安全程式設計與駭客攻防技術期末報告

張家禎

王亭皓

廖亭柔

羅傳郡

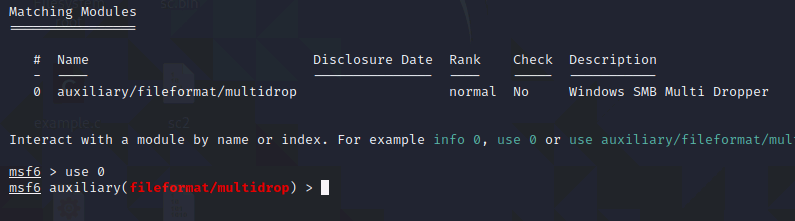
摘要

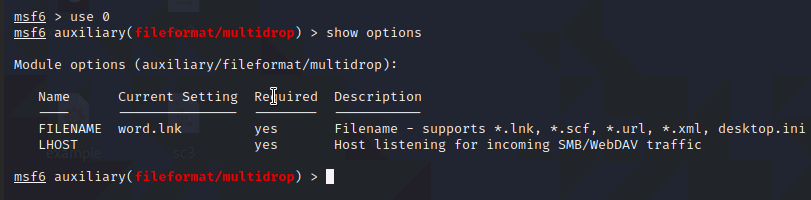
本次期末專案欲先從Exploit database中搜尋幾個常見的系統漏洞並嘗試攻擊，其中被攻擊的靶機可為Metasploitable2 、Metasploitable3或Windows。

可從Exploit database中找可執行的檔案，例：Ruby、Python等，也可直接使用metasploit framework中內建的程式進行攻擊。

# Example1

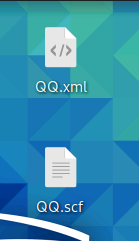
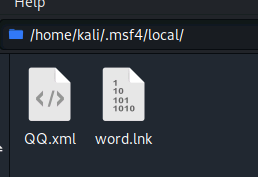
在metasploit framework中找的Windows SMB Dropper，SMB就是Windows的網路檔案分享系統，use它之後show options後可以看到它的必須欄位只有兩個，一個是LHOST可以設定攻擊者的回傳的ip，另一個filename可以設定攻擊的文件名稱，預設為work.lnk，可自己設定成 .scf、.url、.xml等。如下圖





都設定完後可以exploit產生出要攻擊的檔案





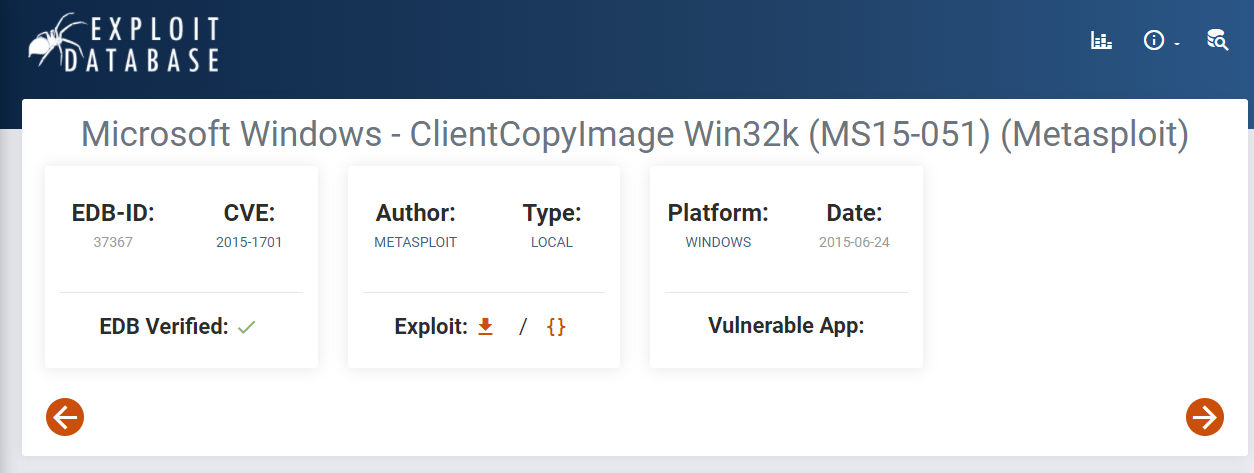
其中lnk 檔是Windows的捷徑檔，可在檔案中存病毒，這種毒很難判斷是不是有害， lnk 檔還能用來呼叫CMD指令，駭客可以把一段有害的CMD指令寫到 lnk 檔的『目標』欄內，當執行這個 lnk 檔時就會去執行目標欄內的CMD指令，

