Modify Authentication Process: Pluggable Authentication Modules, Sub-technique T1556.003 - Enterprise

Archived: 2026-04-05 17:23:46 UTC

Adversaries may modify pluggable authentication modules (PAM) to access user credentials or enable otherwise unwarranted access to accounts. PAM is a modular system of configuration files, libraries, and executable files which guide authentication for many services. The most common authentication module is `pam_unix.so`, which retrieves, sets, and verifies account authentication information in `/etc/passwd` and `/etc/shadow`.[1][2][3]

Adversaries may modify components of the PAM system to create backdoors. PAM components, such as `pam_unix.so`, can be patched to accept arbitrary adversary supplied values as legitimate credentials.[4]

Malicious modifications to the PAM system may also be abused to steal credentials. Adversaries may infect PAM resources with code to harvest user credentials, since the values exchanged with PAM components may be plain-text since PAM does not store passwords.[5][1]

Source: https://attack.mitre.org/techniques/T1556/003