Student:	Email:
Jacob Jeffers	jjeffers6151@ucumberlands.edu

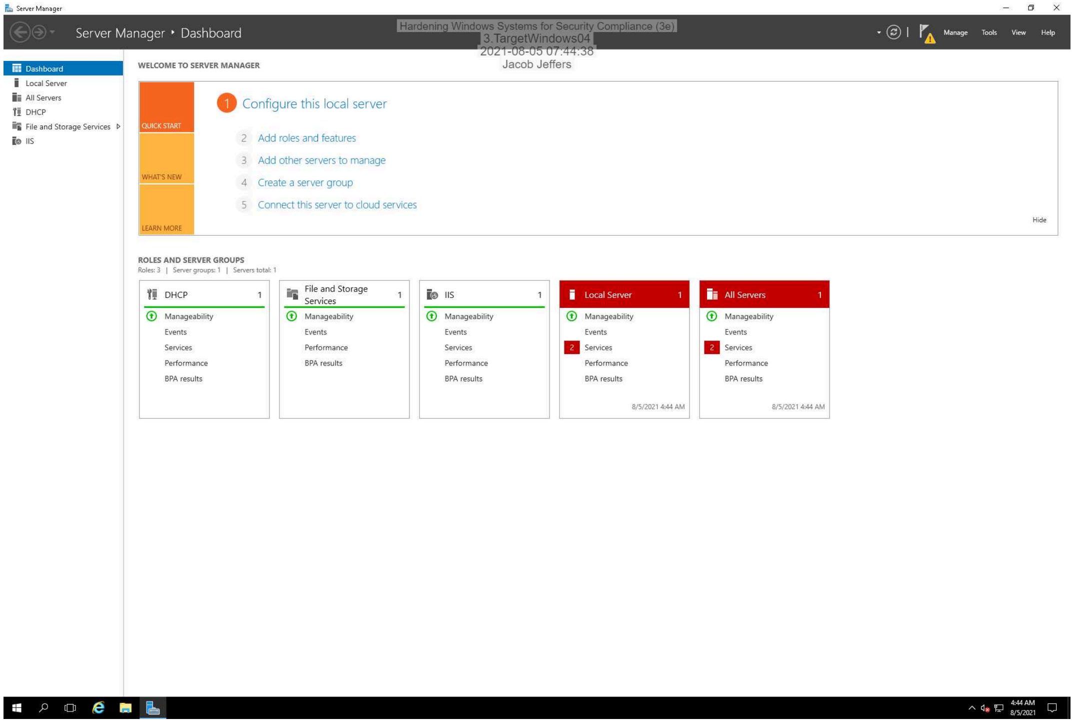
Time on Task:	Progress:
8 hours, 30 minutes	100%

Report Generated: Thursday, August 5, 2021 at 8:38 AM

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)
3.TargetWindows04
2021-08-05 07:44:38
Jacob Jeffers

WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

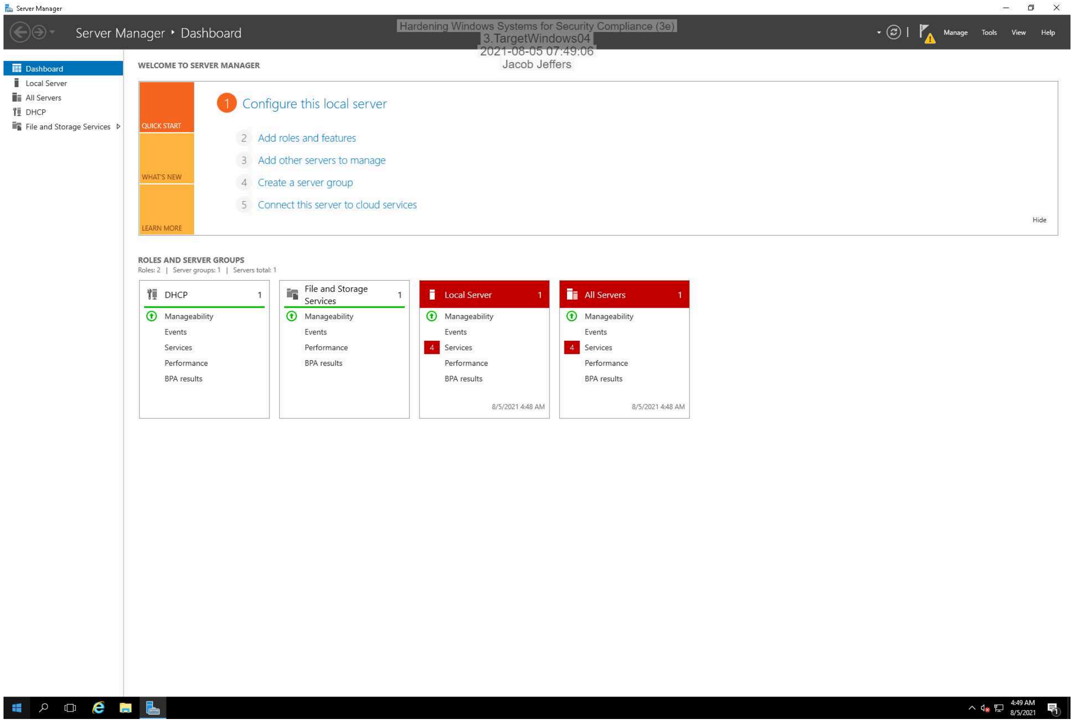
5 Connect this server to cloud services

ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1

DHCP 1	File and Storage Services 1	IIS 1	Local Server 1	All Servers 1
Manageability	Manageability	Manageability	Manageability	Manageability
Events	Events	Events	Events	Events
Services	Performance	Services	2 Services	2 Services
Performance	BPA results	Performance	Performance	Performance
BPA results		BPA results	BPA results	BPA results
			8/5/2021 4:44 AM	8/5/2021 4:44 AM

