Student:	Email:
Bradley Adams	badams10@my.athens.edu

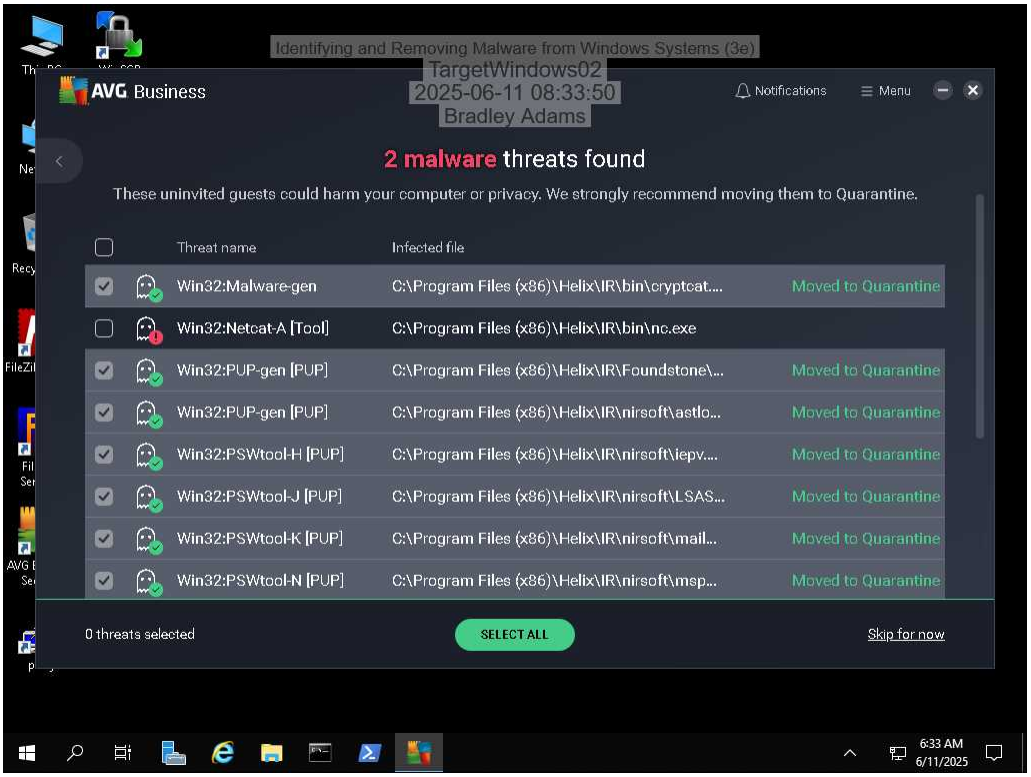
Time on Task:	Progress:
9 hours, 15 minutes	100%

Report Generated: Wednesday, June 11, 2025 at 2:43 PM

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:Netcat-A is a NetCat variant. Trend Micro classifies NetCat as a low-risk hacking utility that can remotely connect to hosts, listen for connections, scan ports, dump traffic, execute programs, persist, randomize ports, etc. It typically shows up because it’s dropped by other malware or is downloaded unknowingly from questionable sites. It enables attackers to establish backdoors, sniff traffic, run commands, or execute further compromises. These actions have a medium damage potential. Trend Micro suggests temporarily disabling System Restore on Windows 7–10 to allow a full disk scan for remediation and recovery.

Source:
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/hacktool.win32.netcat.aarue

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

Win32:PSWtool-H

Kaspersky states that PSWTool is a class of malicious software for password?viewing designed to reveal stored or hidden passwords in browsers and email clients. Microsoft refers to it as Trojan:Win32/PswTool, stating the threat's behavior can include system slowdowns, modified files, altered desktop settings, crashes, or storage issues.

Remediation should begin with a full system scan using an up?to?date antivirus solution like Microsoft Defender to detect and remove the virus. After remediation is complete, all user credentials that may have been exposed should be changed.

