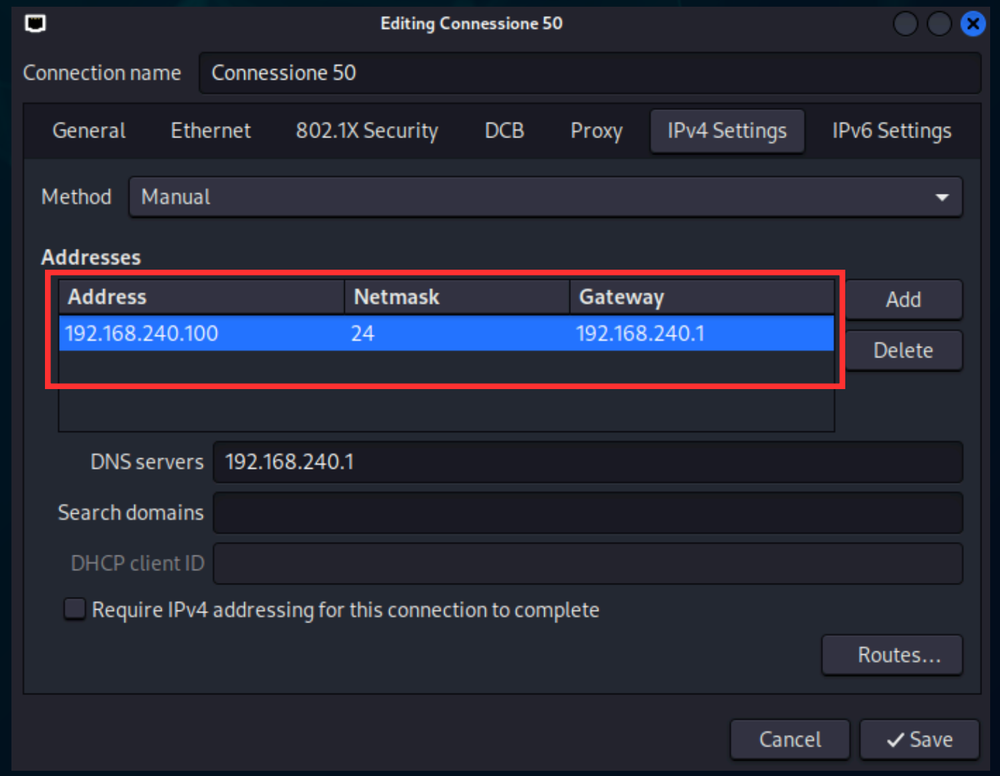
L’esercizio di oggi è verificare in che modo l’attivazione del Firewall impatta il risultato di una scansione dei servizi dall’esterno. Per questo motivo:

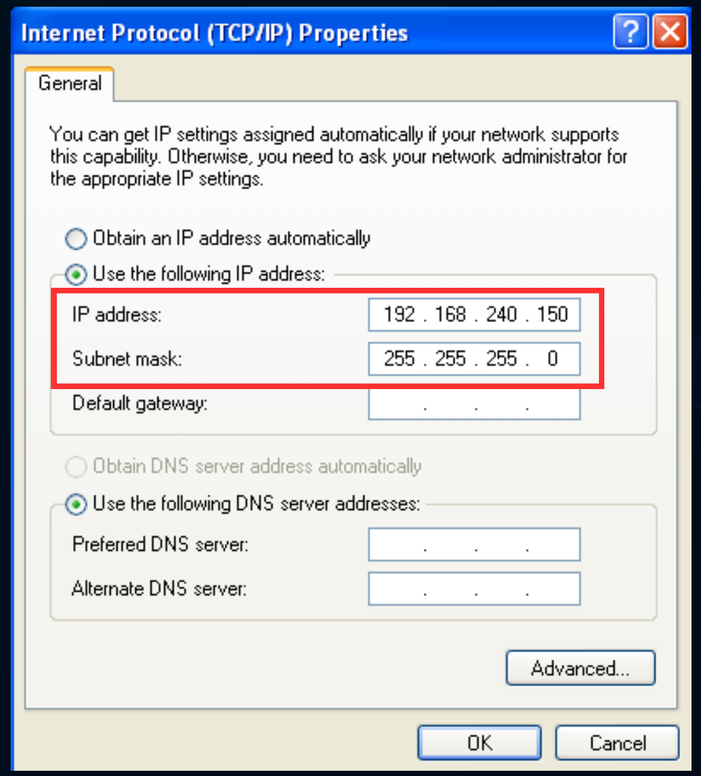
1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection e -o nomefilereport per salvare in un file l’output)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV. 5. Trovare le eventuali differenze e motivarle.