4:44 AM
8/5/2021

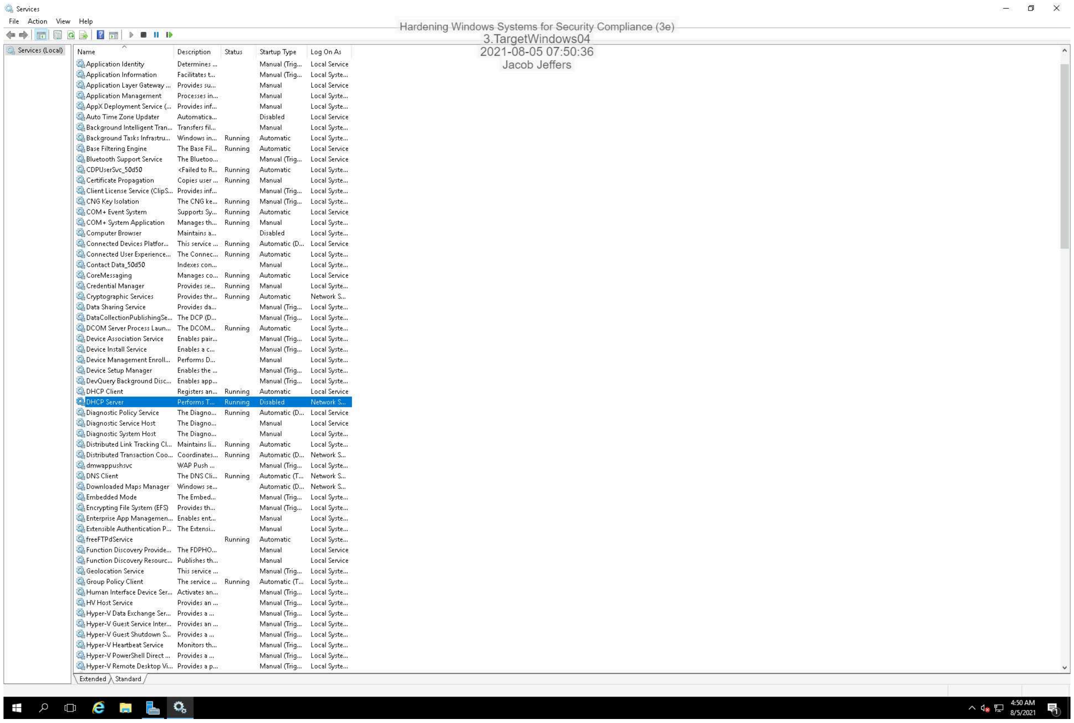
17. **Make a screen capture** showing the **updated Roles and Server Groups**.



Hardening Windows Systems for Security Compliance (3e)
3.TargetWindows04
2021-08-05 07:49:06
Jacob Jeffers

Part 2: Disable Unnecessary Services

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

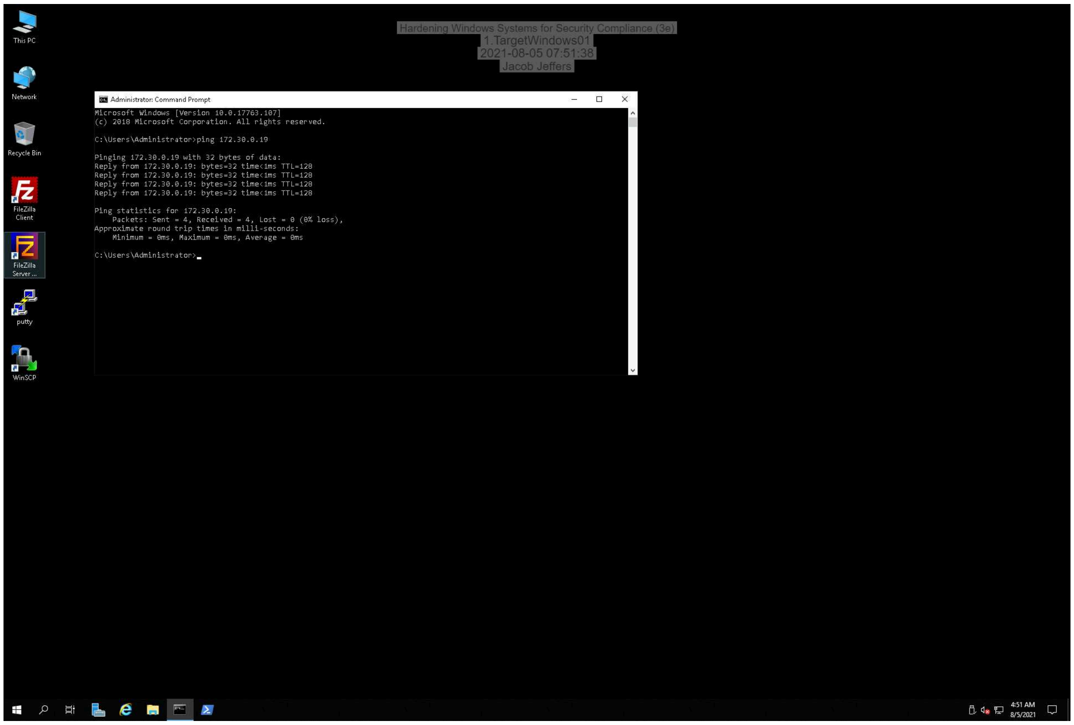


Hardening Windows Systems for Security Compliance (3e)
3.TargetWindows04
2021-08-05 07:50:36
Jacob Jeffers

