Student:	Email:
Jacob Jeffers	jjeffers6151@ucumberlands.edu

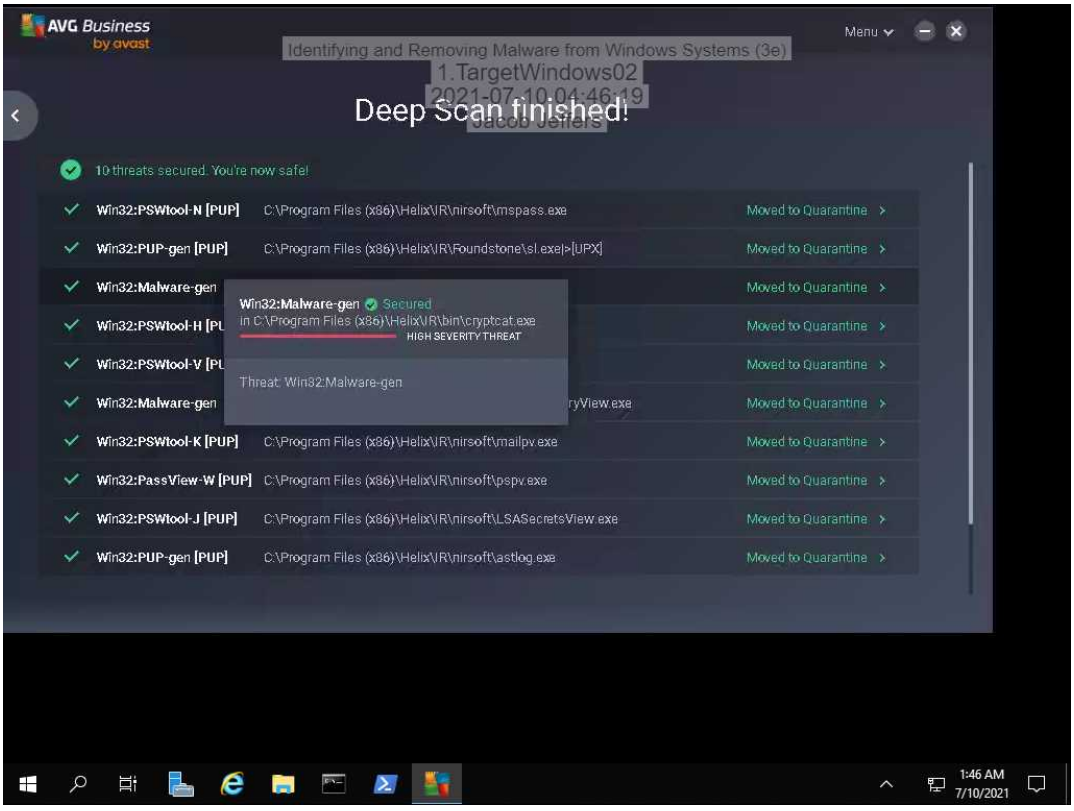
Time on Task:	Progress:
6 hours, 50 minutes	100%

Report Generated: Saturday, July 10, 2021 at 5:47 AM

Section 1: Hands-On Demonstration

Part 1: Scan a Windows Server with AVG Antivirus

7. **Make a screen capture** showing the **Scan Summary**.



9. From your local computer, use your favorite Internet browser to **research** the **identified threat** and **possible remediation steps**, then **document your findings.**

