

Hardening Windows Systems for Security Compliance (3e)

Security Strategies in Windows Platforms and Applications, Third Edition - Lab 08

Student:

Bradley Adams

Email:

badams10@my.athens.edu

Time on Task:

6 hours, 42 minutes

Progress:

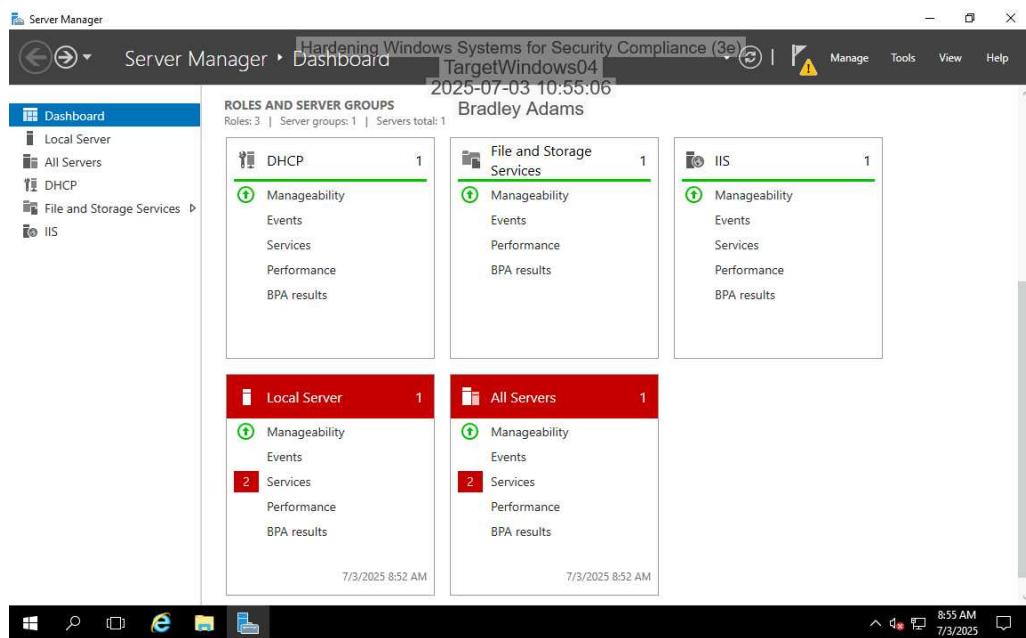
100%

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

Section 1: Hands-On Demonstration

Part 1: Remove Unnecessary Server Roles

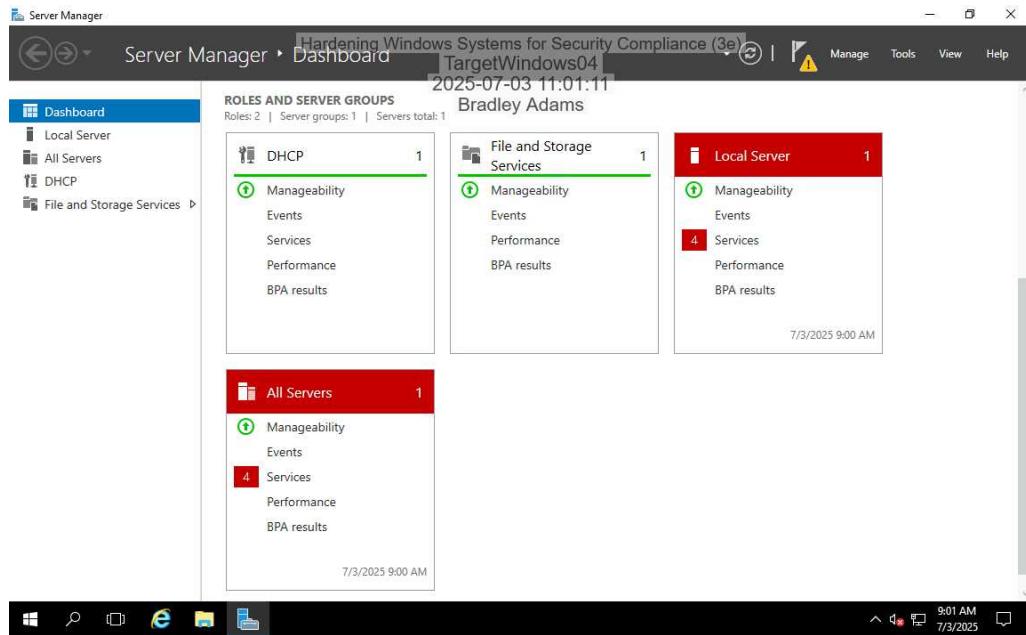
5. Make a screen capture showing the current Roles and Server Groups.



