# TTP Detail – T1003.007

## TTP Information

Name: Proc Filesystem

Description: 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.(Citation: Picus Labs Proc cump 2022)(Citation: baeldung Linux proc map 2022)

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 <code>grep -E "^[0-9a-f-]\* r" /proc/"$pid"/maps | cut -d' ' -f 1</code>, to look for fixed strings in memory structures or cached hashes.(Citation: atomic-red proc file system) 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.(Citation: MimiPenguin GitHub May 2017)(Citation: Polop Linux PrivEsc Gitbook)

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.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* PACEMAKER

## Tools

* LaZagne
* MimiPenguin