Name	Description	Status	Startup Type	Log On As
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...		Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...	Provides inf...		Manual	Local Syste...
Auto Time Zone Updater	Automatica...		Disabled	Local Service
Background Intelligent Tran...	Transfers fil...		Manual	Local Syste...
Background Tasks Infrastru...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Local Service
CDPUserSvc_50d50	<Failed to R...	Running	Automatic	Local Syste...
Certificate Propagation	Copies user ...	Running	Manual	Local Syste...
Client License Service (ClipS...	Provides inf...		Manual (Trig...	Local Syste...
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...	Running	Manual	Local Syste...
Computer Browser	Maintains a...		Disabled	Local Syste...
Connected Devices Platfor...	This service ...	Running	Automatic (D...	Local Service
Connected User Experience...	The Connec...	Running	Automatic	Local Syste...
Contact Data_50d50	Indexes con...		Manual	Local Syste...
CoreMessaging	Manages co...	Running	Automatic	Local Service
Credential Manager	Provides se...	Running	Manual	Local Syste...
Cryptographic Services	Provides thr...	Running	Automatic	Network S...
Data Sharing Service	Provides da...		Manual (Trig...	Local Syste...
DataCollectionPublishingSe...	The DCP (D...		Manual (Trig...	Local Syste...
DCOM Server Process Laun...	The DCOM...	Running	Automatic	Local Syste...
Device Association Service	Enables pair...		Manual (Trig...	Local Syste...
Device Install Service	Enables a c...		Manual (Trig...	Local Syste...
Device Management Enroll...	Performs D...		Manual	Local Syste...
Device Setup Manager	Enables the ...		Manual (Trig...	Local Syste...
DevQuery Background Disc...	Enables app...		Manual (Trig...	Local Syste...
DHCP Client	Registers an...	Running	Automatic	Local Service
DHCP Server	Performs T...	Running	Disabled	Network S...
Diagnostic Policy Service	The Diagno...	Running	Automatic (D...	Local Service
Diagnostic Service Host	The Diagno...		Manual	Local Service
Diagnostic System Host	The Diagno...		Manual	Local Syste...
Distributed Link Tracking Cl...	Maintains li...	Running	Automatic	Local Syste...
Distributed Transaction Coo...	Coordinates...	Running	Automatic (D...	Network S...
dmwappushsvc	WAP Push ...		Manual (Trig...	Local Syste...
DNS Client	The DNS Cli...	Running	Automatic (T...	Network S...
Downloaded Maps Manager	Windows se...		Automatic (D...	Network S...
Embedded Mode	The Embed...		Manual (Trig...	Local Syste...
Encrypting File System (EFS)	Provides th...		Manual (Trig...	Local Syste...
Enterprise App Managemen...	Enables ent...		Manual	Local Syste...
Extensible Authentication P...	The Extensi...		Manual	Local Syste...
freeFTPdService		Running	Automatic	Local Syste...
Function Discovery Provide...	The FDPHO...		Manual	Local Service
Function Discovery Resourc...	Publishes th...		Manual	Local Service
Geolocation Service	This service ...		Manual (Trig...	Local Syste...
Group Policy Client	The service ...	Running	Automatic (T...	Local Syste...
Human Interface Device Ser...	Activates an...		Manual (Trig...	Local Syste...
HV Host Service	Provides an ...		Manual (Trig...	Local Syste...
Hyper-V Data Exchange Ser...	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Guest Service Inter...	Provides an ...		Manual (Trig...	Local Syste...
Hyper-V Guest Shutdown S...	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Heartbeat Service	Monitors th...		Manual (Trig...	Local Syste...
Hyper-V PowerShell Direct ...	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Remote Desktop Vi...	Provides a p...		Manual (Trig...	Local Syste...

Part 3: Secure the Windows Firewall

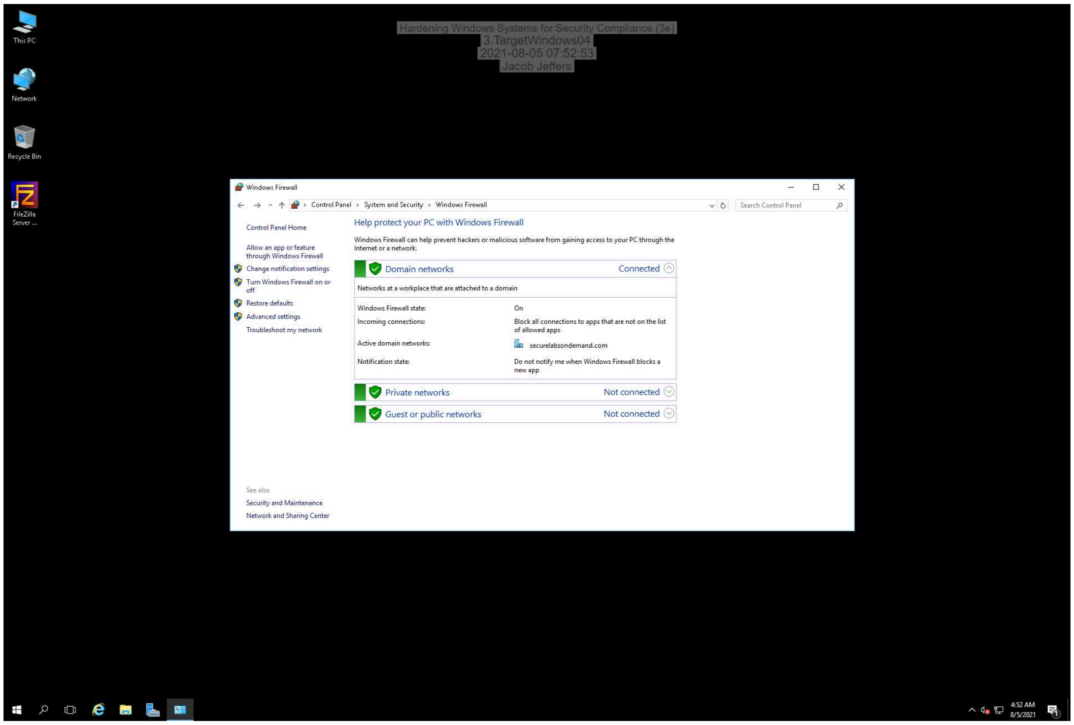
4. **Make a screen capture** showing the **results of the first ping test on TargetWindows01**.



Hardening Windows Systems for Security Compliance (3e)
1.TargetWindows01
2021-08-05 07:51:38
Jacob Jeffers

```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

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
Reply from 172.30.0.19: bytes=32 time<1ms TTL=128
Reply from 172.30.0.19: bytes=32 time<1ms TTL=128
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>_
```

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



Hardening Windows Systems for Security Compliance (3e)
3.TargetWindows04
2021-08-05 07:52:53
Jacob Jeffers

