Student:	Email:
Bradley Adams	badams10@my.athens.edu

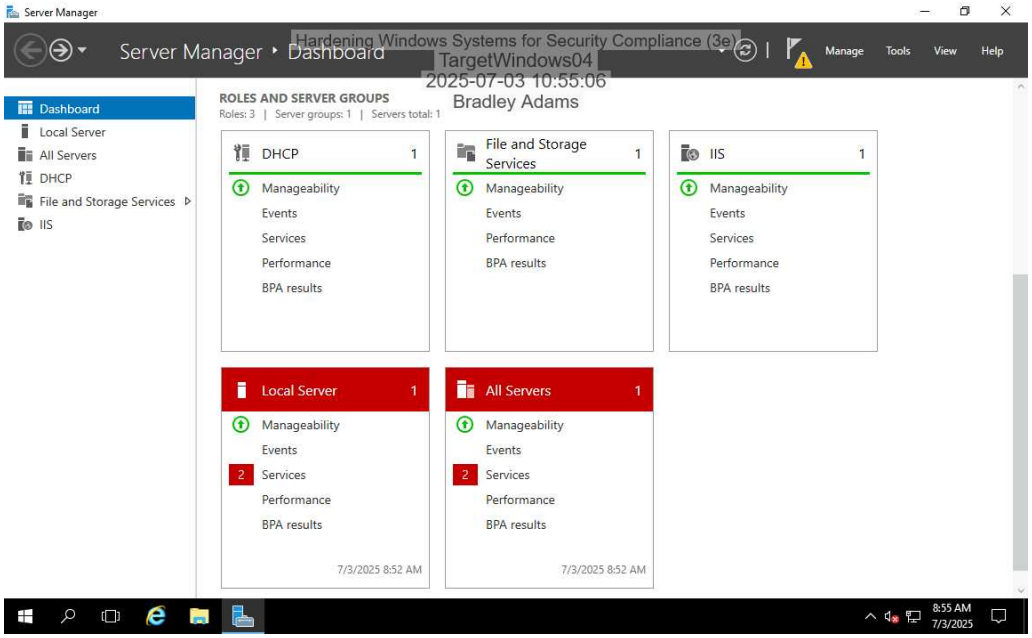
Time on Task:	Progress:
6 hours, 42 minutes	100%

Report Generated: Thursday, July 3, 2025 at 3:16 PM

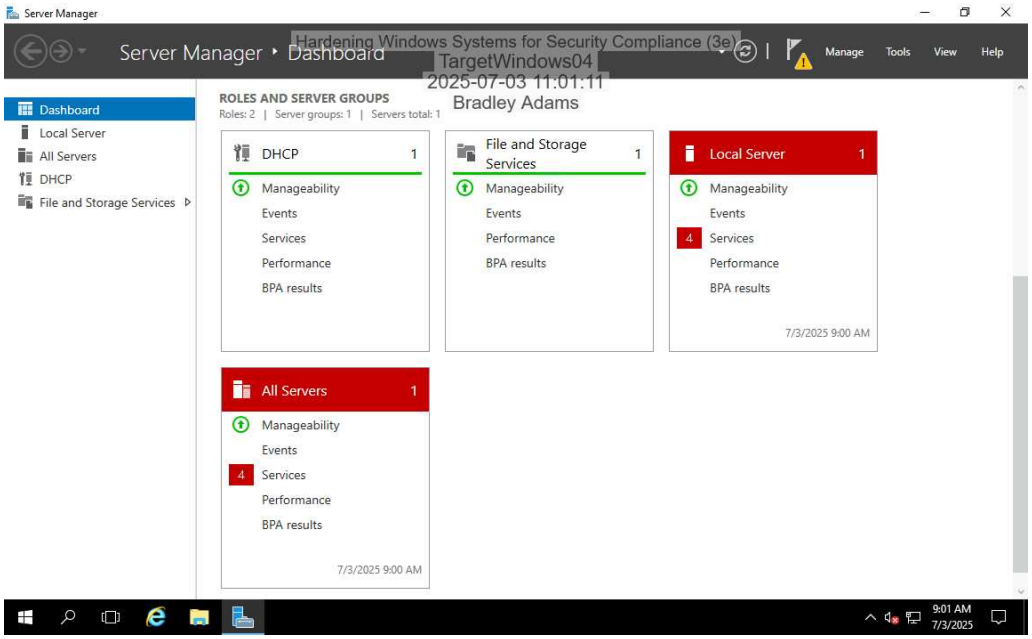
Section 1: Hands-On Demonstration

Part 1: Remove Unnecessary Server Roles

5. **Make a screen capture** showing the **current Roles and Server Groups**.

