Student:	Email:
Yengkong Sayaovong	ysayaovo@asu.edu

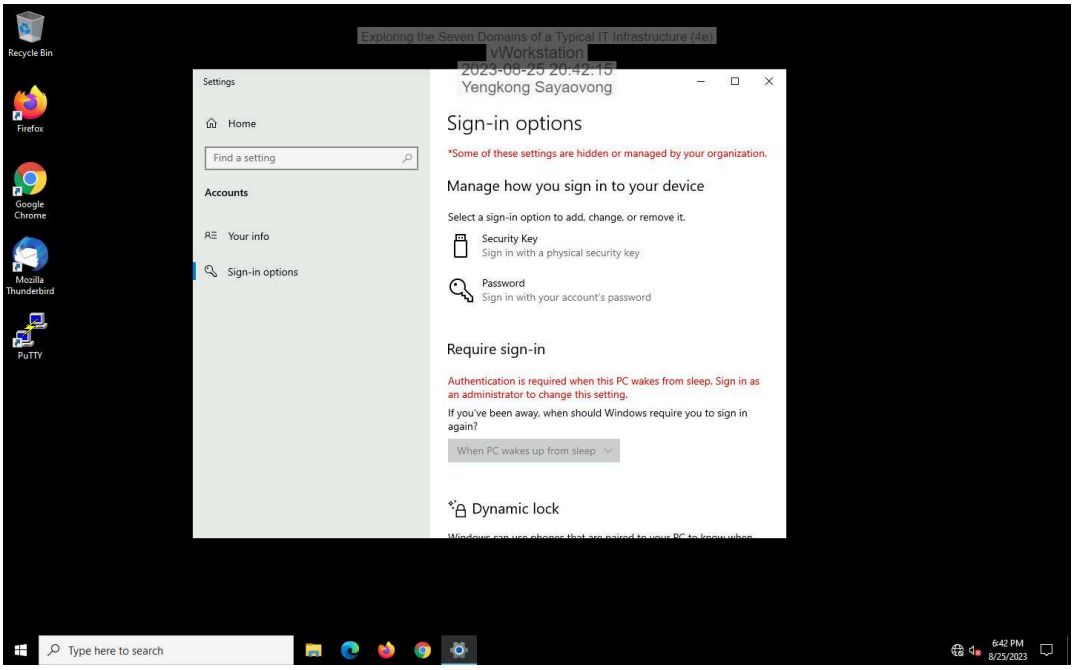
Time on Task:	Progress:
1 hour, 2 minutes	100%

Report Generated: Friday, August 25, 2023 at 10:31 PM

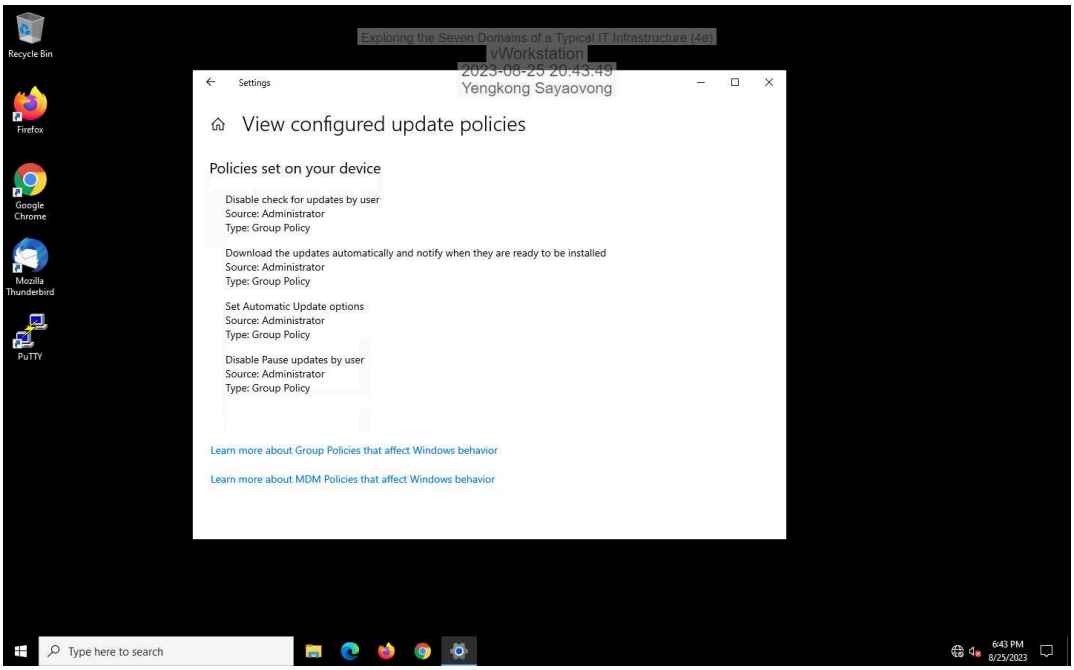
Section 1: Hands-On Demonstration

Part 1: Explore the Workstation Domain

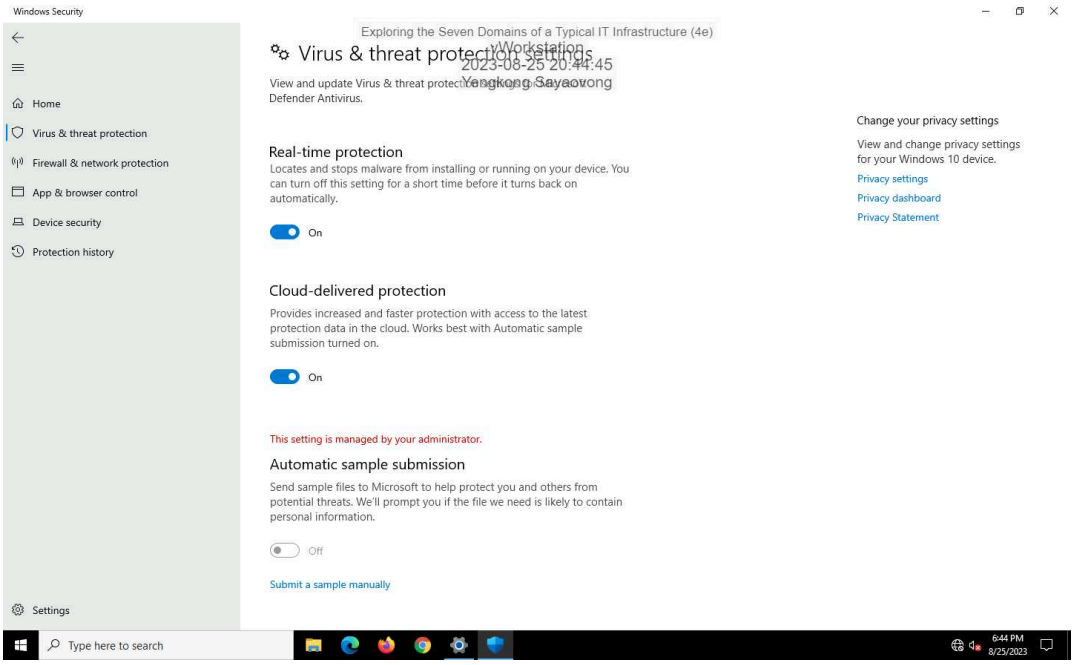
4. **Make screen capture** showing the **Sign-in options for Alice's account**.



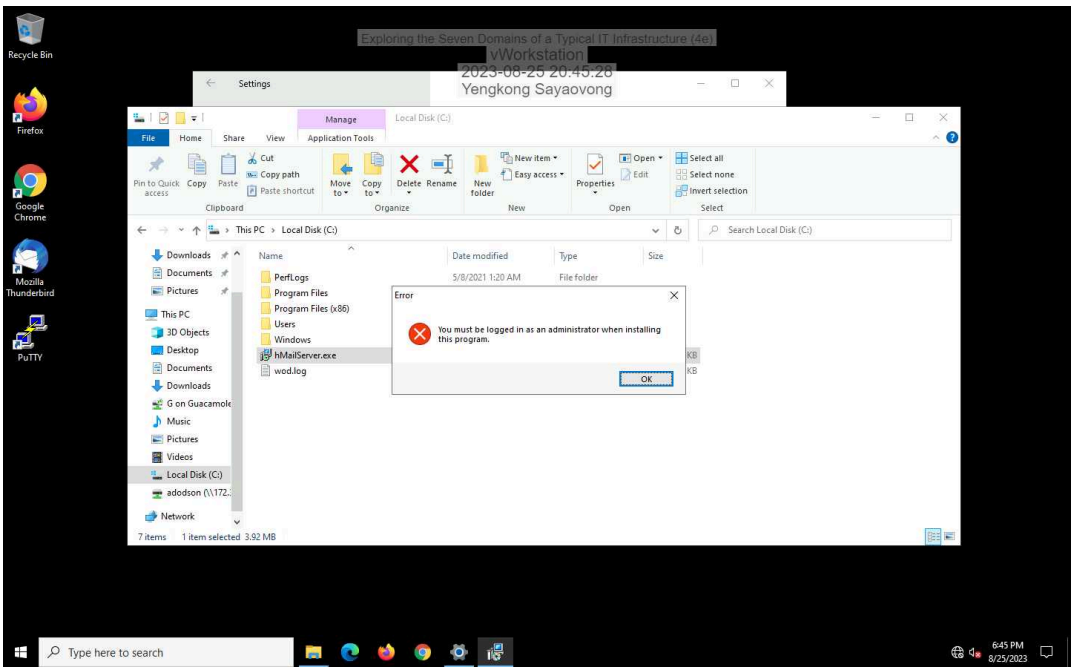
7. **Make a screen capture** showing the **View configured update policies page**.



