CySA+ Lab Series

Lab 07: Host Hardening

Document Version: 2022-10-10

Material in this Lab Aligns to the Following	
CompTIA CySA+ (CS0-002) Exam Objectives	1.3 - Given a scenario, perform vulnerability management activities 1.4 - Given a scenario, analyze the output from common vulnerability tools 1.7 - Given a scenario, implement controls to mitigate attacks and software vulnerabilities 2.1 - Explain software assurance best practices 3.2 - Given a scenario, implement configuration changes to existing controls to improve security
All-In-One CompTIA CySA+ Second Edition ISBN-13: 978-1260464306 Chapters	3: Vulnerability Management Activities 4: Vulnerability Assessment Tools 7: Mitigating Controls for Attacks and Software Vulnerabilities 8: Security Solutions for Infrastructure Management 12: Implement Configuration Changes to Existing Controls to Improve Security

Contents

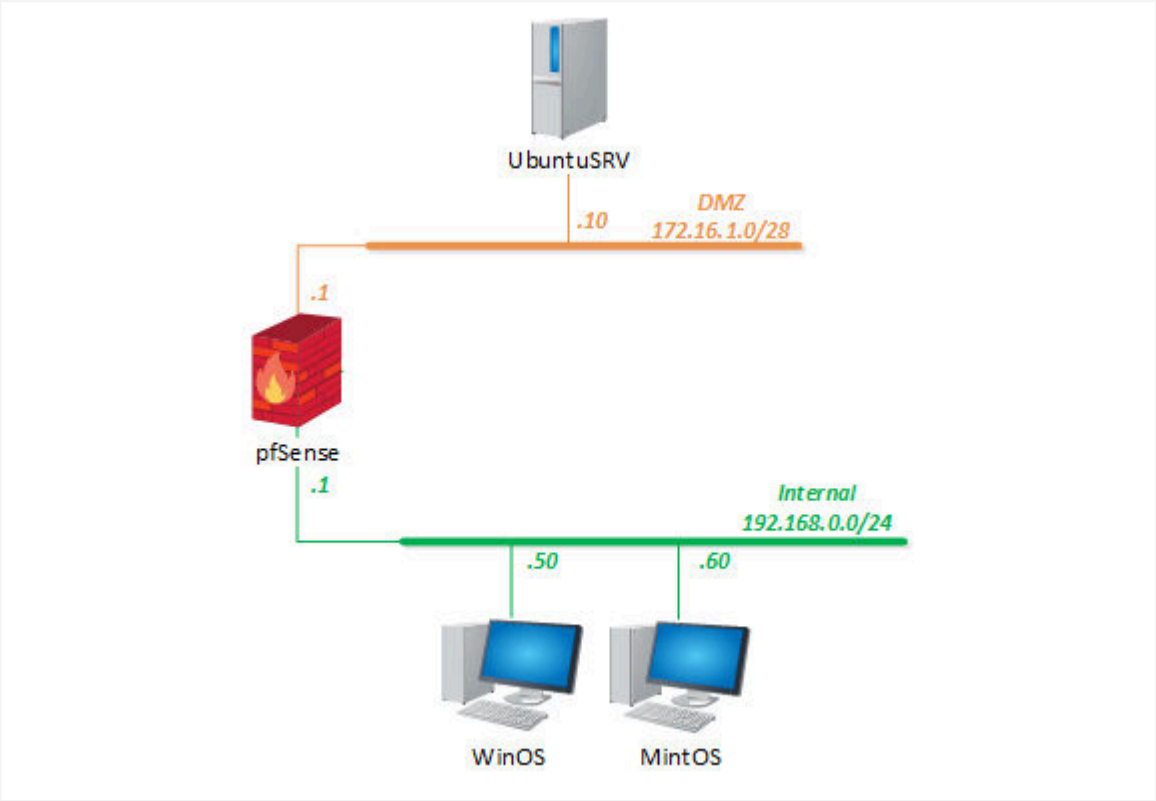
Introduction

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

Objective

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

Lab Topology



Lab Settings

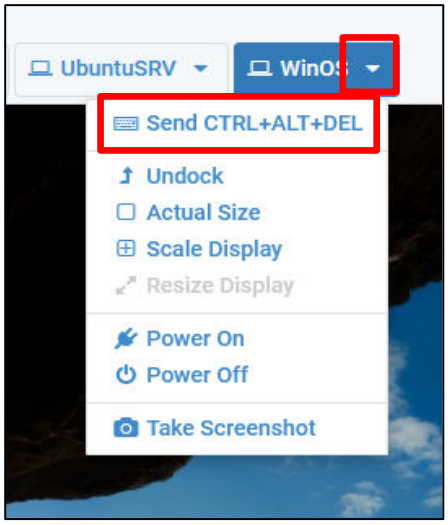
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account	Password
WinOS (Server 2019)	192.168.0.50	Administrator	NDGlabpass123!
MintOS (Linux Mint)	192.168.0.60	sysadmin	NDGlabpass123!
OSSIM (Alien Vault)	172.16.1.2	root	NDGlabpass123!
UbuntuSRV (Ubuntu Server)	172.16.1.10	sysadmin	NDGlabpass123!
Kali	203.0.113.2	sysadmin	NDGlabpass123!
pfSense	203.0.113.1 172.16.1.1 192.168.0.1	admin	NDGlabpass123!

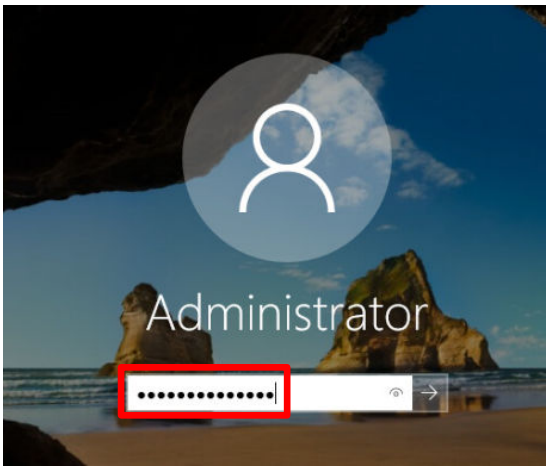
1 Navigating the Local Group Policy Editor

1.1 Modify Password Policies

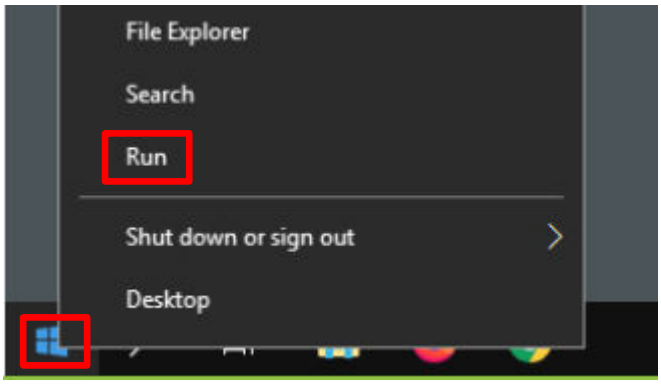
1. Set the focus to the **WinOS** computer.
2. Bring up the login window by sending a Ctrl + Alt + Delete. To do this, click the **WinOS** dropdown menu and click **Send CTRL+ALT+DEL**.



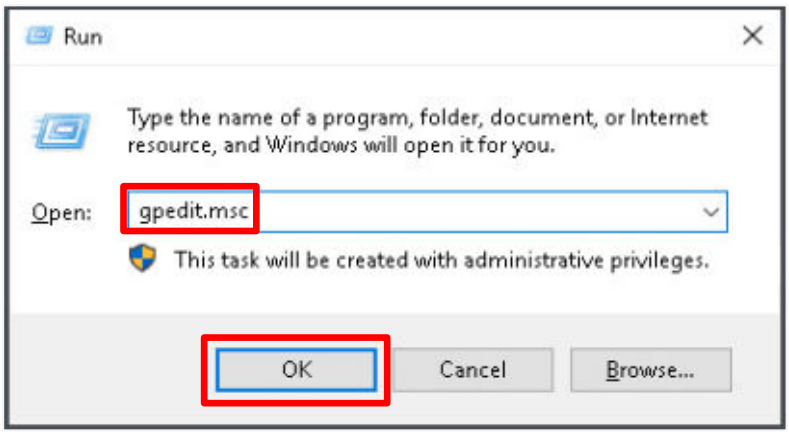
3. Log in as *Administrator* using the password: `NDGlabpass123!`



4. In the lower-left corner of the screen, right-click the **Windows Start** button icon and choose **Run**.

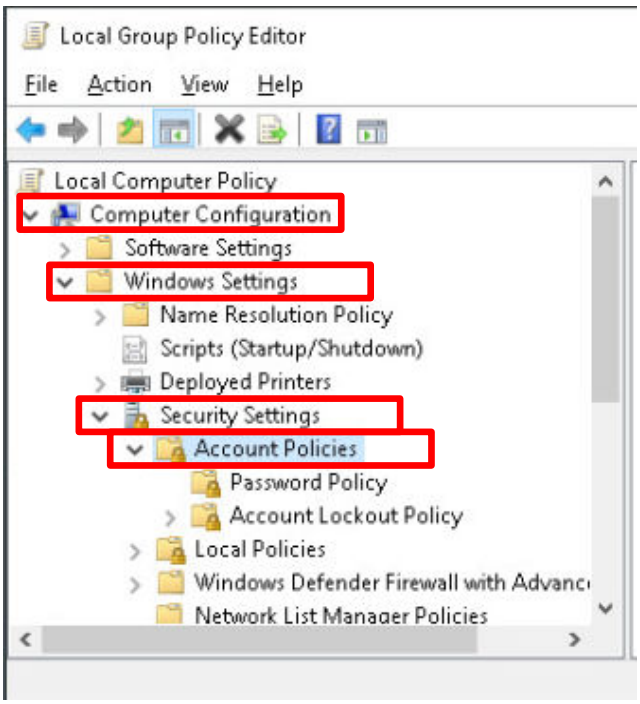


5. When the *Run* window appears, type `gpedit.msc` and click **OK**.



6. In the *Local Group Policy Editor* window, expand the following:

Computer Configuration
→Windows Settings
→Security Settings
→Account Policies



7. Then, click on the **Password Policy** object.

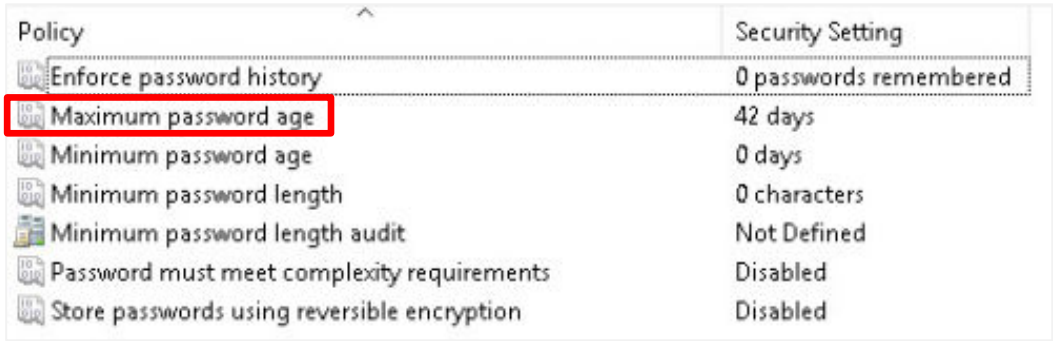
8. In the right pane, you will see all of the password policy settings. Use these settings to enforce stricter password policies. The settings that are most often changed (per company policy) are:

- **Enforce Password History**: The number of previous passwords that will be remembered before one can be reused.
- **Maximum Password Age:** How often (in days) a password change will be required.

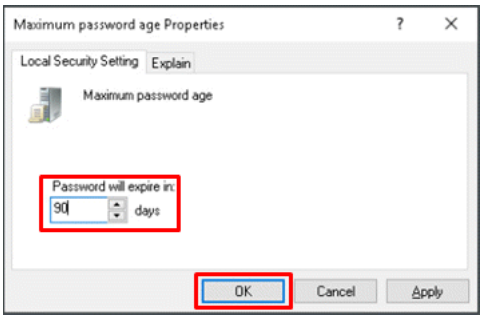
Password Must Meet Complexity Requirements

- Not contain the user's account name or parts of the full user's name that exceed two consecutive characters.
- Contain characters from three of the following five categories:
  - European uppercase characters (A-Z)
  - European lower case characters (a-z)
  - Base 10 digits (0-9)
  - Non-alphabetic characters (i.e. !@#$)
  - Any Unicode character categorized as alphabetic but isn't upper or lower case including Unicode characters from Asian languages

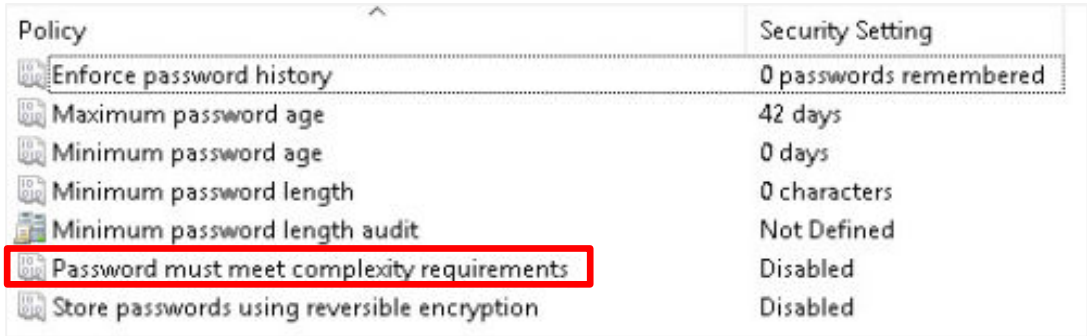
Double-click **Maximum Password Age**.



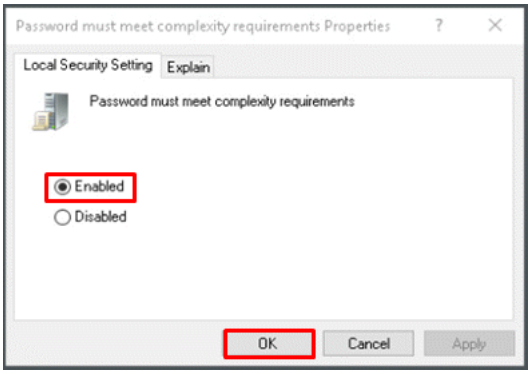
9. In the *Maximum password age Properties* window, change the value from `42` to `90` and click **OK**.



