

# Identifying and Removing Malware from Windows Systems (4e)

## Security Strategies in Windows Platforms and Applications 4e - Lab 4

Student:

Angie Rodriguez

Email:

angie.rodriguez287@my.tccd.edu

Time on Task:

4 hours, 26 minutes

Progress:

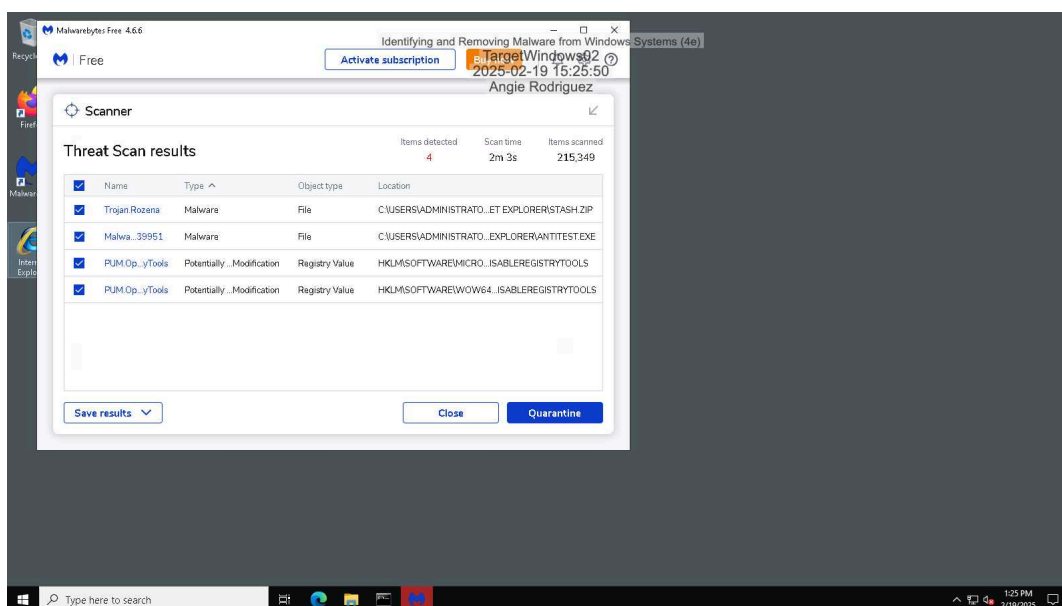
100%

Report Generated: Wednesday, March 5, 2025 at 7:42 PM

## Section 1: Hands-On Demonstration

### Part 1: Scan a Windows Server with Malwarebytes

6. Make a screen capture showing the **scan summary**.

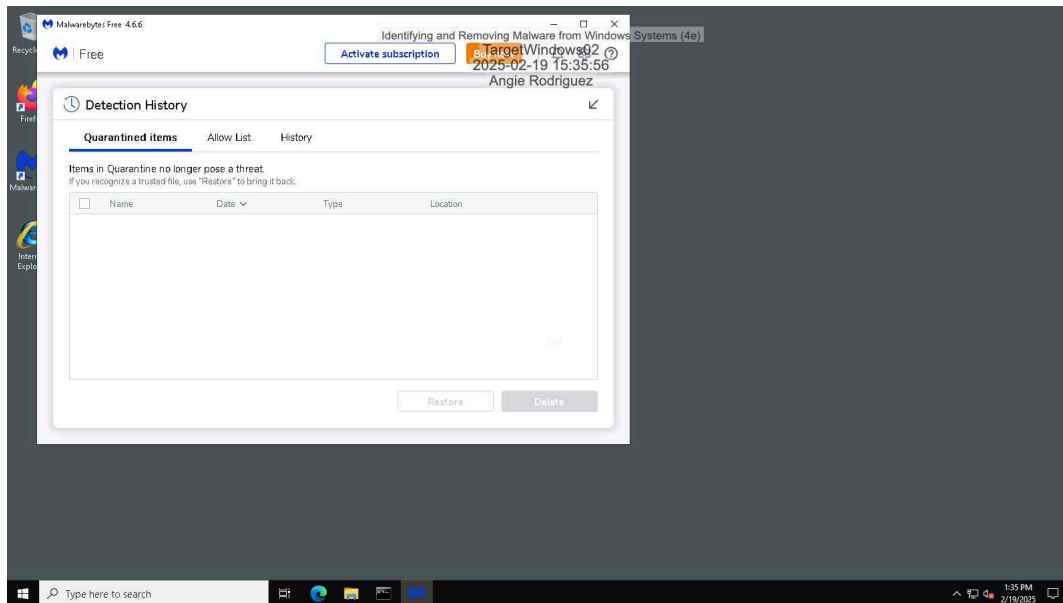


8. From your local computer, use your favorite internet browser to **research** the **identified threat** and **possible remediation steps**, then **document your findings**.

Trojan Rozena: ransomware type of malware. s a type of malware classified as a remote access trojan (RAT). It is designed to provide attackers unauthorized access to an infected system, enabling them to steal data, execute commands, etc.

Malware AI 3724139951 :employs machine learning techniques to identify potential threats without specific detection rules

