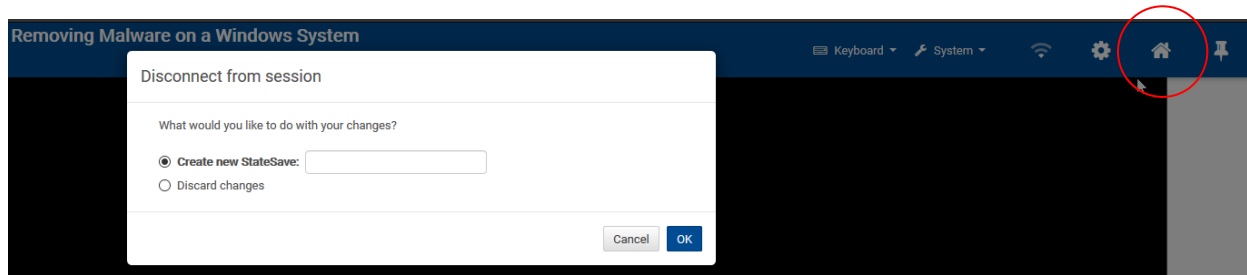


Lab #1 (Required): Identifying and Removing Malware on a Windows System*

Introduction to Information Security (IST623)
School of Information Studies
Syracuse University

Disclaimer: The contents of this document are solely for educational purpose. Misused knowledge of this lab may result in damage of data, security breach, privacy violation, or other undesirable situations. Therefore, using knowledge of this lab other than for the original purpose is prohibited.

**** Save Your Lab Status!**** You may need to save your lab from time to time as each session allows you to be logged in only for two hours at a time. To save your current status in the lab environment, **click the Home icon button** (🏠) in the top right corner and choose **Create new StateSave** if it's your first time saving or **Overwrite existing StateSave** if you have saved it before.



Learning Objectives

Antivirus programs, such as the AVG Business Edition software used in the virtual lab environment, are designed to stop the spread and activity of viruses. Antivirus programs are designed to run in the background on a system, staying vigilant for activity that suggests viruses and stopping or shutting it down. Because there is a wide range of viruses and other malicious code, antivirus programs must be able to detect more than a simple virus. Good antivirus software can detect viruses, worms, Trojans, phishing attacks, and in some cases, spyware.

In this lab, you will use AVG AntiVirus Business Edition to identify the viruses, worms, Trojans, malware, or other malicious software found on a compromised Windows machine. You will complete a scan of the entire computer, learn how to exclude folders to avoid false positives, and understand the importance of maintaining the signatures database. You will discover the difference between a full computer scan and a File Shield scan. Finally, you will also

* Customized lab manual by Dr. Joon S. Park at the School of Information Studies for the virtual online labs provided by Jones & Bartlett Learning.

permanently remove the malware identified by the antivirus software and schedule the scan to run automatically.

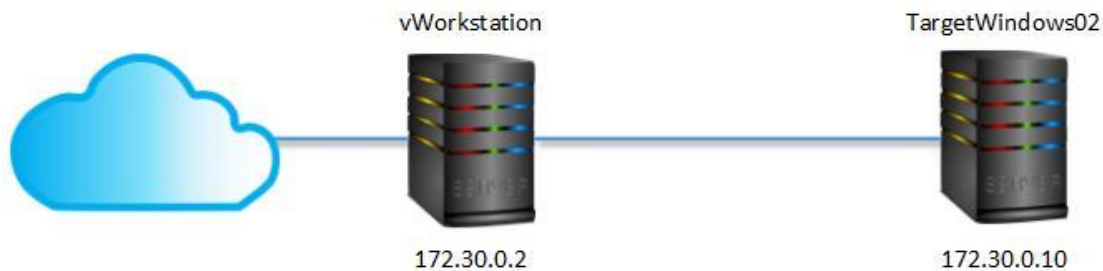
Upon completing this lab, you will be able to:

- Identify malware and other malicious software on a Windows desktop using antivirus software.
- Exclude specific drives or folders from an antivirus scan to prevent false positives.
- Detect a hidden virus embedded in a PDF document.
- Quarantine malware and other malicious software for further investigation and removal.
- Recommend remediation steps for mitigating malware found by an antivirus scan.

Lab Structure

This lab has the following parts, which should be completed in the following order:

1. In the first part of this lab, you will use the AVG (Anti-Virus Guard) to scan the vWorkstation and download a copy of the scan results.
2. In the second part of this lab, you will use the AVG's Resident Shield feature to identify a threat in an encrypted archive file.
3. In the third part of this lab, you will permanently remove malware quarantined by the AVG and schedule the scan to run automatically.
4. In the fourth part of this lab, you will answer a challenge question which will help you understand how anti-virus software isolates malware.



Tools and Software

The following software is required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- AVG (Anti-Virus Guard) AntiVirus Business Edition

Lab Deliverables

- Upon completion of this lab, you are required to turn in a PDF that includes:
 - Screenshots from Part 1: Steps #17 and #25
 - Screenshots from Part 2: Step #11
 - Screenshots from Part 3: Steps #5 and #12
 - Your analysis on the Challenge Question from Part 4 (in 200 words)
- Lab Report Submission
 - Please submit your deliverables through the LMS submission space.
 - The screenshots should be readable.
 - Make sure you include all the items required in your report.

Part 1: Using Antivirus Software to Scan the Potentially Infected System

Note: Malware includes anything developed for the purpose of doing harm. If it were easy to find, it wouldn't cause any damage to an individual machine or to an entire network. Ideally, your antivirus software is running automatically and finding malware on its own. However, if you recognize the symptoms of a malware infection, you can manually scan the computer. These symptoms include:

- Slow response opening applications or browsing the Internet.
- Applications not working as they normally would.
- Operating system not booting up correctly or not functioning normally.
- Event logs reporting numerous, unusual alerts.
- Antivirus software is disabled, not running, or unable to update its virus definitions.
- Numerous windows popping up when trying to access the Internet or opening a browser.

In the next steps, you will use AVG, an antivirus program, to manually scan the TargetWindows02 machine to see how AVG and similar software programs identify malware.

1. On the vWorkstation desktop, **double-click** the **Connections folder**.
2. In the Connections folder, **double-click** the **TargetWindows02 RDP icon** to open a remote connection to the TargetWindows02 machine.

