**Lab Exercises**

**Activity 1.1: Create an Inbound Firewall Rule**

In this lab, you will verify that the Windows Defender Firewall is enabled on a server and then create an inbound firewall rule that blocks file and printer sharing.

These lab instructions were written to run on a system running Windows Server 2022. The process for working on other versions of Windows Server is quite similar, although the exact names of services, options, and icons may differ slightly.

 You should perform this lab on a test system. Enabling file and printer sharing on a production system may have undesired consequences. The easiest way to get access to a Windows Server 2022 system is to create an inexpensive cloud instance through Amazon Web Services (AWS) or Microsoft Azure.

**Part 1: Verify that Windows Defender Firewall is enabled**

1. Open Control Panel for your Windows Server.
2. Choose System and Security.
3. Under Windows Defender Firewall, click Check Firewall Status.
4. Verify that the Windows Defender Firewall state is set to On for Private networks. If it is not on, enable the firewall by using the “Turn Windows Defender Firewall on or off” link on the left side of the window.

**Part 2: Create an inbound firewall rule that allows file and printer sharing**

1. On the left side of the Windows Defender Firewall Control Panel, click “Allow an app or feature through Windows Defender Firewall.”
2. Scroll down the list of applications and find File and Printer Sharing.
3. Check the box to the left of that entry to block connections related to File and Printer Sharing.
4. Confirm that the Private box to the right of that option was automatically selected. This allows File and Printer Sharing only for other systems on the same local network. The box for public access should be unchecked, specifying that remote systems are not able to access this feature.
5. Click OK to apply the setting.

**Activity 1.2: Create a Group Policy Object**

In this lab, you will create a Group Policy Object and edit its contents to enforce an organization's password policy.

These lab instructions were written to run on a system running Windows Server 2022. The process for working on other versions of Windows Server is quite similar, although the exact names of services, options, and icons may differ slightly. To complete this lab, your Windows Server must be configured as a domain controller.

1. Open the Group Policy Management application. (If you do not find this application on your Windows Server, it is likely that it is not configured as a domain controller.)
2. Expand the folder corresponding to your Active Directory forest.
3. Expand the Domains folder.
4. Expand the folder corresponding to your domain.
5. Right-click the Group Policy Objects folder and select New from the pop-up menu.
6. Name your new GPO **Password Policy** and click OK.
7. Click the Group Policy Objects folder.
8. Right-click the new Password Policy GPO and select Edit from the pop-up menu.
9. When Group Policy Management Editor opens, expand the Policies folder under the Computer Configuration section.
10. Expand the Windows Settings folder.
11. Expand the Security Settings folder.
12. Expand the Account Policies folder.
13. Click Password Policy.
14. Double-click Maximum Password Age.
15. In the pop-up window, select the Define This Policy Setting check box and set the expiration value to 90 days.
16. Click OK to close the window.
17. Click OK to accept the suggested change to the minimum password age.
18. Double-click the Minimum Password Length option.
19. As in the prior step, click the box to define the policy setting and set the minimum password length to 12 characters.
20. Click OK to close the window.
21. Double-click the Password Must Meet Complexity Requirements option.
22. Click the box to define the policy setting and change the value to Enabled.
23. Click OK to close the window.
24. Click the X to exit Group Policy Management Editor.

You have now successfully created a Group Policy Object that enforces the organization's password policy. You can apply this GPO to users and/or groups as needed.

**Activity 1.3: Write a Penetration Testing Plan**

For this activity, you will design a penetration testing plan for a test against an organization of your choosing. If you are employed, you may choose to use your employer's network. If you are a student, you may choose to create a plan for a penetration test of your school. Otherwise, you may choose any organization, real or fictitious, of your choice.

Your penetration testing plan should cover the three main criteria required before initiating any penetration test:

* Timing
* Scope
* Authorization

One word of warning: You should not conduct a penetration test without permission of the network owner. This assignment only asks you to design the test on paper.