

## Lab: Troubleshoot Security Issues Scenario #1

### Lab 1: Test anti-malware (1)

Checking the status of Windows Defender Antivirus Service.

The screenshot shows a Windows desktop environment with multiple windows open. In the foreground, the 'Services' window is displayed, listing various system services. The 'Windows Defender Antivirus Service' is highlighted. The service details pane shows it is running and has a manual startup type. To the right of the main window, there is an 'Assisted Lab: Troubleshoot Security Issues Scenario #' interface. It includes a sidebar with navigation links like 'Instructions', 'Resources', and 'Help'. A main area contains numbered tasks related to the service. Task 9 asks about the startup type, with 'Manual' selected. Task 10 asks to start the service, which is noted as having been started and stopped. Task 11 asks to refresh the service status. A green 'Correct!' button is visible. The task bar at the bottom shows the date and time as 7/9/2023, 4:05 PM.

Assisted Lab: Troubleshoot Security Issues Scenario #

23 Minutes Remaining

border of the **Name** column header to show the full text and identify the correct service.

9. What is the Startup Type of the Windows Defender Antivirus Service?

Manual

Automatic (Trigger Start)

Automatic

Manual (Trigger Start)

Score

Correct!

10. Select the **Windows Defender Antivirus Service**. Run the service by clicking the blue **Start** link above the description.

A message indicating the *Windows Defender Antivirus Service started and then stopped* will display.

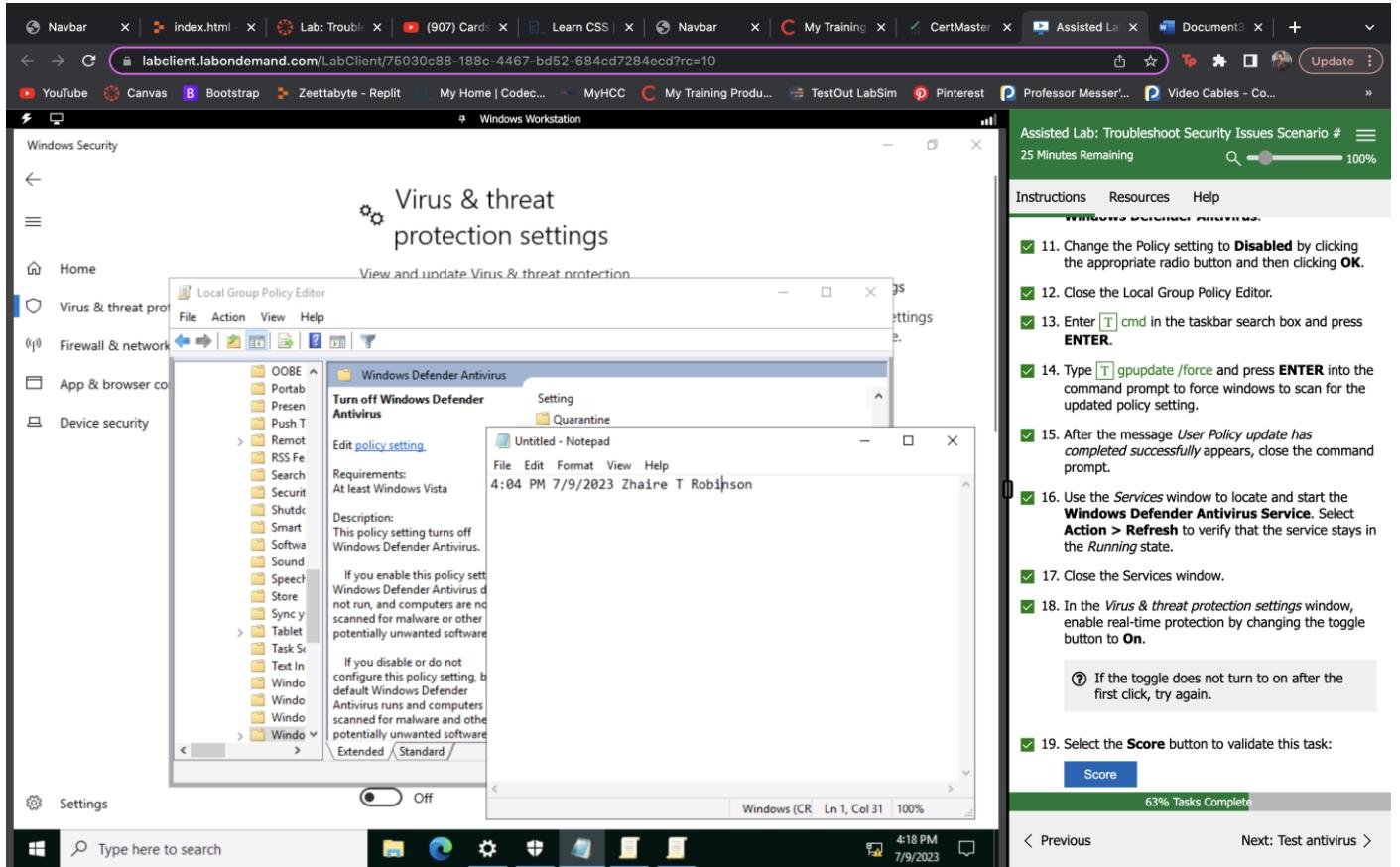
11. From the **Action** menu, select **Refresh**. Check the status of the *Windows Defender Antivirus Service*.

The Windows Defender Antivirus service cannot be started manually. When services behave in this manner, it is a sign they have been disabled by group policy, or that system settings have been compromised by a threat actor.

23% Tasks Complete

< Previous      Next: Enable Windows Defender >

### Lab 2: Enable Windows Defender (1)



### 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 shows a Windows 10 desktop environment. A browser window is open at [labclient.labondemand.com/LabClient/75030c88-188c-4467-bd52-684cd7284ecd?rc=10](http://labclient.labondemand.com/LabClient/75030c88-188c-4467-bd52-684cd7284ecd?rc=10). The page displays a "Threat history" section with a note about detected threats and scan details. It includes a "Last scan" summary from Windows Defender Antivirus. A Notepad window titled "Untitled - Notepad" is visible, showing the text "4:04 PM 7/9/2023 Zhaire T Robinson". On the right side of the browser window, there is a sidebar with "Assisted Lab: Troubleshoot Security Issues Scenario # 21 Minutes Remaining" and a progress bar at 100%. Below the progress bar are numbered tasks:

9. A folder exclusion has been created for the Desktop. Select the item labeled **C:\Users\Administrator\Desktop** and click the Remove button.
10. Try to open the **eicar** file located on the Desktop. After a few seconds, an error should appear indicating the operation did not complete successfully.
11. Select **OK** and close Notepad.
12. Select **Virus & threat protection** by clicking the link on the left side of the **Windows Security** window.
13. Click the blue **Threat history** link located in the **Current threats** section.
14. What is the name of the quarantined threat?
  - EICAR Virus\_Test
  - Virus:DOS/EICAR\_Test\_File
  - Malware:EICAR/Test Virus
  - Virus:DOS:Test

A "Score" button and a "Correct!" button are present. At the bottom, a progress bar shows "92% Tasks Complete". Navigation links "Previous" and "Next: Complete comprehensive..." are also visible.