Hardening Windows Systems for Security Compliance (3e)

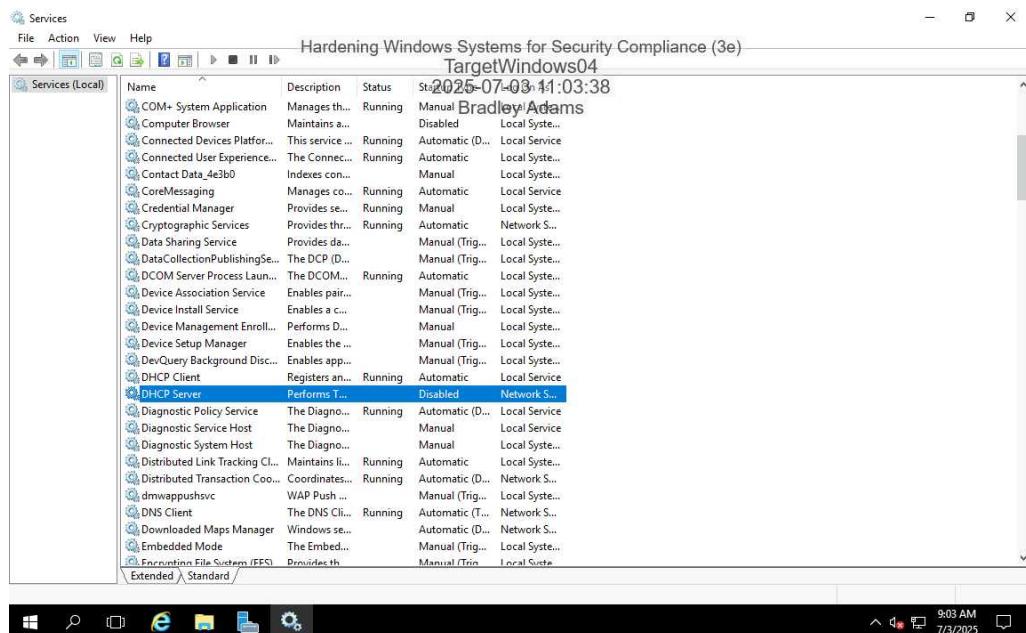
Security Strategies in Windows Platforms and Applications, Third Edition - Lab 08

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

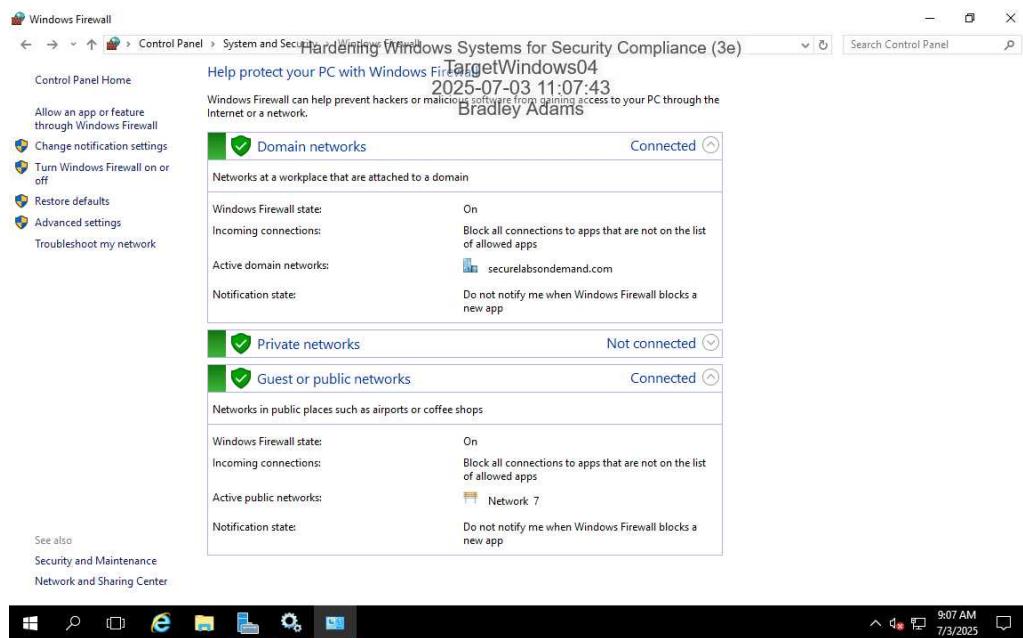
Hardening Windows Systems for Security Compliance (3e)