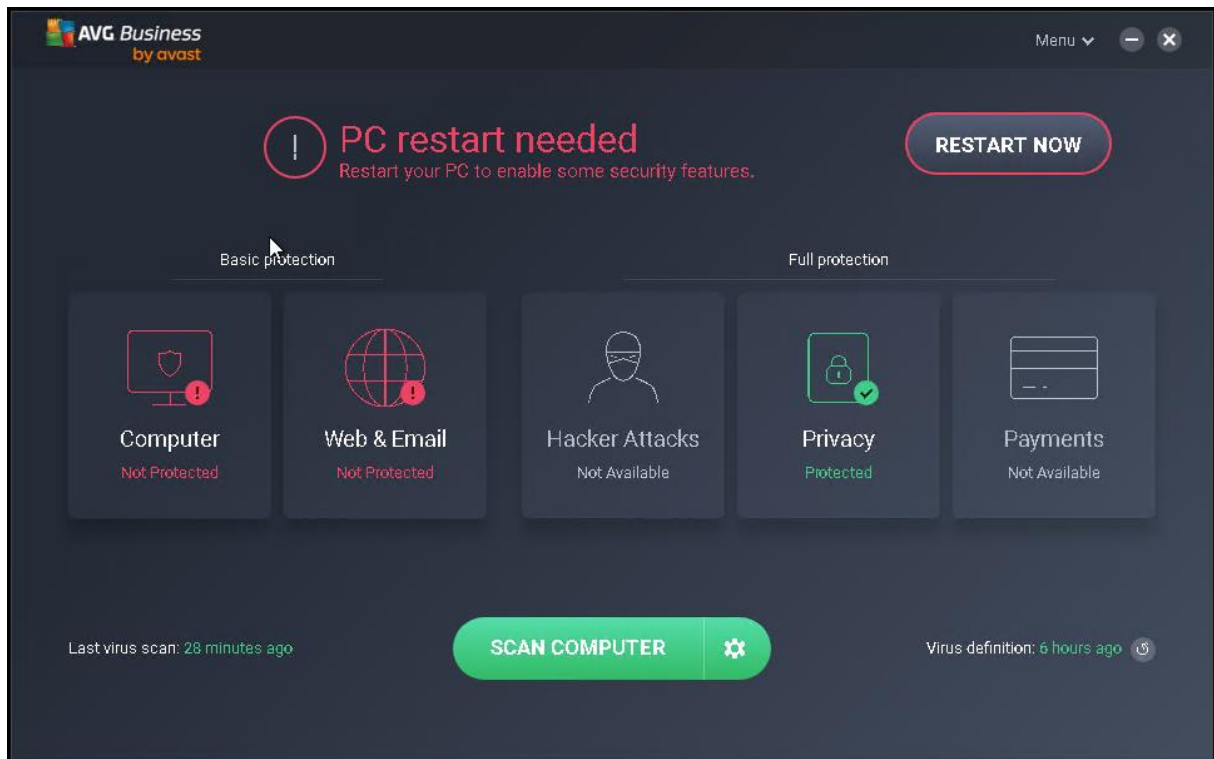
If prompted, **type** the following credentials and **click OK**.

- Username: **Administrator**
- Password: **P@ssw0rd!**

The remote desktop opens with the IP address of TargetWindows02 (172.30.0.10) in the title bar at the top of the window.

3. On the TargetWindows02 desktop, scroll down and **double-click** the **AVG Business Security icon** to start the antivirus application.

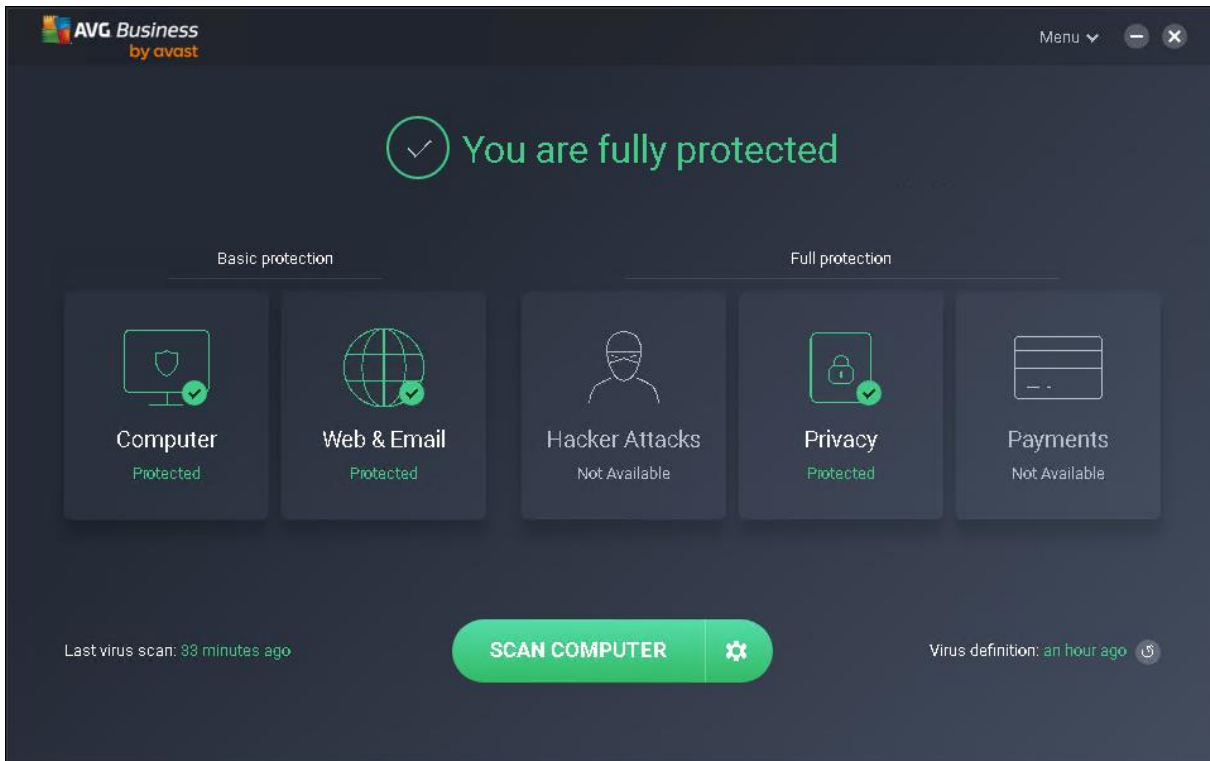
When the application opens, you will notice that the application interface includes a warning that the computer is not fully protected and that some components, specifically the Computer component, are not yet active. You may also see the “**RESTART NOW**” or “**Fix Now**” button.



[Figure 1 AVG interface](#)

4. Click the “**RESTART NOW**” (or “**Fix Now**”) button in the upper right of the screen.


The AVG will enable the antivirus protection on the unprotected components. Please note that if you are presented with the “**RESTART NOW**” button, clicking it will restart TargetWindows02 machine. At this point please perform steps 1, 2 and 3 again. Now, you will be presented with the “**Fix Now**” button. When you click on it you will notice that the warning indicators will change from **RED** to **GREEN** when the application is ready to proceed as seen in the screenshot below.



