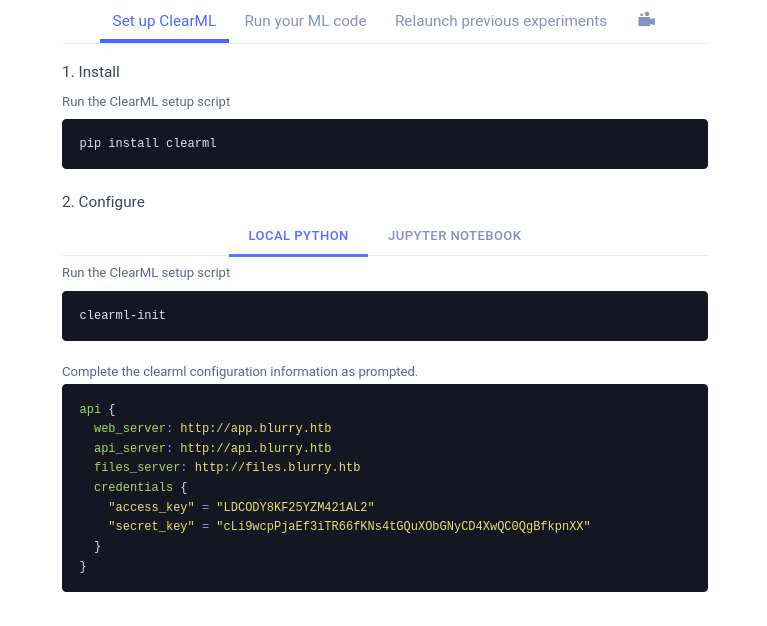
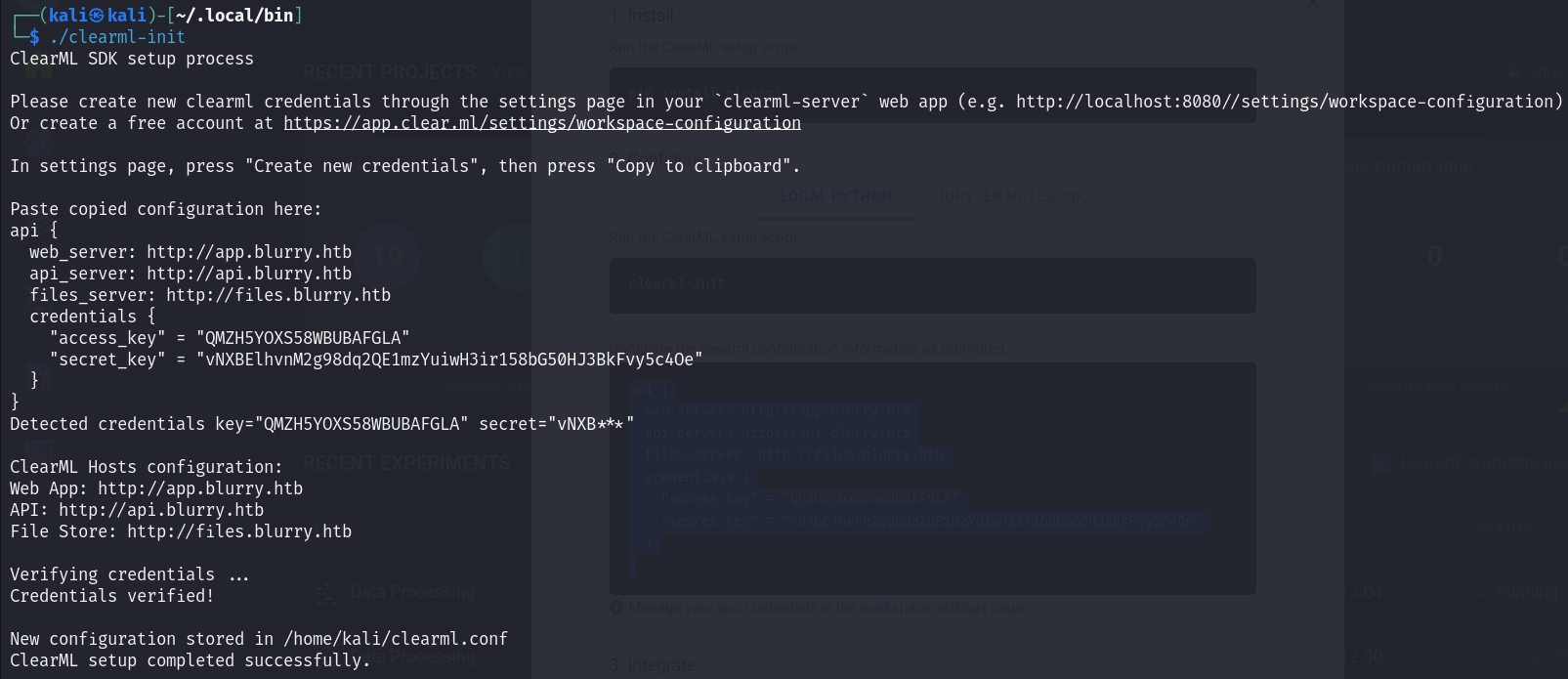


