INFO33192 – Lab Submission Template (Generic for All Labs)

# Student Information

Student ID: 991589924

Name: Majd Abboud

Lab Number: 1

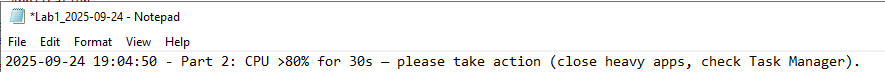
Task Title: **Part 2 CPU usage** > 80% warning for 30 seconds

Screenshot(s):

Picture

Verification Evidence (logs, PowerShell output, configs)

Log File:



Task Title: **Part 2: Memory usage** (if >85%, log warning).

Screenshot(s):



Verification Evidence (logs, PowerShell output, configs)

Log File:



Task Title: **Part 2 Disk space** (if <15% free on C:, log critical)

Screenshot(s):



Verification Evidence (logs, PowerShell output, configs)

Log File:



Task Title: **Part 3 CPU usage** > 80% Terminate After 60 seconds

Screenshot(s):

  
Verification Evidence (logs, PowerShell output, configs)

Log File:



Task Title: **Part 3: Memory usage (if >85%, log warning).**

Screenshot(s):



Verification Evidence (logs, PowerShell output, configs)

Log File:

Task Title: **Part 3 low disk space detected →** delete files in C:\Temp and log space freed.

Screenshot(s):

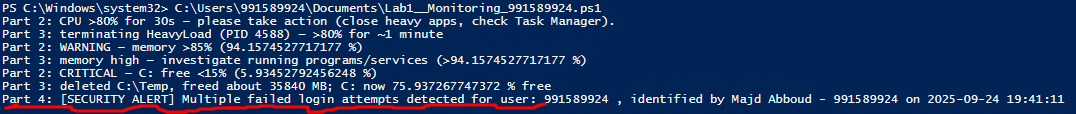


Verification Evidence (logs, PowerShell output, configs)

Log File:

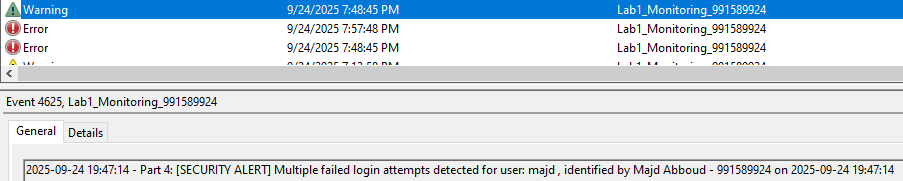
Task Title: **Part 4 Failed login attempts**

Screenshot(s):

  
Verification Evidence (logs, PowerShell output, configs)

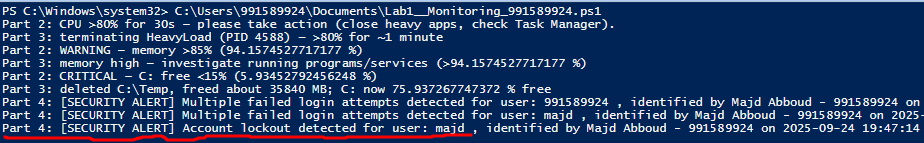
Log File:





Task Title: **Part 4 Account Lockouts**

Screenshot(s):



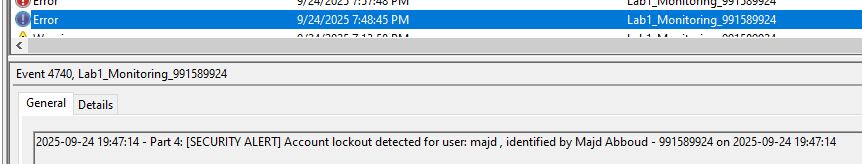
Verification Evidence (logs, PowerShell output, configs)

Changed the lockout threshold to lockout after 2 attempts:



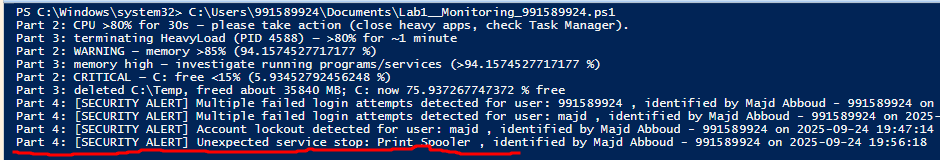
Log file:



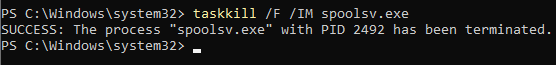


Task Title: **Part 4 Unexpected service stops**

Screenshot(s):

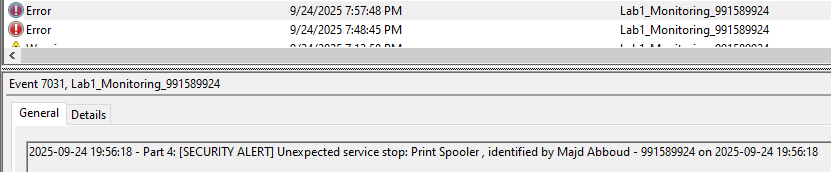


Verification Evidence (logs, PowerShell output, configs)



Log File:

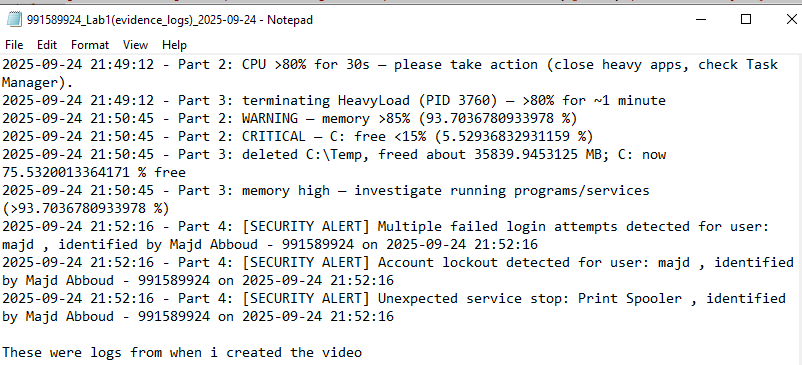




Task Title: **Part 5**

Monitoring screenshot and event viewer logs in parts above. Full log file below.

Screenshot(s):

  
  
Video Confirmation Statement:

My video shows all the steps required within Lab 1 in my windows server VM. At the start of the video, I display my Student ID in Notepad, then I demonstrate the Script, the Event Viewer and the logs as well as any additional configurations or work. The video is named 991589924\_Lab1\_video.mp4.”

# Reflection (5–7 sentences)

Write your reflection here:

1. Why is it important to log both health and security events?  
   Logging health events shows whether systems are running properly, while security events reveal potential threats or attacks. Together, they give context—like whether a crash was caused by a hardware issue or a cyber intrusion. Without both, investigations are incomplete and slower.
2. What risks exist if remediation actions are not logged?  
    If you don’t log remediation, there’s no record of what was done, which makes repeating or verifying fixes difficult. It creates blind spots in audits and compliance reviews. Attackers could even exploit the same issue again because there’s no clear history of resolution.
3. How does least privilege reduce attack surface for automated scripts?  
   Least privilege ensures a script only has access to what it needs, nothing more. This way, if the script is hijacked, the attacker’s reach is very limited. It reduces the overall attack surface and prevents unnecessary system exposure.