[Figure 2 AVG is up-to-date](#)

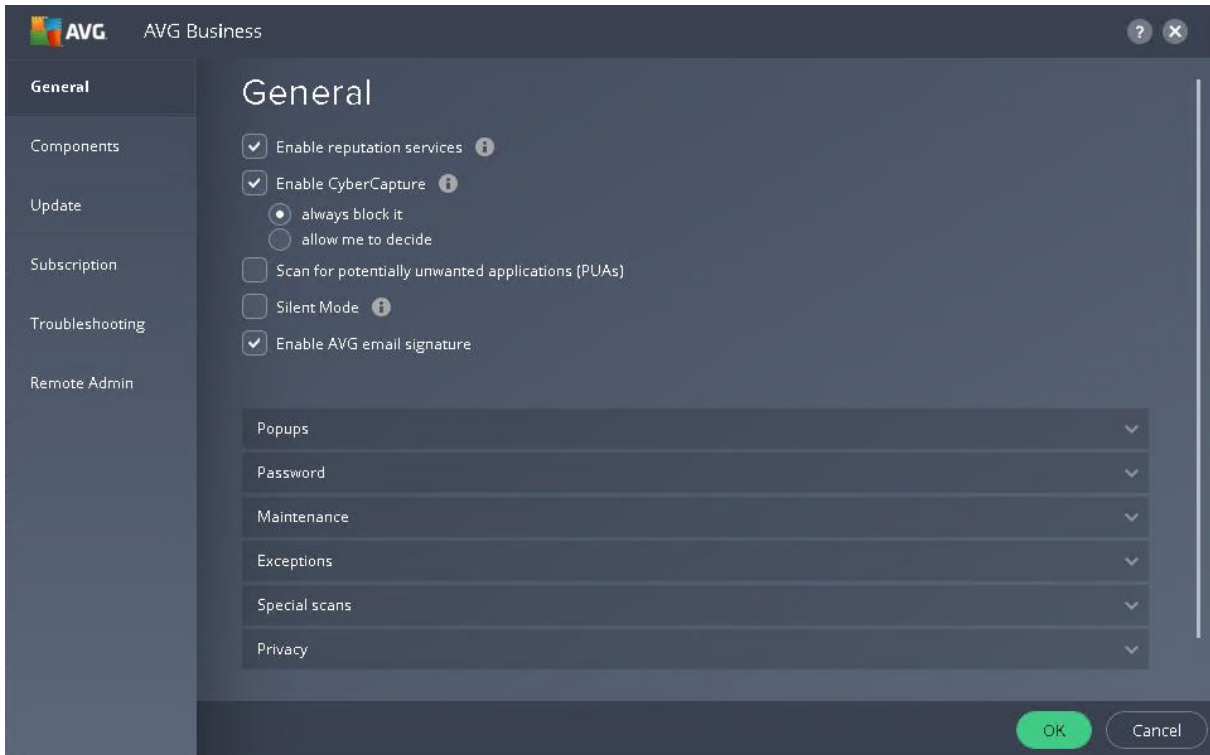
Note: Many new malware and viruses are detected every day, and anti-virus vendors usually update their anti-virus signature files several times per week to keep up with evolving malware. Updating the antivirus software with the latest virus definitions ensures that the software has accurate information to identify and quarantine threats. The AVG automatically updates the database on a regular basis, as long as the machine is able to reach the Internet, or an update server designated in the network.

In addition to updating the database, it is also important to research and apply any patches to the antivirus software itself. These patches often address vulnerabilities in the application as well.

5. Click the **Virus definition button** () in the lower right of the screen to update the signature files.

The AVG will download and install any required signature files and indicate that the software is again up-to-date.

6. On the AVG Home page, **click** the **Menu** icon in the upper right of the screen, then **select Settings** from the available options to open the **AVG Settings** window.

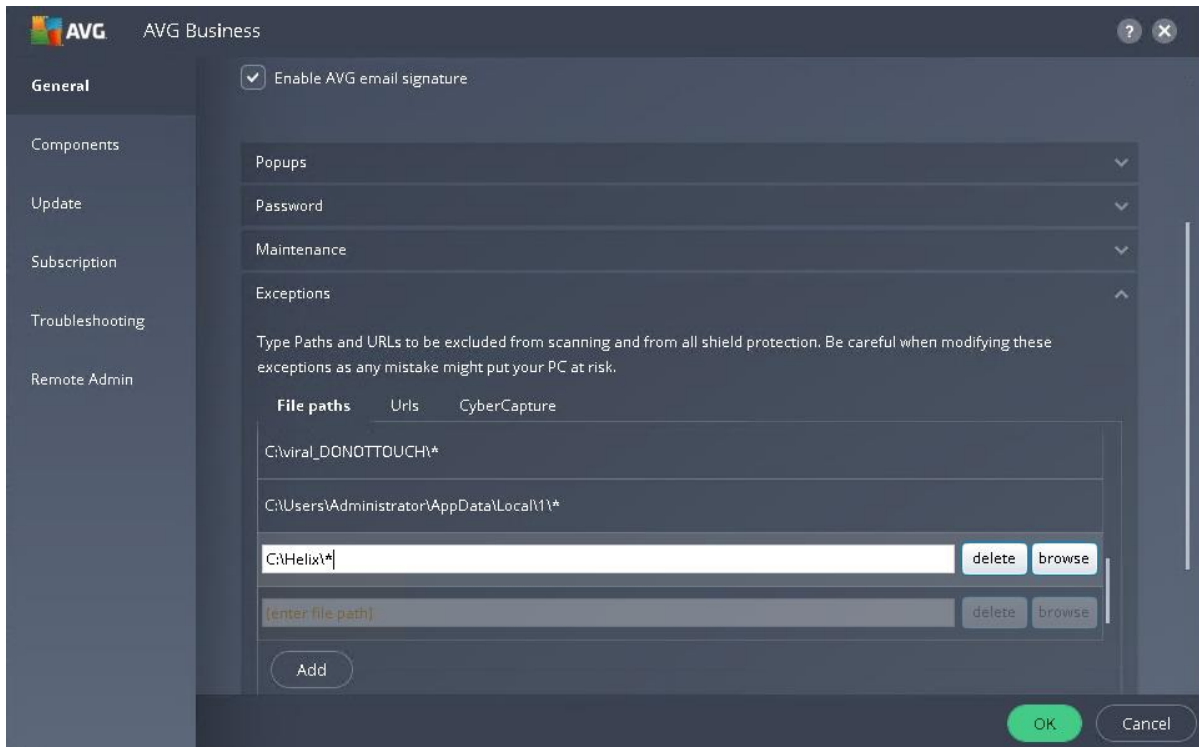


[Figure 3 AVG Settings window](#)



7. In the AVG Settings window, **click the Exceptions header** to expand the AVG Exceptions list.

Note: The Exceptions feature of AVG enables you to remove specific files or folders from the scan. Database files and certain software packages add meta-data to a file that interferes with the antivirus program's ability to recognize the file as safe. What may be a correctly-formatted document may appear to the antivirus program as malware. To avoid this type of “false positive” finding, you may choose to exclude folders containing files that the antivirus program cannot interpret. In this case, the checked Helix folder indicates that this folder has already been excluded. You will remove that checkbox to ensure that there are no exceptions to the scan.