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

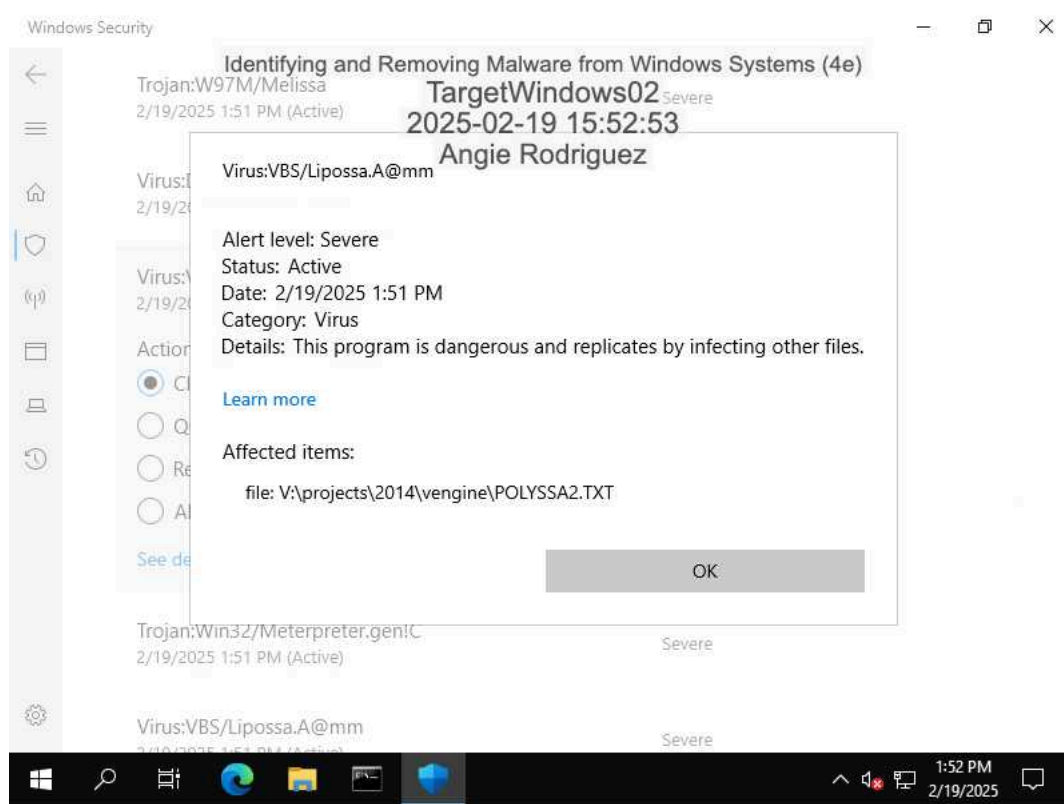


## Part 2: Scan a Windows Server with Microsoft Defender Antivirus

## Identifying and Removing Malware from Windows Systems (4e)

Security Strategies in Windows Platforms and Applications 4e - Lab 4

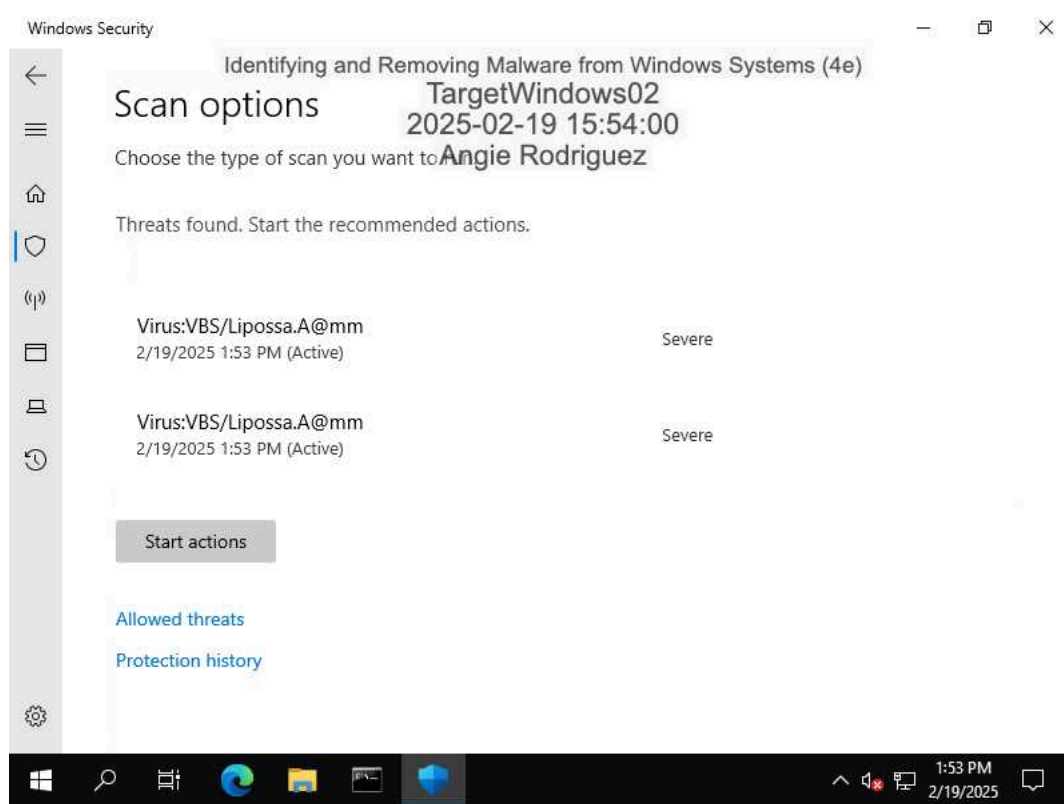
26. Make a screen capture showing the threat details in Microsoft Defender Antivirus.



