

【列舉】 【提權】 【Linux】 unix-privesc-check

/usr/bin/unix-privesc-check

```
kali@kali:~$ unix-privesc-check
unix-privesc-check v1.4 ( http://pentestmonkey.net/tools/unix-privesc-check )
```

```
Usage: unix-privesc-check { standard | detailed }
```

```
"standard" mode: Speed-optimised check of lots of security settings.
```

```
"detailed" mode: Same as standard mode, but also checks perms of open file
handles and called files (e.g. parsed from shell scripts,
linked .so files). This mode is slow and prone to false
positives but might help you find more subtle flaws in 3rd
party programs.
```

```
This script checks file permissions and other settings that could allow
local users to escalate privileges.
```

```
...
```

```
joe@debian-privesc:~$ ./unix-privesc-check standard > output.txt
```

該腳本對常見文件的權限執行了大量檢查。例如，以下節錄顯示了可由非 root 用戶寫入的配置文件：

```
Checking for writable config files
#####
Checking if anyone except root can change /etc/passwd
WARNING: /etc/passwd is a critical config file. World write is set for /etc/passwd
Checking if anyone except root can change /etc/group
Checking if anyone except root can change /etc/fstab
Checking if anyone except root can change /etc/profile
Checking if anyone except root can change /etc/sudoers
Checking if anyone except root can change /etc/shadow
```

此輸出顯示任何系統上的人都可以編輯 /etc/passwd。這相當重要，因為它允許攻擊者輕鬆提升特權或在目標上創建用戶帳戶。我們將在本模塊後面進行演示。

🔗 修訂版本 #2

★ 由 treeman 建立於 21 🍀@🍀🍀 2024 07:35:07

🔧 由 treeman 更新於 8 🍀G🍀🍀 2024 09:52:05