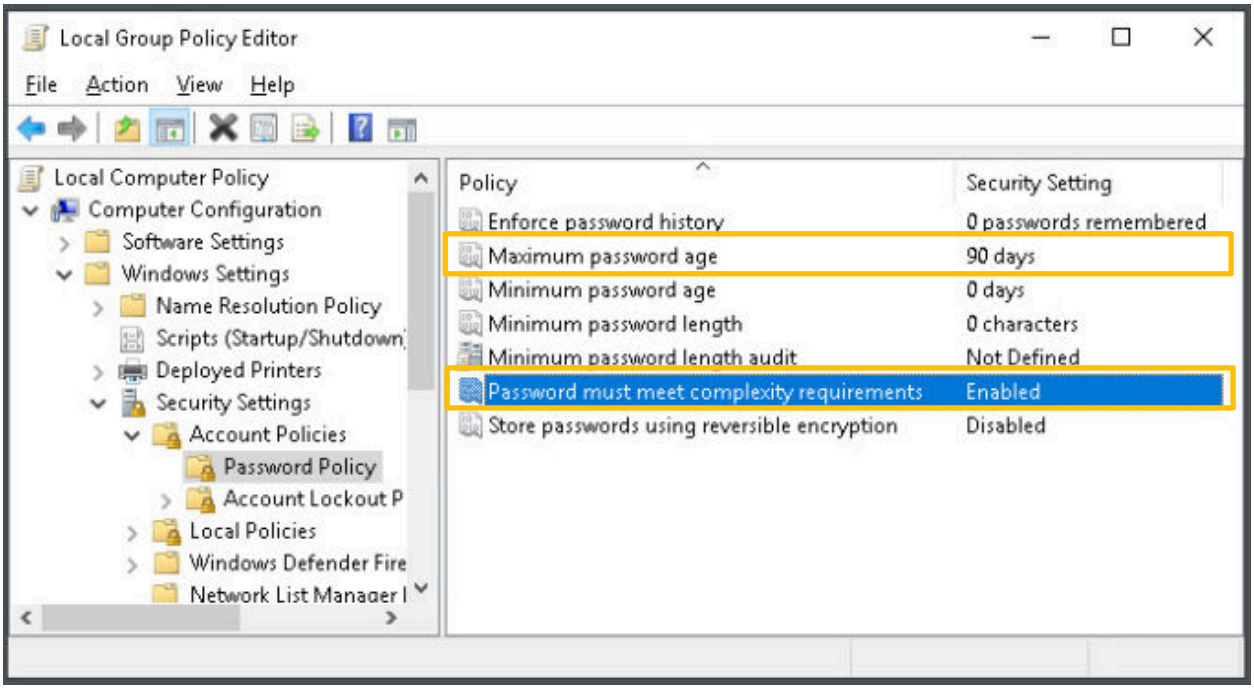
10. Double-click on **Password must meet complexity requirements**.



11. In the *Password must meet complexity requirements Properties* window, click the **Enabled** radio button and click **OK**.



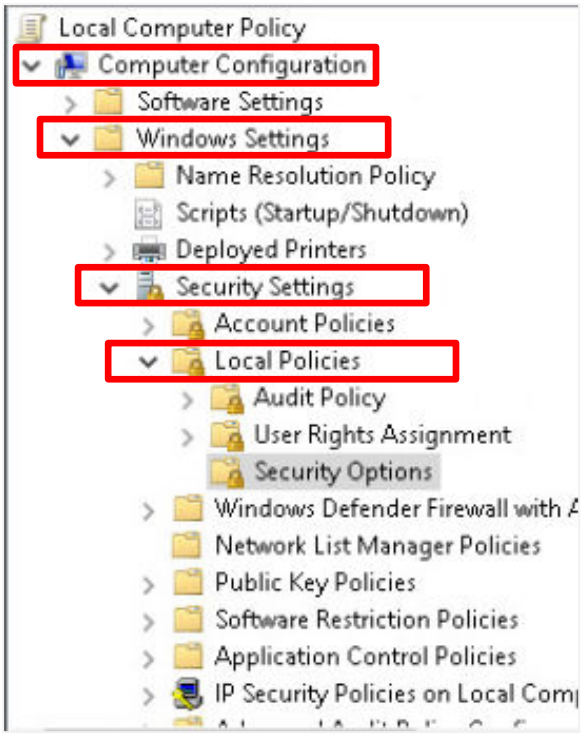
12. Review the policies you just created. Leave the *WinOS* computer on the *Local Group Policy Editor* for the next task.



1.2 Setup a Use Policy Consent Agreement

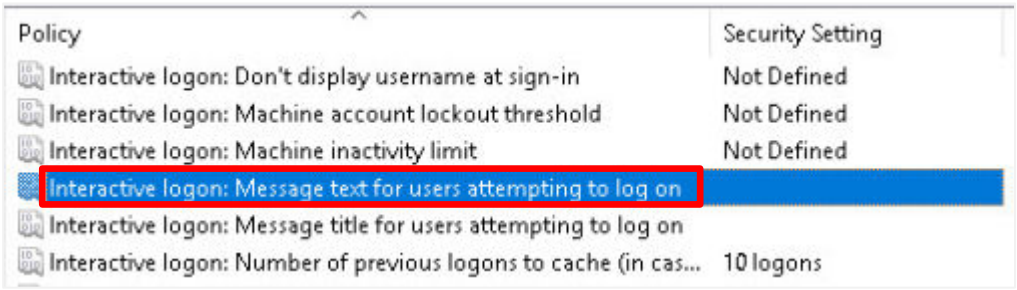
1. In the *Local Group Policy Editor* window, expand the following:

Computer Configuration
→Windows Settings
→Security Settings
→Local Policies



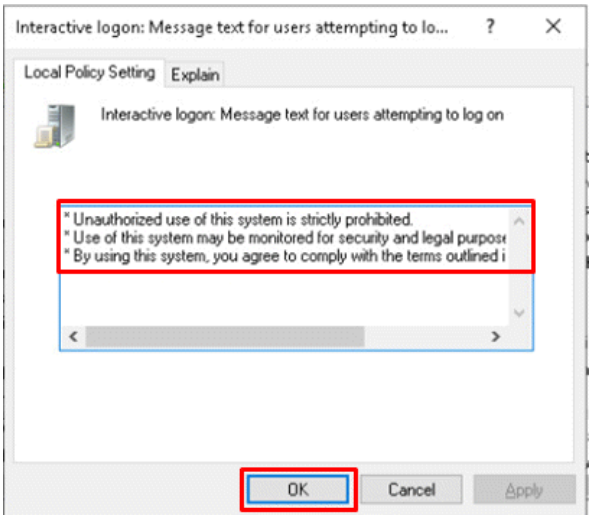
2. Then, click on the **Security Options** object.

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



4. In the *Interactive logon: Message text for users attempting to log on Properties* window, click in the text box, type the text below and then click **OK**.

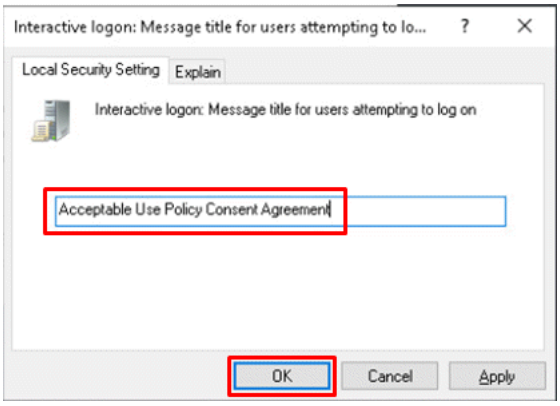
```
* Unauthorized use of this system is strictly prohibited.
* Use of this system may be monitored for security and legal purposes.
* By using this system, you agree to comply with the terms outlined in the
Acceptable Use Policy.
```



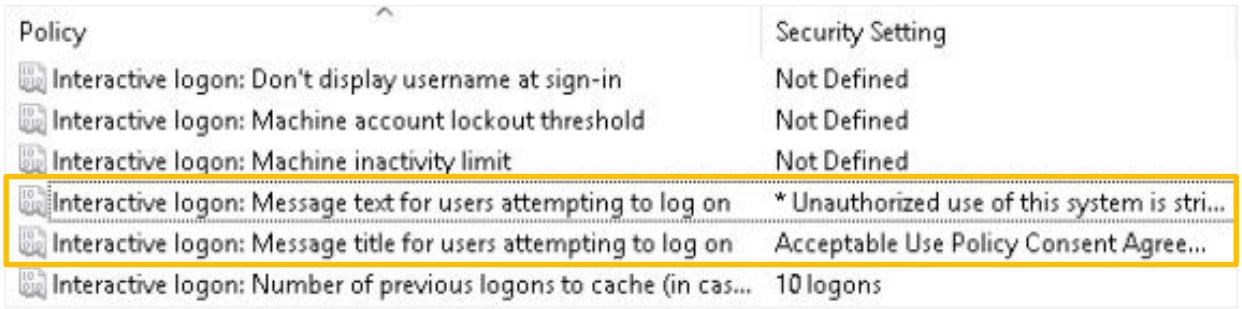
5. In the right pane, double-click **Interactive Logon: Message title for users attempting to log on**.

6. In the *Interactive logon: Message title for users attempting to log on Properties* window, click in the text box, type the text below, and then click **OK**.

   `Acceptable Use Policy Consent Agreement.`

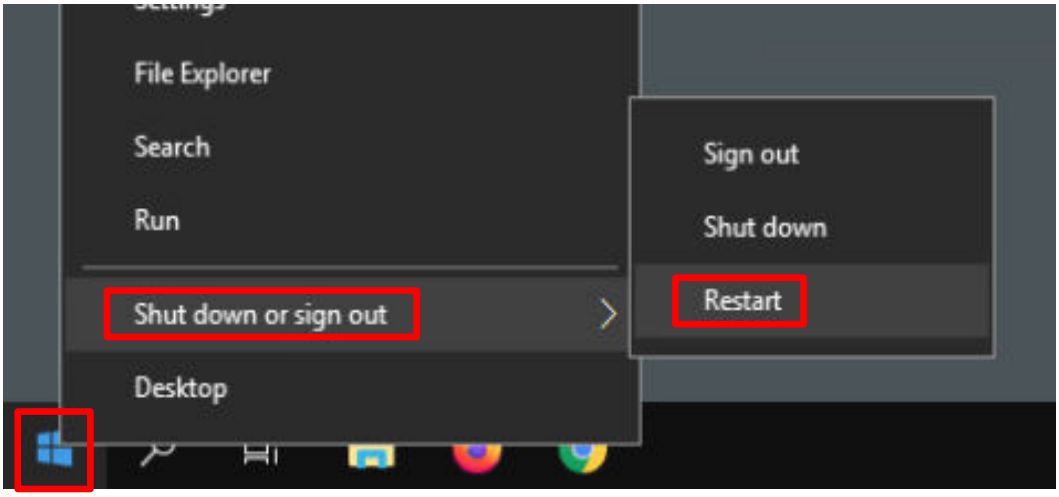


7. Review the settings for the policies you just created.

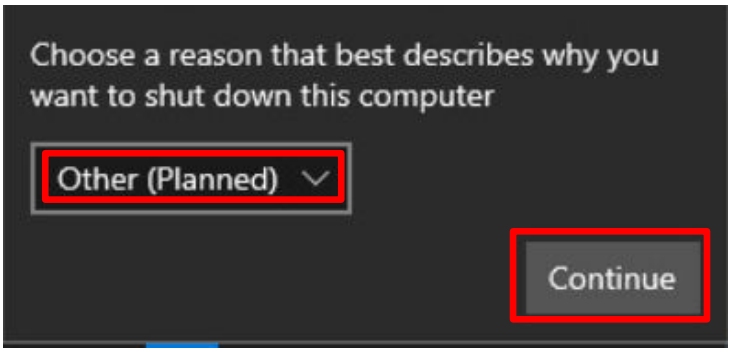


Policy	Security Setting
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	* Unauthorized use of this system is stri...
Interactive logon: Message title for users attempting to log on	Acceptable Use Policy Consent Agree...
Interactive logon: Number of previous logons to cache (in cas...	10 logons

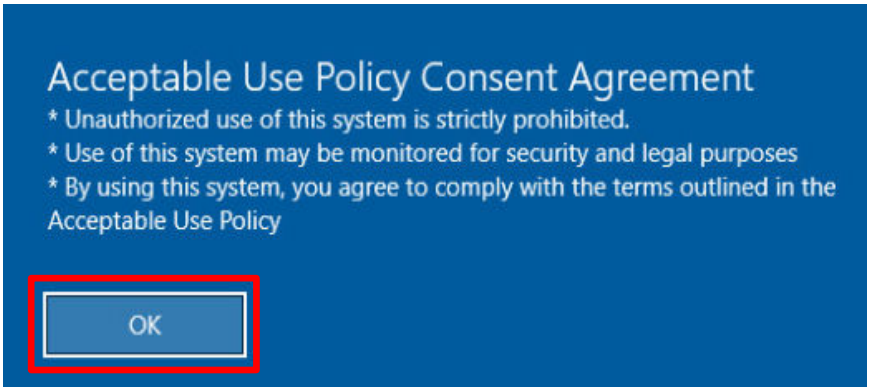
8. Close all windows.
9. In the taskbar, right-click the **Windows Start Button**, then click **Shut down or sign out,** then click **Restart.**



10. Click the list arrow and choose **Other (Planned)** and click **Continue**.



11. Once the computer restarts, send **Ctrl+Alt+Del** to the *WinOS* computer. You should see the *Acceptable Use Policy Consent Agreement.*



12. Click **OK** and log back in as `Administrator` using the password: **NDGlabpass123!**
13. Leave the *WinOS* computer open for the next task.

2 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.

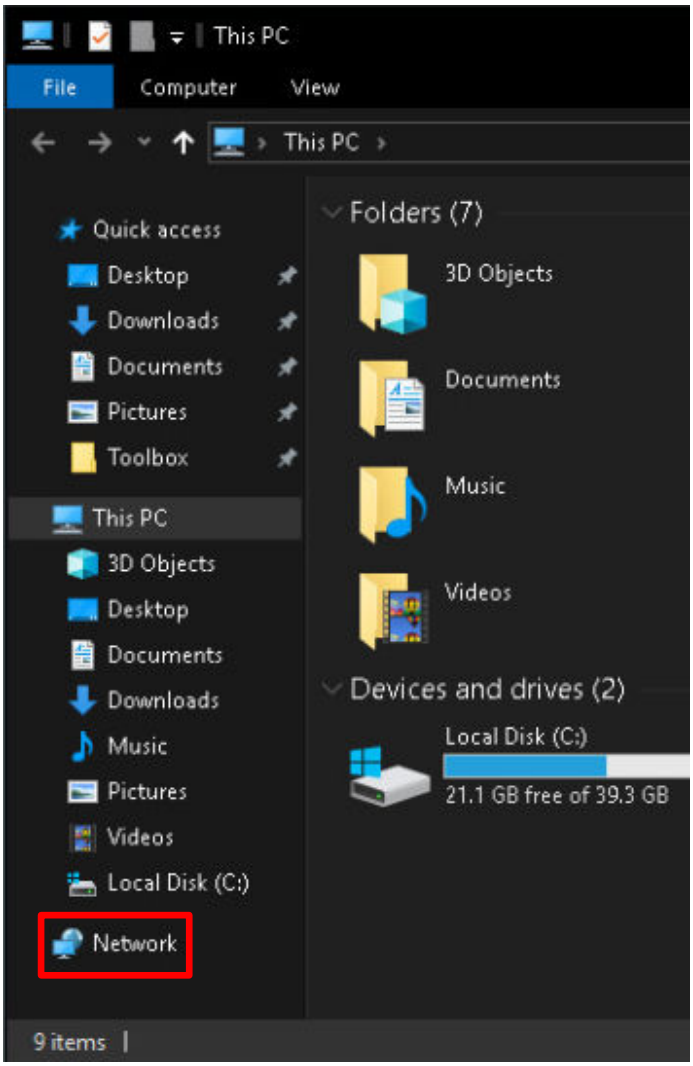
2.1 Set Windows Network to Private

One of the most important issues in cybersecurity is the balance between security and usability. It has been said, jokingly, that a truly secure computer is one that is never turned on. A critical part of a security analyst's job is to study an organization's IT environment and determine what the proper balance is between security and usability.

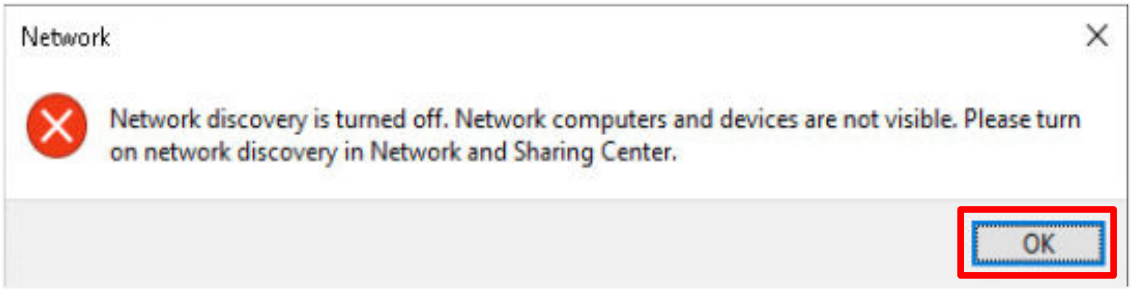
Windows systems tend to lean more toward security, especially in their approach to allowing connections from other computers. Windows has two network settings; *Public Networks* (which is the default) prevents Windows system's resources from being seen by other devices on the network, while *Private Networks* allows the Windows system to be discoverable and allow resource sharing. Windows computers on a LAN, especially servers, need to trust and be trusted by each other. You, as the security analyst, have determined that the *WinOS* computer, which is currently set to Public, needs to be changed to Private to allow computers on the LAN access to the server's resources.