# Identifying and Removing Malware from Windows Systems (4e)

Security Strategies in Windows Platforms and Applications 4e - Lab 4

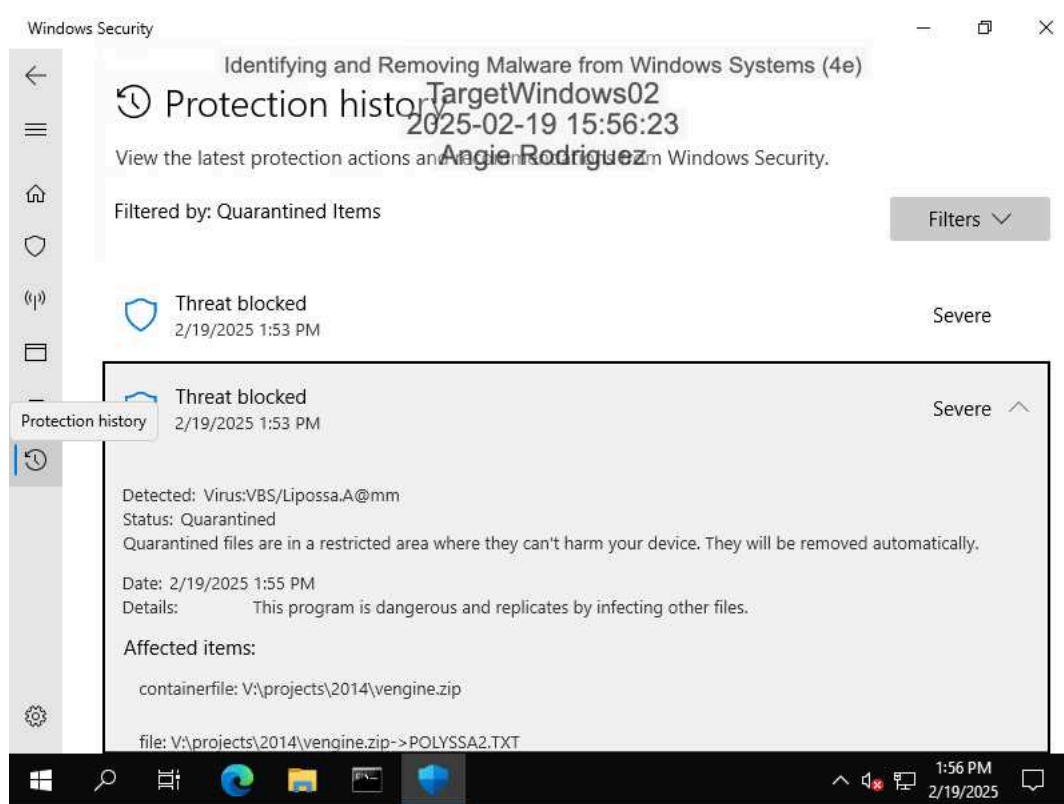
29. Make a screen capture showing the results of the cleaning process.