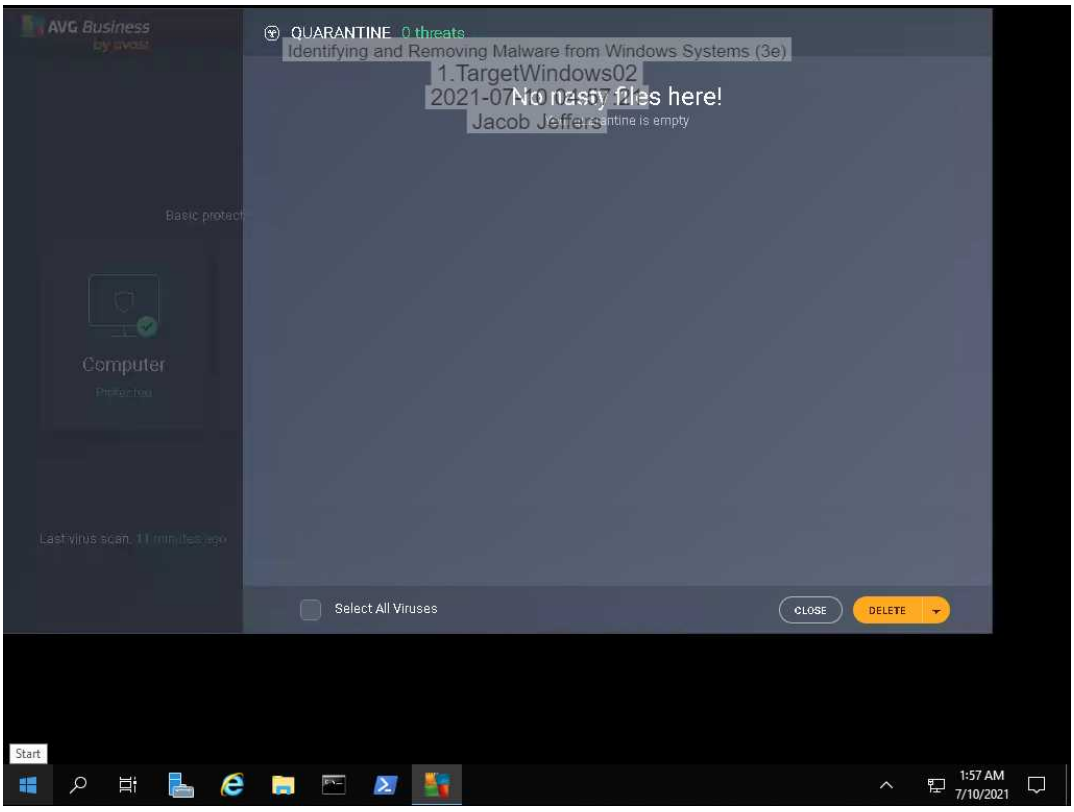
   While AVG Threat Labs is a good place to start, not all of these threats may be listed in that database. Use the entire Internet to find information about the threats in this lab.

Win32.PUP-gen is designed to show ads. The adware can be removed by reinstalling the entire Windows or removed with an external malware finder.

10. **Repeat steps 8-9** for 2 additional threats identified by AVG.

