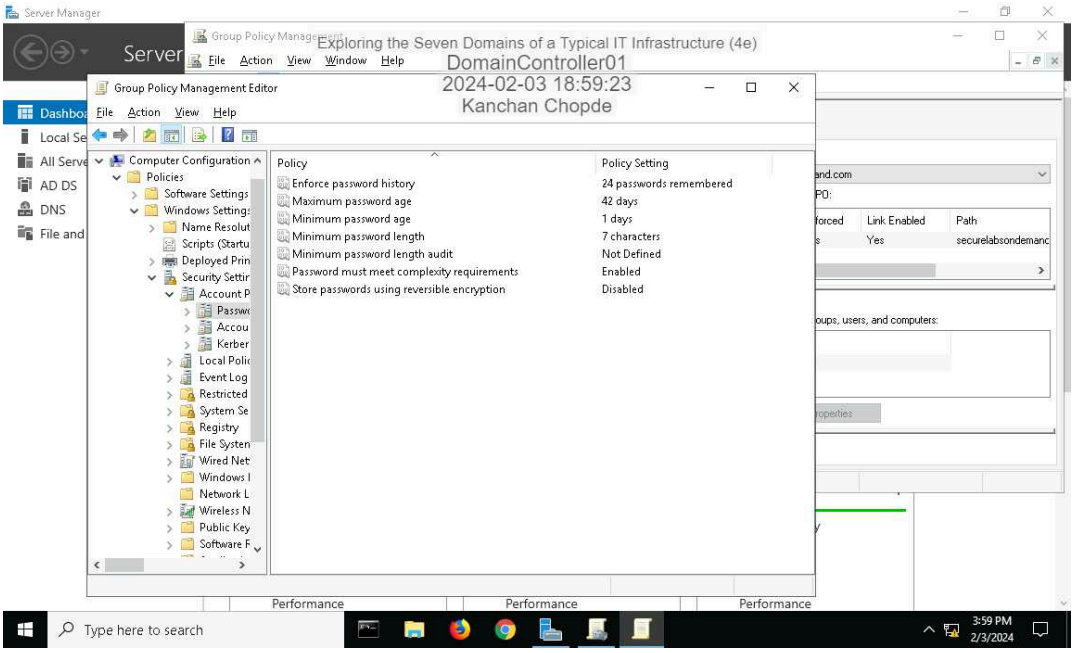
4. **Make a screen capture** showing the **whoami results**.



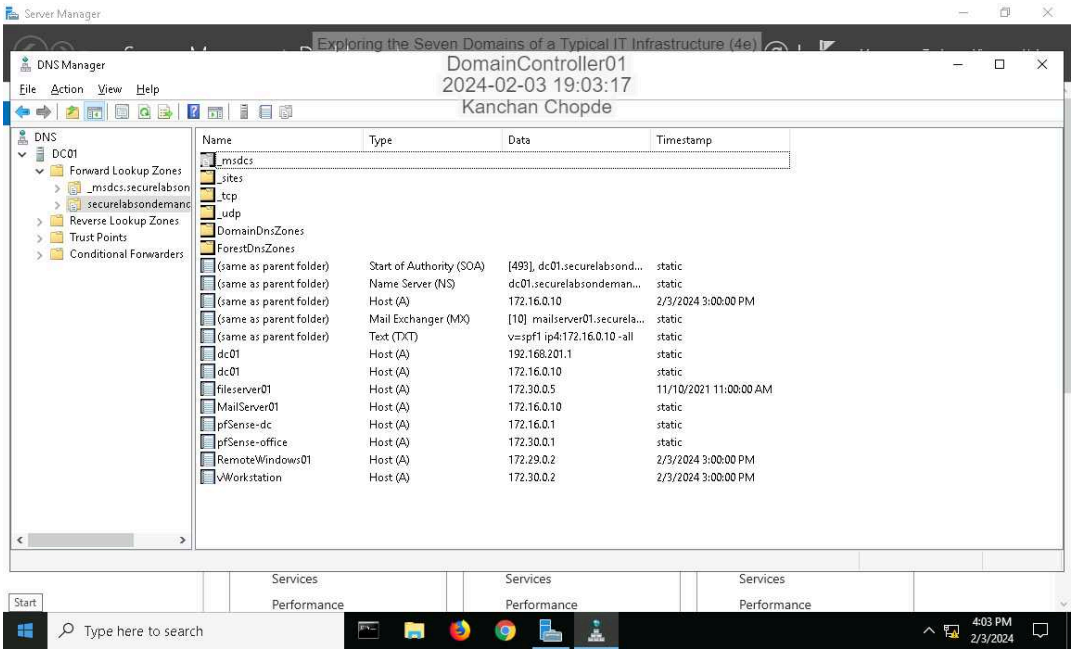
10. **Make a screen capture** showing the **members of the Developers AD group**.



