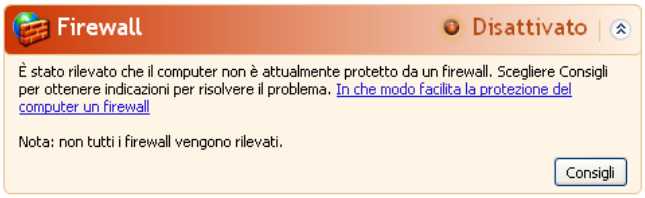
# ESERCIZIO 1 SETTIMANA 9



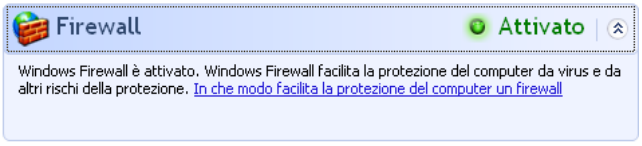

Con il firewall disattivato, grazie a **nmap -sV** possiamo vedere le porte aperte, i servizi e la loro versione.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -o report1 192.168.178.160
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 08:36 EST
Nmap scan report for test-epi.fritz.box (192.168.178.160)
Host is up (0.0023s 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 6.57 seconds
```

Aggiungendo -o possiamo salvare l'output in un file.

```
# Nmap 7.94SVN scan initiated Mon Feb  5 08:36:29 2024 as: nmap -sV -o report1 192.168.178.160
Nmap scan report for test-epi.fritz.box (192.168.178.160)
Host is up (0.0023s 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 at Mon Feb  5 08:36:36 2024 -- 1 IP address (1 host up) scanned in 6.57 seconds
```

Il firewall essendo disattivato ci permette di effettuare scansioni senza problemi, dato che la macchina è senza protezioni.

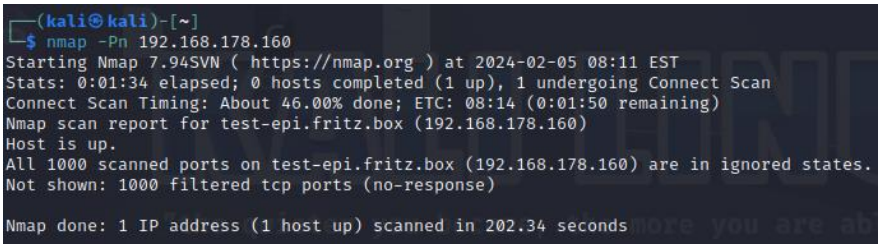



Attivando il firewall invece l'output di nmap cambia:

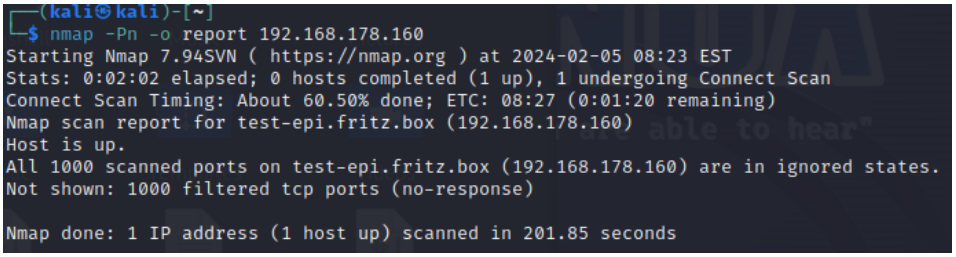
- Utilizzando lo switch -sV, per vedere le porte, i servizi e la loro versione, la scansione non parte perché vengono bloccati i pacchetti inviati alla macchina vittima, in modo da sembrare irraggiungibile.

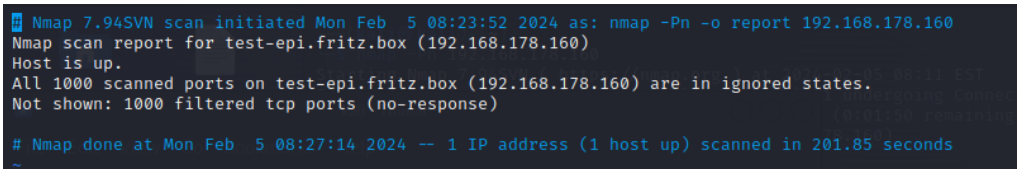
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.178.160
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 08:11 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.20 seconds
```

Provo allora ad usare lo switch -Pn come mi suggerisce nmap stesso, in questo caso i pacchetti vengono inviati senza verificare che l'host sia attivo.




Comando con report




Le differenze principali sono dovute dal fatto che con il firewall attivo vengono bloccati i pacchetti inviati e ciò impedisce di vedere i servizi e le porte aperte. Inoltre, il firewall potrebbe bloccare tutte le scansioni tipo nmap anche se con l'utilizzo degli switch giusti si riesce ad aggirare.

Con il firewall disattivato invece non c'è niente che protegge la macchina vittima quindi le scansioni con nmap avverranno con successo, perché non c'è niente che blocca le connessioni esterne e l'invio di pacchetti di nmap.