

L'esercizio di oggi ci chiede di fare delle scansioni con nmap versione 7.92 sulla nostra macchina virtuale windows xp.

La prima cosa che siamo andati a fare è la scansione con il firewall di windows xp disattivato e come possiamo vedere dalla foto sotto ci restituisce i servizi attivi sulla nostra macchina target con la versione.

La seconda scansione che abbiamo effettuato è con il firewall attivo e come ci mostra la foto sotto non abbiamo ricevuto nessuna informazione riguardante i servizi attivi perché avendo il firewall attivo ci impedisce la connessione verso la nostra macchina target

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ sudo nano /etc/network/interfaces  
[sudo] password di kali:  
(kali@kali)-[~]  
$ nmap -sV 192.168.200.200 -o reportxp.txt  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-12 16:09 CEST  
Nmap scan report for 192.168.200.200  
Host is up (0.0039s 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 20.43 seconds  
zsh: segmentation fault  nmap -sV 192.168.200.200 -o reportxp.txt  
(kali@kali)-[~]  
$ nmap -sV 192.168.200.200 -o report1.txt  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-12 16:11 CEST  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.14 seconds  
zsh: segmentation fault  nmap -sV 192.168.200.200 -o report1.txt
```