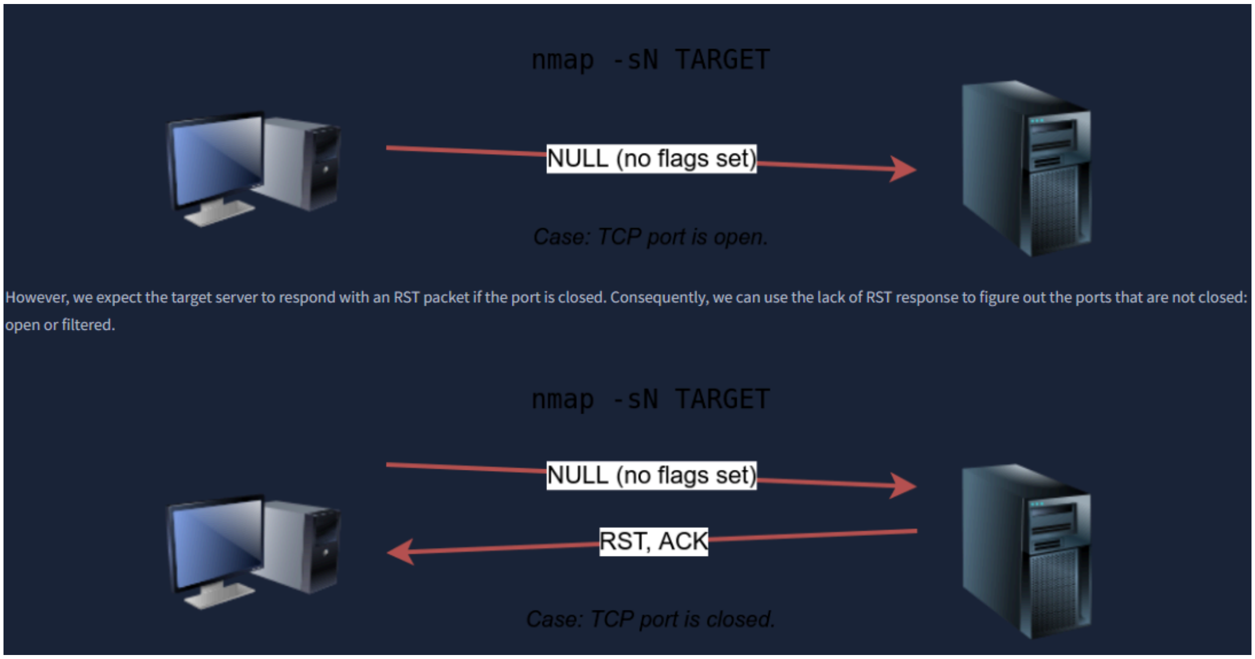
Nmap UDP Scan

We will begin this document with the following 3 types of scan:

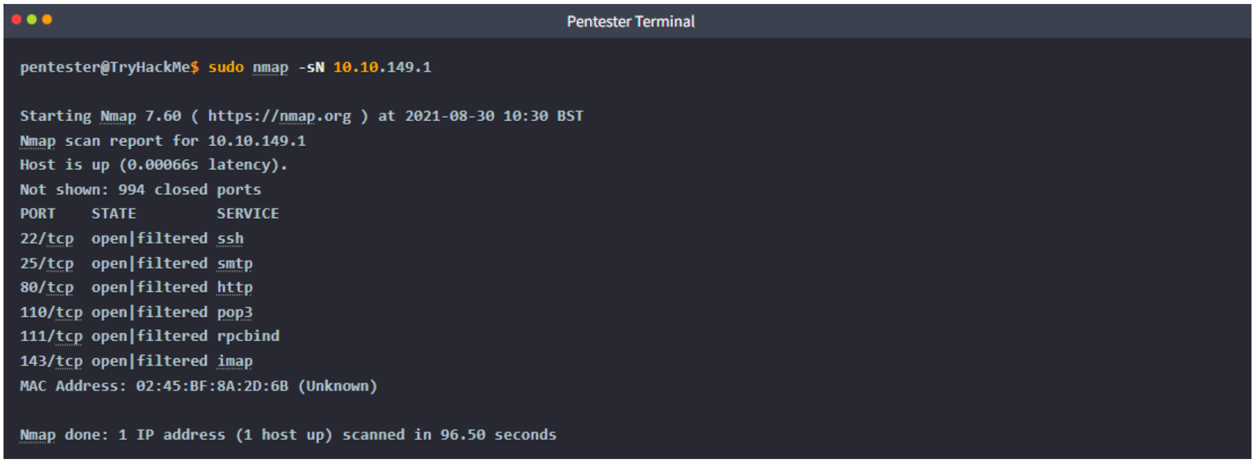
1. **Null Scan**
2. **FIN Scan**
3. **Xmas Scan**