而scf檔，介殼命令檔(Shell Command File)主要是用來開啟檔案總管或是顯示桌面的捷徑檔。Windows作業系統與Chrome瀏覽器在處理SCF檔時，Chrome瀏覽器預設是將SCF檔視為安全的檔案，不需提醒使用者即自動下載此類型的檔案，若攻擊者在網頁中嵌入惡意的SCF檔案，使用者透過Chrome瀏覽器造訪惡意的網頁時，就會自動下載該惡意SCF檔案至使用者電腦中，下載完成後，當使用者開啟存放此檔案之資料夾時，Windows作業系統將自動執行SCF檔案，並嘗試自動登入到攻擊者所架設之SMB伺服器，導致攻擊者可藉此取得使用者所傳送之帳號與密碼資訊。

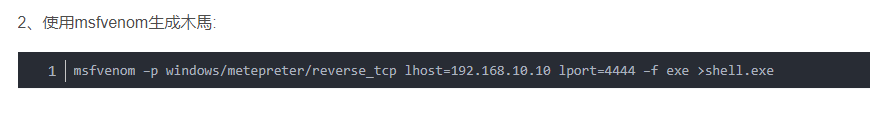
## Example2

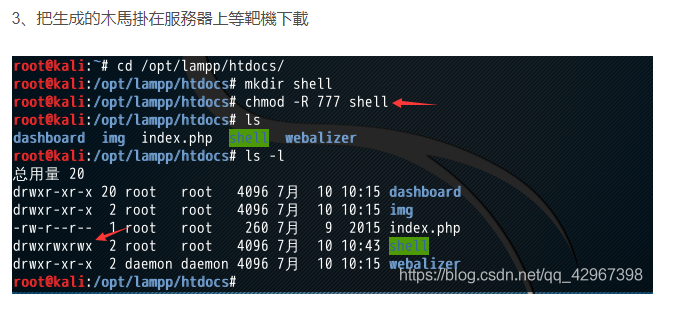
在Exploit database中找到的MS15\_051，CVE編號：2015-1701，也是很有名的例子。主要是進行權限提升獲取window server 2003/2008的system權限，最後進行遠程控制。

這個案例也是本次專題起初欲做的實例，欲使用國網建立的Metasploitable3，內建Window server 2008R2的system，不過最後沒攻擊成功。

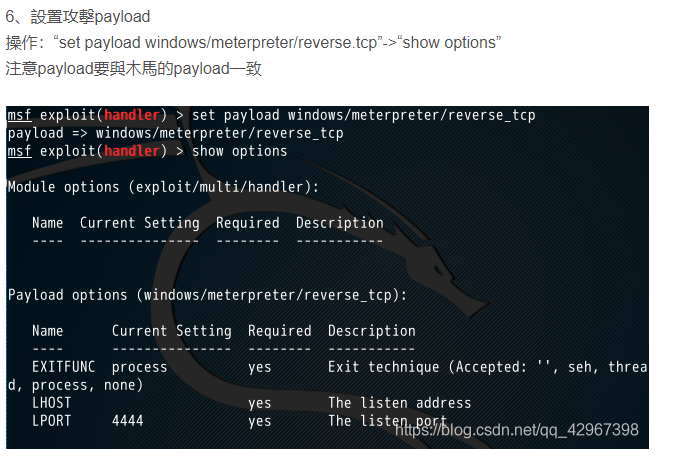


首先先建立靶機，並找到靶機ip，在攻擊機上產生木馬程式，把生成的木馬掛在攻擊機開的服務器上等靶機下載

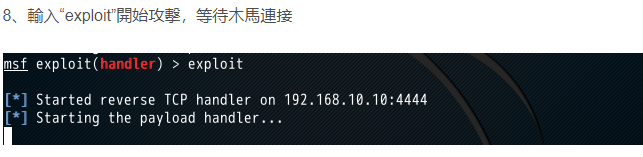




使用msf裡面的handler模塊，操作：msfconsole -> use exploit/multi/handler -> show options，並可開始設置攻擊機的payloads，設定LHOST跟LPORT(預設4444)

