Student:	Email:
Patrick Kierzkowski	pxk405@francis.edu

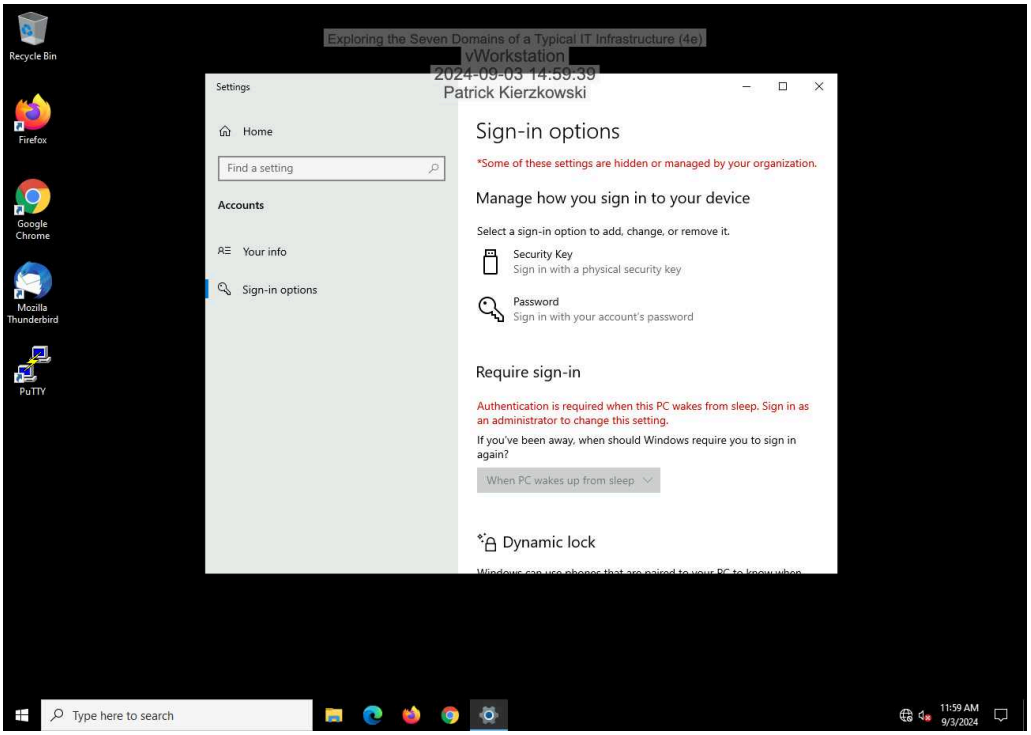
Time on Task:	Progress:
24 hours, 57 minutes	100%

Report Generated: Monday, July 7, 2025 at 9:49 PM

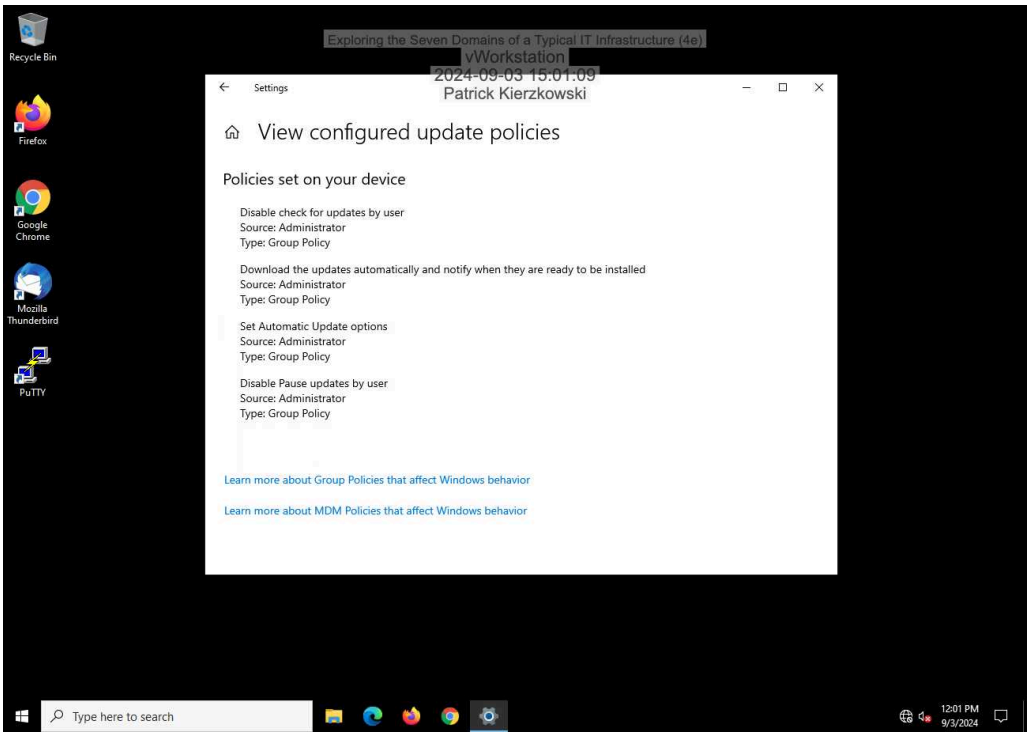
Section 1: Hands-On Demonstration

Part 1: Explore the Workstation Domain

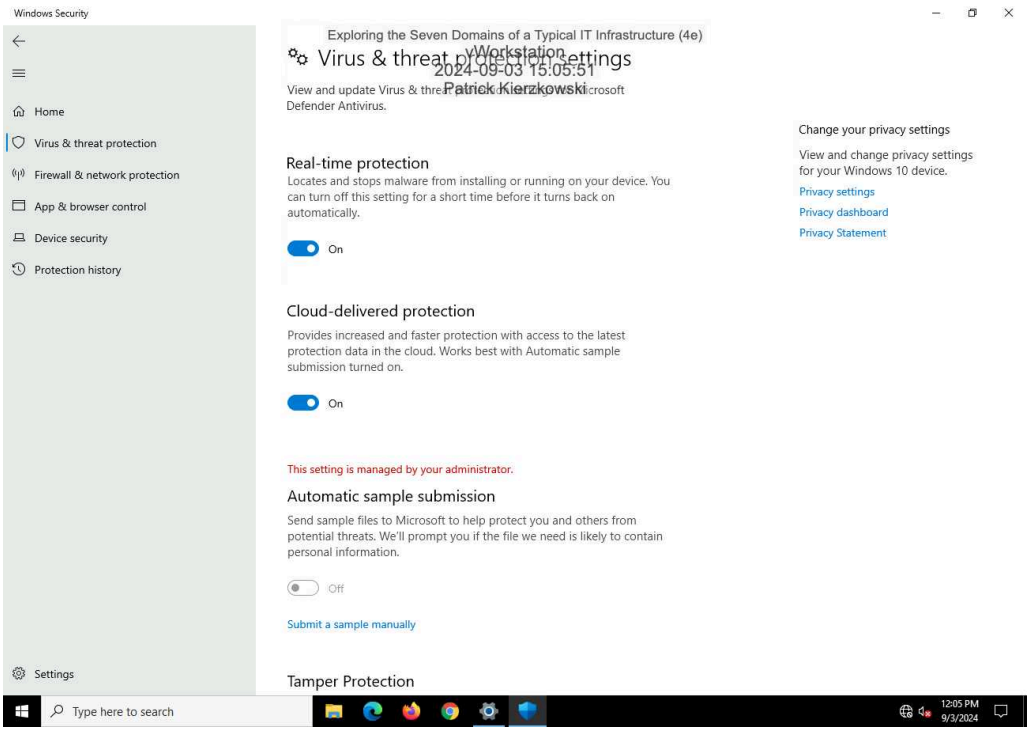
4. **Make screen capture** showing the **Sign-in options for Alice's account**.



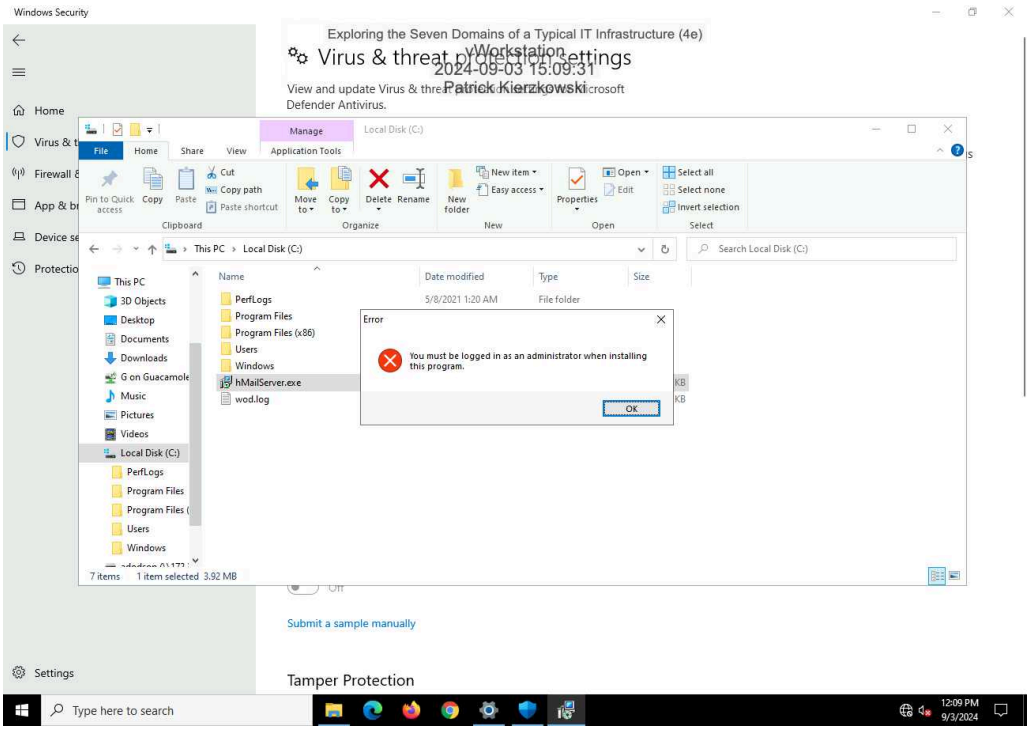
7. **Make a screen capture** showing the **View configured update policies page**.