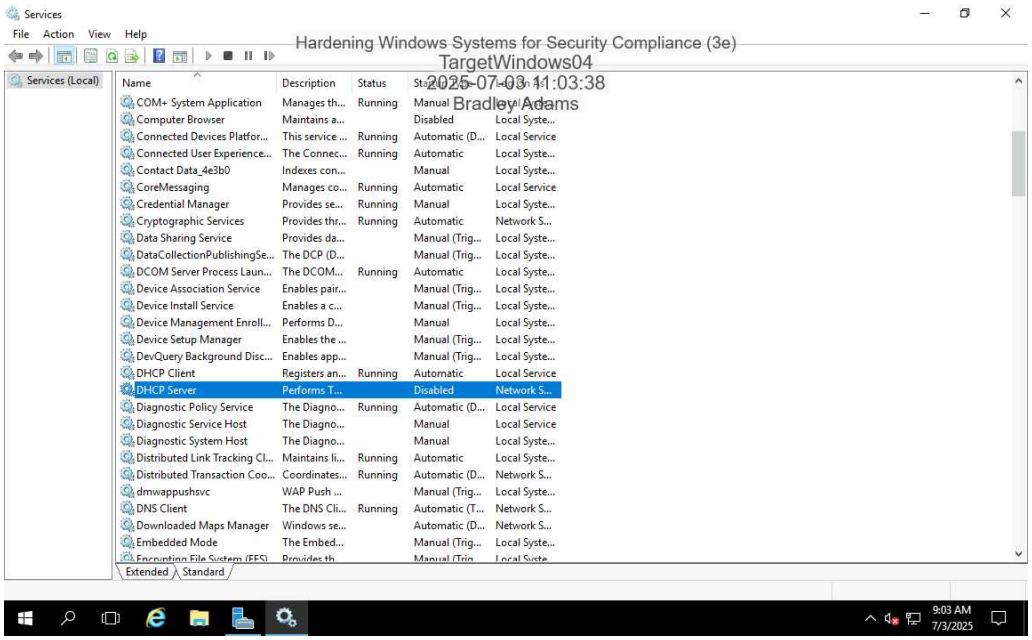


17. **Make a screen capture** showing the **updated Roles and Server Groups**.