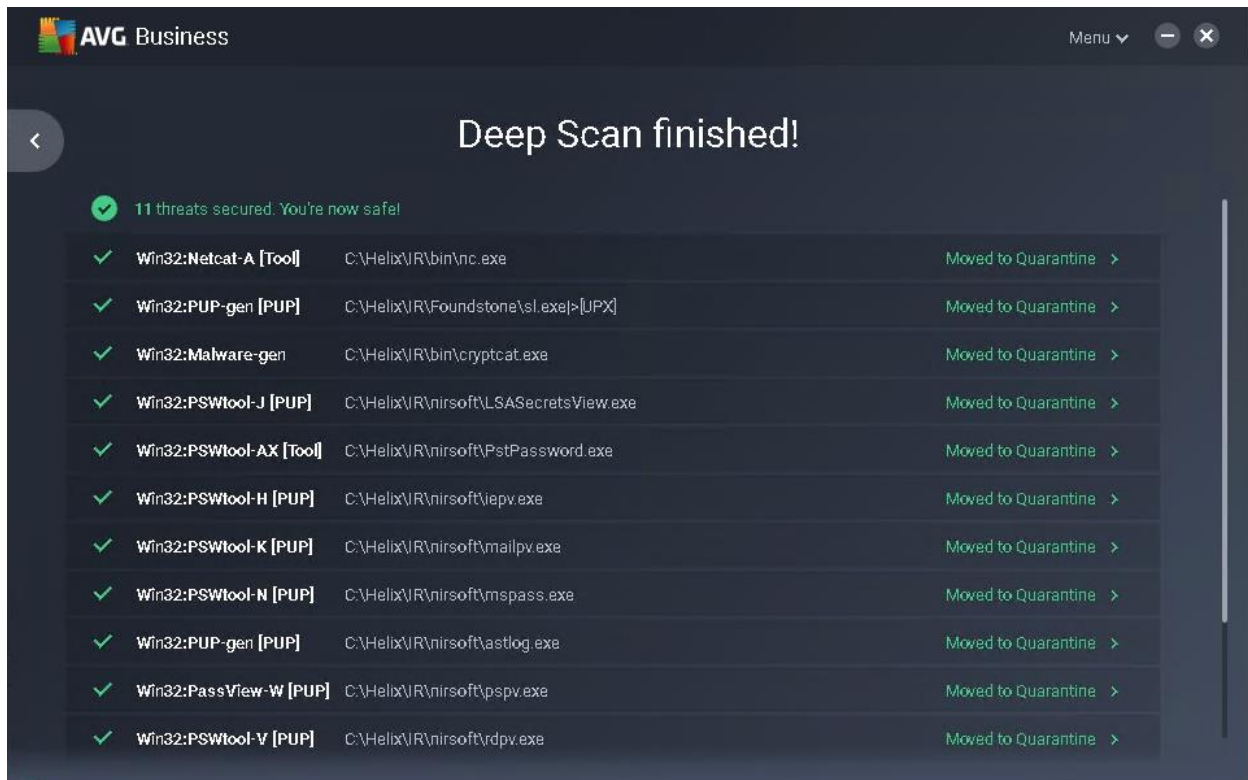
8. From the AVG Exceptions list, **scroll down** and **select the C:\Helix*** exception, then **click the delete** button to remove the exception.



[Figure 4 Scan exceptions](#)

9. In the AVG Settings window, **click** the **OK** button to close the AVG Settings window.
10. On the AVG Home page, **click** the **Configuration** button (, the gear icon to the right of the Scan Computer button) to open the Other Scans page.
11. On the Other Scans page, **click** the **Deep Scan Configuration** button (, the gear icon to the right of the Deep Scan button) to open the Deep Scan Configuration window.
12. In the Deep Scan Configuration window, **locate** the **Report File section** on the left and **click** the **Generate report file checkbox** to configure AVG to output report files.
13. In the File name field, **type** *yourname_S1_AVGscan*, replacing *yourname* with your own name, to name the report file.
13. In the Deep Scan Configuration window, **click** the **OK** button to apply the changes and close the window.
14. On the Other Scans page, **click** the **Deep Scan** button to begin the scanning process and remove any identified threats.

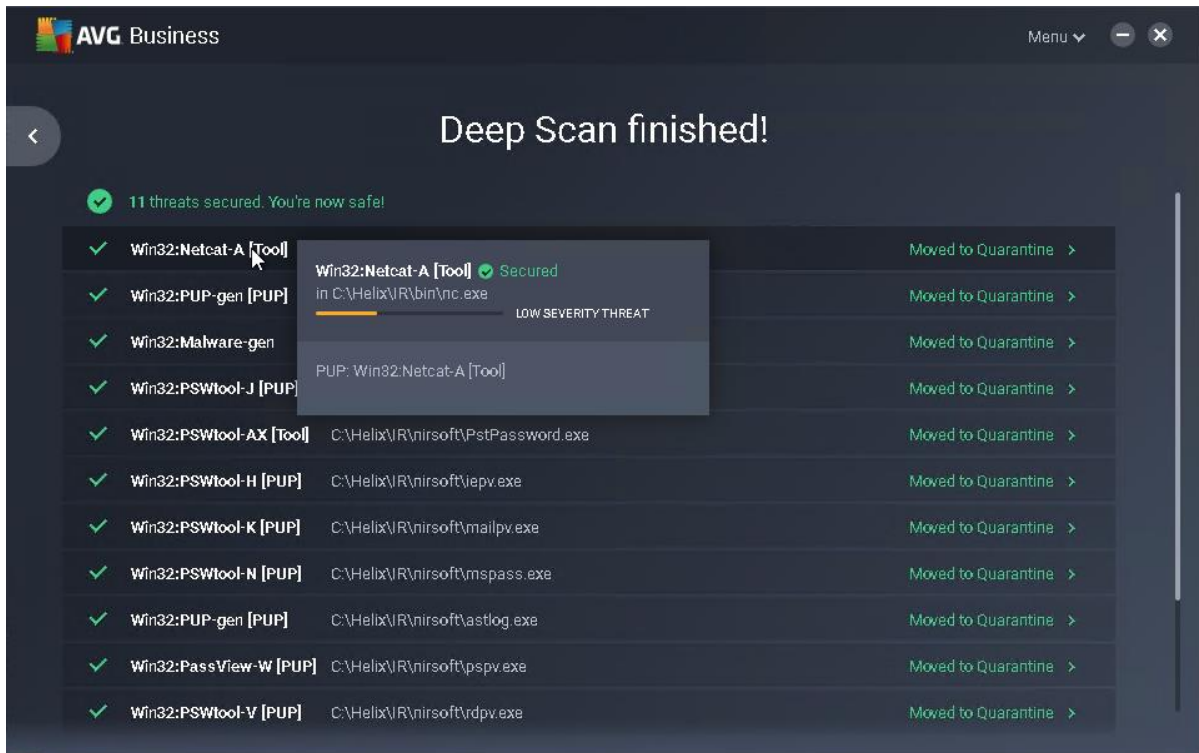
Note: By default, AVG will scan the whole computer. This process will take approximately 15-20 minutes to complete. Do not touch any keys until the scan is finished. When the scan has completed, AVG will display the Scan Summary page showing the number of threats that have been identified and removed. The number of threats is listed at the top of the Scan Summary page.