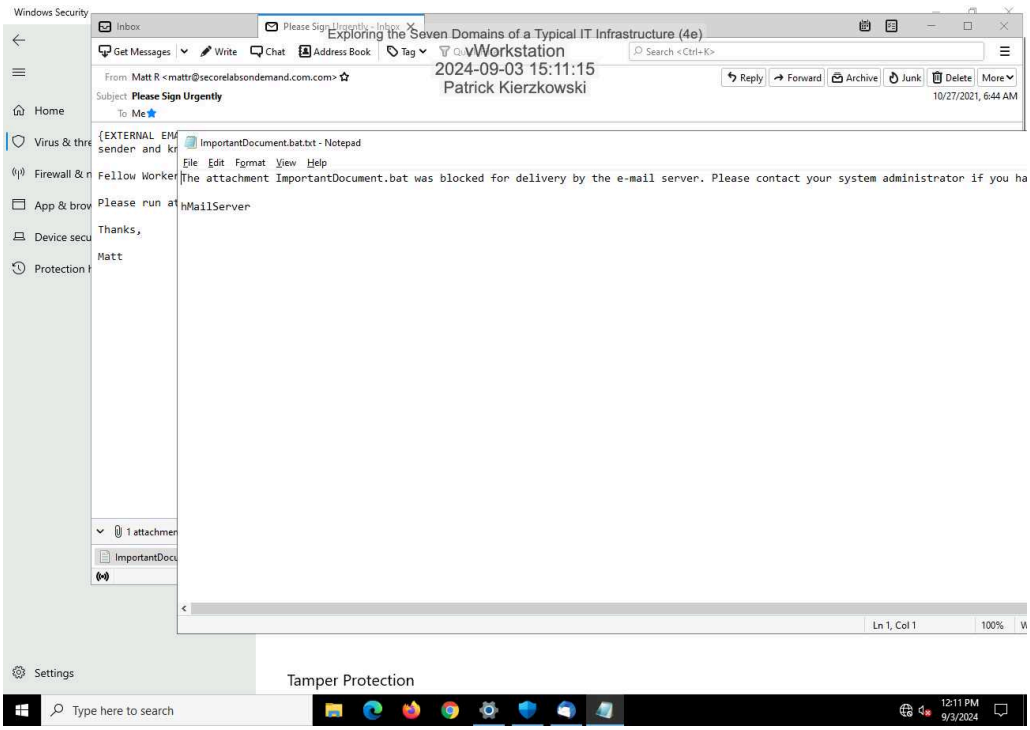
14. **Make a screen capture** showing the **Virus & Threat Protection Settings**.



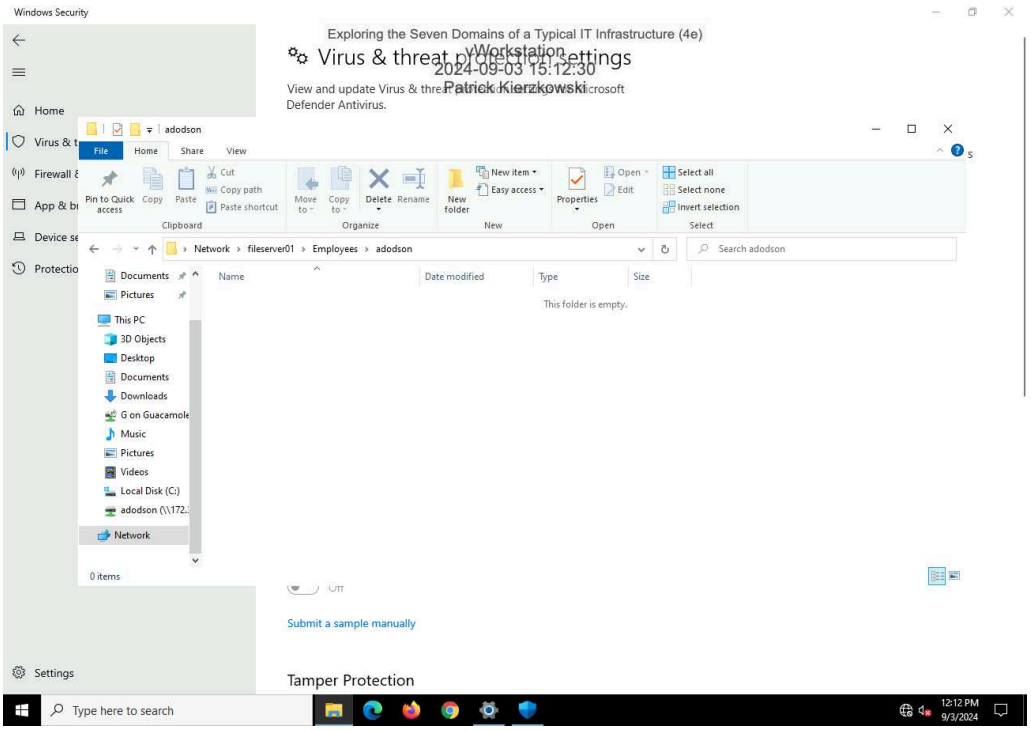
18. **Make a screen capture** showing the **security warning from attempting to run an executable file**.



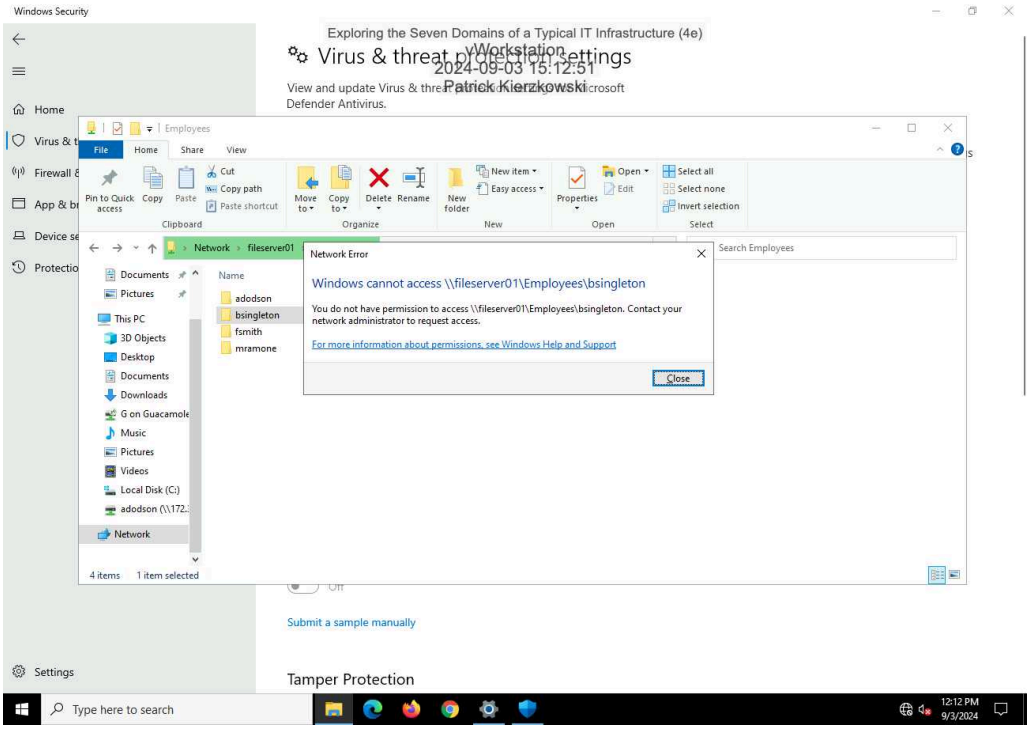
24. **Make a screen capture** showing the **blocked attachment message**.



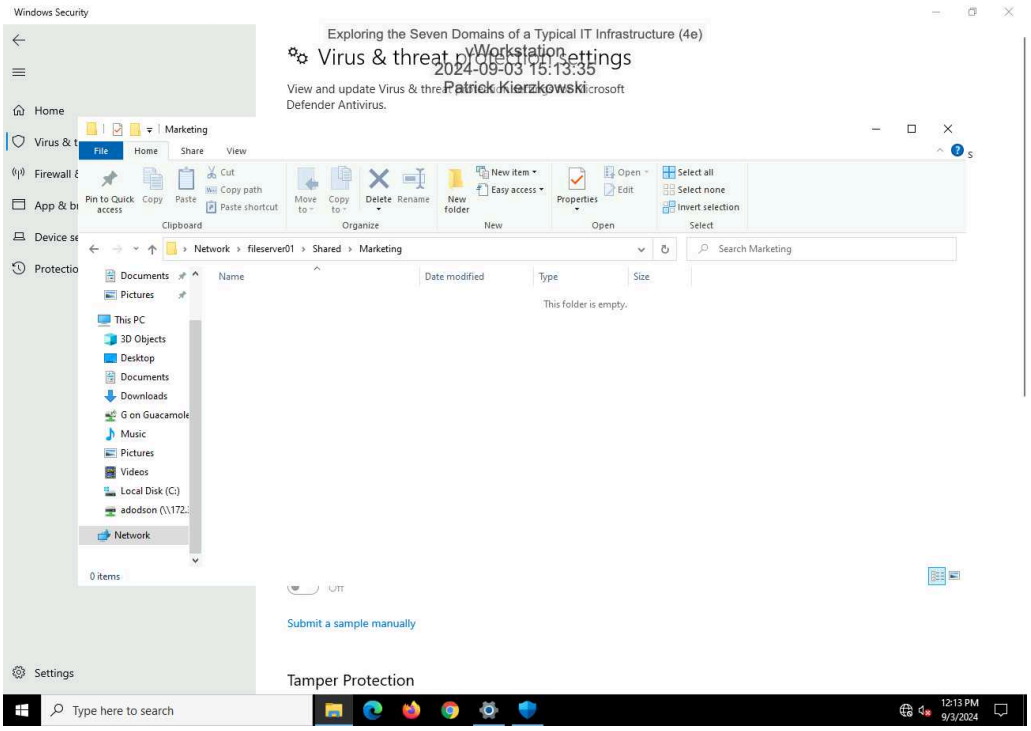
28. **Make a screen capture** showing a **successful connection to the adodson user folder**.