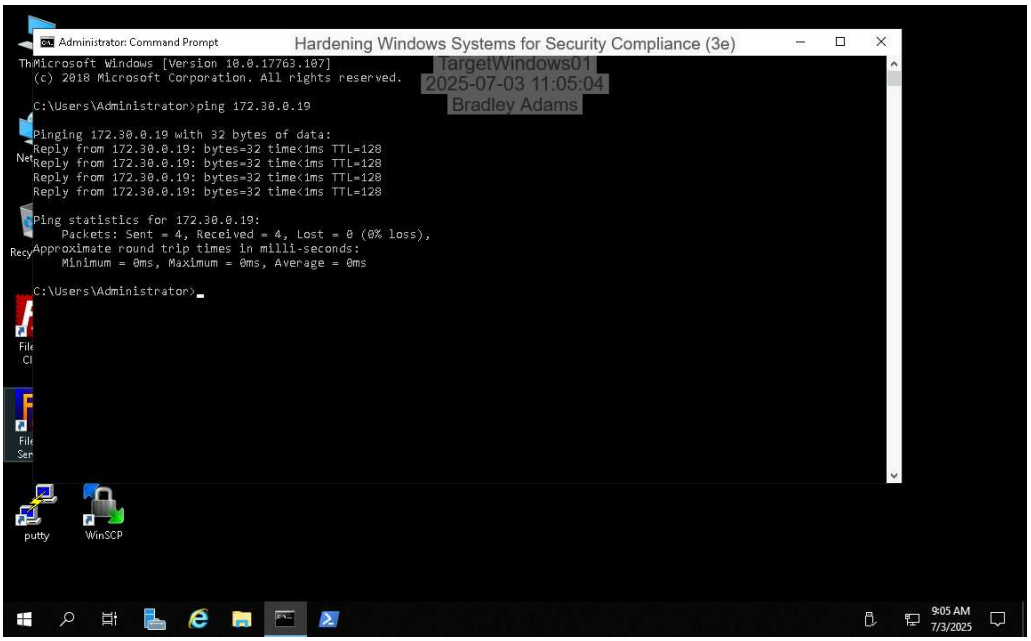
Part 2: Disable Unnecessary Services

8. **Make a screen capture** showing the **disabled DHCP Server service**.

