

## ESERCIZIO W18D1

L'esercizio ci porta a considerare le differenze di nmap scanning su windows xp con firewall e senza firewall. Configuriamo la rete dei due dispositivi, Kali e Windows xp, come requisito fondamentale.

### Configurazione rete

```
GNU nano 2.2.2
# 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

# The ethernet interface
auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.240.150/24
netmask 255.255.255.0
gateway 192.168.1.1
```

Configurazione Kali

È possibile ottenere l'assegnazione automatica delle impostazioni IP se la rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.

☐ Ottieni automaticamente un indirizzo IP

☒ Utilizza il seguente indirizzo IP:

Indirizzo IP:

Subnet mask:

Gateway predefinito:

☐ Ottieni indirizzo server DNS automaticamente

☒ Utilizza i seguenti indirizzi server DNS:

Server DNS preferito:

Server DNS alternativo:

Windows xp configuration

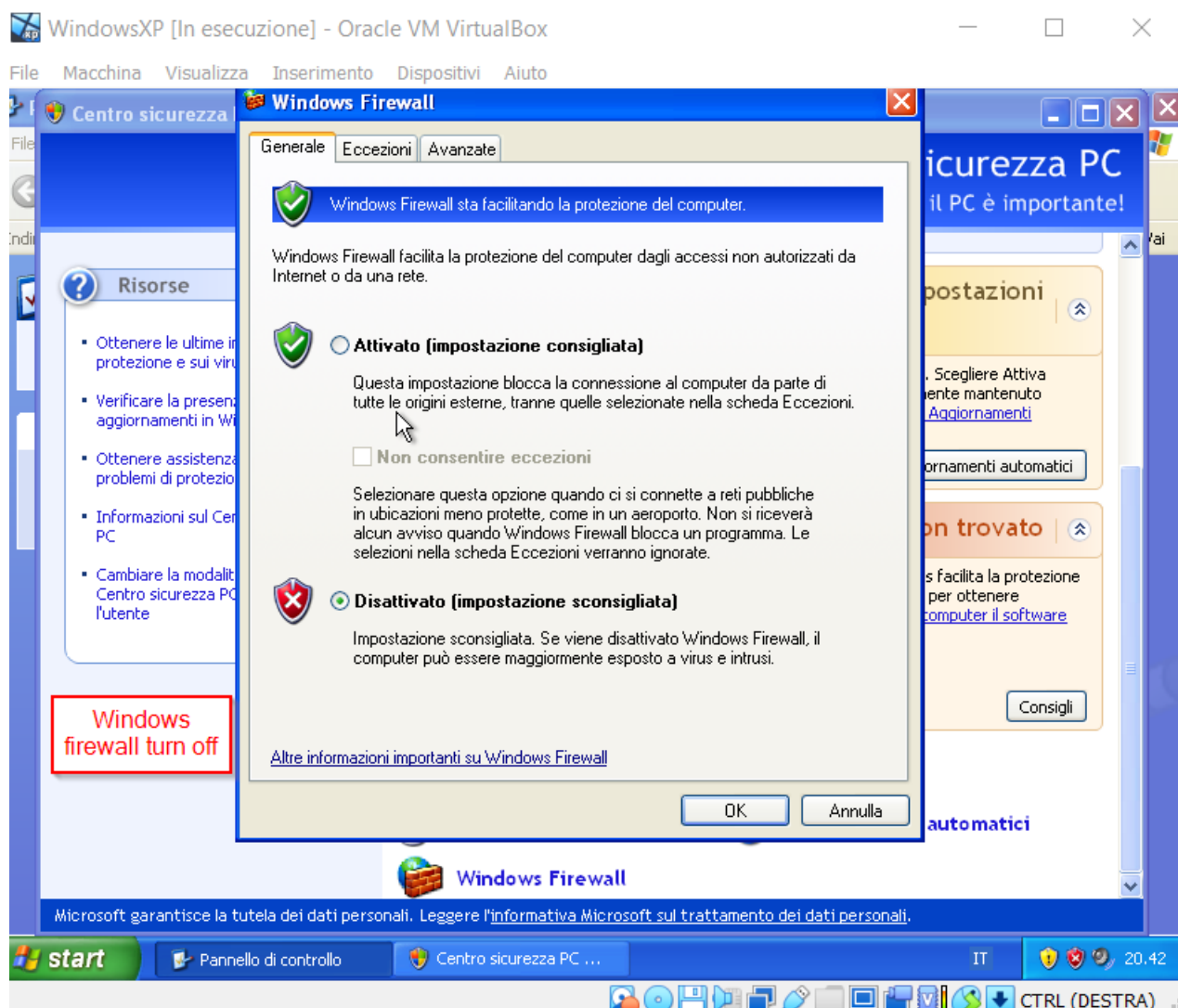
## Scansione nmap con firewall e senza firewall

In base alla presenza o meno del firewall di Windows XP, avremo una certa differenza di banner catturati.

```
(kali@kali)-[~]
└─$ sudo nmap -sV 192.168.240.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 14:58 EST
Nmap scan report for 192.168.240.100
Host is up (0.00052s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
2869/tcp  closed iclslap
MAC Address: 08:00:27:DA:4B:42 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.16 seconds
```

Windows  
firewall up



Windows  
firewall turn off

(kali㉿kali)-[~]

\$ sudo nmap -sV 192.168.240.100

Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2024-03-05 14:52 EST

Nmap scan report for 192.168.240.100

Host is up (0.00054s latency).

Not shown: 997 closed tcp ports (reset)

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
---------	------	--------------	-----------------------------------

MAC Address: 08:00:27:DA:4B:42 (Oracle VirtualBox virtual NIC)

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 21.82 seconds

no firewall  
nmap