SECTION 1: Hands-On Demonstration

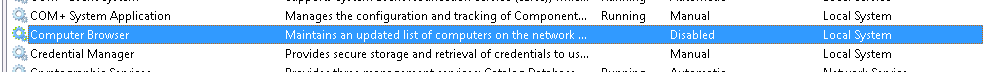
Part 1. Create a Security Policy

Part 2. Disable Unnecessary Services

1. describe the service you selected and explain your rationale for doing so:

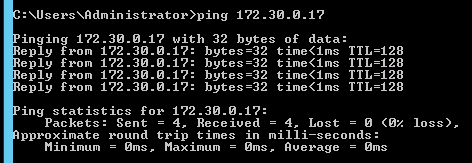
I selected “Computer Browser” because the table shows that disabled is the safest mode for this service.

2. The disabled service in the Services window (screen capture):

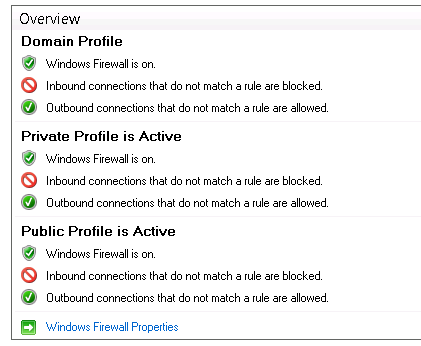


Part 3. Secure the Windows Firewall

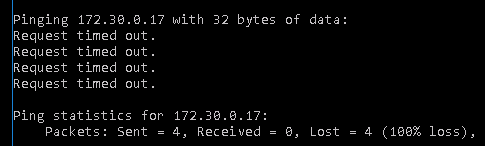
1. results of the Ping test from TargetWindows01b (screen capture):

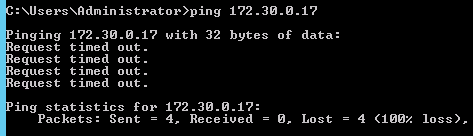


2. the Windows Firewall has been enabled for all profiles (screen capture):



3. results of the Ping test from the vWorkstation (screen capture):

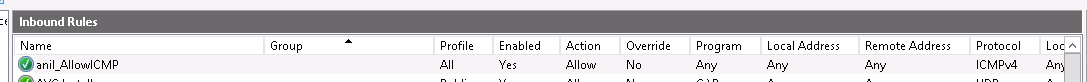




4. discuss how, if at all, the firewall changes affected the results:

The fireball is able to stop network communication to certain types of sources. We disabled them all. This prevented our oings requests from working.

5. *yourname*\_AllowICMP rule (screen capture):



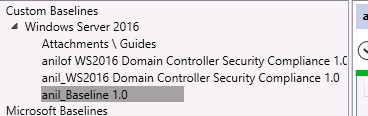
6. describe how the additional firewall changes affected the results:

The latest changess we made to the firewall rules allowed us to send our ping request again.

SECTION 2: Applied Learning

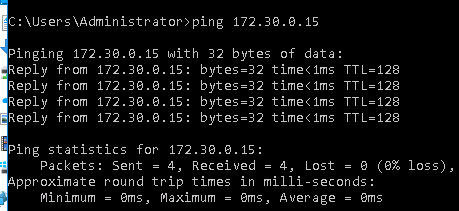
Part 1. Change Security Compliance Baseline on Windows 2016

1. *yourname*\_Baseline settings in the center pane of the SCM (screen capture):

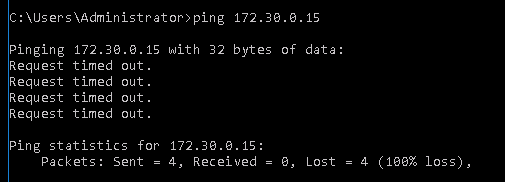


**Part 2. Enable Windows 2016 Firewall**

1. the Ping results (screen capture)



2. discuss how the firewall changes affected the results:



SECTION 3: Observation Summary

We use an executable batch script to prepare the environment for the lab. We use RDP to connect to machine2. We run the SCW from server manager and install remote desktop.

We then choose an unnecessary service to disable and RDP into machine1 and disable the service.

We ping 172.30.0.17 from both other computers to see that we can access it. Then we connect to 2b and turn firewall on. Then we ping 2b from both other machines again. And our requests time out.

We run the batch file to get the environment ready for the lab. We then RDP into machine1. We launch the microsoft security compliance manager and change security settings for notepad. Then we turn on firewall and observe that we cant ping it anymore.