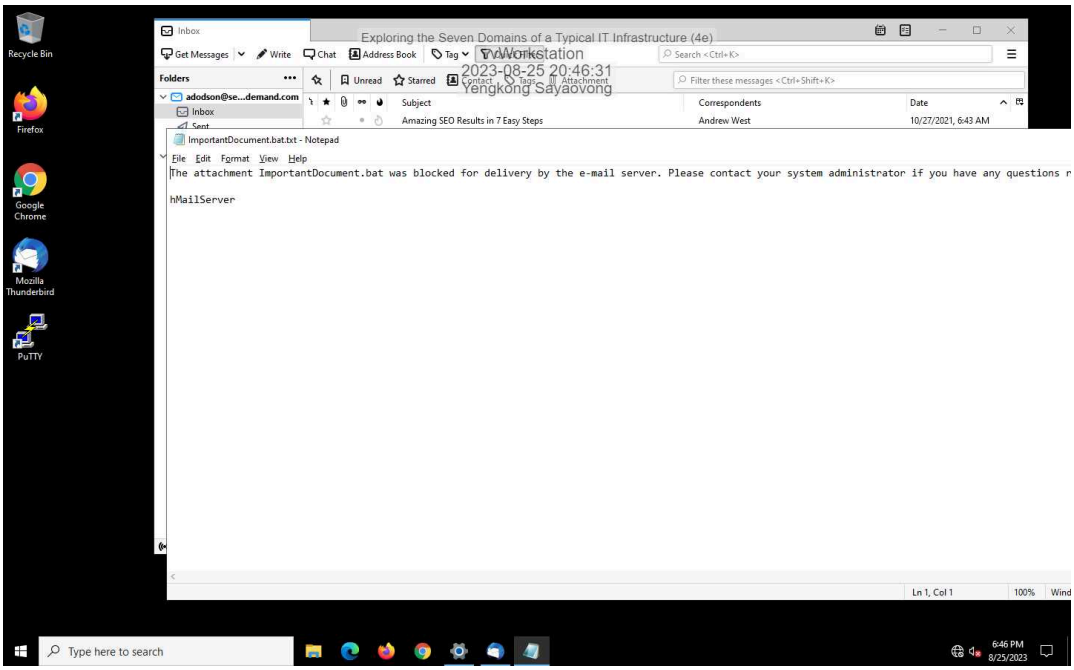
14. **Make a screen capture** showing the **Virus & Threat Protection Settings**.



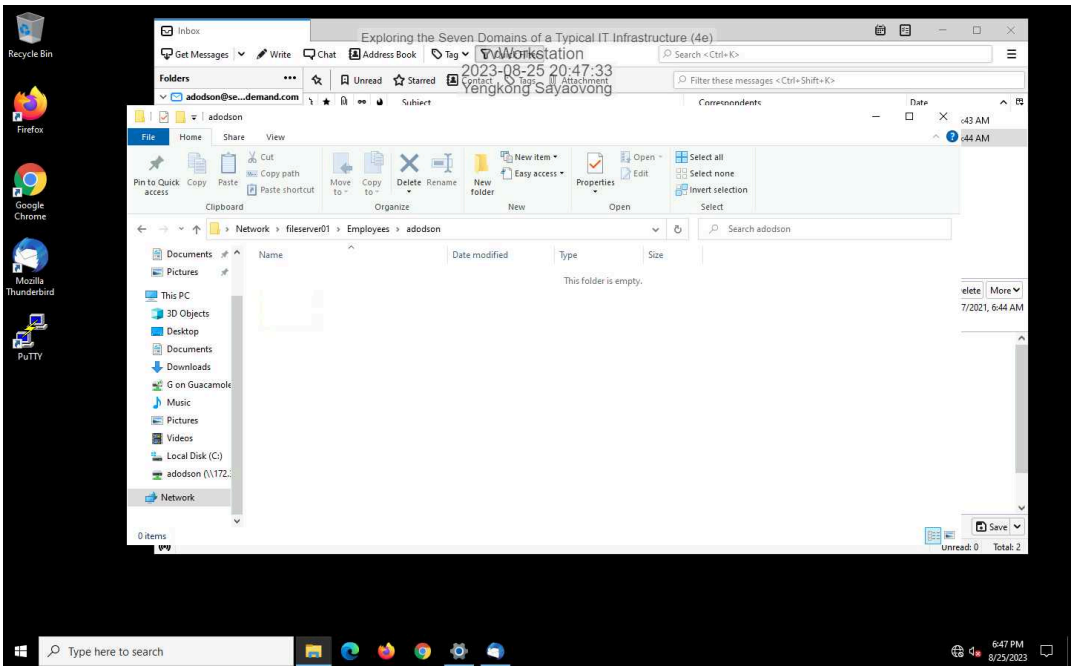
18. **Make a screen capture** showing the **security warning from attempting to run an executable file**.



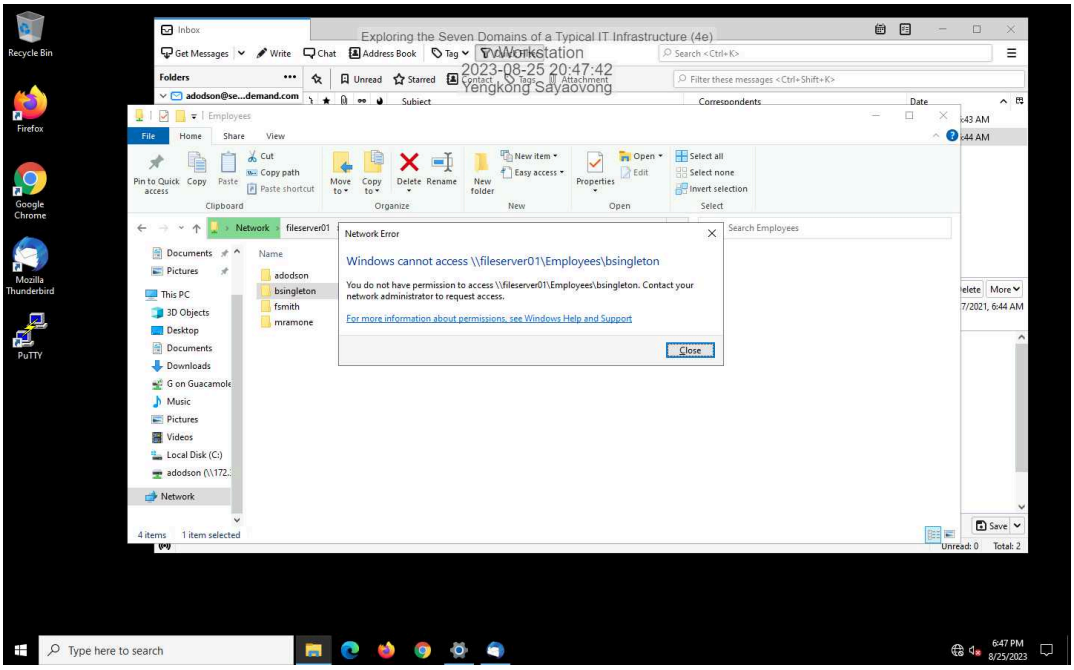
24. **Make a screen capture** showing the **blocked attachment message**.



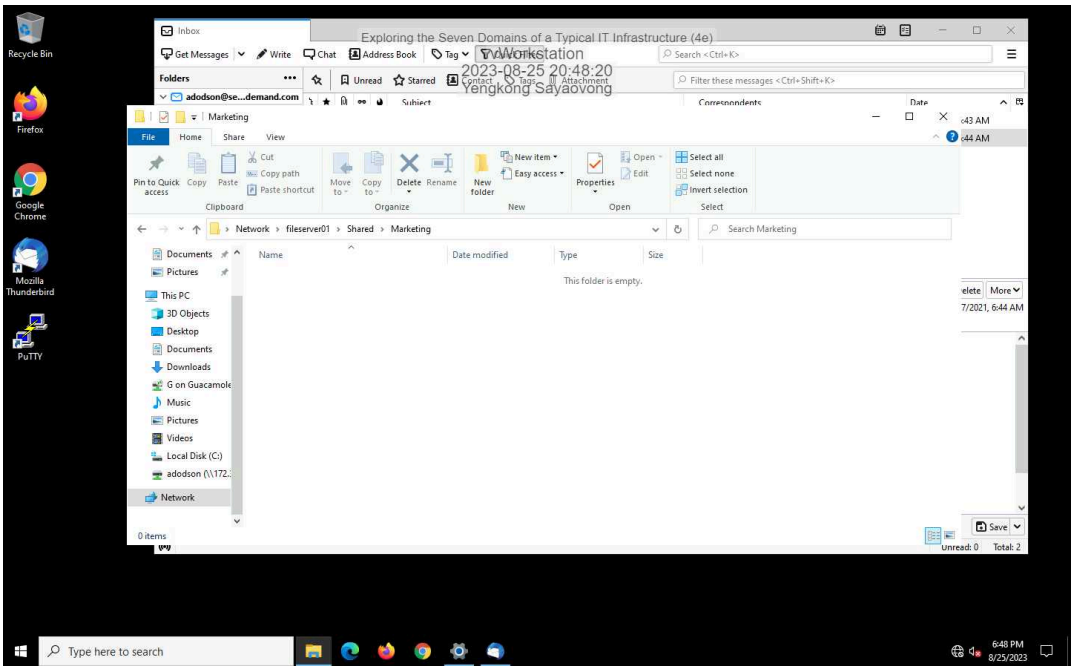
28. **Make a screen capture** showing a **successful connection to the adodson user folder**.