# Identifying and Removing Malware from Windows Systems (4e)

## Security Strategies in Windows Platforms and Applications 4e - Lab 4

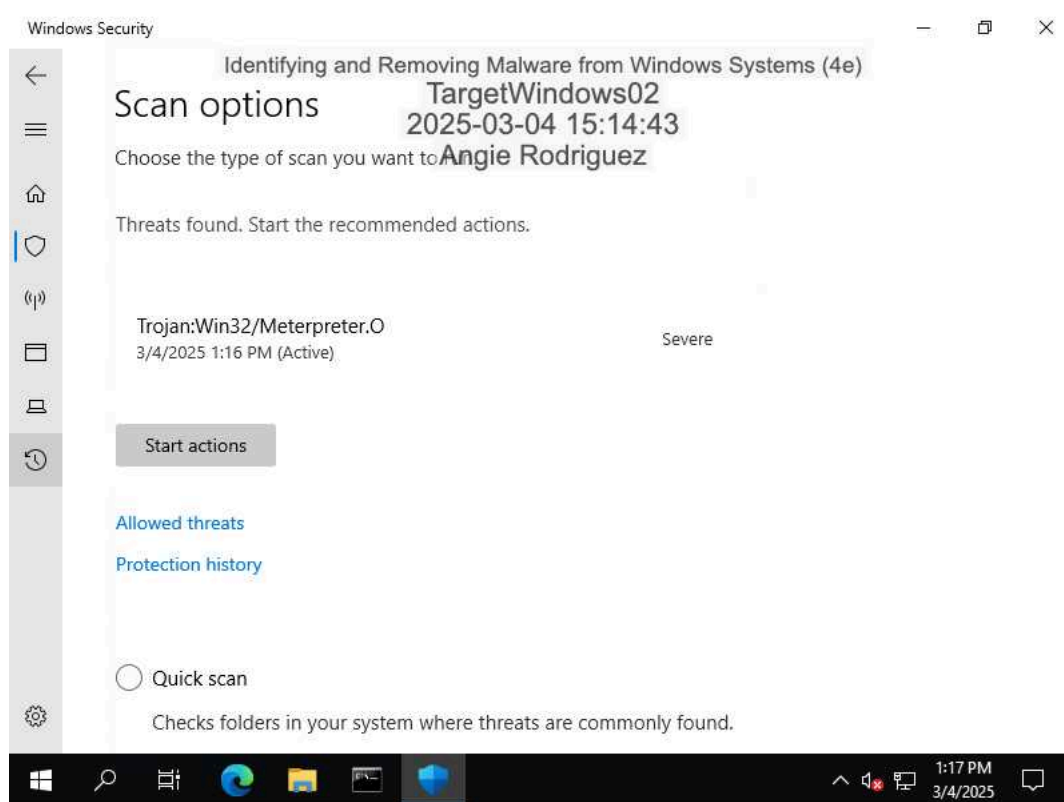
37. Make a screen capture showing the **blocked Quarantined threats list**.



