Hands-on Lab: Windows Defender Antivirus

Estimated time needed: **20** minutes

Objectives

By completing this lab, you will develop a comprehensive understanding of how to secure a Windows operating system using the functionality of real-time protection provided by **Windows Defender**.

In this hands-on lab, you will explore typical settings to enable protection:

- Exercise 1: Review Windows Security Virus and threat protection.
- Exercise 2: Update threat definitions.
- Exercise 3: Run Windows Defender Antivirus quick scan.
- Exercise 4: Run Windows Defender Antivirus custom scan.

Further in this hands-on lab, you will also explore typical use cases:

- Scenario 1 - Schedule a weekly full scan using Windows Defender Antivirus
- Scenario 2 - Simulate downloading a test malware file and activate Windows Defender Antivirus to block and quarantine the file.

Important Notices about This Lab

About Lab Sessions

Lab sessions are not persisted. This means that every time you connect to this lab, a new environment is created for you. Any data or files you saved in a previous session are no longer available. To avoid losing your data, plan to complete these tasks in a single session.

About the Lab Instructions and Solutions

Microsoft Windows operating system features can vary based on the Windows edition. If completing these exercises on your machine, your navigation and solutions may differ from what's presented in this lab.

Configuration of Windows Defender Antivirus

Exercise 1: Review Windows Security Virus & threat protection

In this lab, you'll access and review Windows Security Virus & threat protection. Let’s begin with locating and opening Windows Security Virus & threat protection.

1. Click the Windows **Start** button and select **Settings**.

2. On the Windows Settings page, select **Update & Security**.

3. Under Update & Security, select **Windows Security**. Here, select **Virus and threat protection**.

4. On this screen, you'll see the following features(Scroll down to discover all the features):

- **Current threats**: Here, you can see any threats that have been detected on your device. You can see when the last scan occurred, how long the scan took, and how many files were scanned. Here you can also click the button to start a quick scan or access **scan options** to run a full scan or a custom scan.
- **Virus & threat protection settings**: Here, you can access options for managing your virus and threat protection settings. You can customize your protection level, opt to send sample files to Microsoft, exclude files or folders from scans, or temporarily stop your protection.
- **Virus & threat protection updates**: Here, you can view the last time your virus definitions were updated. You can also opt to manually check for updates.
- **Ransomware protection**: Here, you can choose to enable controlled folder access. This protects memory, files, and folders from unauthorized changes.

Exercise 2: Update Threat Definitions

Windows Security uses security intelligence, also known as definitions, to identify known threats. These definitions include information about known threats. These definitions are updated automatically, but if you suspect a problem with your system, you should ensure that threat definitions are up-to-date before you run a scan.

1. Under Virus & threat protection updates, select **Check for updates**.

2. You can view details for the most recent update to your threat definitions. Select **Check for updates**. This process could take a few minutes. When the update has completed, the **Check for updates** button will return, and you should notice that the last update time and date have changed. Select the back button to return to the **Virus & threat protection** screen.

Exercise 3: Run Antivirus Quick Scan

1. Now we can run an antivirus scan. Click the **Quick scan** button on the **Virus & threat protection** screen. The scan will take several minutes to run. When complete, the **Quick scan** button will reappear. Click **Protection history** to view any recent findings.

2. This page shows you the results of the last scan. You see the files identified as a threat and quarantined, so they cannot damage your device. You then see files identified as potential threats but allowed to continue running.

Exercise 4: Run Antivirus Custom Scan

Run a custom scan that only scans the files in the **Downloads** folder.

▶ Click here for a hint.
▶ Click here for the solution.

Typical Use cases of Windows Defender Antivirus

Scenario 1

Roshan is an employee working from home and needs to access company resources securely while ensuring his personal computer remains protected from potential threats. Enable Windows Defender Antivirus to secure his system and setup scheduled scans to automatically scan his system fully.

The steps below will help you schedule a weekly full scan using Windows Defender Antivirus via Task Scheduler.