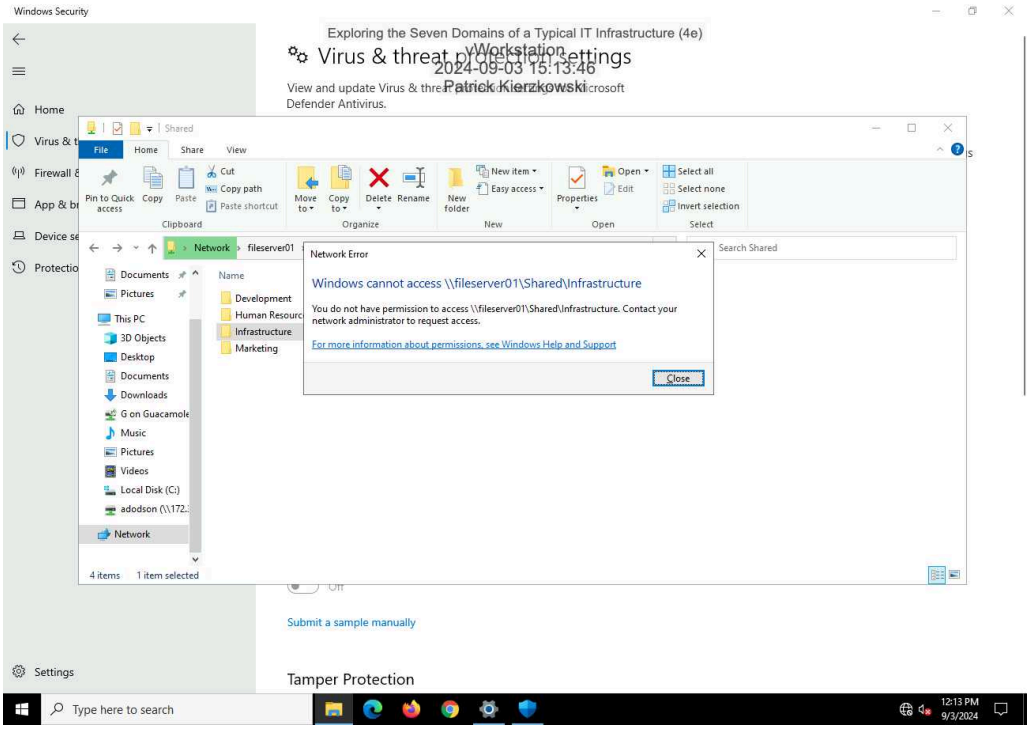
29. **Make a screen capture** showing a **failed connection to another user folder**.



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

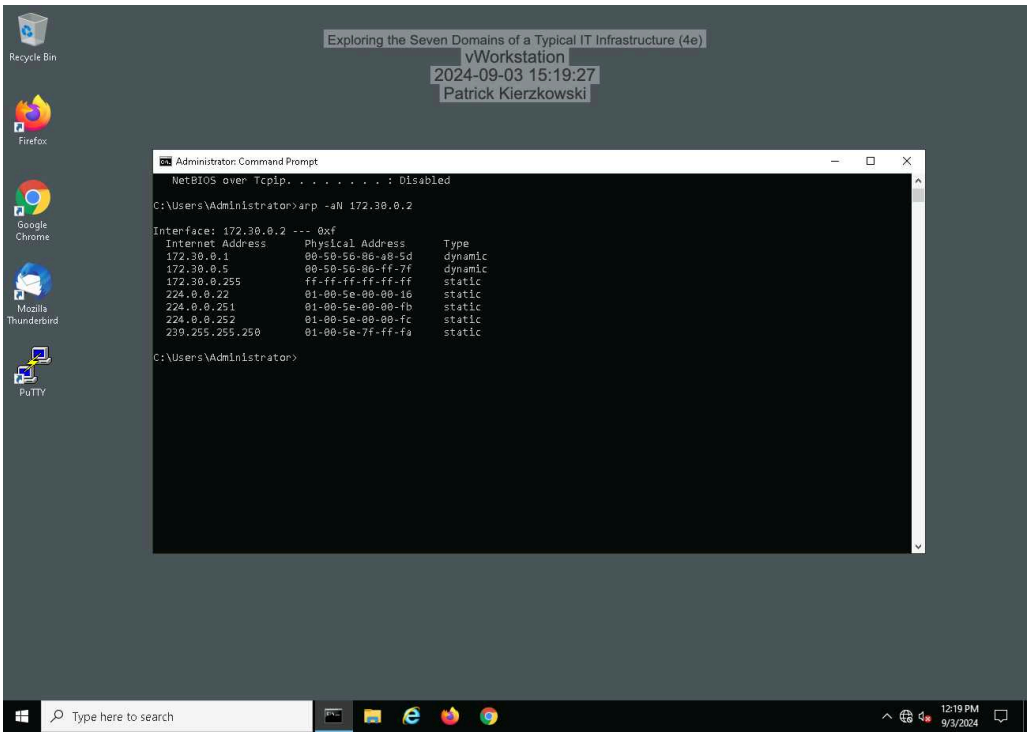


32. **Make a screen capture** showing a **failed connection to another shared folder**.

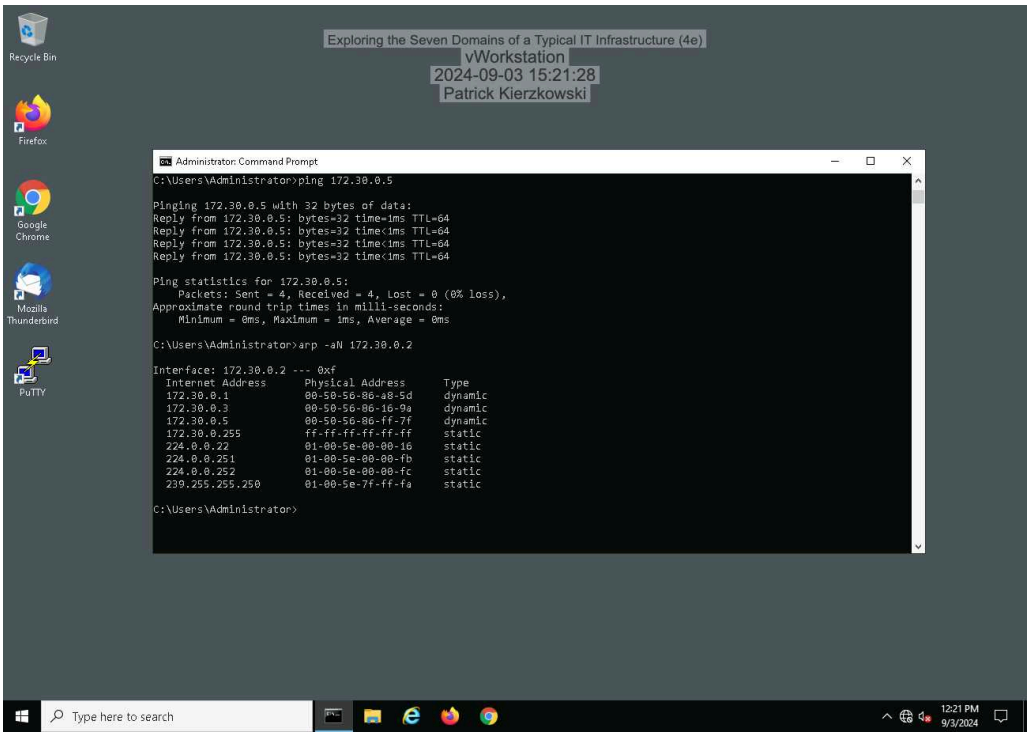


Part 2: Explore the LAN Domain

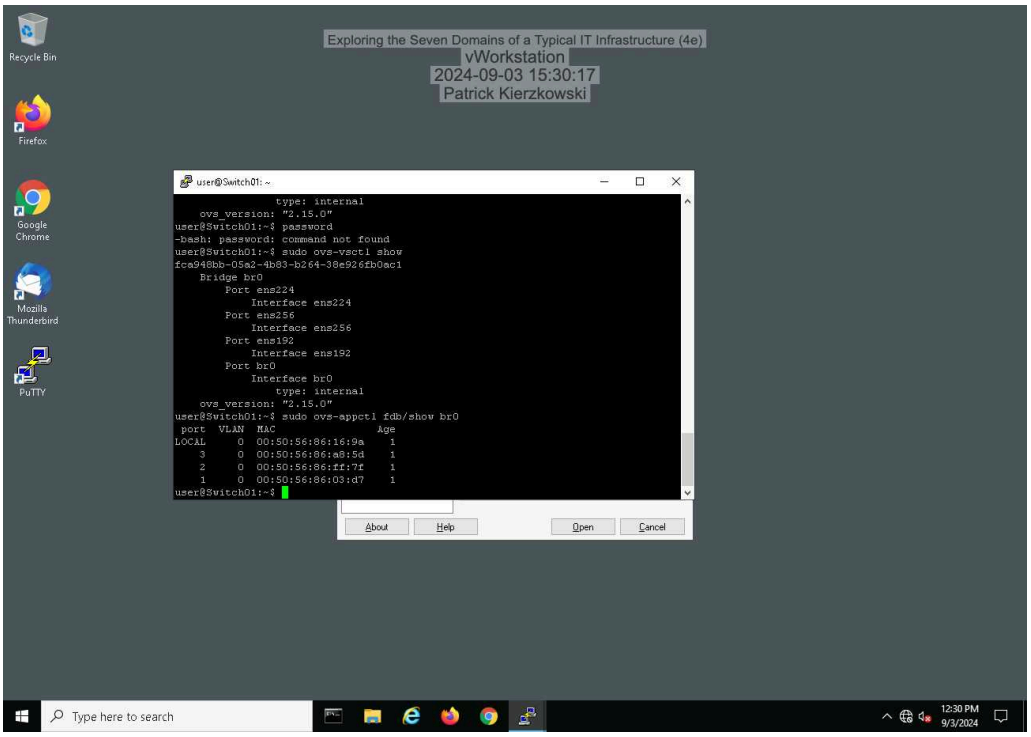
5. **Make a screen capture** showing the **vWorkstation's original ARP table**.