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Domain networks — Connected

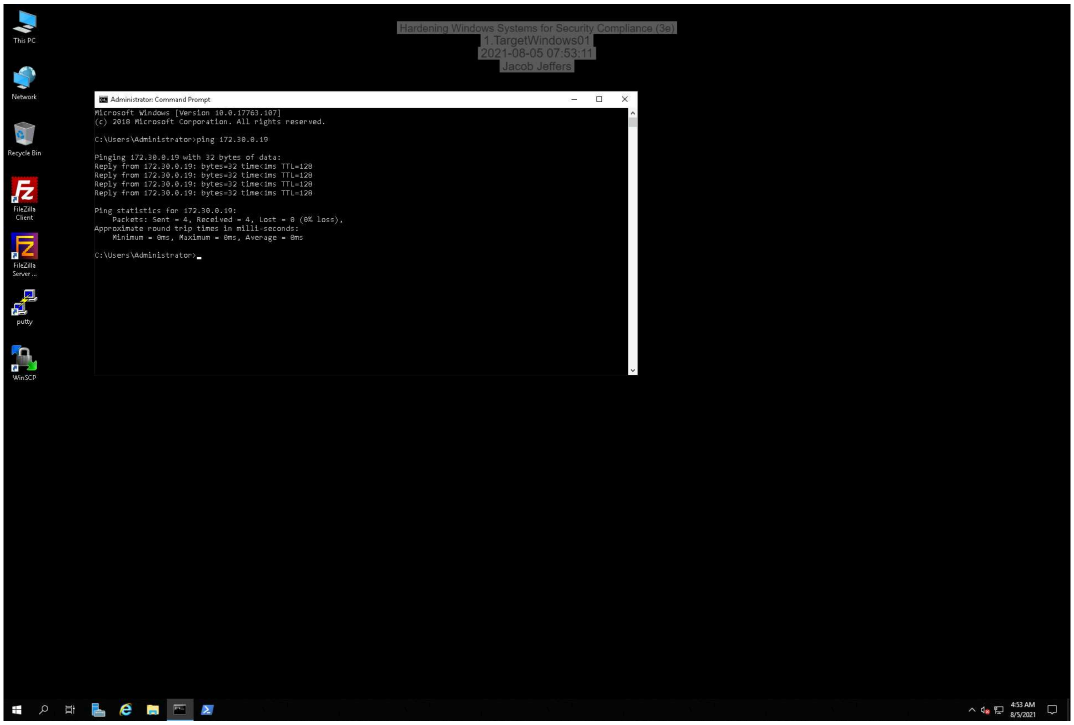
Networks at a workplace that are attached to a domain

Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active domain networks:	securelabsondemand.com
Notification state:	Do not notify me when Windows Firewall blocks a new app

Private networks — Not connected

Guest or public networks — Not connected

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



Hardening Windows Systems for Security Compliance (3e)
1.TargetWindows01
2021-08-05 07:53:11
Jacob Jeffers

```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

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
Reply from 172.30.0.19: bytes=32 time<1ms TTL=128
Reply from 172.30.0.19: bytes=32 time<1ms TTL=128
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>
```

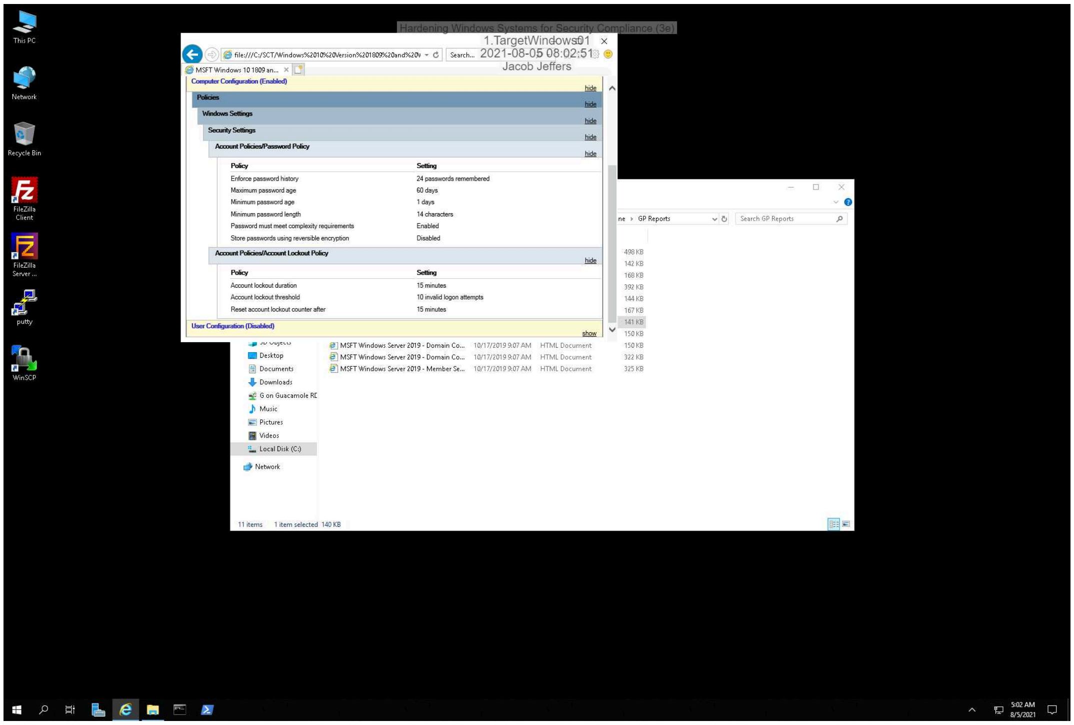
20. **Describe** how the firewall changes affected the results.

The firewall on TargetWindows04 blocks ICMP traffic, and since the ping function utilizes ICMP, this disabled anyone from pinging our server. This is a great way to harden the system to prevent DDoS attacks utilizing ping.

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**.



Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

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

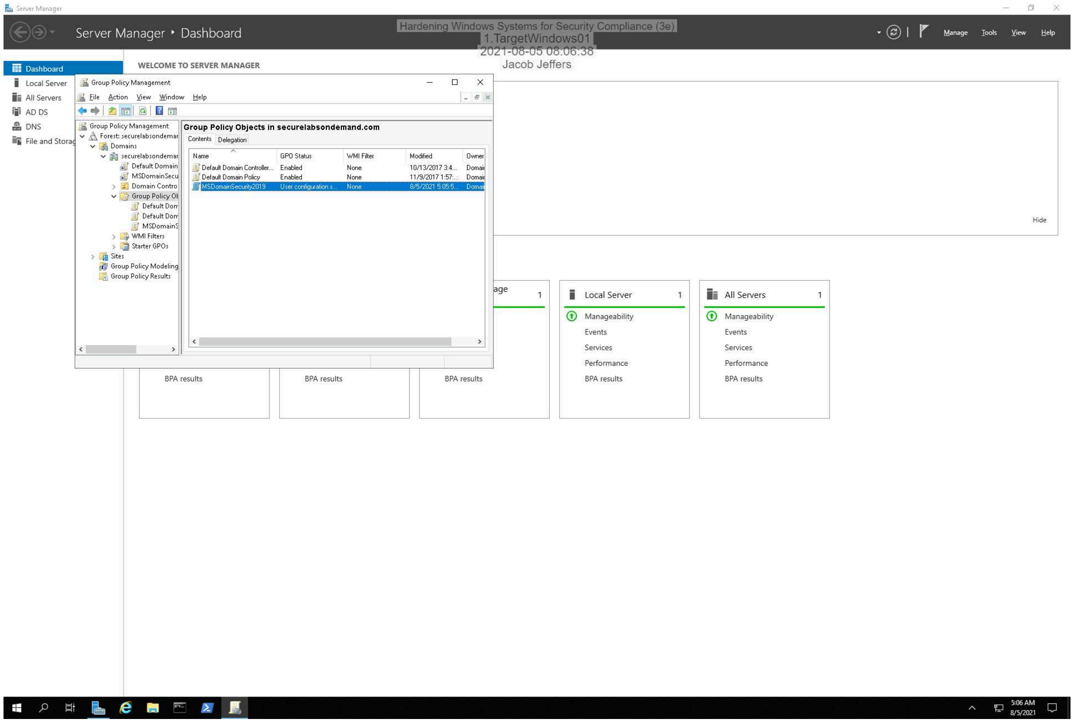
Account Policies/Account Lockout Policy

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

User Configuration (Disabled)

			498 KB
			142 KB
			168 KB
			392 KB
			144 KB
			167 KB
			141 KB
			150 KB
MSFT Windows Server 2019 - Domain Co...	10/17/2019 9:07 AM	HTML Document	150 KB
MSFT Windows Server 2019 - Domain Co...	10/17/2019 9:07 AM	HTML Document	322 KB
MSFT Windows Server 2019 - Member Se...	10/17/2019 9:07 AM	HTML Document	325 KB

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

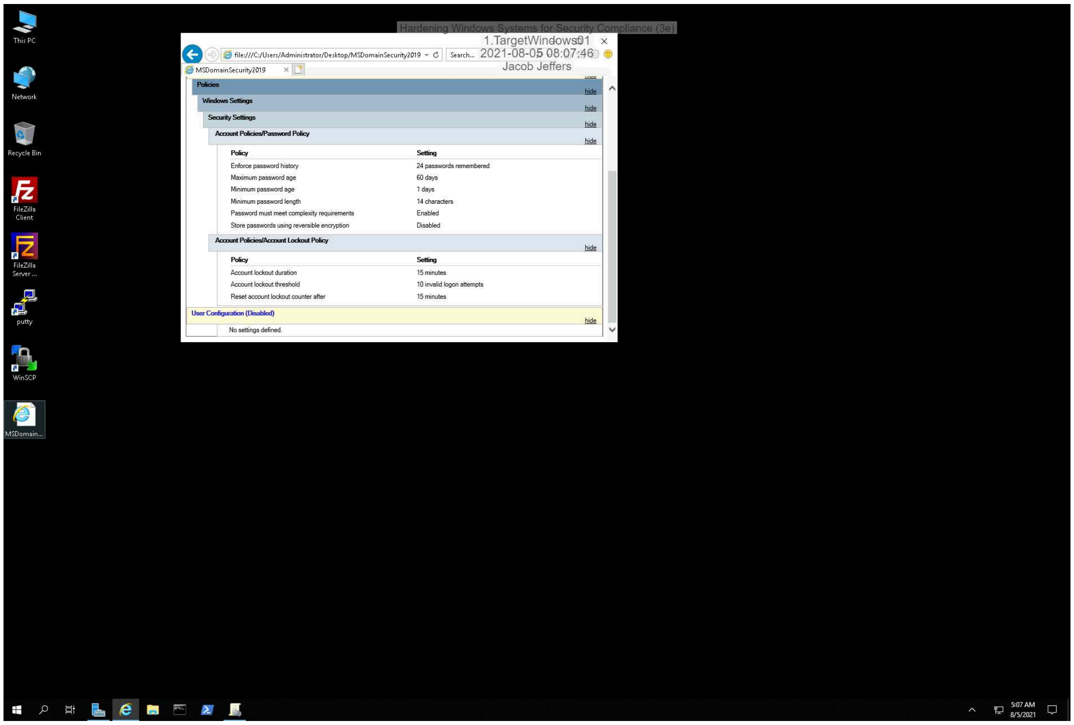


Hardening Windows Systems for Security Compliance (3e)
1.TargetWindows01
2021-08-05 08:06:38
Jacob Jeffers

Group Policy Objects in securelabsondemand.com

Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controller...	Enabled	None	10/13/2017 3:4...	Domai
Default Domain Policy	Enabled	None	11/9/2017 1:57:...	Domai
MSDomainSecurity2019	User configuration s...	None	8/5/2021 5:05:5...	Domai

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



Hardening Windows Systems for Security Compliance (3e)
1.TargetWindows01
2021-08-05 08:07:46
Jacob Jeffers