### Section 2: Applied Learning

#### Part 1: Scan a Windows Server with Microsoft Defender Antivirus

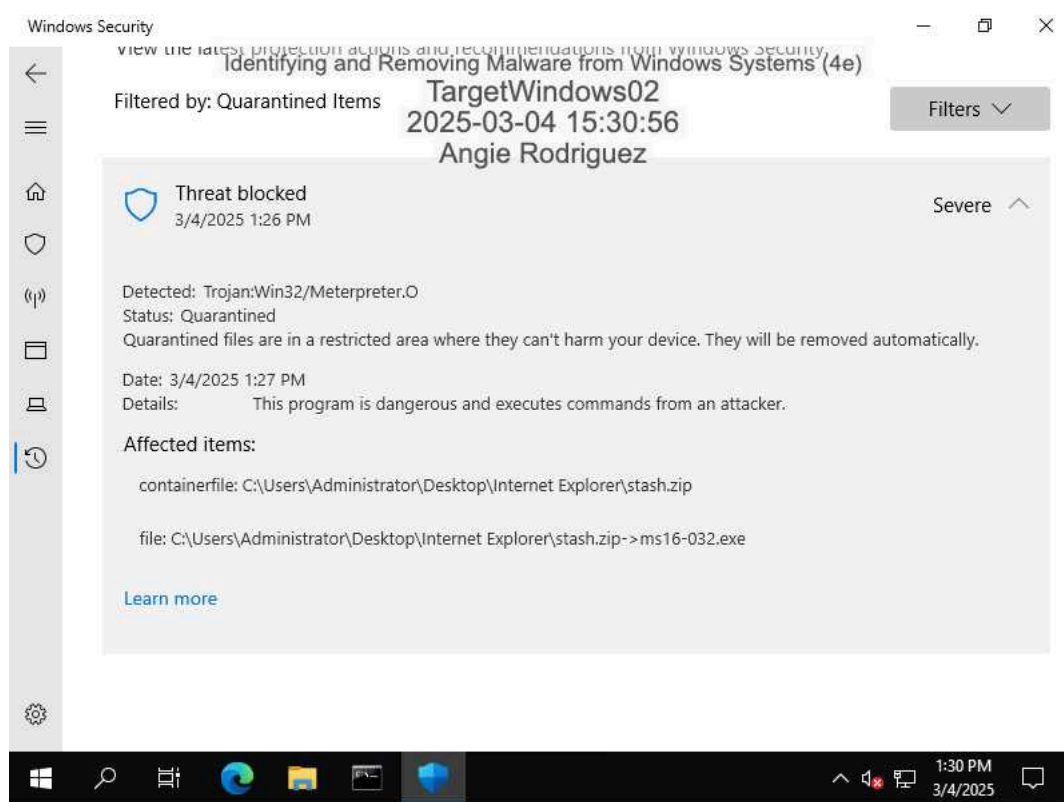
5. Make a screen capture showing the threat detected by the Full Scan.