Sources:
https://threats.kaspersky.com/en/threat/PSWTool.Win32.PassView
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/PswTool&ThreatID=2147852315

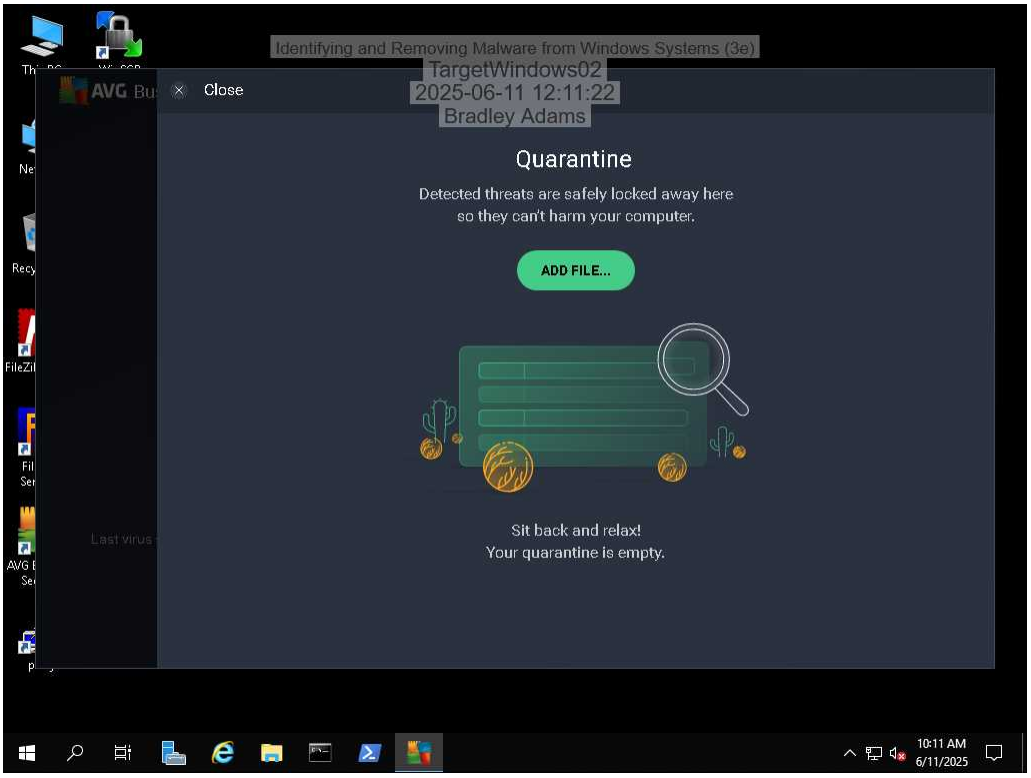
Win32:Malware-gen

Win32:Malware?gen is not a specific strain of malware but a generic flag used by antivirus tools to indicate that a 32?bit Windows file behaves like known malware, even if it doesn't match any exact signature. These files indicate a Trojan capable of downloading and installing additional malware, logging keystrokes, stealing sensitive data, opening backdoors, or displaying aggressive malicious ads.

Remediate Win32:Malware?gen by disconnecting the system from the Internet to prevent further compromise. Boot into Safe Mode and kill any suspicious processes via Task Manager. Then, an antivirus suite such as Windows Defender can perform a full system scan, quarantining or deleting all identified threats. If automated tools fail, follow these manual steps: remove unknown startup entries, delete temporary files, inspect and clean related Registry keys, and uninstall any recently installed software. After cleanup, run a second full scan to confirm removal and restart the system normally.