1. Double-click on the **This PC** icon.

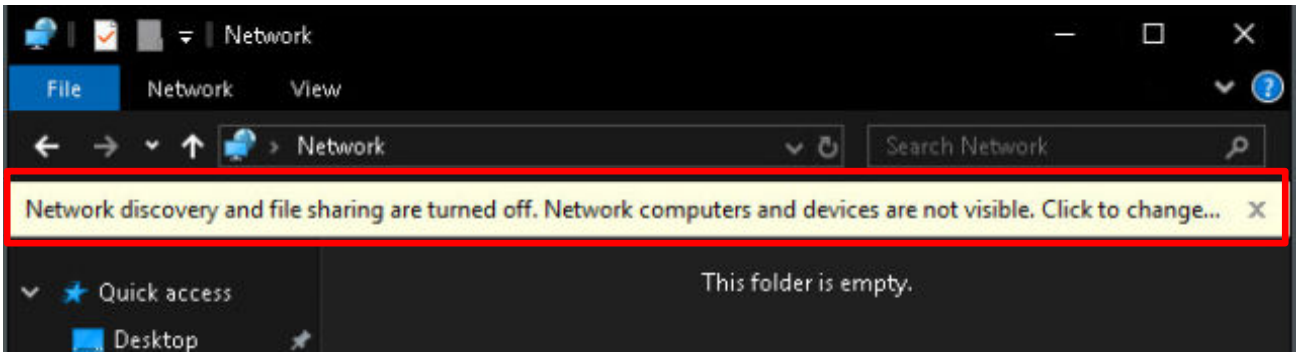
2. On the left side panel of the *File Explorer* window, click on the **Network** item.



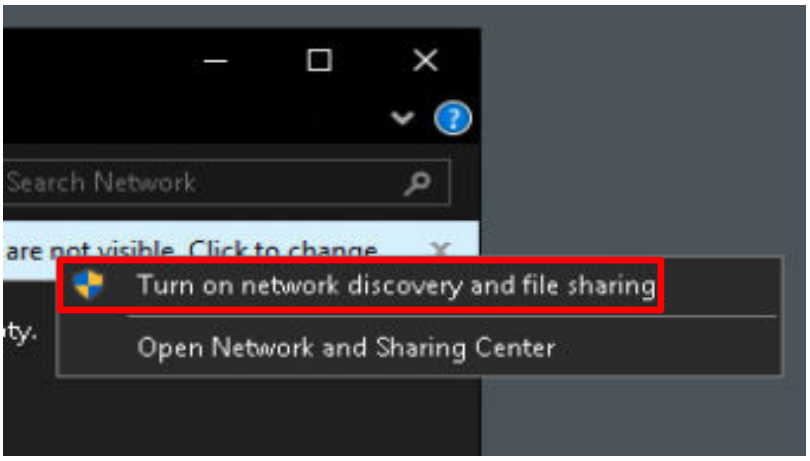
3. The *Network* warning box indicates that **Network Discovery is turned off**; click on the **OK** box.



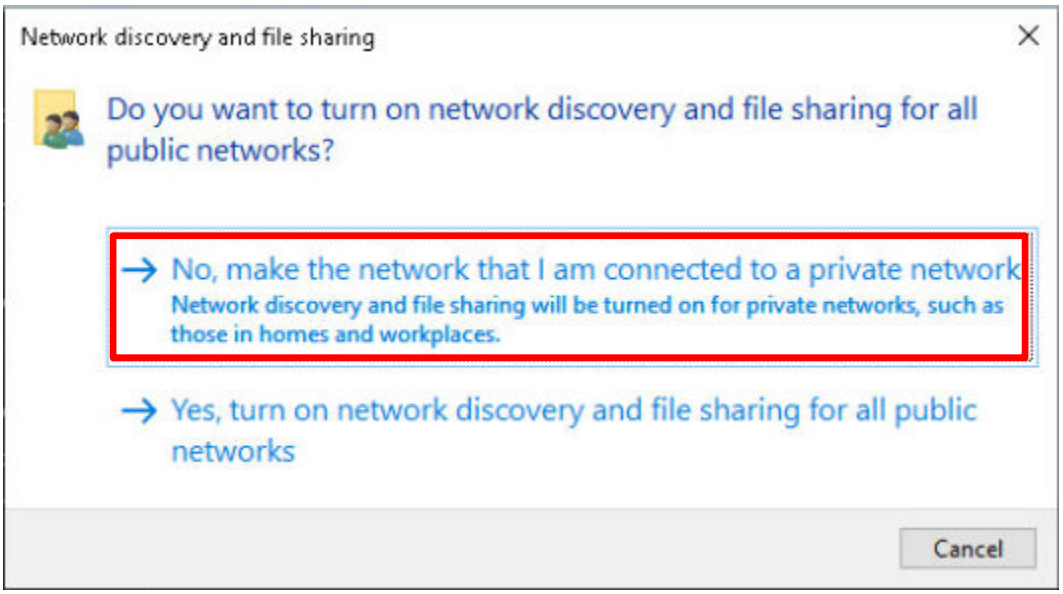
4. Click on the yellow settings change band at the top of the *File Explorer*.



5. In the popup window, click on **Turn on network discovery and file sharing**.



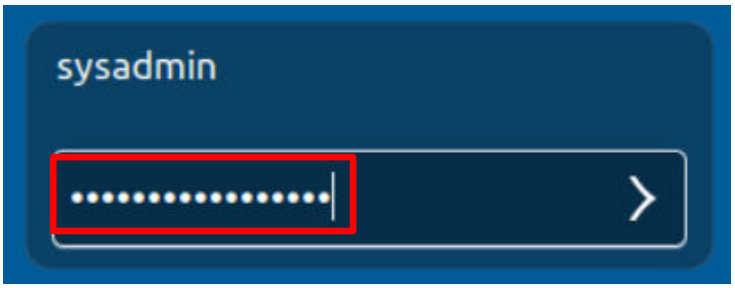
6. In the *Network Discovery and File Sharing* window, click on **No, make the network that I am connected to a private network.**



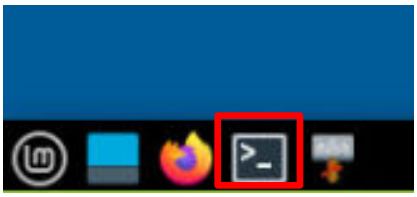
7. Close the **File Explorer** window.

