CCCCO CySA+ Lab Series

Lab 4: Host Hardening

Document Version: 2019-09-06

Contents

Introduction 3
Objectives 3
Lab Topology 4
Lab Settings 5
1 Navigating the Group Policy Management Center 6
2 Creating New Group Policies 8
3 Securing Unused Ports 20
4 Preparing and Applying Patches 28
5 Using Windows Defender to Increase Security 42

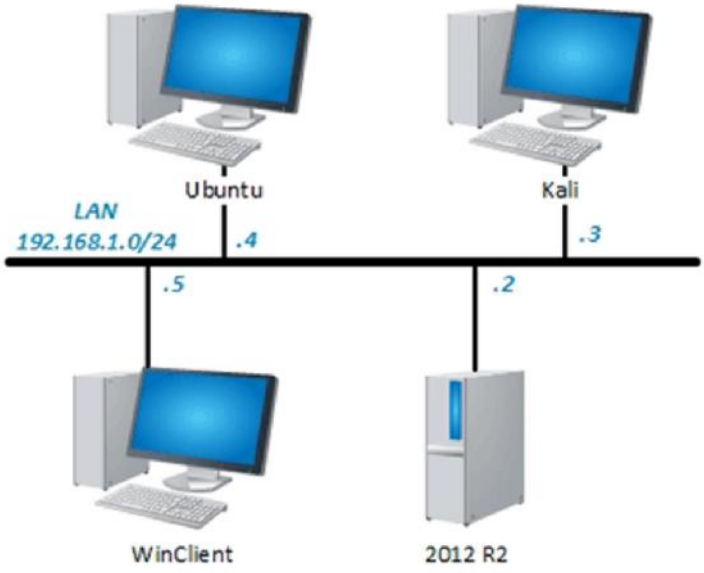
Introduction

In this lab, you will explore various methods for increasing host security. This is known as *hardening*.

Objectives

- Configure various group policies
- Set up an acceptable use splash screen
- Learn how to close unused ports
- Explore manually installing patches
- Use Windows Defender to periodically scan hosts

Lab Topology



Lab Settings

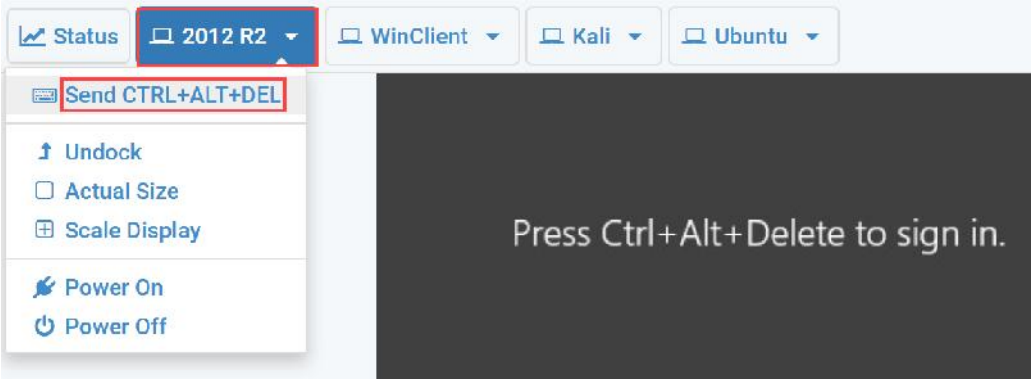
The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account	Password
2012 R2	192.168.1.2	Administrator	Password123
WinClient	192.168.1.5	student	Password123
Kali	192.168.1.3	root	toor
Ubuntu	192.168.1.4	sysadmin	Password123

1 Navigating the Group Policy Management Center

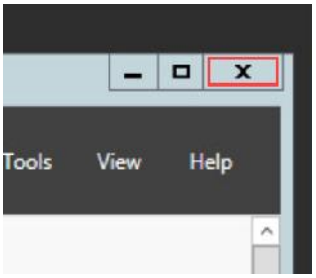
In this task, you will learn how to open the GPMC.

1. Launch the **2012 R2** virtual machine to access the graphical login screen.
2. Bring up the login window by sending a **Ctrl + Alt + Delete**. To do this, click the **2012 R2** drop-down menu and click **Send CTRL+ALT+DEL**.

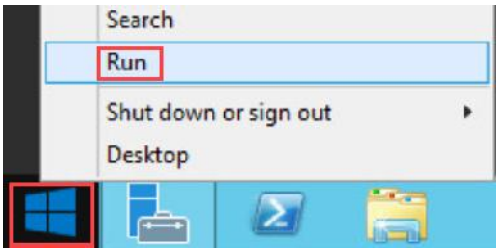


3. Log in as `CySa\Administrator` using the password `Password123`.

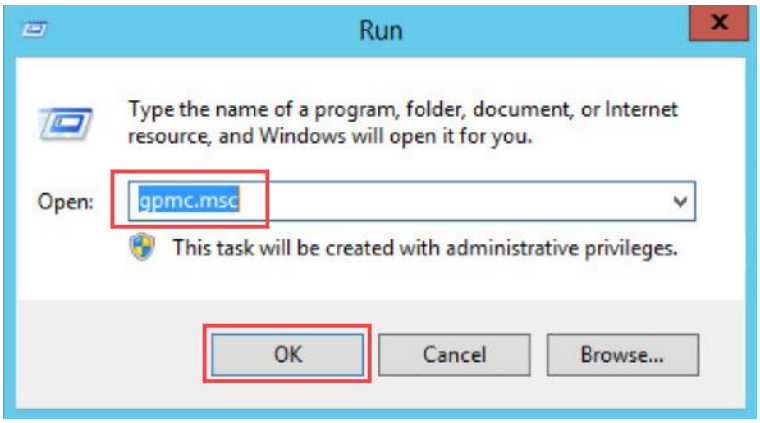
4. Once logged into the virtual machine, close the **Server Manager** by clicking the **x** button in the upper-right.



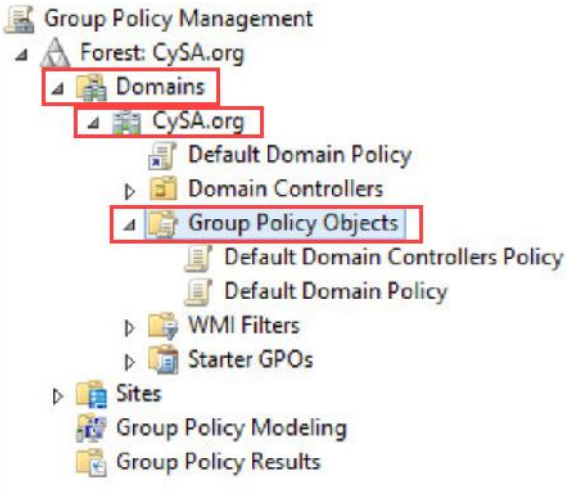
5. In the lower-left of the screen, right-click the **Windows** icon and choose **Run**.



6. When the *run* window appears, type **gpmc.msc** and click **OK**.



7. Expand the trees on the left until you reach **Group Policy Objects**. (Click on **Domains**-> **CySA.org**-> **Group Policy Objects**.)

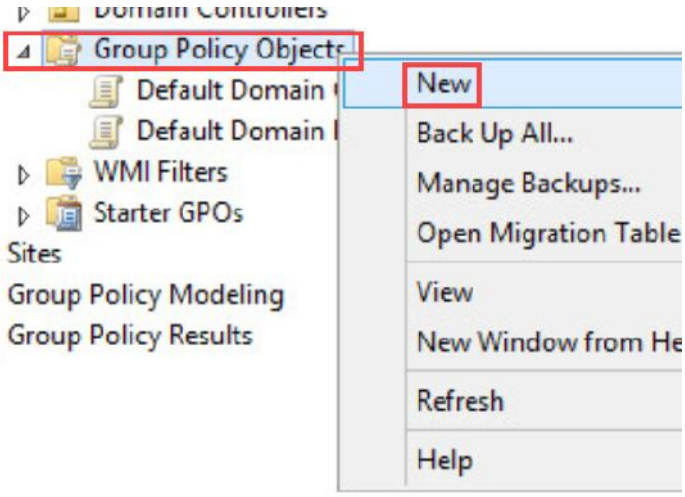


8. Leave this window open for the next task.

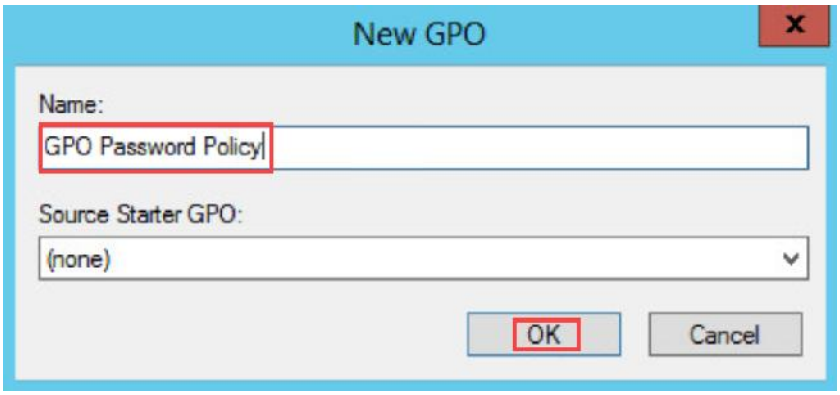
2 Creating New Group Policies

In this task, you will create new group policies pertaining to password rules, as well as setting up an Acceptable Use Policy splash screen.

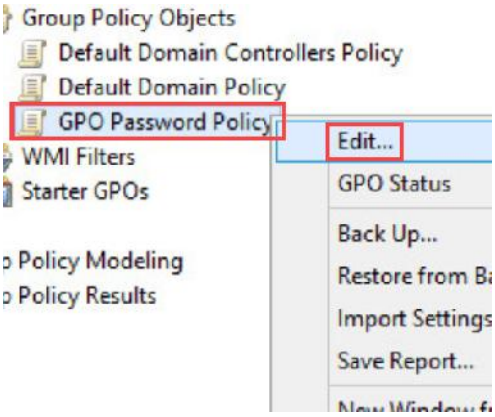
1. In the *Group Policy Management Center*, right-click **Group Policy Objects** and click **New**.



2. Type **GPO Password Policy** into the *Name* field and click **OK**.

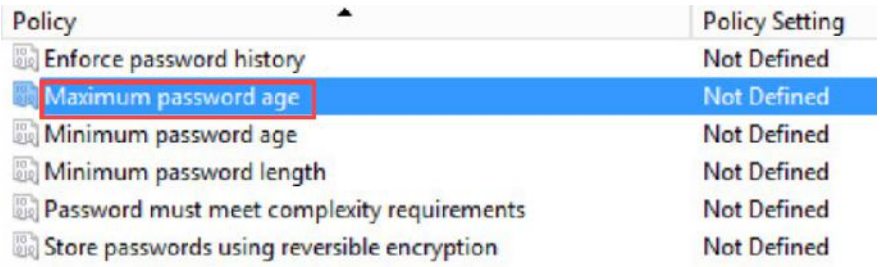


3. Right-click the newly created policy and select **Edit**.

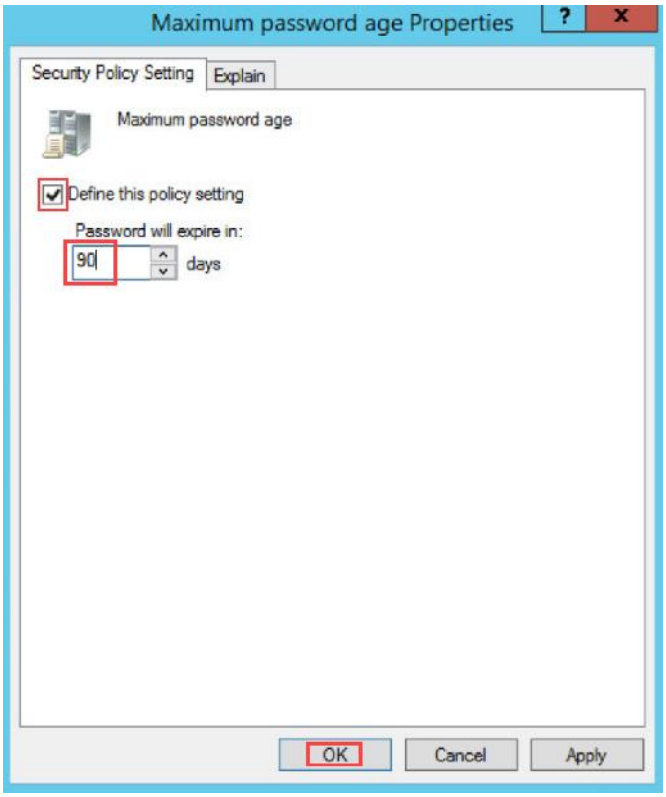


4. Once the *Group Policy Management Editor* opens, navigate to **Computer Configuration**-> **Policies**-> **Windows Settings**-> **Security Settings**-> **Account Policies** and select **Password Policy**.

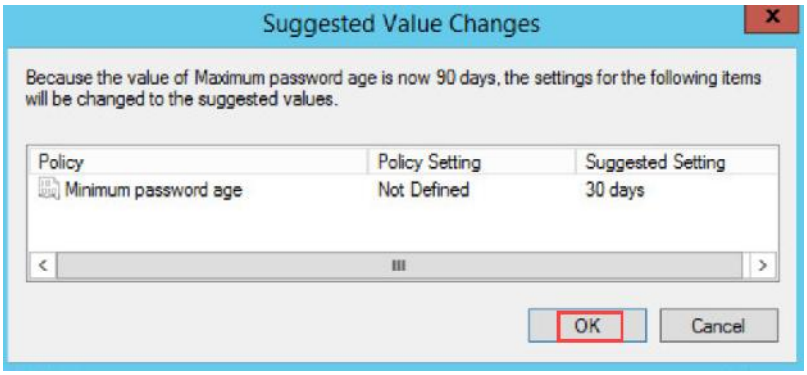
5. Double-click **Maximum Password Age**.



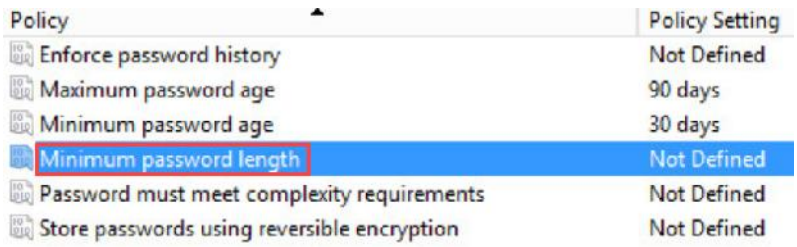
6. In the *Maximum password age Properties* window, place a check in the box that reads **Define this policy setting**. In the box that says **Password will expire in:**, type **90**. Click **OK**.



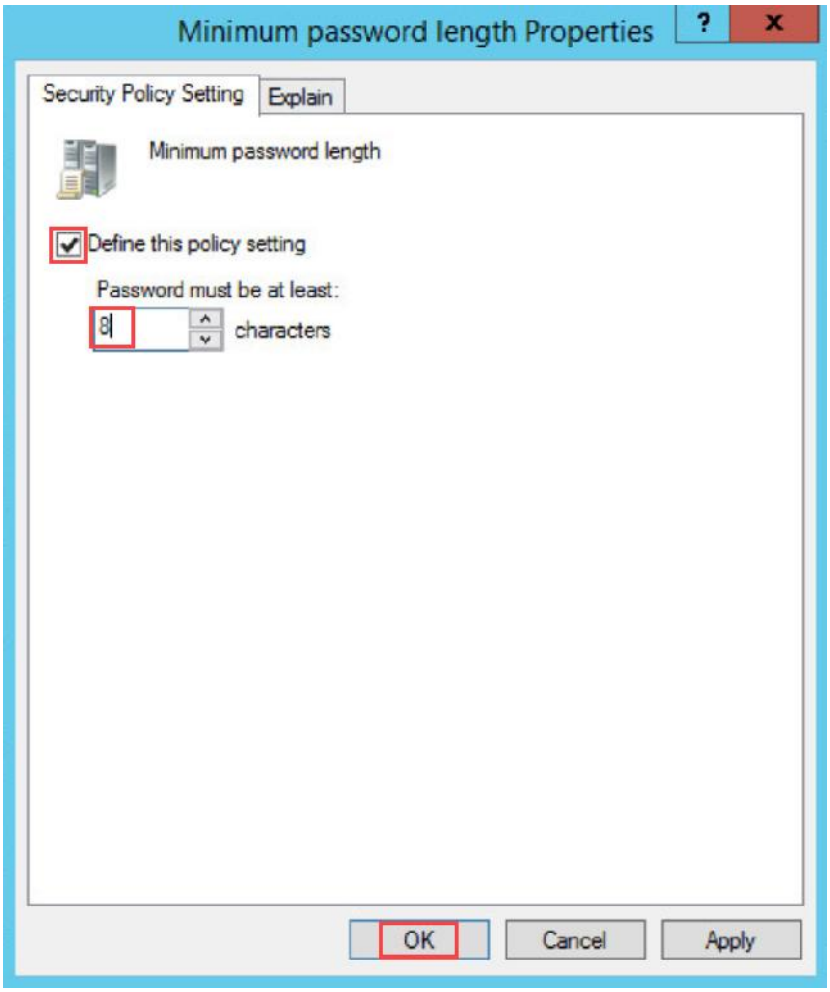
7. When prompted to automatically set a minimum password age, click **OK** to continue.