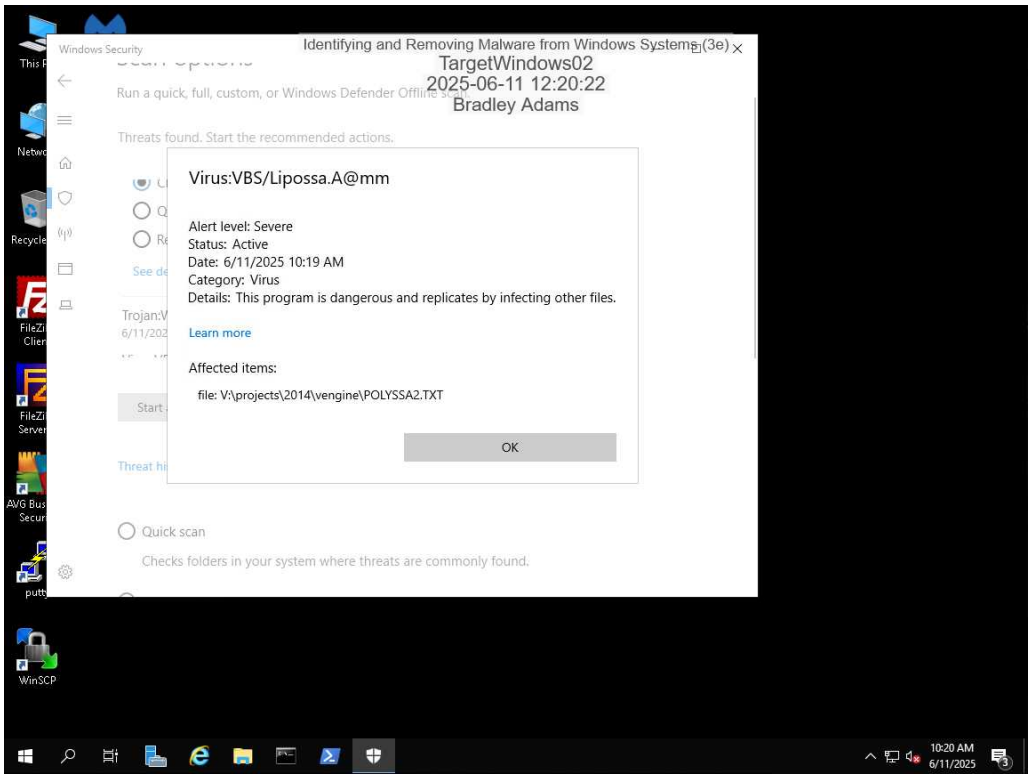
Sources:
https://www.partitionwizard.com/partitionmanager/win32-malware-gen.html

