Step 1: Nmap is capable of performing basic checks for open ports. To conduct this  
simple audit using the nmap utility, add the -sT parameters. Your first scan should be  
done using the loopback address (127.0.0.1). **This allows you to see what network  
services are being offered by your system without any firewall settings interfering with  
the results**:

$ **nmap -sT 127.0.0.1**  
Starting Nmap 5.51 ( http://nmap.org ) at 2015-03-07 13:16 EST  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.0011s latency).  
Not shown: 996 closed ports  
PORT STATE SERVICE  
**22/tcp open ssh**  
**25/tcp open smtp**  
**111/tcp open rpcbind**  
**631/tcp open ipp**  
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

In the preceding example’s Nmap results, you can see that four network services  
(ssh, smtp, rpcbind, and ipp) are currently listening for services requests at designated  
ports (22, 25, 111, 631). However, to see what services can be reached outside the firewall,  
you need to conduct another scan.

Step 2: This scan is almost exactly like the preceding example. It uses the same nmap options,  
-sT. However, this time, the machine’s IP address is used instead of the loopback address.  
**This will allow you to see what services are not being blocked by a firewall**:  
$ **nmap -sT 192.168.56.101**  
Starting Nmap 5.51 ( http://nmap.org ) at 2015-03-07 13:20 EST  
Nmap scan report for 192.168.56.101  
Host is up (0.00049s latency).  
Not shown: 998 closed ports  
PORT STATE SERVICE  
**22/tcp open ssh**  
**111/tcp open rpcbind**  
Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds  
$  
Notice that this time, only two services are displayed. Keep in mind that even though the  
outside world may not see all of the services, you still should disable unneeded  
network services.

As you can see, 25/tcp open smtp, 631/tcp open ipp are not displayed when using

nmap -sT 192.168.56.101

=> It means 25/tcp open smtp, 631/tcp are blocked by firewall.

You can do the same steps (step 1, step 2) to check which UDP ports are blocked by firewall using nmap -sU