Unsecured Credentials: Group Policy Preferences, Sub-technique T1552.006 - Enterprise

Archived: 2026-04-02 10:57:06 UTC

Adversaries may attempt to find unsecured credentials in Group Policy Preferences (GPP). GPP are tools that allow administrators to create domain policies with embedded credentials. These policies allow administrators to set local accounts.[1]

These group policies are stored in SYSVOL on a domain controller. This means that any domain user can view the SYSVOL share and decrypt the password (using the AES key that has been made public).[2]

The following tools and scripts can be used to gather and decrypt the password file from Group Policy Preference XML files:

- Metasploit's post exploitation module: `post/windows/gather/credentials/gpp`
- Get-GPPPassword[3]
- gpprefdecrypt.py

On the SYSVOL share, adversaries may use the following command to enumerate potential GPP XML files: `dir /s * .xml`

Source: https://attack.mitre.org/techniques/T1552/006