

GitHub Gist

All gists

Back to GitHub

Sign in

Sign up

Instantly share code, notes, and snippets.



hook-s3c / info.txt

Created 6 years ago

☆ Star 2

🔗 Fork 6

<> Code

🔄 Revisions 1

☆ Stars 2

🔗 Forks 6

Embed ▾

<script sr



Download ZIP

Disable Powershell logging

<> info.txt

Raw

```
1  Logs are held by default in the user profile:
2  \AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
3
4  this directory also hosts per-application logs
5
6  -----
7  Disable Logging...
8
9  remove-module psreadline
10
11 Set-PSReadlineOption -HistorySavePath path
12 - to change the default path of log file
13
14 Set-PSReadlineOption -HistorySaveStyle SaveNothing
15 - to disable logging feature
16
17 Other;
18 - Get-Credential
19 - variable = Read-Host -AsSecureString "mysecurestring"
20
21 -----
22
23 Scrubbing;
24
25 del (Get-PSReadlineOption).HistorySavePath
26
27 -----
```

```
28 Extracting logs with python;
29 https://github.com/KalibRx/PoshHarvestPy
30
31 -----
32 Sources...
33
34 https://twitter.com/DissectMalware/status/1062879286749773824
35 https://twitter.com/nikhil_mitt/status/1062382974744887296
36 https://twitter.com/DevinStokes/status/1062760239781408768
37 https://twitter.com/IISResetMe/status/1062594906626187264
38 https://blogs.msdn.microsoft.com/stevelasker/2016/03/25/clear-history-powershell-doesnt-clear-the-histo
39 https://0xdf.gitlab.io/2018/11/08/powershell-history-file.html
40 https://yunolikerobots.com/blog/f/log-everything-right
41
42
43
```



hook-s3c commented on Nov 24, 2018

Author ...

linux equivalent;
<https://askubuntu.com/questions/625277/terminal-incognito-mode>



hook-s3c commented on Nov 24, 2018

Author ...

powershell script:
<https://github.com/hlldz/Invoke-Phant0m>



hook-s3c commented on Dec 3, 2018

Author ...

Cut off AMSI;

```
[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetField('amsiInitFailed','NonPu
```

<https://blog.xpnsec.com/exploring-powershell-amsi-and-logging-evasion/>



hook-s3c commented on Dec 4, 2018

Author ...

Blueteam logging presentation, Defcon 26;
<https://www.youtube.com/watch?v=3yYD3CYiwx4>

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.