

Nel caso di **firewall disabilitato** su Windows XP riusciamo ad eseguire la scansione con **nmap** da Kali Linux e trovare dei servizi attivi.

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org )
Nmap scan report for 192.168.240.150
Host is up (0.68s 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 20.89 seconds
```

Nel caso di **firewall abilitato** poiché esso blocca di default il traffico in entrata con protocollo **ICMP** (ping) dobbiamo usare il parametro **-Pn** per evitare il ping e passare direttamente alla scansione dei servizi. Dal risultato della scansione si conclude che l'abilitazione del firewall su Windows XP sta di fatto bloccando la scansione dall'esterno verso i servizi attivi sulla macchina, rendendo **inaccessibili** i servizi sulle porte 135, 139 e 445 **TCP** precedentemente trovati.

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.92 ( https://nmap.org )
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 215.00 seconds
```