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

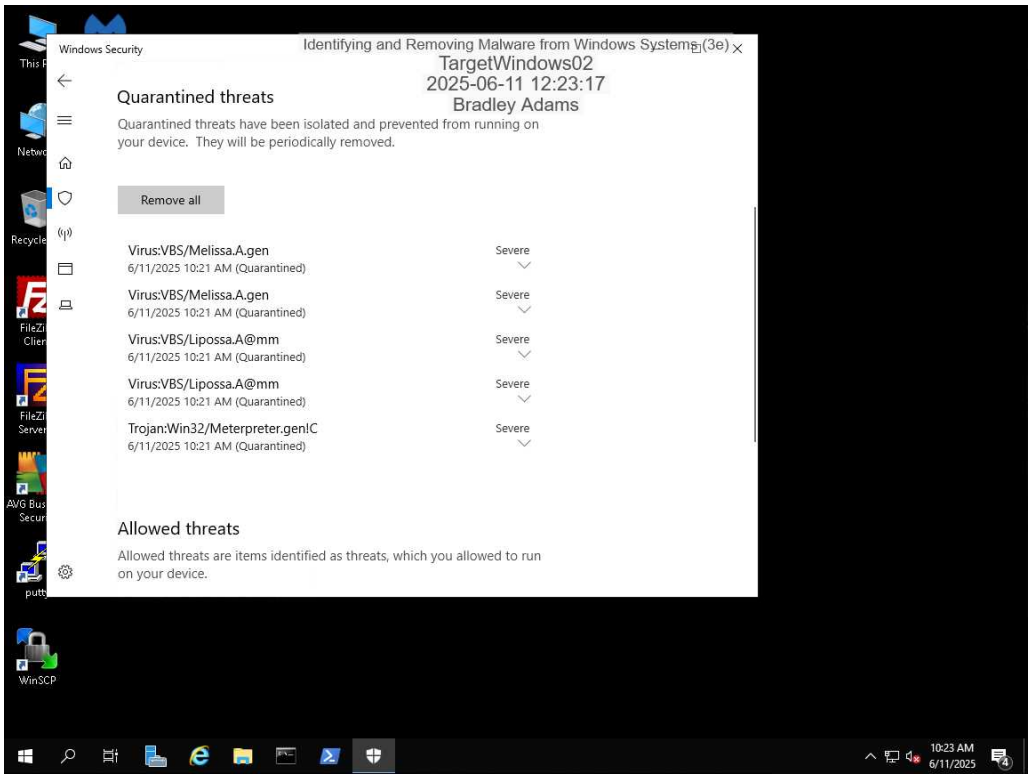


Part 2: Scan a Windows Server with Windows Defender Antivirus

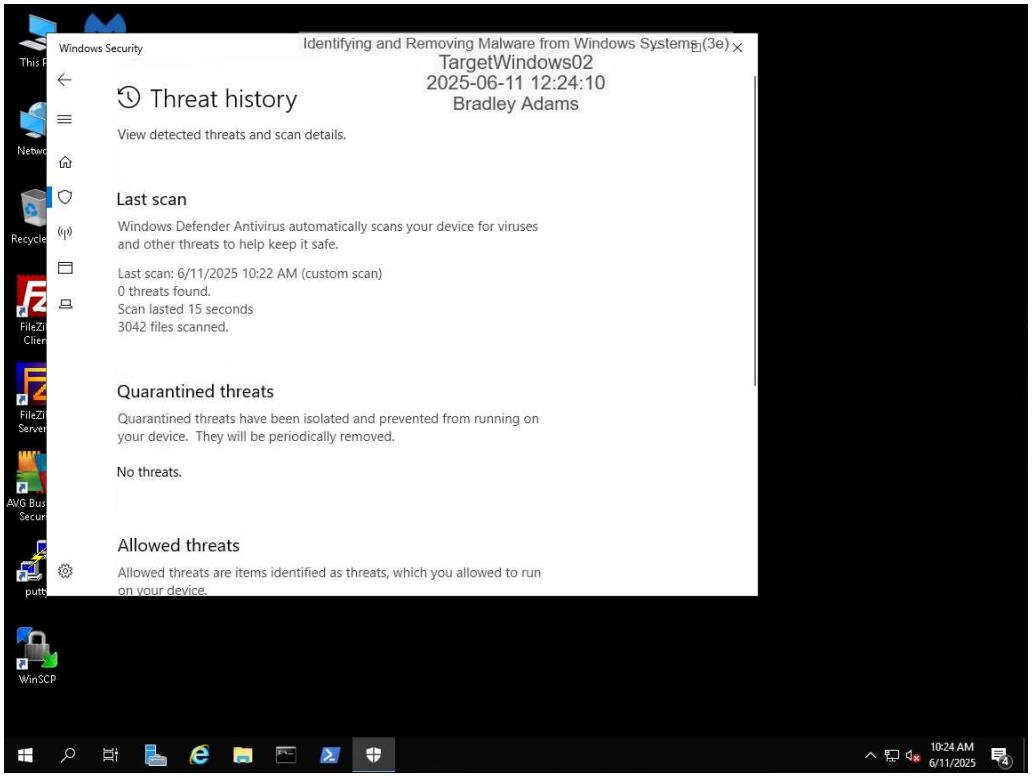
26. **Make a screen capture** showing **the Threat Details in Windows Defender Antivirus**.



