CUORE ANDREA

19/12/2022

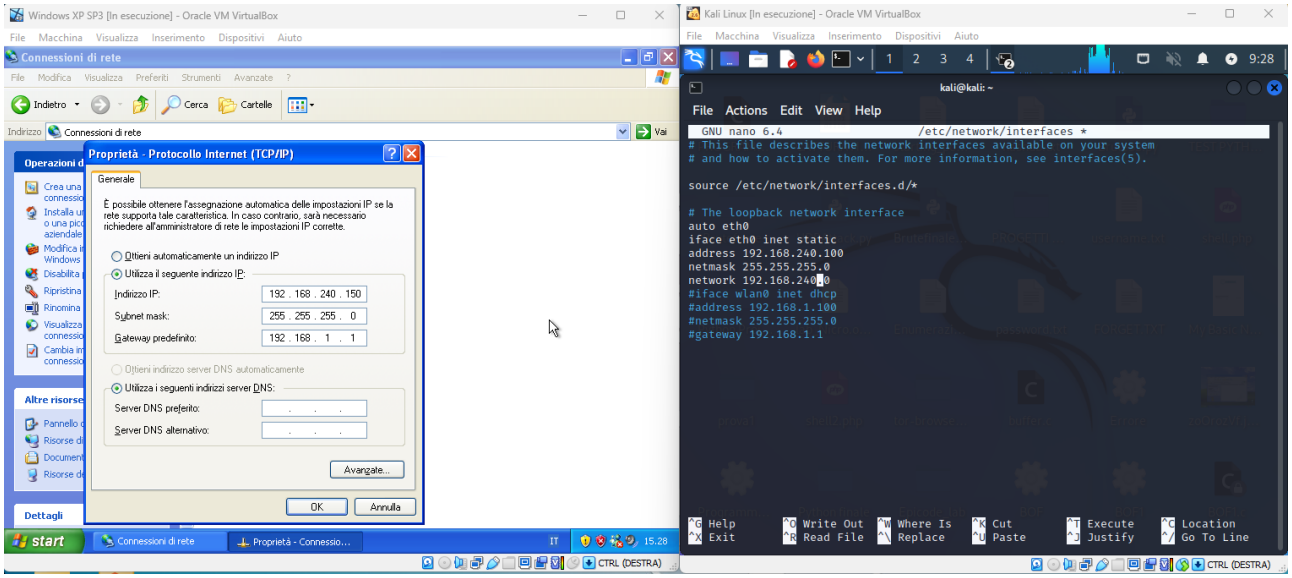
WINDOWS XP FIREWALL / NMAP & LOG

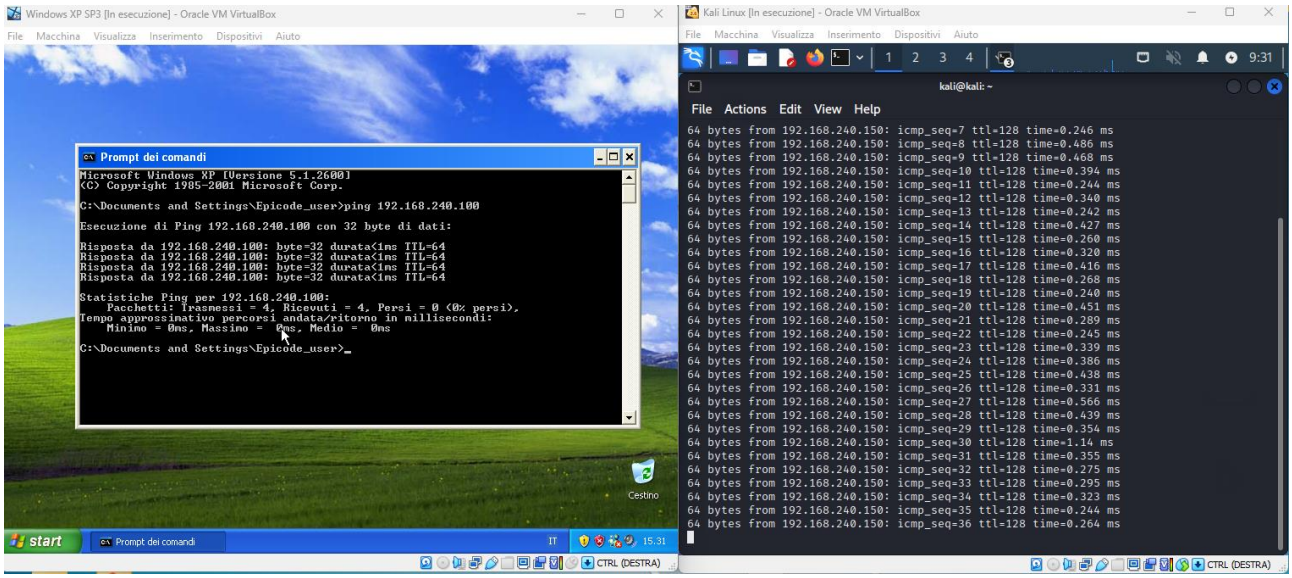
FASE 1) Configurazione indirizzi IP e test di ping

