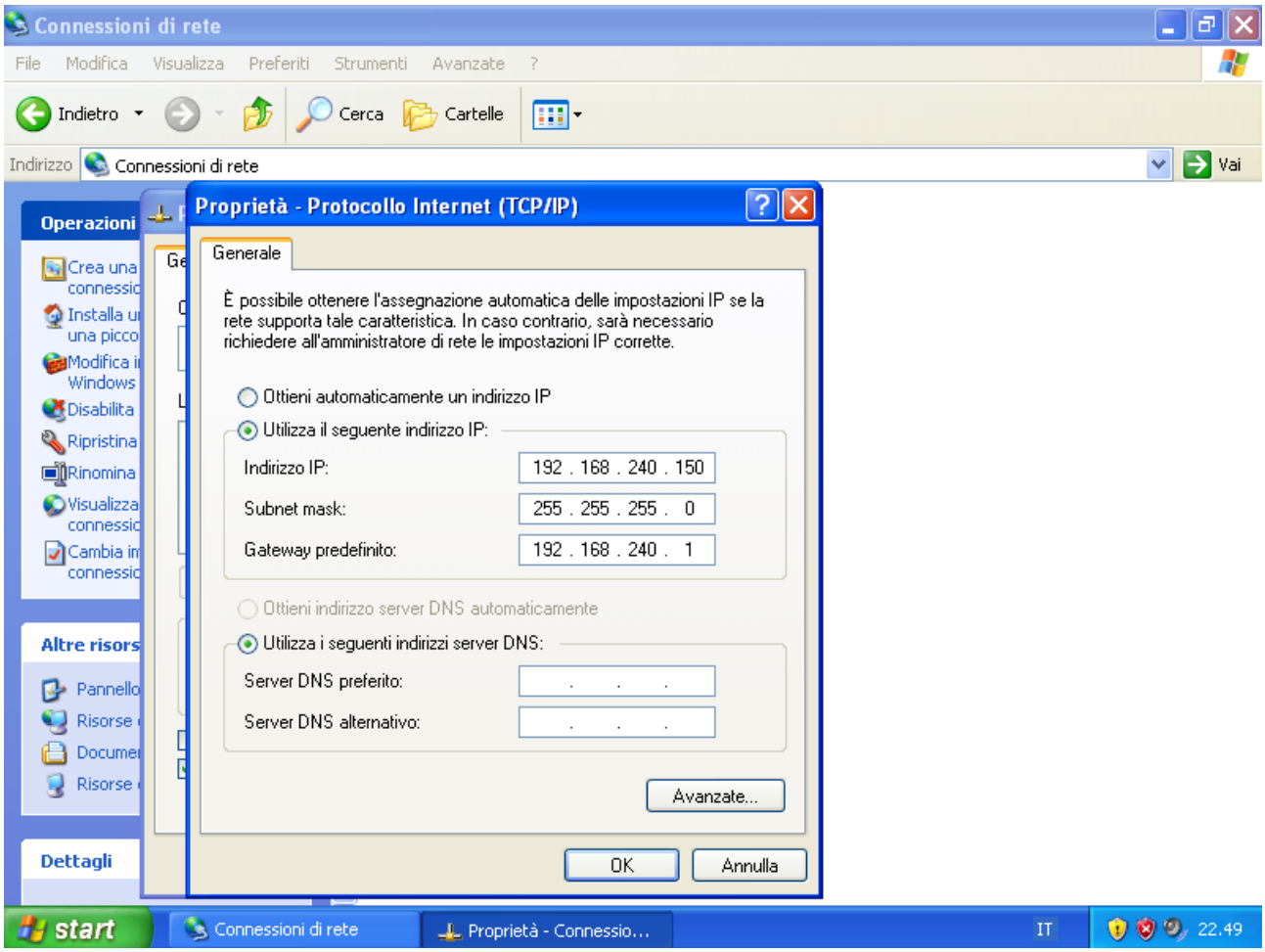
Esercizio S9-L1

Traccia:

Effettuare una scansione alla maccina Windows XP con firewall acceso e spento. Infine notare e descrivere le differenze.