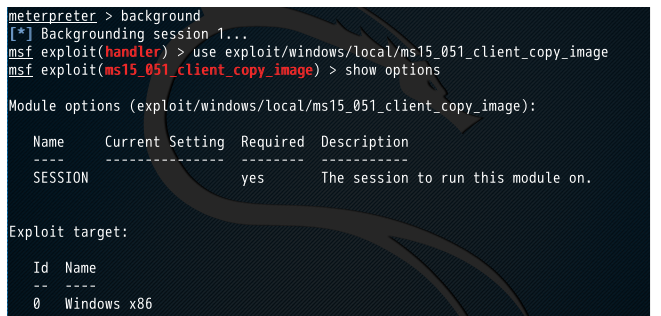


設定完payload後，用lampp重新啟動網站，等待靶機連到網站，靶機可以在IE上輸入http://10.101.9.118/shell 上下載木馬程式

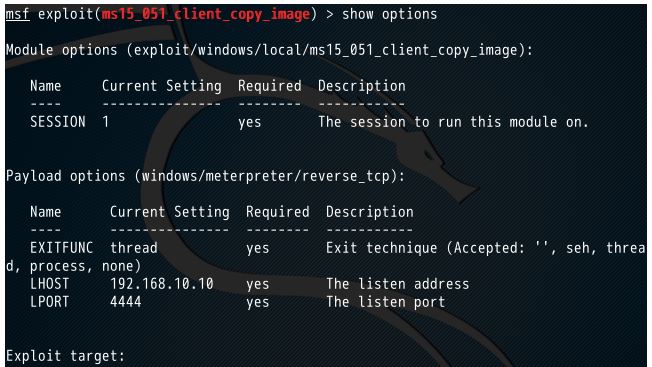


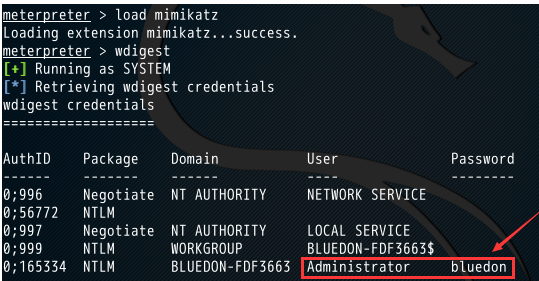


攻擊機成功獲取到靶機的shell，使用“getuid”查看為administrator權限，使用ms15-051漏洞，進一步獲取system最高權限，use exploit/windows/local/ms15\_051\_client\_copy\_image



設置payload，Session用1，輸入“run”攻擊成功，使用“getuid”查看已是system用戶。再輸入load mimikatz獲取administrator的密碼