Come da traccia ci apprestiamo a configurare gli indirizzi IP delle due macchine e proseguiamo con un test di ping.

Windows: 192.168.240.150

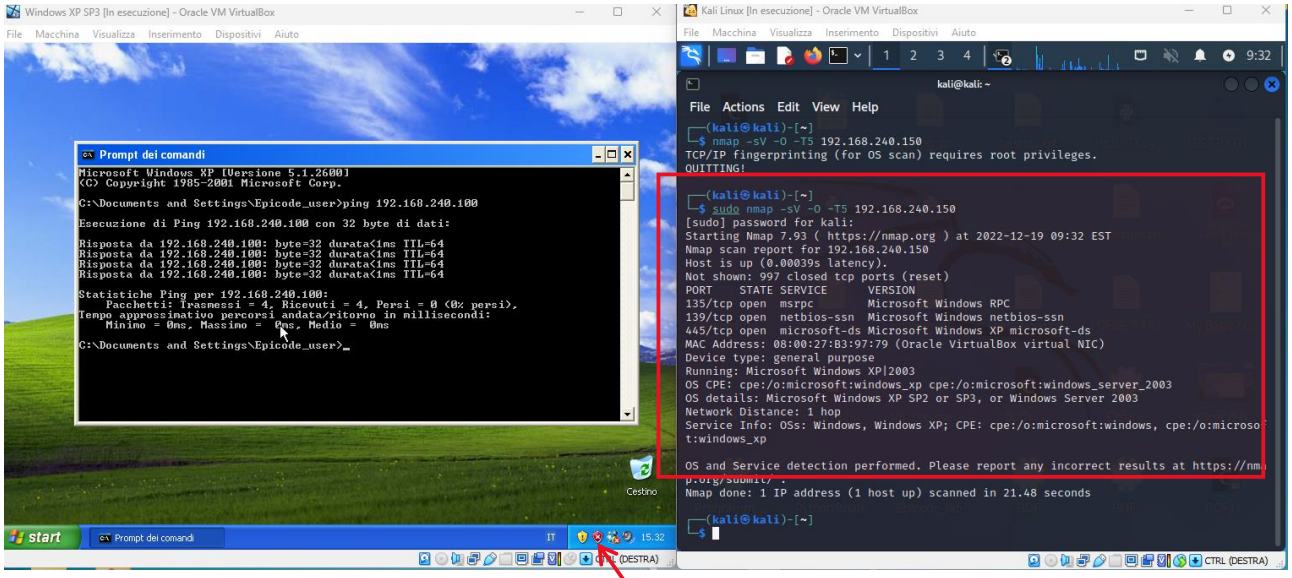
Kali: 192.168.240.100





FASE 2) NMAP CON FIREWALL DISATTIVATO

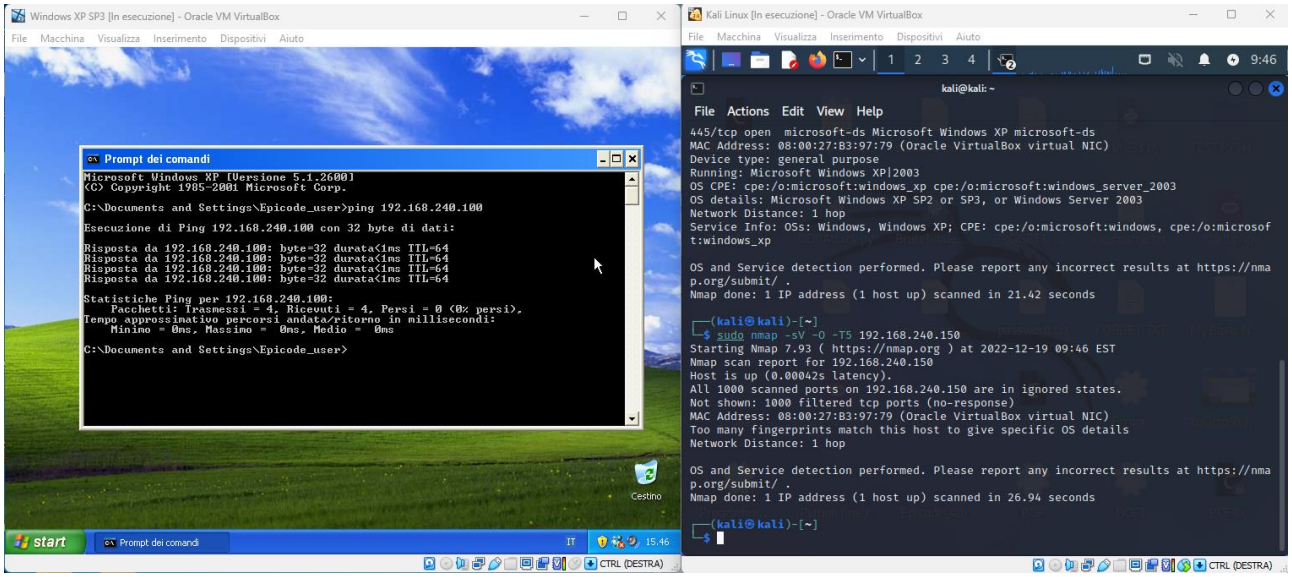
In questa fase ci apprestiamo ad eseguire una scansione con Nmap abilitando gli switch -sV -O per conoscere il tipo di S.O e l'eventuale versione dei servizi attivi sulla macchina.