有開22,80 port，新增app.blurry.htb至/etc/hosts



網頁查看輸入id後會進入clearml的介面，並會出現client端配置command

有發現app、api、files 3個子網域，新增至/etc/hosts



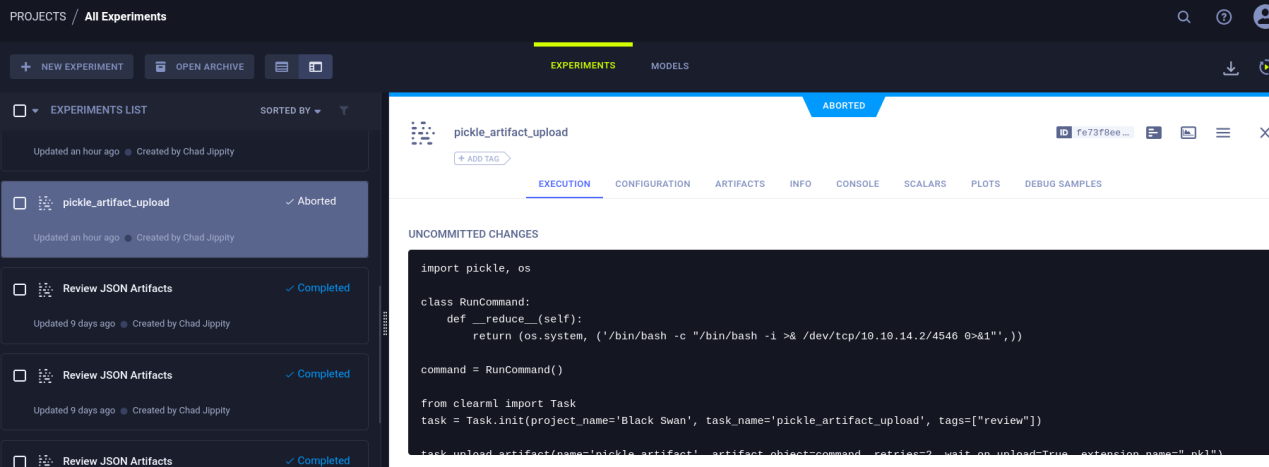
pip install clearml

cd /home/kali/.local/bin

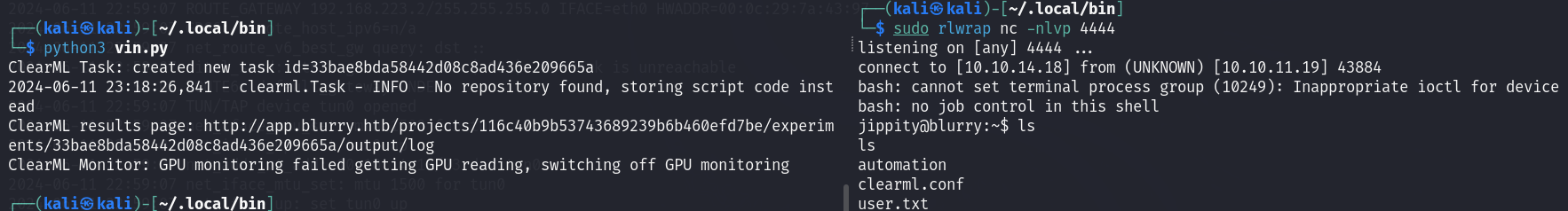
./clearml-init

將上一張圖的credential貼上，即可完成client端配置

在經過研究clearml後得知是一個模型整理平台，在client端執行的python模型會被記錄在server



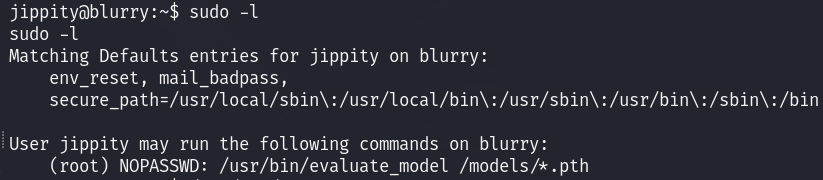
server上有很多模型，經過慢慢觀察後，發現有個模型跟reverse shell有關，內部配置反彈指令，大略猜測可能要藉由上傳後門模型來取得shell



將前面取得的command存成vin.py，ip設為本地

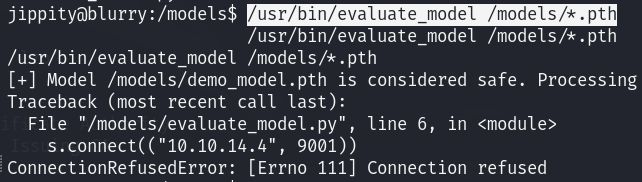
成功取得reverse shell

獲取user.txt



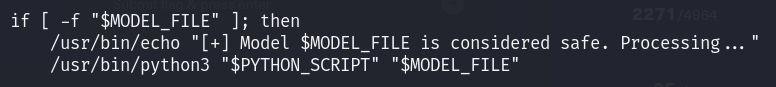
sudo -l

發現一個可執行binary



