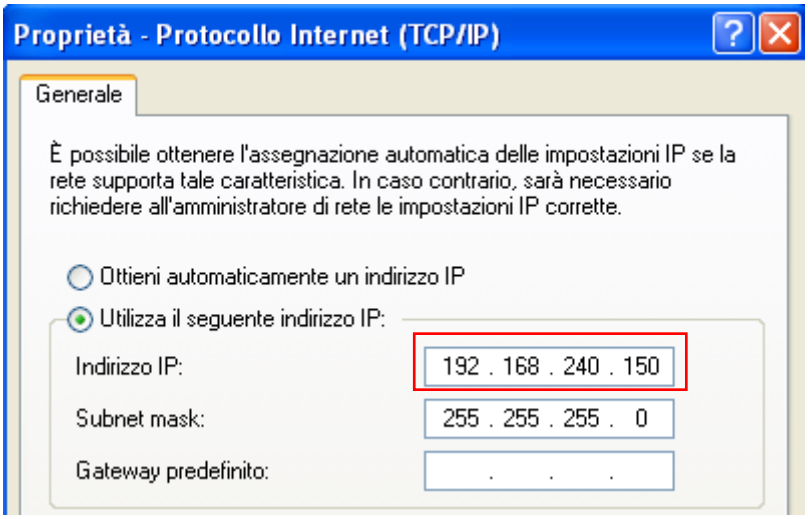
CONSEGNA SETTIMANA 9 LEZIONE 1

SOC: azioni preventive

Per verificare l'efficacia del firewall applicativo di windows XP effettueremo due scansioni nmap dalla macchina kali.

I parametri imposti nell'esercizio richiedevano *l'indirizzo IP di Kali 192.168.240.100/24* e *l'indirizzo IP di WindowsXP 192.168.240.150*, di seguito le configurazioni.

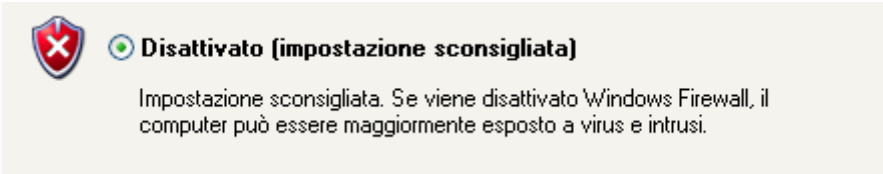
```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.240.100  netmask 255.255.255.0  broadcast 192.168.240.255
        inet6 fe80::a00:27ff:feea:2d58  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ea:2d:58  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 2204 (2.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



[PRIMA SCANSIONE NMAP -sV -T5 -Pn 192.168.240.150]

E' stata effettuata una prima scansione con il firewall disattivato, e possiamo notare che sono state rilevate 2 porte aperte:

- la porta **135** per il servizio *Windows RPC*
- la porta **139** per il servizio *netbios*



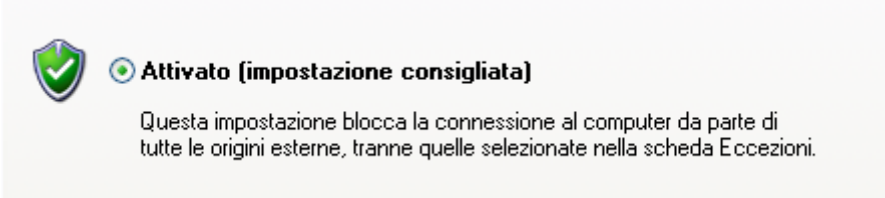

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -T5 -Pn 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 07:50 EST
Nmap scan report for 192.168.240.150
Host is up (0.00021s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.22 seconds
```

[SECONDA SCANSIONE NMAP -sV -T5 -Pn 192.168.240.150]

Dopo aver attivato il firewall all'interno di WindowsXP, ho provveduto ad eseguire una seconda scansione, identica alla precedente.

Il risultato è stata l'assenza totale di porte aperte, visibili tramite nmap.




```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -T5 -Pn 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 07:52 EST
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 65.97 seconds
```