Null Scan:

Does not set any flag, all six flag bits are set to 0. Use **-sN** to achieve this. A TCP packet with no flags set will not trigger any response when it reaches an open port.



However, we expect the target server to respond with an RST packet if the port is closed. Consequently, we can use the lack of RST response to figure out the ports that are not closed: open or filtered.

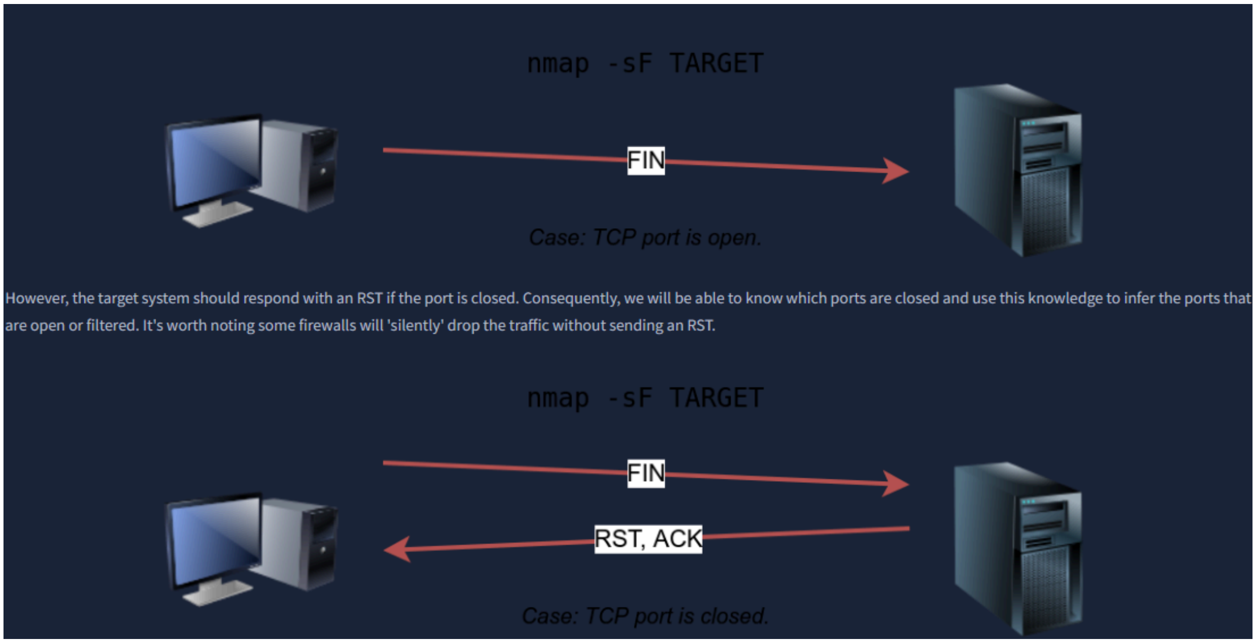


```
pentester@TryHackMe$ sudo nmap -sN 10.10.149.1

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:30 BST
Nmap scan report for 10.10.149.1
Host is up (0.00066s latency).
Not shown: 994 closed ports
PORT    STATE         SERVICE
22/tcp  open|filtered ssh
25/tcp  open|filtered smtp
80/tcp  open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 96.50 seconds
```

