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

```
❯ 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)
```

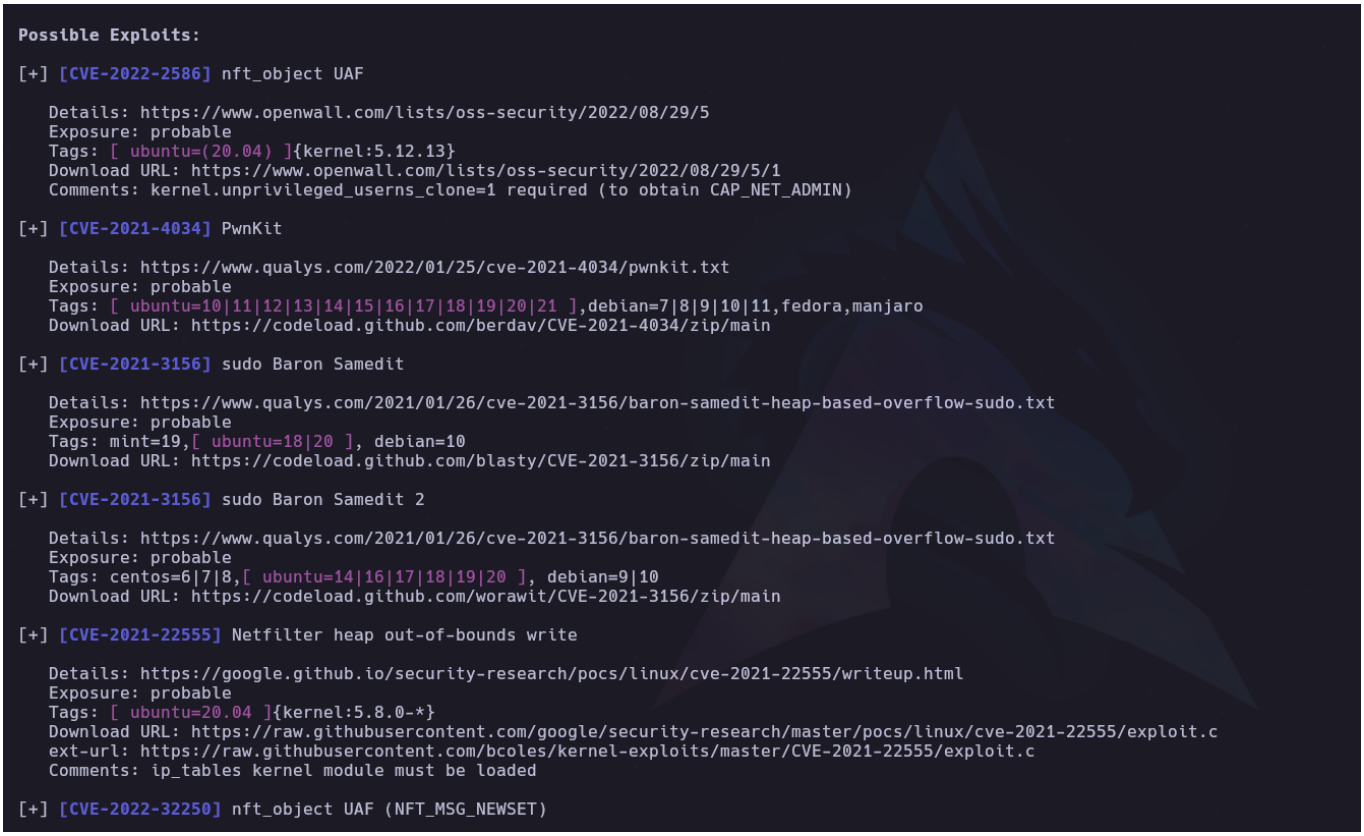
Ponemos la contraseña como dice el pinguno de Mario https://www.youtube.com/watch?v=VeX4S9jSH-0

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
```

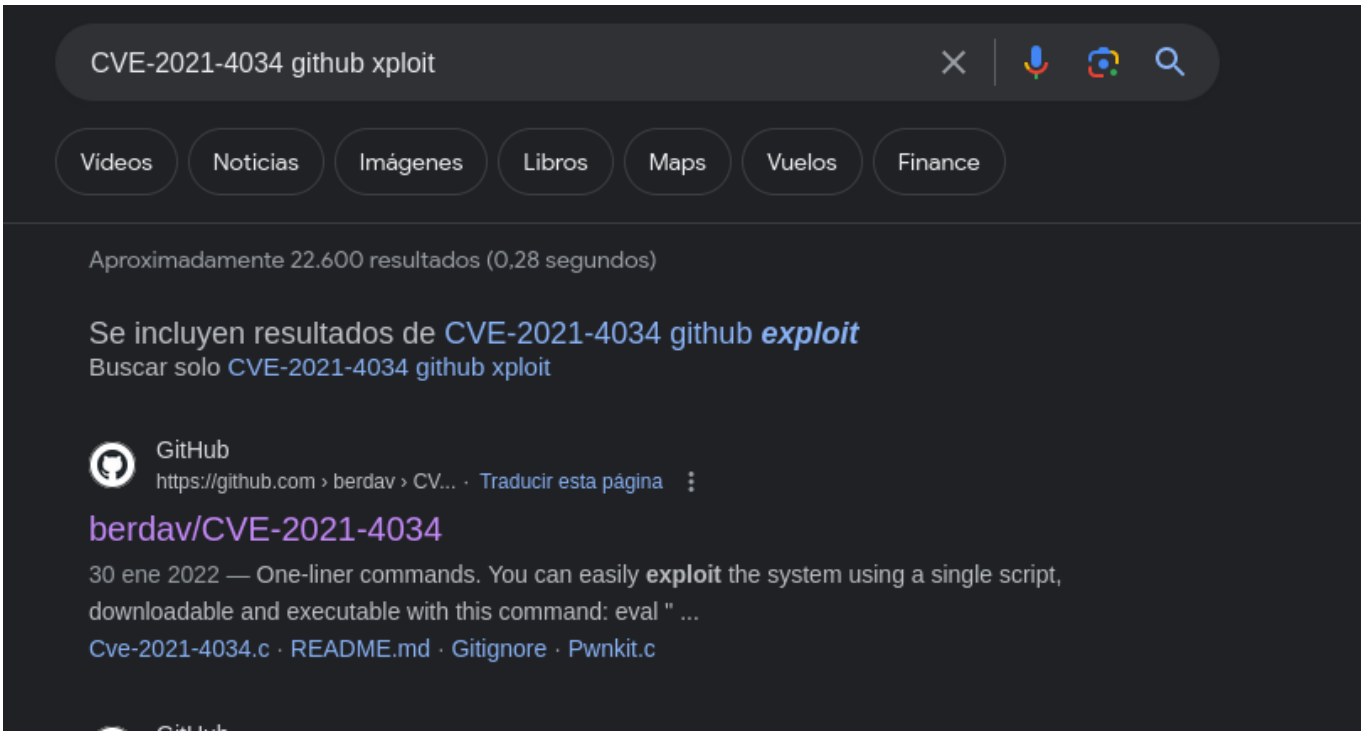