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



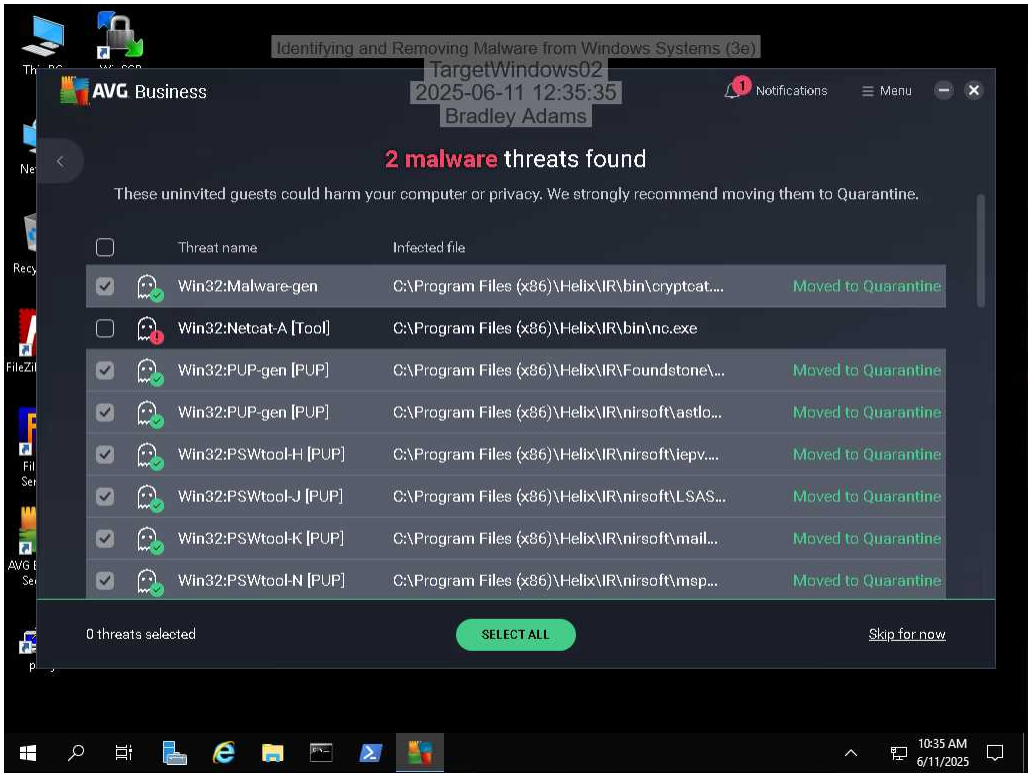
34. **Make a screen capture** showing the **empty Quarantined threats area**.



Section 2: Applied Learning

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

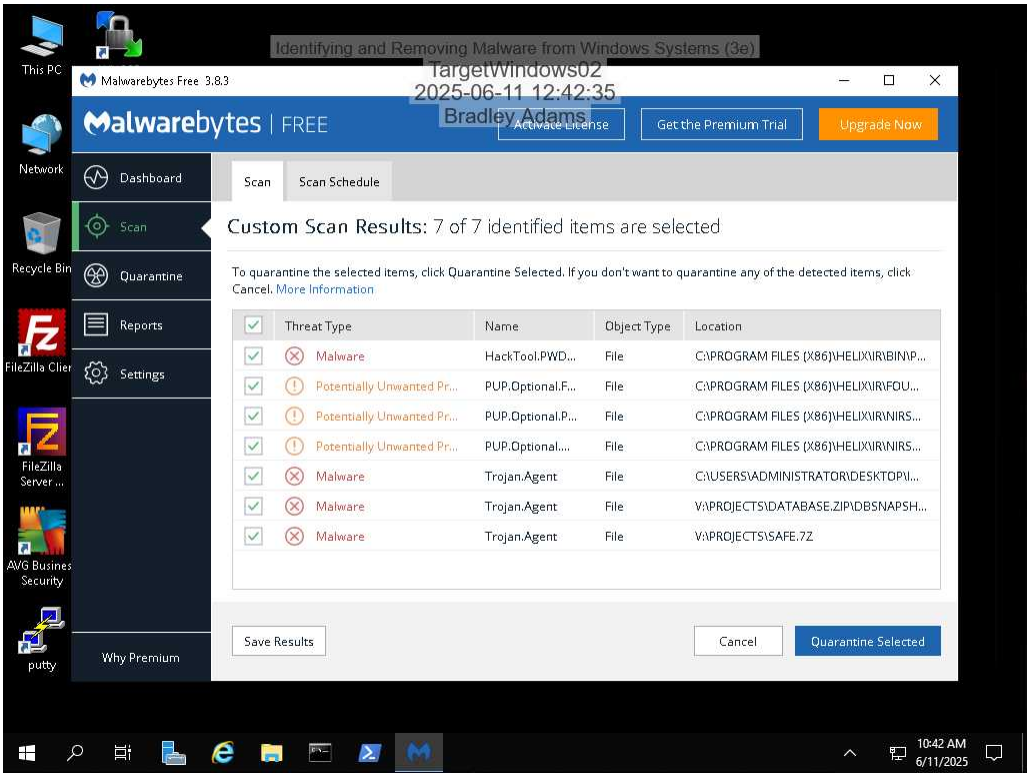
4. **Make a screen capture** showing the **results of the AVG scan.**



