CTF Write-up — Snowdrift Memory

Category: Forensics

Points: 50

Author: p3f0rm3r ({x0x} Team)

Description

The challenge asks which Volatility plugin is used to list running processes from a memory dump.

Solution

I searched online for Volatility process listing plugins and found that the correct plugin is pslist.

Example command:

volatility -f memory.dmp pslist

Flag

atcctf_pslist

Conclusion

This challenge tests basic knowledge of memory forensics and Volatility tools.