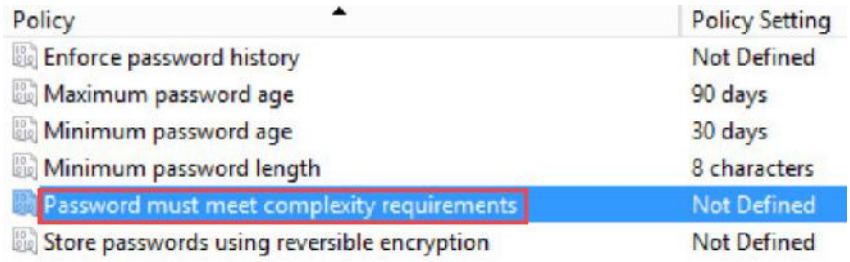
8. Double-click **Minimum Password Length**.



9. In the *Minimum password length Properties* window, place a check in the box that reads **Define this policy setting**. In the box that says **Password must be at least:**, type **8**. Click **OK**.

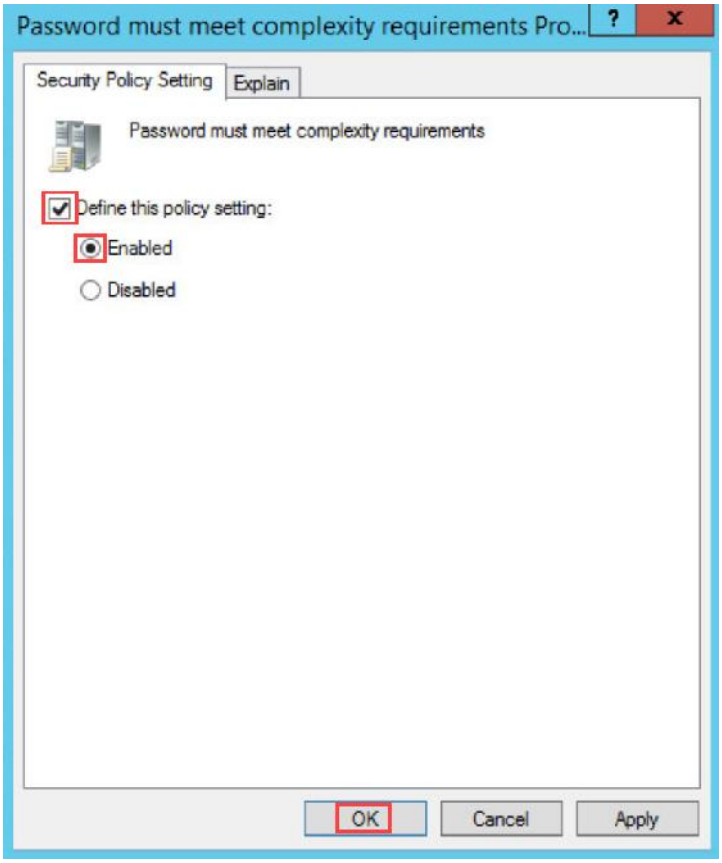


10. Double-click on **Password must meet complexity requirements**.

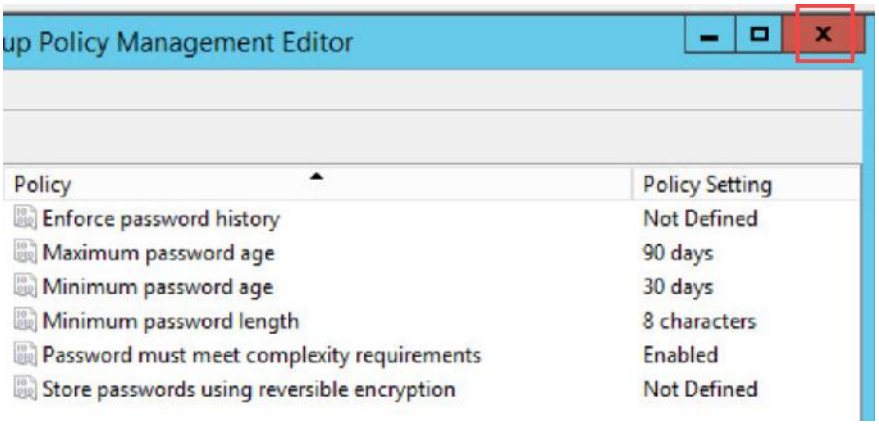


Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	90 days
Minimum password age	30 days
Minimum password length	8 characters
Password must meet complexity requirements	Not Defined
Store passwords using reversible encryption	Not Defined

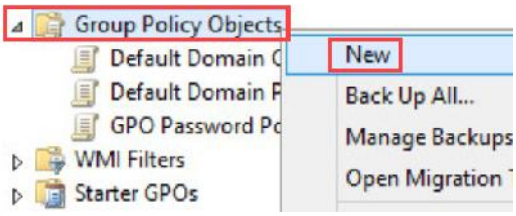
11. In the *Password must meet complexity requirements Properties* window, place a check in the box that reads **Define this policy setting**. Click **Enabled**. Click **OK**.



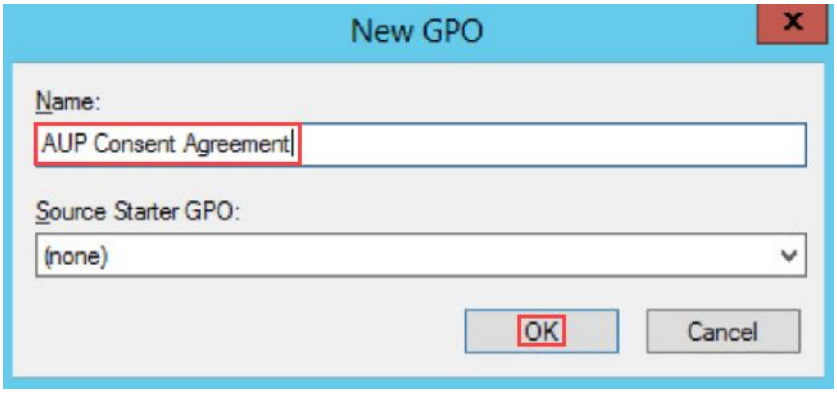
12. Review the policies you just created before closing the **Group Policy Management Editor**.



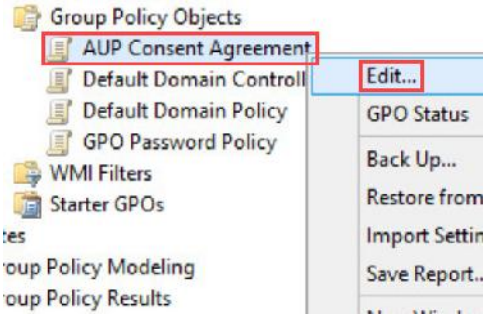
13. To create an *Acceptable Use Policy Consent Agreement*, right-click **Group Policy Objects,** and select **New**.



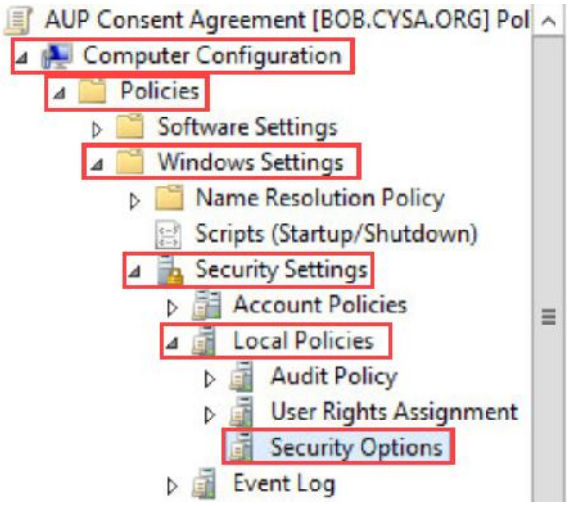
14. In the Name field, type **AUP Consent Agreement** and click **OK**.



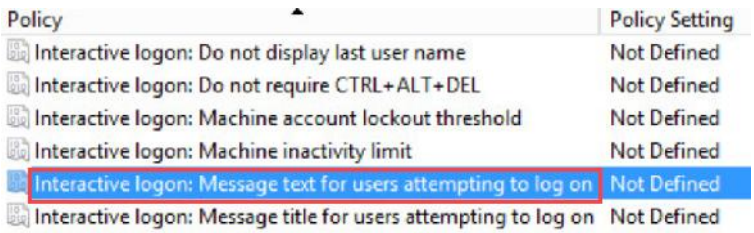
15. Right-click **AUP Consent Agreement** and select **Edit**.



16. In the *Group Policy Management Editor*, navigate to **Computer Configuration**-> **Policies**-> **Windows Settings**-> **Security Settings**-> **Local Policies**-> **Security Options**.

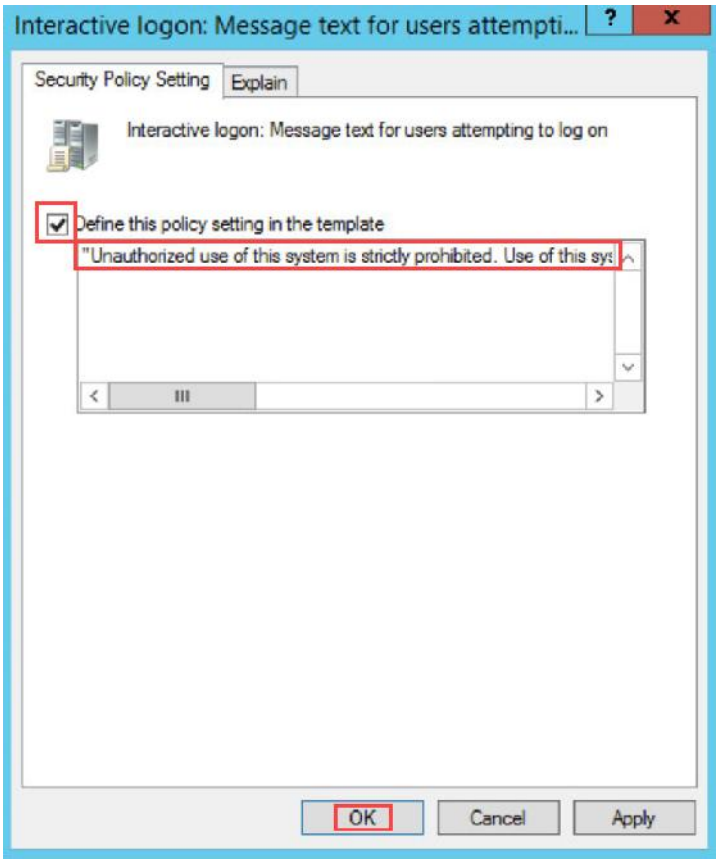


17. In the right pane, scroll down and double-click **Interactive logon: Message text for users attempting to log on**.

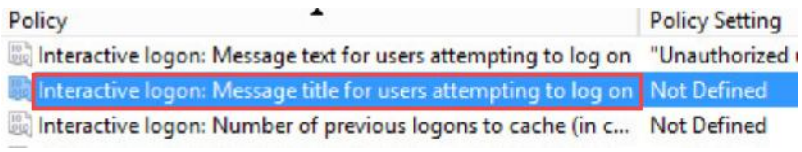


Policy	Policy Setting
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined

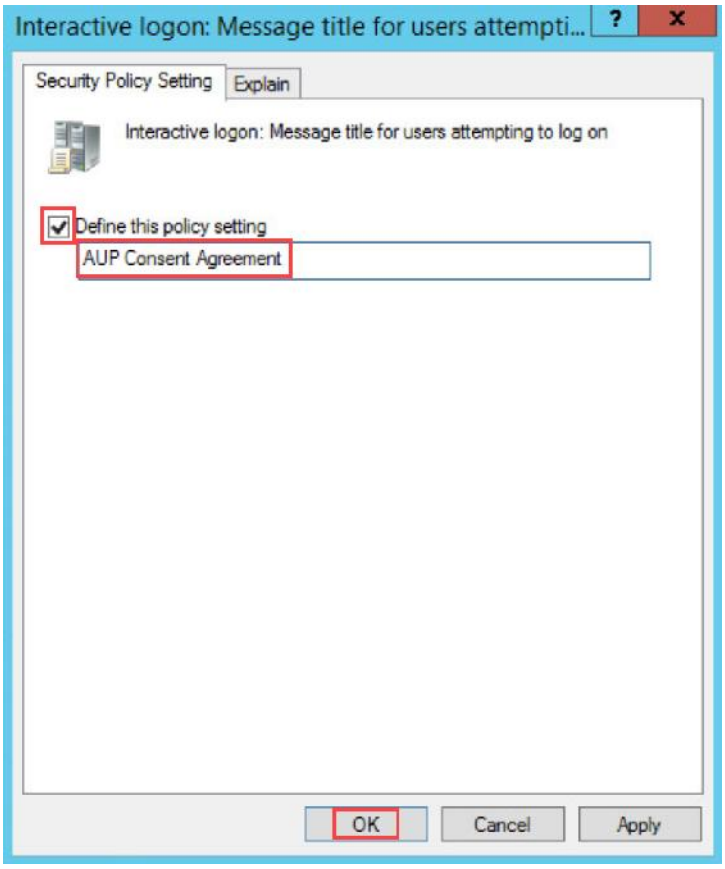
18. In the *Interactive logon: Message text for users attempting to log on Properties* window, place a checkmark in **Define this policy setting in the template**. In the box below, type *"Unauthorized use of this system is strictly prohibited. Use of this system may be monitored for security and legal purposes. By using this system, you agree to comply with the terms outlined in the Acceptable Use Policy."* Click **OK**.



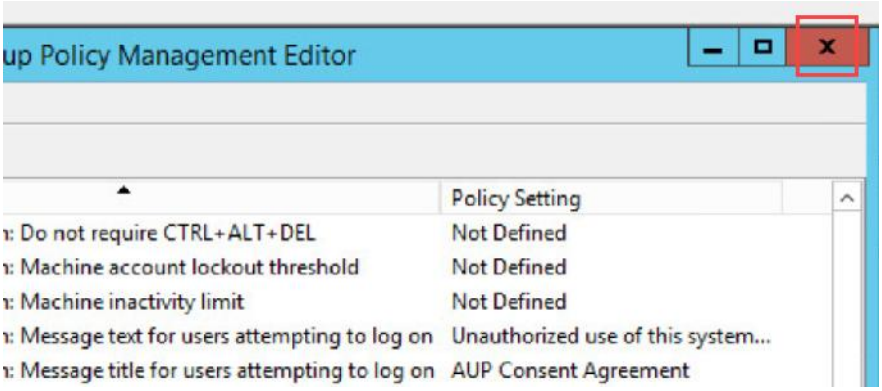
19. In the right pane, double-click **Interactive Logon: Message title for users attempting to log on**.