[Figure 5 Scan summary \(Report Summary\)](#)

15. On the Scan Summary page, **hover your cursor over the first threat** to view additional details about the threat, including the threat severity.

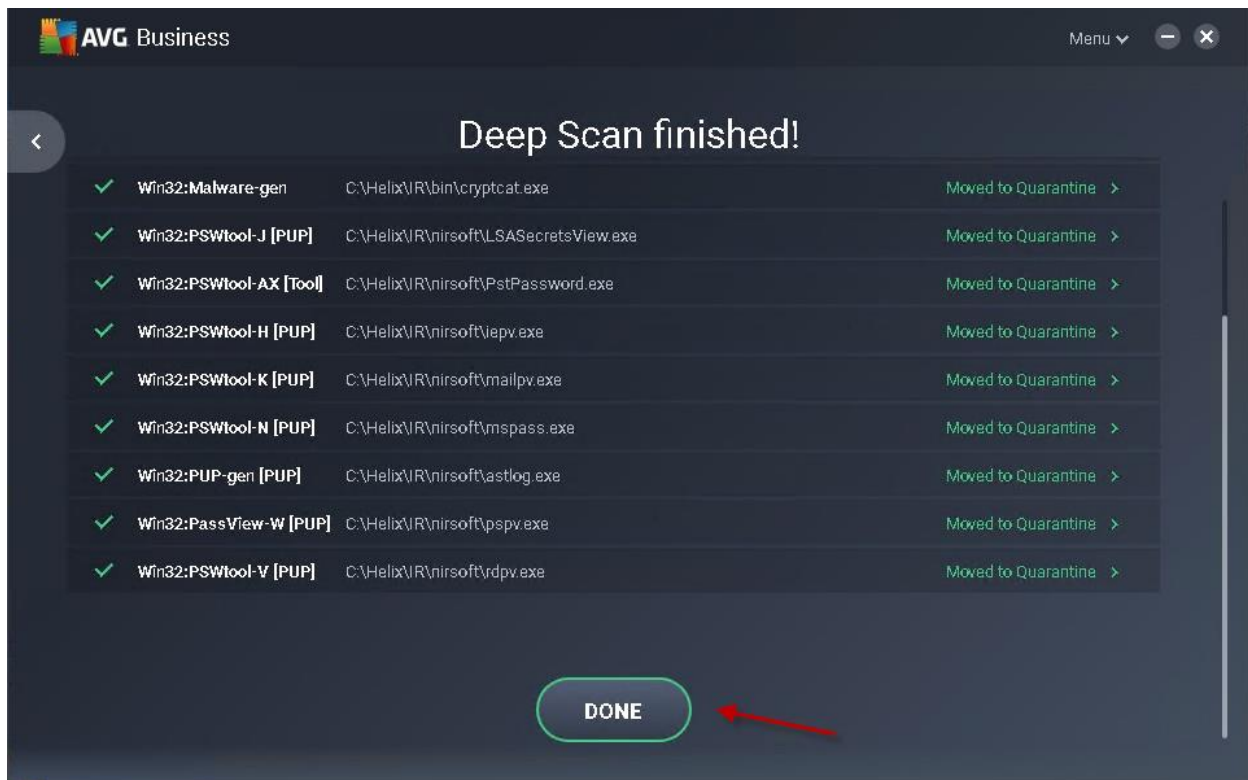
Each threat identified by AVG is given a threat severity rating of **high**, **medium**, and **low**. The page also indicates whether the threat was **removed** (green checkmark) or **not removed** (red exclamation mark) from your computer.



[Figure 6 Threat details](#)

Note: Once you have the name and details for a virus, you can use that information to search the antivirus company's Website or the Internet, in general, for more information about how the virus entered your network in the first place. You can take measures to protect yourself from a recurrence.

16. On the Scan Summary page, **locate the first high severity threat.**
17. Make a screen capture showing the **threat details from Step#16** and paste it into your Lab Report file.
18. **Review** the remaining **high severity threats** detected by AVG.
19. On the Scan Summary page, **click the Done** button to return the AVG Home page.



[Figure 7 AVG Done button](#)

20. **Minimize the AVG window.**
21. On the TargetWindows02 taskbar, **click the File Explorer icon** to open a new File Explorer window.
22. On the File Explorer toolbar, click the **View** tab, then click the **Hidden items** checkbox.
23. In the File Explorer window, **navigate to C:\ProgramData\Avg\Antivirus\report** to access the report generated for your AVG scan.
24. In the Reports folder, **double-click the yourname_S1_AVGscan file** to open the report in Notepad.
25. **Make a screen capture showing the contents of the yourname_S1_AVGscan file and paste it into your lab report file.**
26. **Close the File Explorer window.**