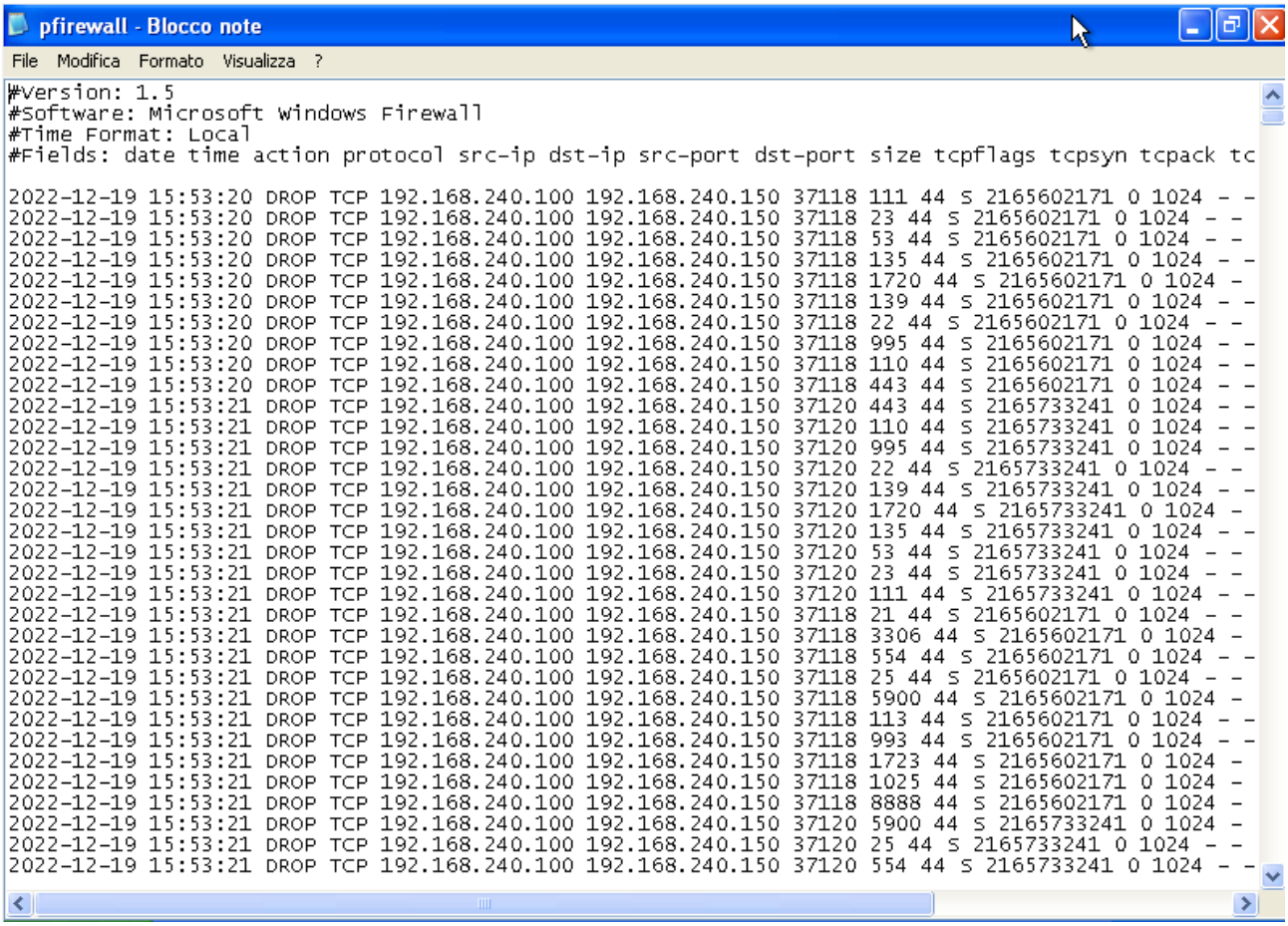


Possiamo notare l'effettiva mancanza del firewall dall'icona di errore di windows XP, come possiamo notare ci vengono restituite 3 porte con la relativa versione.

Fase 3) NMAP CON FIREWALL ABILITATO

Dopo l'abilitazione del Firewall di windows riprocediamo ad effettuare una scansione con nmap e possiamo notare che 1000 porte risultano filtrate, questo perché, come successivamente noteremo nel log di firewall, attivando il firewall tutti i pacchetti in ingresso provenienti da indirizzi IP non autorizzati prendono come action il DROP





pfirewall - Blocco note

File Modifica Formato Visualizza ?

```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tc

2022-12-19 15:53:20 DROP TCP 192.168.240.100 192.168.240.150 37118 111 44 S 2165602171 0 1024 - -
2022-12-19 15:53:20 DROP TCP 192.168.240.100 192.168.240.150 37118 23 44 S 2165602171 0 1024 - -
2022-12-19 15:53:20 DROP TCP 192.168.240.100 192.168.240.150 37118 53 44 S 2165602171 0 1024 - -
2022-12-19 15:53:20 DROP TCP 192.168.240.100 192.168.240.150 37118 135 44 S 2165602171 0 1024 - -
2022-12-19 15:53:20 DROP TCP 192.168.240.100 192.168.240.150 37118 1720 44 S 2165602171 0 1024 -
2022-12-19 15:53:20 DROP TCP 192.168.240.100 192.168.240.150 37118 139 44 S 2165602171 0 1024 - -
2022-12-19 15:53:20 DROP TCP 192.168.240.100 192.168.240.150 37118 22 44 S 2165602171 0 1024 - -
2022-12-19 15:53:20 DROP TCP 192.168.240.100 192.168.240.150 37118 995 44 S 2165602171 0 1024 - -
2022-12-19 15:53:20 DROP TCP 192.168.240.100 192.168.240.150 37118 110 44 S 2165602171 0 1024 - -
2022-12-19 15:53:20 DROP TCP 192.168.240.100 192.168.240.150 37118 443 44 S 2165602171 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37120 443 44 S 2165733241 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37120 110 44 S 2165733241 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37120 995 44 S 2165733241 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37120 22 44 S 2165733241 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37120 139 44 S 2165733241 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37120 1720 44 S 2165733241 0 1024 -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37120 135 44 S 2165733241 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37120 53 44 S 2165733241 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37120 23 44 S 2165733241 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37120 111 44 S 2165733241 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37118 21 44 S 2165602171 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37118 3306 44 S 2165602171 0 1024 -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37118 554 44 S 2165602171 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37118 25 44 S 2165602171 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37118 5900 44 S 2165602171 0 1024 -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37118 113 44 S 2165602171 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37118 993 44 S 2165602171 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37118 1723 44 S 2165602171 0 1024 -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37118 1025 44 S 2165602171 0 1024 -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37118 8888 44 S 2165602171 0 1024 -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37120 5900 44 S 2165733241 0 1024 -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37120 25 44 S 2165733241 0 1024 - -
2022-12-19 15:53:21 DROP TCP 192.168.240.100 192.168.240.150 37120 554 44 S 2165733241 0 1024 - -
```