Prima di tutto assegno i giusti indirizzi IP alle macchine:

Kali: 192.168.240.100



WindowsXP: 192.168.240.150



Ping tra le due macchine

```
┌──(niko㉿kali)-[~]
└─$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=8.79 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=1.11 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=1.31 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=1.22 ms
^C
--- 192.168.240.150 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3035ms
rtt min/avg/max/mdev = 1.114/3.107/8.794/3.283 ms
```

Effettuo una scansione utilizzando nmap e l’opzione -sV per verificare le versioni dei servizi e -o per stampare il risultato di output in un file “scansione”

```
┌──(niko㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o scansione
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-20 11:21 CEST
Nmap scan report for 192.168.240.150
Host is up (0.0010s 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 20.49 seconds
```

Ho trovato tre porte aperte ed informazioni sul sistema operativo

Ora abilito il Windows Firewall ed effettuo una nuova scansione

Inizialmente nmap non riusciva ad effettuare la scansione quindi ho utilizzato l'opzione -Pn per forzare la scansione andando a saltare il ping scan

```
┌──(niko㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-20 11:23 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 3.11 seconds
```

Ho trovato due porte aperte uguali alla scansione precedente e due chiuse

```
┌──(niko㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150 -nP
[sudo] password for niko:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-20 11:23 CEST
Nmap scan report for 192.168.240.150
Host is up (0.0015s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE      VERSION
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  Microsoft Windows XP microsoft-ds
2869/tcp closed icslap
3389/tcp closed ms-wbt-server
MAC Address: 08:00:27:82:77:82 (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 11.06 seconds
```

Utilizzando l’opzione --reason nmap ci darà un motivo per cui una porta si trova in un determinato stato. Possiamo notare che entrambe le porte chiuse hanno come descrizione “reset” questo perchè le porte sono raggiungibili ma su di esse non esiste nessun servizio in ascolto, quindi viene mandato indietro un pacchetto che contiene il campo reset

```
┌──(niko㉿kali)-[~]
└─$ sudo nmap -sV -T3 192.168.240.150 -Pn  --reason
[sudo] password for niko:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-20 13:36 CEST
Nmap scan report for 192.168.240.150
Host is up, received arp-response (0.0034s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE      REASON         VERSION
139/tcp  open   netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds syn-ack ttl 128 Microsoft Windows XP microsoft-ds
2869/tcp closed icslap       reset ttl 128
3389/tcp closed ms-wbt-server reset ttl 128
MAC Address: 08:00:27:82:77:82 (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 24.46 seconds
```

I tre stati principali nei quali Nmap classifica le porte (sono sei totali):

OPEN (APERTA)

Un'applicazione accetta attivamente su questa porta connessioni TCP, datagrammi UDP o associazioni SCTP. La ricerca di questo tipo di porte è spesso l'obiettivo primario del port scanning. Chi si dedica alla sicurezza sa che ogni porta aperta è una strada verso un attacco. Gli attaccanti e i tester di sicurezza (penetration testers, conosciuti anche come "pen-testers") hanno come obiettivo quello di trovare e trarre vantaggio dalle porte aperte, mentre d'altro canto gli amministratori di rete e i sistemisti provano a chiuderle o a proteggerle con firewall senza limitare gli utenti autorizzati al loro uso. Le porte aperte sono anche interessanti per tutta una serie di scansioni non indirizzate unicamente alla sicurezza, perché mostrano che servizi sono disponibili in una rete.

CLOSED (CHIUSA)

Una porta chiusa è accessibile (riceve e risponde ai pacchetti di probe di Nmap) ma non vi è alcuna applicazione in ascolto su di essa. Esse possono rendersi utili nel mostrare che un host è attivo su un indirizzo IP (durante l'host discovery o il ping scanning) o in quanto parte integrante dell'Operating System discovery. Poiché una porta chiusa è raggiungibile, può essere interessante effettuare una scansione più tardi nel caso alcune vengano aperte. Chi amministra una macchina o una rete può voler bloccare tali porte con un firewall ed in questo caso esse apparirebbero come filtrate, come mostrato in seguito.

FILTERED (FILTRATA)

In questo caso Nmap non può determinare con esattezza se la porta sia aperta o meno, perché un filtro di pacchetti impedisce ai probe di raggiungere la porta. Questo filtro può esser dovuto a un firewall dedicato, alle regole di un router, o a un firewall software installato sulla macchina stessa. Queste porte forniscono poche informazioni e rendono frustrante il lavoro dell'attaccante. A volte esse rispondono con un messaggio ICMP del tipo 3, codice 13 ("destination unreachable: communication administratively prohibited", ovvero "destinazione non raggiungibile: comunicazione impedita da regole di gestione"), ma in genere sono molto più comuni i filtri di pacchetti che semplicemente ignorano i tentativi di connessione senza rispondere. Questo obbliga Nmap a riprovare diverse volte, semplicemente per essere sicuri che il pacchetto non sia stato perduto a causa di una congestione di rete o di problemi simili piuttosto che dal firewall o dal filtro stesso. Questo riduce drammaticamente la velocità della scansione.