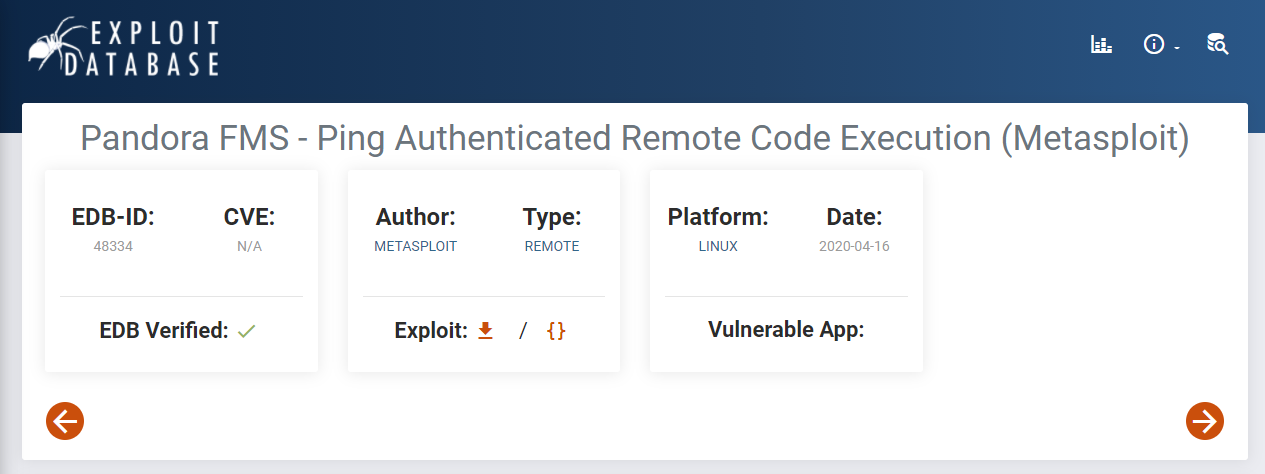


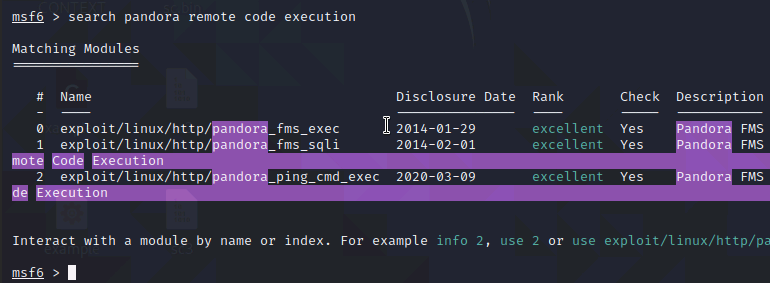




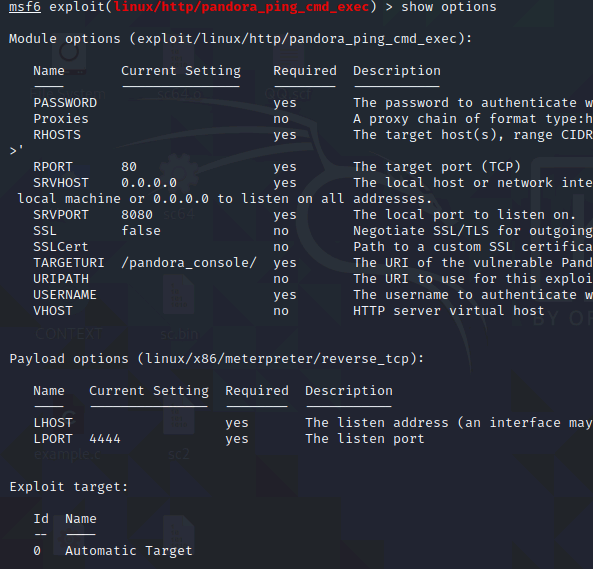
### Example3

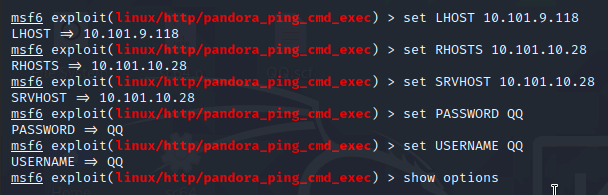
在Exploit database中找到比較新的，目前還沒有CVE編號。主要是進行執行remote code execution，最後進行遠程控制。



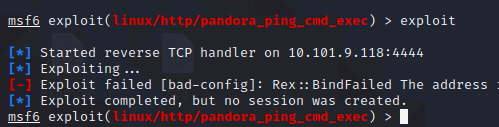


Show options後看到有許多可以設定的，例：RHOST，LHOST，USERNAME，PASSWORD等。RHOST設定攻擊機ip，LHOST設定靶機ip，USERNAME，PASSWORD都隨便設值。如下圖所示



