

win & lin PEAS

winPEAS

Windows Privilege Escalation Awesome Scripts



Check the **Local Windows Privilege Escalation** checklist from book.hacktricks.xyz

Check more information about how to exploit found misconfigurations in book.hacktricks.xyz

Quick Start

Find the latest versions of all the scripts and binaries in [the releases page](#).

WinPEAS .exe and .bat

- [Link to WinPEAS .bat project](#)
- [Link to WinPEAS C# project \(.exe\)](#) (.Net >= 4.5.2 required)
 - Please, read the Readme of that folder to learn how to execute winpeas from memory or how make colors work among other tricks

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

linPEAS

LinPEAS - Linux Privilege Escalation Awesome Script



LinPEAS is a script that search for possible paths to escalate privileges on Linux/Unix*/MacOS hosts. The checks are explained on book.hacktricks.xyz

Check the Local Linux Privilege Escalation checklist from book.hacktricks.xyz.

```
[*] USERS INFO

[+] Help
[!] https://book.hacktricks.xyz/linux-unix/privilege-escalation#groups
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugin)

[+] Testing 'sudo -l' without password & /etc/sudoers
[!] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-with-sudo-and-suid-commands
Matching Defaults entries for user on this host:
    env_reset, env_keep+=LD_PRELOAD

User user may run the following commands on this host:
(root) NOPASSWD: /usr/sbin/iftop
(root) NOPASSWD: /usr/bin/find
(root) NOPASSWD: /usr/bin/lsns
(root) NOPASSWD: /usr/bin/su
(root) NOPASSWD: /usr/bin/sudo
(root) NOPASSWD: /usr/bin/ssh
(root) NOPASSWD: /usr/bin/less
(root) NOPASSWD: /usr/bin/tftp
(root) NOPASSWD: /usr/bin/wget
(root) NOPASSWD: /usr/sbin/apache2
(root) NOPASSWD: /bin/egrep

[+] Testing 'su' as other users with shell without password or with their names as password (only works in modern su binary versions)
Trying with root...
Trying with daemon...
Trying with bin...
Trying with sys...
Trying with games...
Trying with man...
Trying with lp...
Trying with mail...
Trying with news...
Trying with uucp...
```

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

Revision #1

Created 10 July 2022 09:20:05 by Togoboi

Updated 10 July 2022 09:21:38 by Togoboi