Lo clonamos nos metemos dentro con CD y despues para mas pruebas le hacemos un chmod 777 y despies lo ejecutamos con ./+nombredel.sh

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

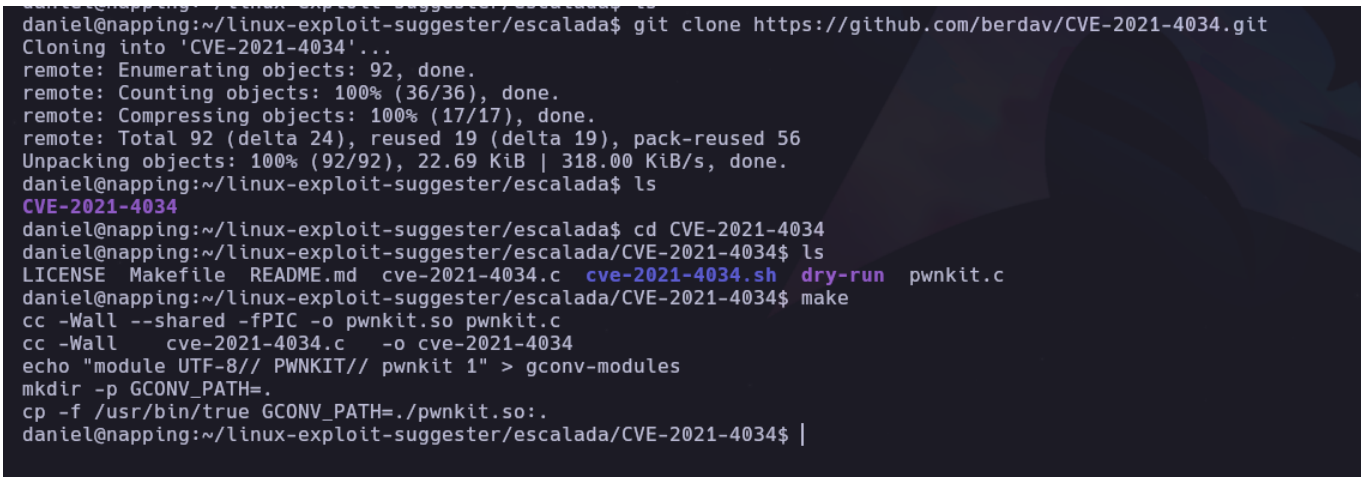


Una vez visto elegimos el que mas nios guste para probar

Elegimos y buscamos en el buscador



Una vez encontrado le clickamos [redacted] y realizamos el mismo procedimiento



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