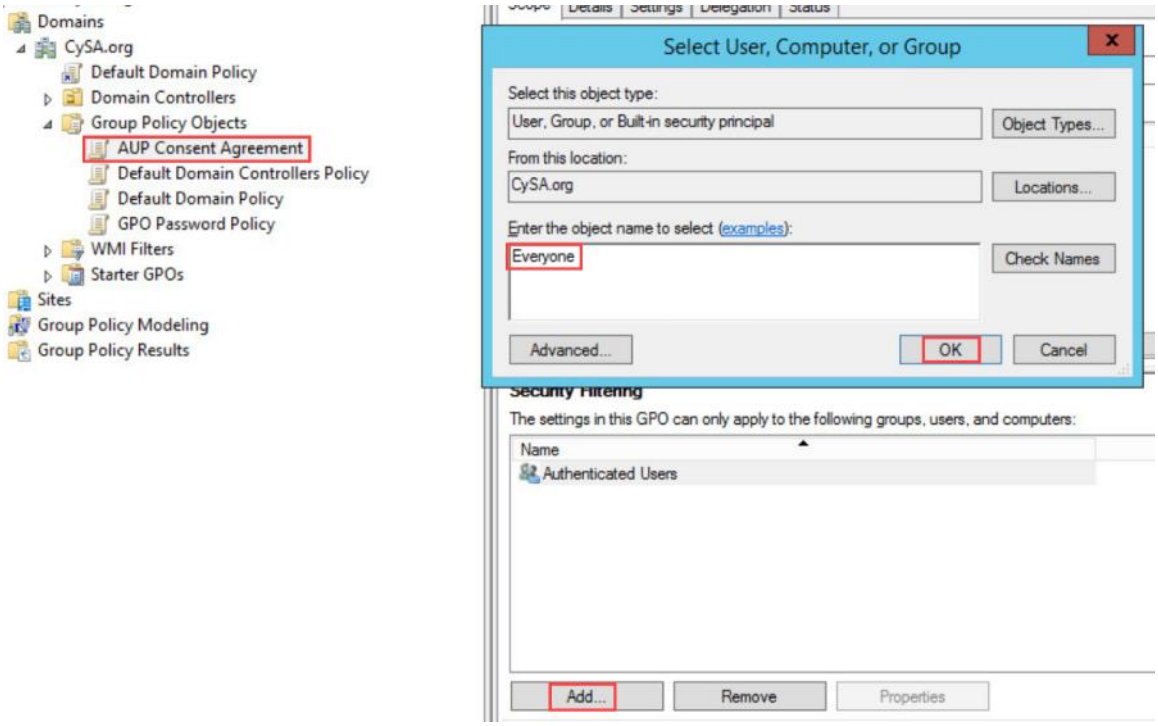
20. In the *Interactive logon: Message title for users attempting to log on Properties* window, place a checkmark in the **Define this policy setting** box. In the box below, type **AUP Consent Agreement**. Click **OK**.



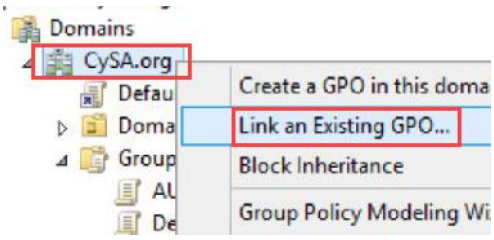
21. Review the settings for the *AUP Consent Agreement* policy you just created before closing the **Group Policy Management Editor**.



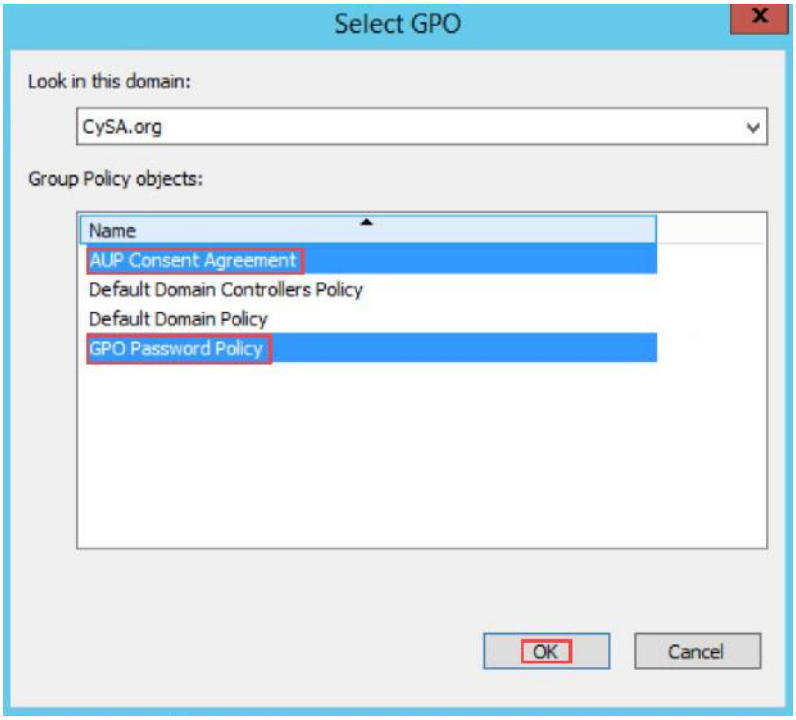
22. In the *Group Policy Management Center*, click on **AUP Consent Agreement**. In the right pane, under the **Scope** tab, click **Add** in the **Security Filtering** section, type **Everyone** in the box and click **OK**.



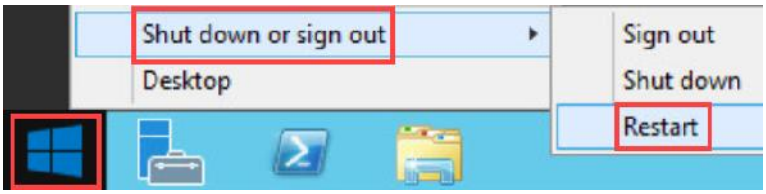
23. Right-click **CySA.org** in the *Group Policy Management Center*. Select **Link an Existing GPO…**



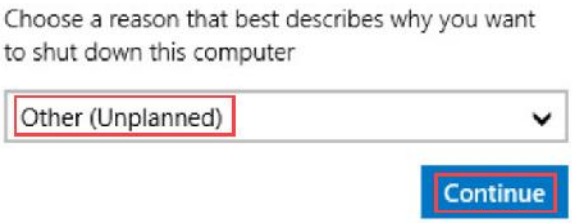
24. Select **AUP Consent Agreement** and **GPO Password Policy** by holding the CTRL button and clicking each one. Once selected, proceed by clicking **OK**.



25. Close all windows to navigate to the desktop. In the taskbar, right-click the **Windows** button-> **Shut down or sign out**-> **Restart**.



26. Choose **Other (Unplanned)** and click **Continue**.

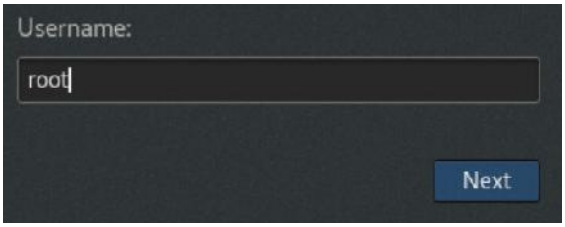


27. Once the computer restarts, you should be met with the *AUP Consent Agreement.* Click **OK** and log in as **`CySa\Administrator`** using the password **`Password123`**. Once logged in, you may close the **Server Manager** window.

3 Securing Unused Ports

In this task, you will explore open ports across the network and various techniques for closing them. In practical application, leaving unnecessary ports open can be a dangerous entry point for intruders and malicious software.

1. Launch the **Kali** virtual machine to access the graphical login screen.
2. Press **ENTER** to bring up the login screen. Log in as **`root`** using the password **`toor`**.



3. Once on the desktop screen, open a **Terminal** window.

4. On the **Terminal** screen, enter the following command to check the **2012 R2** virtual machine for open ports. From the results given, you can see that the **2012 R2** virtual machine has several ports open. For this lab, you will focus on ports 53 and 88, which are used for *DNS* and *Kerberos* authentication, respectively.

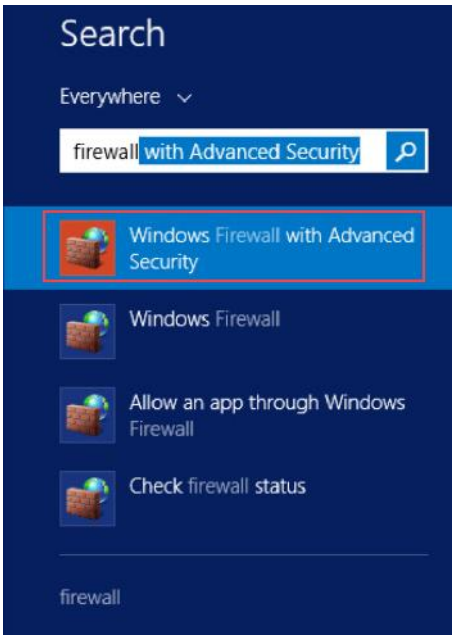
```
root@kali:~# nmap -F 192.168.1.2
```

```
root@kali:~# nmap -F 192.168.1.2

Starting Nmap 7.60 ( https://nmap.org ) at 2019-03-06 08:56 EST
Nmap scan report for 192.168.1.2
Host is up (0.0043s latency).
Not shown: 91 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:50:56:82:D1:CF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds
root@kali:~#
```

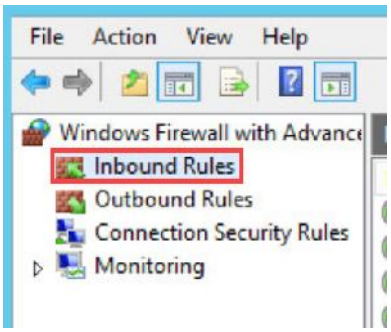
5. Return to the **2012 R2** virtual machine.

6. Click the **Windows** icon in the lower-left to bring up the *Start* menu.

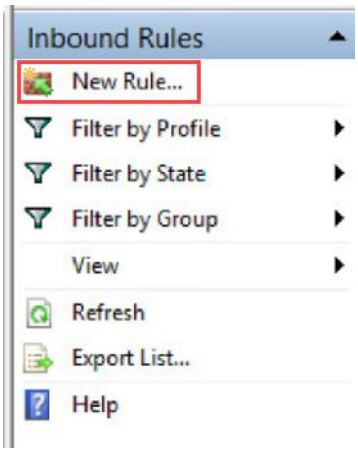
7. Type **Firewall** to bring up a list of options. These options will automatically populate in the search list as you type. Click on **Windows Firewall with Advanced Security**.



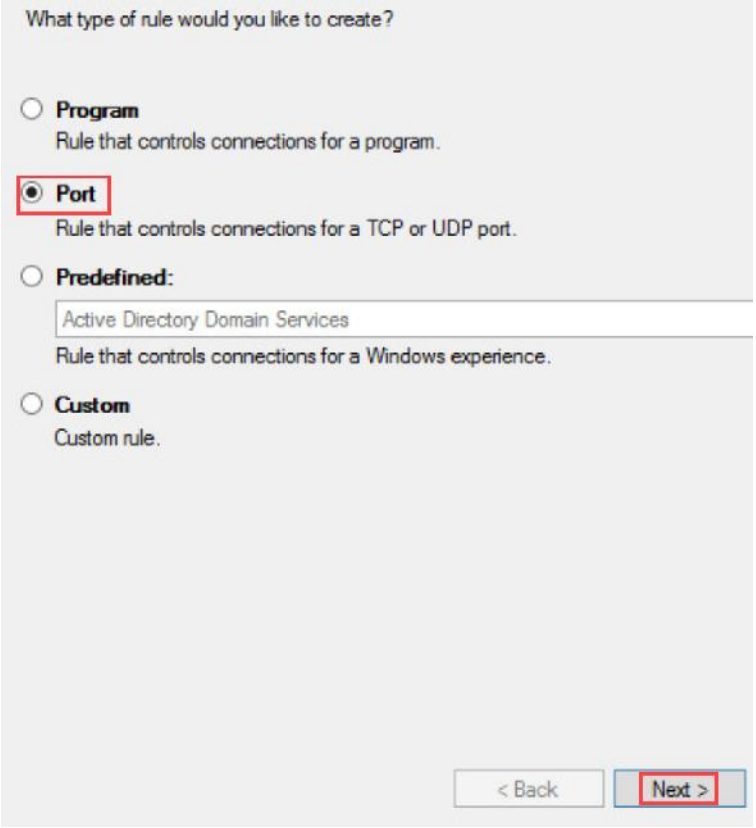
8. Once the *Windows Firewall with Advanced Security* window loads, click on **Inbound Rules** in the left pane.



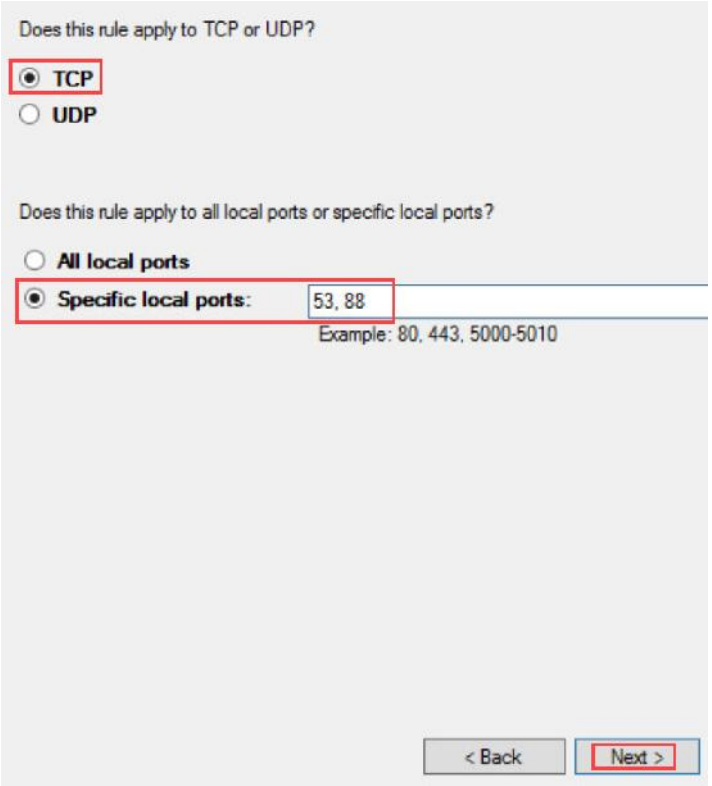
9. Click on **New Rule…** in the far-right pane.



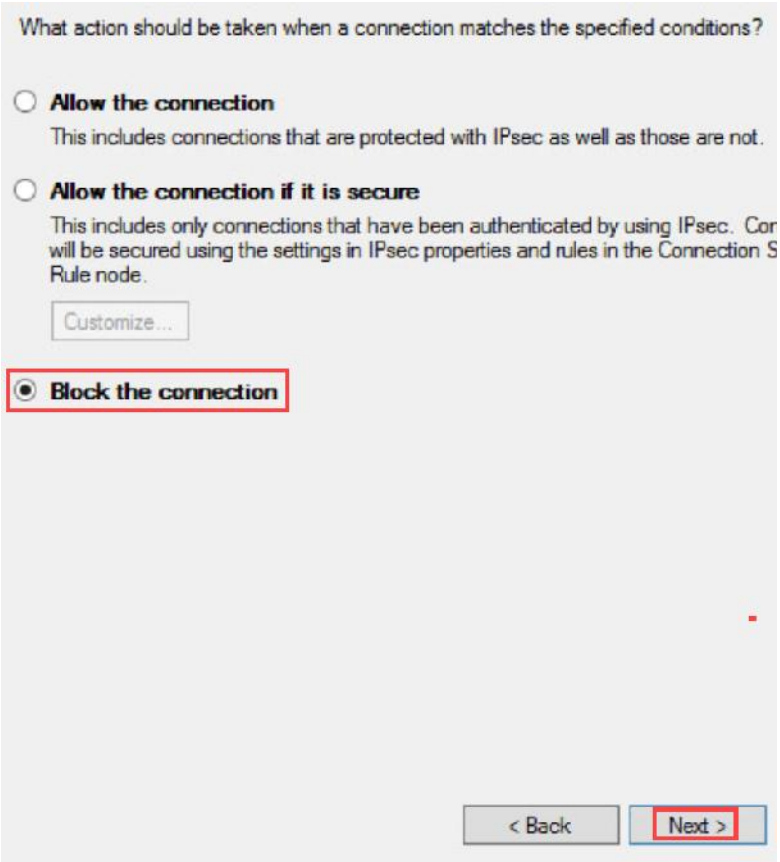
10. In the New Inbound Rule Wizard, click **Port**, followed by the **Next** button.