2.2 Using the Windows Defender Firewall to Manage Resource Access

1. Set the focus to the **MintOS** computer.
2. Log in to the sysadmin using the password: `NDGlabpass123!`

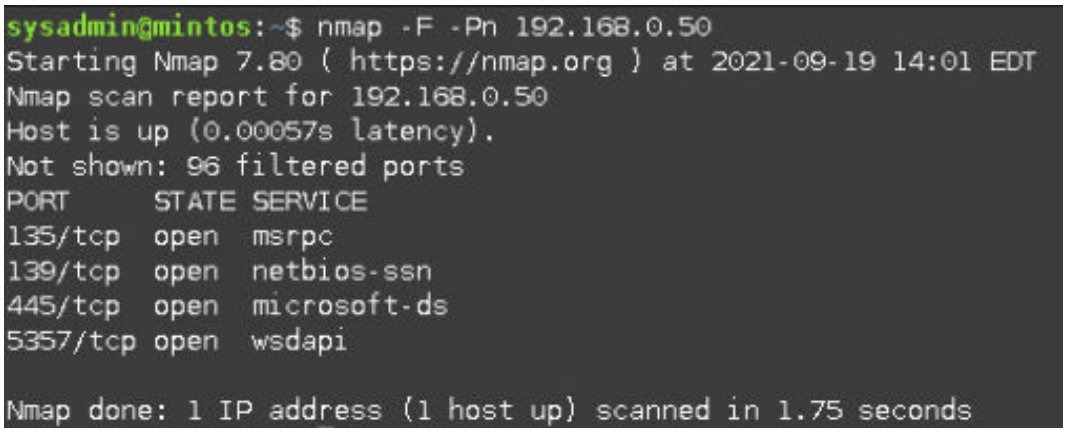


3. Click on the **Terminal** icon in the taskbar at the bottom of the screen.



4. Scan the *WinOS* computer at **192.168.0.50** using *nmap* by typing the command:

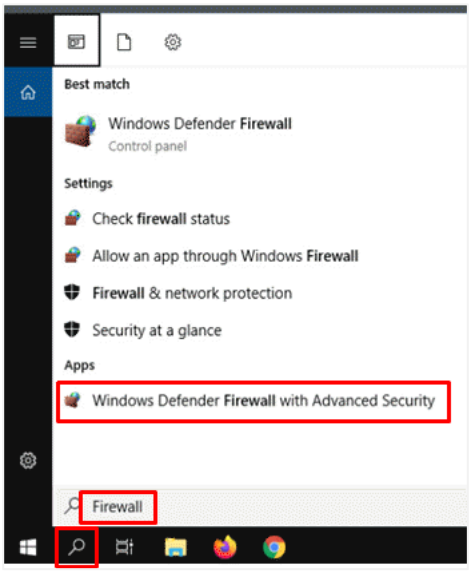
```
nmap -F -Pn 192.168.0.50
```



```
sysadmin@mintos:~$ nmap -F -Pn 192.168.0.50
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-19 14:01 EDT
Nmap scan report for 192.168.0.50
Host is up (0.00057s latency).
Not shown: 96 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

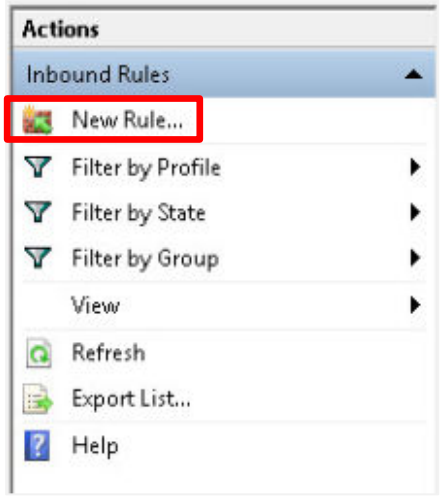
5. From the results given, you can see that the **WinOS** computer has several ports open. For this lab, you will focus on ports **135** and **139**.
6. Return to the **WinOS** computer.

7. Click on the **Search** icon in the taskbar and type `Firewall` to bring up a list of options. These options will automatically populate in the search list as you type. Click on **Windows Defender Firewall with Advanced Security**.

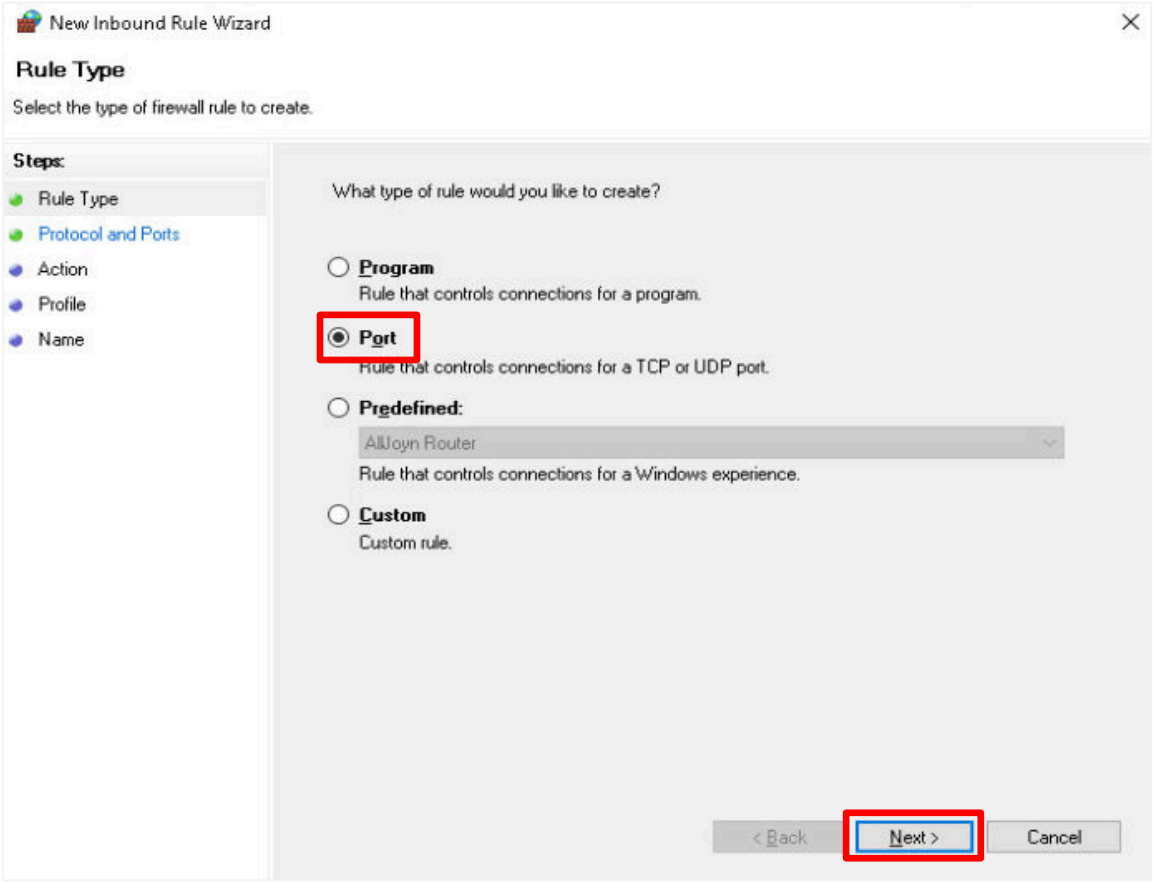


8. You will see the *Windows Defender Firewall with Advanced Security* screen. Click on **Inbound Rules** in the left pane.

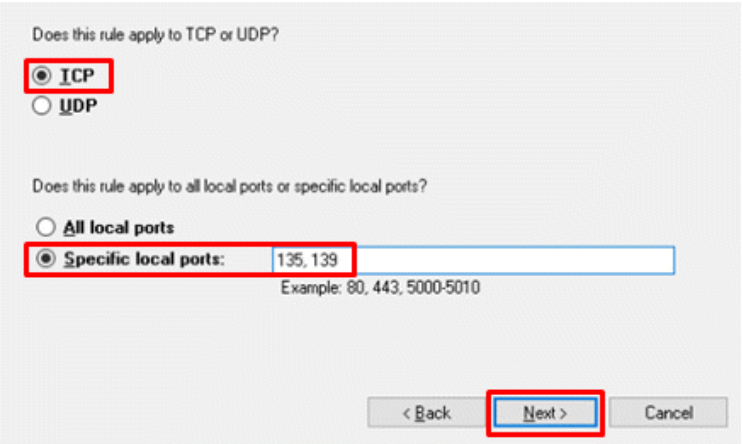
9. In the *Actions* pane located to the right, click on **New Rule.**



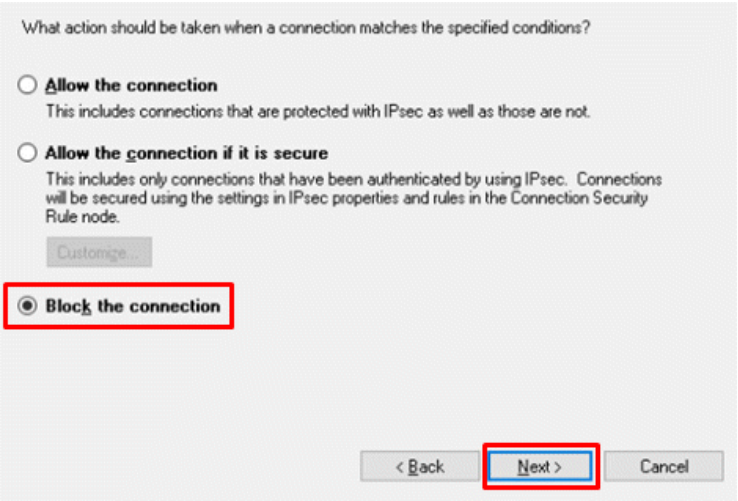
10. In the *New Inbound Rule Wizard,* click the **Port** radio button, then click the **Next** button.



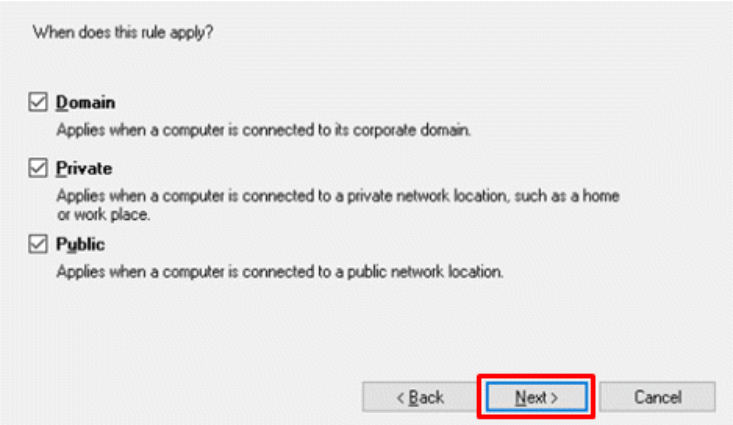
11. Click the **TCP** radio button followed by the **Specific local ports** radio button and, type 135**, 139** into the field, then click **Next**.



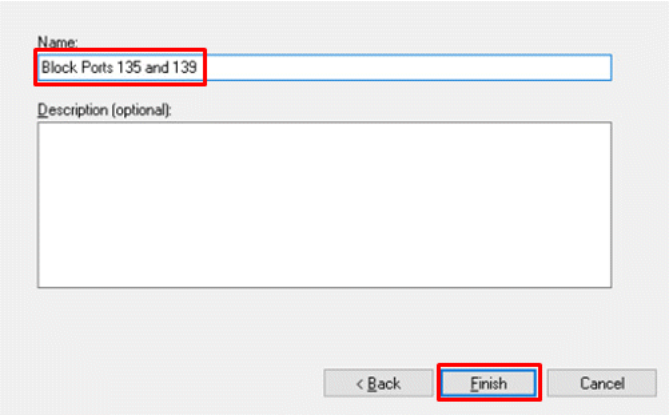
12. Click **Block the connection**, followed by **Next**.



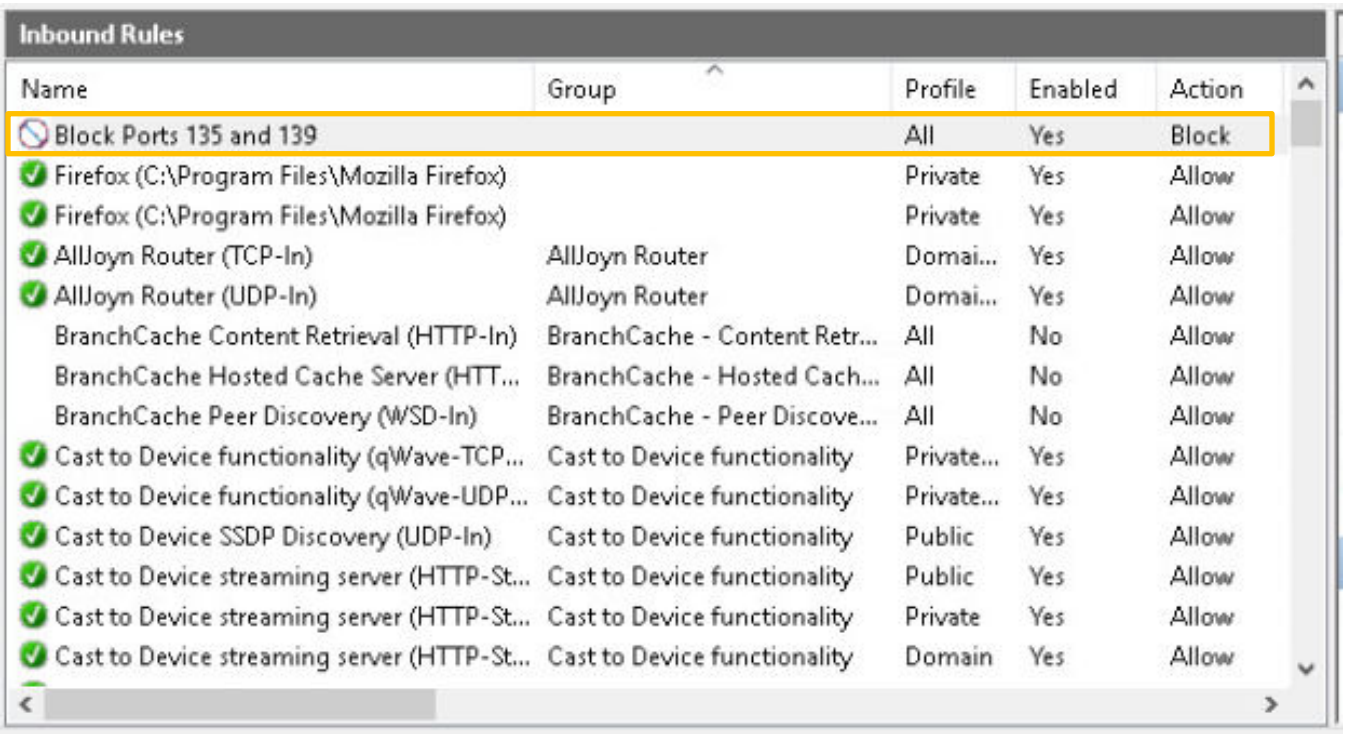
13. On the *When does this rule apply?* step, leave all three options checked and click **Next**.



14. In the *Name* field, type `Block Ports 135 and 139` and then click **Finish**.



15. You will see the new rule in the *Inbound Rules* window.

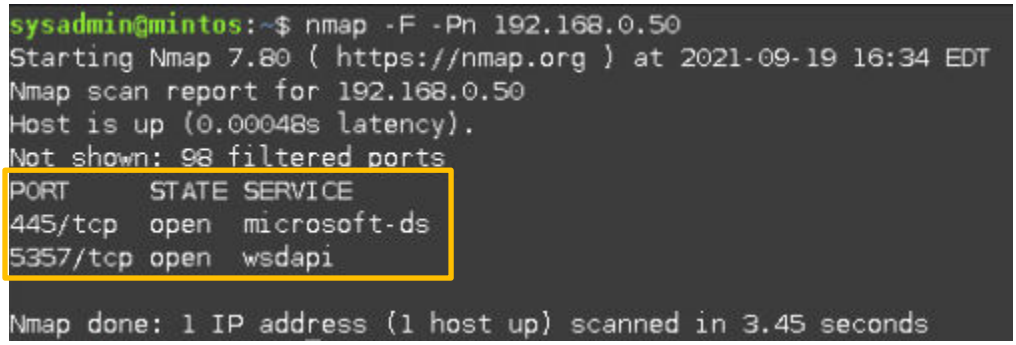


Name	Group	Profile	Enabled	Action
Block Ports 135 and 139		All	Yes	Block
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes	Allow
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes	Allow

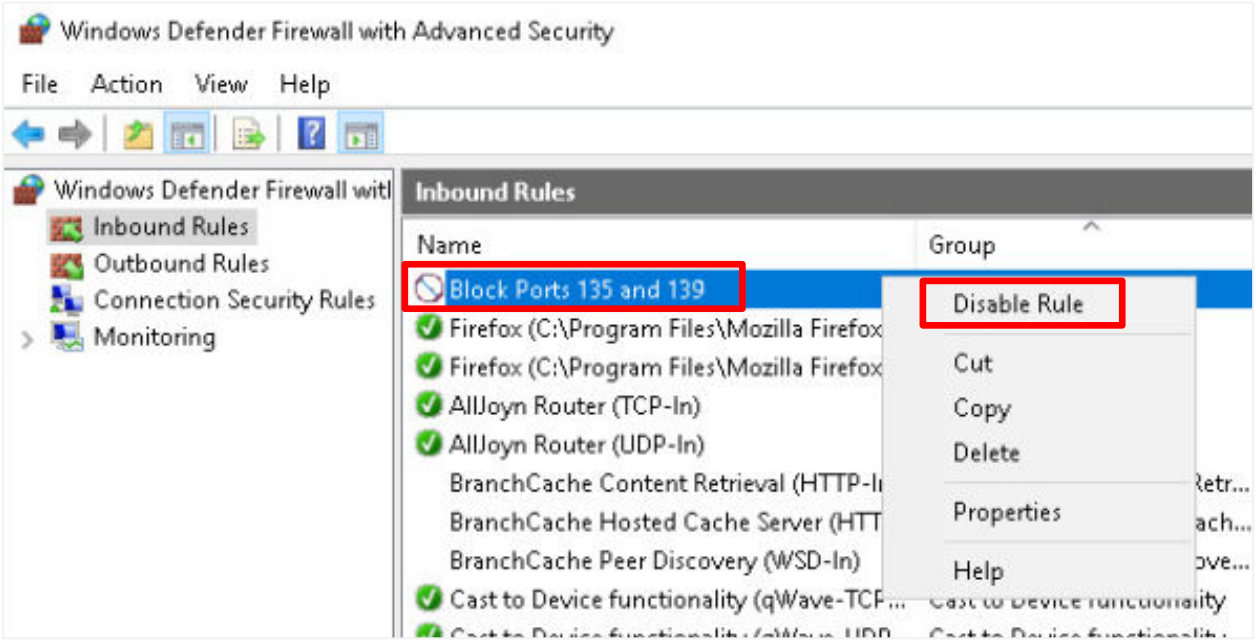
16. Return to the **MintOS** computer.

17. In the terminal window, repeat the *nmap* command. Notice in the results that ports **135** and **139** are no longer open.

```
nmap –F –Pn 192.168.0.50
```



18. Return to the **WinOS** computer. The *Windows Defender Firewall with Advanced Security* window should still be open. Right-click on the **Block Ports 135 and 139** rule, and select **Disable Rule**.



19. Close the **Windows Defender Firewall with Advanced Security** window on the *WinOS* computer.
20. Return to the **MintOS** computer.

21. In the terminal window, repeat the *nmap* command. Notice in the results that ports **135** and **139** are open.

```
nmap -F -Pn 192.168.0.50
```

```
sysadmin@mintos:~$ nmap -F -Pn 192.168.0.50
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-10 14:26 EDT
Nmap scan report for 192.168.0.50
Host is up (0.00040s latency).
Not shown: 96 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds
```

22. Remain on the terminal window on the *MintOS* computer and continue to the next task.

2.3 Using the Kill Command in Linux to Stop Listening on Ports

1. Set the focus on the **MintOS** computer.
2. In the terminal window, use the *nmap* command to scan the **UbuntuSRV** computer at **172.16.1.10** using the following command:

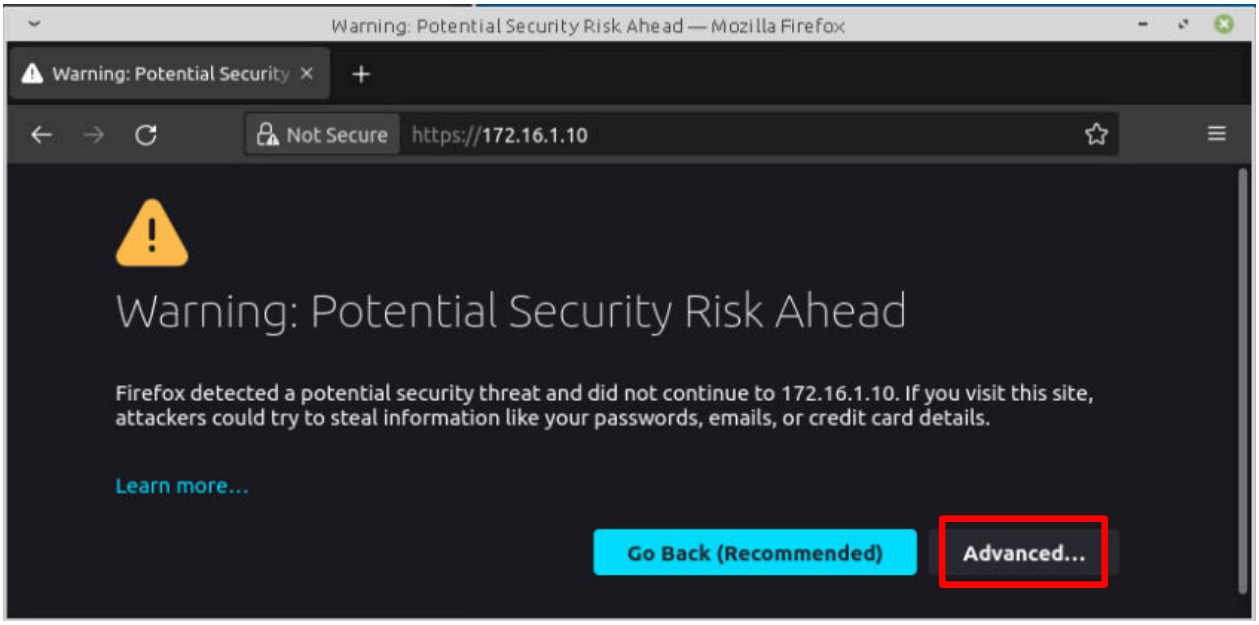
```
nmap -F -Pn 172.16.1.10
```

```
sysadmin@mintos:~$ nmap -F -Pn 172.16.1.10
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-19 16:46 EDT
Nmap scan report for 172.16.1.10
Host is up (0.00042s latency).
Not shown: 97 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

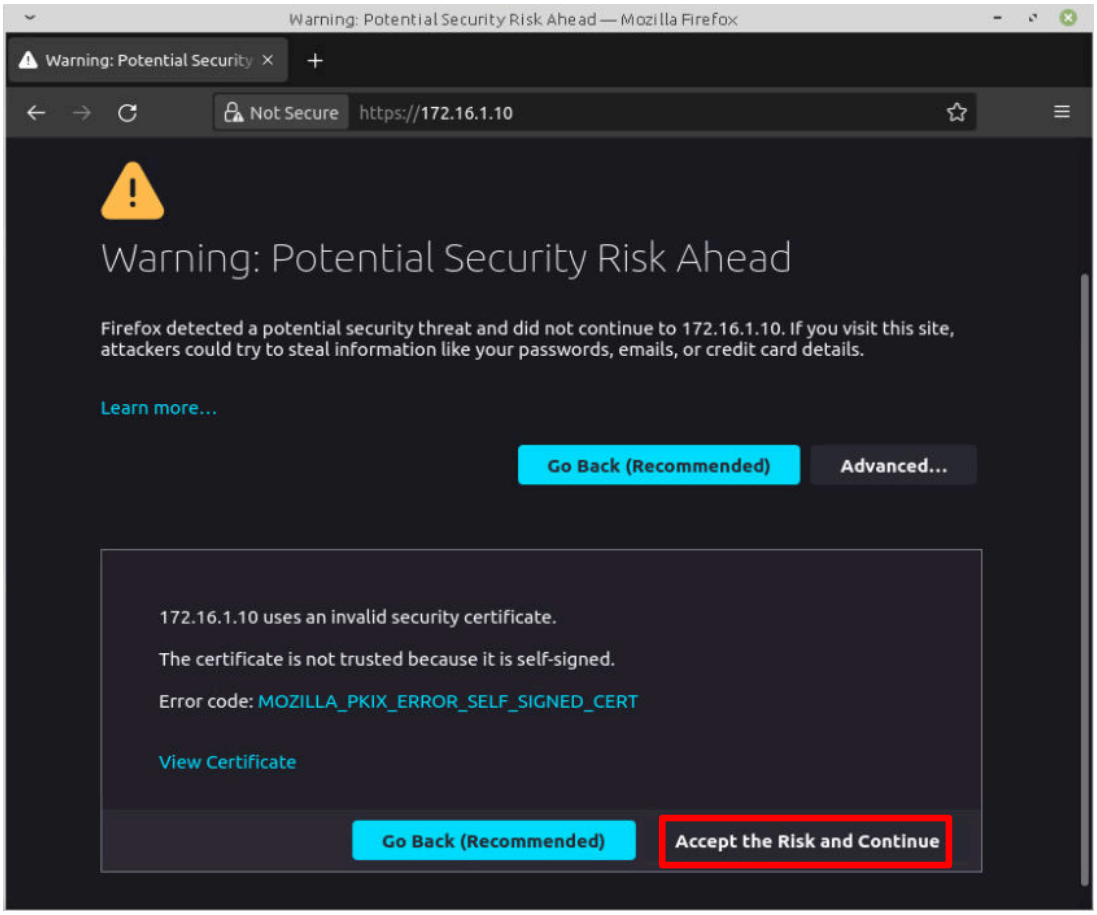
From the results, you can see that **Port 22** (for SSH), **Port 80** (for HTTP) and **Port 443** (for HTTPS) are open.