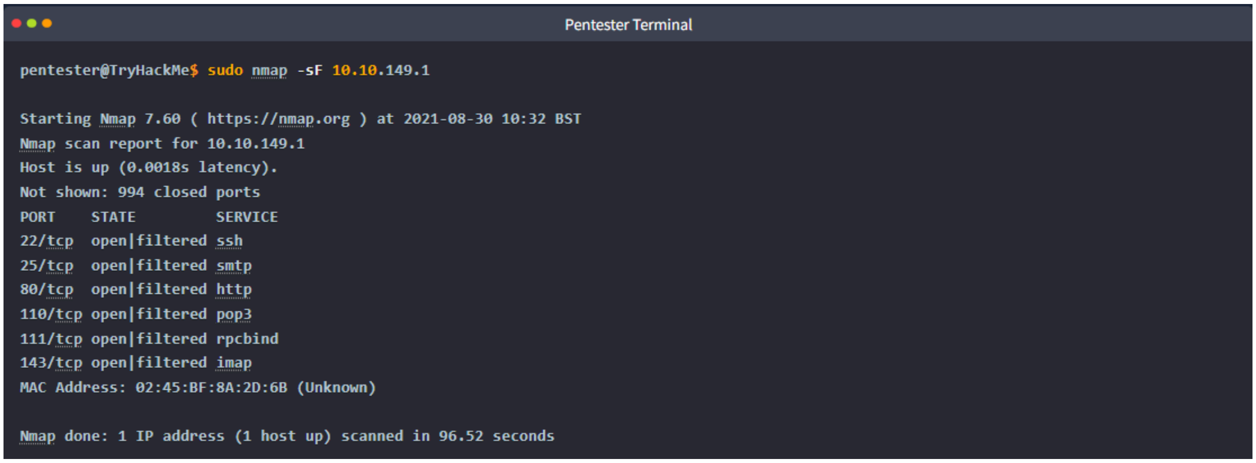
This is a linux example, but note again, using the sudo using the -sN option you must be running Nmap as root.

FIN Scan:

Sends a TCP packet with the FIN flag set. This can be done by using **-sF** to achieve this. Similarly no response will be sent if the TCP port is open. Nmap cannot be sure if the port is open if a **firewall is blocking traffic related to this TCP port.**



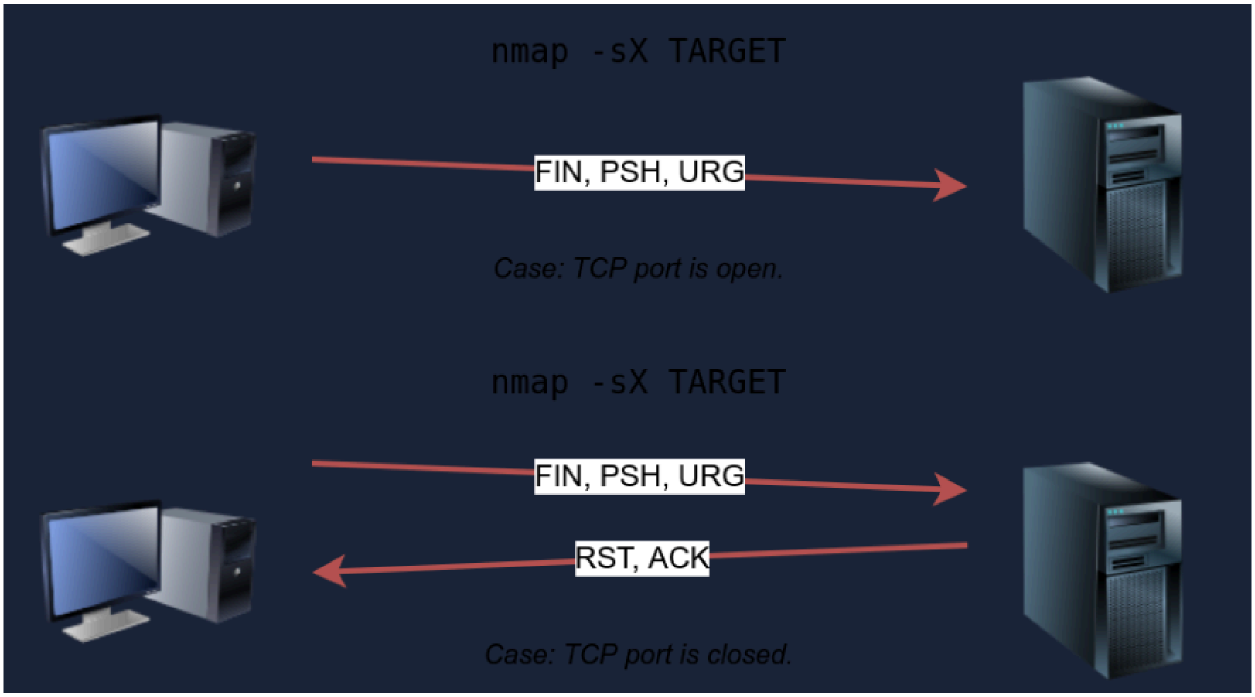
However, the target system should respond with an RST if the port is closed. Consequently, we will be able to know which ports are closed and use this knowledge to infer the ports that are open or filtered. It's worth noting some firewalls will 'silently' drop the traffic without sending an RST.