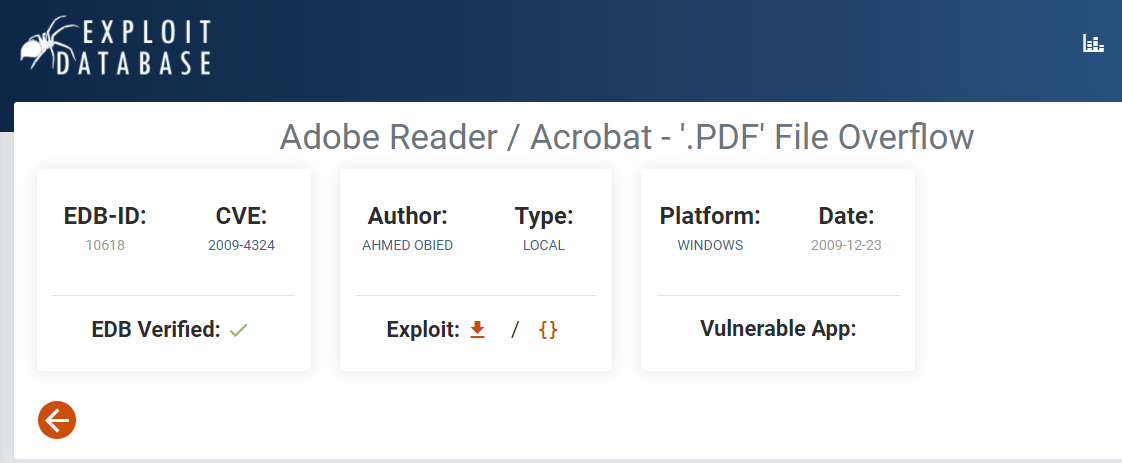


設定完後執行exploit失敗，礙於這在Exploit database上比較新，上網找也找不太到有人已經攻擊成功的案例，也不太清楚攻擊fail主因為何，因此此案例做到這邊。



### Example4

在Exploit database中找到的MS15\_051，CVE編號：2009-4324，也是很有名的例子，並通過平台驗證。主要是Adobe Reader 和 Acrobat 9.x 9.3 之前的 Multimedia.api 中的 Doc.media.newPlayer 方法中的 Use-after-free 漏洞，Windows 和 Mac OS X 8.2 之前的 8.x 允許遠程攻擊者執行任意程式碼使用 ZLib 壓縮製作的 PDF 文件，於 2009 年 12 月被exploit。

****

不過，此攻擊方法沒建在metasploit framework中。我還下載並建立了windows XP虛擬機，一樣嘗試許久仍未做出結果，攻擊失敗

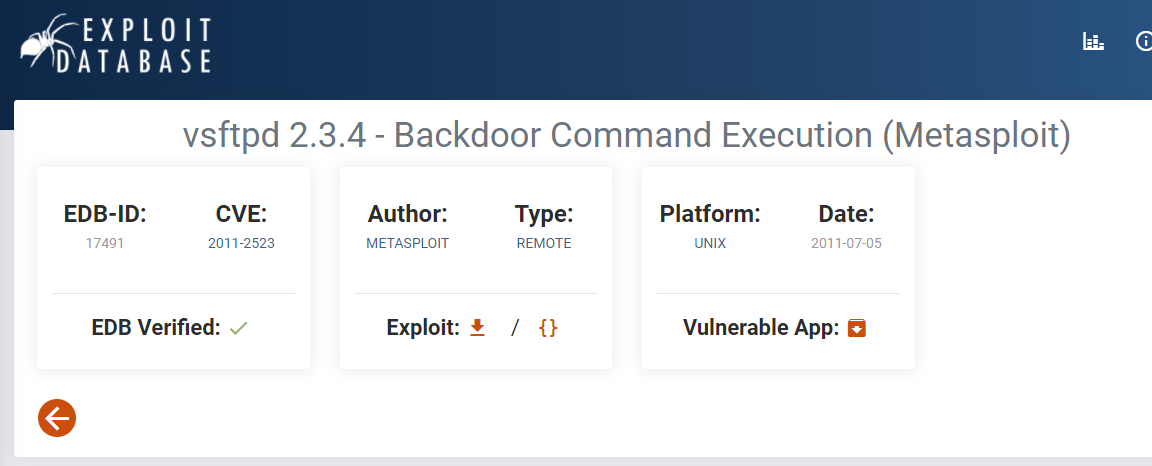
****

### Example5 (攻擊成功)

在Exploit database中找到的，CVE編號：2011-2523，也是很有名的例子。和老師上課提到Unreal IRCD一樣是後門程式，也有內建在metasploit framework中，可進到靶機的shell執行CMD。

