









- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005
- >  T1039
- >  T1040

## Atomic Test #2 - Basic Permission Groups Discovery Windows (Local)

Basic Permission Groups Discovery for Windows. This test will display some errors if run on a computer not connected to a domain. Upon execution, domain information will be displayed.

Supported Platforms: Windows

auto\_generated\_guid: 1f454dd6-e134-44df-bebb-67de70fb6cd8

Attack Commands: Run with `command_prompt` !

```
net localgroup
net localgroup "Administrators"
```



## Atomic Test #3 - Permission Groups Discovery PowerShell (Local)

Permission Groups Discovery utilizing PowerShell. This test will display some errors if run on a computer not connected to a domain. Upon execution, domain information will be displayed.

Supported Platforms: Windows

auto\_generated\_guid: a580462d-2c19-4bc7-8b9a-57a41b7d3ba4

Attack Commands: Run with `powershell` !

```
get-localgroup
Get-LocalGroupMember -Name "Administrators"
```



## Atomic Test #4 - SharpHound3 - LocalAdmin

This module runs the Windows executable of SharpHound in order to remotely list members of the local Administrators group (SAMR)

Supported Platforms: Windows

auto\_generated\_guid: e03ada14-0980-4107-aff1-7783b2b59bb1

Inputs:

Name	Description	Type	Default Value
domain	FQDN of the targeted domain	string	<code>\$env:UserDnsDomain</code>
sharphound_path	SharpHound Windows executable	path	<code>\$env:TEMP\SharpHound.exe</code>
output_path	Output for SharpHound	path	<code>\$env:TEMP\SharpHound\</code>

Attack Commands: Run with `powershell` !

```
New-Item -Path "#{output_path}" -ItemType Directory > $null
& "#{sharphound_path}" -d "#{domain}" --CollectionMethod LocalAdmin --No
```



Cleanup Commands:

```
Remove-Item -Recurse #{output_path} -ErrorAction Ignore
```

Dependencies: Run with powershell!

Description: SharpHound binary must exist on disk and at specified location (#{sharphound\_path}).  
And the computer must be domain joined (implicit authentication).

Check Prereq Commands:

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

Get Prereq Commands:

```
Invoke-WebRequest "https://github.com/BloodHoundAD/BloodHound/blob/e062f
```

## Atomic Test #5 - Wmic Group Discovery

Utilizing wmic.exe to enumerate groups on the local system. Upon execution, information will be displayed of local groups on system.

Supported Platforms: Windows

auto\_generated\_guid: 7413be50-be8e-430f-ad4d-07bf197884b2

Attack Commands: Run with powershell!

```
wmic.exe group get name
```

## Atomic Test #6 - WMIObject Group Discovery

Utilizing PowerShell cmdlet - get-wmiobject, to enumerate local groups on the endpoint. Upon execution, Upon execution, information will be displayed of local groups on system.

Supported Platforms: Windows

auto\_generated\_guid: 69119e58-96db-4110-ad27-954e48f3bb13

Attack Commands: Run with powershell!

```
Get-WMIObject Win32_Group
```