Security Strategies in Windows Platforms and Applications, Third Edition - Lab 08

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

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The title bar also displays "Hardening Windows Systems for Security Compliance (3e)", the computer name "TargetWindows01", the date and time "2025-07-03 11:05:04", and the user "Bradley Adams". The command entered was "ping 172.30.0.19". The output shows four successful replies from the target IP address. Below the ping command, statistics are provided: 4 packets sent, 4 received, 0 lost (0% loss), and approximate round trip times (Minimum = 0ms, Maximum = 0ms, Average = 0ms). The prompt then changes to "C:\Users\Administrator>". The desktop background is visible, showing icons for File Explorer, File Server, PuTTY, and WinSCP. The taskbar at the bottom shows the Start button, a search icon, Task View, Internet Explorer, File Explorer, Taskbar settings, and a clock indicating 9:05 AM on 7/3/2025.

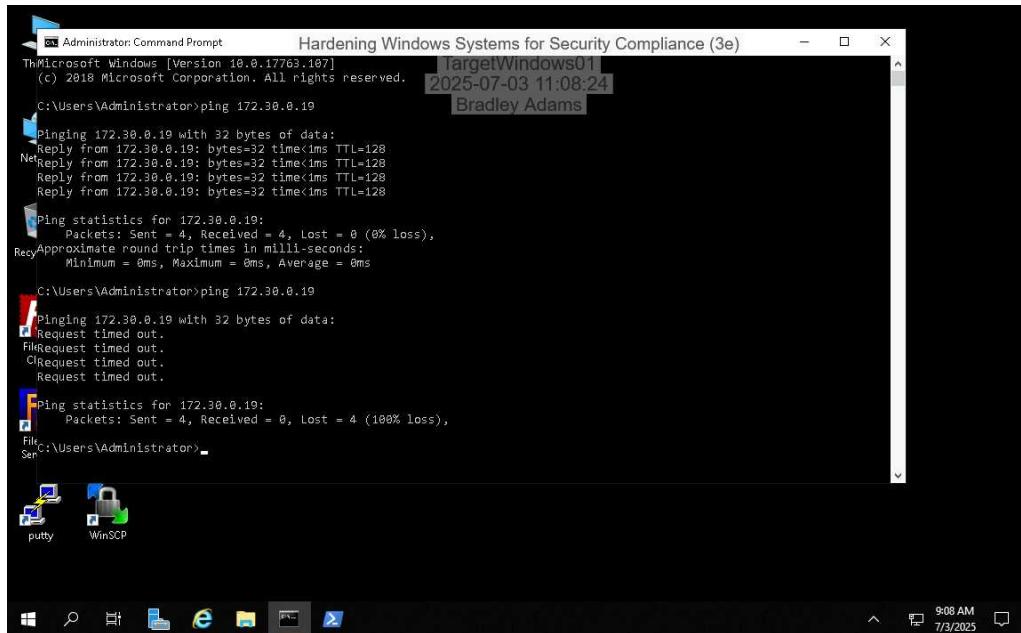
15. Make a screen capture showing the enabled Windows Firewall for all three profiles.