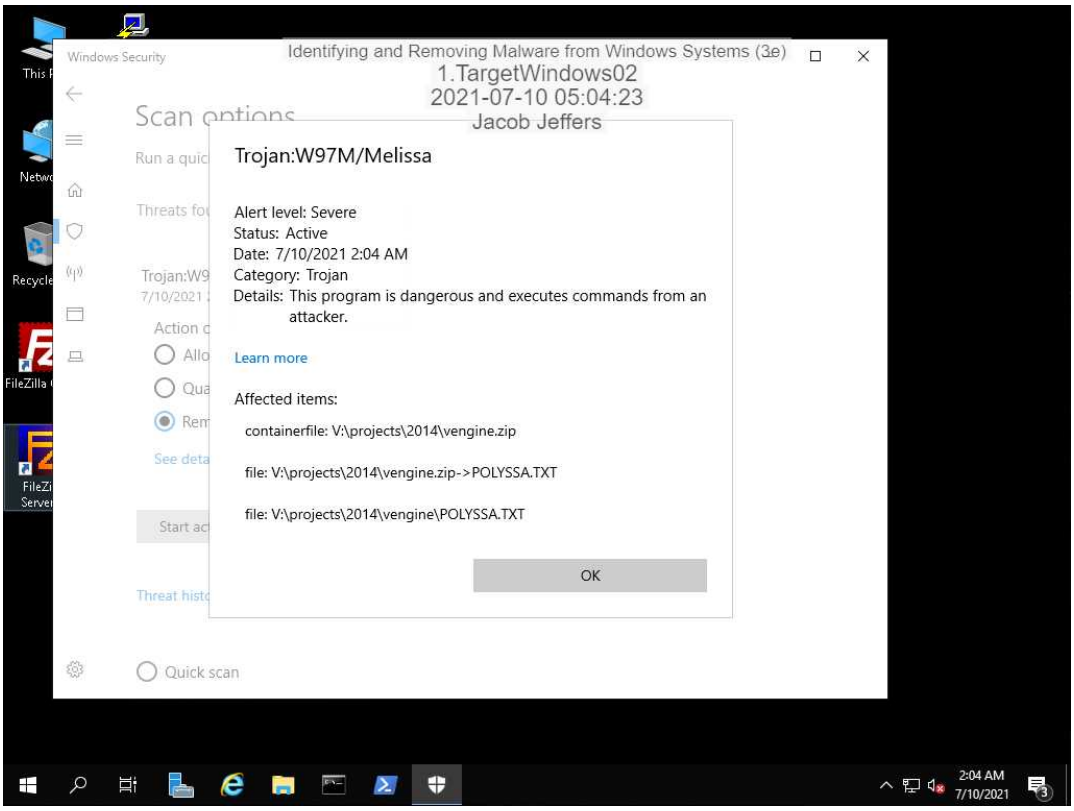
Win32:PassView-W is a dangerous Trojan horse designed to steal password information. It can be removed by reinstalling OS or with a removal tool. Cryptcat is a tool used as a backend tool, and there was an exploit that wasn't recognized by AVG. There are currently no fixes in AVG. The best strategy would be to reinstall Windows.