直接執行後發現evaluate\_model會取執行/models下的.pth file，且跳出connection refused，看起來有其他人將reverse shell command放進evaluate\_model.py裡

也因如此得知執行過程會讀取evaluate\_model.py的內容



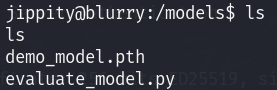
cat /usr/bin/evaluate\_model

查看evaluate\_model code也可發現最後會python3 $PYTHON\_SCRIPT $MODEL\_FILE

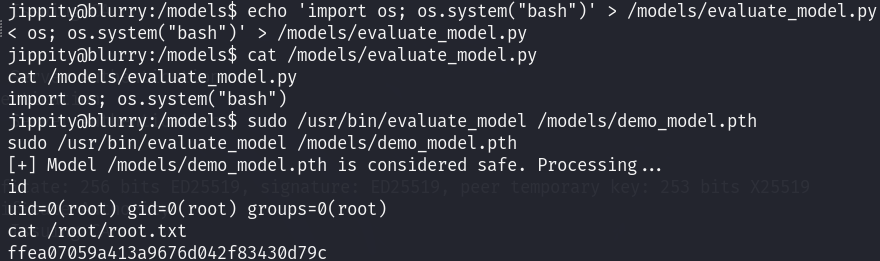
$PYTHON\_SCRIPT = /models/evaluate\_model.py

$MODEL\_FILE = demo\_model.pth

所以可以在evaluate\_model.py做手腳



查看/models下有2個file，剛剛的\*.pth應是執行demo\_model.pth



echo ‘import os; os.system(“bash”)’ > /models/evaluate\_model.py

sudo /usr/bin/evaluate\_model /models demo\_model.pth

用sudo執行bash command成功取得root privilege

獲取root flag