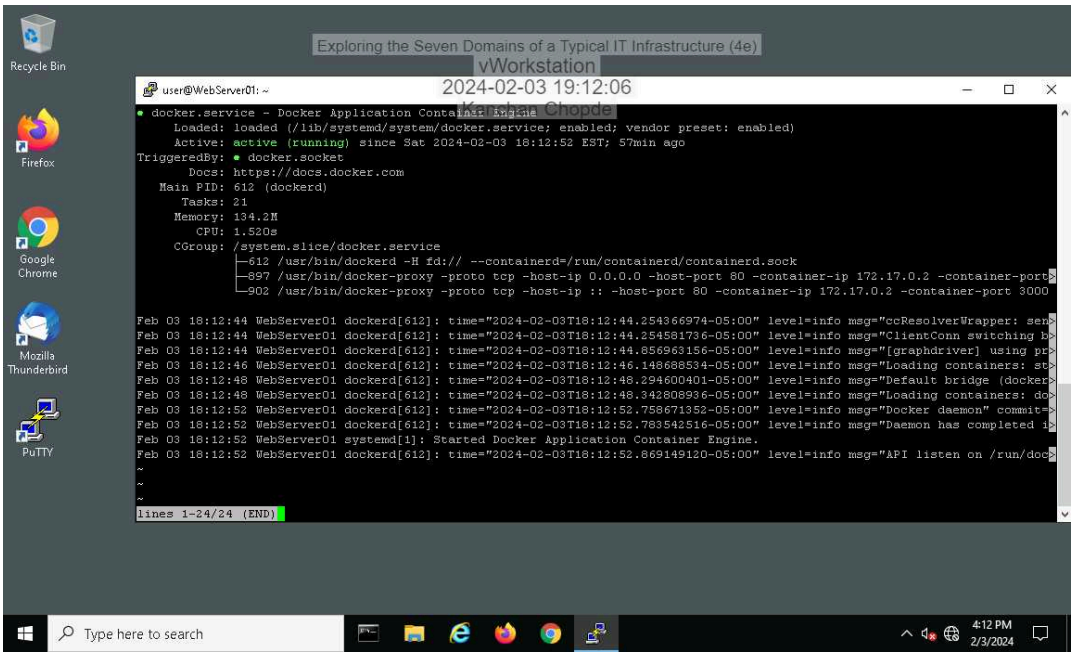
16. **Make a screen capture** showing the **password policy settings in the Group Policy Management Console**.



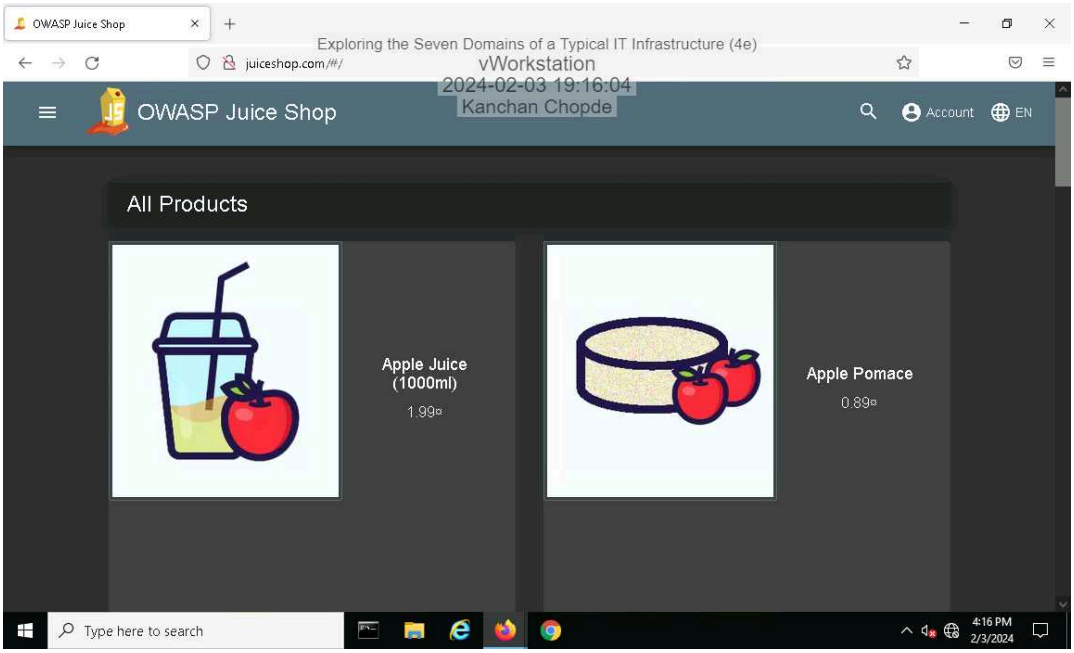
20. **Make a screen capture** showing the **DNS entries**.