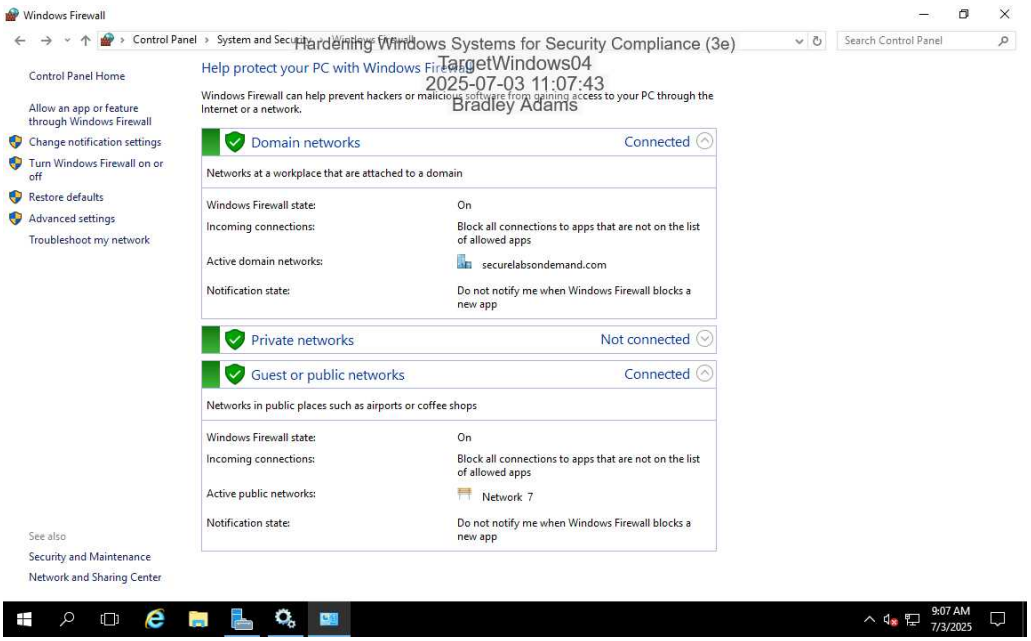


Part 3: Secure the Windows Firewall

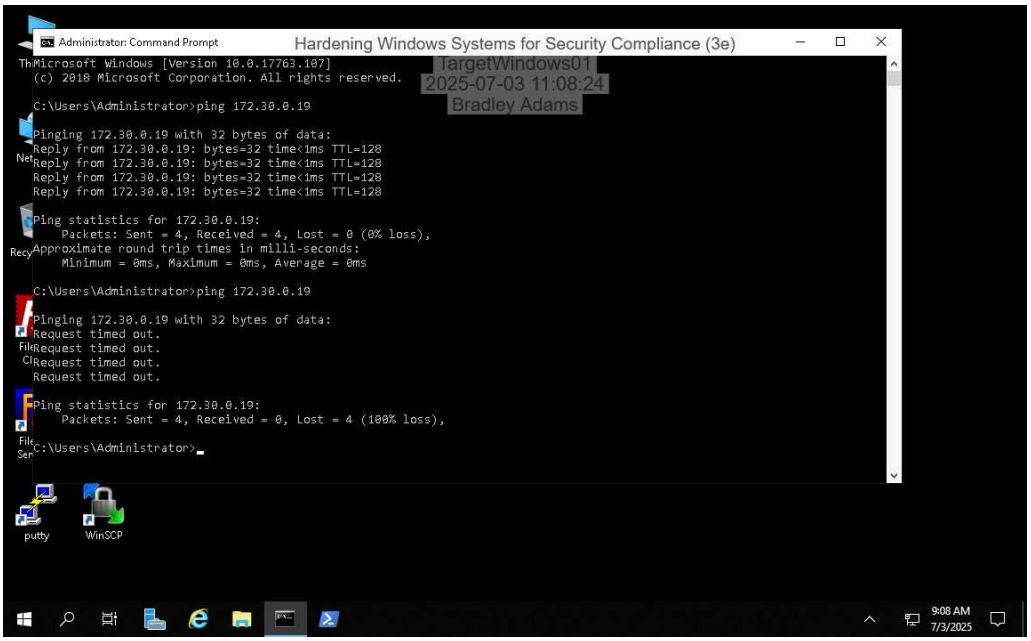
4. **Make a screen capture** showing the **results of the first ping test on TargetWindows01**.



15. **Make a screen capture** showing the **enabled Windows Firewall for all three profiles**.



19. **Make a screen capture** showing the **results of the second Ping test**.



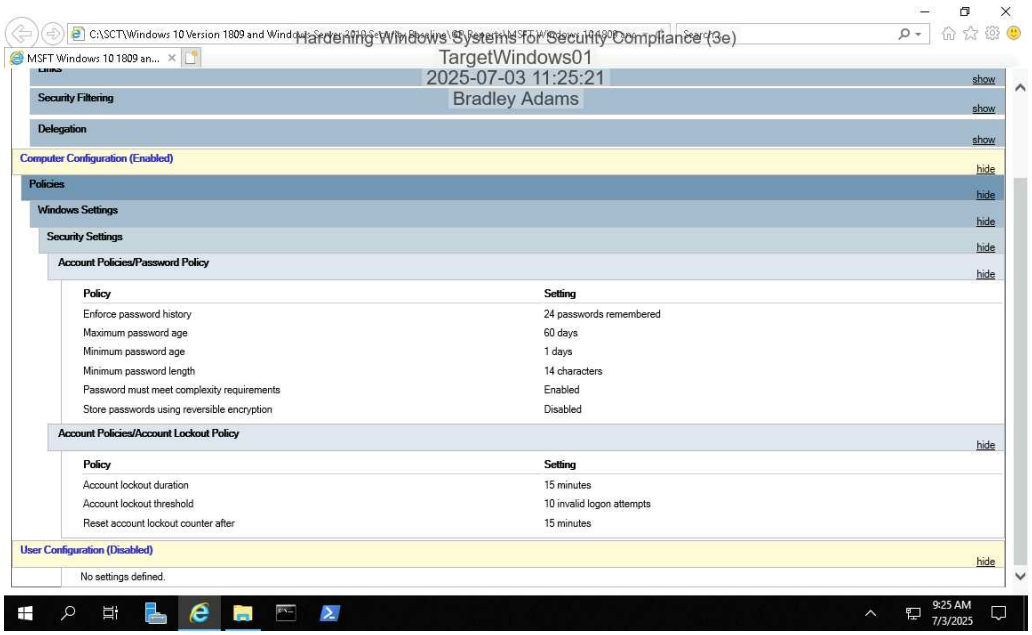
20. **Describe** how the firewall changes affected the results.

The firewall blocks ping requests, ICMP Echo Requests, by filtering incoming ICMP traffic. When a ping is sent to a machine, the firewall inspects the packet. If there's no rule allowing ICMP Echo Requests, the packet is dropped, preventing an Echo Reply, and the host appears offline or unreachable.