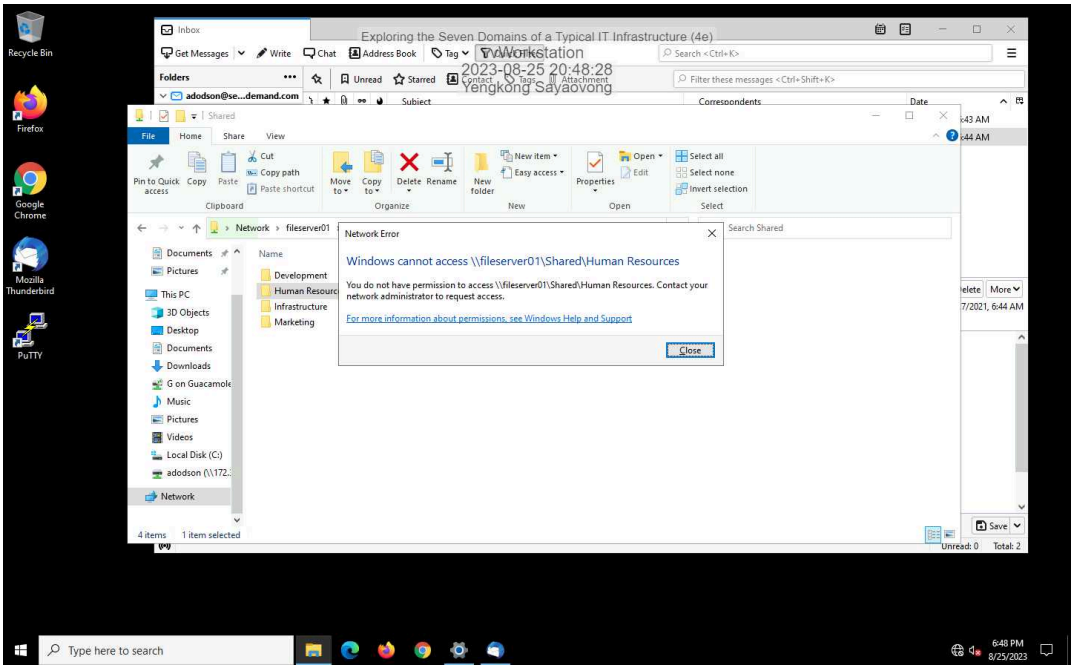
29. **Make a screen capture** showing a **failed connection to another user folder**.



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

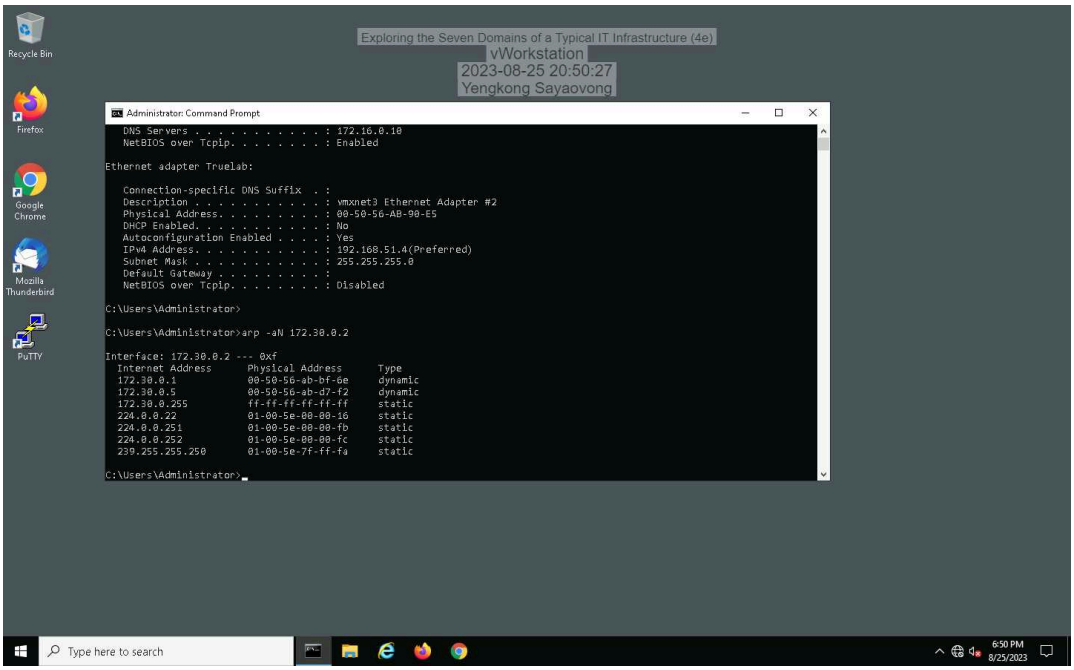


32. **Make a screen capture** showing a **failed connection to another shared folder**.

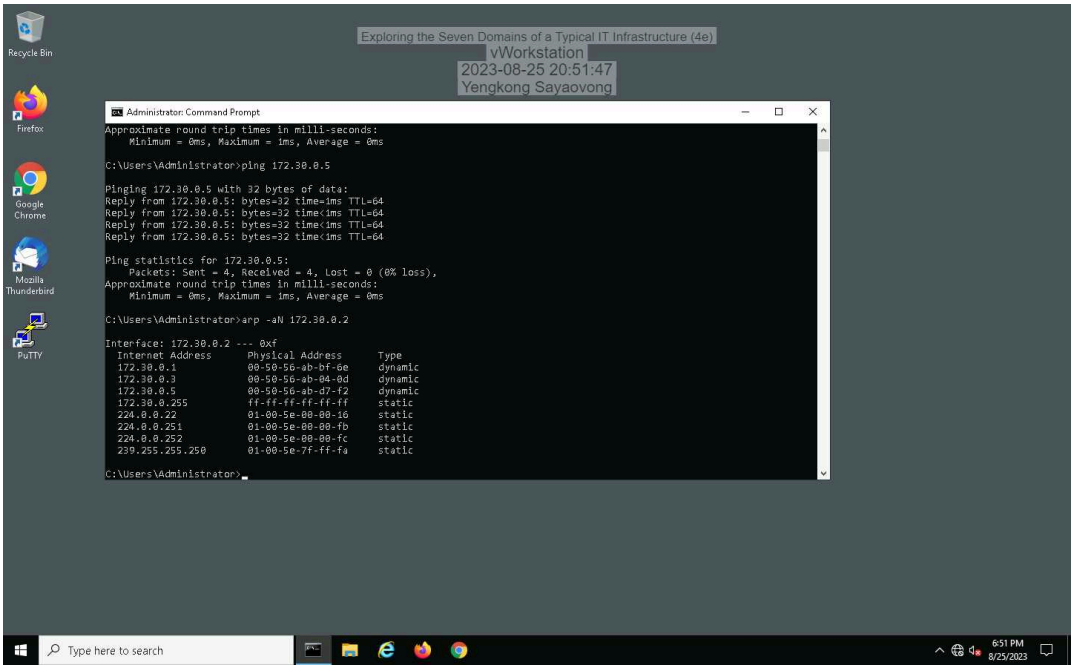


Part 2: Explore the LAN Domain

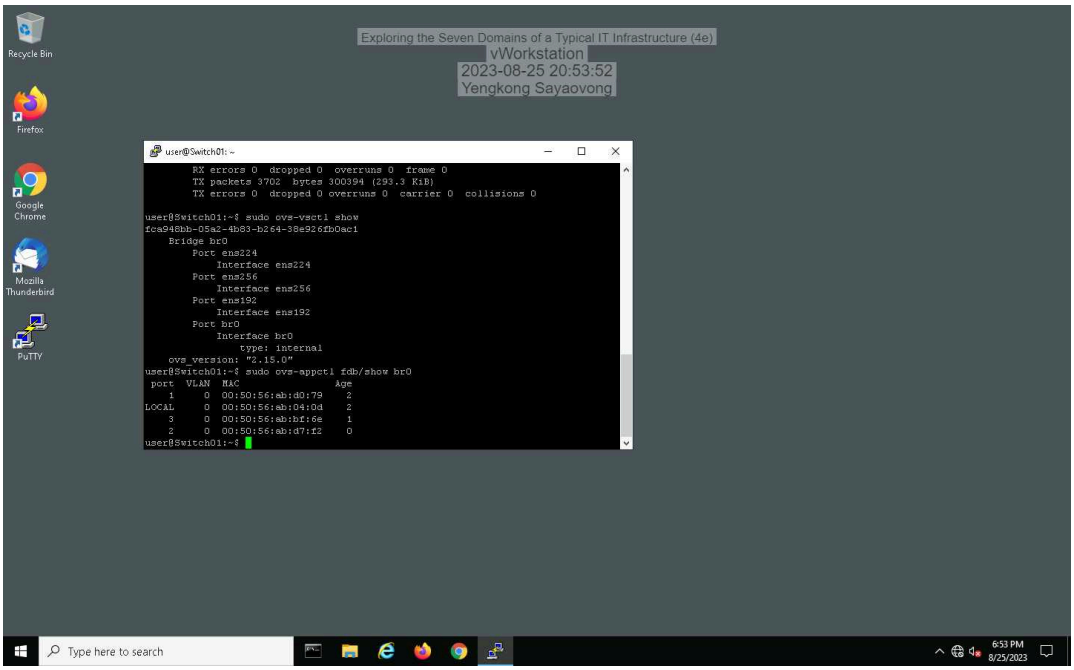
5. **Make a screen capture** showing the **vWorkstation's original ARP table**.