15. **Make a screen capture** showing the **empty Quarantine area**.

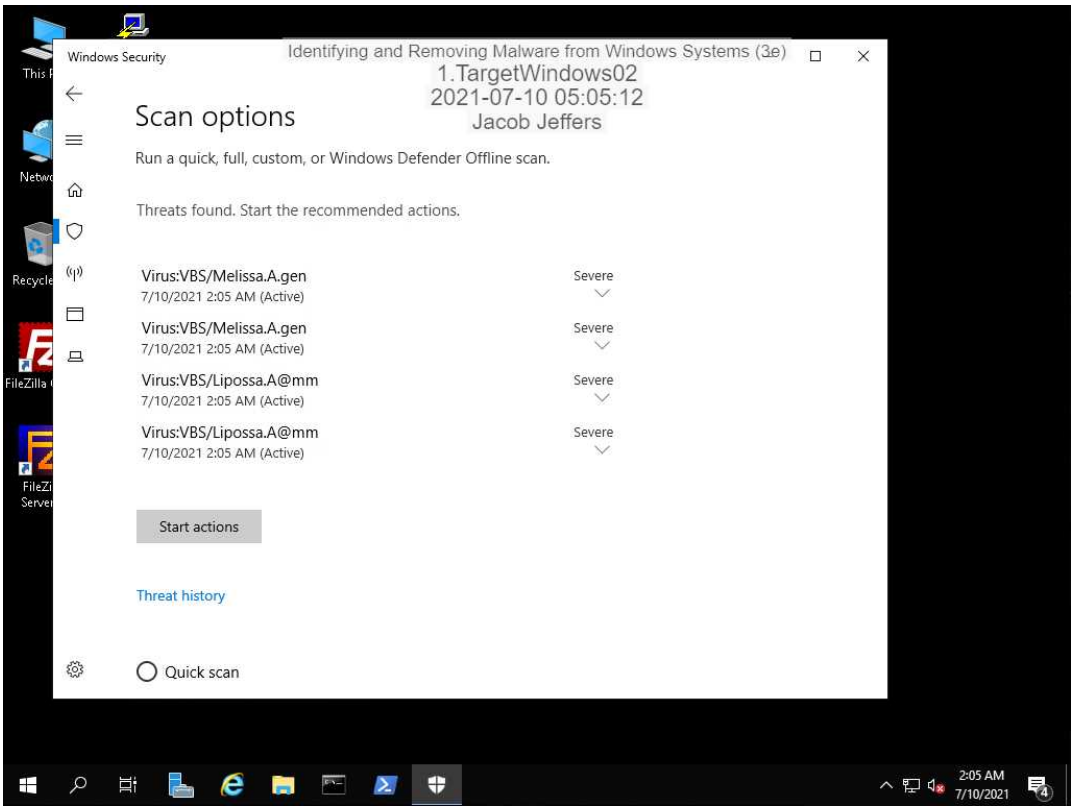


Part 2: Scan a Windows Server with Windows Defender Antivirus

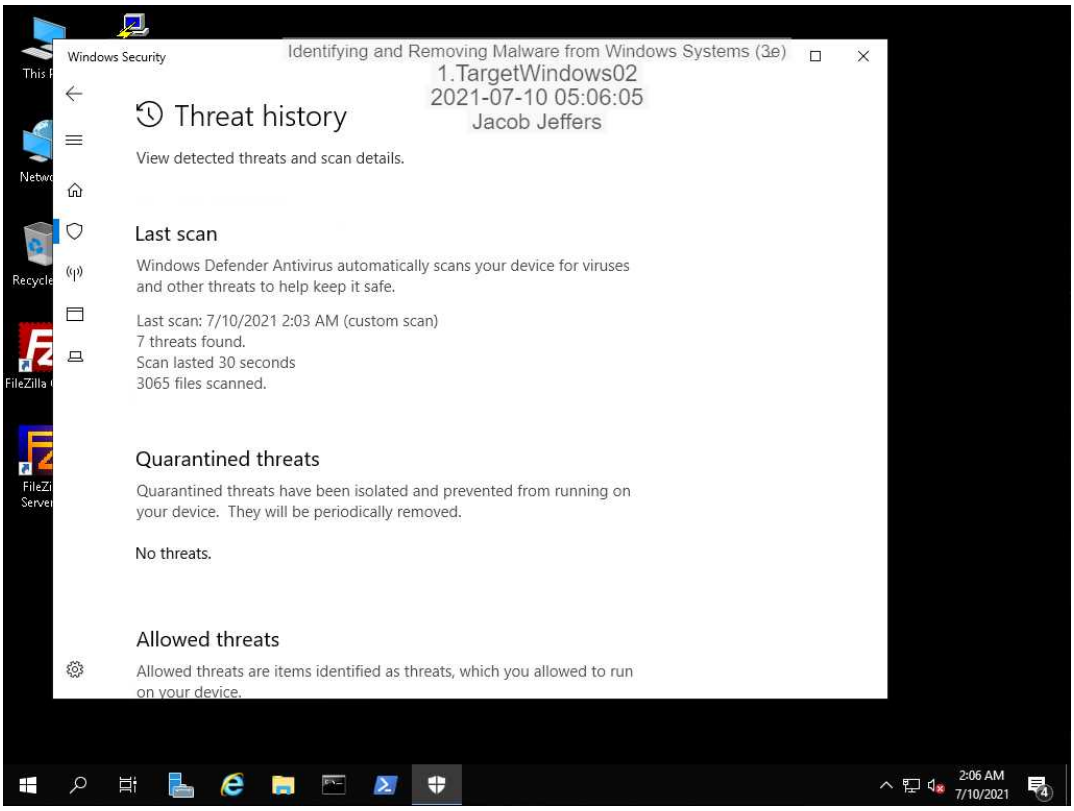
26. **Make a screen capture** showing **the Threat Details in Windows Defender Antivirus**.



29. **Make a screen capture** showing the **results of the cleaning process**.