file:///C:/Users/Administrator/Desktop/MSDomainSecurity2019

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

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

Account Policies/Account Lockout Policy

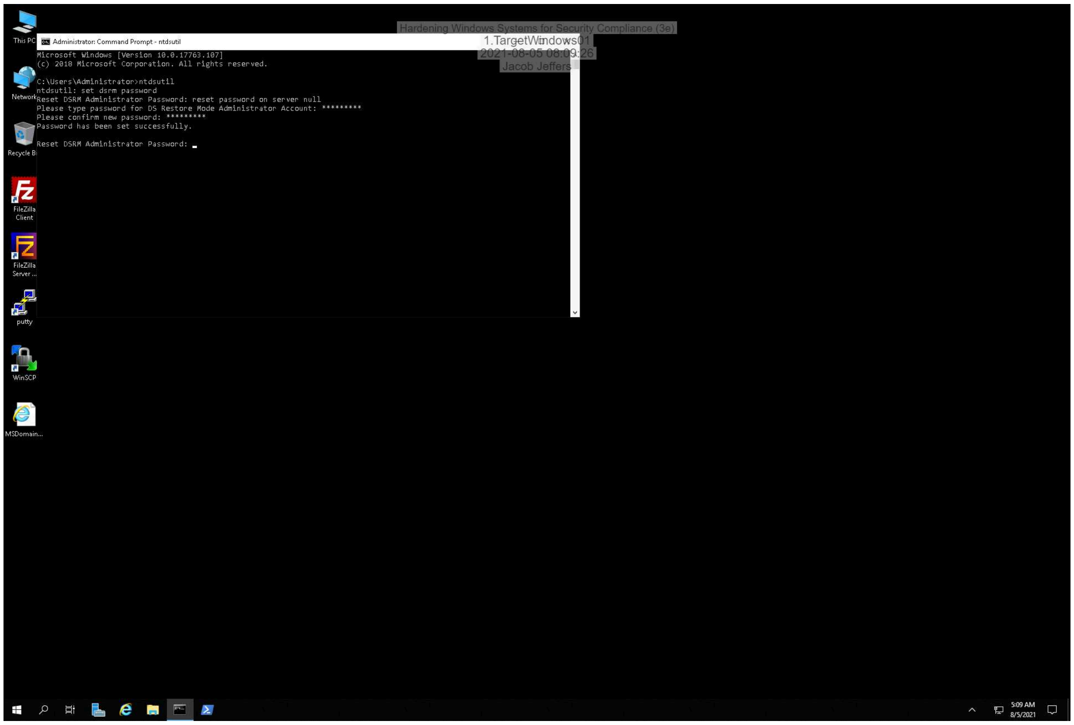
Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

User Configuration (Disabled)

No settings defined.

Part 2: Reset the DSRM Password

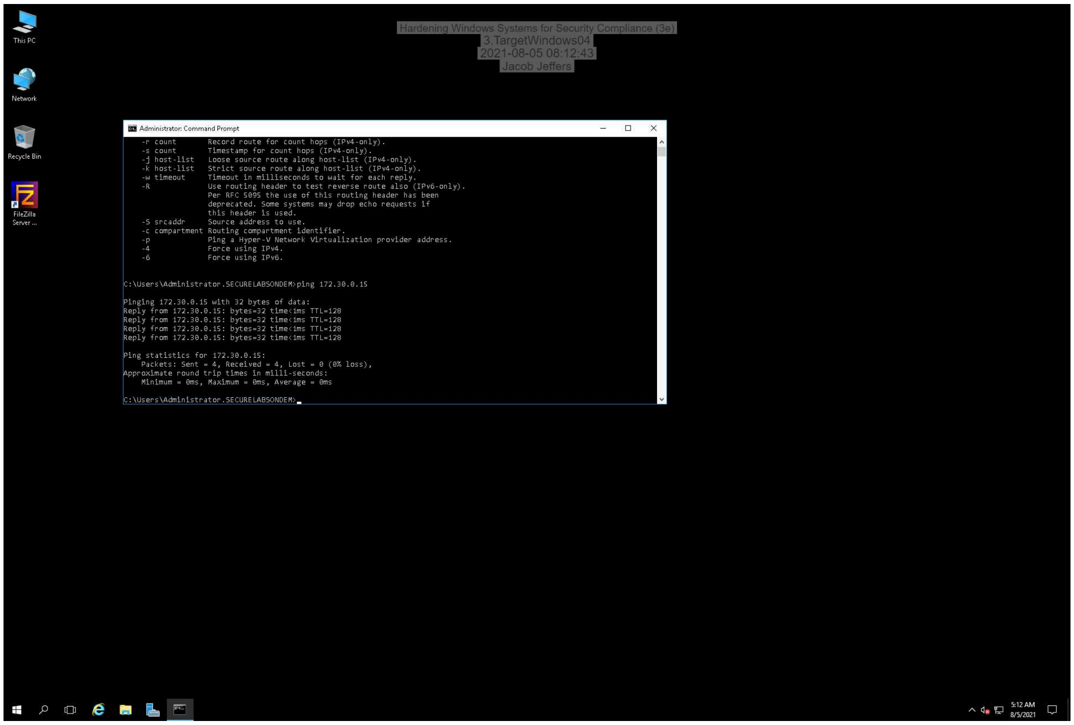
7. **Make a screen capture** showing the **successful DSRM password change**.



```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ntdsutil
ntdsutil: set dsrm password
Reset DSRM Administrator Password: reset password on server null
Please type password for DS Restore Mode Administrator Account: *********
Please confirm new password: *********
Password has been set successfully.

Reset DSRM Administrator Password: _
```

Part 3: Secure the Windows Defender Firewall

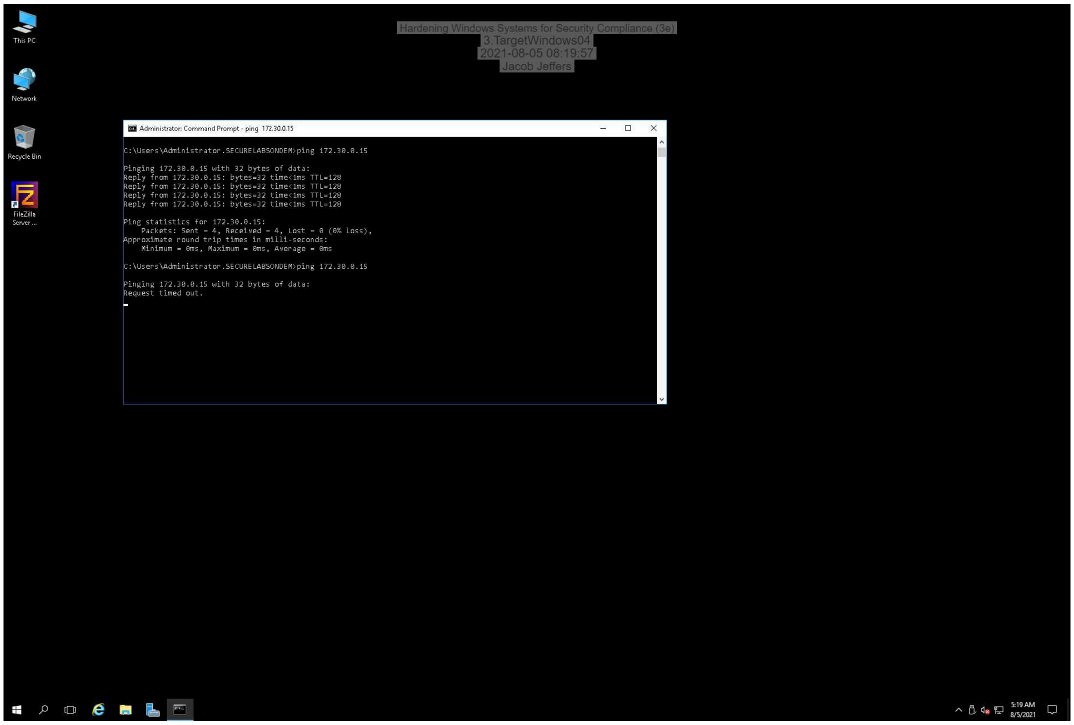
4. **Make a screen capture** showing the **results of the first ping test on TargetWindows04**.



