

渗透技巧——获得Powershell命令的历史记录

0x00 前言

我在最近的学习过程中，发现Powershell命令的历史记录有时会包含系统敏感信息，例如远程服务器的连接口令，于是我对Powershell的历史记录功能做了进一步研究，总结一些渗透测试中常用导出历史记录的方法，结合利用思路，给出防御建议。

0x01 简介

本文将介绍以下内容：

- 两种Powershell命令的历史记录
- 导出Powershell命令历史记录的方法
- 防御建议

0x02 两种Powershell命令的历史记录

记录Powershell命令的历史记录有两种方式，可分别使用Get-History和Get-PSReadlineOption读取

1、Get-History

参考文档：

<https://docs.microsoft.com/en-us/powershell/module/Microsoft.PowerShell.Core/Get-History?view=powershell-3.0>

默认Powershell v2及以上支持

能够记录当前会话中输入的命令，多个Powershell进程之间不共享，Powershell进程退出后自动清除所有记录

1. 常用命令

获得历史记录完整信息：

```
Get-History | Format-List -Property *
```

包括：

- Id
- CommandLine
- ExecutionStatus
- StartExecutionTime
- EndExecutionTime

测试如下图

```
c:\test>powershell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\test> $host

Name           : ConsoleHost
Version        : 2.0
InstanceId      : d33f54f2-56f9-4e18-824c-84d7d95de38b
UI             : System.Management.Automation.Internal.Host.InternalHostUserInterface
CurrentCulture : en-US
CurrentUICulture : en-US
PrivateData    : Microsoft.PowerShell.ConsoleHost+ConsoleColorProxy
IsRunspacePushed : False
Runspace       : System.Management.Automation.Runspaces.LocalRunspace

PS C:\test> Get-History | Format-List -Property *

Id           : 1
CommandLine  : $host
ExecutionStatus : Completed
StartExecutionTime : 6:54:42 PM
EndExecutionTime : 6:54:42 PM

PS C:\test>
```

删除所有历史记录：

```
Clear-History
```

按ID号删除命令：

```
Clear-History -Id 3
```

2. 利用思路

获得了一台Windows系统的权限，发现后台有Powershell进程，想要读取Powershell进程中的历史记录

(1) Powershell进程无法接收键盘输入命令

例如Powershell加载了一个在后台运行的脚本: Powershell -ep bypass -f 1.ps1

此时无法向Powershell进程发送键盘消息，这时可以通过读取进程的命令行参数获得有用的信息，开源代码：

<https://github.com/3gstudent/Homework-of-C-Language/blob/master/GetProcessCommandLine.cpp>

代码实现了读取指定进程的命令行参数，通常能够获得有用的信息

(2) Powershell进程能够接收键盘输入命令

这里可以模拟发送键盘消息，导出历史记录

程序实现思路：

- 通过遍历枚举所有窗口
- 通过GetWindowThreadProcessId从窗口（HWND）获得PID
- 比较PID，找到符合条件的窗口
- 向符合条件的窗口发送键盘消息（PostMessage）

程序细节：

1.Virtual-Key Codes

每一个键盘输入消息对应一个Virtual-Key Code

参考资料：<https://docs.microsoft.com/en-us/windows/desktop/inputdev/virtual-key-codes>

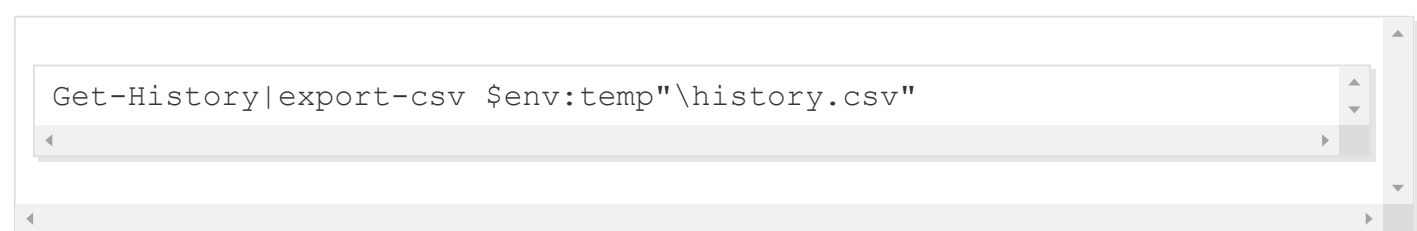
需要模拟键盘按下和键盘抬起两个操作，开源的测试代码：

<https://github.com/3gstudent/Homework-of-C-Language/blob/master/SendKeyboardMessageToPowershell.cpp>