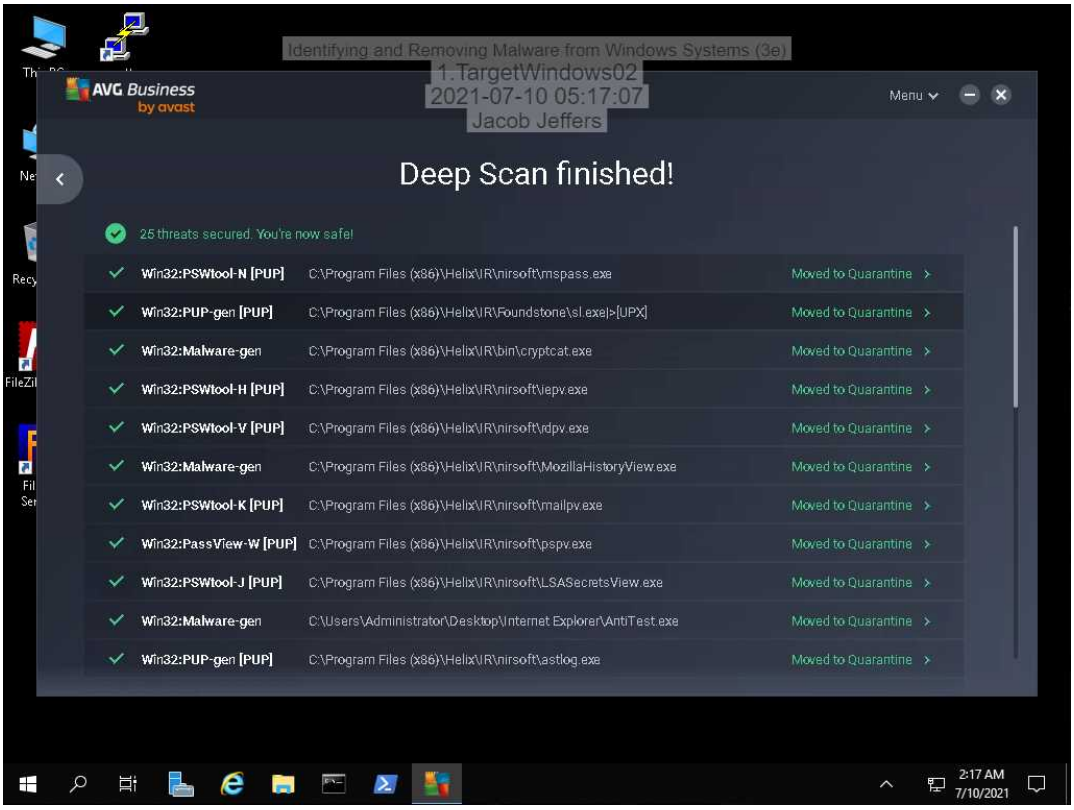
34. **Make a screen capture** showing the **empty Quarantined threats area**.



Section 2: Applied Learning

Part 1: Scan a Windows Server with AVG Antivirus and MalwareBytes Anti-Malware

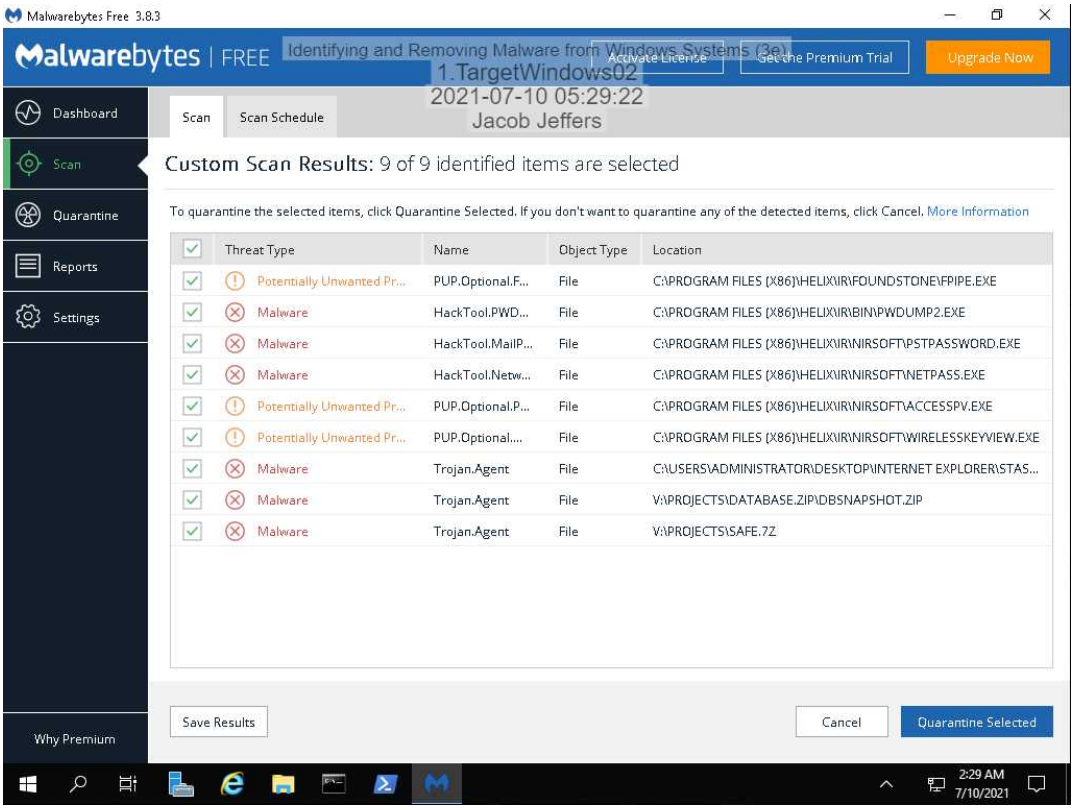
4. **Make a screen capture** showing the **results of the AVG scan.**