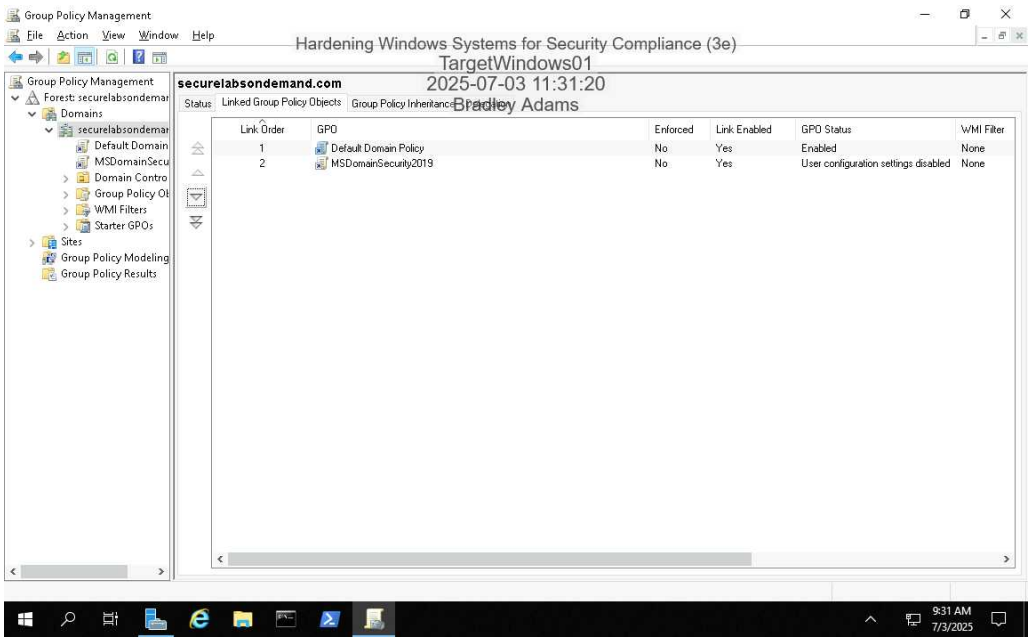
Section 2: Applied Learning

Part 1: Apply Windows Security Baselines

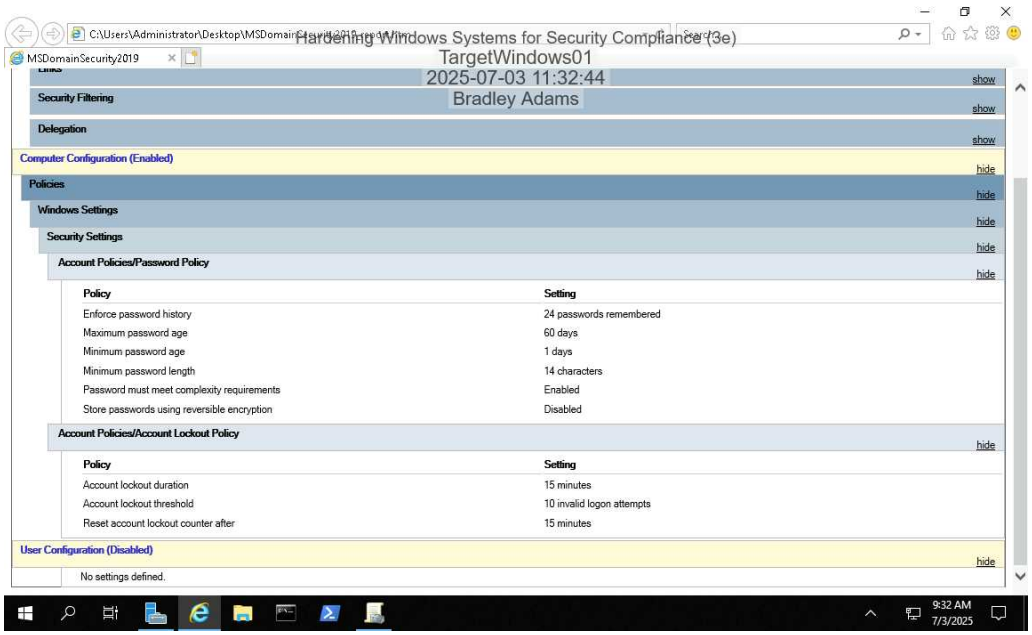
5. **Make a screen capture** showing **Microsoft's recommended Password and Account Lockout policy settings**.



18. **Make a screen capture** showing the **linked MSDomainSecurity2019 object**.