Preparazione dell'ambiente:

Cambiamo gli indirizzi ip delle macchine come richiesto dall'esercizio:
IP Windows XP: 192.168.240.150



IP Kalilinux: 192.168.240.100

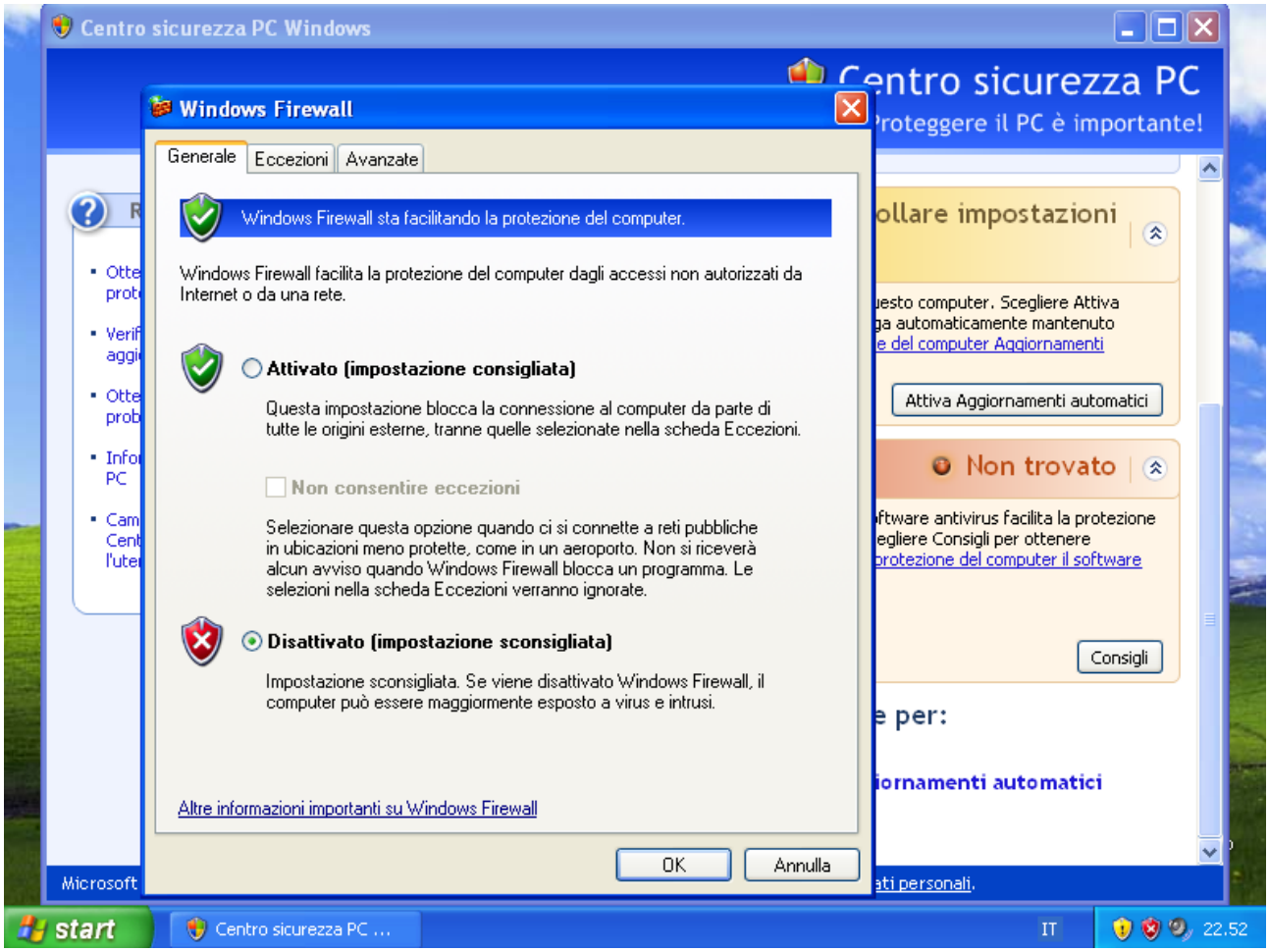
```
  GNU nano 7.2                                  /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.240.100/24
gateway 192.168.240.1
```

Infine si esegue su Kali il comando: " *sudo /etc/init.d/networking restart* " per riavviare il servizio di rete

Esercizio S9-L1

Svolgimento:

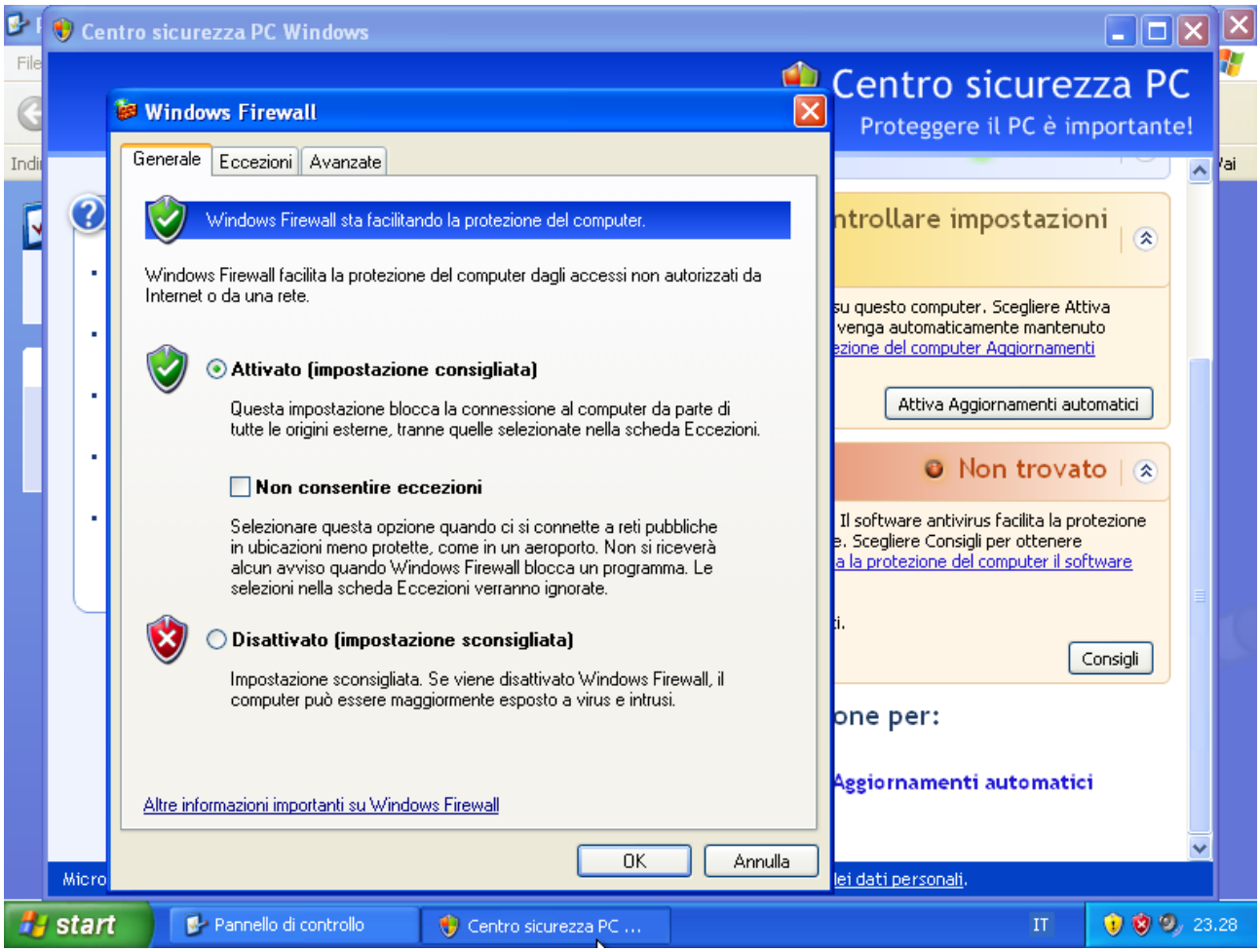
Con il Firewall disattivato su Windows XP, nmap è in grado di eseguire una scansione efficace dei servizi sulla macchina target, rilevando e identificando correttamente i servizi attivi e le relative versioni.




```
C:\home\kali\Desktop> nmap -sV 192.168.240.150 -o firewalloff.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 23:43 CET
Nmap scan report for 192.168.240.150
Host is up (0.00024s 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 20.55 seconds
```

Esercizio S9-L1

Tuttavia, una volta attivato il Firewall su Windows XP, nmap riscontra delle difficoltà nel completare la scansione dei servizi.




```
C:\home\kali\Desktop> nmap -sV 192.168.240.150 -o firewallon.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 23:41 CET
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 3.25 seconds
```

Questo accade perché il Firewall blocca le richieste di scansione provenienti dall'esterno, impedendo a nmap di ottenere le informazioni dettagliate sui servizi. In conclusione, l'attivazione del Firewall su Windows XP limita l'efficacia delle scansioni di nmap dall'esterno.

Glossario:

Firewall: Un firewall è un dispositivo hardware o software utilizzato per proteggere una rete da intrusioni non autorizzate provenienti da Internet o da una rete privata.

Nmap: Nmap è uno strumento di scansione di rete utilizzato per esaminare/mappare la topologia di una rete, per individuare i dispositivi connessi e i servizi in esecuzione su di essi.