

Lab: Troubleshoot Security Issues Scenario #1

Lab 1: Test anti-malware (1)

Checking the status of Windows Defender Antivirus Service.

The screenshot displays a Windows workstation with a browser window at the top showing a lab client URL. Below the browser, the Windows Security app is open, displaying the Windows Defender Antivirus Service. The service is listed in the Services (Local) console with the following details:

Name	Description	Status	Startup Type	Log
Windows Defender Antivirus Service	Helps protect users from malware and other potentially unwanted software	Running	Automatic (Trigger Start)	Local

The service is currently running. The lab interface on the right side of the screen shows the following instructions:

- 9. What is the Startup Type of the Windows Defender Antivirus Service?
 - ☒ Manual
 - ☐ Automatic (Trigger Start)
 - ☐ Automatic
 - ☐ Manual (Trigger Start)

Score: 100% Correct!
- 10. Select the **Windows Defender Antivirus Service**. Run the service by clicking the blue **Start** link above the description.
- 11. From the **Action** menu, select **Refresh**. Check the status of the **Windows Defender Antivirus Service**.

The lab interface also shows a progress bar at the bottom indicating 23% tasks complete.

Lab 2: Enable Windows Defender (1)

Windows Security

Virus & threat protection settings

View and update Virus & threat protection

Local Group Policy Editor

File Action View Help

Windows Defender Antivirus

Turn off Windows Defender Antivirus

Edit policy setting

Requirements: At least Windows Vista

Description: This policy setting turns off Windows Defender Antivirus. If you enable this policy setting, Windows Defender Antivirus does not run, and computers are not scanned for malware or other potentially unwanted software. If you disable or do not configure this policy setting, the default Windows Defender Antivirus runs and computers are scanned for malware and other potentially unwanted software.

Settings

Off

Windows (CR Ln 1, Col 31 100%)

4:18 PM 7/9/2023

Assisted Lab: Troubleshoot Security Issues Scenario #

25 Minutes Remaining

Instructions Resources Help

11. Change the Policy setting to **Disabled** by clicking the appropriate radio button and then clicking **OK**.

12. Close the Local Group Policy Editor.

13. Enter **T cmd** in the taskbar search box and press **ENTER**.

14. Type **T gpupdate /force** and press **ENTER** into the command prompt to force windows to scan for the updated policy setting.

15. After the message *User Policy update has completed successfully* appears, close the command prompt.

16. Use the **Services** window to locate and start the **Windows Defender Antivirus Service**. Select **Action > Refresh** to verify that the service stays in the **Running** state.

17. Close the **Services** window.

18. In the **Virus & threat protection settings** window, enable real-time protection by changing the toggle button to **On**.

If the toggle does not turn to on after the first click, try again.

19. Select the **Score** button to validate this task:

Score

63% Tasks Complete

Previous Next: Test antivirus >

Lab 3: Test antivirus (1)

Using the blue Threat history link located in the Current threats section to view threat history in Windows.

The screenshot displays a Windows Security window titled "Threat history" with the subtitle "View detected threats and scan details." The left sidebar shows navigation options: Home, Virus & threat protection (selected), Firewall & network protection, App & browser control, and Device security. The main content area shows "Last scan" information: "Windows Defender Antivirus automatically scans your device for viruses and other threats to help keep it safe." and "Last scan: Not available." To the right, there are links for "Change your privacy settings", "View and change privacy settings for your Windows 10 device.", "Privacy settings", "Privacy dashboard", and "Privacy Statement".

Overlaid on the Windows Security window is a Notepad window titled "Untitled - Notepad" with a menu bar (File, Edit, Format, View, Help). The text inside the Notepad window reads: "4:04 PM 7/9/2023 Zhaire T Robinson".

On the right side of the screenshot is a lab interface titled "Assisted Lab: Troubleshoot Security Issues Scenario #". It shows a progress bar at 100% and a timer at 21 Minutes Remaining. Below the header are tabs for "Instructions", "Resources", and "Help". A list of instructions is visible, with steps 9 through 14. Step 14 is currently selected and shows a multiple-choice question: "What is the name of the quarantined threat?" with four options: "EICAR Virus_Test", "Virus:DOS/EICAR_Test_File" (selected), "Malware:EICAR/Test Virus", and "Virus:DOS:Test". Below the question are buttons for "Score" and "Correct!".

At the bottom of the lab interface, a green bar indicates "92% Tasks Complete". Navigation links for "Previous" and "Next: Complete comprehensive..." are also present.