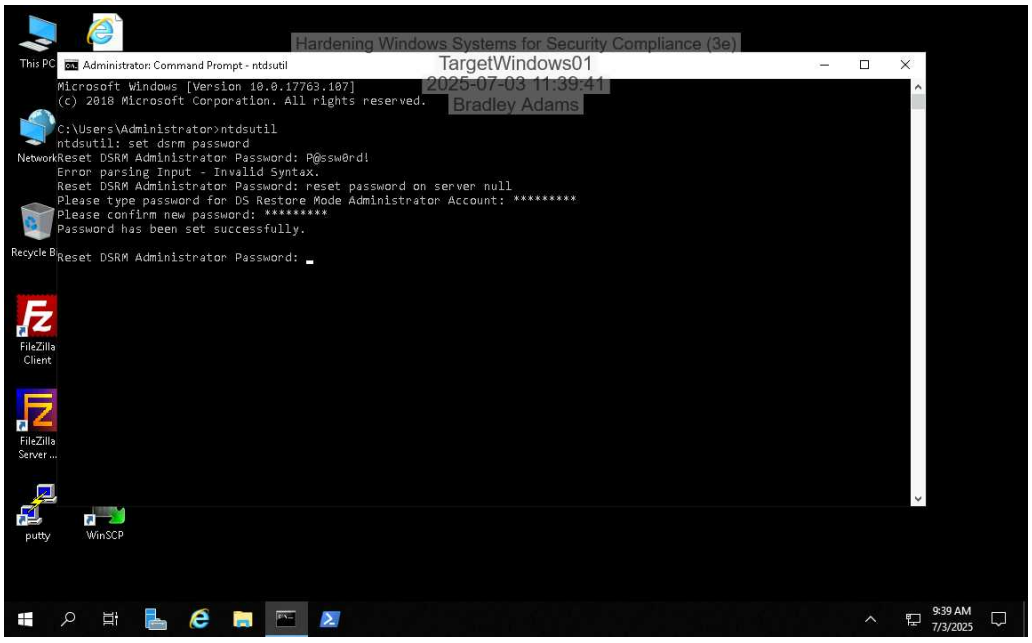


22. **Make a screen capture** showing the **implemented Password and Account Lockout policy settings**.



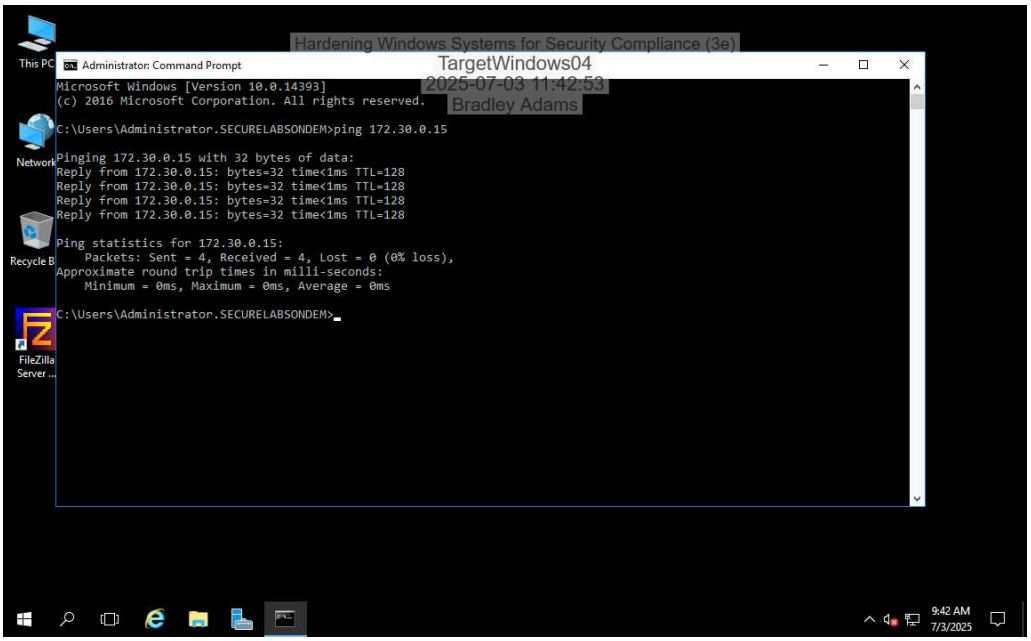
Part 2: Reset the DSRM Password

7. **Make a screen capture** showing the **successful DSRM password change**.