代码实现了搜索指定pid的进程，向进程发送键盘消息，内容为:whoami

2.导出历史记录

命令如下：



```
Get-History | export-csv $env:temp\history.csv
```

其中需要考虑字符"|"、"\$"和"\"", 模拟键盘输入时需要加Shift键

这里的实现方法是先使用keybd_event按下Shift键，再用PostMessage发送按键的字母，最后抬起两个按键

开源的测试代码：

[https://github.com/3gstudent/Homework-of-C-Language/blob/master/SendKeyboardMessageToPowershell\(Get-History\).cpp](https://github.com/3gstudent/Homework-of-C-Language/blob/master/SendKeyboardMessageToPowershell(Get-History).cpp)

代码实现了搜索指定pid的进程，向进程发送键盘消息，内容为:Get-History | export-csv \$env:temp\history.csv

3. 补充：查看cmd.exe的历史记录

命令如下：

```
doskey /h
```

清空：

```
doskey /reinstall
```

也可以通过发送键盘消息的方式导出cmd.exe的命令历史记录

2、Get-PSReadlineOption

参考文档：

<https://docs.microsoft.com/en-us/powershell/module/psreadline/?view=powershell-5.1>

默认Powershell v5支持

Powershell v3和Powershell v4需要安装Get-PSReadlineOption后才可以使

用，所有Powershell命令的历史记录会保存在同一位置，可随时查看

1. Powershell v3和Powershell v4的安装和使用

这里以64位系统为例，安装方法如下：

(1)安装PowerShellGet

下载：

<https://www.microsoft.com/en-us/download/details.aspx?id=51451>

注：

安装前需要关闭powershell进程

可以通过命令行实现隐蔽安装，命令如下：

```
msiexec /q /i PackageManagement_x64.msi
```

安装成功后，在控制面板的已安装程序列表(Control Panel\Programs\Programs and Features)有显示:Package Management Preview - x64

可以通过删除对应的注册表项进行隐藏，更多细节可参考《[渗透基础——获得当前系统已安装的程序列表](#)》

Package Management Preview - x64的注册表路径为
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\
{57E5A8BB-41EB-4F09-B332-B535C5954A28}

只需要删除这个注册表项及子项即可实现在已安装程序列表中隐藏

删除注册表项的cmd命令：

```
reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\
```

(2)安装PSReadLine

通过Install-Module命令安装

```
Install-Module -Name PSReadLine
```

弹出提示：

```
NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to
with NuGet-based repositories. The NuGet provider must be available in
'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\Administrator\AppData\Local\PackageManagement\ProviderAssemblies'
You can also install the NuGet provider by running 'Install-PackageProvider
-Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to
install and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"):
```

需要再次输入Y进行安装

如果需要实现一键安装，可以先安装NuGet，再安装PSReadLine，完整命令如下：

```
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
Install-Module -Name PSReadLine
```

(3)使用

所有powershell命令将会保存在固定位

置:%appdata%\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

查看命令的历史记录:

```
Get-Content (Get-PSReadlineOption).HistorySavePath
```

清除命令的历史记录:

```
Remove-Item (Get-PSReadlineOption).HistorySavePath
```

2. 利用思路

获得了Windows系统的访问权限, 首先查看Powershell版本, 如果是v5, 可通过读取文件%appdata%\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt获得历史记录

如果系统是Powershell v3或Powershell v4, 可通过命令行安装PSReadLine, 这样就能记录后续系统所有的Powershell命令

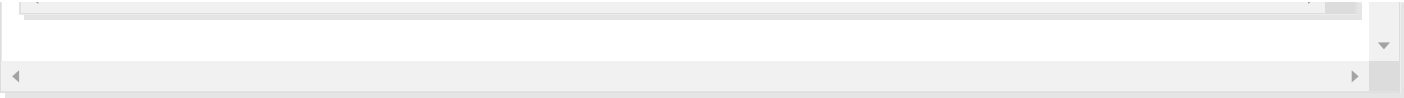
0x03 防御建议

如果使用高版本的Windows系统, 如Win10, 默认Powershell版本为5.0, 会记录Powershell的命令, 建议定时进行清除, 位置:

%appdata%\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

清除命令的历史记录:

```
Remove-Item (Get-PSReadlineOption).HistorySavePath
```



对于低版本的Powershell，如果命令中包含敏感信息(如远程连接的口令)，需要及时清除，命令为：
Clear-History

对于cmd.exe，如果命令中包含敏感信息(如远程连接的口令)，需要及时清除，命令为：doskey
/reinstall

0x04 小结

本文介绍了两种Powershell命令的历史记录，总结常用导出历史记录的方法，结合利用思路，给出防御建议。

LEAVE A REPLY

Written on May 16, 2019