Security Best Practices Server 2019

This lab will teach you the basic steps to locally secure a server and demonstrate how vulnerable a server can be if it can be accessed by unauthorized personnel. Server security needs to be configured differently depending on the role of the server. A server functioning as a web server needs to have the IIS service enabled, but it would be a mistake to enable the IIS service for a file or print server. Why? Because the attack surface of the OS is much greater and opens more potential vulnerabilities.

*Perform this lab on **Server2 VM** because we require DNS and Active Directory.*

Instructions:

Assume you have the responsibility to “harden” or secure a company’s domain controller. What would you do? Hardening a server involves the following steps:

1. Secure the server with good physical security
2. Create a Decoy administrative account and rename the true Administrator account
3. Disable unnecessary applications and services
4. Limit remote administration to specific users
5. Set Disk Quotas and Create Large File on AD volume
6. Create a security baseline using Security Configuration Wizard (SCW)
7. Create a Group Policy Object for the Domain
8. Configure the Windows Firewall
9. Download the latest patches for OS and applications
10. Test the system using Microsoft Baseline Security Analyzer (MBSA)

1. Configure good physical security for the server

We can’t demonstrate physical security in this lab, but you need to know what it involves. Physical security is extremely important because many administrative tools can be used as hacker tools. Anyone with such tools and a minimal skill level can hack a server in a matter of minutes once they have physical access to the machine. You will hack your server to see how easy it is. To prevent this intrusion the server must be in a secure area. There must also be a record of whom and when the server room was entered. At Seneca, for example, the administrators responsible for a server have a key to unlock the door, plus there is an access card reader which records when the room was entered and who entered it.

In addition, electrical access panel and wiring closets must also be secure.It makes no sense to have a secure server room, if an unauthorized person can tap into the network or turn off the power to the server.

2. Create a Decoy administrative account and rename the true Administrator account

During the installation of the 2019 server, by default, local user accounts are automatically created: the **Administrator, and Guest**. The administrator account is the hacker's "holy grail" because of its high privilege. As a security best practice, the administrator account should be renamed from its default name; this would make it more difficult for an attackers to find the administrative account should they gain access locally or remotely. Don't rename the account. "topdog", or "GOD" (for obvious reasons). Rather use a made up name that conforms to the user name policy of the company. Also, the account description needs to be changed as well to hide the fact that this is an administrative account. In this way, no one, except the actual administrator knows which account is the true administrative account. For increased security, a decoy administrative account should be created which has only user rights. If a hacker does gain access he/she will spend time cracking an account with limited privilege. Lastly, the Guest accountshould be disabled at all times because it allows anyone to log onto the system, even if they do not have an account.

Exercise 1: To create an account with administrative privileges and rename the default Administrator account

1. Log on with your Domain Administrator account, and then open Active Directory Users and Computers.
2. Create a NEW user account for a user named **Martin Sanchez**. The user name will be **msanchez** and then fill in the **First Name, Last name** and **Display name** appropriately. Set the password to **P@ssw0rd**. Ensure that you do not have to change the password when you login.
3. Add this user to the **Domain Admins** group. This will make Martin Sanchez a Domain Administrator account.
4. It is also a good idea to change the desktop background to a unique color so you know when you are using the administrative account. Change the desktop background to a different color. To do this, logout from the **Administrator** account and login as **msanchez**. Change the desktop colour. Stay logged in as **msanchez** because this is the new administrator account.
5. Now, we are going to rename the built-in Administrator account. Right-click the **Administrator** account and select **Rename**. Rename the account to **brobertson**.
6. Open the **Properties** dialog box, make the following changes:
   - change the **Full name, First name, Last name, Display name,** to **Bobby Robertson**
   - click **OK**.

Exercise 2: To create a decoy Administrator account

1. Ensure you are still logged in with Domain Admin credentials (**msanchez**), and then open Active Directory Users and Computers.
2. In the console tree, right-click the **Users** container, click **New**, and then click **User.**
3. Type the following information:
   - In **First name** and **User logon name**, type **Administrator**
   - Type and confirm **P@ssw0rd** as the password
   - Uncheck User must change password at next logon
   - Check User cannot change password and password never expires

   Since this is a decoy account there is no need to manage this account. Your new account appears in the Users container.

4. In the details pane, right-click **Administrator**, and then click **Properties**.
5. On the **General** tab, in the **Description** box, type **Built-in account for administering the computer/domain**, and then click **OK**.
6. Now try to log in to the Server as this new user. Notice that you get an error message because by default regular users cannot logon to the server, unless the right to log on locally is granted to them by and administrator.
7. Log back in as Martin Sanchez and Open Active Directory Domain Users and Computers

You have now hidden the true administrative account and created a decoy account with limited user rights to fool a potential hacker.