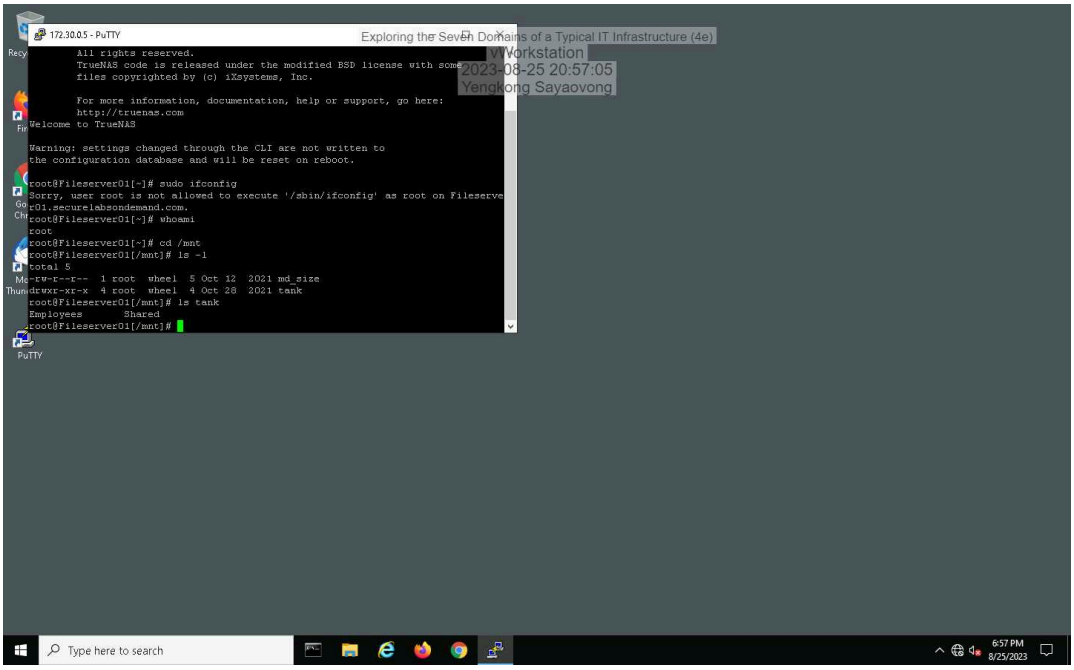
10. **Make a screen capture** showing the **vWorkstation's updated ARP table.**



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

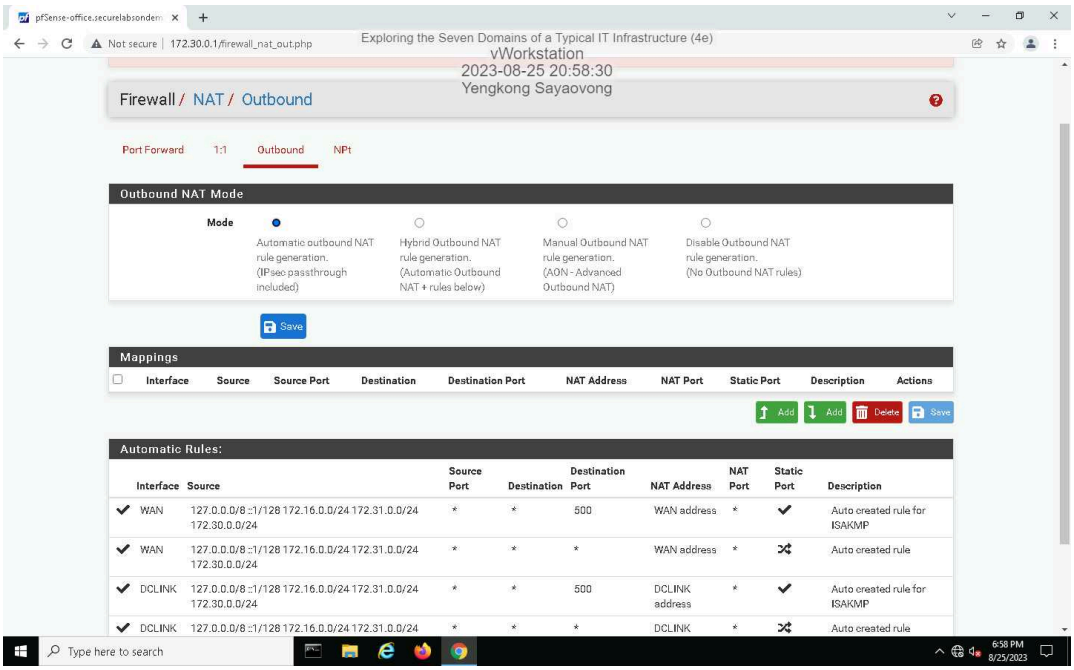


30. **Make a screen capture** showing the **contents of the Employees directory**.

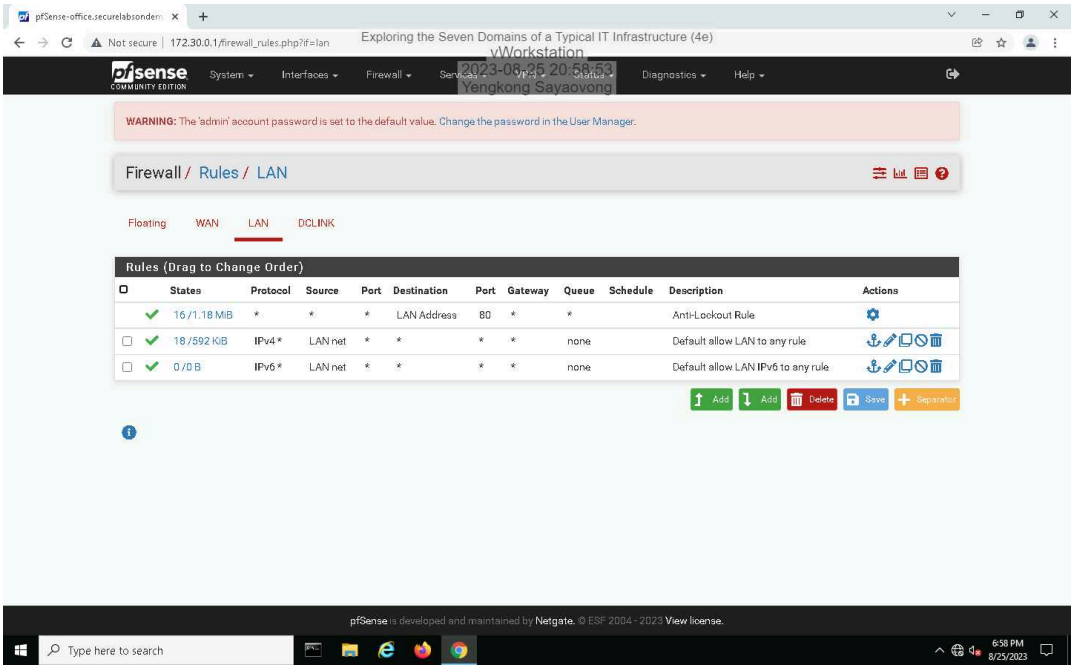


Part 3: Explore the LAN-to-WAN Domain

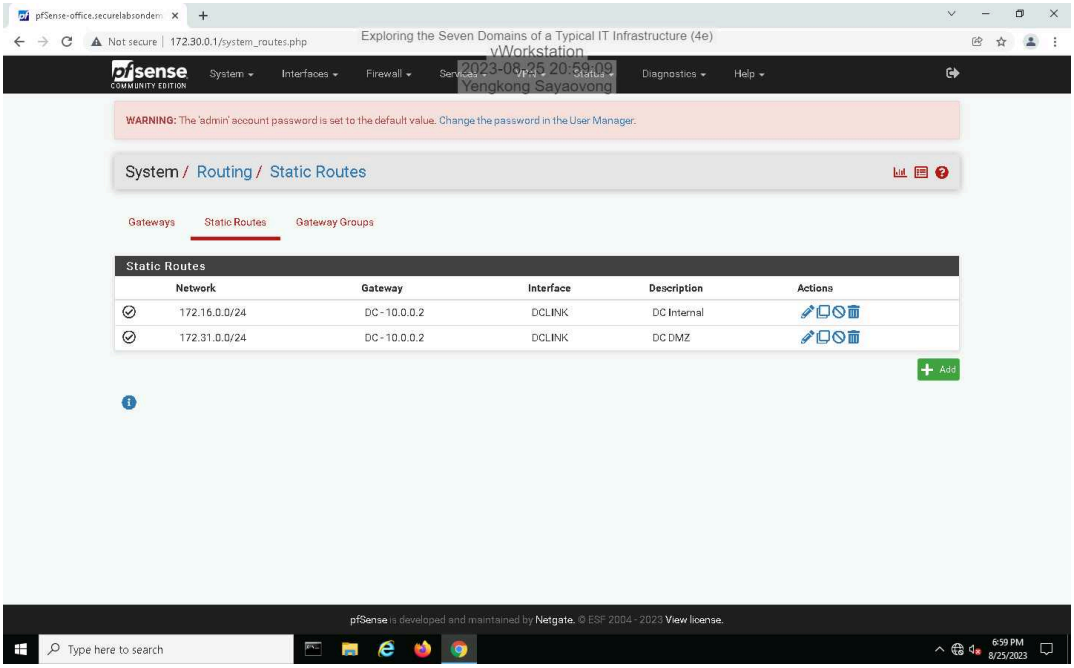
6. **Make a screen capture** showing the **Outbound NAT settings**.



