【powershell】PsLoggedOn

PsLoggedOn將列舉HKEY_USERS下的注冊表密鑰，以檢索已登錄用戶的安全標識符（SID）並將SID轉換為用戶名。 PsLoggedOn還將使用NetSessionEnum API查看誰通過資源共享登錄到計算機上。

然而，有一個局限性，就是PsLoggedOn依賴於遠程注冊表服務來掃描相關的密鑰。遠程注冊表服務自Windows 8以來就不再默認啟用在Windows工作站上，但系統管理員可能出於各種管理任務啟用它，以實現向後兼容性，或者用於安裝監控/部署工具、腳本、代理等。

它還在後來的Windows Server操作系統上默認啟用，如Server 2012 R2、2016（1607）、2019（1809）和Server 2022（21H2）。如果啟用了該服務，則該服務將在十分鐘的閒置後停止以節省資源，但一旦我們使用PsLoggedOn連接，它將重新啟用（帶有自動觸發器）。

現在，理論暫時告一段落，讓我們嘗試對之前嘗試列舉的計算機運行PsLoggedOn，首先是FILES04和WEB04。 PsLoggedOn位於CLIENT75的C:\Tools\PSTools目錄中。要使用它，我們只需將它與目標主機名一起運行：

```
PS C:\Tools\PSTools>  .\PsLoggedon.exe \\files04

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
     <unknown time>             CORP\jeff
Unable to query resource logons
```

運行這個命令，以查看WEB04上已登錄的用戶信息。 PsLoggedOn將返回登錄到這個計算機上的用戶列表。

```
PS C:\Tools\PSTools>  .\PsLoggedon.exe \\web04

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

No one is logged on locally.
Unable to query resource logons
```

運行這個命令，以查看CLIENT74上已登錄的用戶信息。 PsLoggedOn將返回登錄到這個計算機上的用戶列表。由於我們在CLIENT74啟用了Remote Registry服務，我們應該能夠成功列舉用戶會話。

```
PS C:\Tools\PSTools>  .\PsLoggedon.exe \\client74

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
     <unknown time>             CORP\jeffadmin

Users logged on via resource shares:
     10/5/2022 1:33:32 AM       CORP\stephanie
```

看起來jeffadmin在CLIENT74上有一個開啟的會話，輸出顯示了一些非常有趣的信息。如果我們的枚舉是準確的，並且我們實際上在CLIENT74上擁有管理特權，我們應該能夠登錄並可能竊取jeffadmin的憑據！儘管立即嘗試這樣做可能很誘人，但最佳實踐是堅持原計畫，繼續我們的枚舉。畢竟，我們的目標不是迅速獲得勝利，而是提供徹底的分析。

修訂版本 #1
★由 treeman 建立於 28 ��@�@ 2024 04:03:41
✎由 treeman 更新於 8 ��G�@ 2024 09:52:05