1. **Enable Antivirus Protection**
   - Open Virus Protection:
     - Follow steps 1 to 3 mentioned in Exercise 1 above to open **Virus & threat protection**
   - Enable Virus & Threat Protection:
     - Under the Virus & threat protection settings, click on Manage settings.
     - Turn **On** Real-time Protection:
       Ensure the Real-time protection toggle is turned on. This will enable continuous monitoring of your system for threats.
2. Schedule Weekly scans
   - **Open Task Scheduler**
     - In the search bar, type **Task Scheduler** and click on Task Scheduler.
   - **Create a New Task**
     - In Task Scheduler, click on **Create Task** in the Actions pane on the right.
   - **General Settings**
     - In the **General** tab, name your task (e.g., "Weekly Full Scan").
     - Optionally, add a description.
     - Select **Run whether user is logged on or not**.
   - **Specify Triggers**
     - Go to the **Triggers** tab and click on **New**.
     - Set **Begin the task** to **On a schedule**.
     - Select **Weekly** and set the start time to `3:00 AM`.
     - Choose **Sunday** and click **OK**.
   - **Specify Actions**
     - Go to the **Actions** tab and click on **New**.
     - Set **Action** to **Start a program**.
     - In the **Program/script** field, enter:

       ```
       C:\Program Files\Windows Defender\MpCmdRun.exe
       ```

        - In the **Add arguments** field, enter:

          ```
          -Scan -ScanType
          ```

        - Click **OK**. You will be promted with confirmation to add arguments to specified program.
        - Click **Yes** to accept this condition.

    - **Specify Conditions**

        - Go to the **Conditions** tab.
        - Check **Start the task only if the computer is on AC power** to avoid running the scan on battery power.
        - Optionally, set **Wake the computer to run this task** if your computer is usually asleep at this time.

    - **Settings**

        - Go to the **Settings** tab.
        - Check **Allow task to be run on demand**.
        - Ensure **If the task fails, restart every** is checked with **1 hour** and appropriate retry settings.
        - Click **OK** to save the task.

    - **Conclusion**

      These steps will schedule a weekly full scan using Windows Defender Antivirus, ensuring your system is regularly checked for threats.

Scenario 2

You can simulate downloading a test file that is known to contain harmless malware for testing purposes (such as the EICAR test file) and activate Windows Defender Antivirus to block and quarantine the file.

1. **Enable Antivirus Protection**

   Follow all the steps mentioned in the Scenario 1 to Enable Antivirus Protection.

2. **Enable Notifications**

    - In the Windows Security app, click on Virus & threat protection.

    - Manage Notifications:

        - Scroll down to the Virus & threat protection settings section.

        - Click on **Manage settings**.

  - Scroll down to **Notifications** and click on **Change notification settings**.
  - Ensure that the toggles for Recent activity and scan results, Threats found, but no immediate action is needed, and Files or activities are blocked are turned on.

3. **Download a Sample File for Testing**

The EICAR Anti-Virus Test File, often referred to as the EICAR test file, is a standardized test file developed by the European Institute for Computer Antivirus Research (EICAR) and Computer Antivirus Research Organization (CARO). It is designed to safely test the response of antivirus software without the risk of using real malware.

The EICAR test file contains a specific string of characters. When this string is executed or scanned by antivirus software, it should trigger a detection alert.

- Visit the EICAR website:- https://www.eicar.org/download-anti-malware-testfile/
- On the EICAR download page, you will find links to different versions of the test file (e.g., .com, .txt, .zip).
- Click on the **EICAR.COM-ZIP** link to download the file.

4. **Observing Detection**

- During the download process, observe how Windows Defender reacts. As the file is being written to the disk, Windows Defender scans it in real-time. If the file contains known malware signatures or behaves suspiciously (like trying to modify system settings or files), Windows Defender immediately flags it.
- As soon as the file is detected, Windows Defender triggers an alert. You will see real-time alerts and actions being taken without any need for manual scans.

5. **Reviewing Alerts and Logs**

- Upon detection, Windows Defender takes immediate action. It will quarantine the file, preventing it from executing and spreading malware on the system.
- A notification pops up, informing the user of the detected threat and the action taken. You can click on the notification to open Windows Security or you can open Windows Security and navigate to the “Virus & threat protection” section to view the history of detected items, actions taken, and detailed reports.
- Review the threat's severity, the recommended actions, and options for handling the threat.

Conclusion

- Real-time protection continues to monitor the system, scanning other files, and processes in real-time to ensure no other threats are present.

Author(s)

Shilpa Giridhar