3. Connect to the web server setup on the **UbuntuSRV** computer. Open **Firefox** by clicking the icon on the bottom taskbar.

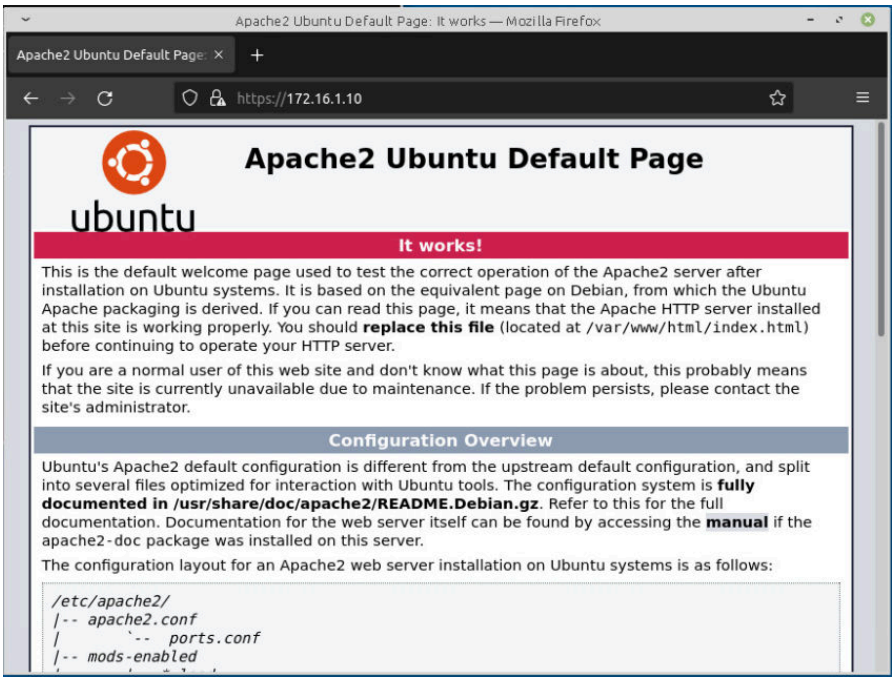
4. In the browser window, type the address `https://172.16.1.10`. On the *Warning* window, click the **Advanced** button.



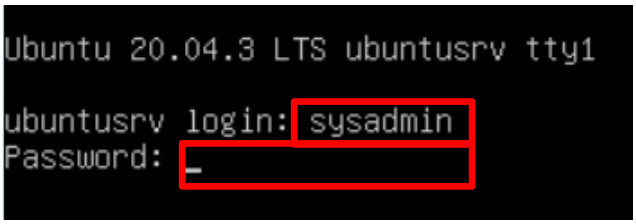
5. The *Warning* window will expand (you may have to scroll the window down to see the message), saying that 172.16.1.10 is not trusted because it uses a self-signed certificate. Click on **Accept the Risk and Continue.**



6. You will then see the *Apache2 Default* web page.



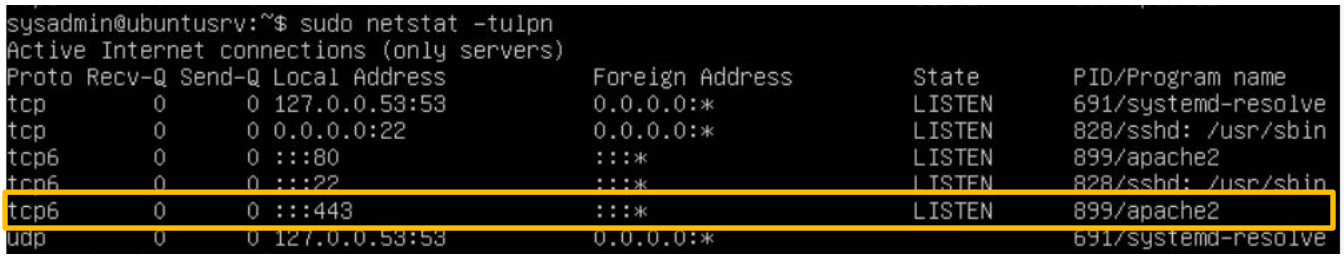
7. Close the browser window.
8. Set the focus to the **UbuntuSRV** and log in as `sysadmin` with the password: `NDGlabpass123!`



9. If there are open ports on the *UbuntuSRV* machine, there is likely a process actively listening on them. To discover what this process is, type the following command, using the password `NDGlabpass123!` if prompted.

```
sudo netstat -tulpn
```

10. Notice that the process using **Port 443** is **apache2** (the web server); also note the **PID,** which is **899** (the PID value will be different every time you run the lab).



11. To stop this port from listening, use the **kill** command using the **PID** for the **apache2** webs server with the following command (replace 899 with the value of the PID in your output):

```
sudo kill 899
```

```
sysadmin@ubuntusrv:~$ sudo kill 899
sysadmin@ubuntusrv:~$
```

12. Return to the **MintOS** computer.
13. In the terminal window, use the *nmap* command to scan the **UbuntuSRV** computer again using the following command:

```
nmap -F -Pn 172.16.1.10
```