11. Click **TCP**, followed by **Specific local ports**. Enter **53, 88** into the field and click **Next**.

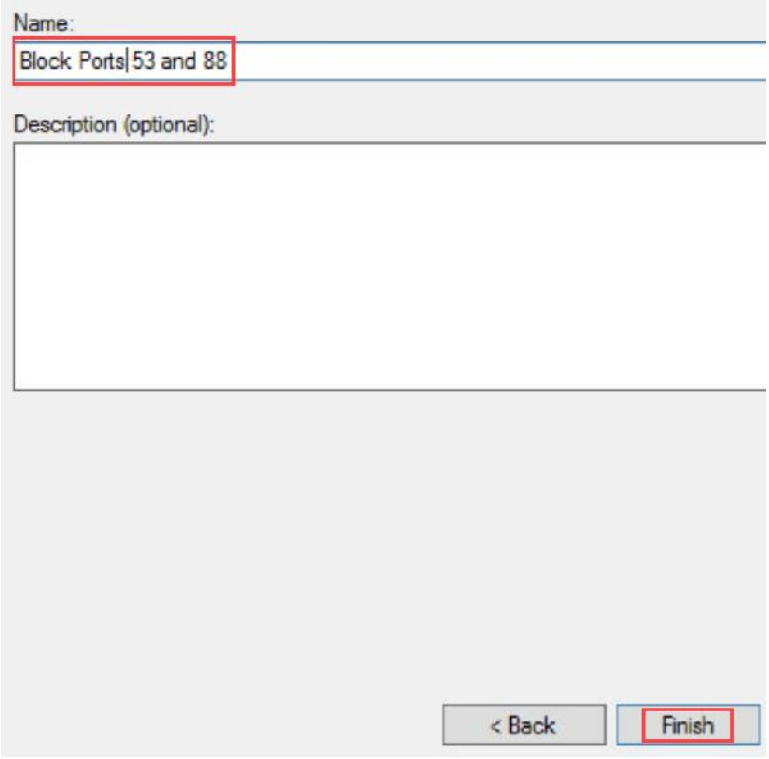


12. Click **Block the connection**, followed by **Next**.

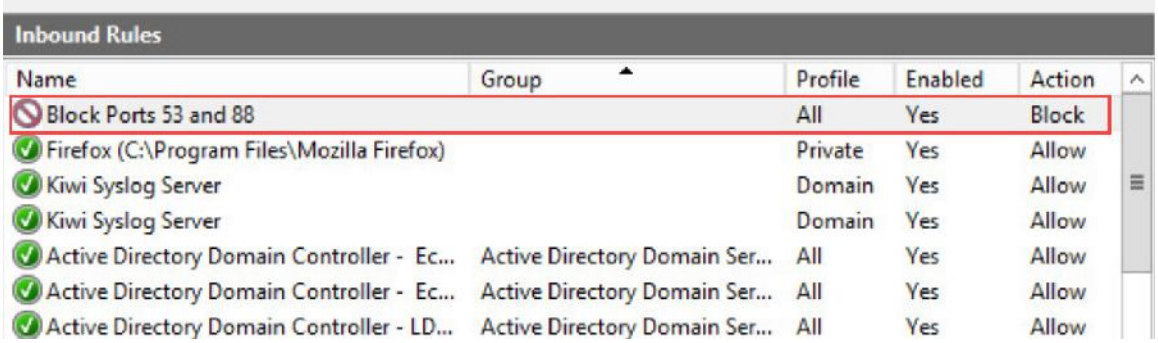


13. On the following screen, leave all three options checked and click **Next**.

14. In the name field, type **Block Ports 53 and 88**, then click **Finish**.



15. Notice the new rule in the *Inbound Rules* window. Close the *Windows Firewall with Advanced Security* window.

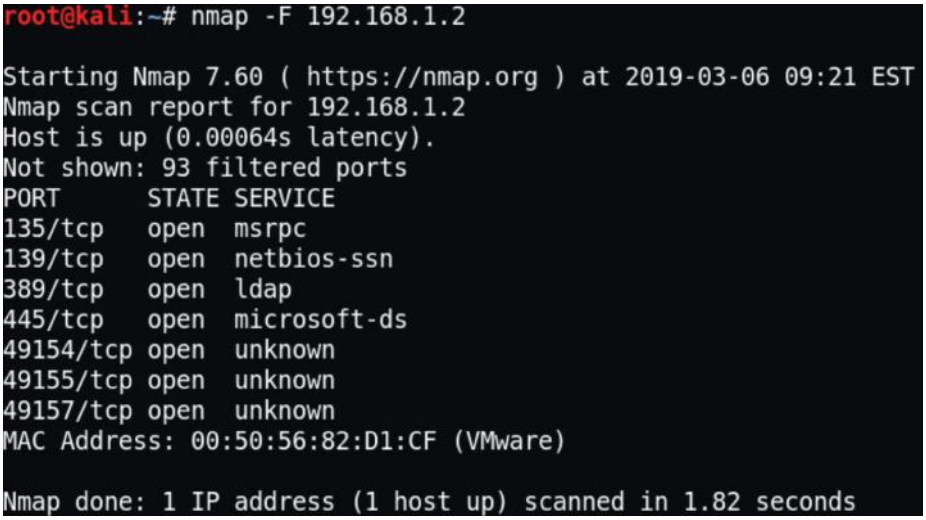


Inbound Rules

Name	Group	Profile	Enabled	Action
Block Ports 53 and 88		All	Yes	Block
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
Kiwi Syslog Server		Domain	Yes	Allow
Kiwi Syslog Server		Domain	Yes	Allow
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes	Allow

16. Return to the **Kali** virtual machine.
17. In the **Terminal**, repeat the following command. Notice in the results that ports 53 and 88 are no longer open.

```
root@kali:~# nmap -F 192.168.1.2
```



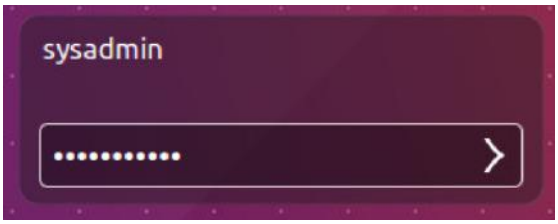
```
root@kali:~# nmap -F 192.168.1.2

Starting Nmap 7.60 ( https://nmap.org ) at 2019-03-06 09:21 EST
Nmap scan report for 192.168.1.2
Host is up (0.00064s latency).
Not shown: 93 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:50:56:82:D1:CF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
```


18. Now, run a scan against the **Ubuntu** virtual machine by running the following command. From the results, you can see that ports 21 (for FTP) and 80 (for HTTP) are open.

```
root@kali:~# nmap -F 192.168.1.4
```

```
root@kali:~# nmap -F 192.168.1.4

Starting Nmap 7.60 ( https://nmap.org ) at 2019-03-06 09:25 EST
Nmap scan report for 192.168.1.4
Host is up (0.00042s latency).
Not shown: 98 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
MAC Address: 00:50:56:82:D8:97 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
root@kali:~#
```

19. Launch the **Ubuntu** virtual machine to access the graphical login screen.
20. Log in as **`sysadmin`** using the password **`Password123`**.



21. Open a **Terminal** once the desktop has loaded.

22. If the *FTP* port is open on the Ubuntu machine, there is likely a process actively listening on it. To discover what this process is, enter the following command, using the password **Password123** if prompted. Notice that the process using port 21 is *proftpd*, also note the PID (this may be different every time you run the lab).

```
sysadmin@sysadmin-virtual-machine:~# sudo netstat -tulpn | grep :21
```

```
sysadmin@sysadmin-virtual-machine:~$ sudo netstat -tulpn | grep :21
[sudo] password for sysadmin:
tcp6       0      0 :::21                   :::*
 LISTEN      2538/proftpd: (acce
sysadmin@sysadmin-virtual-machine:~$
```


23. To stop this port from listening, kill the process using the PID found in the previous step with the following command. Once finished, you may close the **Terminal** window.

```
sysadmin@sysadmin-virtual-machine:~# sudo kill <pid>
```

```
sysadmin@sysadmin-virtual-machine:~$ sudo kill 2538
```

24. Return to the **Kali** virtual machine.
25. In the **Terminal**, probe the **Ubuntu** machine once more with the following command. Notice that port 21 is no longer open. Once you have finished examining the output, you may close the **Terminal** window.

```
root@kali:~# nmap -F 192.168.1.4
```