Hardening Windows Systems for Security Compliance (3e)

Security Strategies in Windows Platforms and Applications, Third Edition - Lab 08

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



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The title bar also displays "Hardening Windows Systems for Security Compliance (3e)". The window content shows the following command and its output:

```
C:\Users\Administrator>ping 172.30.0.19

Pinging 172.30.0.19 with 32 bytes of data:
Reply from 172.30.0.19: bytes=32 time<1ms TTL=128

Ping statistics for 172.30.0.19:
    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>ping 172.30.0.19

IRequest timed out.
FileRequest timed out.
ClipboardRequest timed out.
Request timed out.

Ping statistics for 172.30.0.19:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

The taskbar at the bottom shows icons for File Explorer, Edge, Task View, and Start. The system tray indicates the date and time as 9:08 AM, 7/3/2025.

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.

The screenshot shows the 'Computer Configuration (Enabled)' section of the application. Under 'Policies', the 'Windows Settings' tab is selected, which contains the 'Account Policies/Password Policy' and 'Account Policies/Account Lockout Policy' sections. The 'Account Policies/Password Policy' section displays the following settings:

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

The 'Account Policies/Account Lockout Policy' section displays the following settings:

Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

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

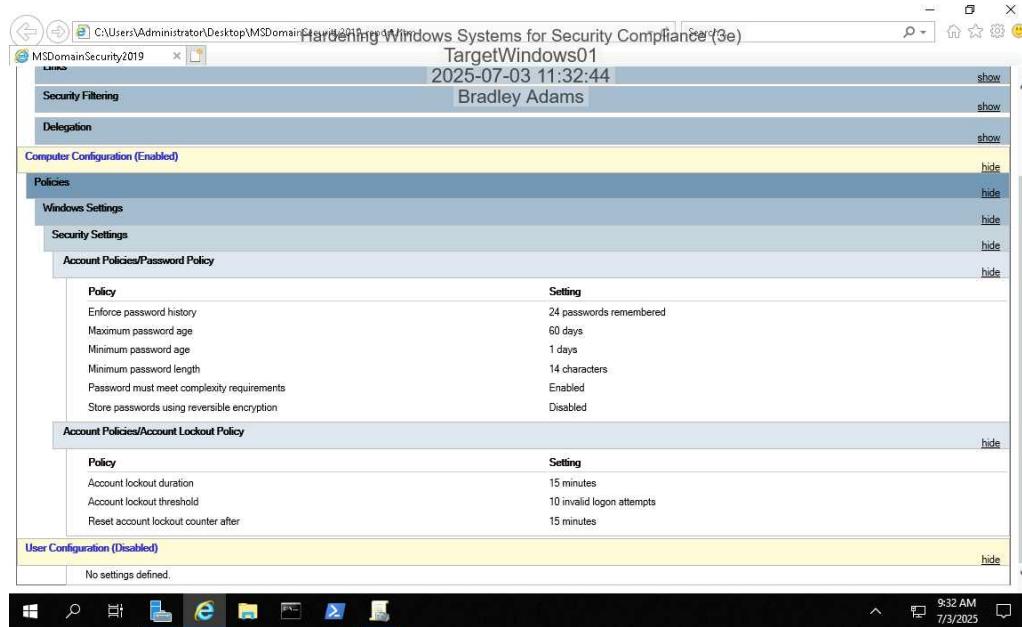
The screenshot shows the 'Group Policy Management' console. The left navigation pane shows a tree structure with 'securelabsondemand.com' selected. The main pane displays the 'Linked Group Policy Objects' table:

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter
1	Default Domain Policy	No	Yes	Enabled	None
2	MSDomainSecurity2019	No	Yes	User configuration settings disabled	None

Hardening Windows Systems for Security Compliance (3e)

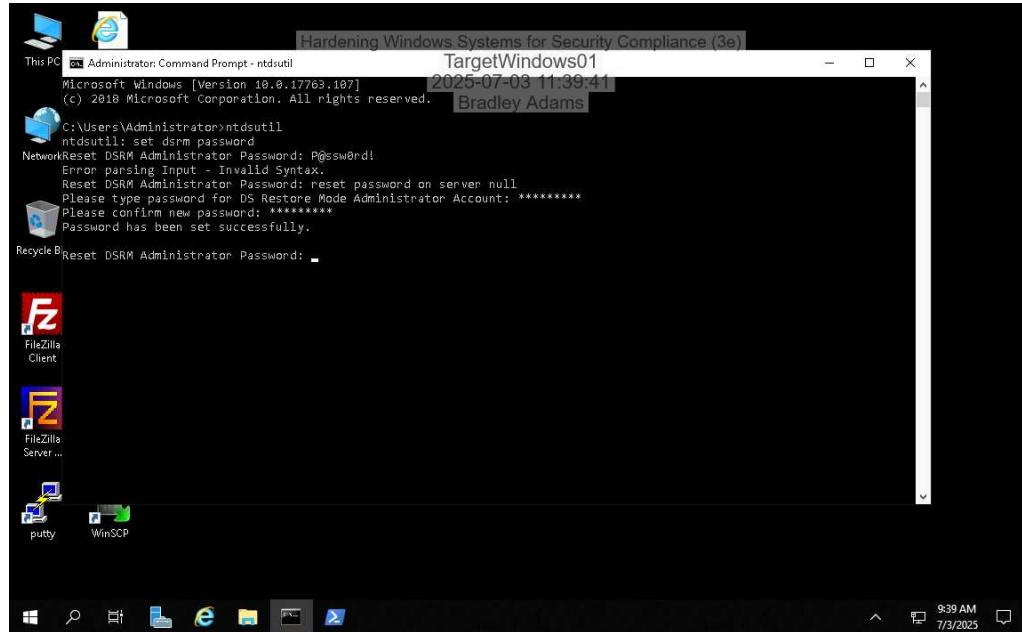
Security Strategies in Windows Platforms and Applications, Third Edition - Lab 08

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.

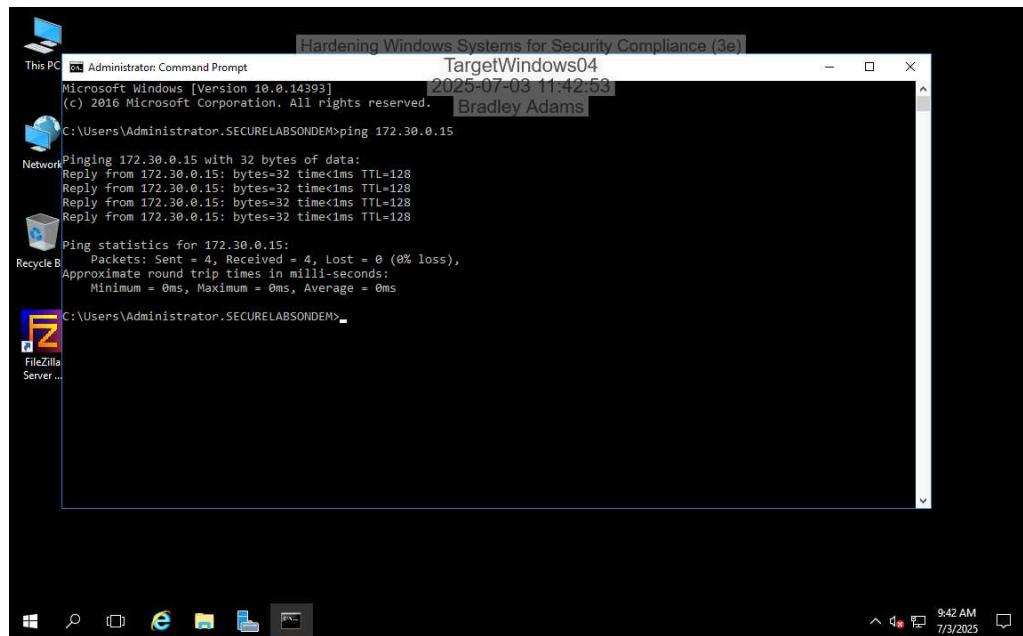


Part 3: Secure the Windows Defender Firewall

Hardening Windows Systems for Security Compliance (3e)

Security Strategies in Windows Platforms and Applications, Third Edition - Lab 08

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