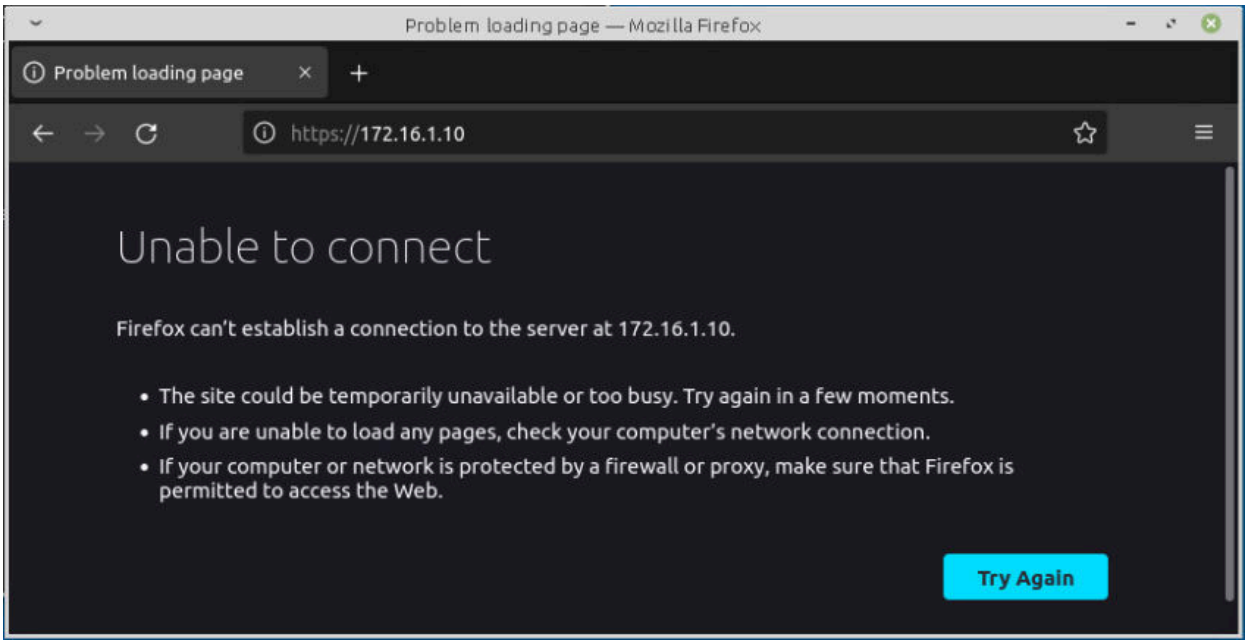
```
sysadmin@mintos:~$ nmap -F -Pn 172.16.1.10
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-19 17:15 EDT
Nmap scan report for 172.16.1.10
Host is up (0.00024s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

14. Notice that **Port 80** and **Port 443** are no longer open.

Port 80 is also closed since it is **HTTP** and uses the same **PID** as Port 443

15. To make sure the port is really closed, try opening the **Apache2** web page. Open **Firefox** by clicking the icon in the bottom taskbar.

16. In the browser window, type the address `https://172.16.1.10`.



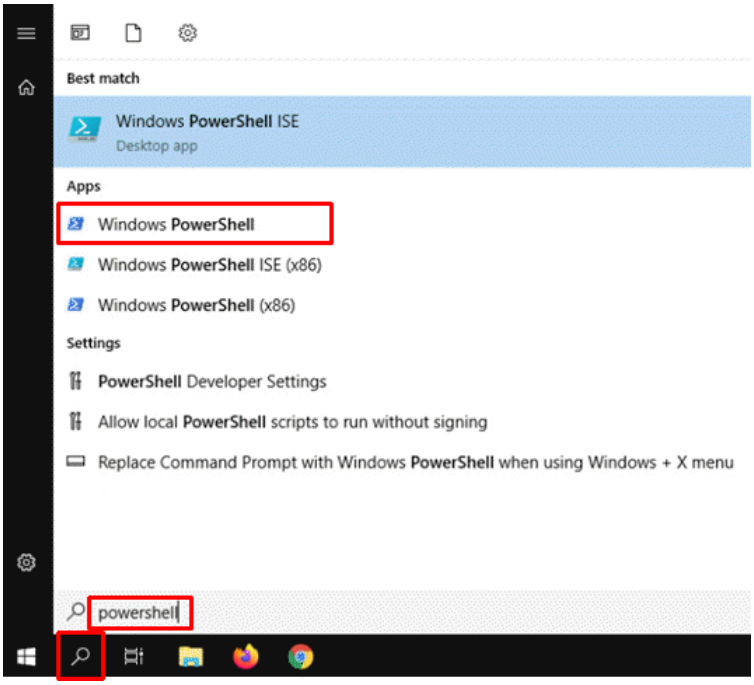
You can see that the HTTPS service has been terminated.

17. Close all open windows on the **MintOS** computer.

3 Apply Patches to Windows Servers

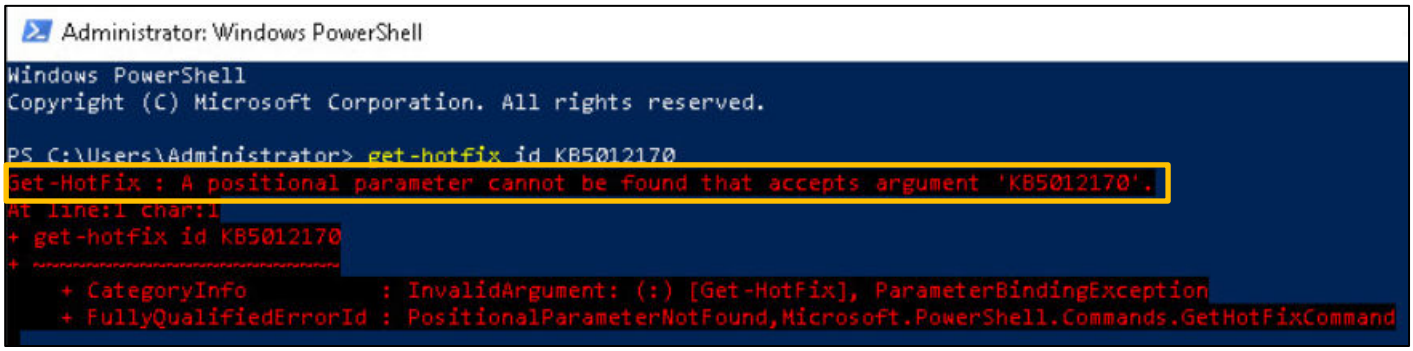
Microsoft has issued a security update that "Updates an issue that prevents you from changing a password that has expired when you sign in to a Windows device." The patch is identified as April 12, 2022—KB5012647 (OS Build 17763.2803). You need to check to see if the patch has been installed, and if not, you will need to apply it to the *WinOS* computer.

1. Set the focus to the **WinOS** computer.
2. Click on the **Search** icon in the taskbar, then type `powershell` to bring up a list of options. These options will automatically populate in the search list as you type. Click on **Windows PowerShell** under *Apps*.



3. At the *PowerShell* prompt, check to see if the update you want to install is currently installed, using the following command:

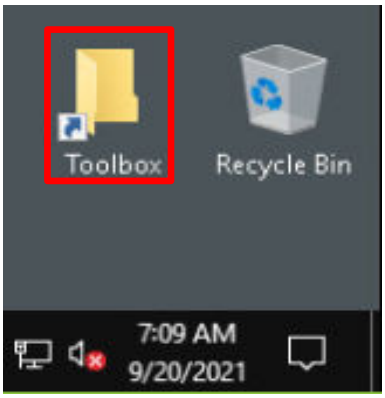
```
get-hotfix -id KB5012170
```



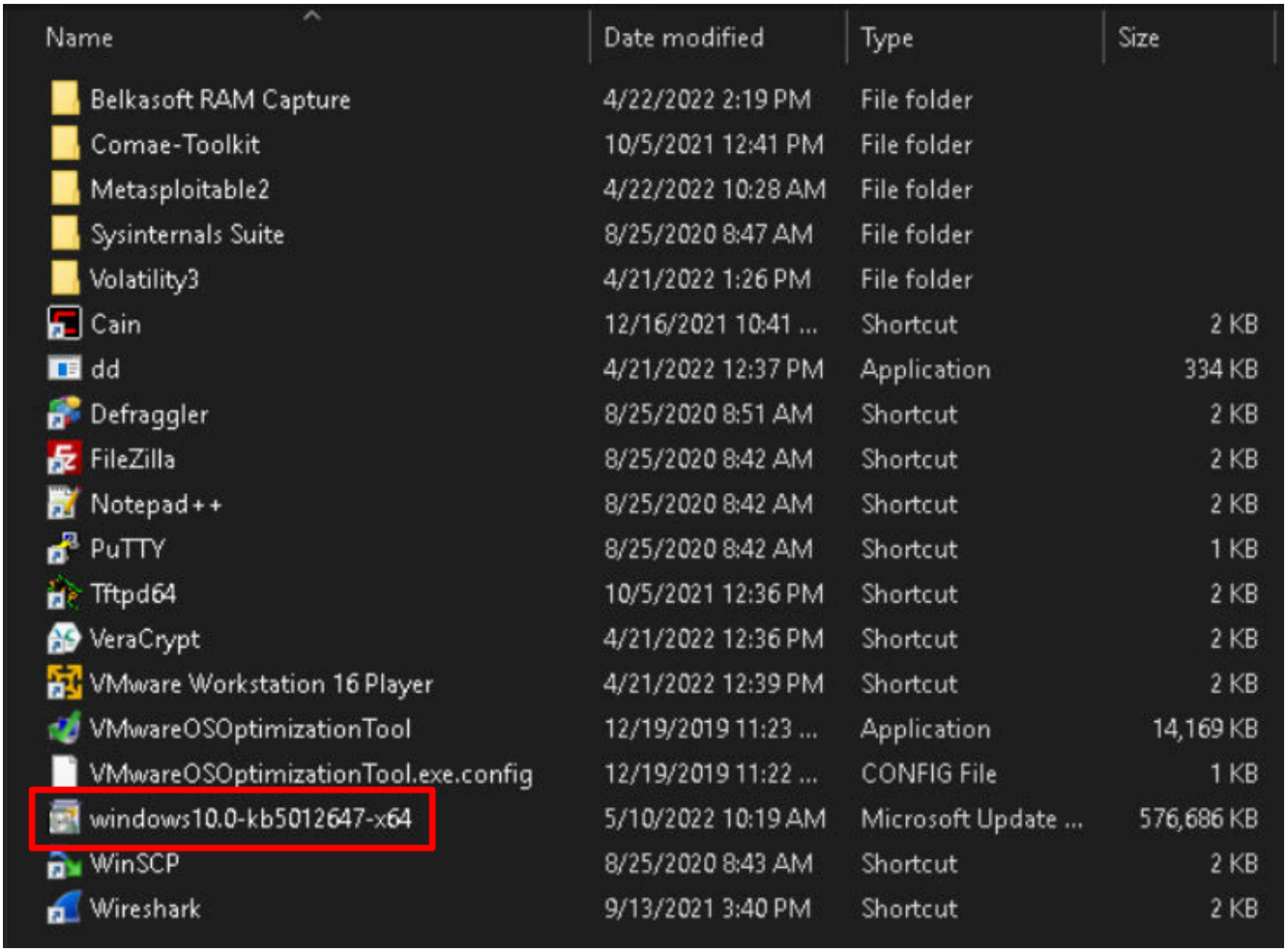
Note that no hotfix can be found. The patch has not yet been installed

At this point, the update patch, *KB5012170*, would need to be downloaded from Microsoft. Since there is no internet access, the patch has already been downloaded and saved in the Toolbox folder on the *WinOS* computer's desktop.

4. Minimize the *Powershell* window. On the **WinOS** computer's desktop, double-click the **Toolbox** folder.

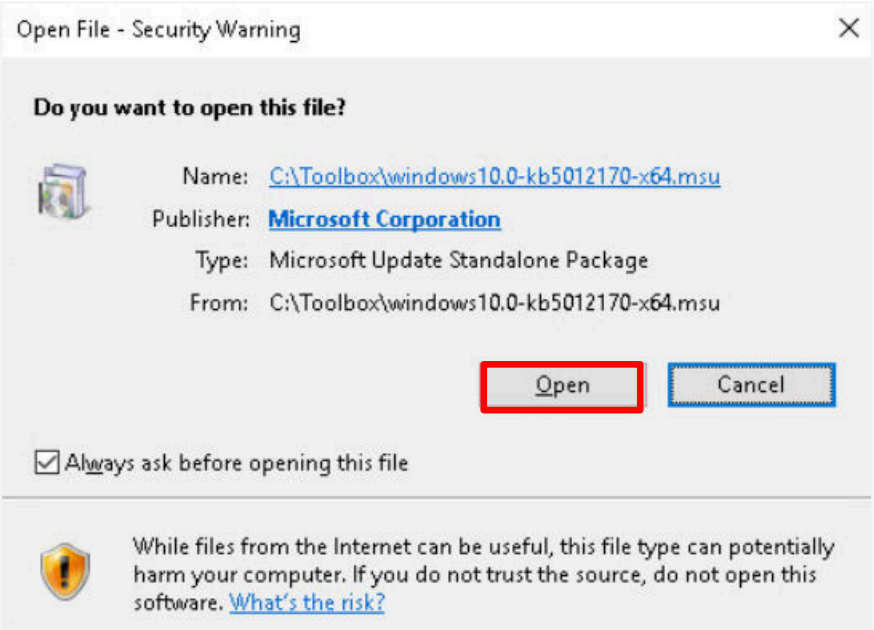


5. Double-click on **Windows10.0-kb5012170-x64** to install the update you just searched for in *PowerShell*.

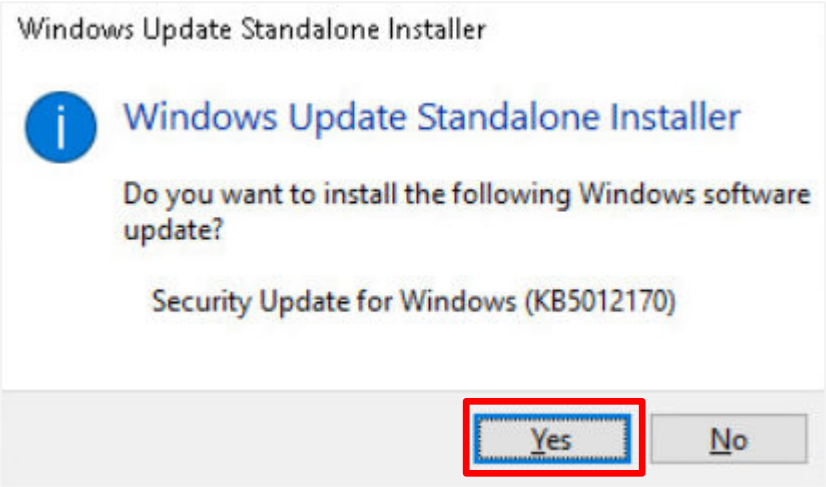


Name	Date modified	Type	Size
Belkasoft RAM Capture	4/22/2022 2:19 PM	File folder	
Comae-Toolkit	10/5/2021 12:41 PM	File folder	
Metasploitable2	4/22/2022 10:28 AM	File folder	
Sysinternals Suite	8/25/2020 8:47 AM	File folder	
Volatility3	4/21/2022 1:26 PM	File folder	
Cain	12/16/2021 10:41 ...	Shortcut	2 KB
dd	4/21/2022 12:37 PM	Application	334 KB
Defraggler	8/25/2020 8:51 AM	Shortcut	2 KB
FileZilla	8/25/2020 8:42 AM	Shortcut	2 KB
Notepad++	8/25/2020 8:42 AM	Shortcut	2 KB
PuTTY	8/25/2020 8:42 AM	Shortcut	1 KB
Tftpd64	10/5/2021 12:36 PM	Shortcut	2 KB
VeraCrypt	4/21/2022 12:36 PM	Shortcut	2 KB
VMware Workstation 16 Player	4/21/2022 12:39 PM	Shortcut	2 KB
VMwareOSOptimizationTool	12/19/2019 11:23 ...	Application	14,169 KB
VMwareOSOptimizationTool.exe.config	12/19/2019 11:22 ...	CONFIG File	1 KB
windows10.0-kb5012647-x64	5/10/2022 10:19 AM	Microsoft Update ...	576,686 KB
WinSCP	8/25/2020 8:43 AM	Shortcut	2 KB
Wireshark	9/13/2021 3:40 PM	Shortcut	2 KB

6. On the *Open File – Security Warning* popup window, click **Open**.



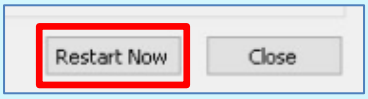
7. When asked to confirm the installation, click the **Yes** button.



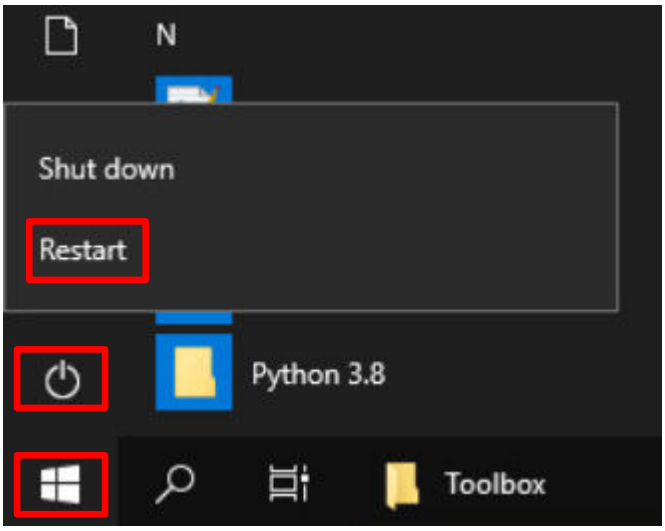
Larger updates take extended periods of time to install. This update takes about 5 minutes.

8. Once the update has been installed, you will be prompted to restart the machine. Click **Close**.

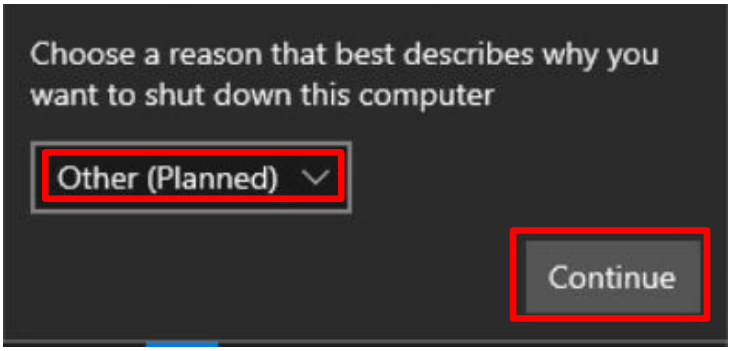
This update does not require a reboot. Some updates will require that the computer be rebooted and instead of the *Close* button, it will have a *Restart Now* button. But it is a good idea to reboot a Windows computer after an update.



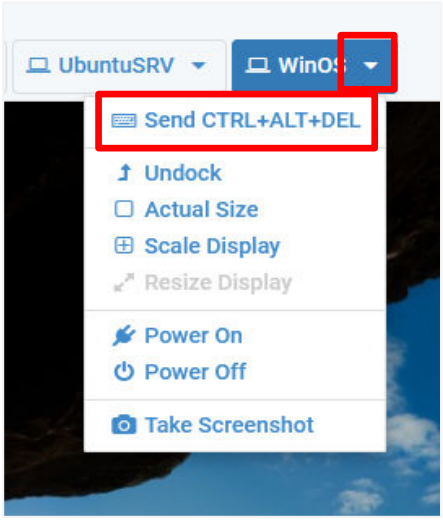
9. Click on the **Windows Start** button, then click on the **On/Off** icon and select **Restart**.



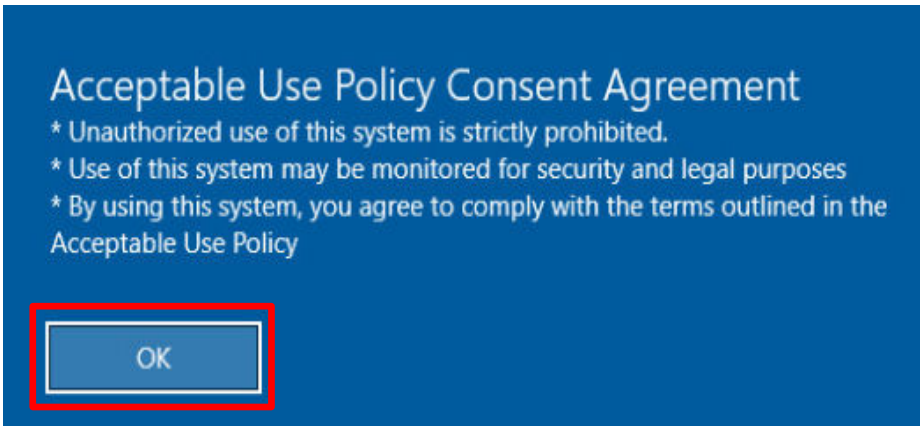
14. Click the list arrow and choose **Other (Planned)** and click **Continue**.



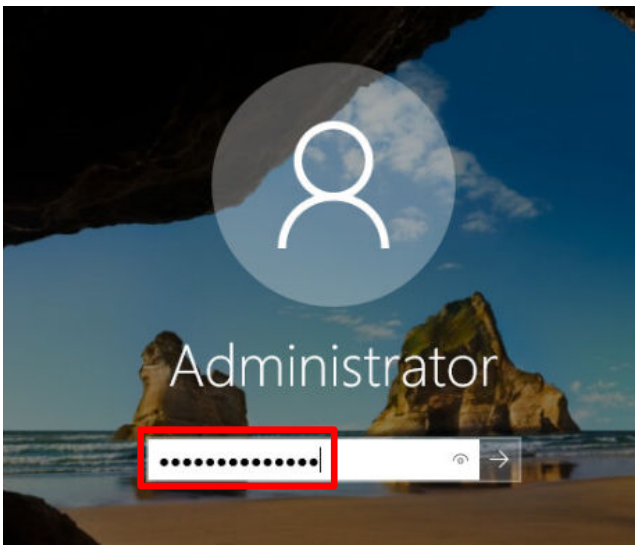
13. Bring up the login window by sending a Ctrl + Alt + Delete. To do this, click the **WinOS** dropdown menu and click **Send CTRL+ALT+DEL**.



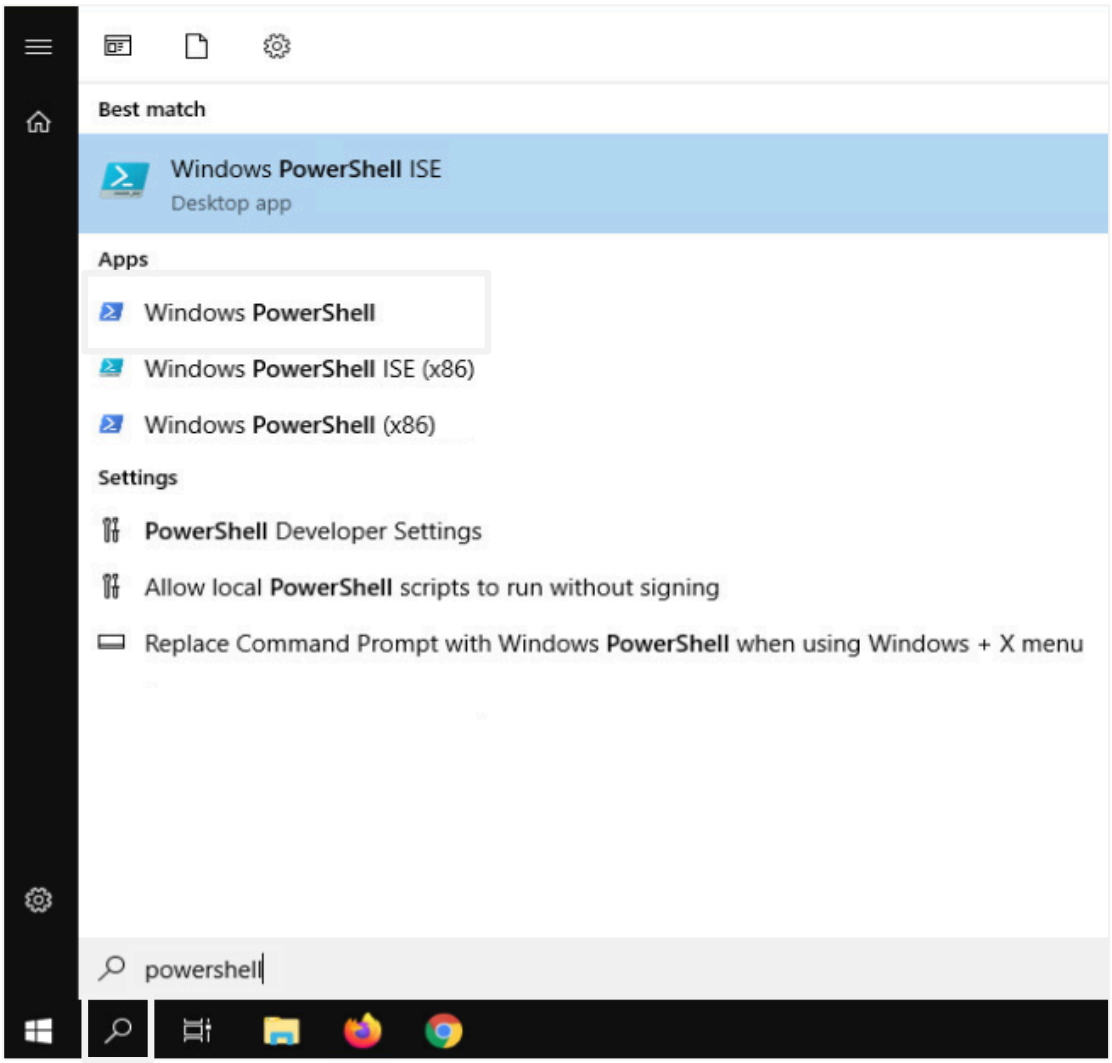
14. You should see the *Acceptable Use Policy Consent Agreement.* Click **OK.**



15. Log back in as **Administrator** using the password: **NDGlabpass123!**



10. Click on the **Search** icon in the taskbar. Type `powershell` to bring up a list of options. These options will automatically populate in the search list as you type. Click on **Windows PowerShell** under *Apps*.



11. At the *PowerShell* prompt, check to see if the patch was installed by typing the following command.

