OS Credential Dumping: Proc Filesystem, Sub-technique T1003.007 - Enterprise

Archived: 2026-04-05 18:24:03 UTC

Adversaries may gather credentials from the proc filesystem or `/proc`. The proc filesystem is a pseudo-filesystem used as an interface to kernel data structures for Linux based systems managing virtual memory. For each process, the `/proc/<PID>/maps` file shows how memory is mapped within the process's virtual address space. And `/proc/<PID>/mem`, exposed for debugging purposes, provides access to the process's virtual address space.[1][2]

When executing with root privileges, adversaries can search these memory locations for all processes on a system that contain patterns indicative of credentials. Adversaries may use regex patterns, such as `grep -E "^[0-9a-f-]*r" /proc/"$pid"/maps | cut -d' ' -f 1`, to look for fixed strings in memory structures or cached hashes.[3] When running without privileged access, processes can still view their own virtual memory locations. Some services or programs may save credentials in clear text inside the process's memory.[4][5]

If running as or with the permissions of a web browser, a process can search the `/maps` & `/mem` locations for common website credential patterns (that can also be used to find adjacent memory within the same structure) in which hashes or cleartext credentials may be located.

Source: https://attack.mitre.org/techniques/T1003/007