Hardening Windows Systems for Security Compliance (3e)
3.TargetWindows04
2021-08-05 08:12:43
Jacob Jeffers

```
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.


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
Reply from 172.30.0.15: bytes=32 time<1ms TTL=128
Reply from 172.30.0.15: bytes=32 time<1ms TTL=128
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**.



Hardening Windows Systems for Security Compliance (3e)
3.TargetWindows04
2021-08-05 08:19:57
Jacob Jeffers

```
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
Reply from 172.30.0.15: bytes=32 time<1ms TTL=128
Reply from 172.30.0.15: bytes=32 time<1ms TTL=128
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

Pinging 172.30.0.15 with 32 bytes of data:
Request timed out.
```

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

By doing it this way, we ensured that the remote connections in the virtual lab will not be blocked. We disabled the rules that permit ICMP traffic; therefore, we ensured that all ICMP requests were blocked by default. Activating the firewall simply blocked the ICMP traffic from reaching TargetWindows01.

Section 3: Challenge and Analysis

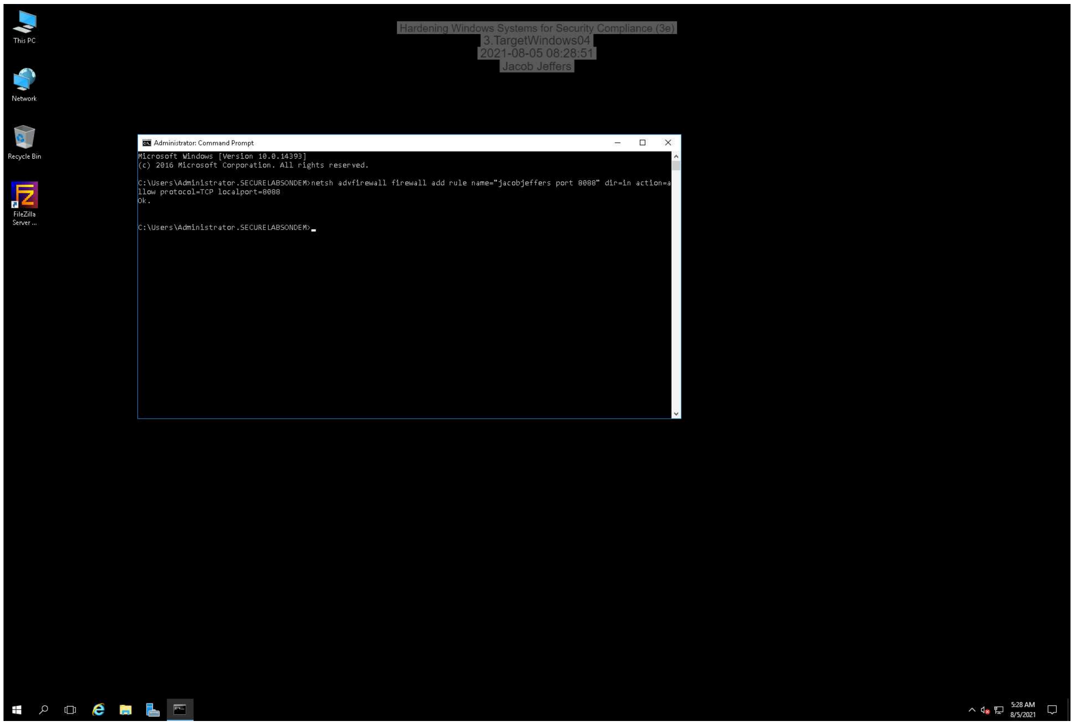
Part 1: Analysis and Discussion

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

Disabling services is able to prevent many attacks, and it optimizes the server for performance. For example, a DDoS utilizing the ping function is now blocked due just by making a small change to the rules. The server now utilizes the roles it needs too, thus optimizing it.

Part 2: Tools and Commands

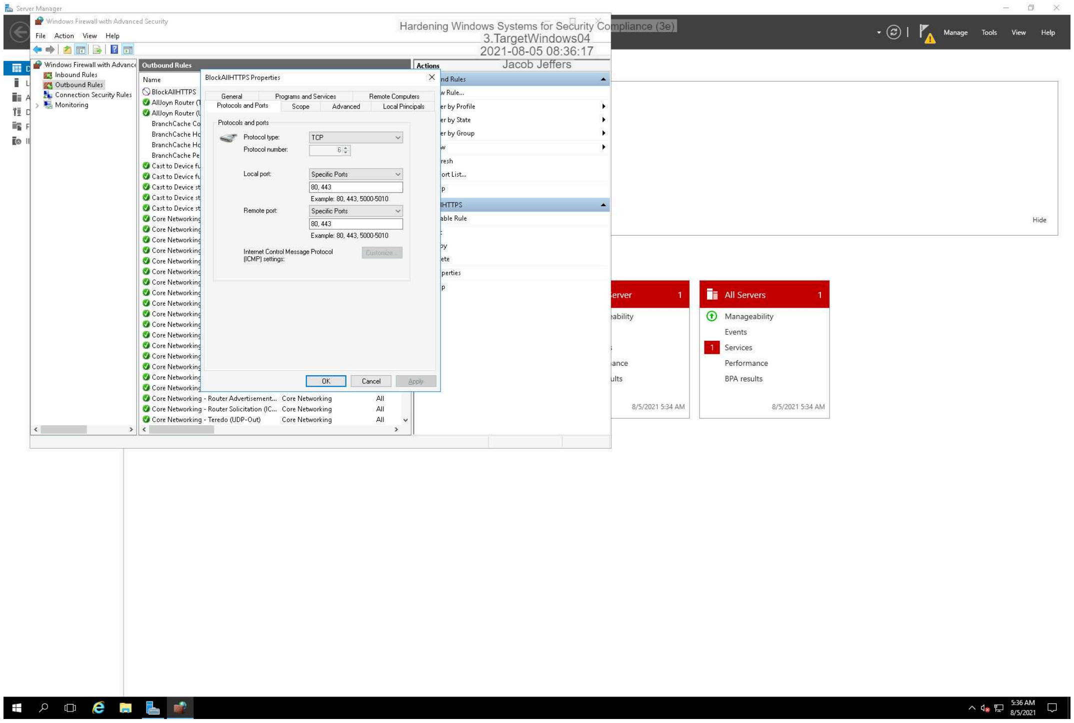
Make a screen capture showing your **executed command line statement**.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.SECURELABSONDEM>netsh advfirewall firewall add rule name="jacobjeffers port 8088" dir=in action=a
llow protocol=TCP localport=8088
Ok.


C:\Users\Administrator.SECURELABSONDEM>
```