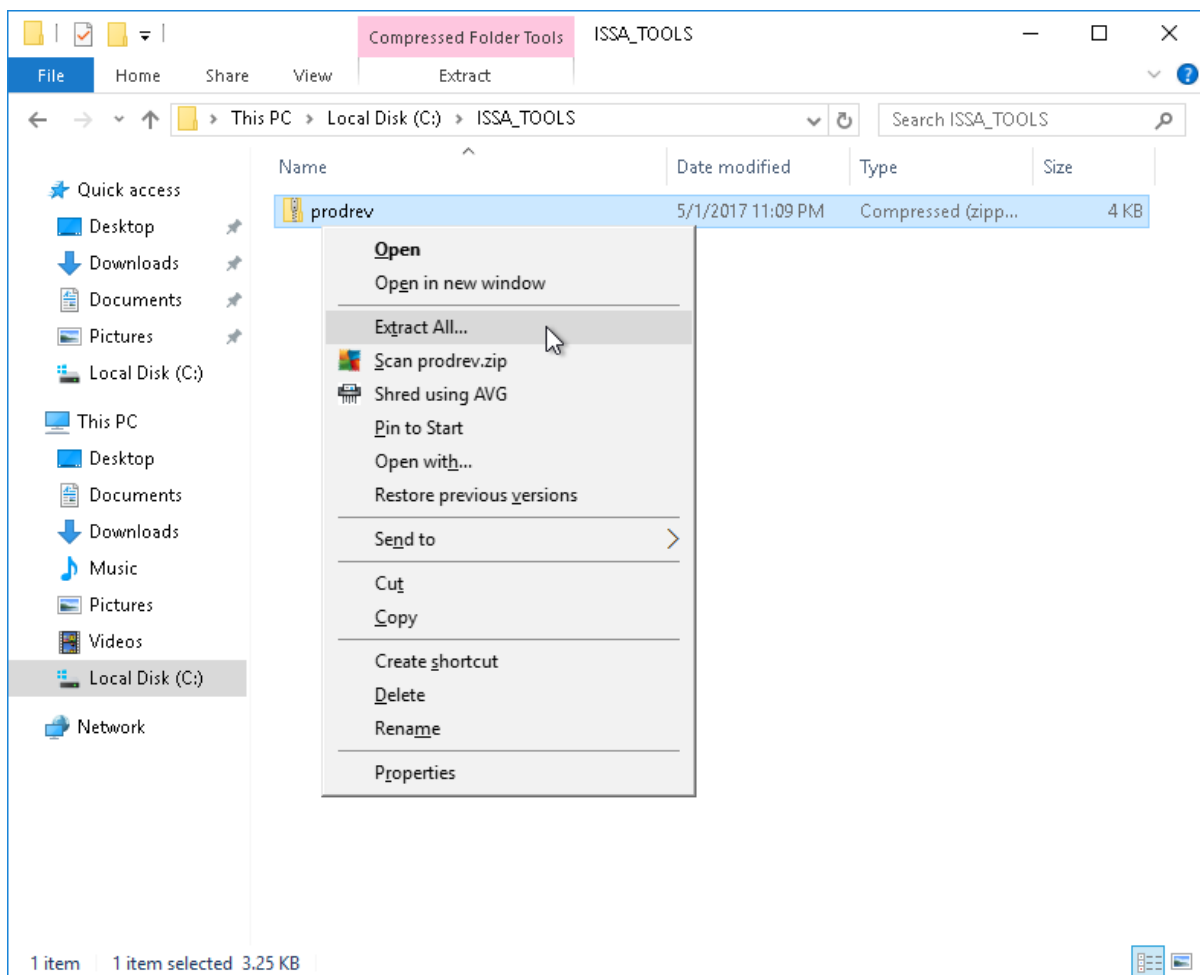
Part 2: Identify Threats in Encrypted Archive Files

Note: In the next steps, you will use the AVG to scan a single folder on the TargetWindows02 machine to detect a hidden virus embedded in an encrypted file. First, you will extract the malware from the folder structure to simulate how easily the virus can affect an unknowing victim.

1. From the TargetWindows02 taskbar, **click the File Explorer icon** to open a new File Explorer window.
2. **Navigate** to the ISSA_TOOLS folder (**This PC > Local Disk (C:) > ISSA_TOOLS**).

The password-protected prodrev.zip archive file has been infected with malware.

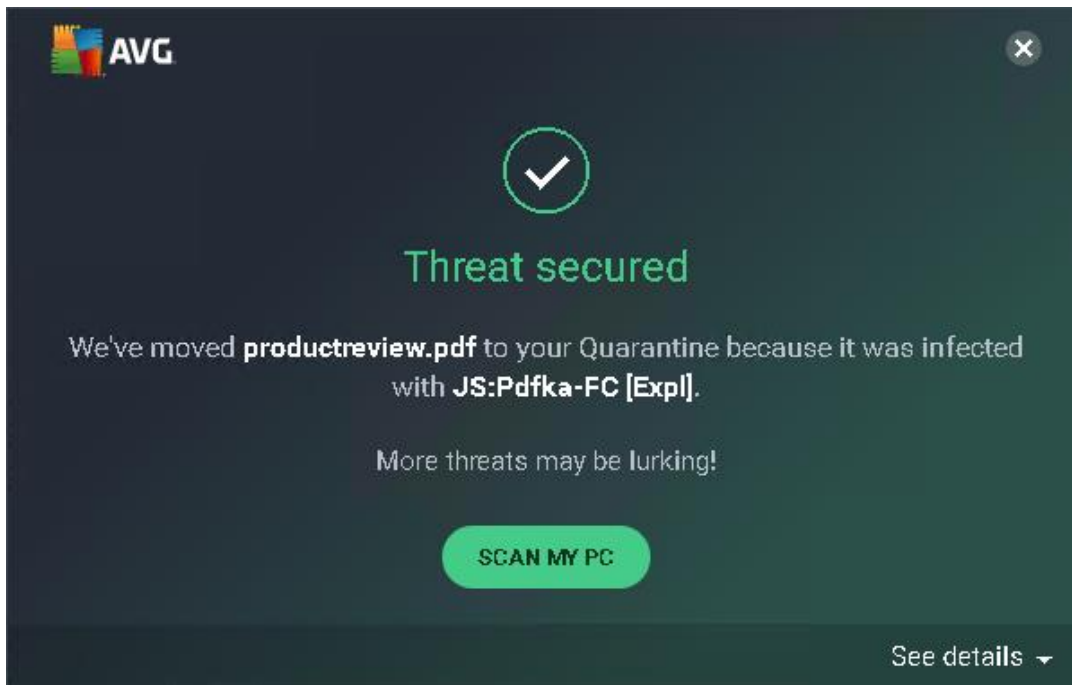
3. **Right-click the prodrev.zip file** and **select Extract All** from the context menu.



[Figure 8 Extract the archive file](#)

4. In the resulting window, **click** the **Extract button** to unpack the zip file in the same folder.
5. When prompted for the document's password, **type password123** and **click OK** to decrypt the zipped file and begin the unpacking process.

