

T1552.006 - Group Policy Preferences

Description from ATT&CK

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. (Citation: Microsoft GPP 2016)

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).(Citation: Microsoft GPP Key)

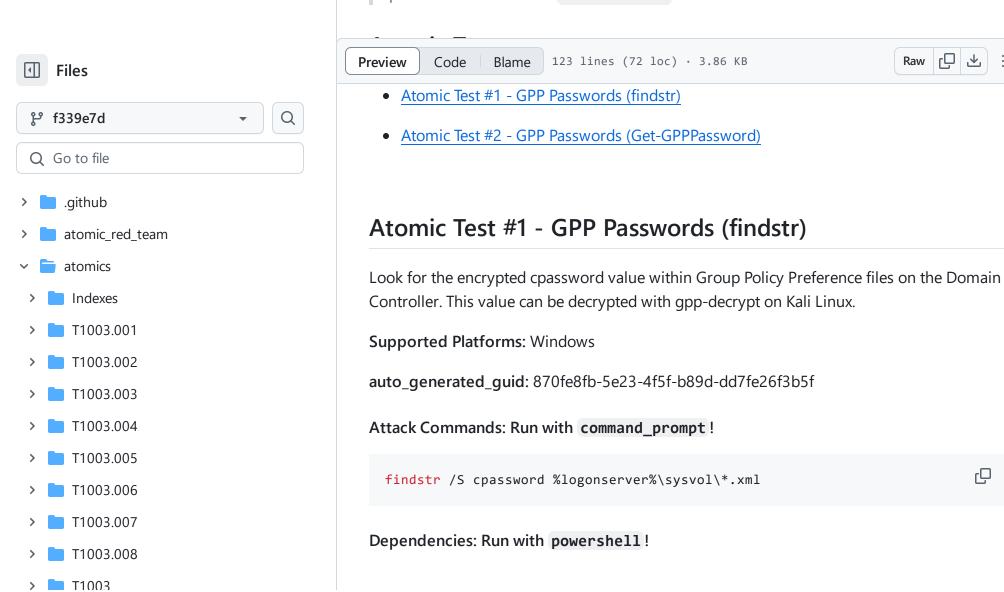
The following tools and scripts can be used to gather and decrypt the password file from Group Policy Preference XML files:

- Metasploit's post exploitation module: post/windows/gather/credentials/gpp
- Get-GPPPassword(Citation: Obscuresecurity Get-GPPPassword)
- gpprefdecrypt.py

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

Raw 📮 🕹

Q



passwords-findstr T1006 T1007 T1010 T1012 T1014 T1016 T1018 T1020 T1021.001 T1021.002 T1021.003 T1021.006 T1027.001 T1027.002 T1027.004 T1027 T1030 T1033 T1036.003 T1036.004 T1036.005 T1036.006 T1036 T1037.001 T1037.002 T1037.004

T1037.005

T1039

> T1040

Description: Computer must be domain joined

Check Prereq Commands:

```
if((Get-CIMInstance -Class Win32_ComputerSystem).PartOfDomain) {exit ∅} ، □
```

Get Prereq Commands:

```
Write-Host Joining this computer to a domain must be done manually
```

Atomic Test #2 - GPP Passwords (Get-GPPPassword)

Look for the encrypted cpassword value within Group Policy Preference files on the Domain Controller. This test is intended to be run from a domain joined workstation, not on the Domain Controller itself. The Get-GPPPasswords.ps1 executed during this test can be obtained using the get-prereq_commands.

Successful test execution will either display the credentials found in the GPP files or indicate "No preference files found".

Supported Platforms: Windows

auto_generated_guid: e9584f82-322c-474a-b831-940fd8b4455c

Inputs:

Name	Description	Туре	
gpp_script_url	URL of the Get- GPPPassword PowerShell Script	Url	https://raw.githubusercontent.com/PowerS GPPPassword.ps1
gpp_script_path	Path to the Get- GPPPassword PowerShell Script	Path	PathToAtomicsFolder\T1552.006\src\Get-G

Attack Commands: Run with powershell!

```
. #{gpp_script_path}
Get-GPPPassword -Verbose
```

Dependencies: Run with powershell!

Description: Get-GPPPassword PowerShell Script must exist at #{gpp_script_path}

Check Prereq Commands:

```
if(Test-Path "#{gpp_script_path}") {exit 0 } else {exit 1 }
```

Get Prereq Commands:

Description: Computer must be domain joined