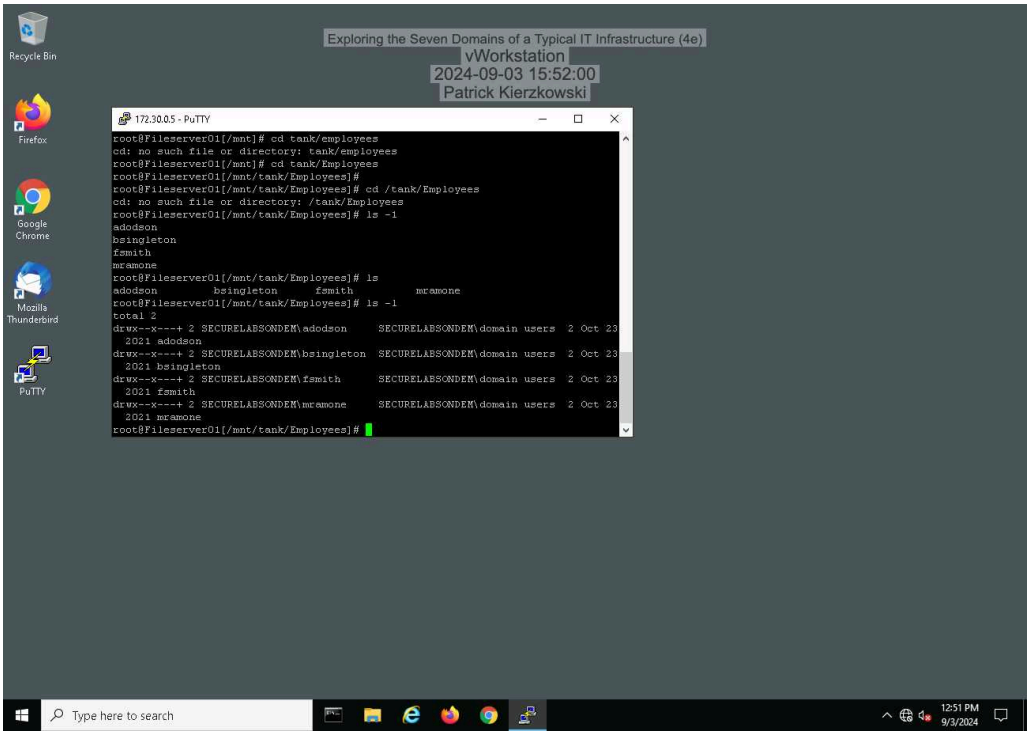
10. **Make a screen capture** showing the **vWorkstation's updated ARP table.**



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

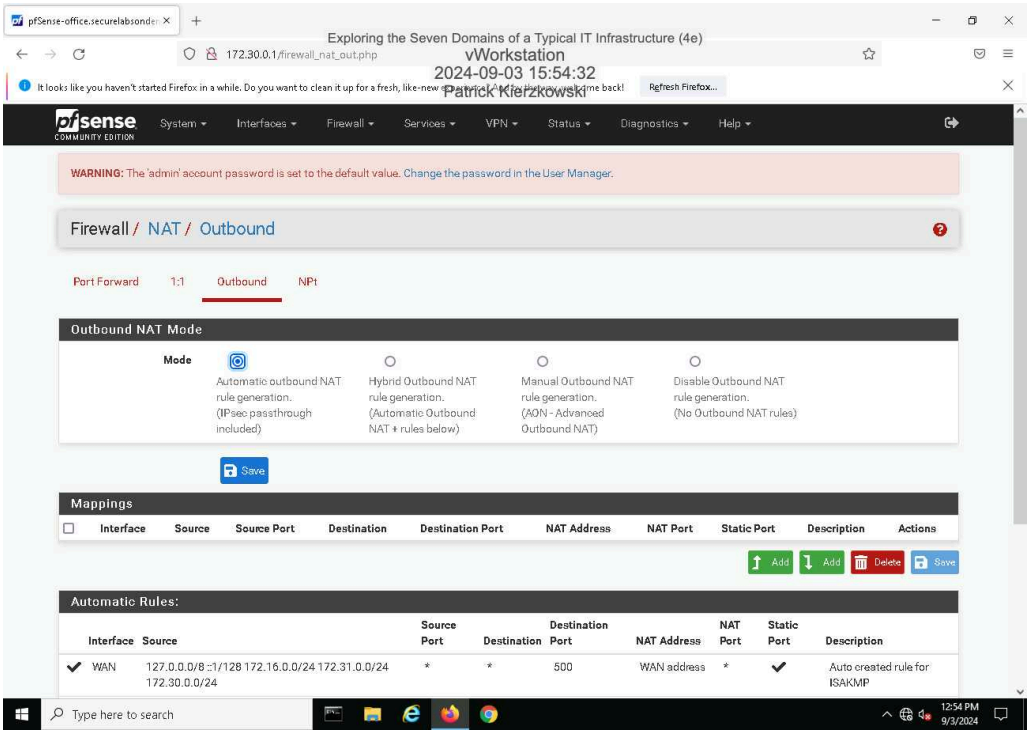


30. **Make a screen capture** showing the **contents of the Employees directory**.

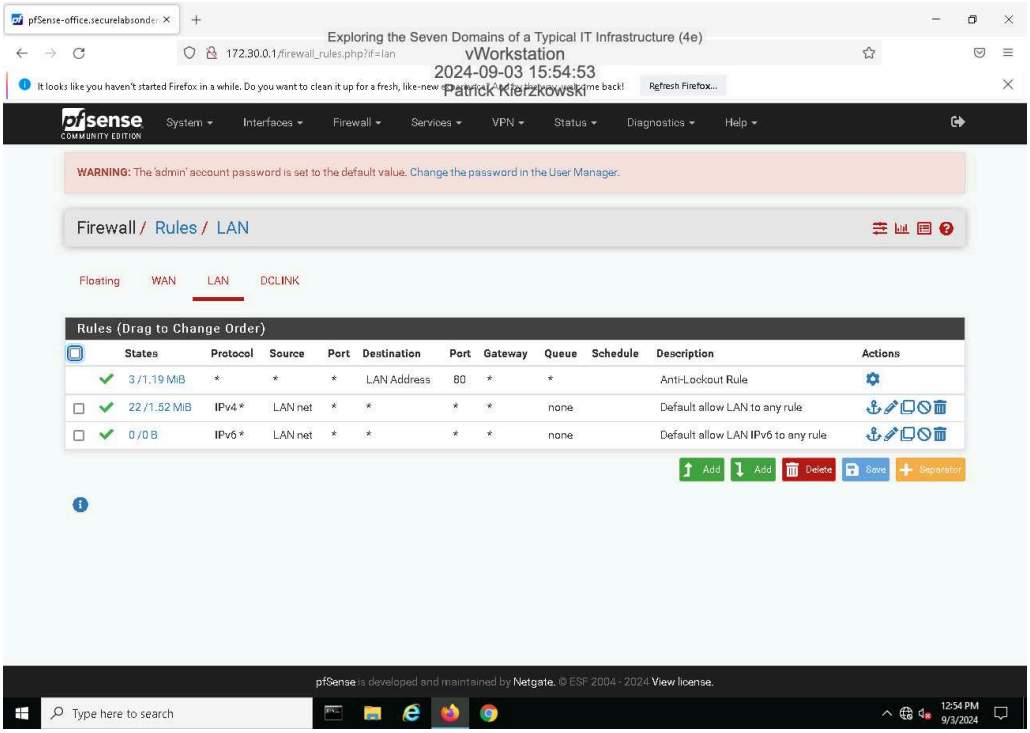


Part 3: Explore the LAN-to-WAN Domain

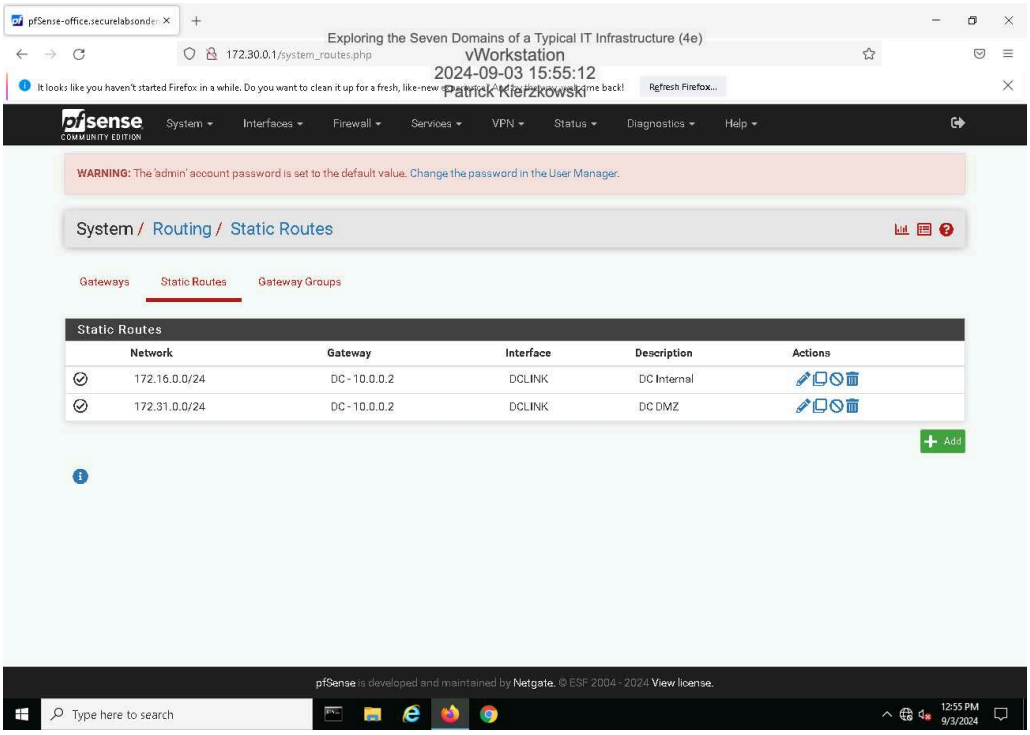
6. **Make a screen capture** showing the **Outbound NAT settings**.



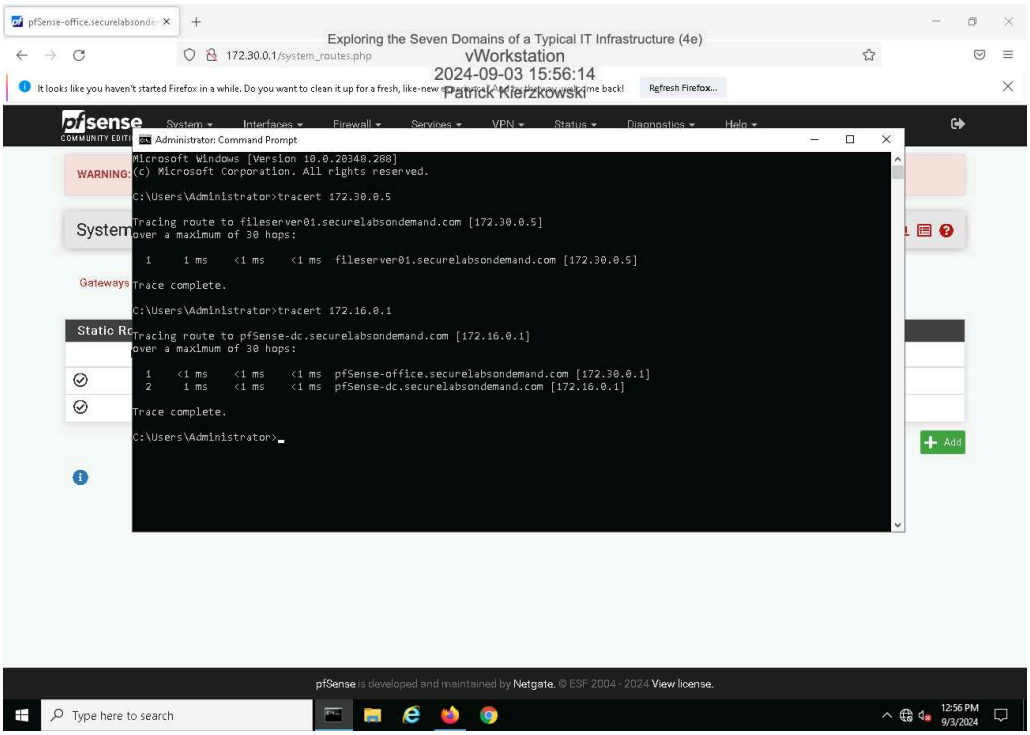
9. **Make a screen capture** showing the **permissive LAN rules**.