```
Administrator: Command Prompt
TargetWindows04
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
Bradley Adams

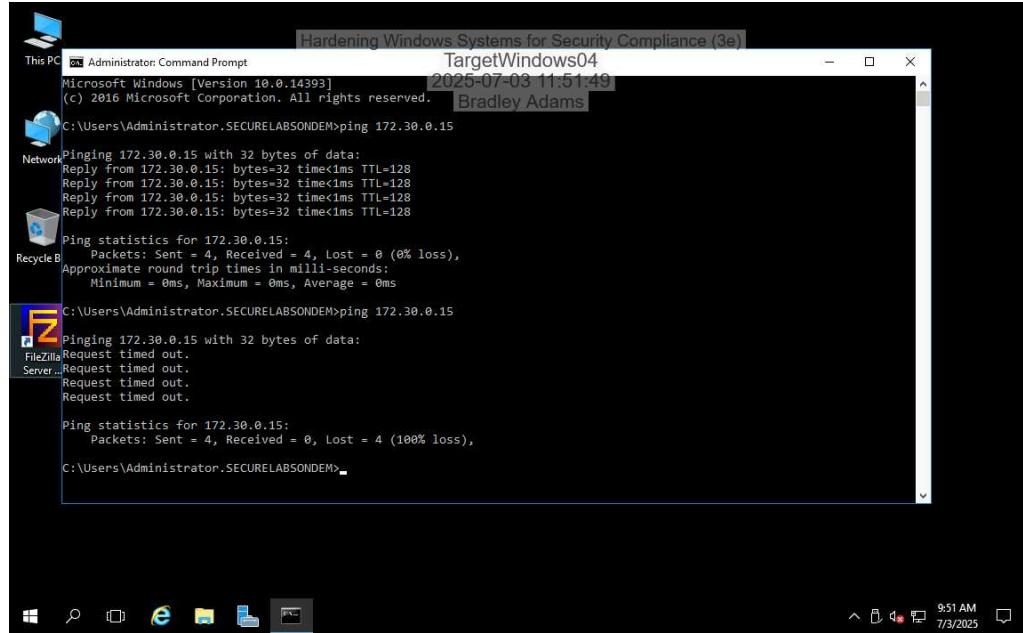
C:\Users\Administrator.SECURELABSONDEM>ping 172.30.0.15

Pinging 172.30.0.15 with 32 bytes of data:
Reply from 172.30.0.15: bytes=32 time<1ms TTL=128

Ping statistics for 172.30.0.15:
    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.SECURELABSONDEM>
```

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



```
Administrator: Command Prompt
TargetWindows04
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
Bradley Adams

C:\Users\Administrator.SECURELABSONDEM>ping 172.30.0.15

Pinging 172.30.0.15 with 32 bytes of data:
Reply from 172.30.0.15: bytes=32 time<1ms TTL=128

Ping statistics for 172.30.0.15:
    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.SECURELABSONDEM>ping 172.30.0.15