Part 3: Challenge Exercise

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


Server Manager
Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanced Security
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules
Name
BlockAllHTTPS
Core Networking - Router Advertisement... Core Networking All
Core Networking - Router Solicitation (IC... Core Networking All
Core Networking - Teredo (UDP-Out) Core Networking All
Actions
Manage Tools View Help
All Servers 1
Manageability
Events
Services
Performance
BPA results
8/5/2021 5:34 AM
Hide
5:36 AM
8/5/2021

Hardening Windows Systems for Security Compliance (3e)
3.TargetWindows04
2021-08-05 08:36:17
Jacob Jeffers

BlockAllHTTPS Properties

General | Programs and Services | Remote Computers | Protocols and Ports | Scope | Advanced | Local Principals

Protocols and ports

Protocol type: TCP

Protocol number: 6

Local port: Specific Ports

80, 443

Example: 80, 443, 5000-5010

Remote port: Specific Ports

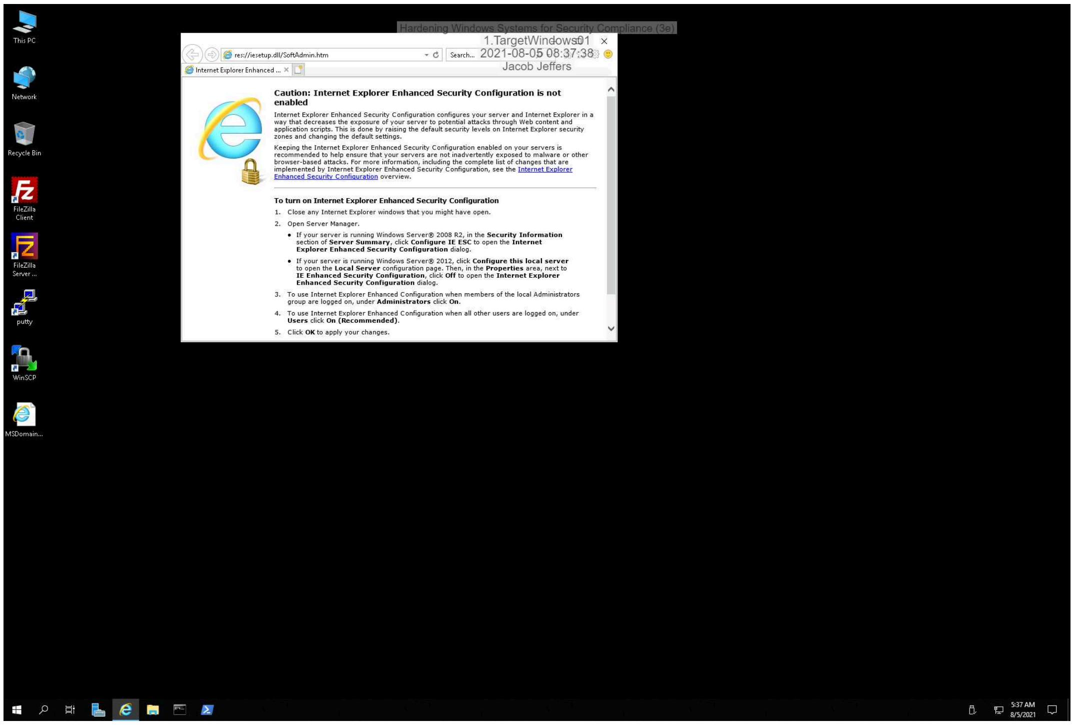
80, 443

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings: Customize...

OK Cancel Apply

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



Hardening Windows Systems for Security Compliance (3e)
1.TargetWindows01
2021-08-05 08:37:38
Jacob Jeffers

res://iesetup.dll/SoftAdmin.htm

Caution: Internet Explorer Enhanced Security Configuration is not enabled

Internet Explorer Enhanced Security Configuration configures your server and Internet Explorer in a way that decreases the exposure of your server to potential attacks through Web content and application scripts. This is done by raising the default security levels on Internet Explorer security zones and changing the default settings.

Keeping the Internet Explorer Enhanced Security Configuration enabled on your servers is recommended to help ensure that your servers are not inadvertently exposed to malware or other browser-based attacks. For more information, including the complete list of changes that are implemented by Internet Explorer Enhanced Security Configuration, see the Internet Explorer Enhanced Security Configuration overview.

To turn on Internet Explorer Enhanced Security Configuration

1. Close any Internet Explorer windows that you might have open.
2. Open Server Manager.
   - If your server is running Windows Server® 2008 R2, in the **Security Information** section of **Server Summary**, click **Configure IE ESC** to open the **Internet Explorer Enhanced Security Configuration** dialog.
   - If your server is running Windows Server® 2012, click **Configure this local server** to open the **Local Server** configuration page. Then, in the **Properties** area, next to **IE Enhanced Security Configuration**, click **Off** to open the **Internet Explorer Enhanced Security Configuration** dialog.
3. To use Internet Explorer Enhanced Configuration when members of the local Administrators group are logged on, under **Administrators** click **On**.
4. To use Internet Explorer Enhanced Configuration when all other users are logged on, under **Users** click **On (Recommended)**.
5. Click **OK** to apply your changes.