```
get-hotfix -id KB5012170
```

Notice the update has been installed. Close the **PowerShell** window.

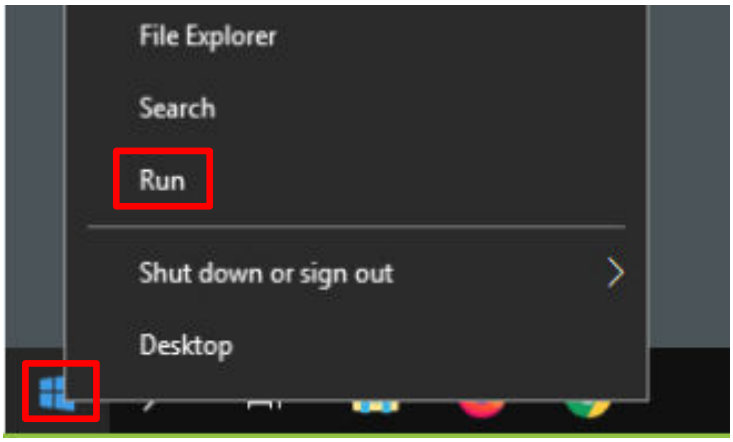
```
PS C:\Users\Administrator> get-hotfix -id KB5012170

Source        Description      HotFixID      InstalledBy          InstalledOn
WIN-E3AIDI... Security Update  KB5012170     WIN-E3AIDIHECNG\A... 8/10/2022 12:00:00 AM
```

12. Remain on the *WinOS* computer for the next task.

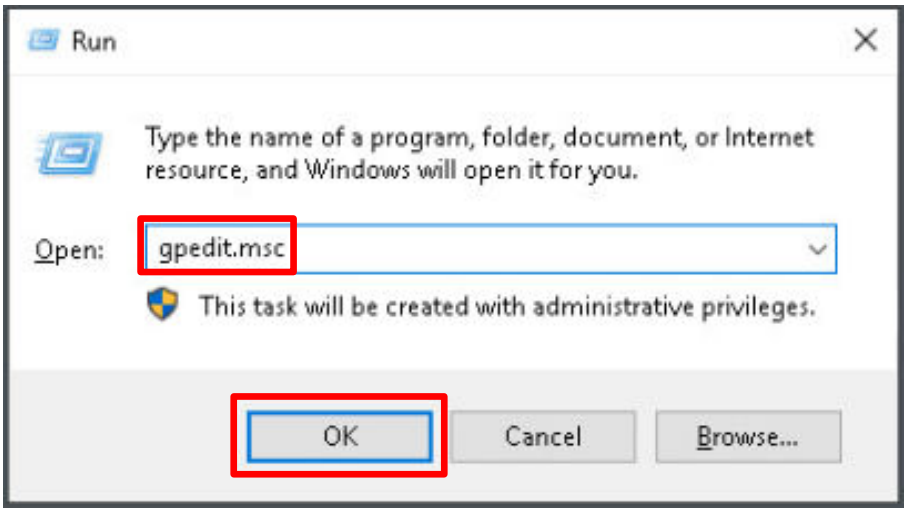
4 Using Windows Defender to Increase Security

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

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

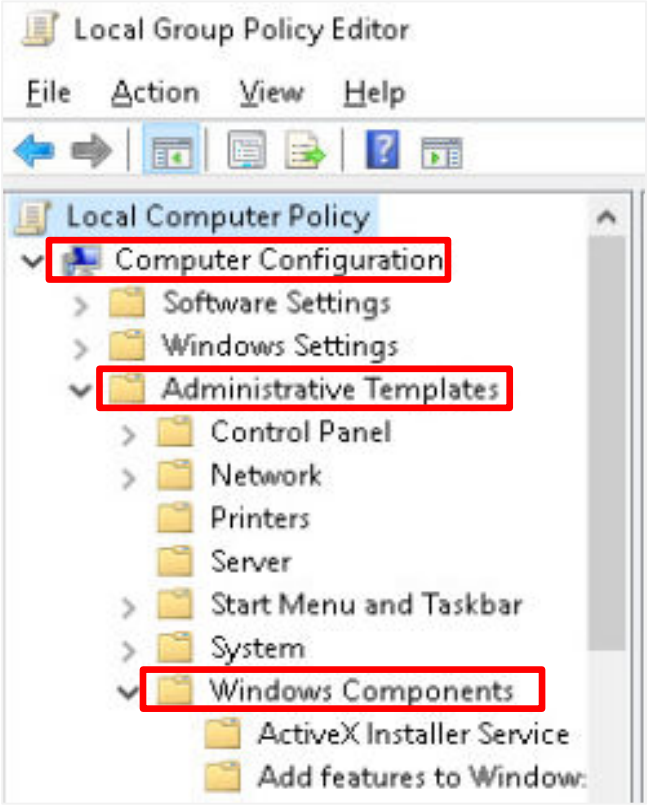


2. When the *Run* window appears, type `gpedit.msc` and click **OK**.

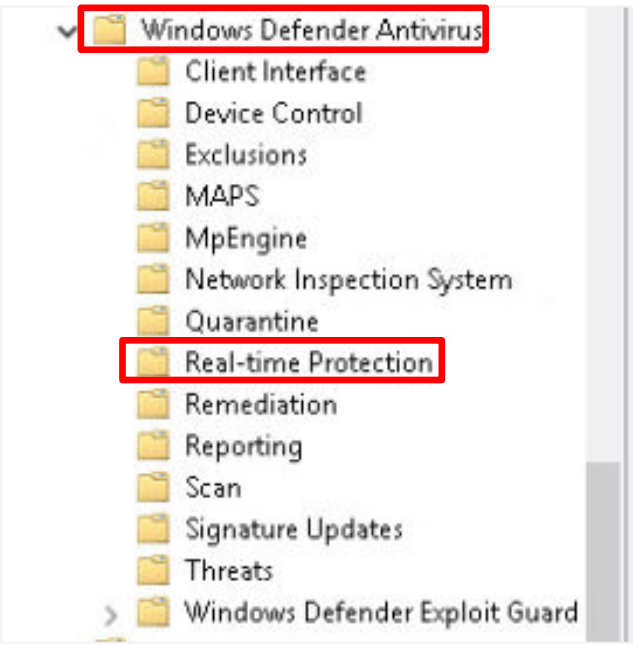


3. In the *Local Group Policy Editor* window, expand the following:

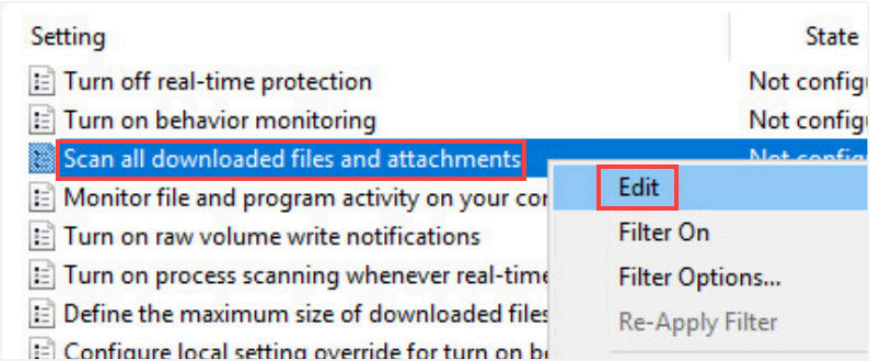
Computer Configuration
→Administrative Templates
→Windows Components



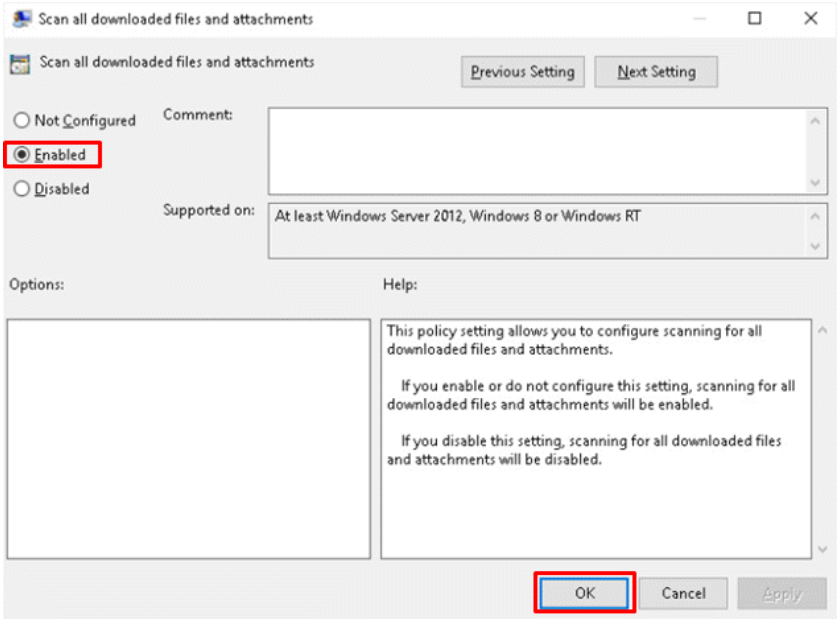
4. Scroll down and expand **Windows Defender Antivirus**. Then click on **Real-Time Protection**.



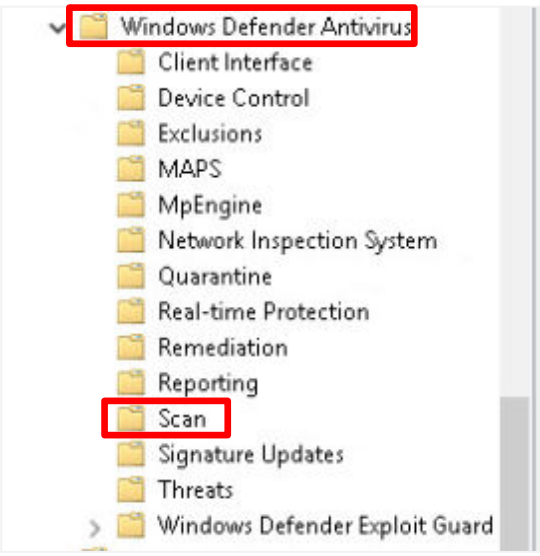
5. In the right pane, right-click **Scan all downloaded files and attachments** and click **Edit**.



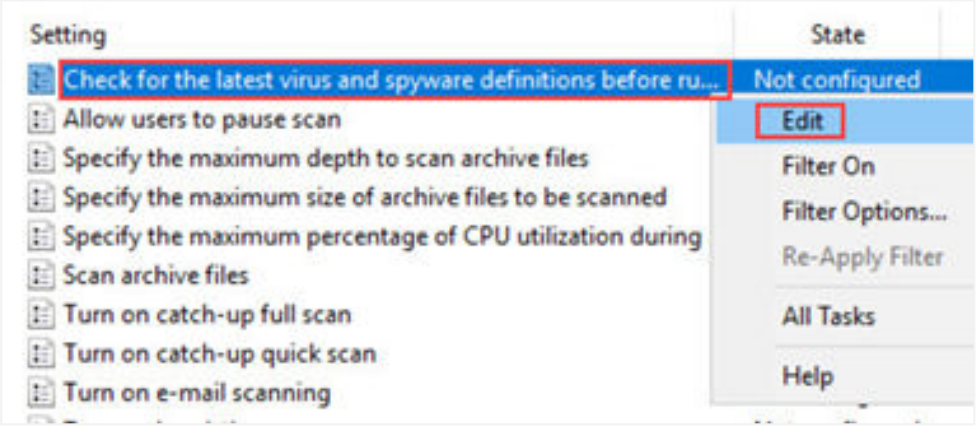
6. Click **Enabled** and click **OK**.



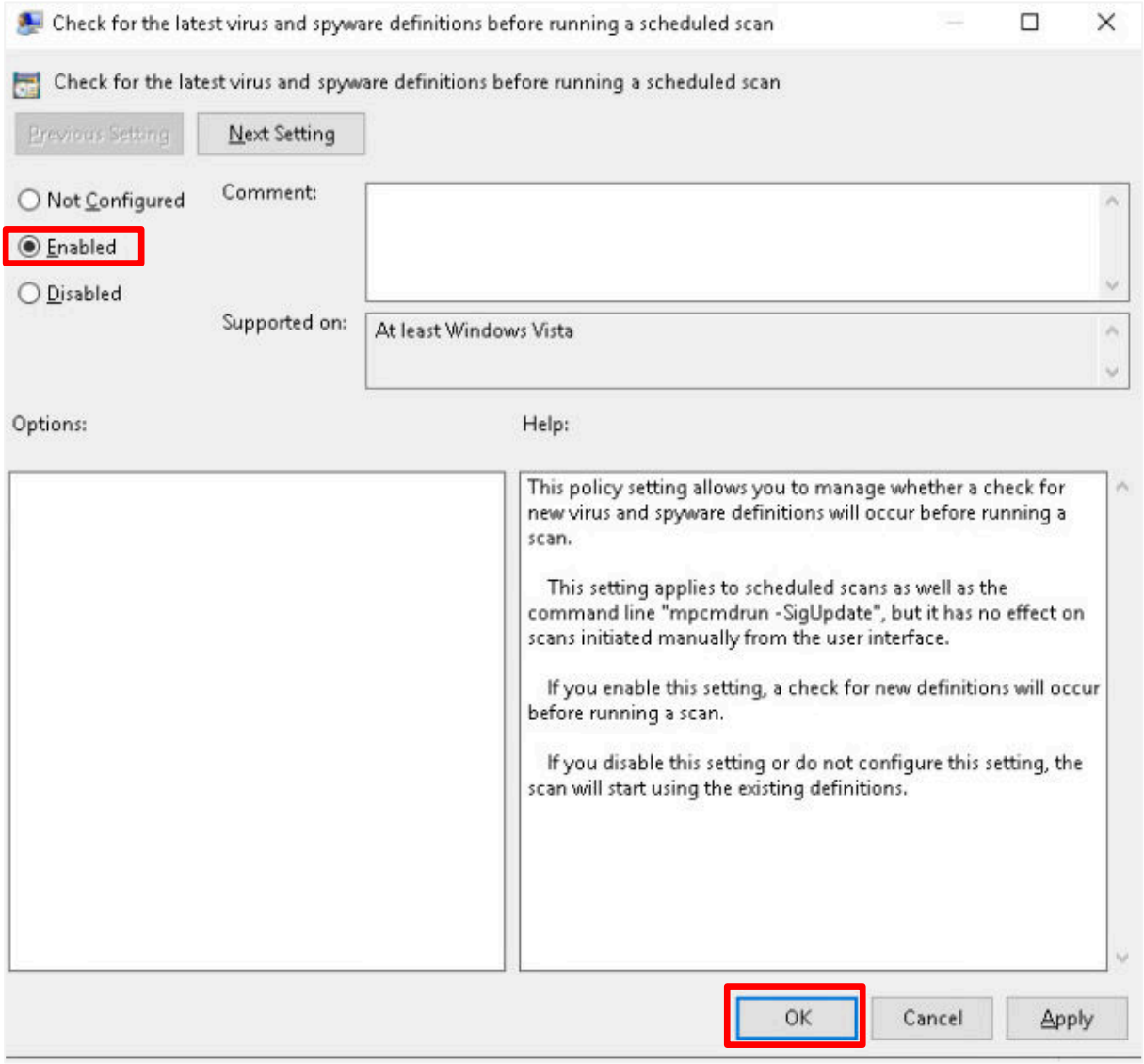