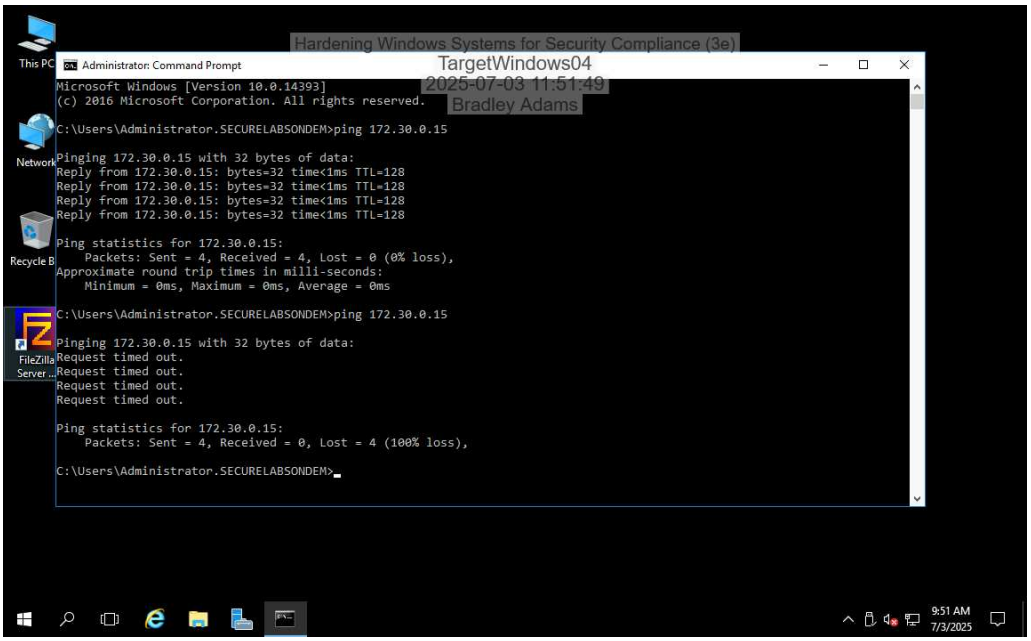


Part 3: Secure the Windows Defender Firewall

4. **Make a screen capture** showing the **results of the first ping test on TargetWindows04**.



17. **Make a screen capture** showing the **results of the second ping test on TargetWindows04**.



18. **Describe** how the firewall changes affected the results.

The firewall blocks ping requests, specifically ICMP Echo Requests, by filtering incoming ICMP traffic. When a ping reaches the machine, the firewall examines the packet. If no rule permits ICMP Echo Requests, the packet is dropped, preventing an Echo Reply and making the host appear offline or unreachable.

