Enumeration Scripts

Consider using these scripts as is, or refactoring / porting them into your own. They don’t modify anything on the filesystem, nor do they make any attempt to start or stop any services. They were designed with the assumption the user has no privileges to do such things, otherwise there would be no need to run them. They check for bad file permissions, sudoers, config files, running services, sticky bits, bad cronjobs, etc looking for any tips to give to a hacker on how they can further exploit the system. All things you should have fixed, so they can give you in the least a hint towards something you may have missed.

## Lynis

<https://github.com/CISOfy/lynis>

## LinEnum (sh)

<https://github.com/rebootuser/LinEnum>

2ez4me method

|  |
| --- |
| wget -O- <https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh> | bash |

## Linux Exploit Suggester (sh)

<https://github.com/mzet-/linux-exploit-suggester>

2ez4me method

|  |
| --- |
| wget -O- <https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh> | bash |

## LinuxPrivChecker (python)

<https://github.com/sleventyeleven/linuxprivchecker>

2ez4me method

|  |
| --- |
| wget -O- <https://raw.githubusercontent.com/sleventyeleven/linuxprivchecker/master/linuxprivchecker.py> | python - |

# Linux Enumeration Methodologies

These are guides for offsec people on how to escalate the privileges after getting an initial foothold on the server as a low privileged user. I think it would behoove you to learn how to think offensively.

<https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>

<https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_-_linux.html>