7. Now, click **Scan** in the left pane.



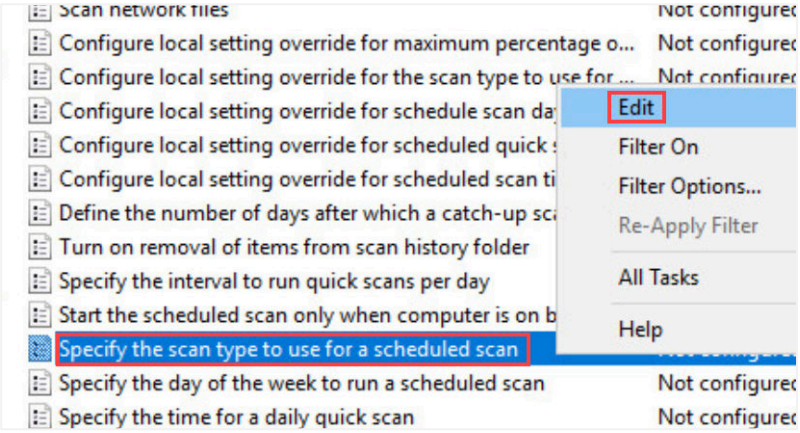
8. In the right pane, right-click on **Check for the latest virus and spyware definitions before running a scheduled scan**. Click **Edit**.



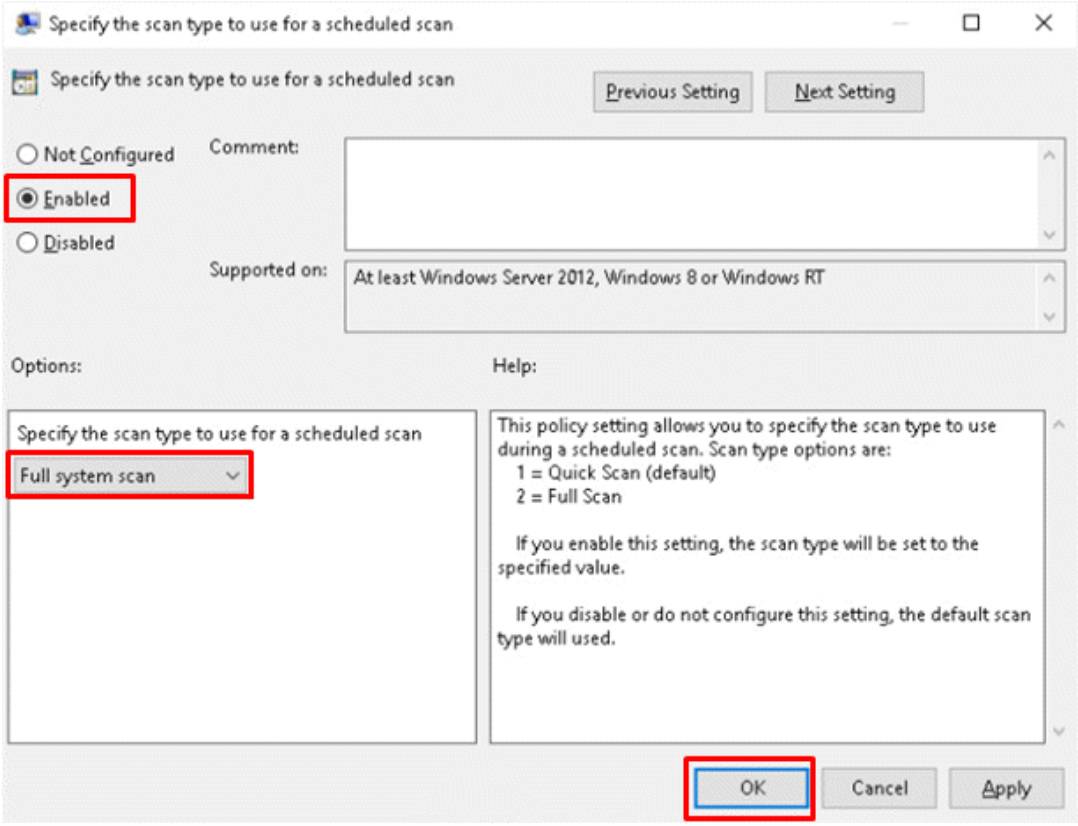
9. Click the **Enabled** radio button, then click **OK**.



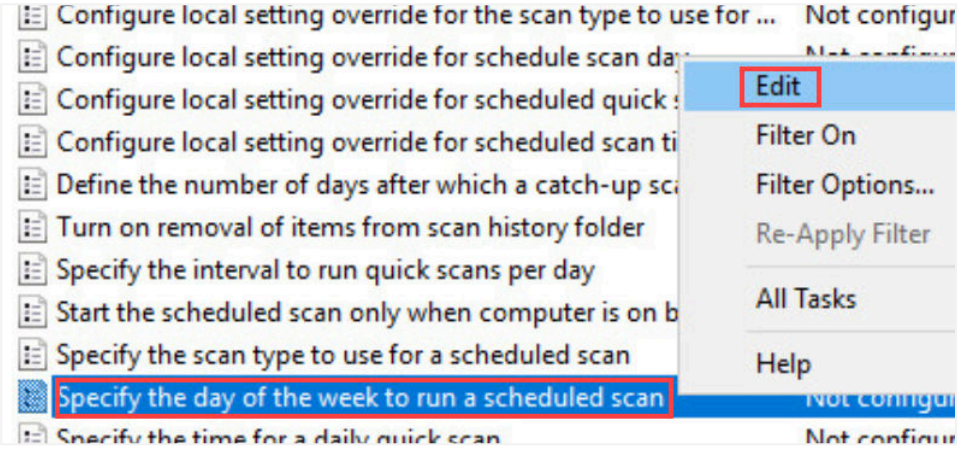
10. Scroll down if necessary and right-click **Specify the scan type to use for a scheduled scan**. Click **Edit**.



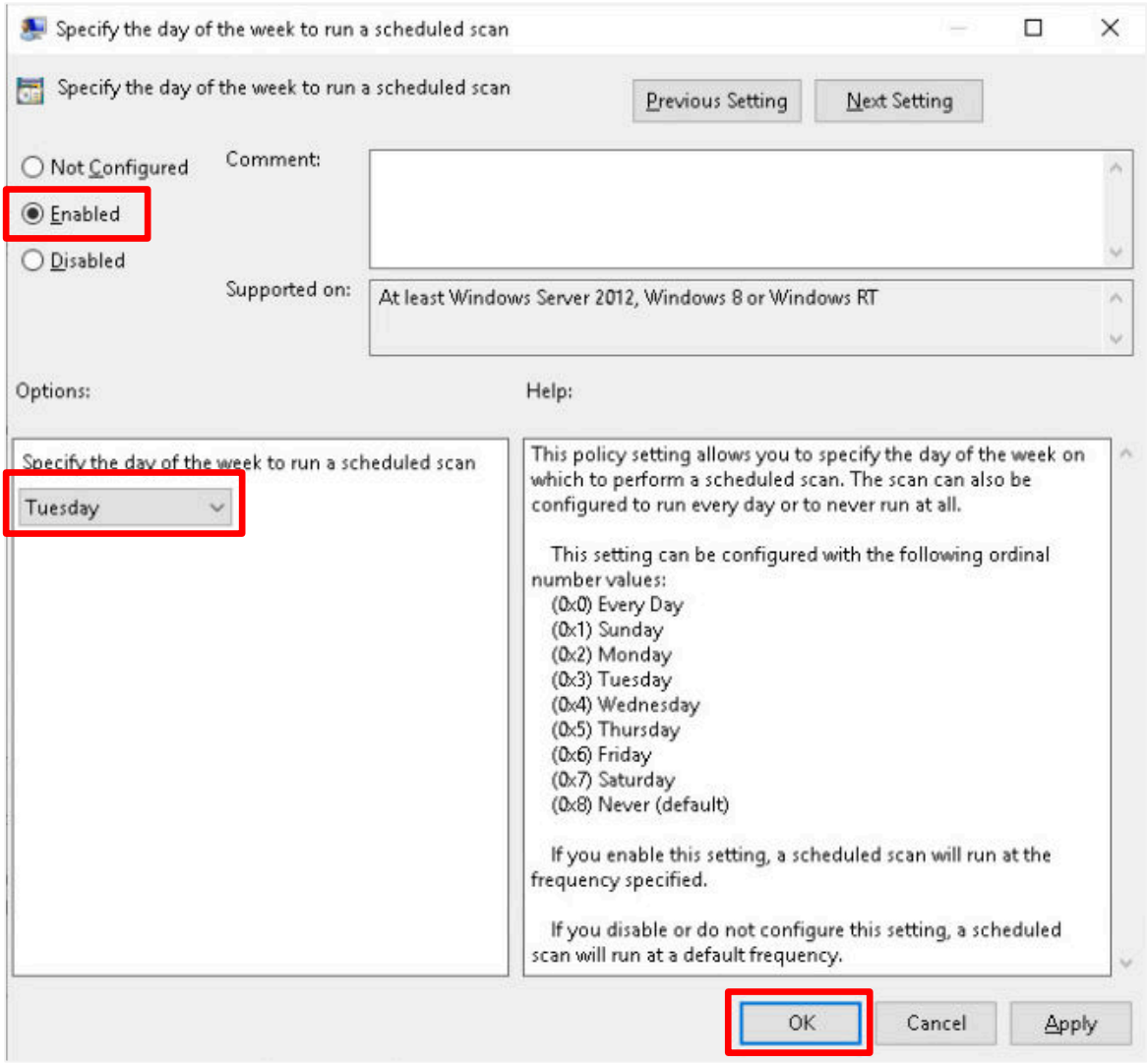
11. Click the **Enabled** radio button. In the dropdown menu, select **Full system scan** and click **OK**.



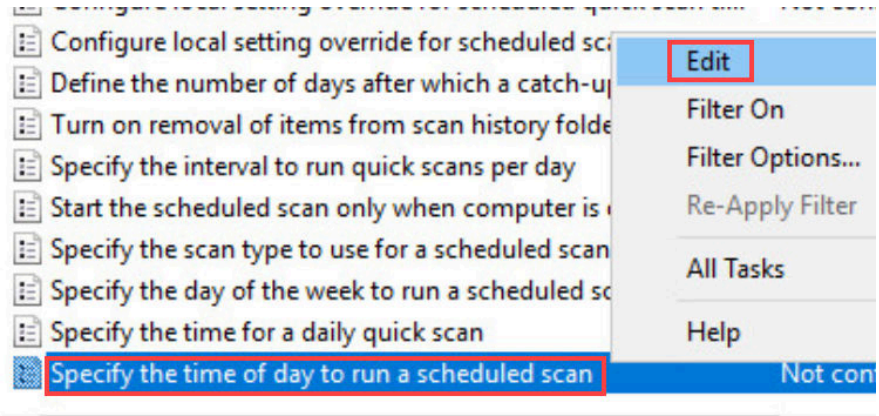
12. Right-click on **Specify the day of the week to run a scheduled scan.** Click **Edit**.



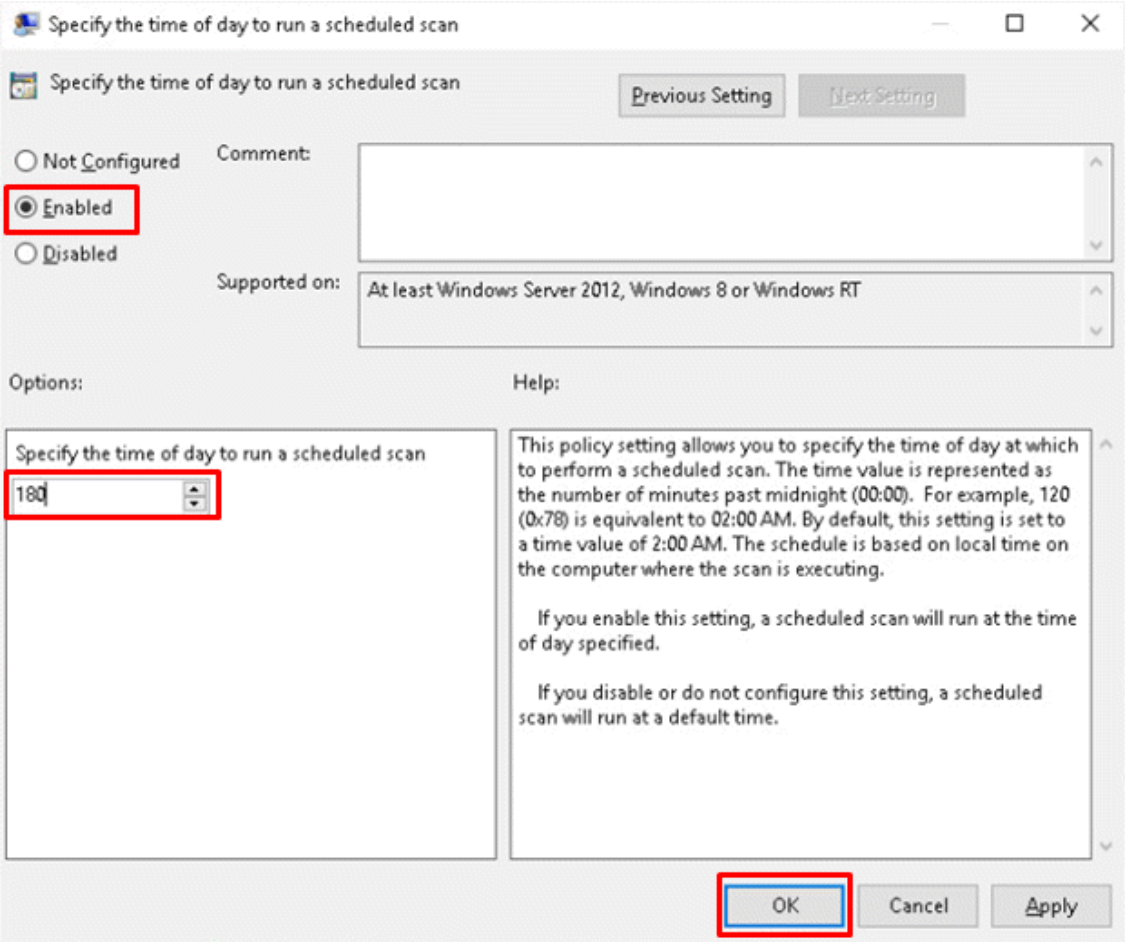
13. Click **Enabled**. In the dropdown menu, select **Tuesday** and click **OK**.



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



15. Click the **Enabled** radio button. In the **Specify the time of day to run a scheduled scan**, type `180`. This will tell the scheduler to run a scan at 3:00 AM. Click **OK**.



16. With these options set, you have set up group policies in **Windows Defender**, 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.
17. This concludes the lab. You may now end the reservation.