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

2 malware threats found

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

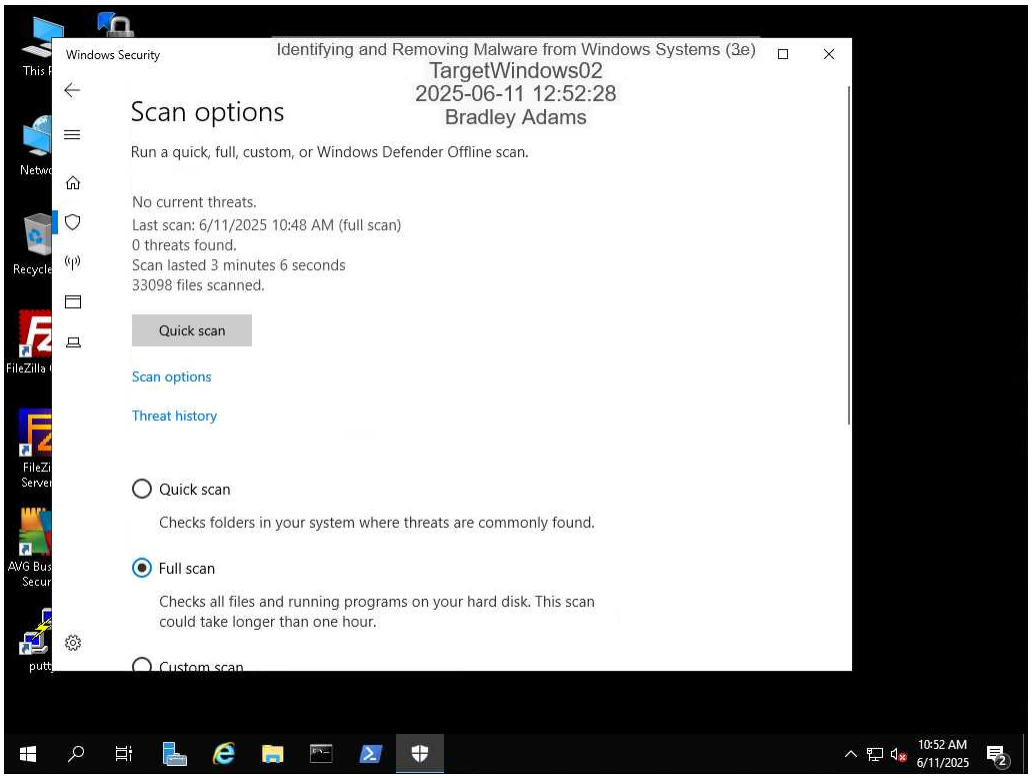


15. **Document** the **number of threats** identified by MalwareBytes.

