

【AD】 【列舉】 Get-Acl

我們將使用PowerShell的Get-Acl cmdlet。這個命令本質上將檢索我們使用 -Path 標誌定義的對象的權限並將它們打印在我們的PowerShell提示中。

```
PS C:\Tools> Get-Acl -Path HKLM:SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity\ | fl
```

```
PS C:\Tools> Get-Acl -Path
HKLM:SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity\ | fl

Path      :
Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
\Services\LanmanServer\DefaultSecurity\
Owner     : NT AUTHORITY\SYSTEM
Group     : NT AUTHORITY\SYSTEM
Access    : BUILTIN\Users Allow ReadKey
           BUILTIN\Administrators Allow FullControl
           NT AUTHORITY\SYSTEM Allow FullControl
           CREATOR OWNER Allow FullControl
           APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadKey
           S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-
3232135806-4053264122-3456934681 Allow ReadKey
```

在清單中突出顯示的輸出顯示了擁有FullControl或ReadKey權限的組和用戶，這意味著它們都可以讀取SrvsvcSessionInfo密鑰本身。

🕒 修訂版本 #1

★ 由 treeman 建立於 12 🕒🕒🕒🕒 2023 00:05:47

✍ 由 treeman 更新於 7 🕒@🕒🕒 2024 19:30:26