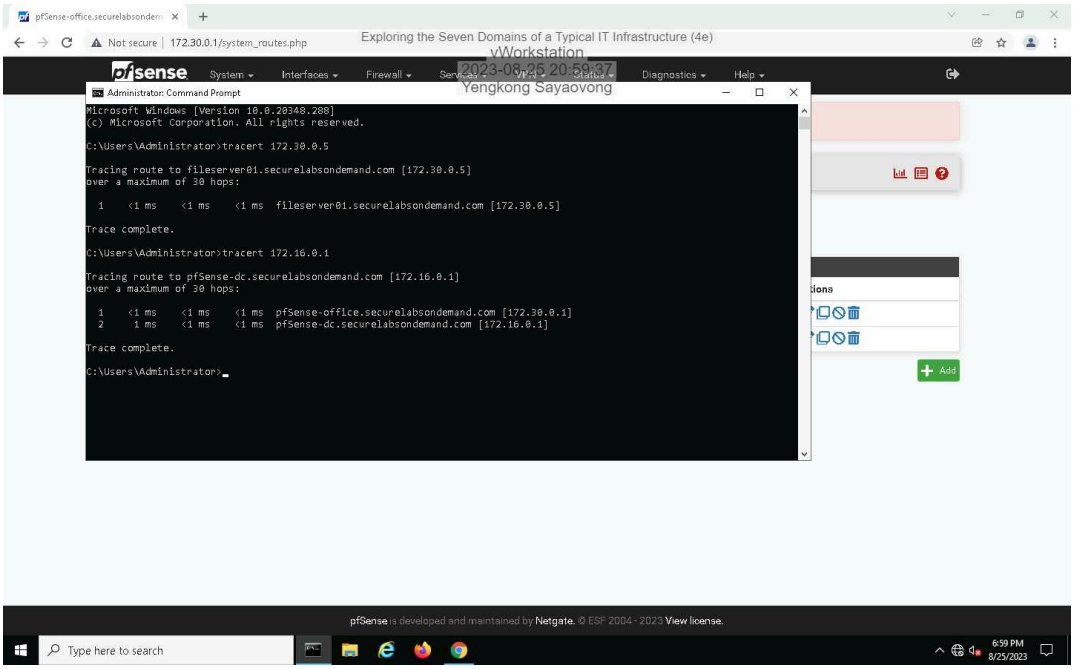
9. **Make a screen capture** showing the **permissive LAN rules**.



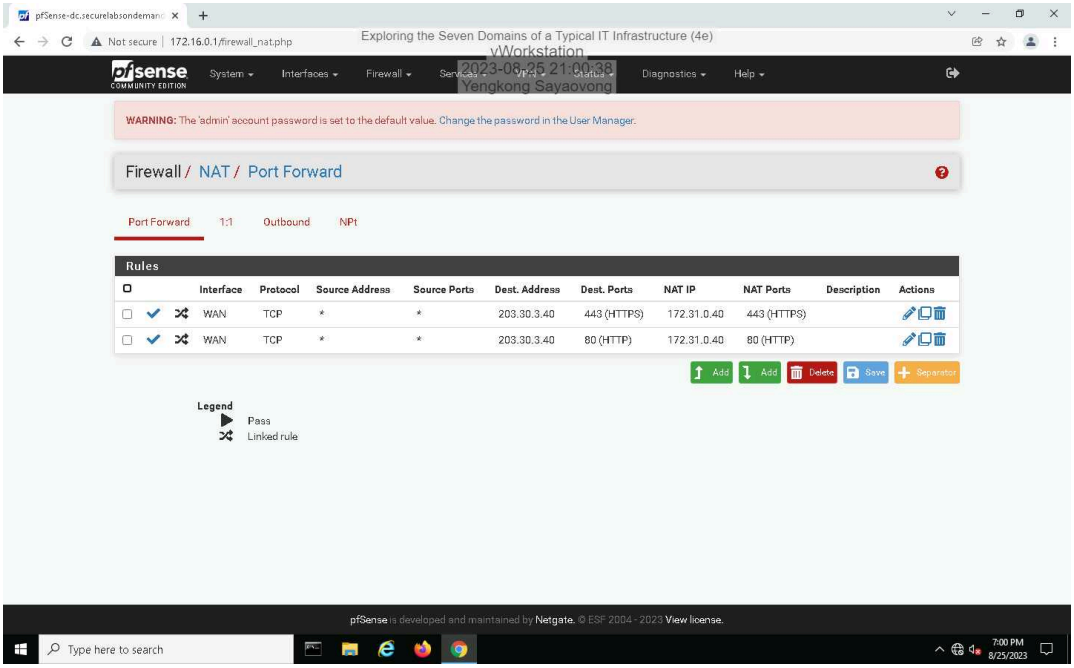
12. **Make a screen capture** showing the **Static Routes page**.



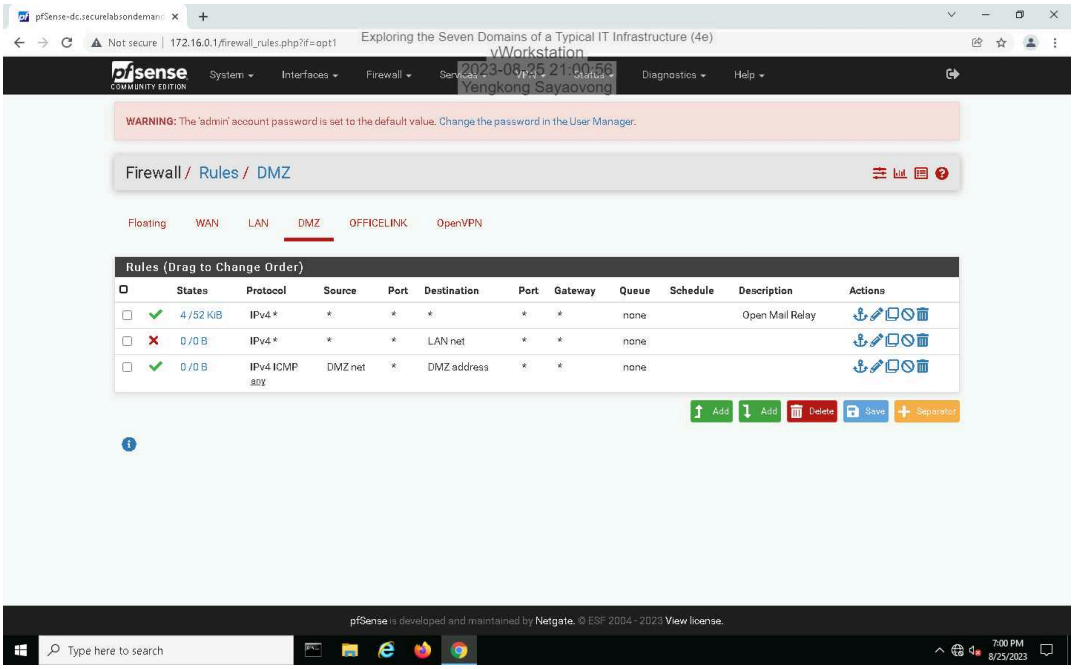
16. **Make a screen capture** showing the **result of your tracert to the pfsense-dc appliance**.



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



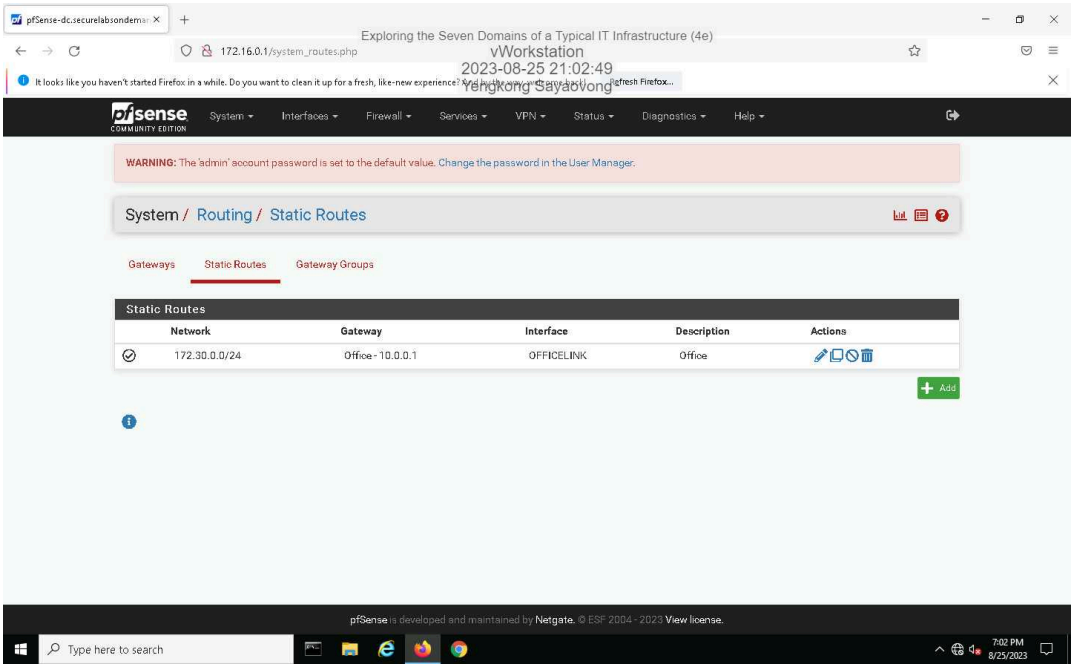
25. **Make a screen capture** showing the **DMZ firewall rules**.