5. **Document** the **number of threats** identified by AVG.

25 threats

14. **Make a screen capture** showing the **results of the MalwareBytes scan**.

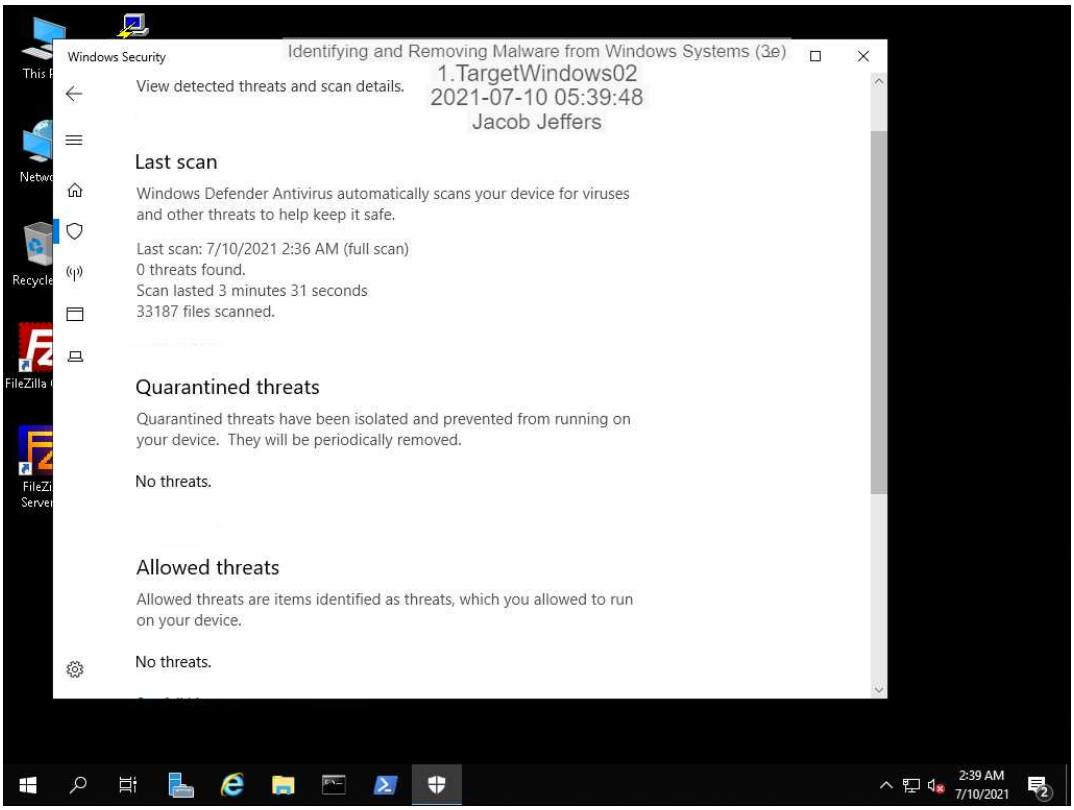


15. **Document** the **number of threats** identified by MalwareBytes.