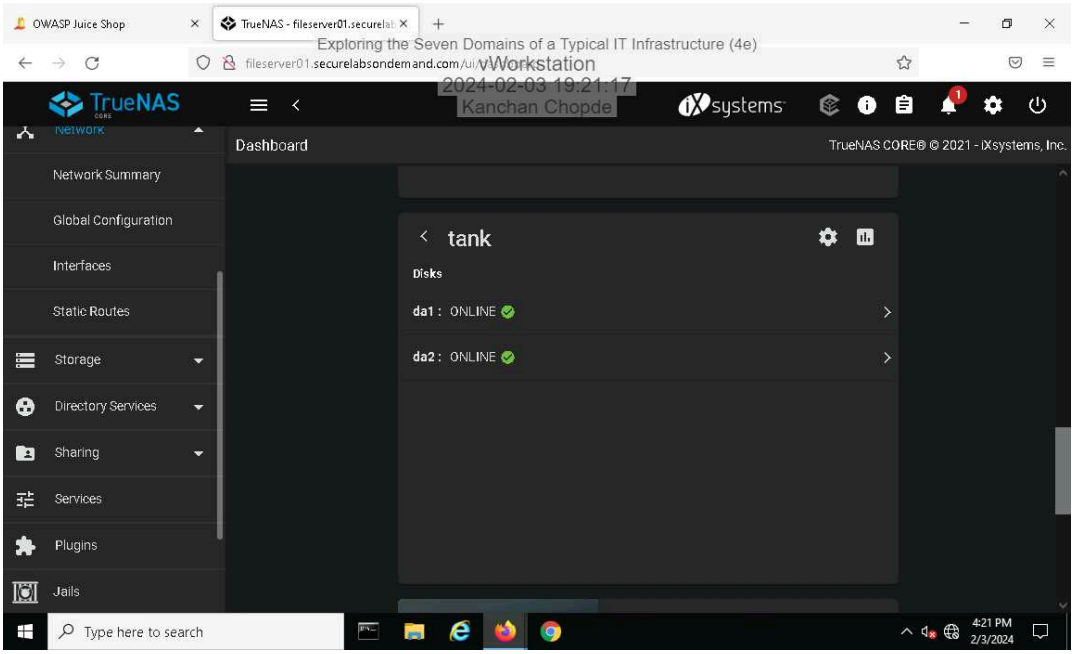
28. **Make a screen capture** showing the **Docker service status**.



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



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.

At least 2 compelling threats to the User Domain can be :
1. Unauthorized Access
Intruders can gain illegitimate access to user accounts, network or even systems by performing attacks from various techniques such as password guessing, using malicious script to gain user details or exploiting vulnerabilities in infrastructure and software.

2.Phishing Attacks:
Attackers may user various techniques to trick users into clicking malicious link which gives the attacker access to user details. Links appears to be legitimate and hence user tends to click links or share information to such phising attacks. Most common type is through emails or messages where users are tricked to either enter personal details, click malicious links or install some software. (ref:https://support.google.com/a/answer/7492705?hl=en)

Effective Security Controls:
Physical security controls: such as making use of surveillance cameras, access cards, security cams, biometric entries etc.

Digital security controls: usage of firewalls, multi-factor authentication mechanisms, password keeping etc.

Cyber security controls:Awarness trainings, firewalls, encryptions techniques etc

Cloud security controls: meeting industry and policy regulations if using cloud services.

(ref: https://www.ibm.com/topics/security-controls)

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.

Security Controls to implement:

Workstation: For a workstation, using antivirus software can be one of the best options to prevent,

detect and remove malware. It gives us complete protection against any attack by running in regular intervals and giving us the indication if anything seems suspicious. Also it provides way to repair the damage.
(ref: https://en.wikipedia.org/wiki/Antivirus_software)

LAN: In local area network, there is a requirement to access network security for devices connecting to LAN , for them NAC Network Access Control can access the security by providing security, restricting access to non-compliant users, enforcing policies such as type of users allowed to access area of network.

(ref:https://en.wikipedia.org/wiki/Network_Access_Control)

LAN-to-WAN: Network-based Firewalls can be positioned between LAN and WAN networks. They help in controlling data flow between these connected networks. They can be either software applications installed or hardware appliances running on some specially allocated hardware.
(ref:https://en.wikipedia.org/wiki/Firewall_(computing))

WAN: VPNs virtual private networks can be used to establish secure tunnels over public networks. VPNs provide confidentiality and authentication for data in transit.

(ref:https://en.wikipedia.org/wiki/Virtual_private_network)

Remote Access: MFA- is multi-factor authentication used to provide multiple ways of authentication such as passwords, security tokens, biometrics, one-time passwords email verifications, etc.

(ref:https://www.onelogin.com/learn/what-is-mfa)

System/Application Domain: Access Controls: enforcing controls within applications to restrict users from using particular/sensitive data such as adding authorized users in active directory groups and ensuring authenticated users have access to assigned domains.

(ref:https://learn.microsoft.com/en-us/windows/win32/ad/how-access-control-works-in-active-directory-domain-services)