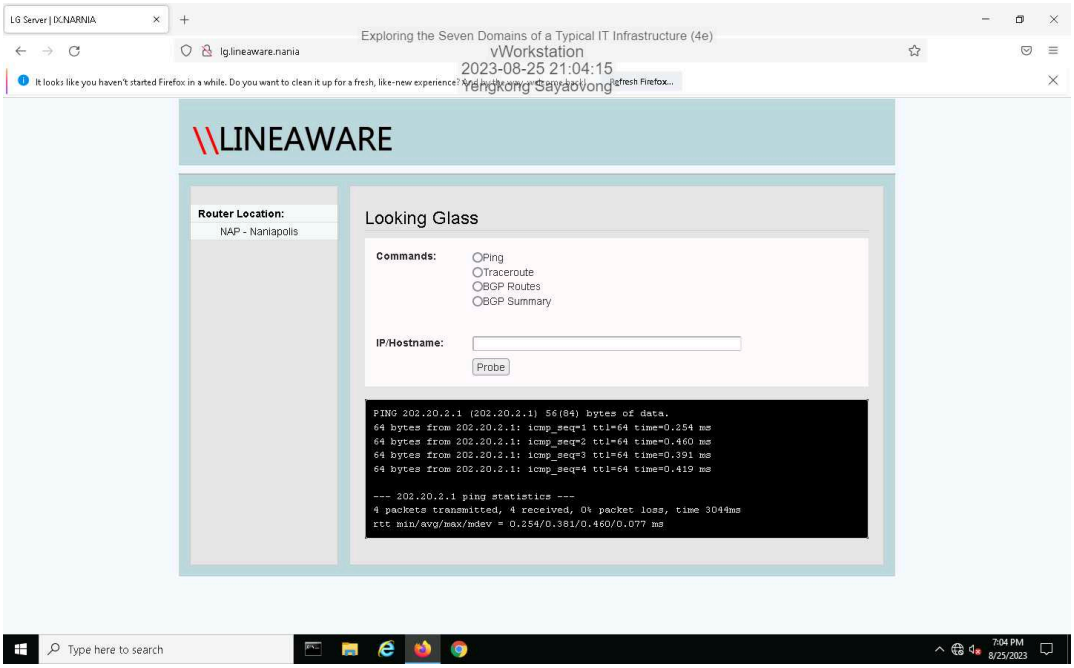
Section 2: Applied Learning

Part 1: Explore the WAN Domain

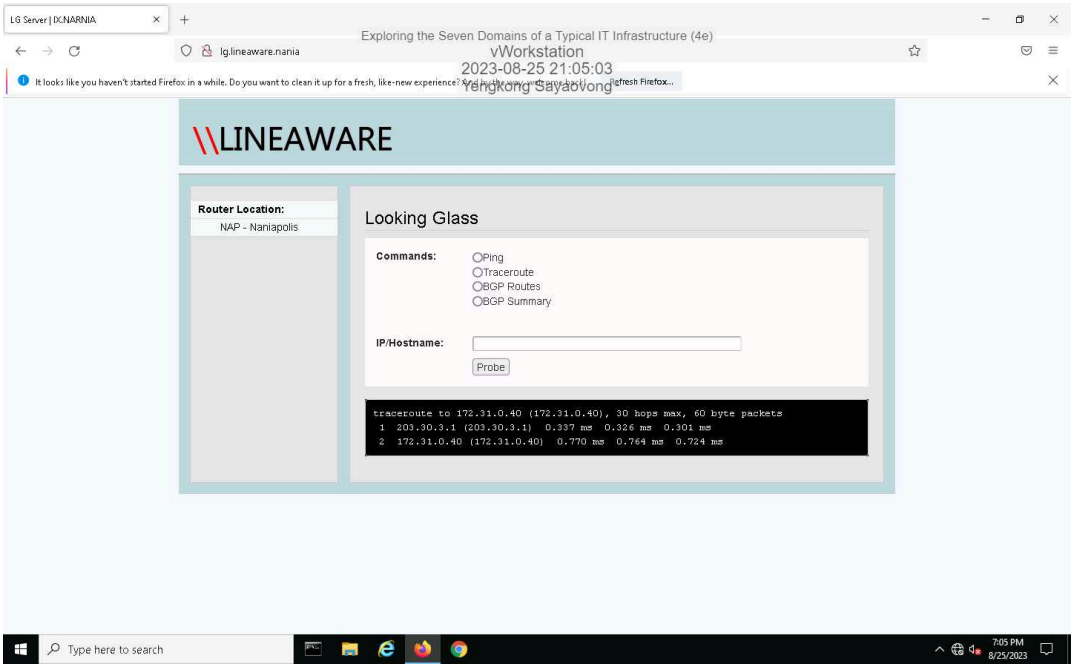
5. **Make a screen capture** showing the **static route for the point-to-point connection**.



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

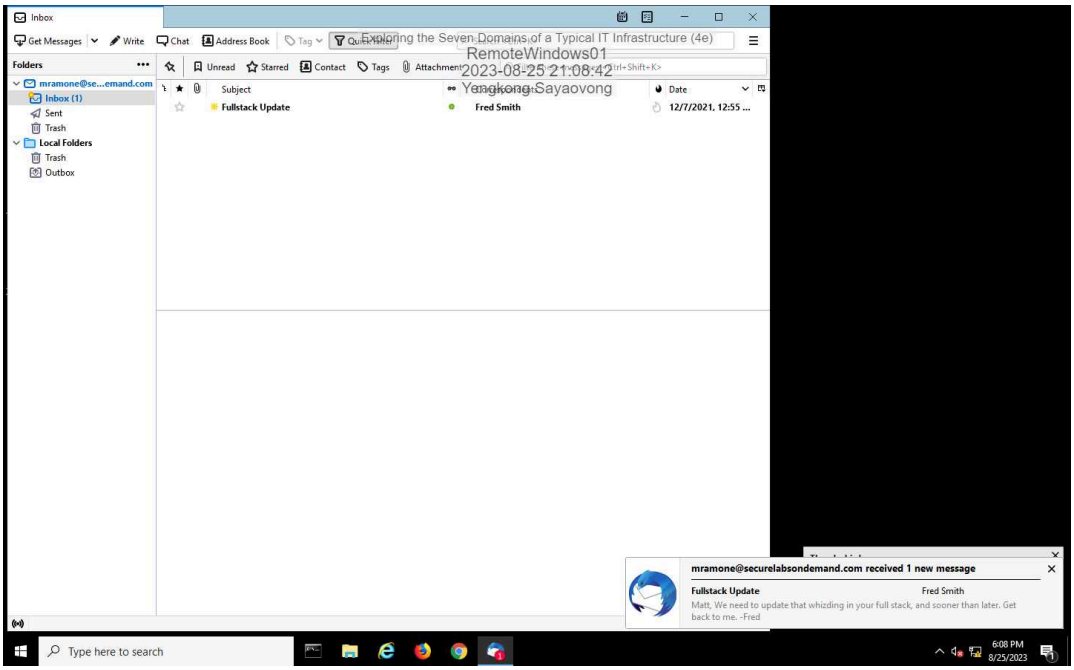


12. **Make a screen capture** showing the **traceroute to the file server**.