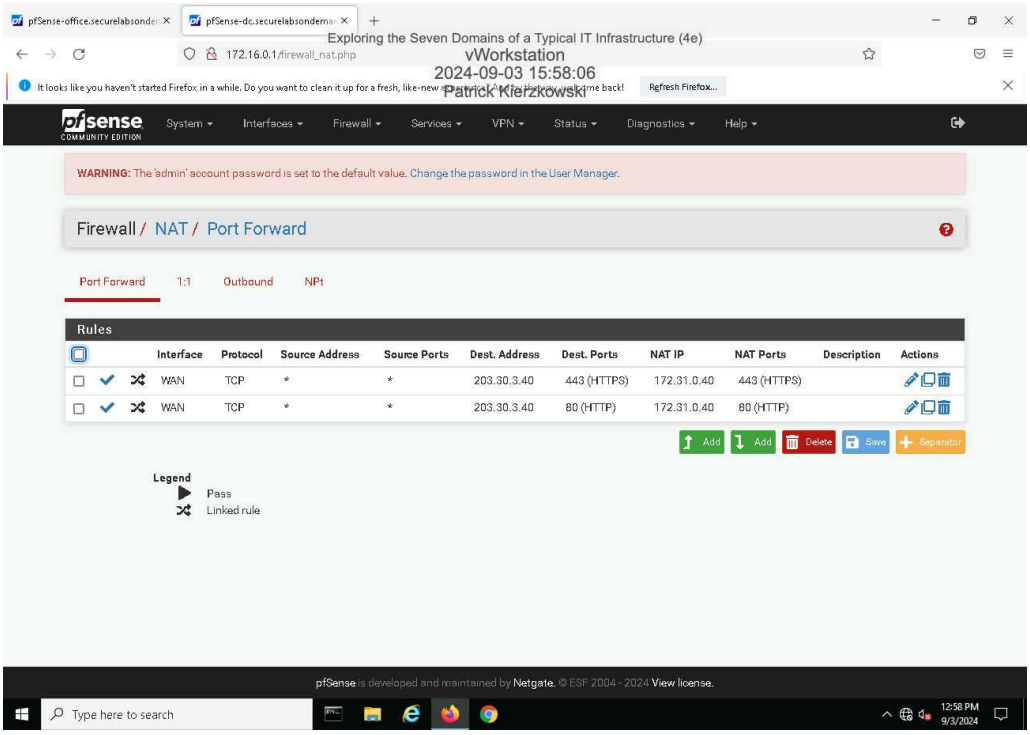
12. **Make a screen capture** showing the **Static Routes page**.



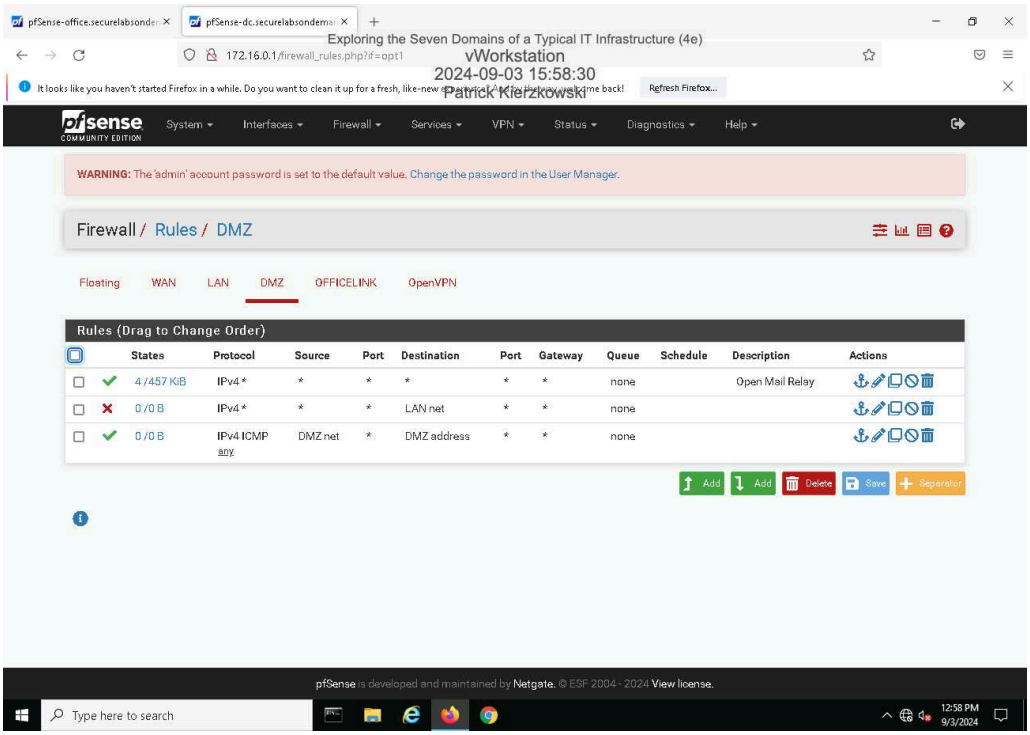
16. **Make a screen capture** showing the **result of your tracert to the pfsense-dc appliance**.



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



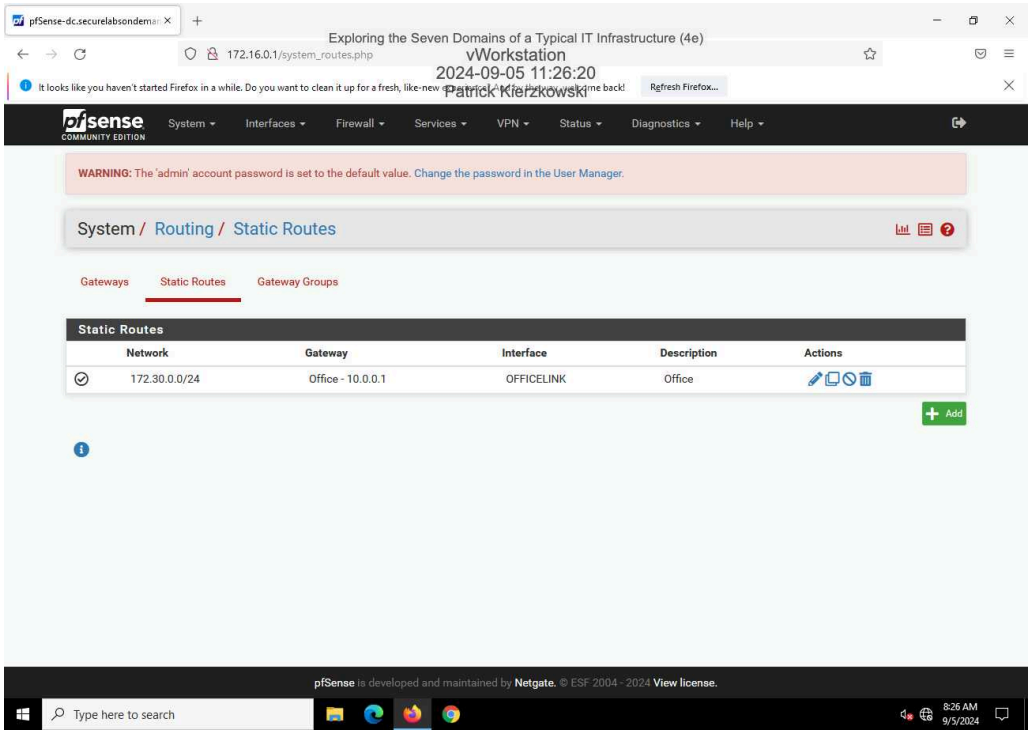
25. **Make a screen capture** showing the **DMZ firewall rules**.