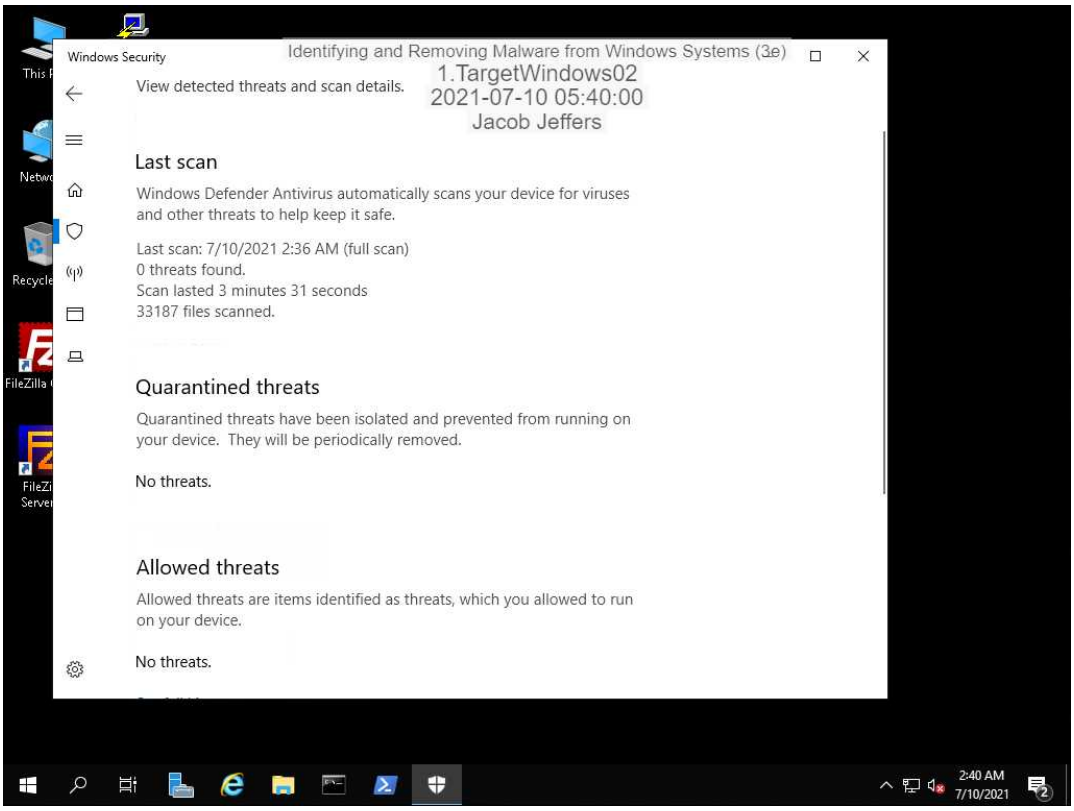
9 threats identified

Part 2: Scan a Windows Server with Windows Defender Antivirus

5. **Make a screen capture** showing the **threats detected by the Full Scan**.



8. **Make a screen capture** showing the **empty Quarantined threats area**.



Section 3: Challenge and Analysis

Part 1: Analysis and Discussion

In the lab, you experimented with three different antivirus software applications: AVG, Windows Defender, and MalwareBytes. Why might someone use more than one application to protect their computer?

It provides vendor diversity for an organization. This is good because each software might have different virus definitions.

Part 2: Tools and Commands

Use the Internet to identify three more commercially available anti-spyware software distributions for home users. Compare the features of each and describe how they vary from the antivirus software applications you used in this lab.

BitDefender, Norton, and WebRoot are all commercially available anti-spyware software distributions. They work similarly to the ones used in this lab.

Part 3: Challenge Exercise

Run a virus scan on your own computer using your existing antivirus program. Provide a summary of the findings and the actions you will take to address them, if necessary. If you do not currently have an antivirus program, research freely available antivirus programs (such as the free versions of AVG and MalwareBytes) and download one.

No current threats found. I use Microsoft Defender for my desktop machine, and I used Clam Antivirus for my Linux VM.