vsftpd 2.3.4 包含一個後門程式，利用ftp它在Port 6200/tcp 上打開一個 shell，可以利用nmap掃描看看靶機有沒有開啟這服務。



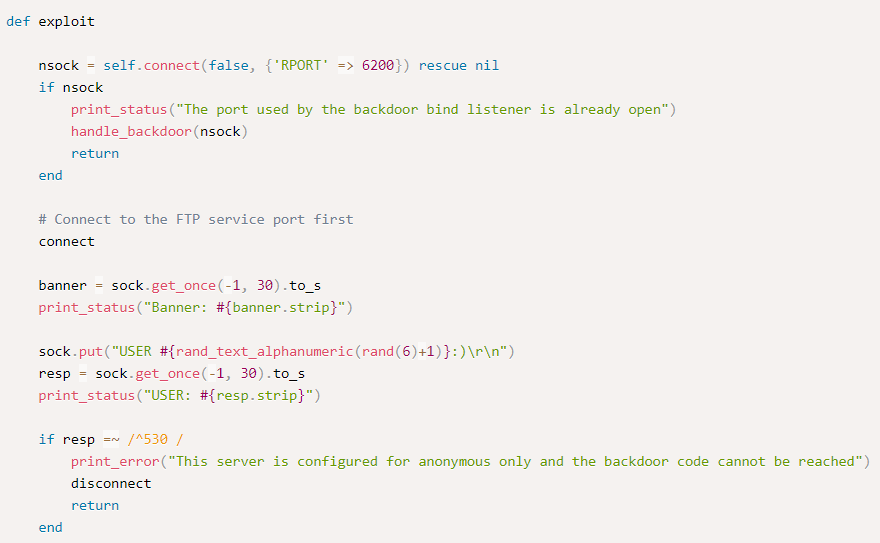


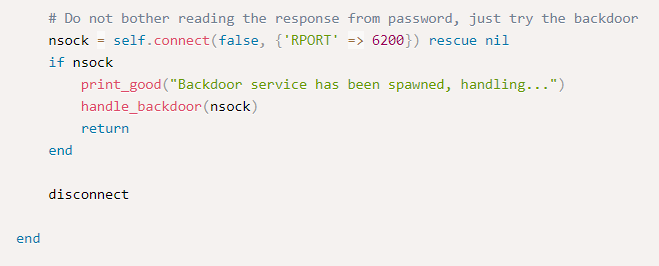
Code：

主要執行handle\_backdoor()此函數

nsock在判斷有沒有連線，類似錯誤偵測做的事。

Resp也類似錯誤偵測。





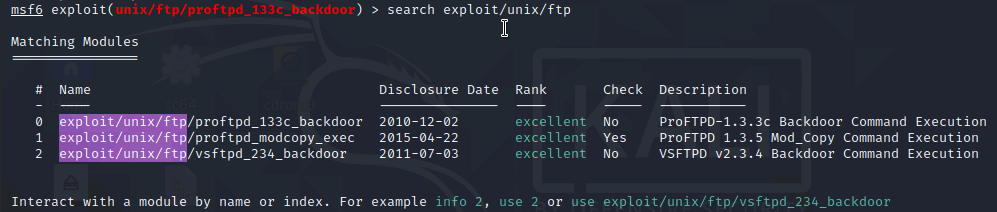
進到handle\_backdoor()，r做錯誤偵測，如果有錯誤，就連線取消

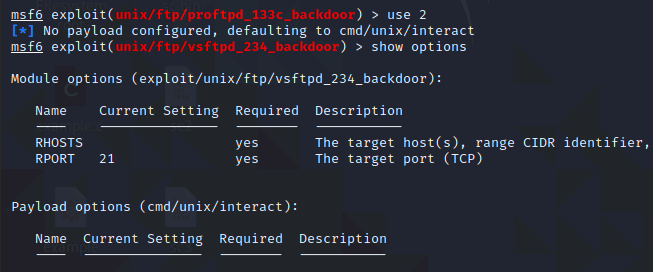
成功的話就會把加上設定好的payload資訊，執行handler()函式中的程式。