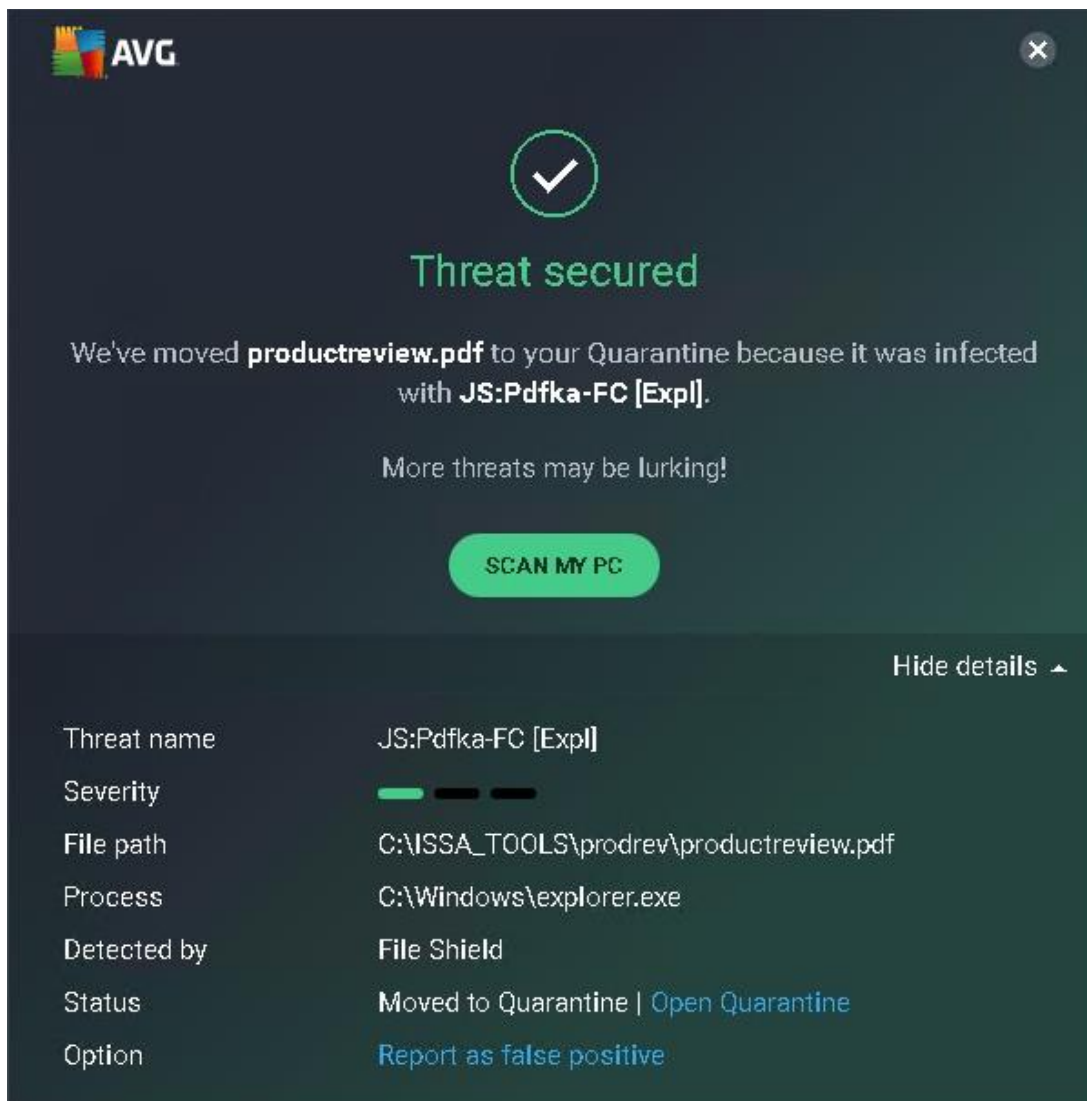
The AVG, running in the background, will detect the virus within the file and display an alert message.



[Figure 9 AVG Detection warning](#)

6. In the AVG Detection window, **click** the **See details link** to show additional details about the threat and what was done to secure it.

AVG provides information about the actual name of the virus (JS:Pdfka-fc) and reports that the infected file (productreview.pdf, part of the prodrev.zip file) has been deleted and the virus has been moved to the Quarantine area (Virus Vault).



[Figure 10 Virus details](#)

Note: AVG, like other antivirus programs, cannot scan compressed files such as *.zip files which was why the scan you conducted in Part 1 of this lab did not detect a virus. The File Shield (previously called Resident Shield) feature of AVG, however, scans every single file as it is opened, saved, or copied. Since the process runs in the background, you will never notice unless AVG identifies a threat.

7. Close the **Threat Detection** window.

In the File Explorer, the **prodrev** folder should be empty, verifying that AVG did indeed remove the infected file.

8. Close the **prodrev File Explorer** window.

9. In the ISSA_TOOLS File Explorer window, **navigate** to **C:\ProgramData\Avg\Antivirus\report** to access the File Shield Report.

This report is automatically generated and contains information about the virus detected by the File Shield in the productreview.pdf file.

10. In the report folder, **double-click** the **FileSystemShield** file to open the report in Notepad.

11. **Make a screen capture** showing the **Pdfka-FC threat detection in the FileSystemShield file** and add it to your Lab Report file.

12. **Close** the **Notepad** window.

13. **Close** the **File Explorer** window.

Part 3: Manage AVG Scans and the Virus Vault

Note:

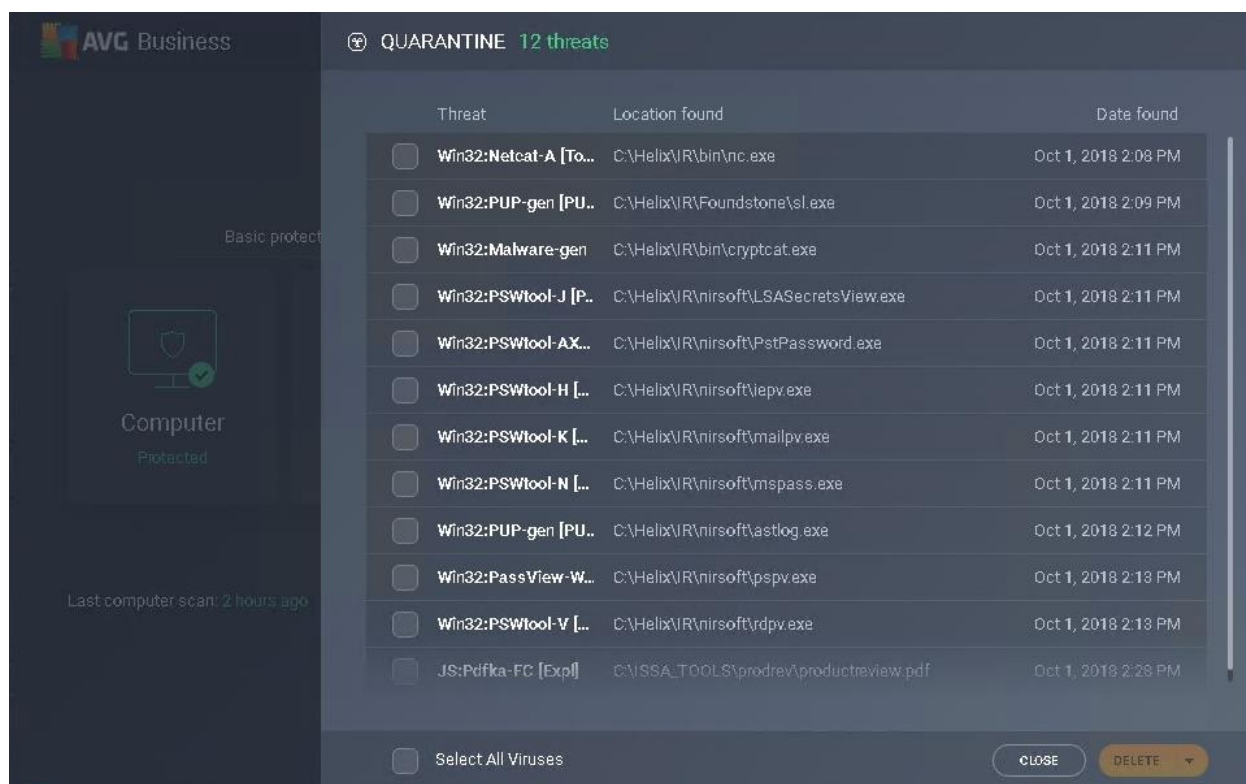
The Quarantine area (previously referred to as the Virus Vault) is where all removed files, virus infected or suspicious, are stored until you take action on them. All of the files in the quarantine area are encrypted and cannot do your computer any harm. The main purpose of the Quarantine area is to keep any suspicious file for a certain period of time, so that you can make sure you do not need the file any more and manually delete it. If you find that the AVG has quarantined a valid file (a false positive), it can be restored easily from this interface.