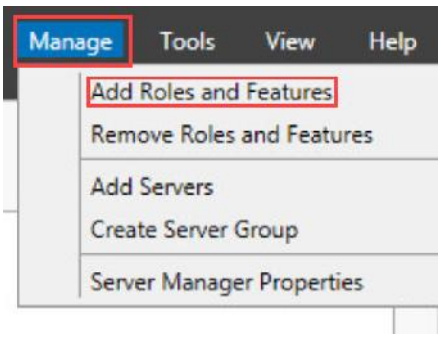
```
root@kali:~# nmap -F 192.168.1.4

Starting Nmap 7.60 ( https://nmap.org ) at 2019-03-06 09:38 EST
Nmap scan report for 192.168.1.4
Host is up (0.00014s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:50:56:82:D8:97 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```


4 Preparing and Applying Patches

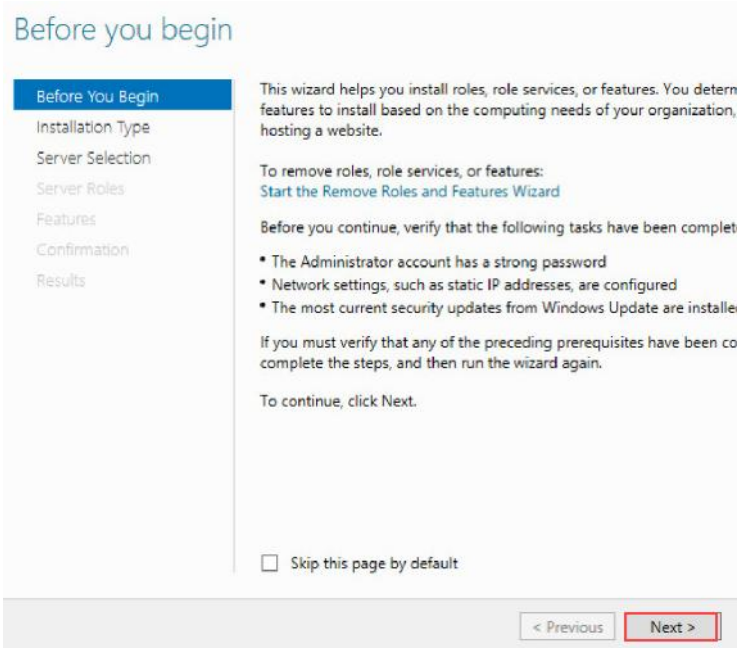
In this task, you will create a backup of the current system files before manually installing updates to the Windows 2012 R2 server.

1. Return to the **2012 R2** virtual machine.
2. Open the **Server Manager** if it does not open automatically. To do this, click the **Server Manager** icon on the taskbar.

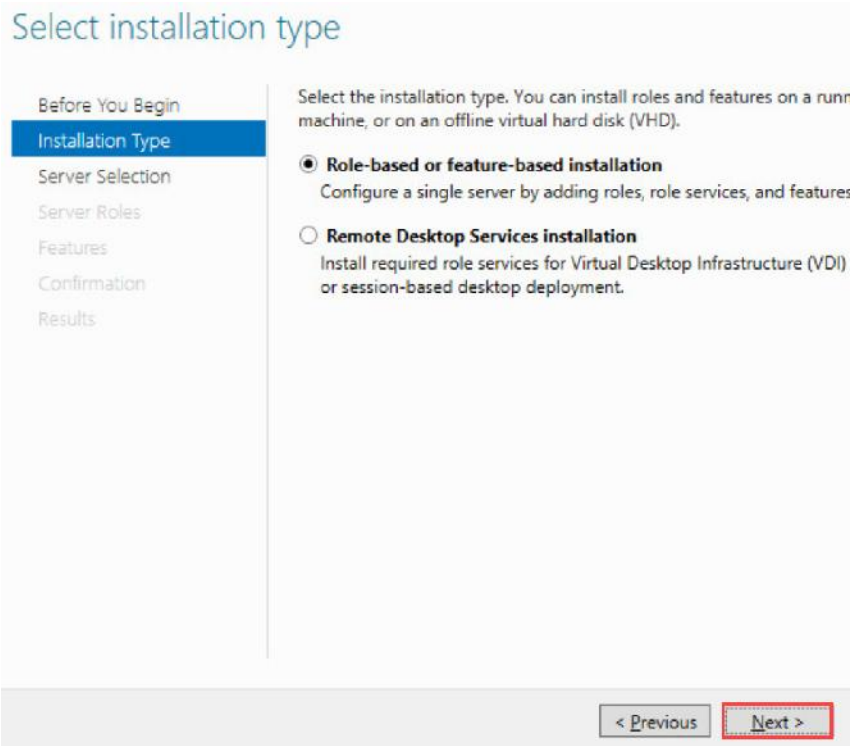
3. In the *Server Manager* window, click on **Manage**-> **Add Roles and Features**.



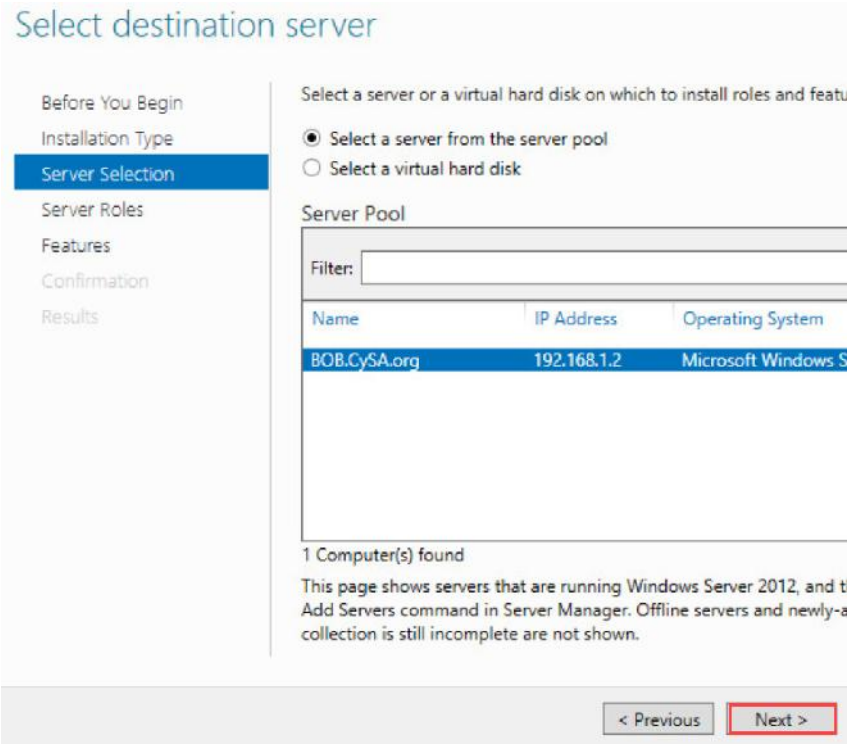
4. On the **Before you begin** screen, click **Next.**



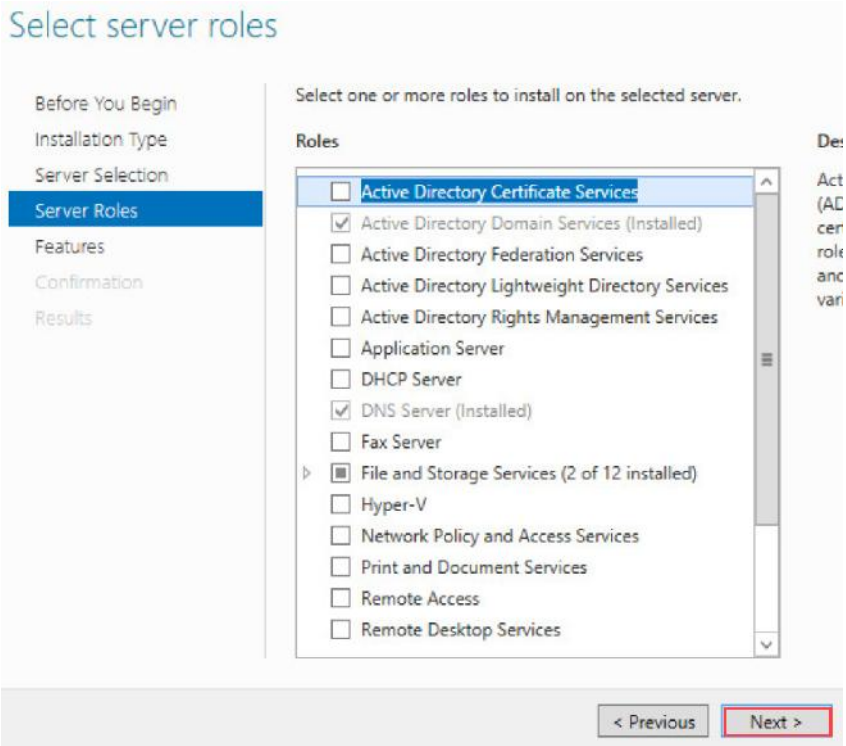
5. On the **Select installation type** screen, ensure **Role-based or feature-based installation** is selected and click **Next**.



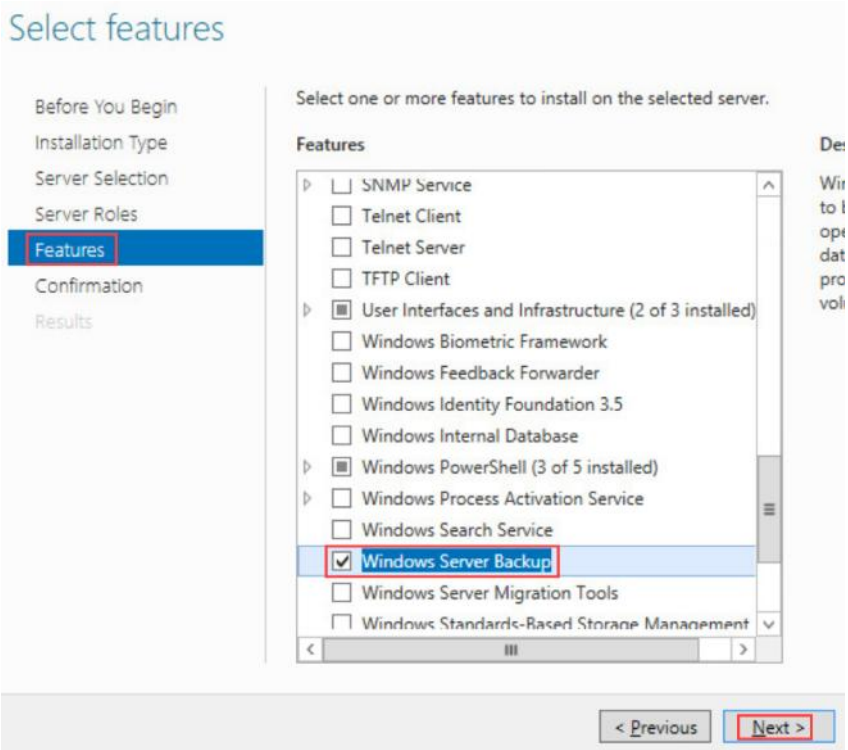
6. On the **Select destination server** screen, ensure **Select a server from the server pool** is selected and click **Next**.



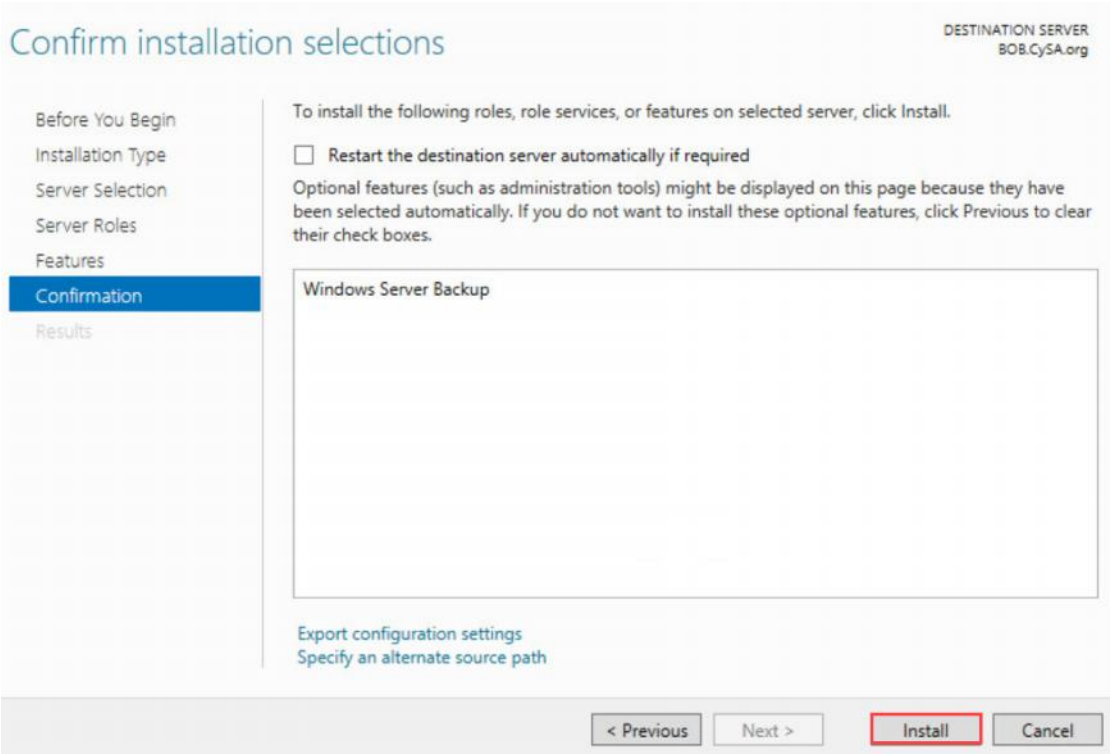
7. On the **Select server roles** screen, click **Next**.



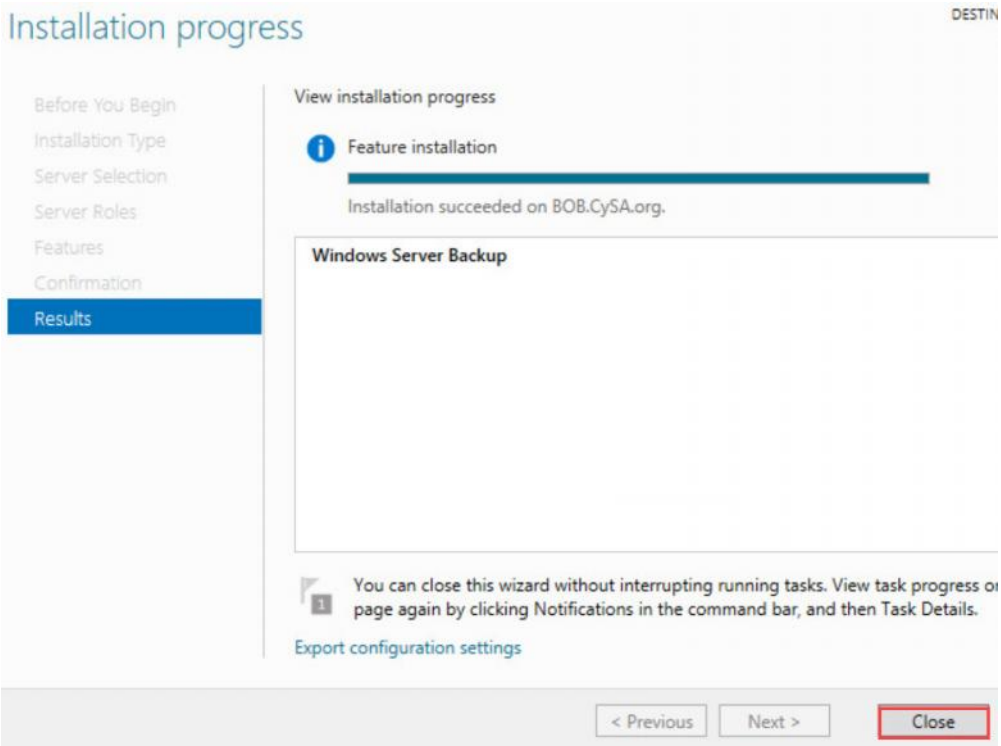
8. On the **Select features** screen, select **Windows Server Backup** and click **Next**.



9. On the **Confirm installation selections** screen, confirm that **Windows Server Backup** is due to be installed, then click **Install**.

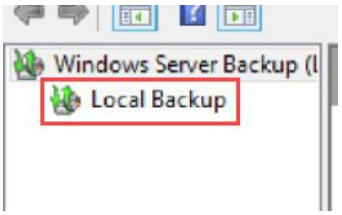


10. Once the installation finishes, close the **Installation progress** window by clicking **Close**.

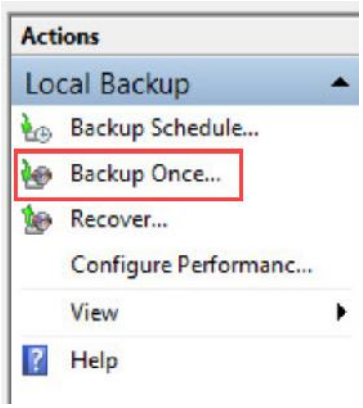


11. Now that *Windows Server Backup* is installed, you can proceed to create a backup. It is important to maintain fallback points in case an update fails or causes system functions to perform undesirably. To do so, in the Windows Server Manager, click **Tools**-> **Windows Server Backup**.