而handler()正是在msfconsole -> use exploit/multi/handler之中。



一開始先到metasploit framework中搜尋剛剛在Exploit database中找有關的程式名稱，找到之後use並利用show options看需需要設定的欄位

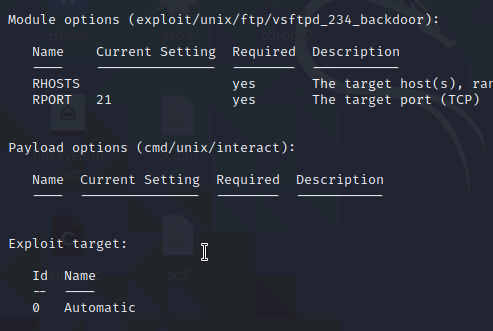


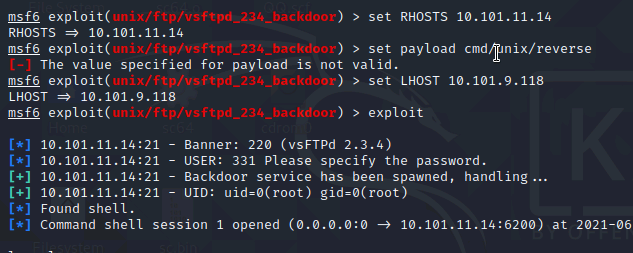


設定此backdoor程式需要設定LHOST(i.e.攻擊者的ip)及RHOST(i.e.靶機的ip)，target預設為自動。

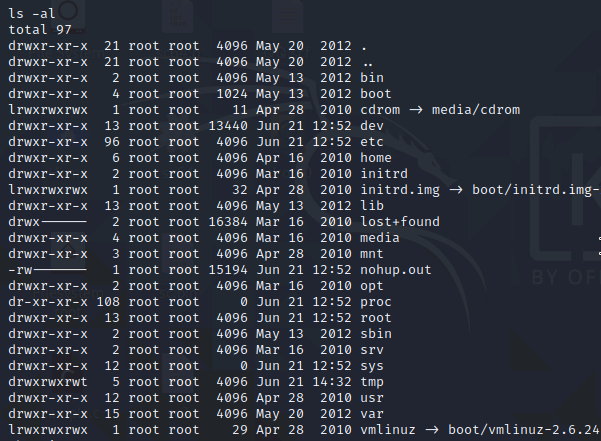
原本我還想設定payload，將其設為reverse\_tcp，不過這個ftp的backdoor程式好像不能設定，我就使用他預設的payload，也就是unix/interact 。

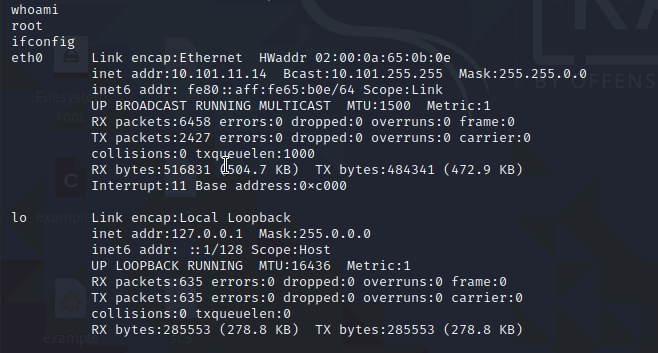
設定完成後就進行exploit





攻擊成功，在kali linus中可以查看靶機的資訊，可以執行CMD





參考資料

https://www.exploit-db.com/

https://blog.csdn.net/qq\_42967398/article/details/100777498

工作分配

張家禎：PPT準備與修改、書面報告準備與修改、EX2實作、EX3實作、EX5實作

王亭皓：PPT準備與修改、EX2實作、EX3實作

廖亭柔：書面報告準備與修改、EX2實作、EX4實作

羅傳郡： Exploit database中搜尋範例所需程式、PPT準備與修改、書面報告準備與修改、上台報告、EX1實作、EX2實作、EX3實作、EX4實作、EX5實作