In the next steps, you will empty the Quarantine area and schedule a complete scan to run daily.

1. From the TargetWindows02 taskbar, **restore** the **AVG** window.

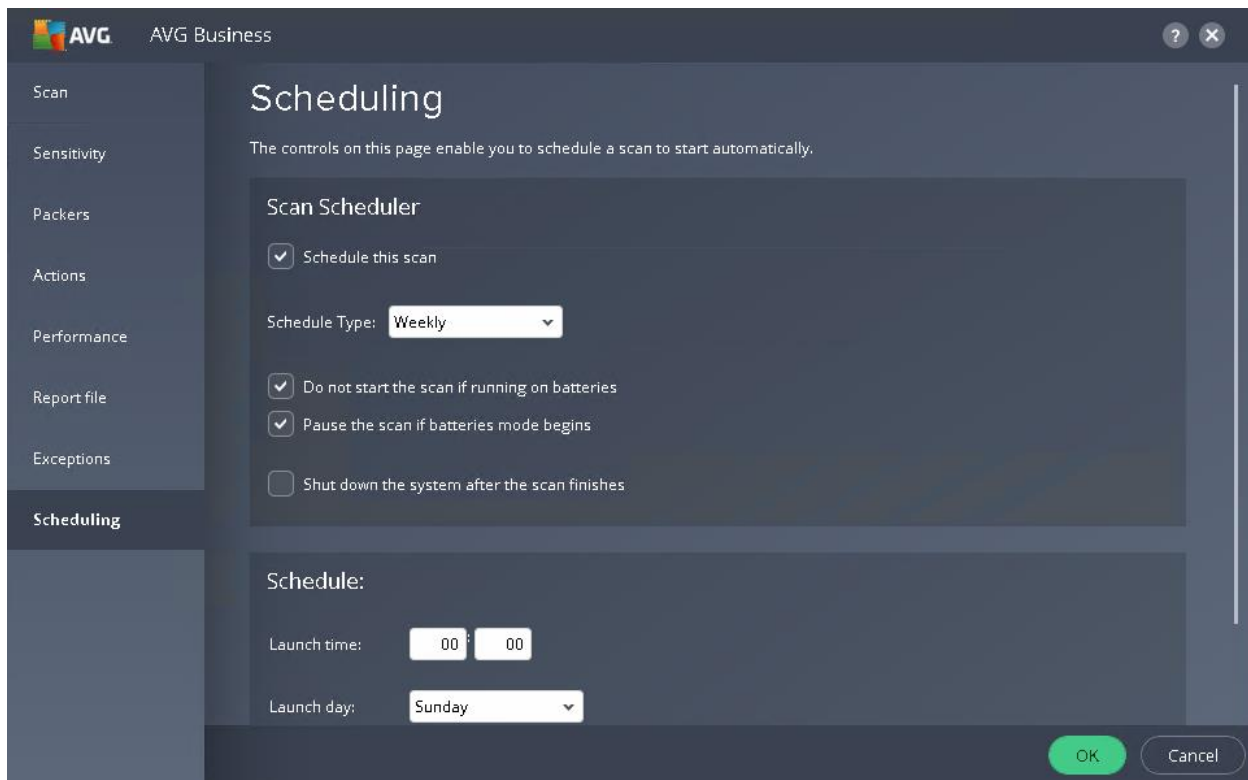
2. On the AVG Home page, **click** the **Menu icon**, then **select Quarantine** from the available options to open the Quarantine area.

On the Quarantine area page, use the scrollbar to view the complete list of results. From this screen, you can select individual files to delete or restore in the case of a false positive result, or you can empty the entire contents at once.



[Figure 11 Quarantine area \(Virus Vault\)](#)

3. On the Quarantine page, **click the Select all viruses checkbox** to select all viruses in the Quarantine area.
4. On the Quarantine page, **click the Delete button** to delete all viruses, malware, and malicious software detected by the application.
5. **Make a screen capture showing the empty Quarantine area (Virus Vault) and paste it into your Lab Report file.**
6. On the Quarantine page, **click the Close button** to close the Quarantine area and return to the AVG Home page.
7. On the AVG Home page, **click the Configuration button** (the gear icon to the right of the Scan Computer button) to open the Other Scans page.
8. On the Other Scans page, **click the Deep Scan Configuration button** (the gear icon to the right of the Deep Scan button) to open the Deep Scan Configuration window.
9. In the Deep Scan Configuration window, **locate the Scheduling section** and **click the Schedule this scan checkbox** to configure AVG to run a scheduled scan.



[Figure 12 Scheduled scan](#)

10. Under the Scan Scheduler header, **select Daily** from the Schedule Type menu.
11. Under the Schedule header, **use the toggle buttons** to set the scheduled run time to **06:00**.
12. **Make a screen capture showing the scheduled scan and paste it into your Lab Report file.**
13. In the Deep Scan Configuration window, **click OK** to apply the changes and return to the AVG home page.
14. **Close the AVG window.**

Part 4: Challenge Question

Explain how the Quarantine mechanism is working in antivirus software packages (in 200 words.)