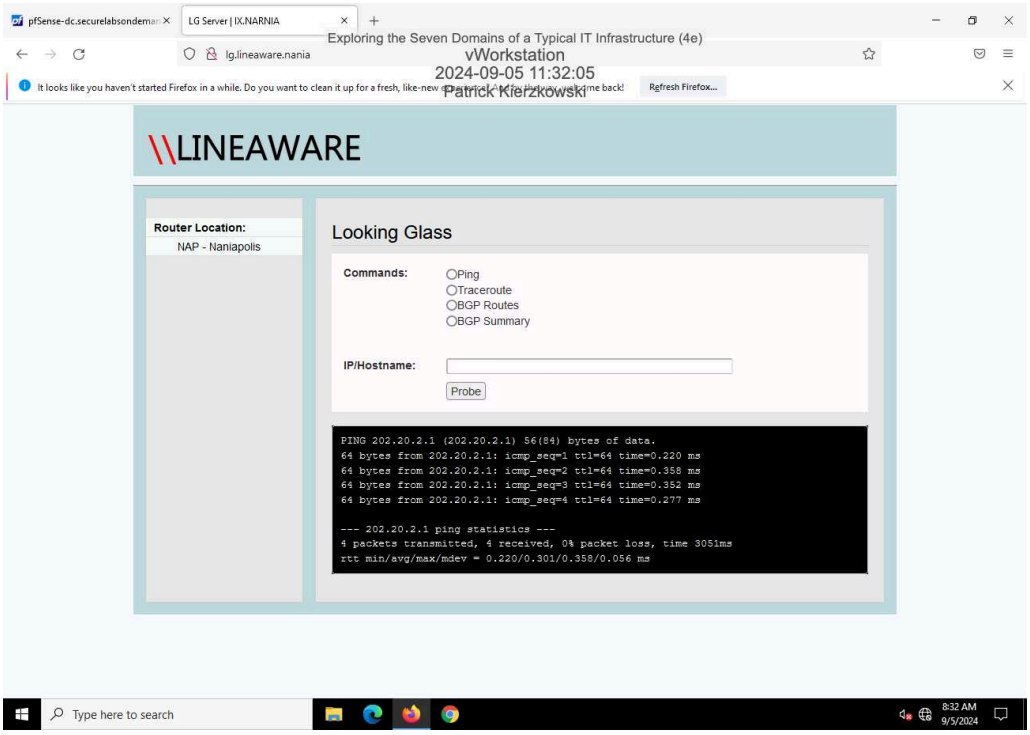
Section 2: Applied Learning

Part 1: Explore the WAN Domain

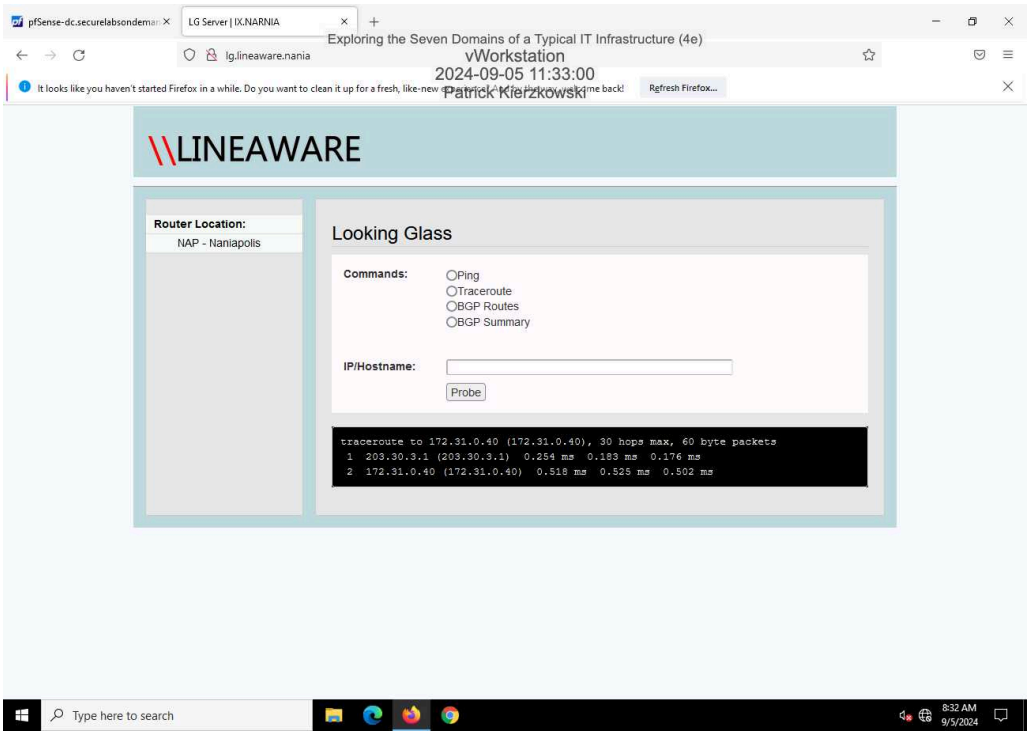
5. **Make a screen capture** showing the **static route for the point-to-point connection**.



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

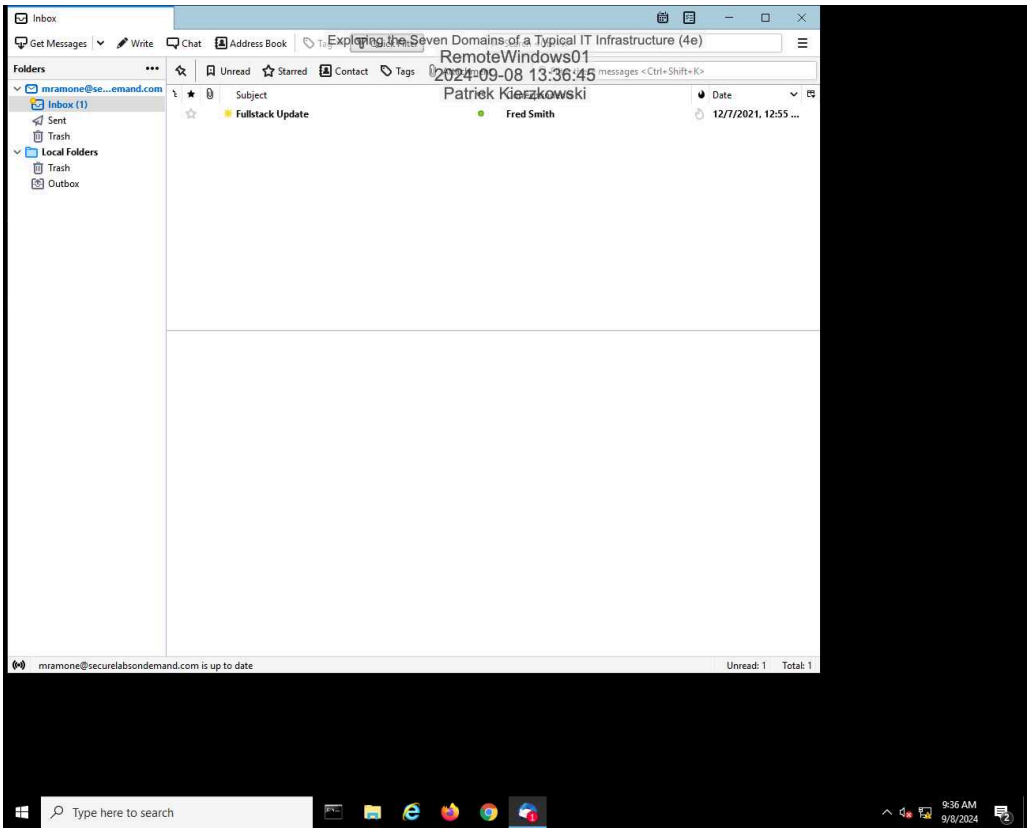


12. **Make a screen capture** showing the **traceroute to the file server**.



Part 2: Explore the Remote Access Domain

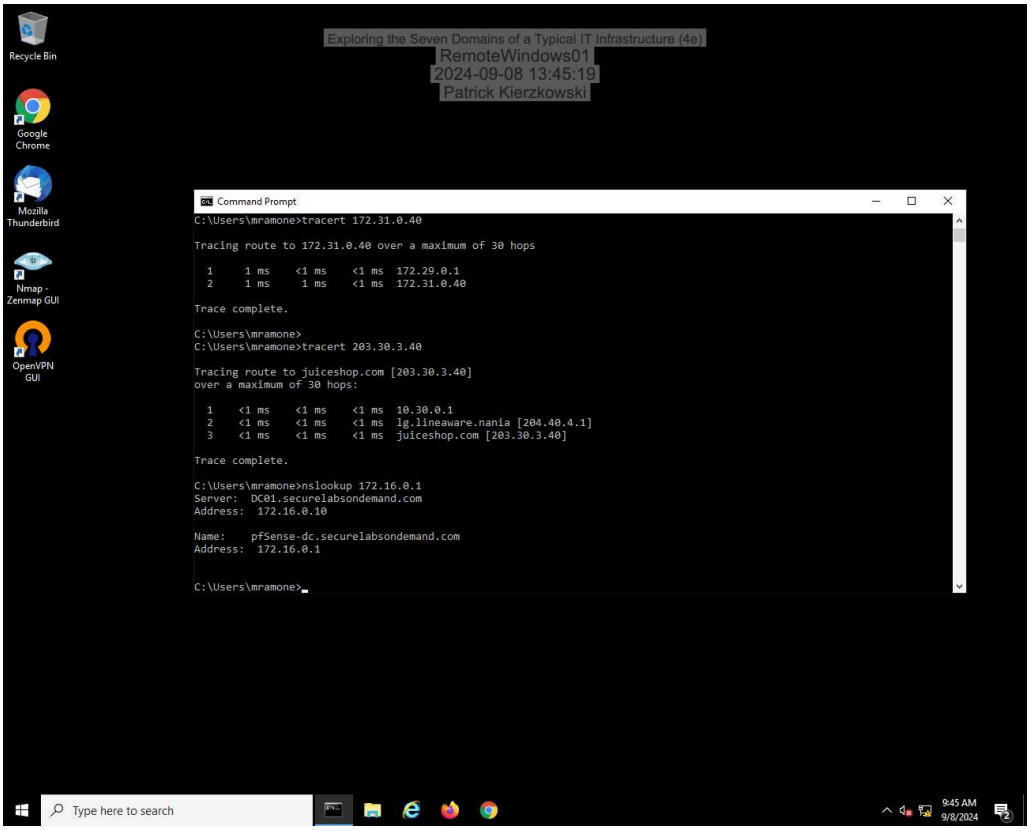
9. **Make a screen capture** showing the **successful connection to the email server**.



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

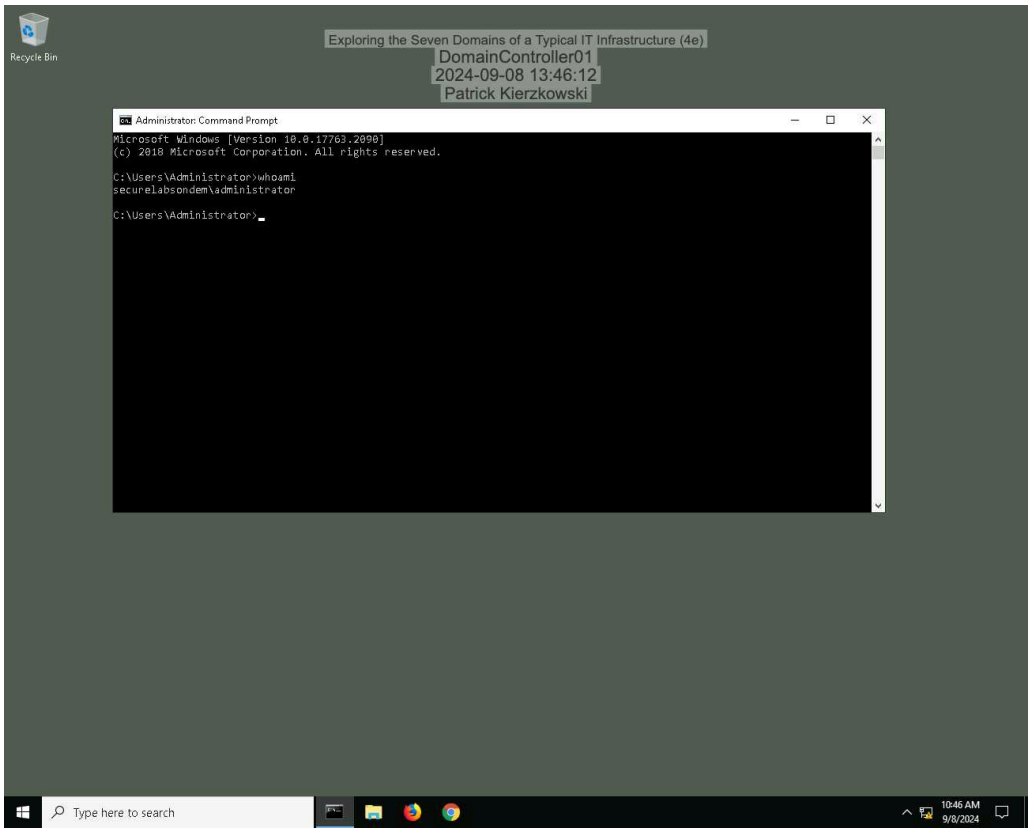
The first one was a full tunnel, meanwhile the second one was a split tunnel