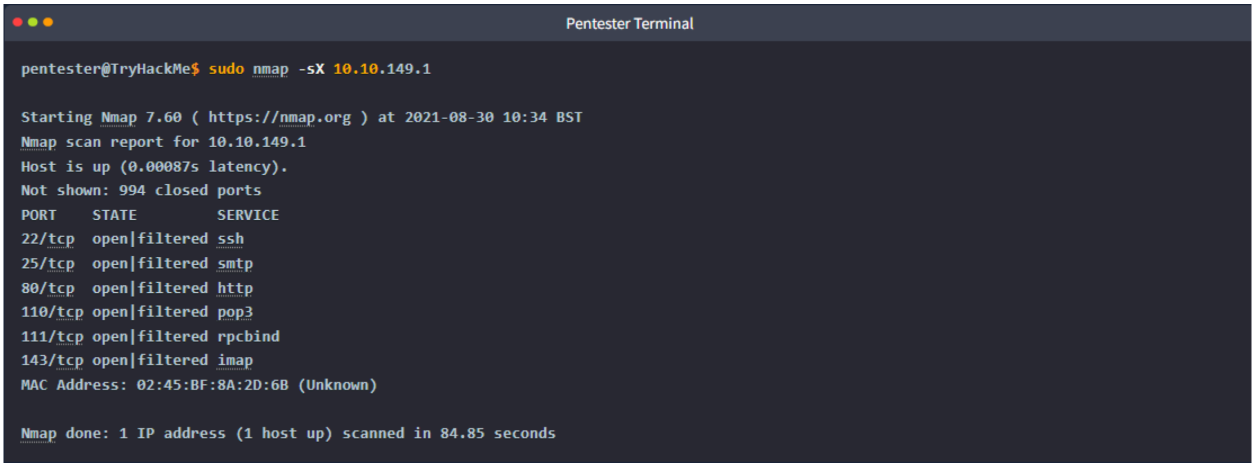


```
pentester@TryHackMe$ sudo nmap -sF 10.10.149.1

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:32 BST
Nmap scan report for 10.10.149.1
Host is up (0.0018s latency).
Not shown: 994 closed ports
PORT    STATE         SERVICE
22/tcp  open|filtered ssh
25/tcp  open|filtered smtp
80/tcp  open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 96.52 seconds
```

Xmas Scan:

Gets its name after christmas tree lights. Sets the FIN,PSH and URG flag simultaneously use **-sX** to achieve this. Like the Null scan and FIN scan, if an RST packet is received it means the port is closed otherwise it will be reported as Open|Filtered.





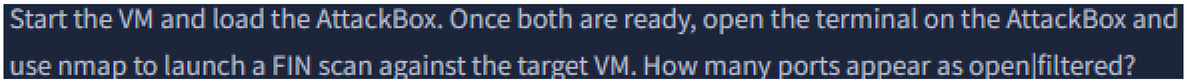
```
pentester@TryHackMe$ sudo nmap -sX 10.10.149.1

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:34 BST
Nmap scan report for 10.10.149.1
Host is up (0.00087s latency).
Not shown: 994 closed ports
PORT    STATE         SERVICE
22/tcp  open|filtered ssh
25/tcp  open|filtered smtp
80/tcp  open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 84.85 seconds
```

However, these 3 scan types are efficient when scanning behind a stateless (non-stateful_ firewall. A stateless firewall will check incoming packets has the SYN flag to detect a connection attempt. Using a flag combination that does not match the SYN packet makes it possible to **deceive the firewall and reach the system behind it.** However a stateful fire wall will practical block all crafted packets, making them useless.

