

【Linux】【列舉】linpeas

<https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS>

`linpeas.sh` 是一個用於 Linux 系統的自動化信息搜集工具，特別是用於提取有關系統環境、配置和潛在安全問題的信息。該工具的全名是 "Linux Privilege Escalation Awesome Script"，簡稱 linpeas。

以下是 linpeas.sh 的主要功能和用途：

- 信息搜集**：linpeas.sh 會掃描系統，收集關於用戶、組、進程、網絡配置、文件權限等方面的信息。
- 特權升級檢測**：該工具通常被用於檢測潛在的特權升級漏洞。它會尋找與系統特權升級有關的信息，例如 SUID、SGID 文件，可寫的配置文件，或者用戶可以執行的任何特權命令。
- 漏洞檢測**：linpeas.sh 會檢查系統上是否存在已知的漏洞，這有助於確保系統的安全性。
- 配置問題**：工具可以檢測系統中的配置問題，例如未限制的訪問權限、過多的開啟端口等。

使用 linpeas.sh 的基本步驟：

- 下載腳本**：通常，您需要從 GitHub 或其他可信的源下載 linpeas.sh 腳本。
- 授予執行權限**：在執行 linpeas.sh 之前，確保腳本有執行權限。您可以使用 `chmod +x linpeas.sh` 命令來授予執行權限。
- 執行腳本**：運行 `./linpeas.sh` 以啟動信息搜集和分析過程。腳本會生成一個包含系統信息和可能的問題的報告。
- 分析報告**：查看生成的報告，並根據其中的信息來進行進一步的調查和修復。

請注意，linpeas.sh 僅是安全測試和信息搜集的工具，應該僅在合法和授權的環境中使用。未經授權使用此類工具可能導致法律問題。

```
# /usr/share/peass/winpeas/winPEASx64.exe
sudo apt-get install peass
```

🕒 修訂版本 #2

★ 由 treeman 建立於 4 🕒@🕒🕒 2024 19:51:20

🔧 由 treeman 更新於 7 🕒@🕒🕒 2024 19:30:26