Part 2: Explore the Remote Access Domain

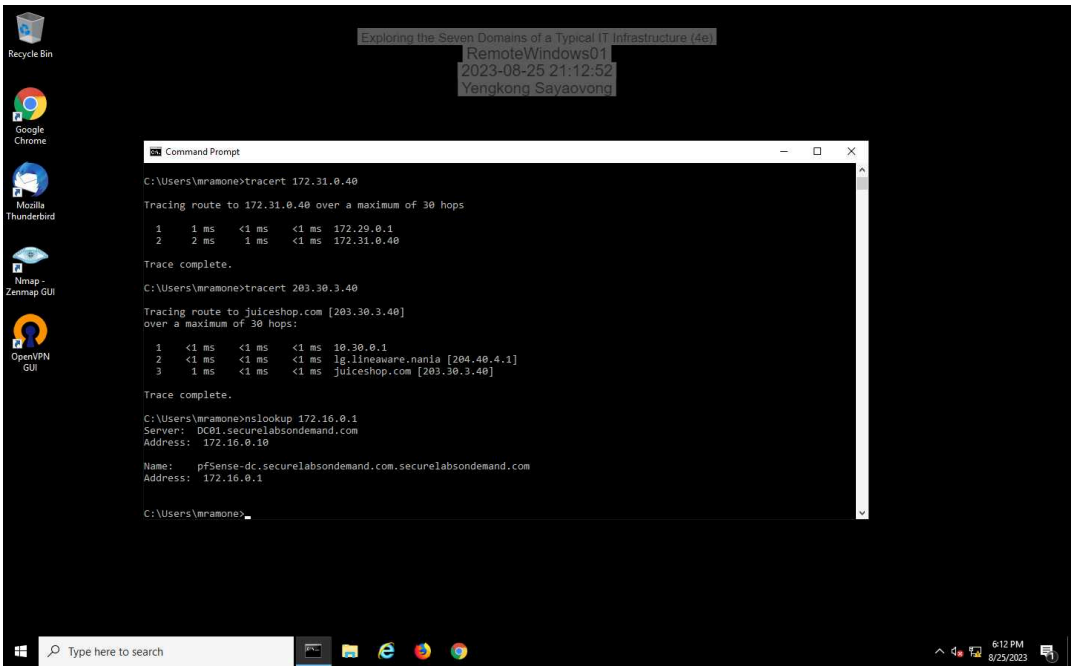
9. **Make a screen capture** showing the **successful connection to the email server**.



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

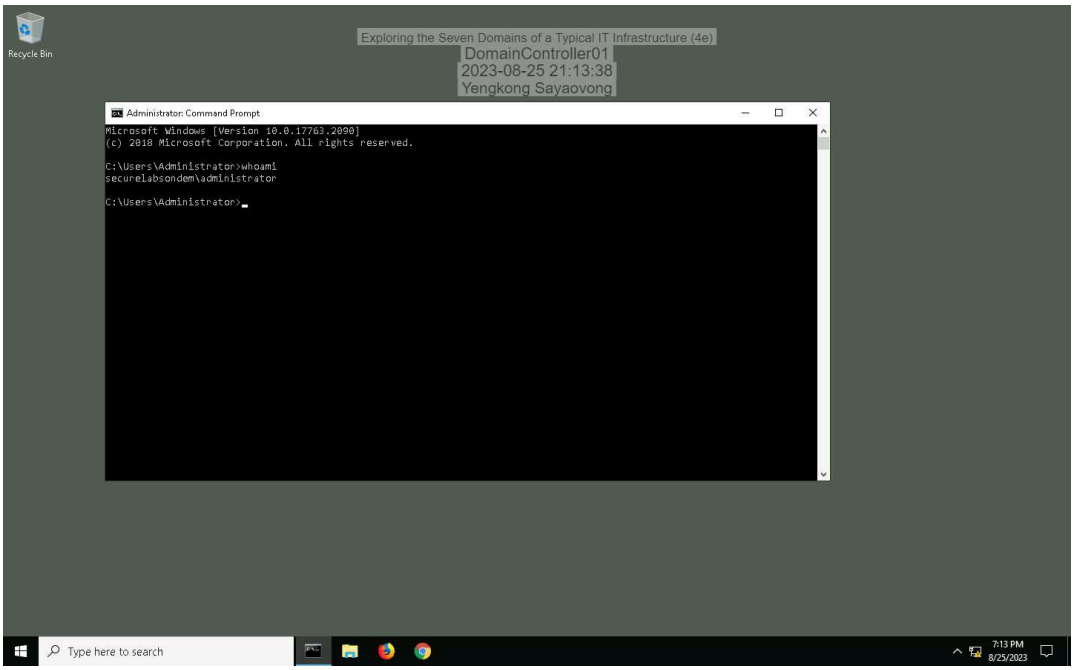
full tunnel

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

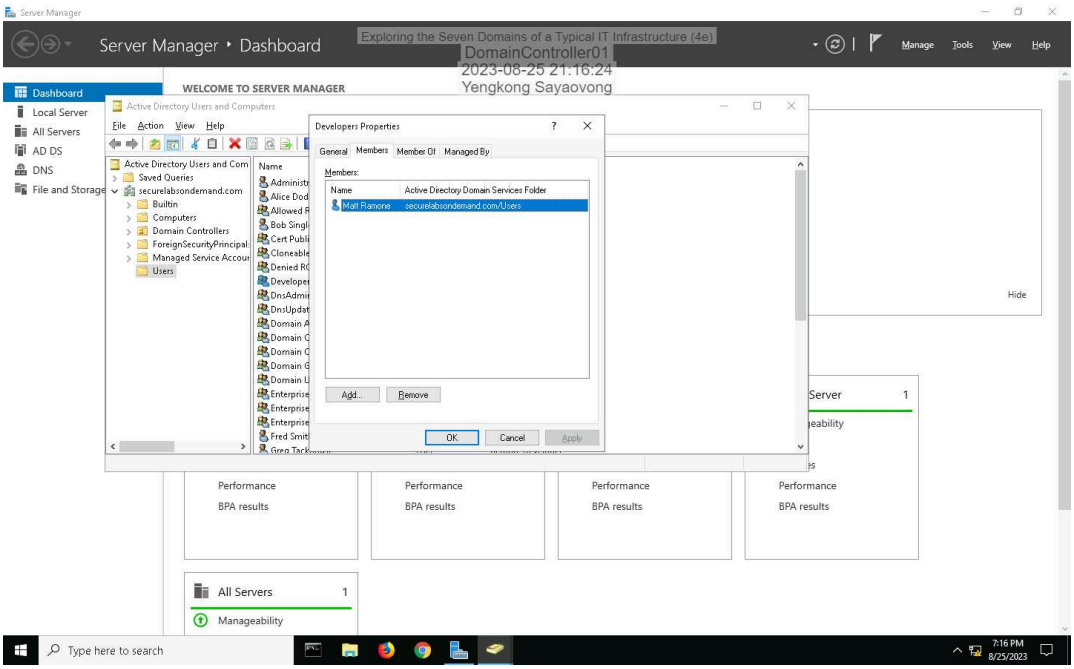


Part 3: Explore the System/Application Domain

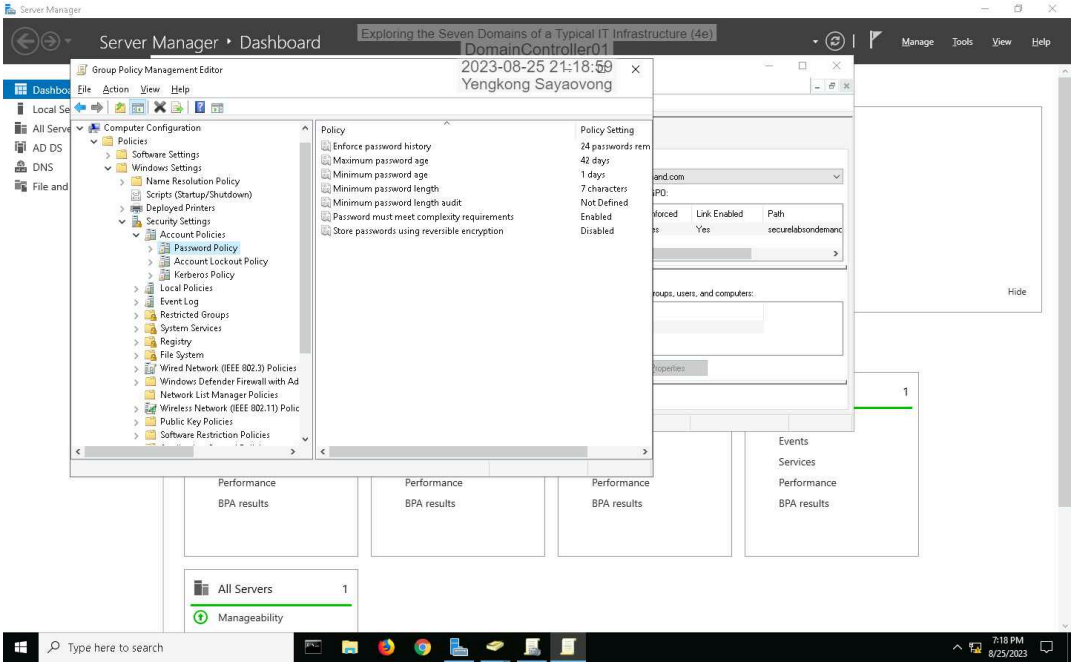
4. **Make a screen capture** showing the **whoami results**.