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

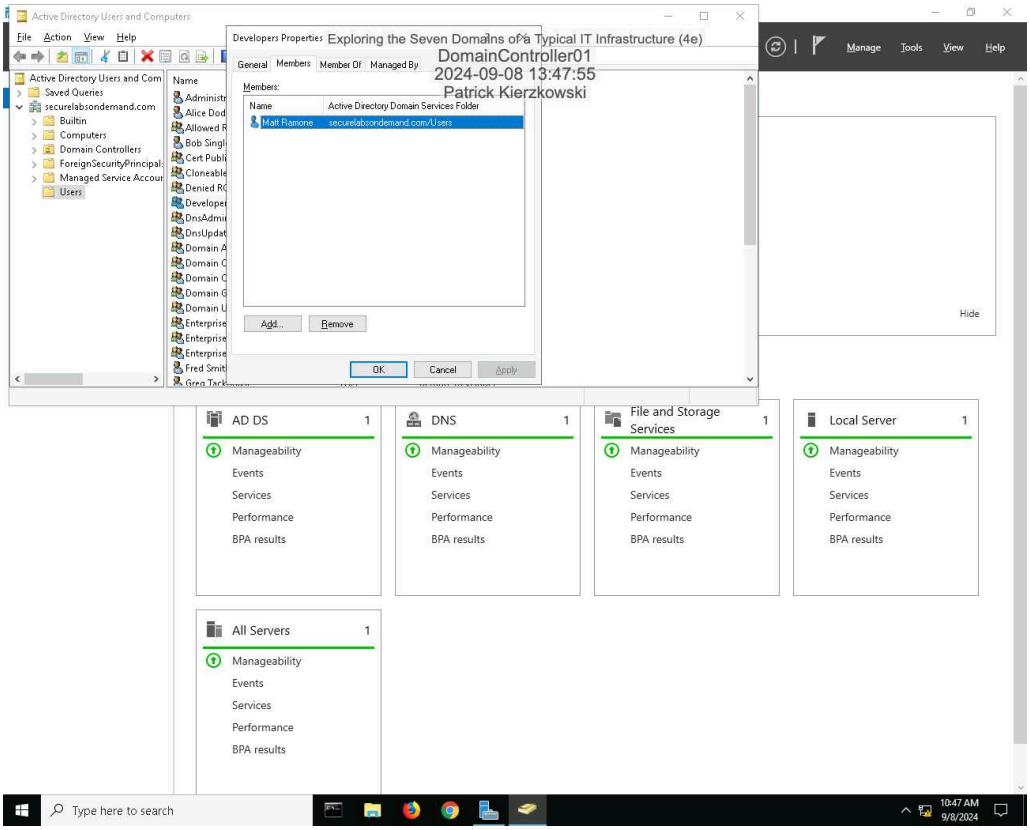


Part 3: Explore the System/Application Domain

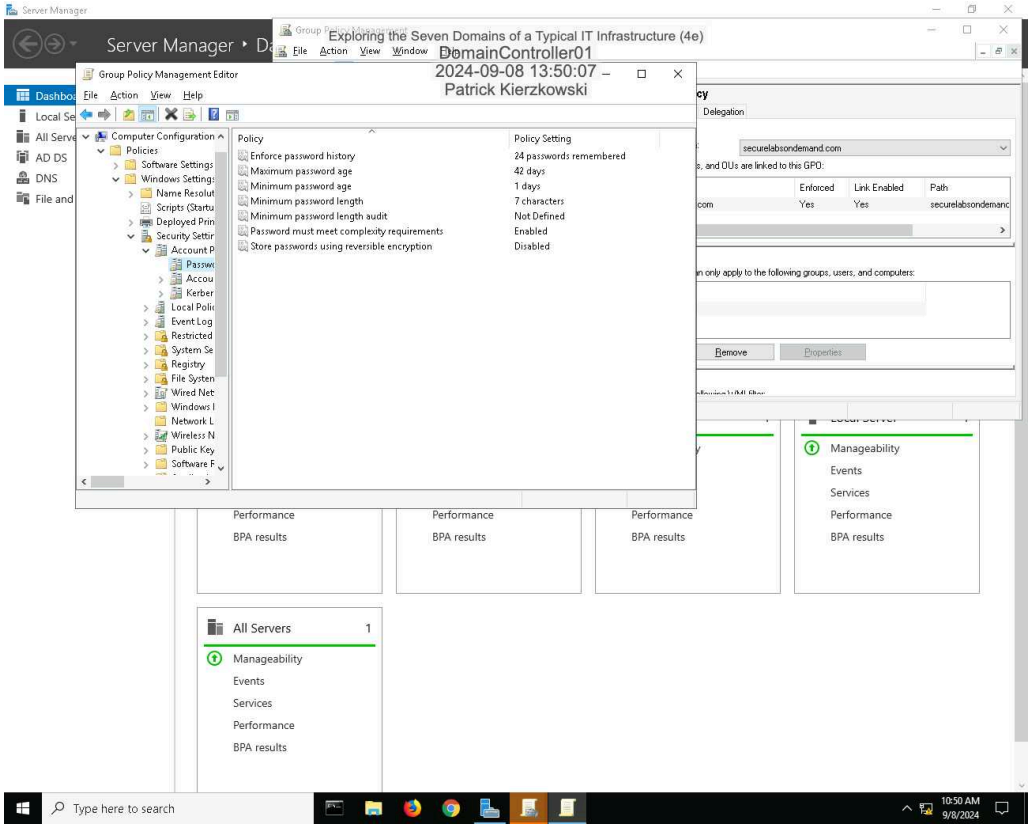
4. **Make a screen capture** showing the **whoami results**.



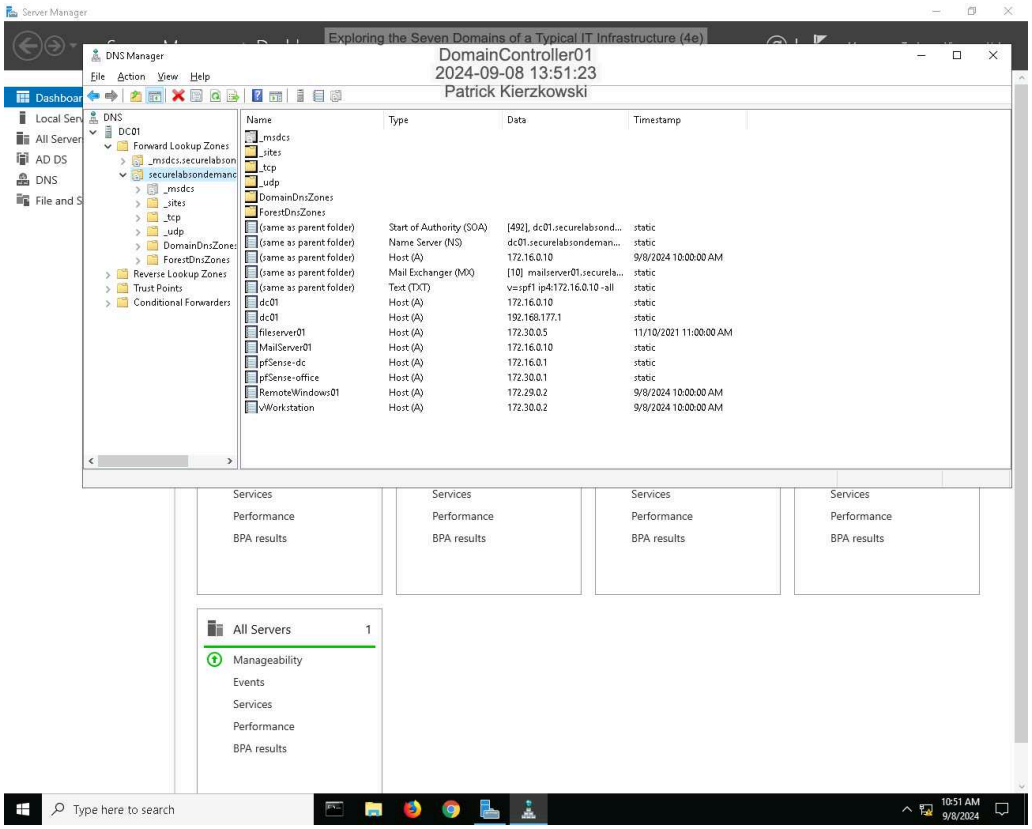
10. **Make a screen capture** showing the **members of the Developers AD group**.