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.30.0.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Administrator.SECURELABSONDEM>
```

Hardening Windows Systems for Security Compliance (3e)

Security Strategies in Windows Platforms and Applications, Third Edition - Lab 08

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

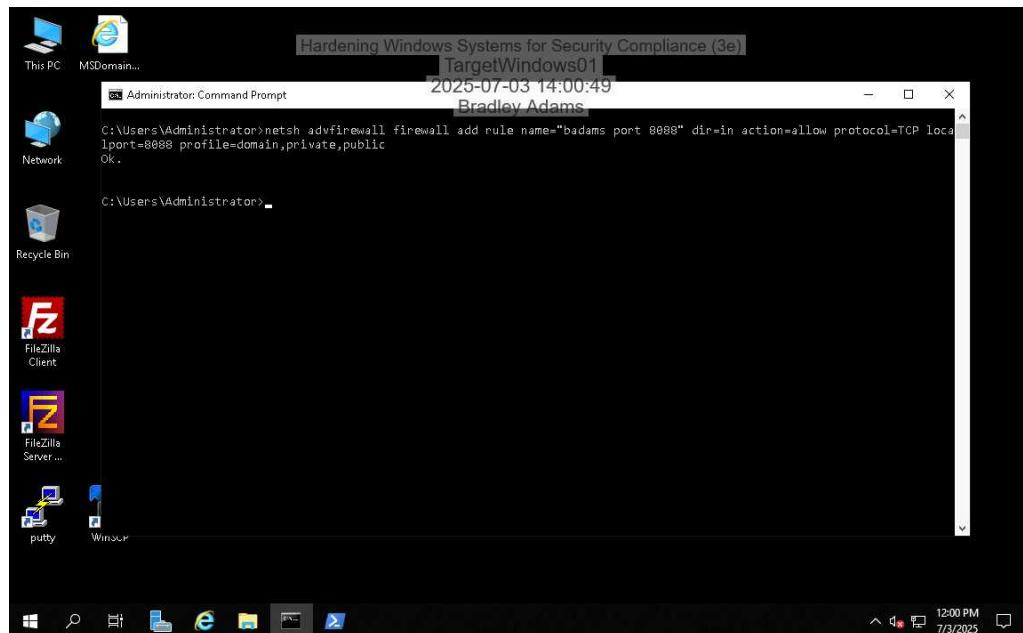
Why would disabling services be important in securing and optimizing server performance? What determines which services are disabled?

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.



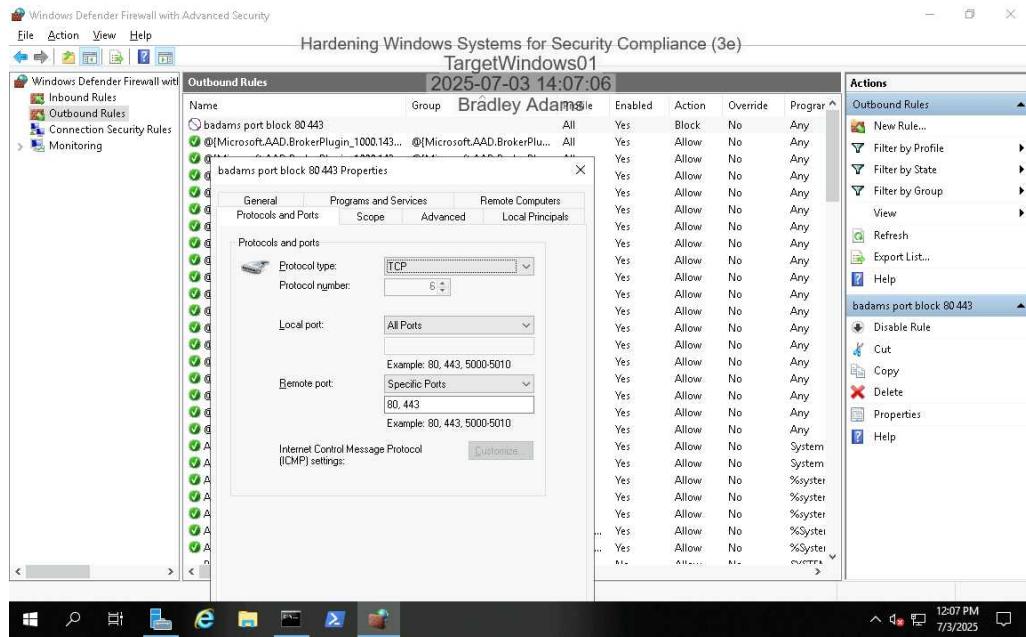
The screenshot shows a Windows desktop environment. On the left is a dark-themed desktop icon bar with icons for This PC, MSDomain..., Network, Recycle Bin, FileZilla Client, FileZilla Server ..., putty, and Winscp. In the center is a Command Prompt window titled 'Administrator: Command Prompt' with the title bar 'Hardening Windows Systems for Security Compliance (3e)' and 'TargetWindows01'. The window shows the command: 'netsh advfirewall add rule name="badams port 8088" dir=in action=allow protocol=TCP loca'. Below the command is the output 'Ok.' and the prompt 'C:\Users\Administrator>'. The taskbar at the bottom shows standard Windows icons like Start, Search, Task View, Edge, File Explorer, and Task Manager. The system tray in the bottom right corner shows the date '7/3/2025' and time '12:00 PM'.

Part 3: Challenge Exercise

Hardening Windows Systems for Security Compliance (3e)

Security Strategies in Windows Platforms and Applications, Third Edition - Lab 08

Make a screen capture showing your new Outbound rule.



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

