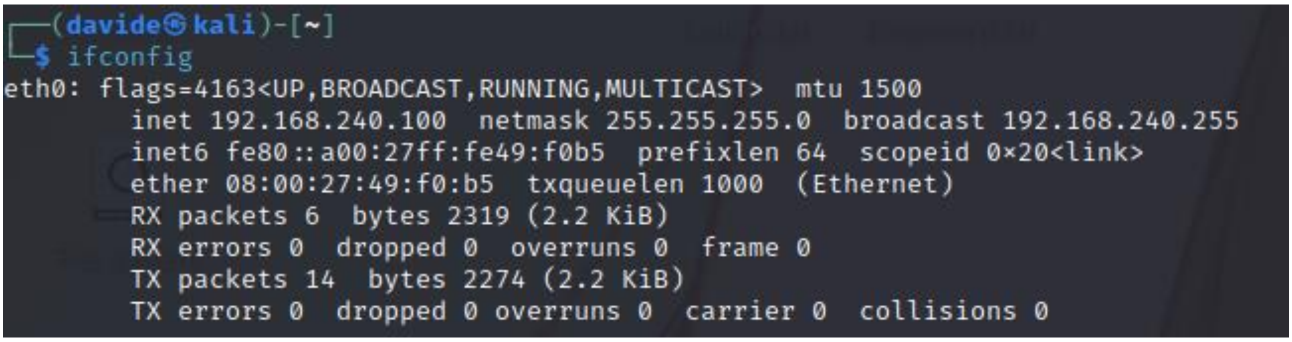
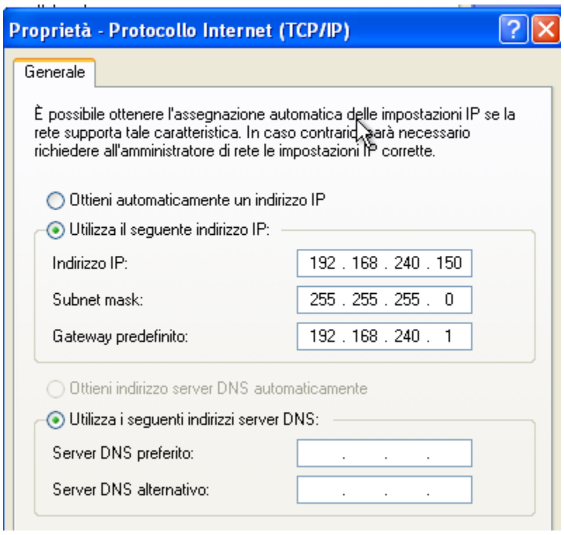
Configurazione Kali



```
┌──(davide㉿kali)-[~]
└─$ 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:fe49:f0b5  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:49:f0:b5  txqueuelen 1000  (Ethernet)
        RX packets 6  bytes 2319 (2.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 2274 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Configurazione Windows



Proprietà - Protocollo Internet (TCP/IP)

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: 192 . 168 . 240 . 150

Subnet mask: 255 . 255 . 255 . 0

Gateway predefinito: 192 . 168 . 240 . 1

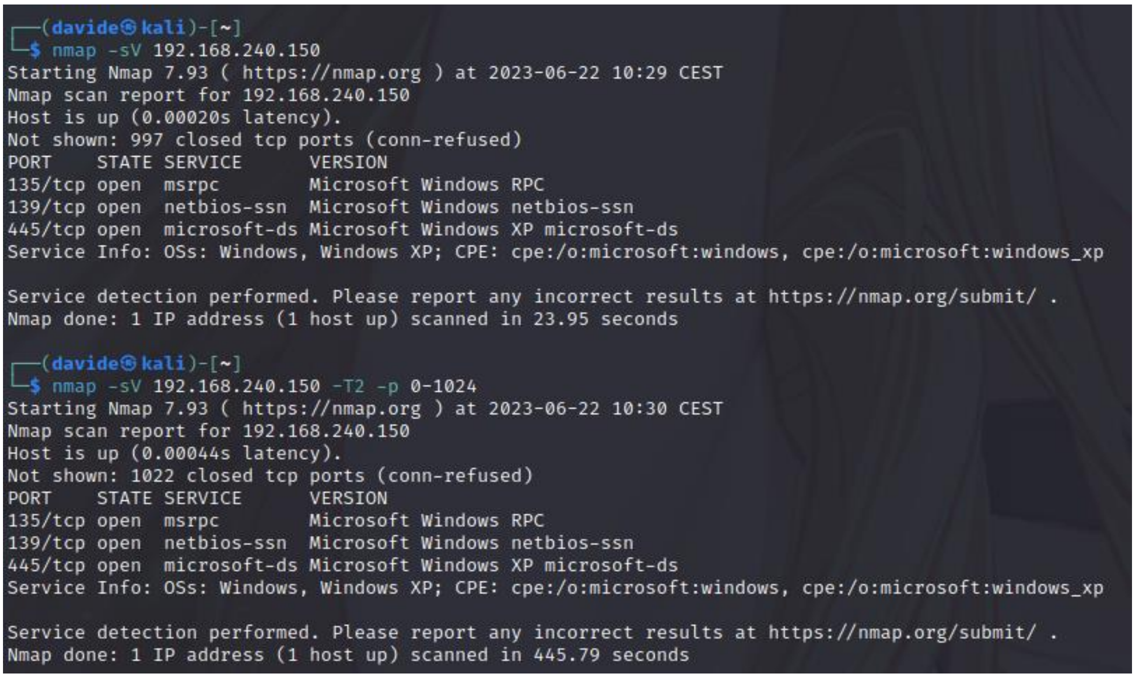
○ Ottieni indirizzo server DNS automaticamente

● Utilizza i seguenti indirizzi server DNS:

Server DNS preferito: . . .

Server DNS alternativo: . . .

Scansione nmap (rifatta per sicurezza del risultato) senza firewall attivo



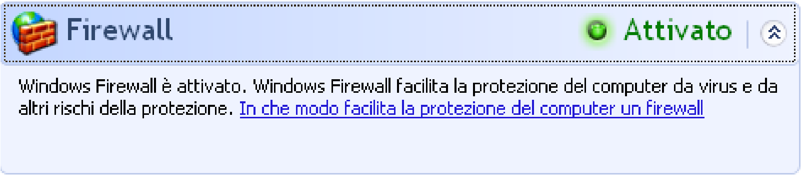
```
┌──(davide㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 10:29 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00020s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft 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 23.95 seconds