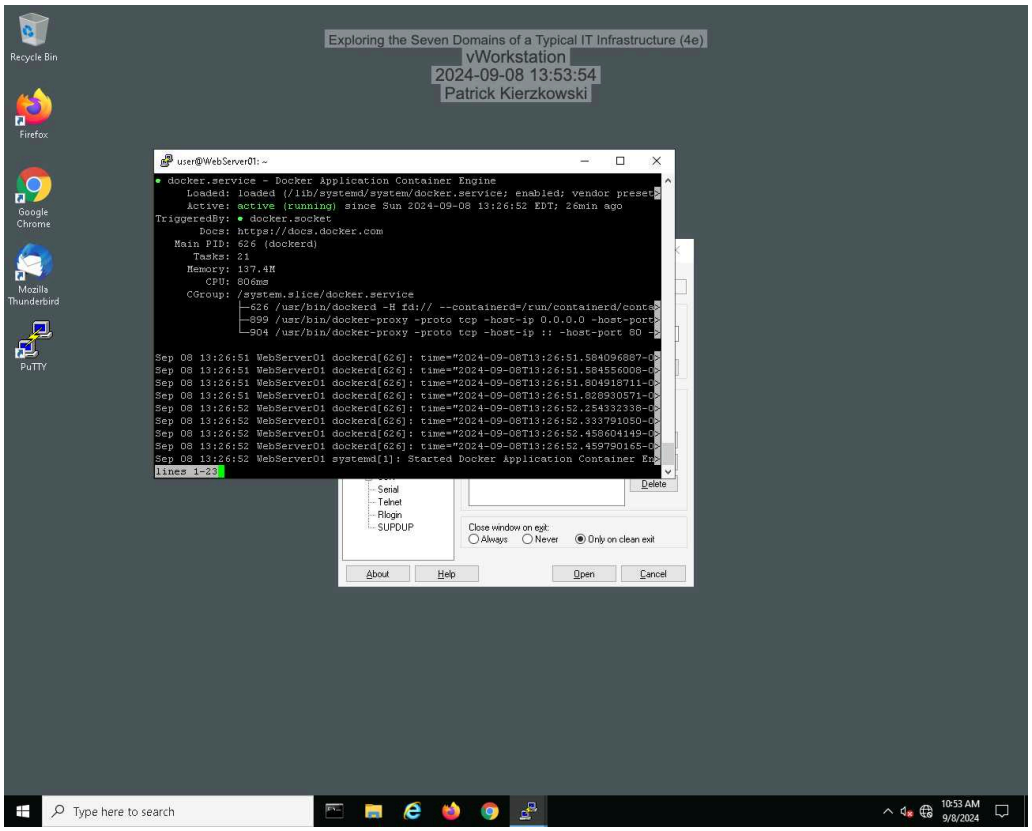
16. **Make a screen capture** showing the **password policy settings in the Group Policy Management Console**.



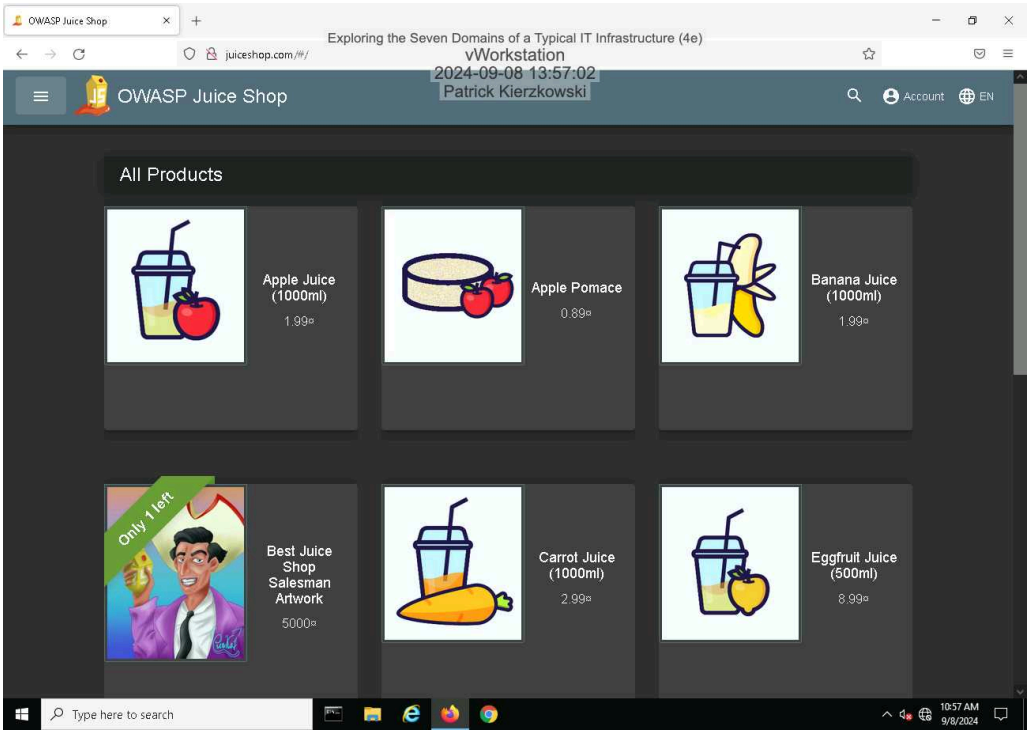
20. **Make a screen capture** showing the **DNS entries**.



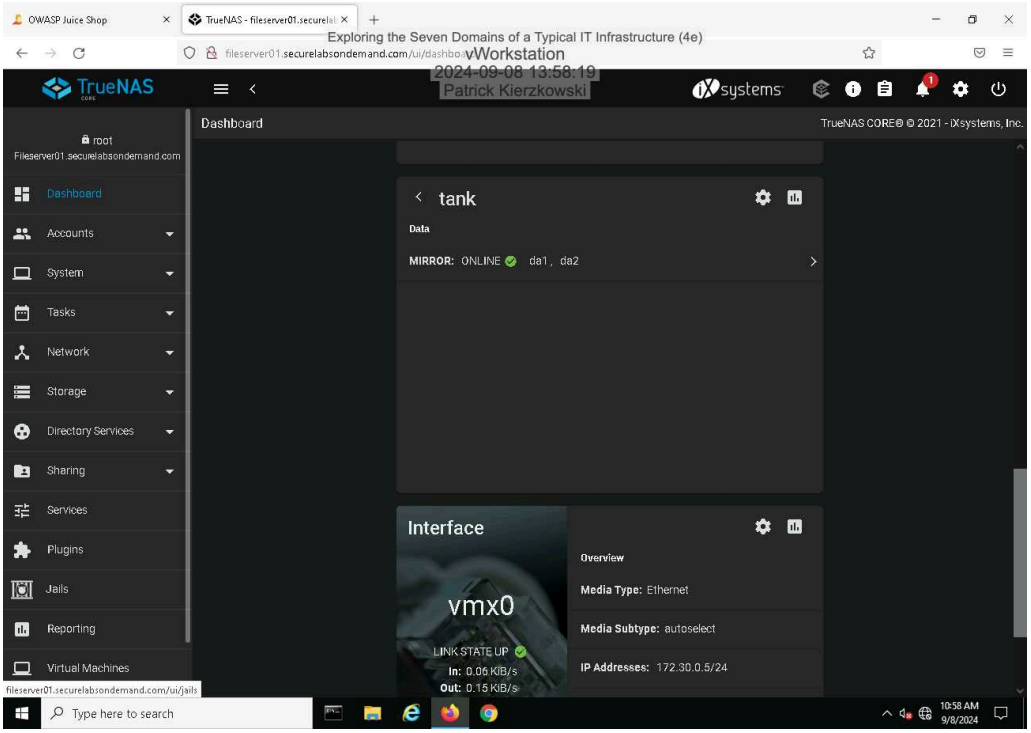
28. **Make a screen capture** showing the **Docker service status**.



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.

Two compelling threats to the User Domain would be phishing attacks and insider threats. Phishing attacks are when people outside of the company try to trick employees into giving away information by pretending to be a trusted source in an email or website. Insider threats on the other hand is when the companies own employees misuse sensitive data, either by accident or for their own gain. These are both serious threats to the User Domain, but they also have security controls that are effective at protecting against it. For example to protect yourself against phishing attacks, you shouldn't respond to spam and make your email uncommon so its hard to guess your email. You should also implement spam filters and anti-phishing software incase spammers do get your email. Then they will get blocked out before they reach your inbox and reduce the chance that they can fall victim to phishing (Kaspersky, n.d.). To protect yourself from insider threats, you should assess access levels, and review how much access everyone has. Then you give everyone the minimum to where they can still complete their tasks, and minimize the amount of data everyone can obtain , so insider threats are less likely to happen (Netwrix, n.d.). You should also pinpoint the areas where the most harm can be done, and use data classification to prioritize and focus your security efforts efficiently (Netwrix, n.d.).Kaspersky. (n.d.). Phishing Prevention Tips. https://usa.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tipsNetwrix. (n.d.). Insider Threat Prevention Best Practices. https://www.netwrix.com/insider-threat-prevention-best-practices.html

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.

There are various security controls that can be added in the Workstation, Lan, LAN-to-WAN, WAN, Remote Access, and System/Application Domains, respectively. For example in the Workstation you can implement a endpoint security software. This essentially enables businesses to protect devices that employees use for work by allowing them to quickly detect malware and other cyber threats (Fortinet, n.d.). A software that could be installed for endpoint security software is ESET Endpoint Security. A security control for LAN is network segmentation. This essentially means that you control how the traffic flows amongst a network by splitting it into subnetworks. By reducing overall traffic, the system will work better for employees that use it and makes it safer (Cisco n.d.). This can be enforced by including internal firewalls, but the less costly resolution would be for technology to group and tag network traffic, then using the traffic tags to enforce segmentation policy directly onto the network equipment (Cisco, n.d.). Firewalls can be used to secure LAN-to-WAN. Firewalls allows traffic flows from the LAN, while blocking it out from the WAN. When a local client initiates a session to the internet, return traffic is allowed, but any traffic initiated from the internet, is blocked (Sandu, n.d.). The traffic from the internet could be an attacker, so its blocked. To protect the WAN and remote access I would recommend using a VPN because a VPN creates a tunnel between two points for data privacy (Paloalto, n.d.). This tunnel encrypts data and protects it from unwanted access, and it keeps all data confidential that travels over the WAN. For remote access the VPN adds in an extra layer of security by using a secure tunnel, allowing them to access the network as if they were at work, which reduces the risk of being exposed to cyber attacks. The security control for System/Application Domains would be patch managements. If a hacker or malware find out about the system vulnerabilities, a patch is sent out to correct it (Essex, 2024). If not it can be exploited, which would be bad for the company

Fortinet. (n.d.). What Is Endpoint Security?. https://www.fortinet.com/resources/cyberglossary/what-is-endpoint-security#:~:text=The%20endpoint%20security%20solution%20enables,face%20of%20a%20security%20threat.Cisco. (n.d.). What Is Network Segmentation?. https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.htmlDimi Sandu. (n.d.). Firewalls - Securing the LAN-WAN border. https://info.verkada.com/firewalls/#:~:text=In%20simple%20terms%2C%20by%20default,return%20traffic%20is%20not%20blocked).
Paloalto. (n.d.). SD-WAN vs. VPN: How Do They Compare?. https://www.paloaltonetworks.com/cyberpedia/sd-wan-vs-vpn#:~:text=It%20can%20adapt%20quickly%20and,network%20as%20the%20VPN%20server.David Essex (2024, May). What is patch management? Lifecycle, benefits and best practices.https://www.techtarget.com/searchenterprisedesktop/definition/patch-management