IMAGE 1. Take a screen shot of Active Directory Users and Computers. Name the file **SenecaID_ADUC.jpeg** (replace **SenecaID** with your Seneca user name)

3. Disable unnecessary applications and services

The domain controller is an essential part of your network. The number of applications installed on it should set to a minimum. Some applications make use of service backdoors, which can sometimes compromise the overall security of the server, or they operate with a high level of privilege. The Print spooler is one such service. There are countless Trojans that work by replacing the Print Spooler's executable file because it operates as a system-level service. So any Trojan posing as the print spooler can also gain these high-level privileges. To protect your server from such an attack, just prevent the Print Spooler service from running. Since this is a domain controller, there is no need for someone to be working at it so the print spooler is unnecessary.

Many viruses and utilities that are used by attackers are 16-bit applications that expect file names to be compatible with 8.3 automatic name generations. Secure domain controllers do not run 16bit applications locally. Therefore, disable 8.3 automatic name generations to prevent these viruses and utilities from compromising security.

Exercise1: Disabling the Print Spooler Service

1. Open a CLI Window and type **net start.** This is a list of running services. Notice print spooler is running by default.
2. Click on Computer Management**\Services and Applications** tree
3. Double-click on Services in the middle pane
4. Scroll the middle pane to find the Print Spooler service. Click on **Print Spooler**.
5. Notice the Description of the Print Spooler
6. Right-click on Print Spooler and select **Stop**.
7. Type **net start** again and notice the printer service is not running.
8. Leave the Window open.

IMAGE 2. Take a screen shot of the open window. Name the file **SenecaID_SERVICES.jpeg**

4. *Limit remote administration*

It is important for server administrators to be able to remotely access the server in order to solve a problem. However, remote access must be limited to as few individuals as possible because remote access can also be used by a hacker to take control of the server. To minimize the threat Server 2008 users remote desktop with Network Level Authentication (NLA); this form of authentication discourages man-in-the-middle attacks.It is essential that you configure a very strong password for the account which will perform remote administration.

Exercise1: Enabling remote access through Remote Desktop

1. Open Server Manager
2. Click the link for **Configure Remote Desktop.**
3. Select **Allow connections only form computers running Remote Desktop with Network Level Authentication (more secure)**.

4. Click **Apply**. Notice the Windows Firewall will automatically be configured to allow access.
5. Click **OK** to close the Firewall Properties windows
6. Click on the **Select Users** button.
7. Notice the administrator Martin Sanchez automatically has access.
8. Close Server Manager
9. Open Control Panel
10. In the Control Panel Home view, click **Allow a program through Windows Firewall**.
11. Notice the check the boxes for **Remote Desktop** checked
12. Click **OK**

Exercise2: To add users to the Remote Desktop Users group

By default, the Remote Desktop Users group is not populated. You must decide which users and groups should have permission to log on remotely, and then manually add them to the group.

1. Open Domain Users and Computers.
2. Create a new user
3. Add the user to the **Remote Desktop Users** group
4. Open remote desktop and notice that the new user and Martin Sanchez have access to the server.

IMAGE 3. Take a screen shot of the Remote Desktop Dialog box showing the new user. Name the file **SenecaID_REMOTE.jpeg**

5. Set Disk Quotas and Create Large File on AD volume

It is important to set disk quotas for all users because attacks attempt to consume the system resources of the targeted system. One of the commonly attacked system resources is available disk space. Available disk space can be exhausted by the addition of a large number of objects to the directory by a malicious user or administrator. You can delete the added objects, but Active Directory requires that deleted objects continue to exist in the directory as tombstones for an extended period of time to allow the deletion to replicate. Therefore, the disk space that is consumed by the deleted objects cannot be reclaimed until the tombstone lifetime has expired, **which is 60 days by default**.

To reduce the effects of this type of attack, you can create a reserve file on the same disk volume as the Active Directory database (Ntds.dit). A reserve file is simply a large file that takes up available disk space. In the event that an attacker exhausts all disk space by adding a large number of objects to the directory, you can delete the reserve file to quickly restore normal operation until the rogue objects inside Active Directory are identified and removed.

