# TTP Detail – T1003.008

## TTP Information

Name: /etc/passwd and /etc/shadow

Description: Adversaries may attempt to dump the contents of <code>/etc/passwd</code> and <code>/etc/shadow</code> to enable offline password cracking. Most modern Linux operating systems use a combination of <code>/etc/passwd</code> and <code>/etc/shadow</code> to store user account information, including password hashes in <code>/etc/shadow</code>. By default, <code>/etc/shadow</code> is only readable by the root user.(Citation: Linux Password and Shadow File Formats)

Linux stores user information such as user ID, group ID, home directory path, and login shell in <code>/etc/passwd</code>. A "user" on the system may belong to a person or a service. All password hashes are stored in <code>/etc/shadow</code> - including entries for users with no passwords and users with locked or disabled accounts.(Citation: Linux Password and Shadow File Formats)

Adversaries may attempt to read or dump the <code>/etc/passwd</code> and <code>/etc/shadow</code> files on Linux systems via command line utilities such as the <code>cat</code> command.(Citation: Arctic Wolf) Additionally, the Linux utility <code>unshadow</code> can be used to combine the two files in a format suited for password cracking utilities such as John the Ripper - for example, via the command <code>/usr/bin/unshadow /etc/passwd /etc/shadow > /tmp/crack.password.db</code>(Citation: nixCraft - John the Ripper). Since the user information stored in <code>/etc/passwd</code> are linked to the password hashes in <code>/etc/shadow</code>, an adversary would need to have access to both.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Tools

* LaZagne