Questions:

In a null scan how many flags are set to 1? 0 - No flags are set.

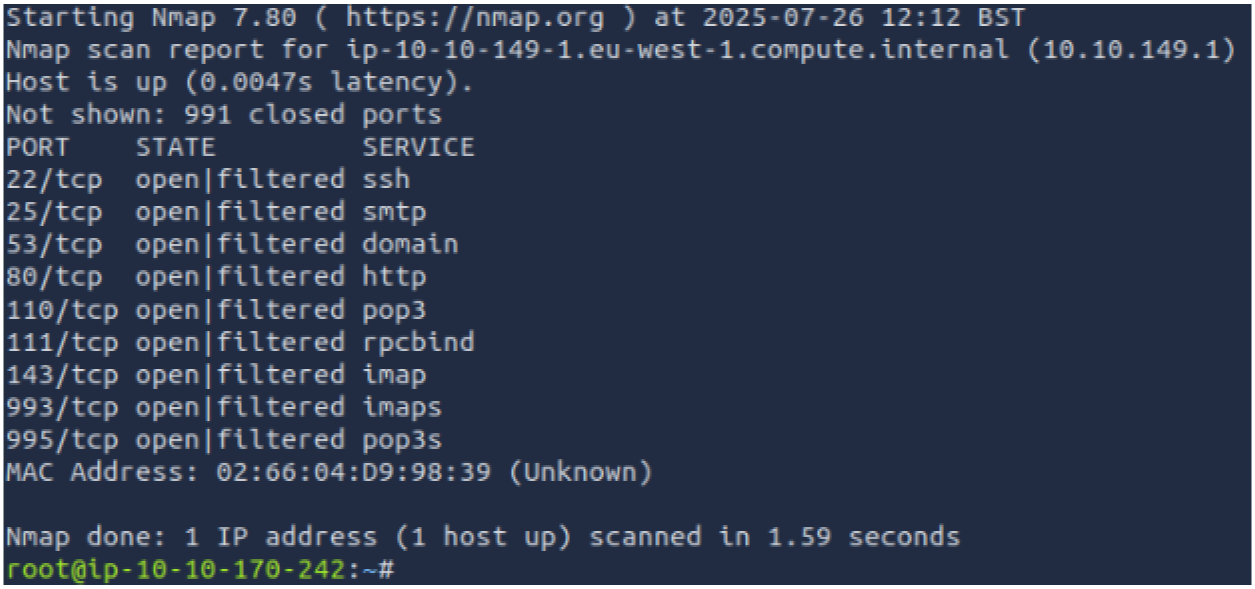
In a FIN scan how many flags are set to 1? 1 - You are sending the FIN flag only.
In an Xmas scan how many flags are set to 1? 3 - Sending FIN,PSH and URG all at once.



Start the VM and load the AttackBox. Once both are ready, open the terminal on the AttackBox and use nmap to launch a FIN scan against the target VM. How many ports appear as open|filtered?

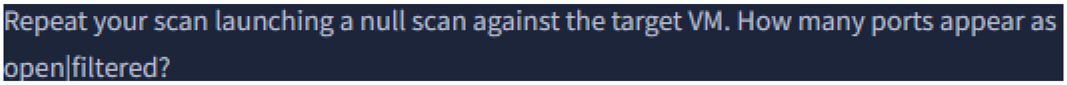
So opening the attack box! Getting the command prompt ready and the target IP is: 10.10.149.1

So we need to perform a **FIN** scan, against 10.10.149.1. To do this we must remember that the FIN scan code in the prompt will be: nmap -sF 10.10.149.1