6. Create a security baseline with SCW

Windows server 2019 has a Security Template MMC snap-in that enables you to create a security baseline. A baseline is a collection of configuration settings which serves as a checklist to avoid common misconfigurations which could be taken advantage of by malicious hackers. Using the snap-in you can set local and remote security policy, account policies, auditing, firewall and registry settings.

Exercise1: Using the Security Configuration Wizard

1. Log on as **Martin Sanchez**
2. Open Server Manager and select **Run Security Configuration Wizard**
3. Read the Welcome to the Security Configuration Wizard start up screen. Notice you are creating a security policy based on the role of the computer. It will configure auditing and Windows Firewall and Registry settings.
4. Select to Create a **New Security Policy**
5. Accept the default server name
6. Accept the default server roles. Make sure that Active Directory is checked
7. Accept the default client roles the server performs
8. Under the optional services the server performs check Active Directory – RsoP Planning Mode and Remote Desktop
9. Click **Next twice** to see a summary of the security policy.
10. Click **Next** until you get to the **LDAP Signing window**. Check the box and click **Next**
11. Under the System Audit Policy. Select both successful and Unsuccessful activities
12. Save your Security Policy and Name it **IOS110_DC**
13. **Click Next**
14. **Select to Apply Now**
15. **Click Next**

7. Configure the Windows Firewall

The Windows Firewall is a stateful inspection firewall which is generally regarded as the best compromise between performance and security. Firewalls work by filtering packets and comparing them to a list of instructions called ACLs, Access Control Lists. ACLs are a set of rules which instruct the firewall how to handle inbound and outbound packets.

Exercise1: Configuring the Windows Firewall using MMC Snap-in

1. Click Start, Run and type **mmc** and click **OK**
2. Click the File menu and click **Add/Remove** Snap-in

3. Click ***Windows Firewall with Advanced Security*** and click the **Add** button. In the ***Select Computer*** dialog box, leave *Local computer* (the computer this console is running on) selected and click **Finish**.
4. Click **OK** in the *Add or Remove Snap-in* windows
5. In the tree, double-click *Windows Firewall with advanced Settings on Local computer*
6. Click Inbound Rules in the tree. Notice the inbound rules in the middle pane. These rules have been set based on the role of the server and the security policy you created.
7. A good rule is to block incoming PING requests because this is used by hackers to get the IP addresses of hosts and to see that they are alive
8. Click on **New Rule** in the right pane
9. Click on **Custom** and click **Next**
10. On the New Inbound Rule Wizard leave the **All Programs selected** and click **Next**
11. Use the drop down box to **select ICMPv4** as the Protocol type.
12. Leave *which local IP addresses does this rule apply to* set to **All IP Addresses**. Click **Next**
13. Select ***Block the Connection***. Click **Next**.
14. Leave the **Domain, Private** and **Public** checked networks and Click **Next**.
15. Name the rule ***PING Passive Attack*** and in the Description type ***All inbound Ping requests are blocked.***
16. Click **Outbound Rules** in the tree and examine the outbound rules in the middle pane.

IMAGE 4. Take a screen shot of your in rule. Name the file **SenecaID_RULE.jpeg**

17. Close the Console Window
18. Save **YES** to save the Firewall Snap-in

8. Download the latest patches for the OS and Applications

An important step to harden a server is to download the latest patches for the operating system and any applications that are running on the server. The top 20 vulnerabilities that hackers use to gain access to servers are found in common applications. The version of Server 2008 R2 we installed contains Service Pack 1, but there are many patches and updates since this release was created. However, given the restrictions on the Seneca network, it will take too long to download and install these updates. We will recognize that this is an important step, but bypass it at this time.

9. Testing the System with MBSA

Microsoft Baseline Security Analyzer (**MBSA**) is a software tool released by Microsoft to determine security state by assessing missing security updates and less-secure security settings within Microsoft Windows, Windows components such as Internet Explorer, and IIS web server. Security updates are determined by the current version of MBSA using the Windows Update Agent present on Windows computers. The less-secure settings, often called Vulnerability Assessment (VA) checks, are assessed based on a hard-coded set of registry and file checks. An example of a VA might be that permissions for one of the directories in the /www/root folder of IIS could be set at too low a level, allowing unwanted modification of files from outsiders.

We will not be downloading and running MBSA in the lab.

Your lab is now complete.

For Grading:

Attach the following images in a document/word file and save the file as Lab7-Security.docx and upload to blackboard.

- **SenecaID_ADUC.jpeg**
- **SenecaID_SERVICES.jpeg**
- **SenecaID_REMOTE.jpeg**
- **SenecaID_RULE.jpeg**