Section 3: Challenge and Analysis

Part 1: Analysis and Discussion

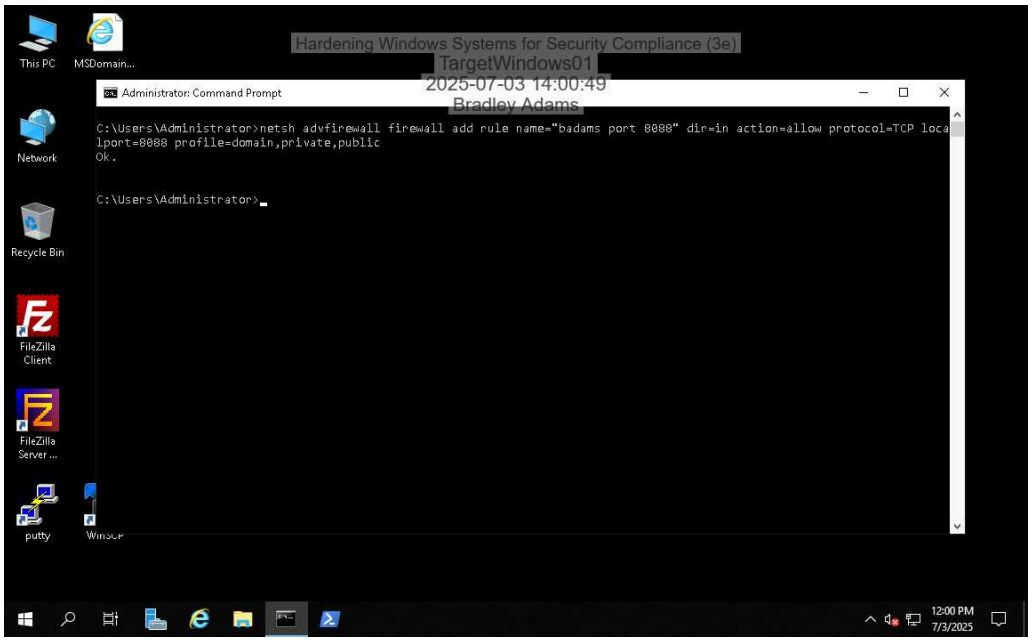
Why would disabling services be important in securing and optimizing server performance? What determines which services are disabled?

Disabling unnecessary services on a Windows server is an essential practice for both securing the system and optimizing performance. Every service running on a server means not only the consumption of CPU and memory resources but also increases the attack surface. Unused or redundant services can expose vulnerabilities. Once disabled, the server can dedicate more memory and processing power to essential functions.

To determine which services to disable, the server's role and responsibilities must be defined and aligned with the services currently installed and/or running. If a service does not support the intended role of the server, that service should be disabled. Administrators should audit the server's purpose and consult security best practices to determine a minimal service set, avoiding 'feature creep.'

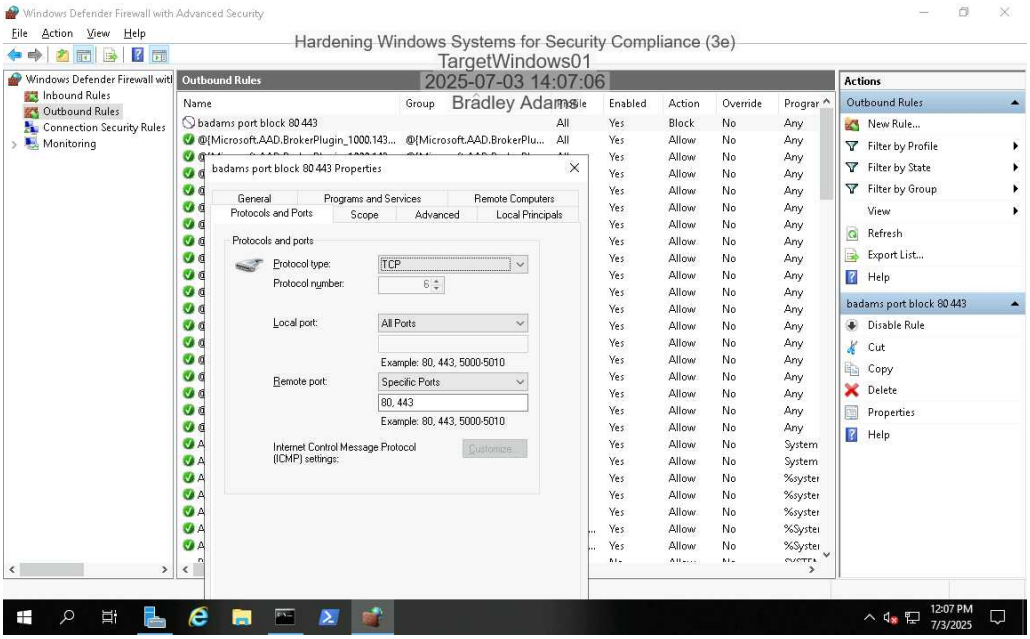
Part 2: Tools and Commands

Make a screen capture showing your **executed command line statement**.



Part 3: Challenge Exercise

Make a screen capture showing your **new Outbound rule**.



Make a screen capture showing the **result of the rule in a browser window**.