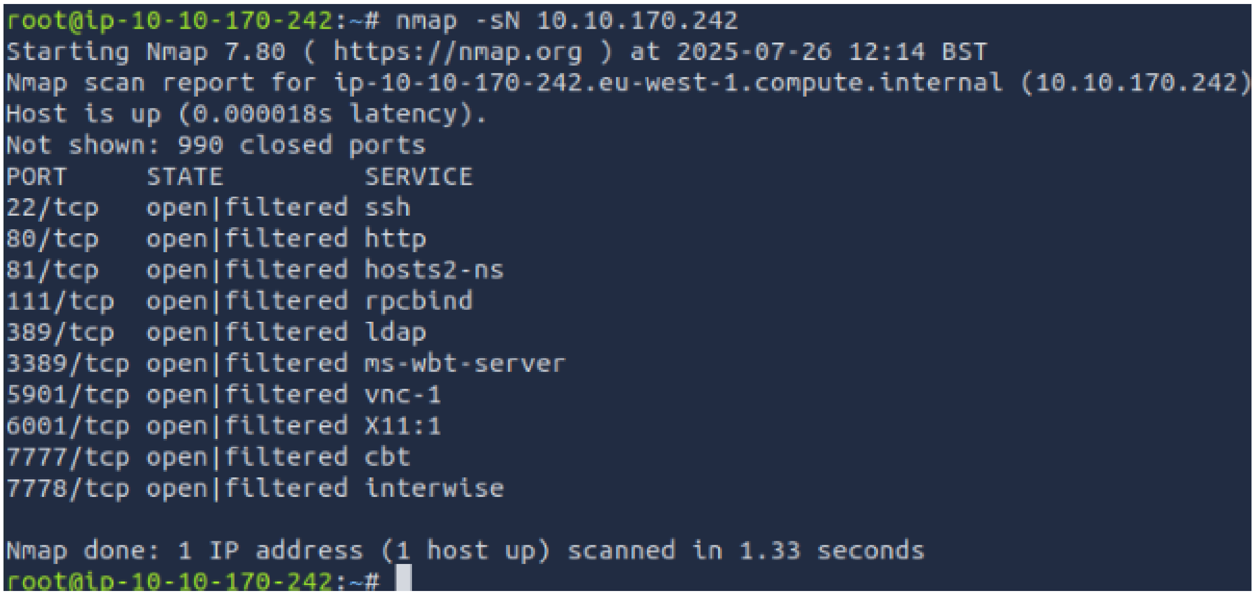
```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-26 12:12 BST
Nmap scan report for ip-10-10-149-1.eu-west-1.compute.internal (10.10.149.1)
Host is up (0.0047s latency).
Not shown: 991 closed ports
PORT    STATE         SERVICE
22/tcp  open|filtered ssh
25/tcp  open|filtered smtp
53/tcp  open|filtered domain
80/tcp  open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
993/tcp open|filtered imaps
995/tcp open|filtered pop3s
MAC Address: 02:66:04:D9:98:39 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
root@ip-10-10-170-242:~#
```

Like so. We can see 9 ports are **FILTERED**. Including domain! Which is new to me. So to answer the question, we have 9 ports Filtered.



Repeat your scan launching a null scan against the target VM. How many ports appear as open|filtered?

So using a null scan, we would put the code in the command prompt reading: nmap -sN 10.10.170.242



```
root@ip-10-10-170-242:~# nmap -sN 10.10.170.242
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-26 12:14 BST
Nmap scan report for ip-10-10-170-242.eu-west-1.compute.internal (10.10.170.242)
Host is up (0.000018s latency).
Not shown: 990 closed ports
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
80/tcp   open|filtered http
81/tcp   open|filtered hosts2-ns
111/tcp  open|filtered rpcbind
389/tcp  open|filtered ldap
3389/tcp open|filtered ms-wbt-server
5901/tcp open|filtered vnc-1
6001/tcp open|filtered X11:1
7777/tcp open|filtered cbt
7778/tcp open|filtered interwise

Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds
root@ip-10-10-170-242:~# 
```

Awesome! Hey we discovered another port too! A total of 10 ports were revealed.
So, to answer the question, technically we would put 10, but it is only asking for 1 character/value. In this case I put 9 in and got it correct! Got to work with what you have!

Conclusion:
Sometimes using multiple scans can increase the information available to us as the attacker. When gaining as much information is paramount especially using public accessible information such as Nmap, we can obtain a data collection of all ports known, even if it is open|filtered we can get a better understanding of what security is in place, if it is effective, and if there is any way of bypassing it secretly.