Memory Forensics Analysis Report

Report Information

Analysis Date:	2025-10-13 16:04:51
Memory File:	/Users/tharageshtharun/Downloads/Challenge.raw
Total Processes:	53
Suspicious Processes:	9
Analysis Status:	COMPLETED

Executive Summary

SECURITY ALERT: 9 suspicious processes detected out of 53 total processes analyzed. This indicates potential malicious activity in the memory dump. Immediate investigation is recommended.

Detailed Findings

Process ID: 336 - csrss.exe

Process Name:	csrss.exe
Parent PID:	328
Parent Name:	

Security Concerns:

1. Orphaned process. Parent with PID 328 is not in the process list.
2. Unexpected parent. Expected: 'smss.exe', Found: 'None'

Process ID: 384 - wininit.exe

Process Name:	wininit.exe
Parent PID:	328

Parent Name:	

Security Concerns:

1. Orphaned process. Parent with PID 328 is not in the process list.
2. Unexpected parent. Expected: 'smss.exe', Found: 'None'

Process ID: 396 - csrss.exe

Process Name:	csrss.exe
Parent PID:	376
Parent Name:	

Security Concerns:

1. Orphaned process. Parent with PID 376 is not in the process list.
2. Unexpected parent. Expected: 'smss.exe', Found: 'None'

Process ID: 436 - winlogon.exe

Process Name:	winlogon.exe
Parent PID:	376
Parent Name:	

Security Concerns:

1. Orphaned process. Parent with PID 376 is not in the process list.
2. Unexpected parent. Expected: 'smss.exe', Found: 'None'

Process ID: 1944 - explorer.exe

Process Name:	explorer.exe
Parent PID:	1844
Parent Name:	

Security Concerns:

1. Orphaned process. Parent with PID 1844 is not in the process list.
2. Unexpected parent. Expected: 'userinit.exe', Found: 'None'

Process ID: 1292 - GoogleCrashHan

Process Name:	GoogleCrashHan
Parent PID:	1928
Parent Name:	Unknown (Parent PID not in list)

Security Concerns:

1. Orphaned process. Parent with PID 1928 is not in the process list.

Process ID: 924 - GoogleCrashHan

Process Name:	GoogleCrashHan
Parent PID:	1928
Parent Name:	Unknown (Parent PID not in list)

Security Concerns:

1. Orphaned process. Parent with PID 1928 is not in the process list.

Process ID: 2080 - firefox.exe

Process Name:	firefox.exe
Parent PID:	3060
Parent Name:	Unknown (Parent PID not in list)

Security Concerns:

1. Orphaned process. Parent with PID 3060 is not in the process list.

Process ID: 2256 - GoogleUpdate.e

Process Name:	GoogleUpdate.e
Parent PID:	2396
Parent Name:	Unknown (Parent PID not in list)

Security Concerns:

1. Orphaned process. Parent with PID 2396 is not in the process list.

Recommendations

Immediate Actions:

- Investigate flagged processes immediately
- Check for persistence mechanisms

- Review network connections and firewall logs
- Consider system isolation if critical threats are found
- Document all findings for incident response

Generated by AI-Powered Memory Analyzer