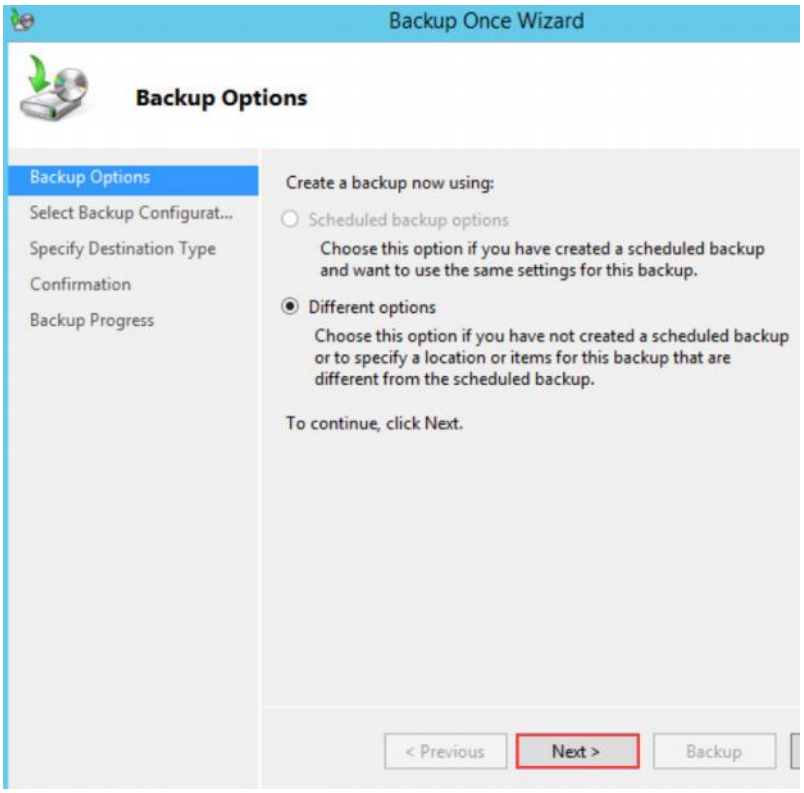
12. In the *Windows Server Backup* tool, click **Local Backup** in the left pane.



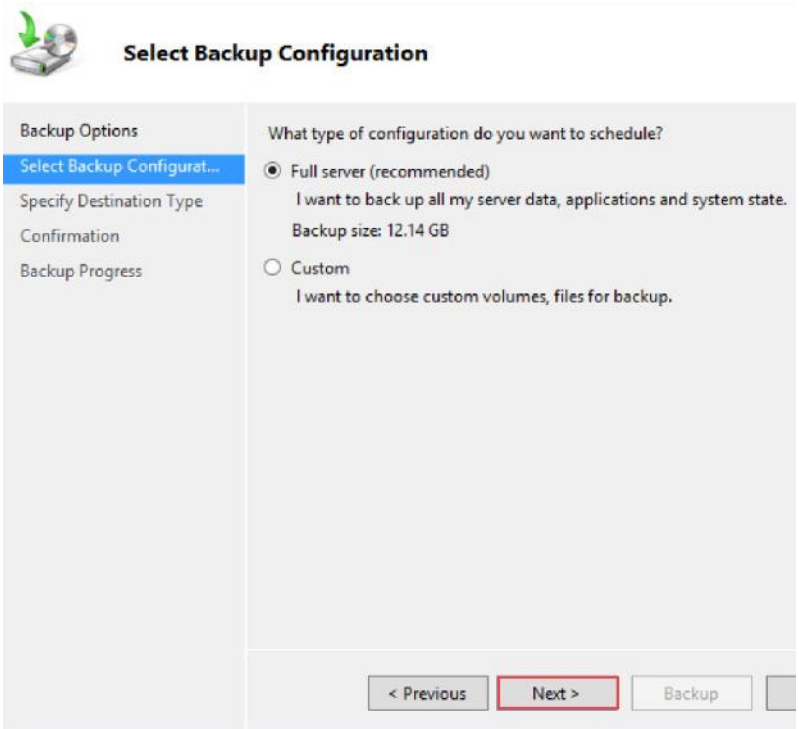
13. Click **Backup Once** in the *Actions* pane on the far-right side of your screen.



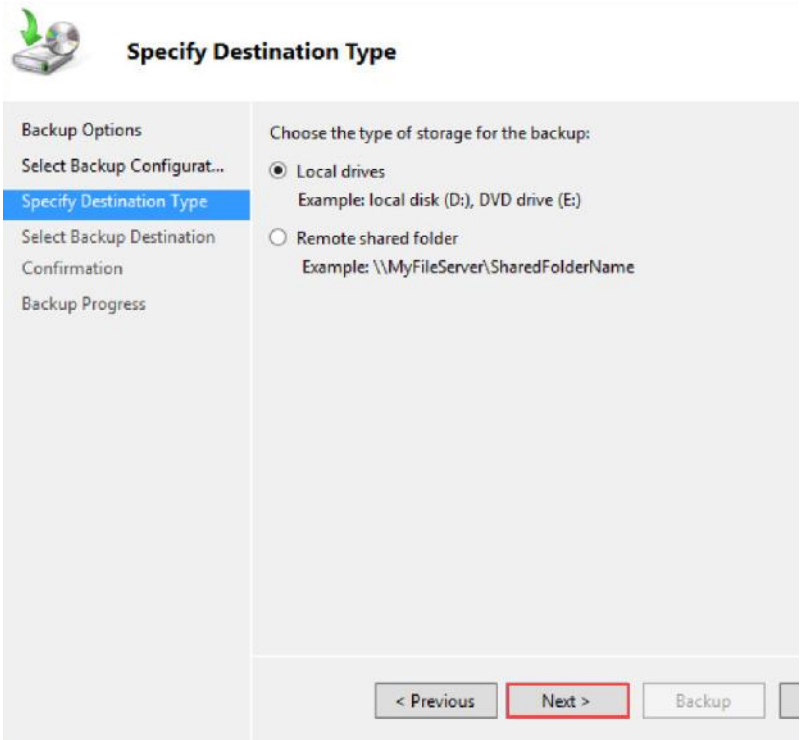
14. Once the *Backup Once Wizard* opens, you will be on the **Backup Options** screen. Confirm that **Different options** is selected and click **Next**.



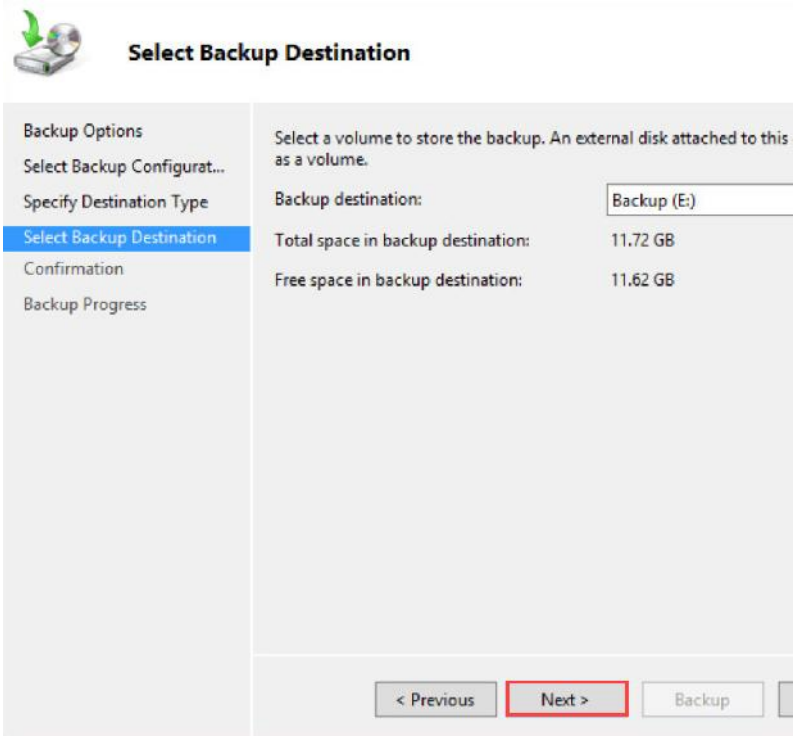
15. On the **Select Backup Configuration** screen, ensure that **Full server (recommended)** is selected and click **Next**.



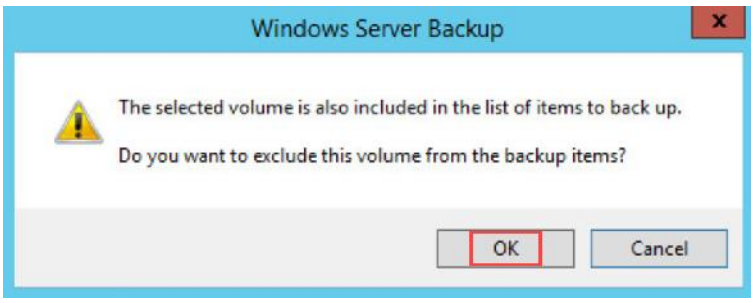
16. On the **Specify Destination Type** screen, ensure **Local drives** is selected and click **Next**.



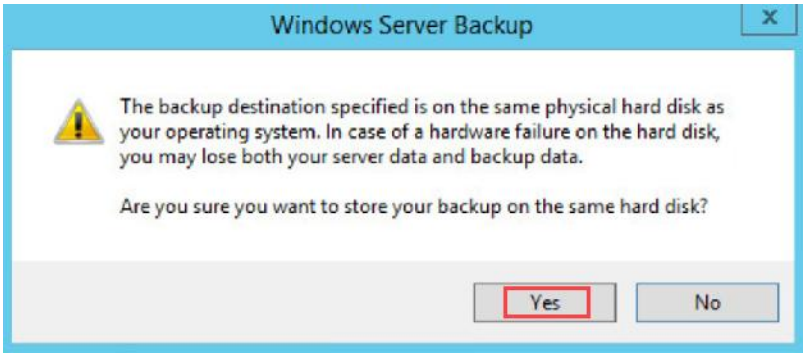
17. On the **Select Backup Destination** screen, ensure that **Backup (E:)** is being used as the destination for the backup and click **Next**.



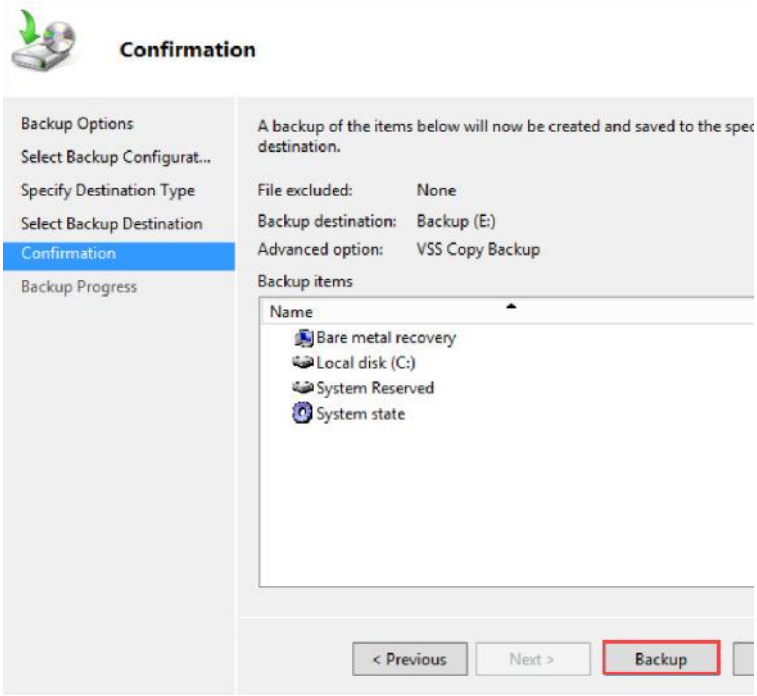
18. You will receive a warning saying that "The selected volume is also included in the list of items to back up." To prevent this, click **OK** to remove E: from being backed up into itself.



19. You will receive a warning saying that “The backup destination specified is on the same physical hard disk as your operating system. In case of a hardware failure on the hard disk, you may lose both your server data and backup data.” For this lab, disregard this warning and click **Yes**.

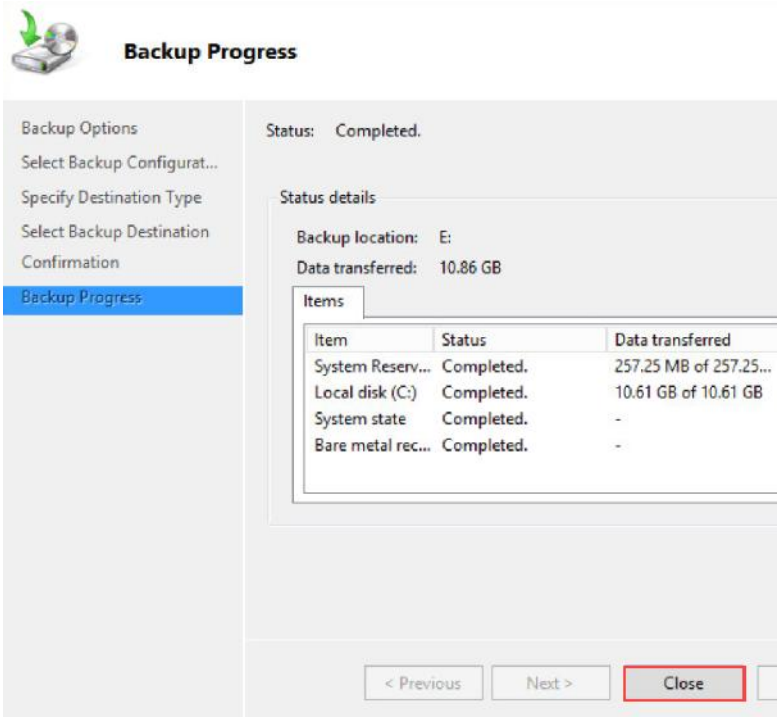


20. Confirm the information on the **Confirmation** screen and click **Backup**.



Backing up the server will take approximately 4 minutes to complete.

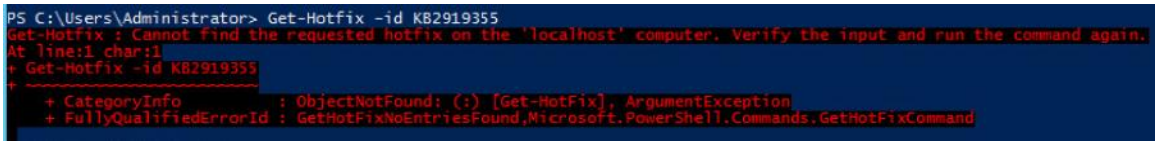
21. Once the backup finishes, click **Close**.



22. Close all open windows. Open a **PowerShell** window by clicking the icon on the taskbar.

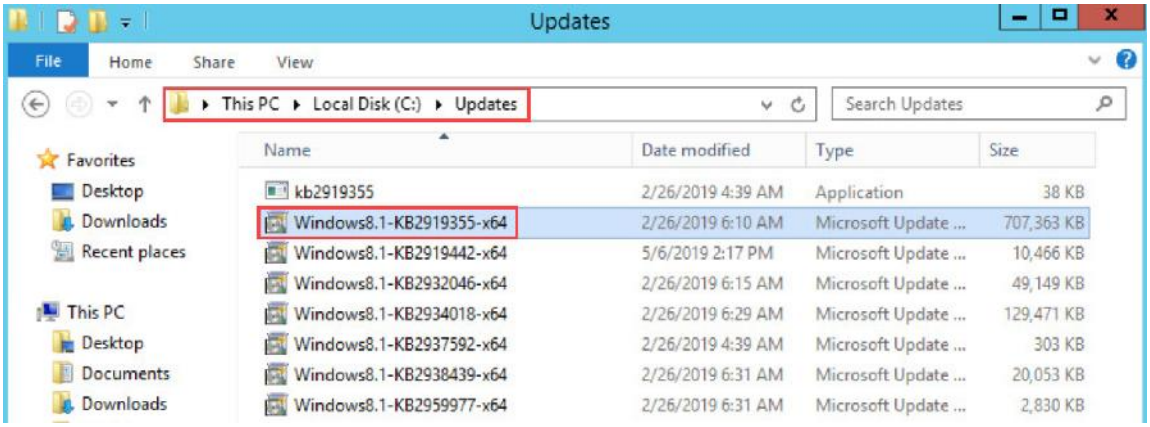
23. In the **PowerShell** prompt, check to see if the update you want to install is currently installed with the following command. Note that no hotfix can be found, and thus the patch has not yet been installed.