# Identifying and Removing Malware from Windows Systems (4e)

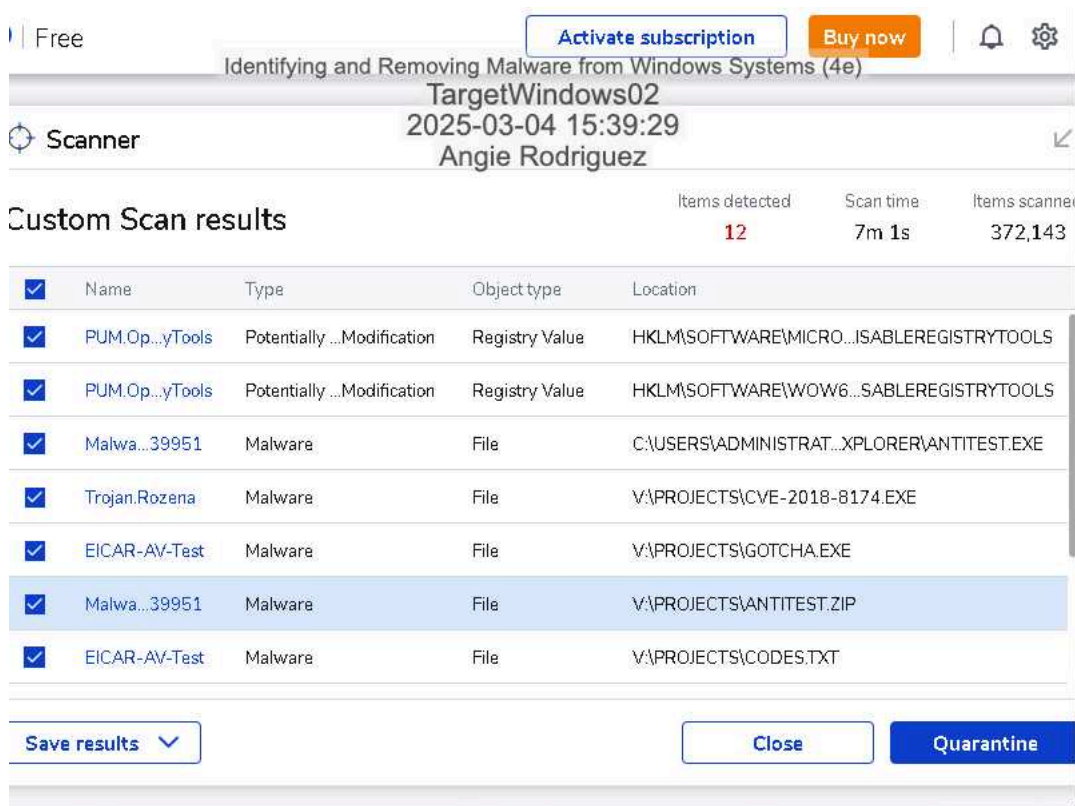
## Security Strategies in Windows Platforms and Applications 4e - Lab 4

8. **Make a screen capture** showing the **confirmation that the threat was successfully blocked**.