┌──(davide㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -T2 -p 0-1024
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 10:30 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00044s latency).
Not shown: 1022 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 445.79 seconds
```

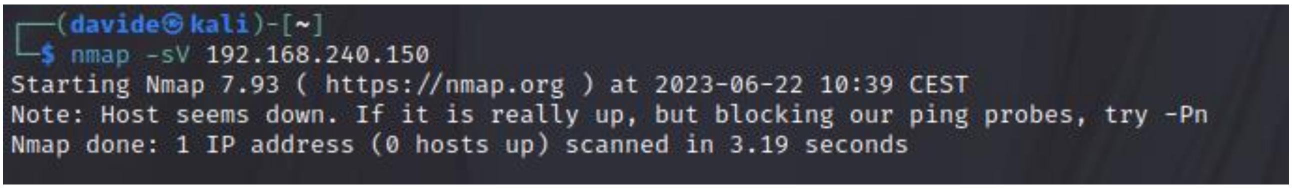
Attivazione firewall e successiva scansione nmap



Firewall Attivato

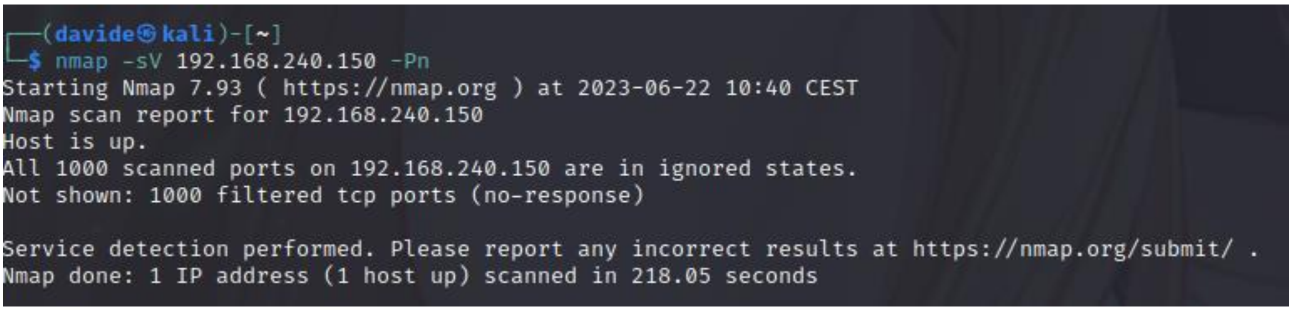
Windows Firewall è attivato. Windows Firewall facilita la protezione del computer da virus e da altri rischi della protezione. In che modo facilita la protezione del computer un firewall

Nmap senza switch -Pn



```
┌──(davide㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 10:39 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 3.19 seconds
```

Nmap con -Pn

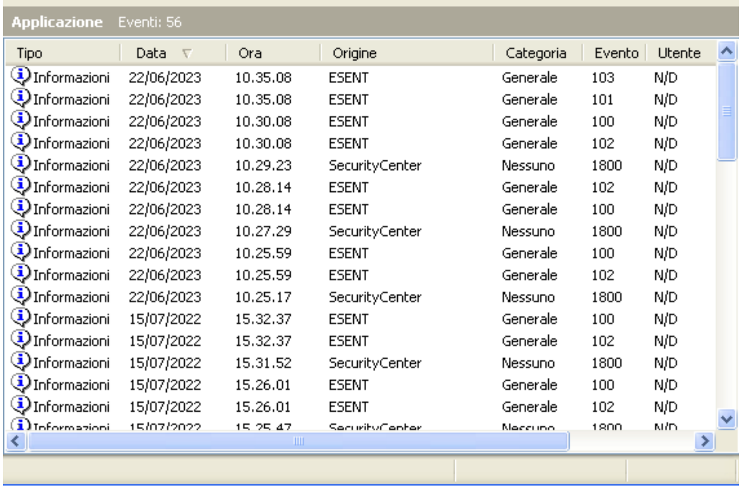


```
┌──(davide㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 10:40 CEST
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 218.05 seconds
```