```
PS C:\Users\Administrator> Get-Hotfix -id KB2919355
```

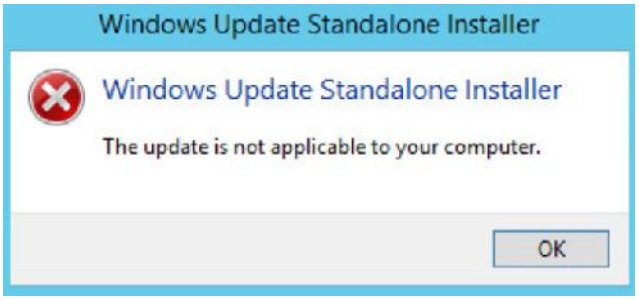


24. To begin the process to install the patch, open the **File Explorer** by clicking its icon on the taskbar.

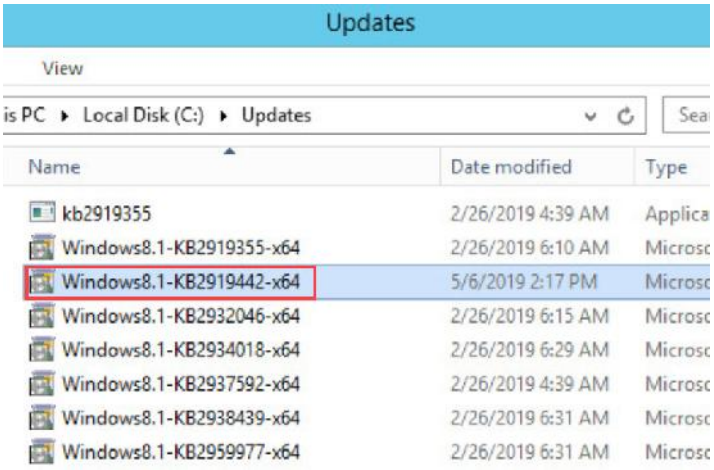
25. Navigate to **C:\Updates**. Double-click on **Windows8.1-KB2919355-x64.msu** to install the update you just searched for in *PowerShell*.



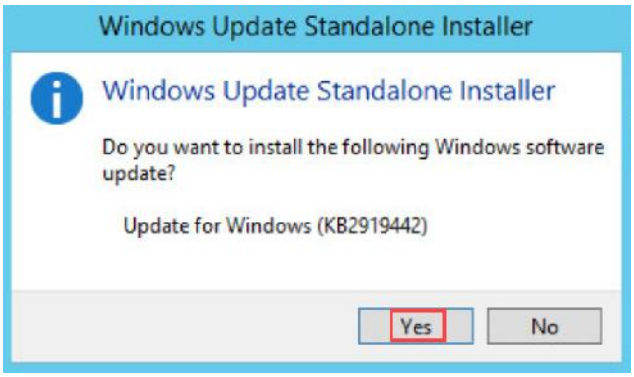
26. You will receive an error message stating that "The update is not applicable to your computer." This is because this update has a prerequisite that must be installed first. Click **OK**.



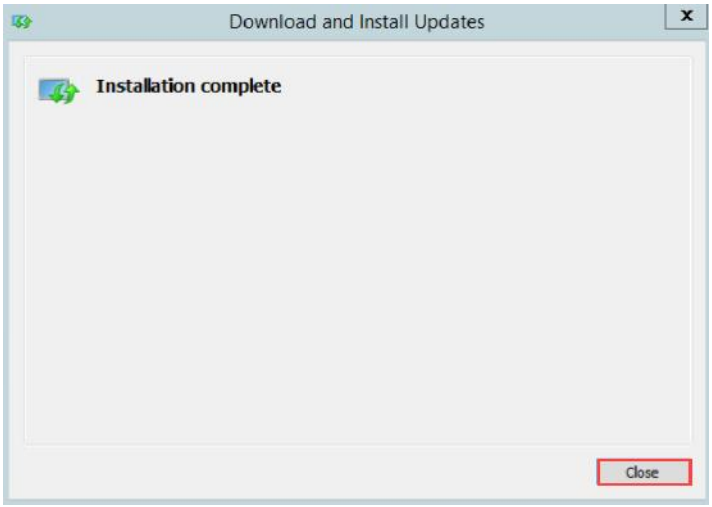
27. To install the prerequisite update, double-click **Windows8.1-KB2919442-x64.msu**.



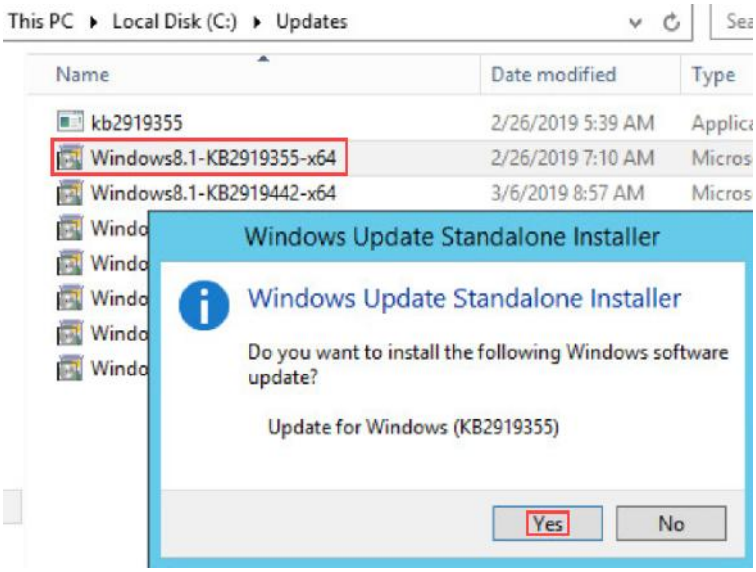
28. When asked to confirm the installation, select **Yes**.



29. Once the update is installed, click **Close**.

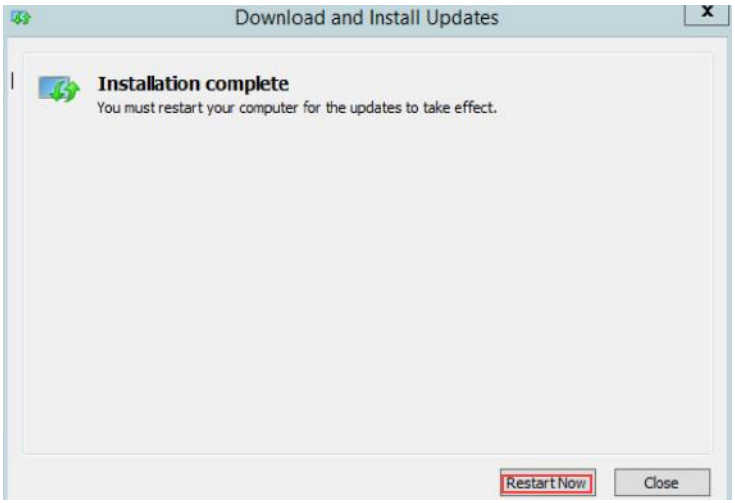


30. Now that you have installed the prerequisite patch, you can install the much larger update. Double-click on **Windows8.1- KB2919355-x64** once more and select **Yes** when prompted.



Larger updates take extended periods of time to install. This update will take approximately 12 minutes.

31. Once the update has installed, you will be prompted to restart the machine. Click **Restart Now**.



32. Once the machine has restarted, log in as `CySa\Administrator` using the password `Password123`. Once loaded, you may close the **Server Manager** window.

33. Open a **PowerShell** window by clicking the icon on the taskbar.

34. To check for the installed update, repeat the command **Get-Hotfix -id KB2919355**. Notice now that the update has been installed, different results are received than in step 23. You may now close the **PowerShell** window.

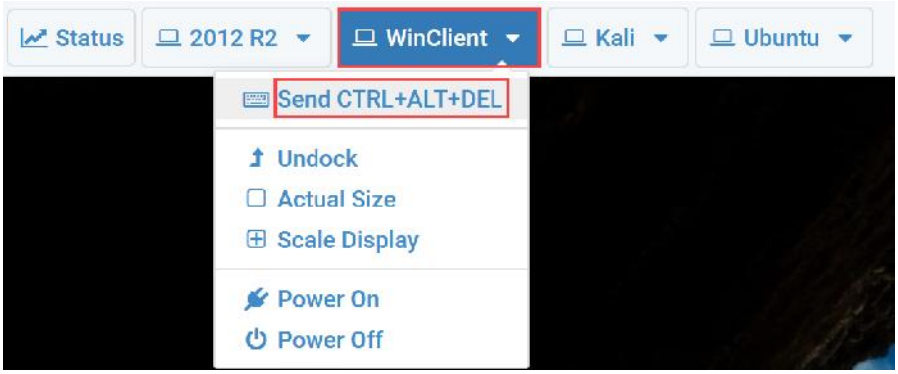
```
PS C:\Users\Administrator> Get-Hotfix -id KB2919355
```