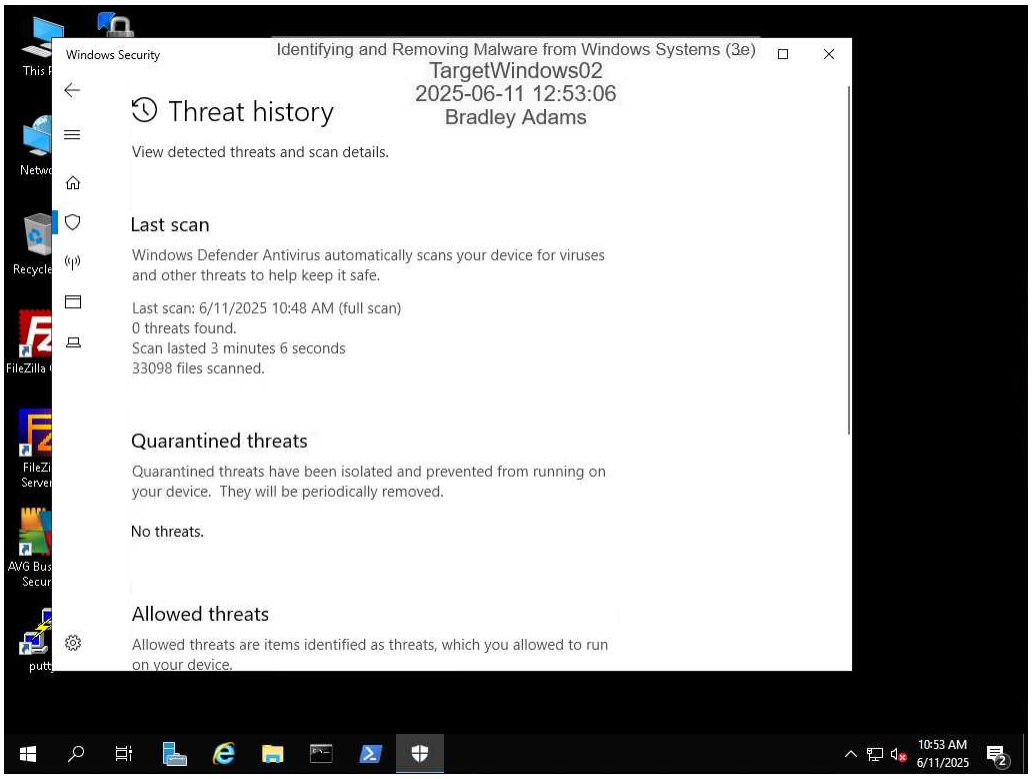
7 items identified

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?

Anti-malware programs can play tug-of-war with each other if they are run simultaneously. However, if they are run independently in a toolset, different vendors can offer increased protection from various engines and detection methods. Running a primary antivirus platform with a "second or third opinion" option may improve the ability to catch missed threats or further remove 'stubborn' threats.

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.

I chose the following 'anti-spyware distributions': IronVest, Bitdefender, and Privacy Bee.

IronVest is a password manager, email and credit card masker, virtual phone numbers manager, anti?phishing, and anti?tracker protection application. It provides a decentralized, blockchain?based foundation designed to secure account access from login through session and transaction signing without friction.

Bitdefender offers malware and ransomware protection, phishing and web?attack defenses, a built?in password manager, secure VPN, crypto mining defense, safe banking tools, anti?tracker modules, and cross?platform coverage for Windows, macOS, iOS, and Android.

Privacy Bee focuses on privacy by removing personal data from data broker sites, monitoring exposure, and helping users manage their digital footprint. It lacks direct malware protection or system defense.

AVG is a general?purpose antivirus with AI?driven detection and decent web and email protection.

Malwarebytes specializes in malware and adware cleanup with a strong heuristic engine and fast scanning. While its premium version adds real?time protection, it doesn't offer safeguards for sandboxing, password management, or identity theft.

Windows Defender integrates malware protection with good usability and offline scanning. However, it lacks the advanced privacy shields, layered ransomware tools, password vaults, or data masking that the others offer.

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.

I use Windows Defender under Windows 11 on my student laptop. I occasionally download and run the Microsoft Windows Malicious Software Removal Tool.

When I log in to my laptop, I immediately run three routines: Windows Update, Microsoft Store Updates, and a PowerShell 'winget upgrade' script.

Here is the script:

```
# Upgrade all installed applications using winget
Write-Output "Starting upgrade for all applications..."
winget upgrade --all --silent --accept-package-agreements --accept-source-agreements
Write-Output "Upgrade complete."
```

This keeps all my applications and the Windows OS updated.

The Windows Defender Quick scan took 6 minutes and 19 seconds, and 42523 files were scanned. I did not have any threats or actions to take.