Come possiamo vedere, il firewall filtra le porte del PC, non permettendo ad eventuali scansioni di identificare quali servizi possono essere sfruttati per avere accesso non autorizzato al computer della vittima.

Log



Applicazione Eventi: 56

Tipo	Data	Ora	Origine	Categoria	Evento	Utente
Informazioni	22/06/2023	10.35.08	ESENT	Generale	103	N/D
Informazioni	22/06/2023	10.35.08	ESENT	Generale	101	N/D
Informazioni	22/06/2023	10.30.08	ESENT	Generale	100	N/D
Informazioni	22/06/2023	10.30.08	ESENT	Generale	102	N/D
Informazioni	22/06/2023	10.29.23	SecurityCenter	Nessuno	1800	N/D
Informazioni	22/06/2023	10.28.14	ESENT	Generale	102	N/D
Informazioni	22/06/2023	10.28.14	ESENT	Generale	100	N/D
Informazioni	22/06/2023	10.27.29	SecurityCenter	Nessuno	1800	N/D
Informazioni	22/06/2023	10.25.59	ESENT	Generale	100	N/D
Informazioni	22/06/2023	10.25.59	ESENT	Generale	102	N/D
Informazioni	22/06/2023	10.25.17	SecurityCenter	Nessuno	1800	N/D
Informazioni	15/07/2022	15.32.37	ESENT	Generale	100	N/D
Informazioni	15/07/2022	15.32.37	ESENT	Generale	102	N/D
Informazioni	15/07/2022	15.31.52	SecurityCenter	Nessuno	1800	N/D
Informazioni	15/07/2022	15.26.01	ESENT	Generale	100	N/D
Informazioni	15/07/2022	15.26.01	ESENT	Generale	102	N/D
Informazioni	15/07/2022	15.25.47	SecurityCenter	Nessuno	1800	N/D