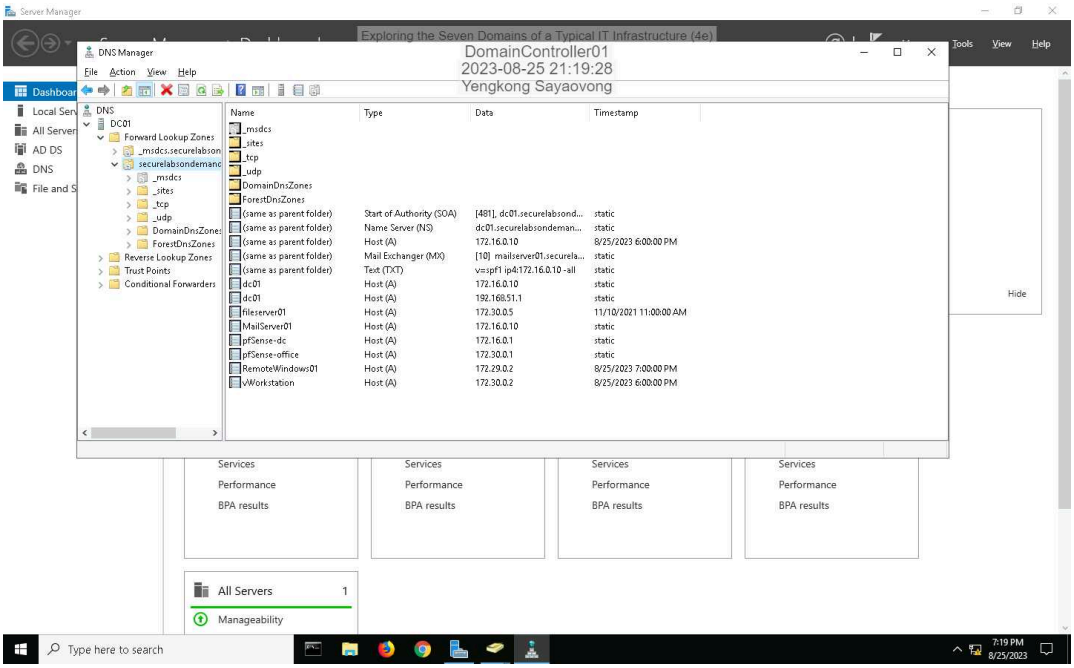
10. **Make a screen capture** showing the **members of the Developers AD group**.



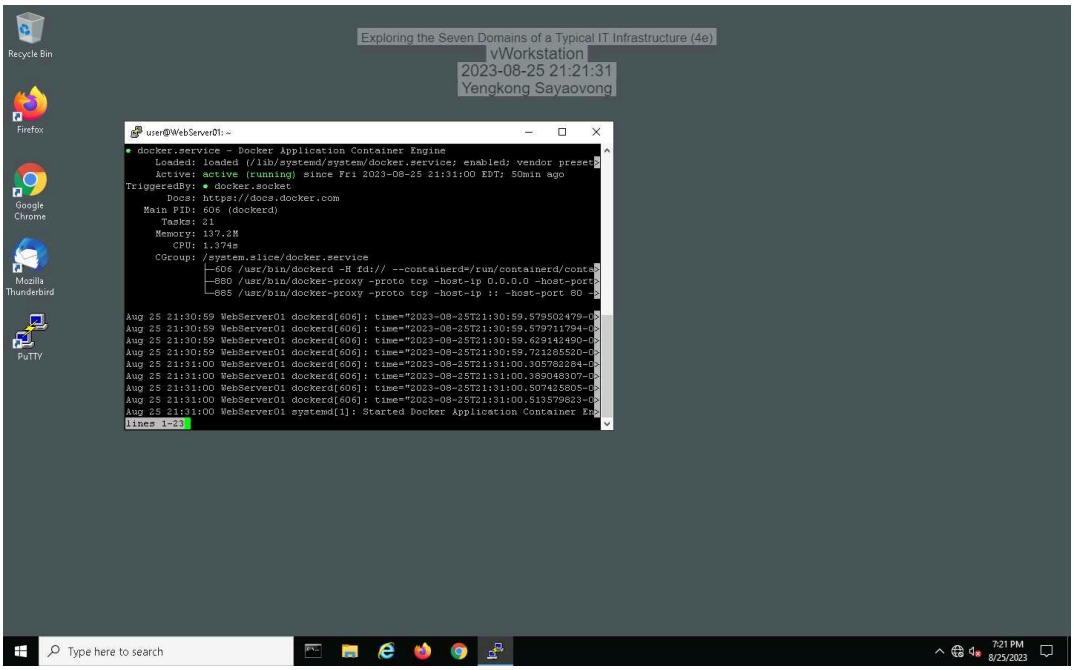
16. **Make a screen capture** showing the **password policy settings in the Group Policy Management Console**.



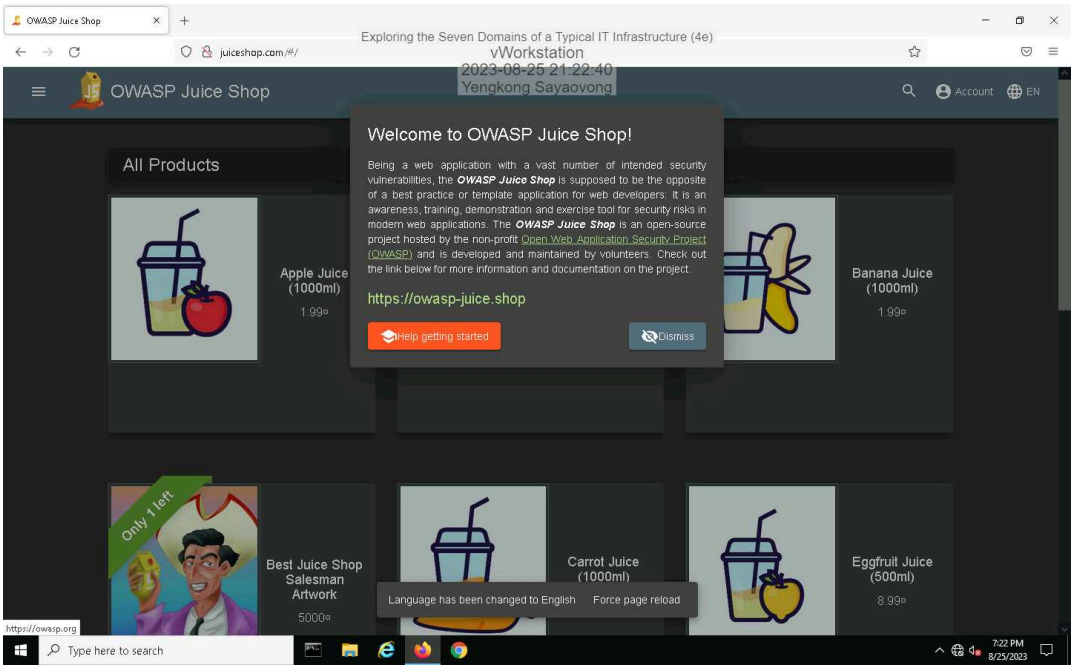
20. **Make a screen capture** showing the **DNS entries**.



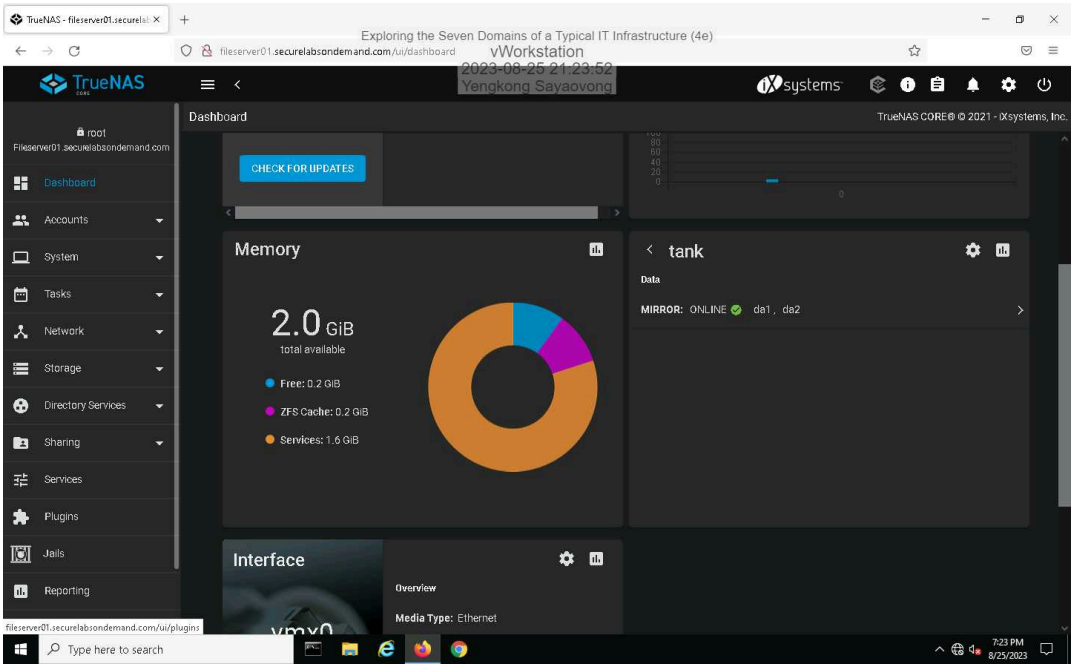
28. **Make a screen capture** showing the **Docker service status**.



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.

Theft of user data and Denial of service attacks are threats to the user domain. An effective security control to protect against this is data encryption. Malicious software and access to user data can also lead to the loss of confidential information.

https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz/ransomware

Part 2: Research Additional Security Controls

Based on your research, **identify** security controls that could be implemented in the Workstation, LAN, LAN-to-WAN, WAN, Remote Access, and System/Application Domains. **Recommend** and **explain** one security control for each domain. Be sure to cite your sources.

1) Workstation: Foe the workstations the best thing to do os to use One security control that could be implemented in the Workstation as to use anti-virus software with regular updates to protect against malware and other malicious software. This will provide good security. Other thing is to put workstation under good firewall.

2) LAN: One security control that could be implemented in the LAN Domain is to use firewalls to block unauthorized access and traffic to the LAN.

3) LAN-to-WAN : Use of VLANs.One security control that could be implemented in the LAN-to-WAN

https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks