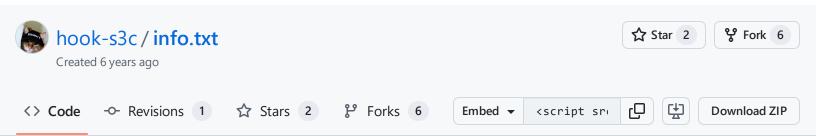
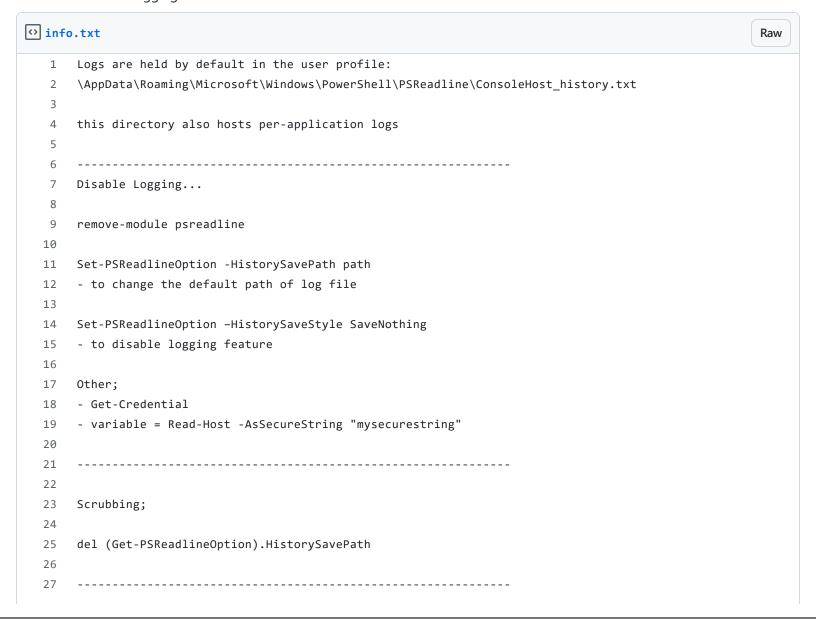


Instantly share code, notes, and snippets.



## Disable Powershell logging



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