```
PS C:\Users\Administrator> Get-Hotfix -id KB2919355

Source        Description      HotFixID      InstalledBy          InstalledOn
------        -----------      --------      -----------          -----------
BOB           Update           KB2919355     CYSA\Administrator   3/6/2019 12:00:00 AM
```


5 Using Windows Defender to Increase Security

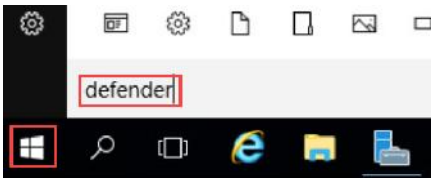
In this task, you will set up various settings with Windows Defender to improve the security of the host.

1. Launch the **WinClient** virtual machine to access the graphical login screen.
2. Bring up the login window by sending a **Ctrl + Alt + Delete**. To do this, click the **WinClient** drop-down menu and click **Send CTRL+ALT+DEL**.

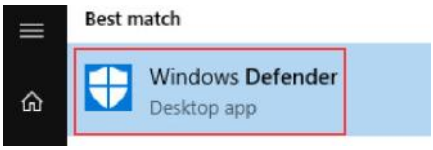


3. Log in as `CySa\Administrator` using the password `Password123`.

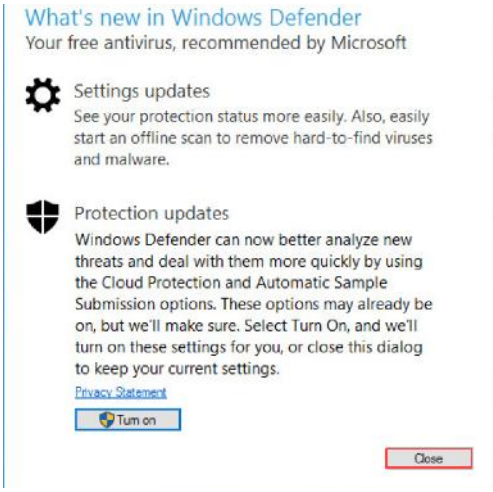
4. Click the **Windows** icon in the lower-left and type **defender**.



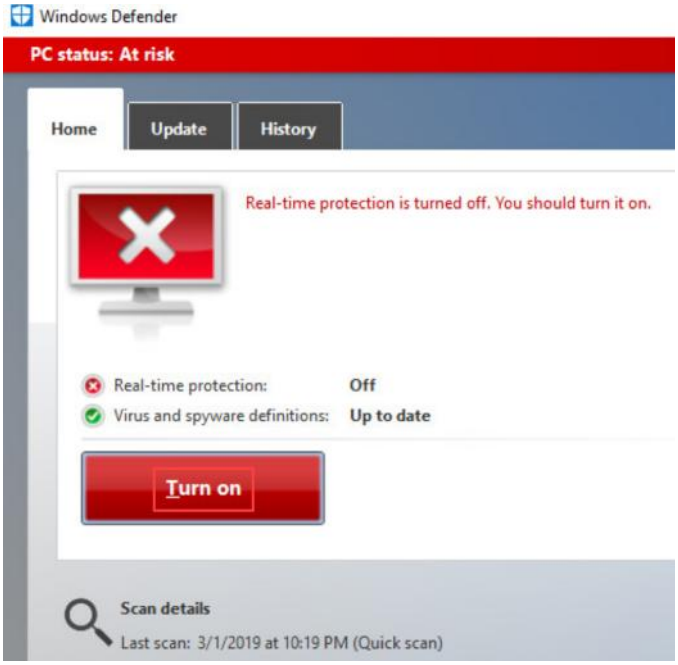
5. Click on **Windows Defender**.

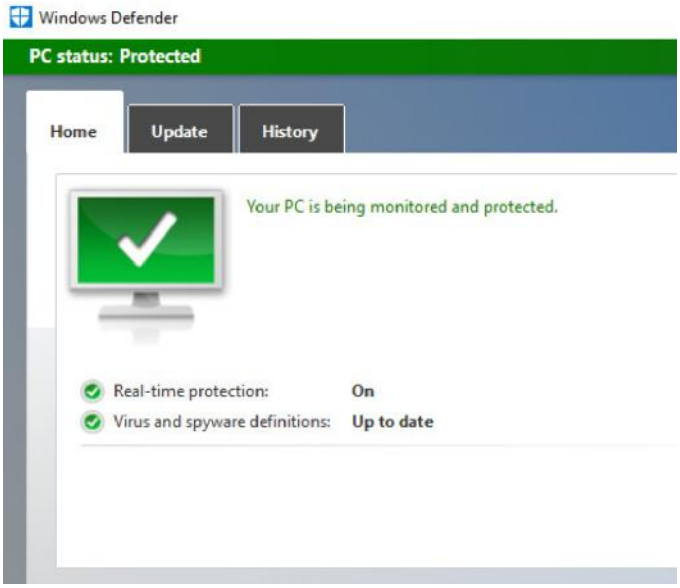


6. You may be met with a *What's new in Windows Defender* window. If so, click **Close.**



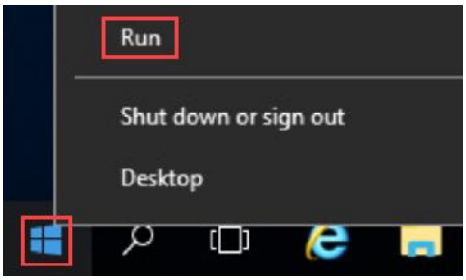
7. Once **Windows Defender** loads click the **Turn On** button to enable *Real-Time Protection*.



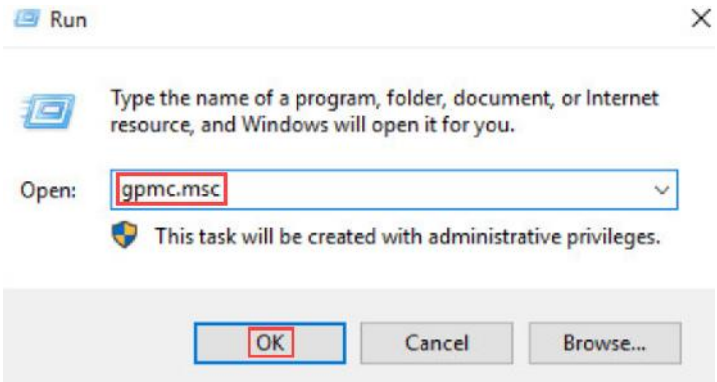


Your *Windows Defender* may state that your virus and spyware definitions are out of date. You can safely ignore this warning, as the lab environment lacks internet access.

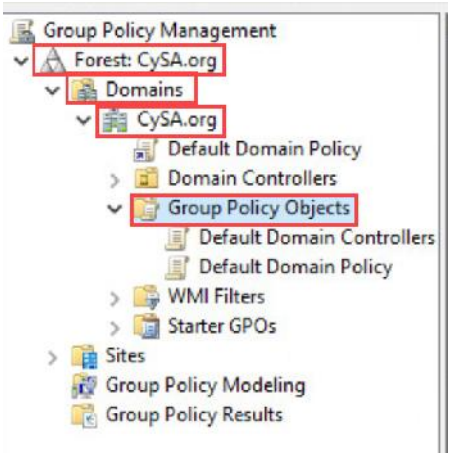
8. Next, you will explore various group policy settings related to *Windows Defender*. Right-click the **Windows** icon in the lower-left of the screen, then click **Run**.



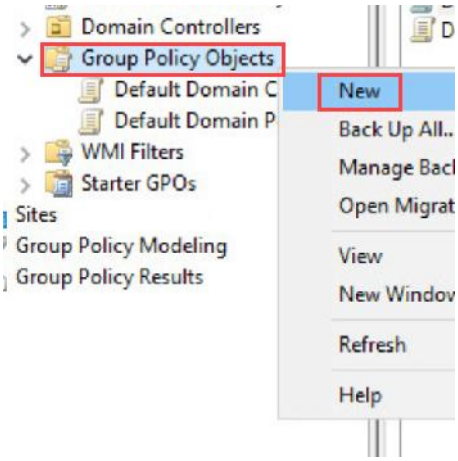
9. Type **gpmc.msc** into the window and click **OK**.



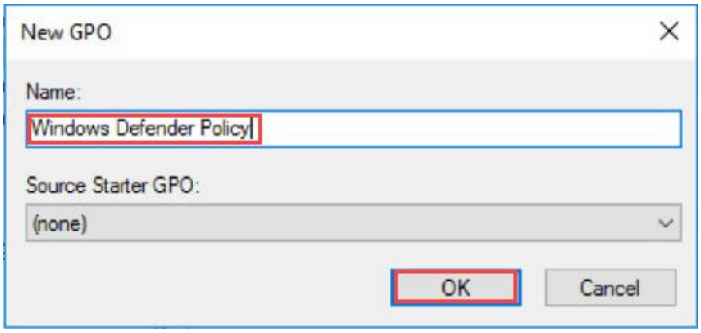
10. In the left pane of the *Group Policy Management* window, navigate to **Forest: CySA.org**-> **Domains**-> **CySA.org**-> **Group Policy Objects**.



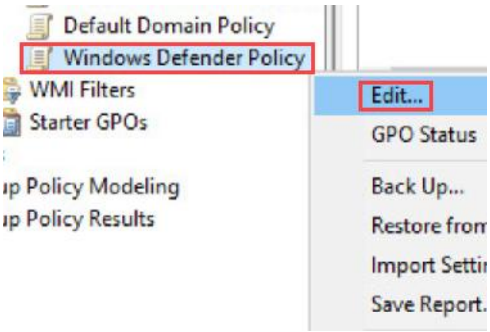
11. Right-click **Group Policy Objects** and select **New**.



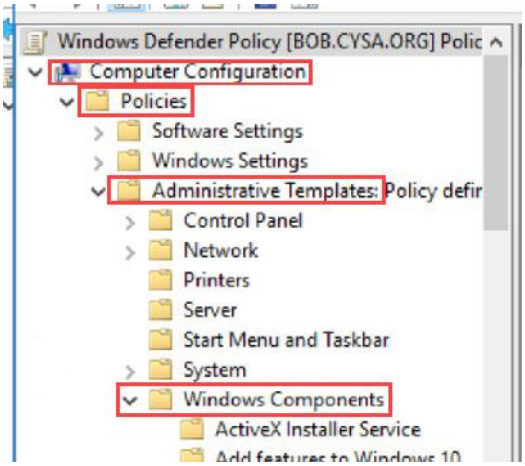
12. In the **New GPO** window's **Name** field, type **Windows Defender Policy** and click **OK**.



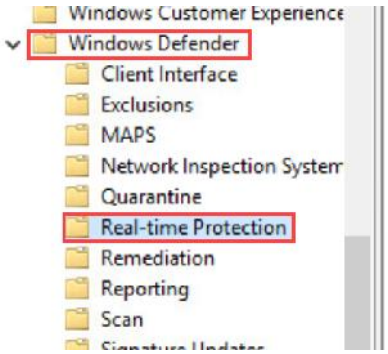
13. Right-click **Windows Defender Policy** and click **Edit**.



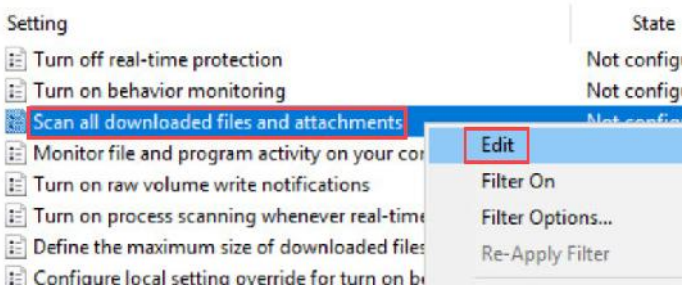
14. In the left pane of the *Group Policy Management Editor*, expand **Computer Configuration**-> **Policies**-> **Administrative Templates**-> **Windows Components**.



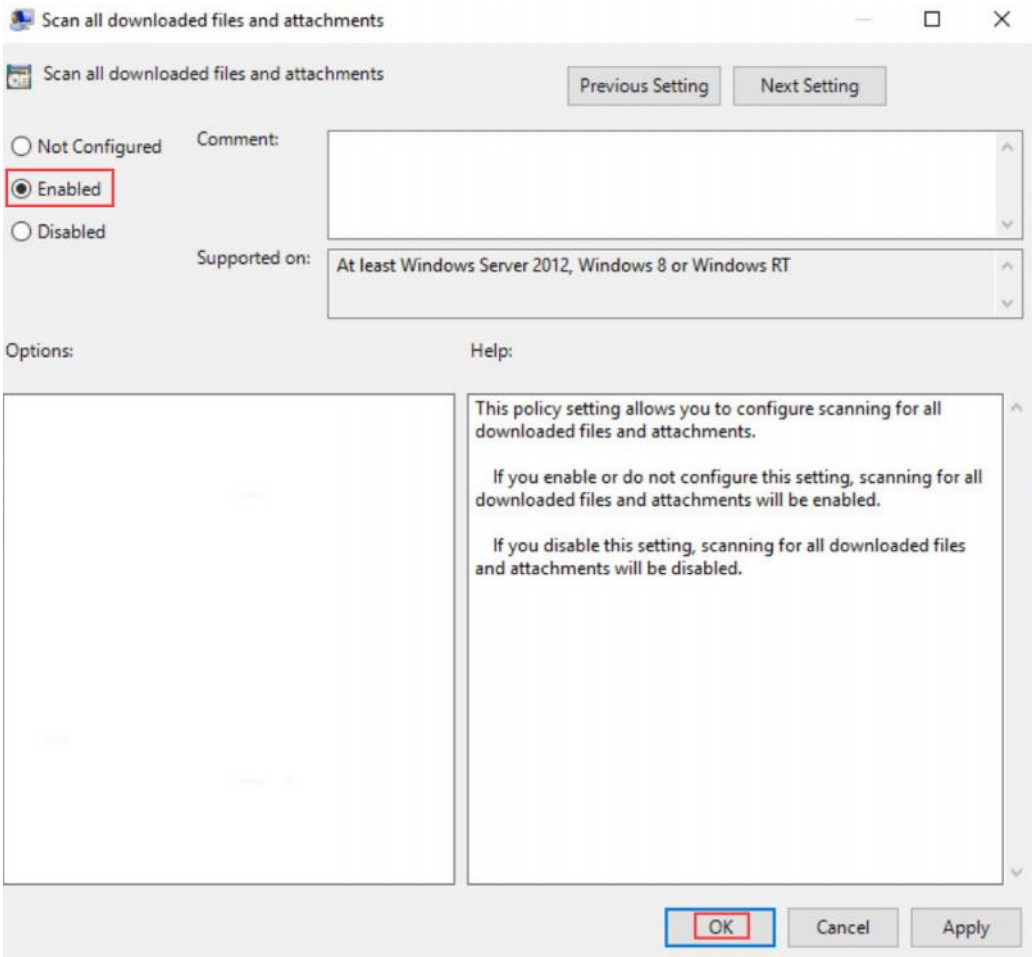
15. Scroll down and expand **Windows Defender**. Click on **Real-Time Protection**.



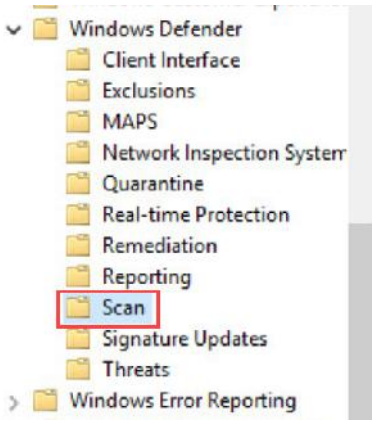
16. In the right pane, right-click **Scan all downloaded files and attachments** and click **Edit**.



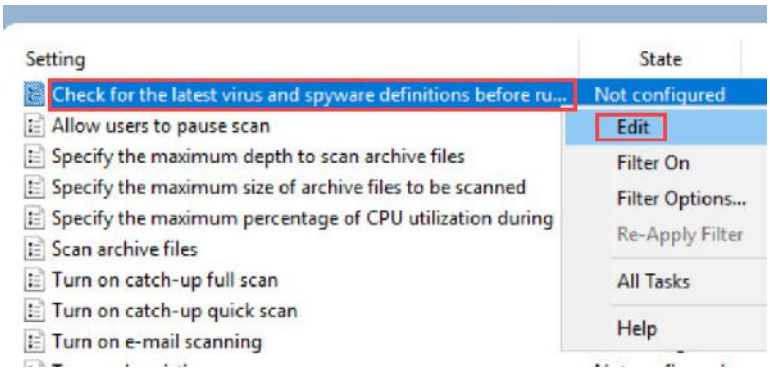
17. Click **Enabled** and click **OK**.



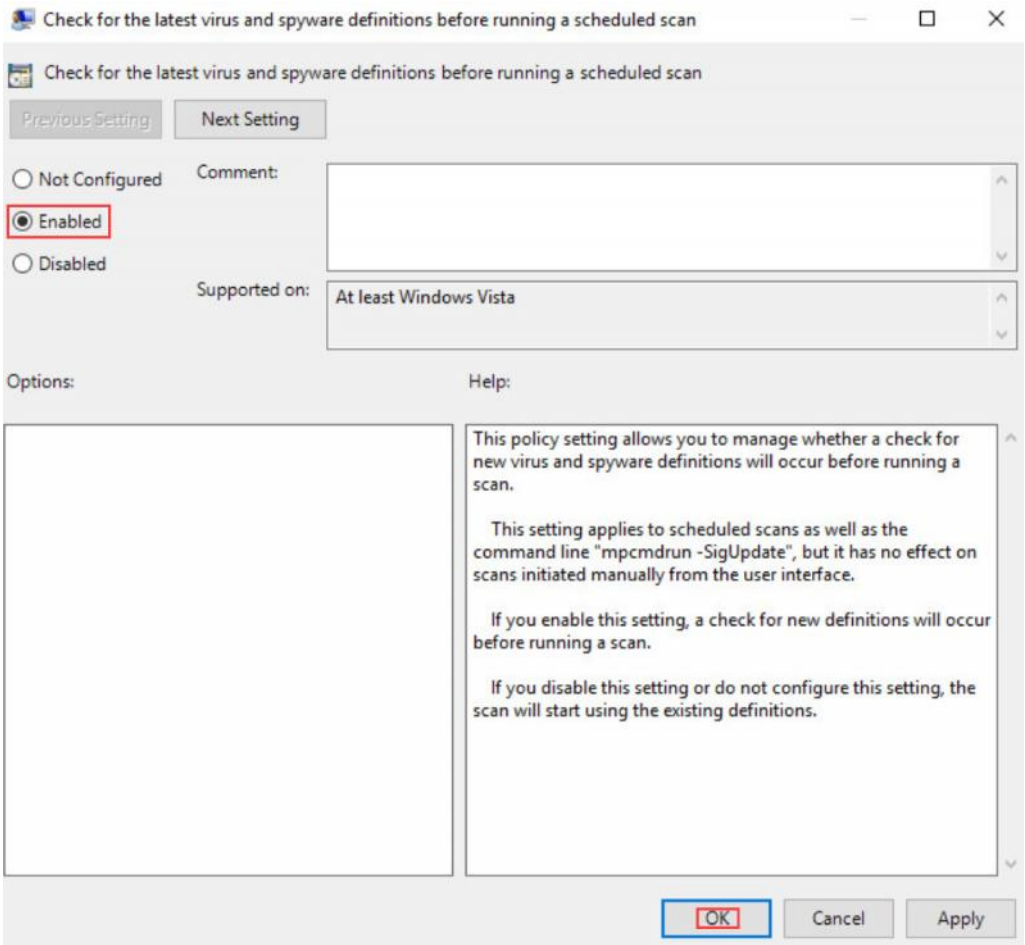
18. On the *Windows Group Policy Management Editor*, click **Scan** in the left pane.



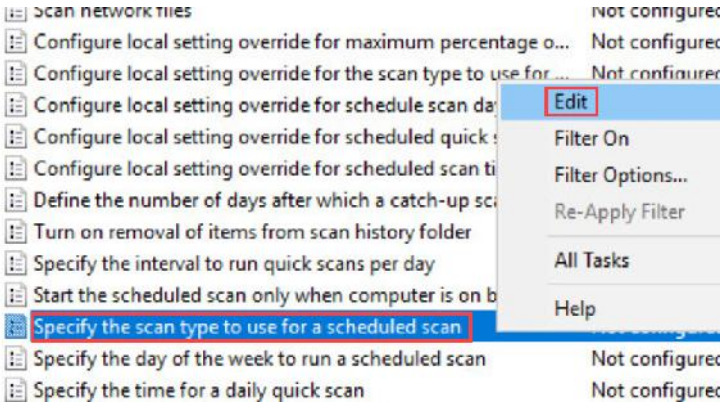
19. In the right pane, Right-click on **Check for the latest virus and spyware definitions before running a scheduled scan**. Click **Edit**.



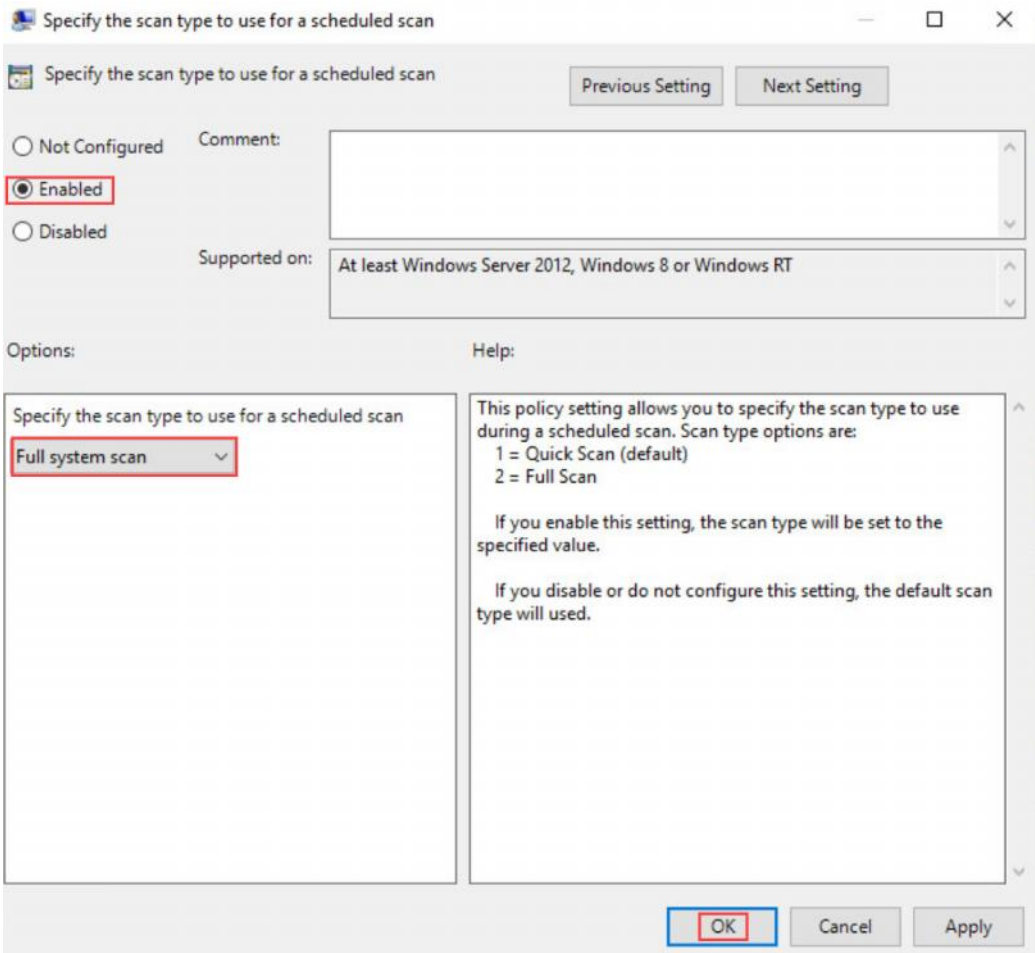
20. Click **Enabled**, then click **OK**.



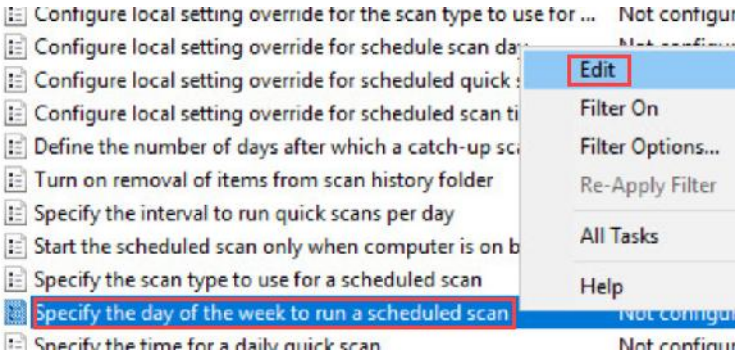
21. Right-click **Specify the scan type to use for a scheduled scan**. Click **Edit**.



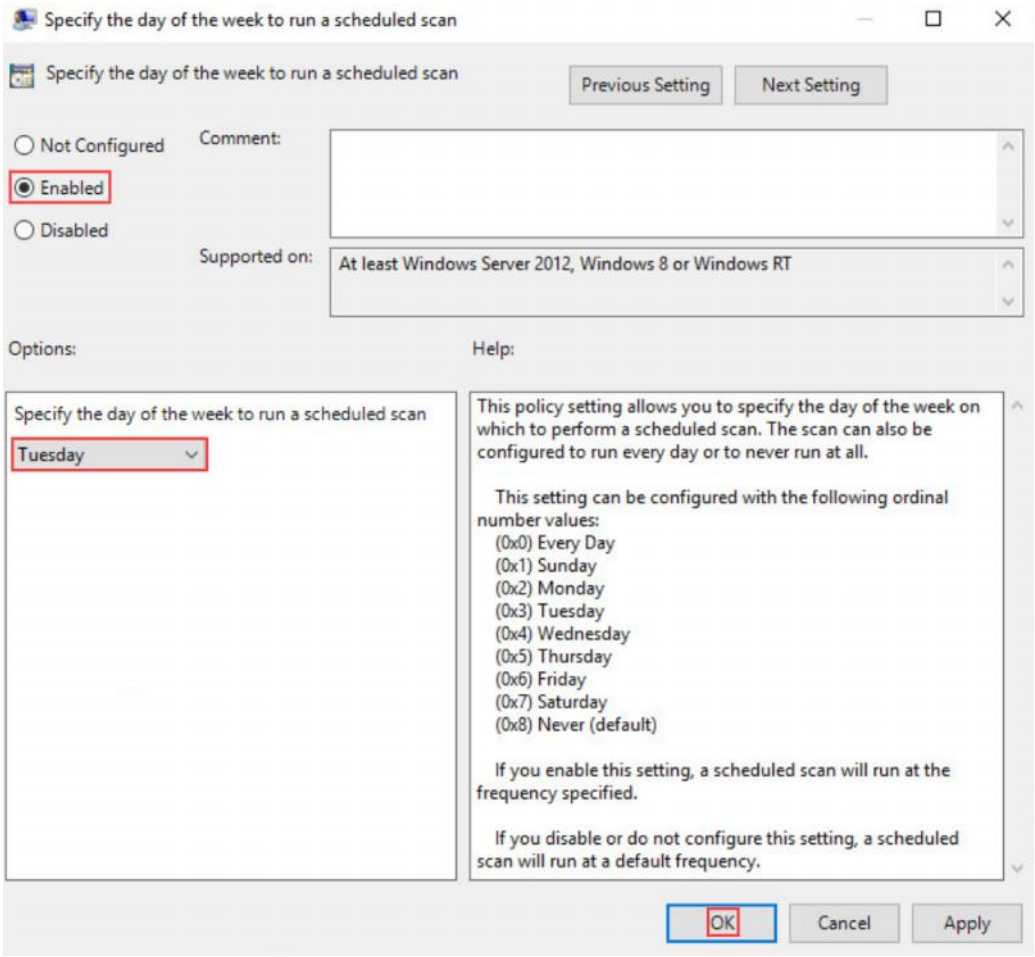
22. Click **Enabled**. In the drop-down menu, select **Full system scan**. Click **OK**.



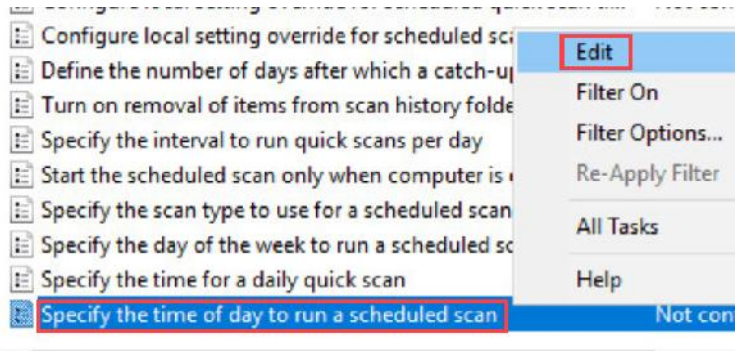
23. Right-click on **Specify the day of the week to run a scheduled scan.** Click **Edit**.



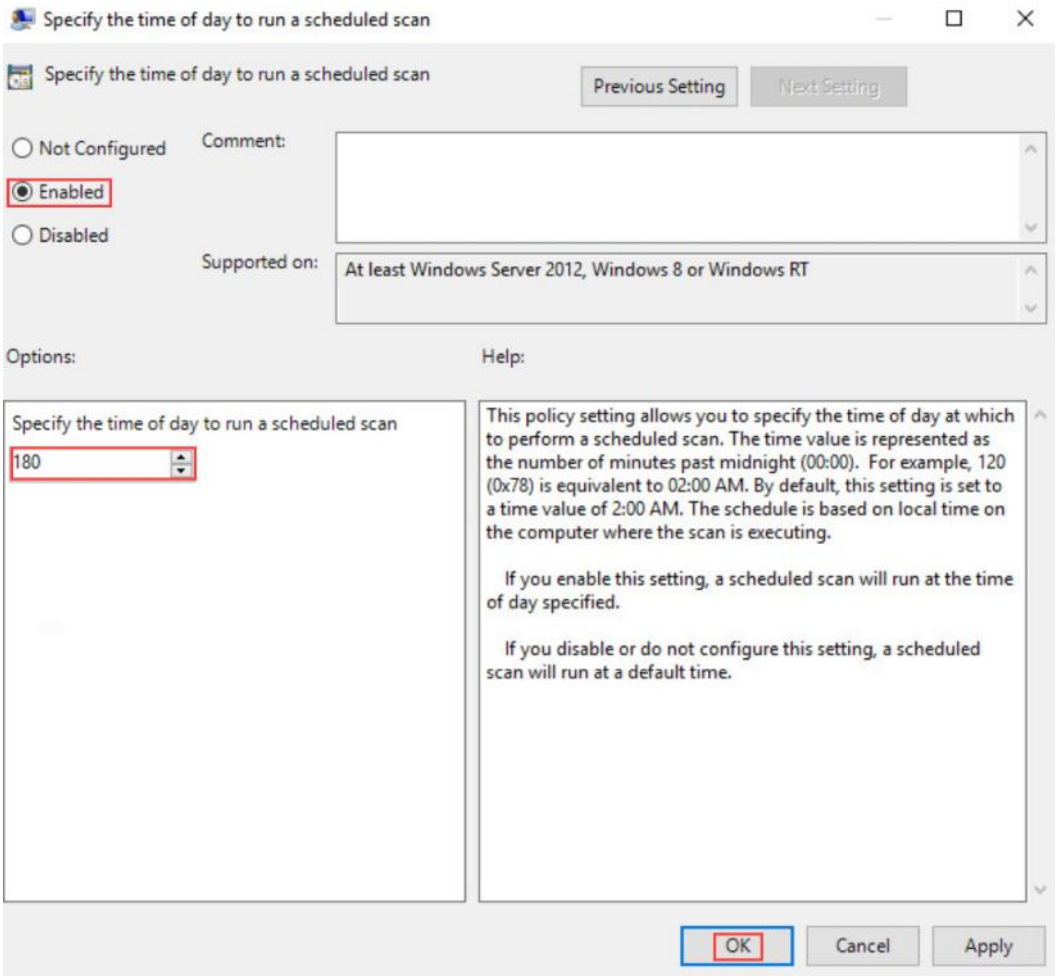
24. Click **Enabled**. In the drop-down menu, select **Tuesday**. Click **OK**.



25. Right-click on **Specify the time of day to run a scheduled scan.** Click **Edit**.



26. Click **Enabled**. In the spin box, enter **180**. This will tell the scheduler to run a scan at 3:00 AM. Click **OK**.



27. With these options, you have now activated *Windows Defender*, and set up group policies to run full system scans every Tuesday morning at 3:00 AM. Additionally, you have told *Windows Defender* to scan all downloaded files, and to update virus definitions before every weekly scan. This concludes the lab. You may now end the Reservation.