## Part 2: Run a Custom Scan on a Windows Server with Malwarebytes

7. Make a screen capture showing the results of the Malwarebytes scan.



8. Document the number of threats identified by Malwarebytes.

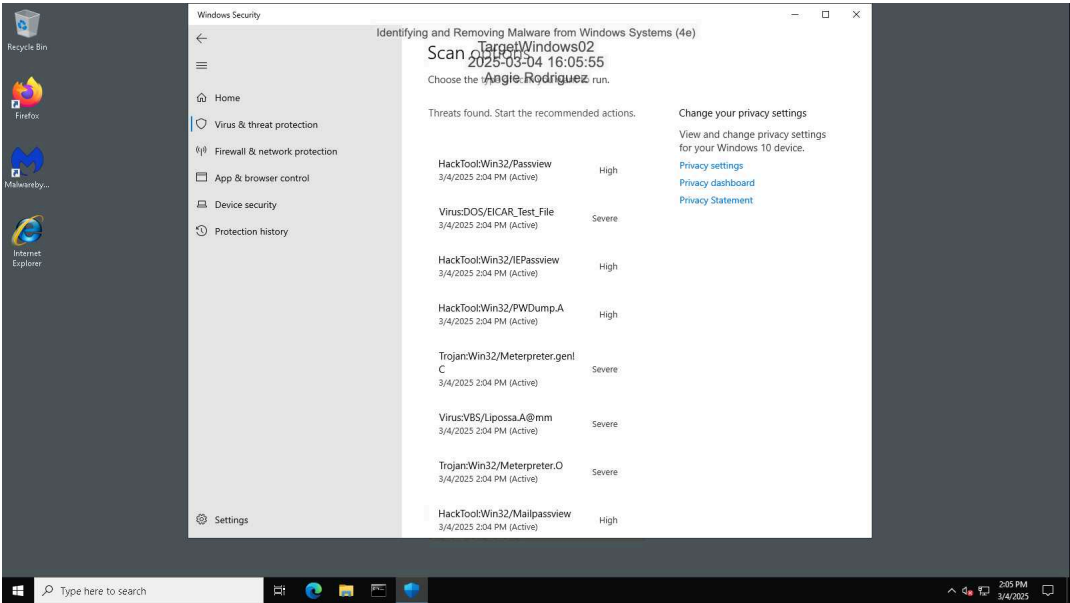
items detected 12



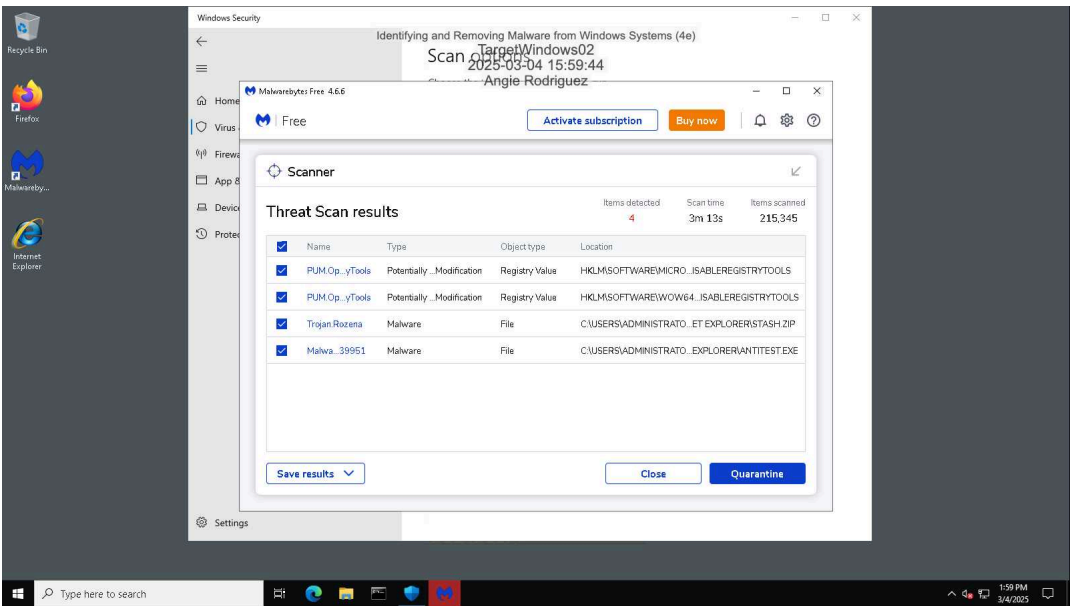
Section 3: Challenge and Analysis

Part 1: Compare Malwarebytes and Microsoft Defender Scan Results

Make a screen capture showing the results of the Windows Defender scan.



Make a screen capture showing the results of the Malwarebytes scan.



# Identifying and Removing Malware from Windows Systems (4e)

## Security Strategies in Windows Platforms and Applications 4e - Lab 4

---

**Compare the results** of the two scans and **note the differences** in the threats detected.

the microsoft defender results were definitely more extensive than the malwarebytes results

**Make a screen capture** showing the **cleared Quarantined items list in Malwarebytes**.

