Nmap Tutorial

hackertarget.com/nmap-tutorial

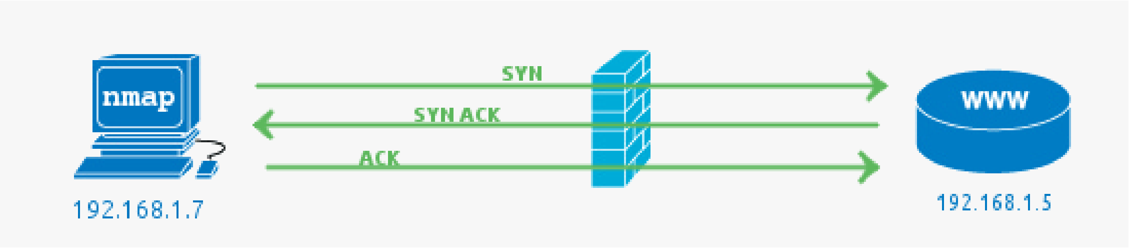
Understanding Open, Closed and Filtered

Nmap has a variety of scan types. Understanding how the default and most common `SYN` scan works is a good place to start to examine how the scan works and interpreting the results.

The 3 way TCP handshake

First, a bit of background, during communication with a TCP service, a single connection is established with the TCP 3 way handshake. This involves a `SYN` sent to an TCP open port that has a service bound to it, typical examples are HTTP (port 80), SMTP (port 25), POP3 (port 110) or SSH (port 22).

The server side will see the `SYN` and respond with `SYN ACK`, with the client answering the `SYN ACK` with an `ACK`. This completes the set up and the data of the service protocol can now be communicated.

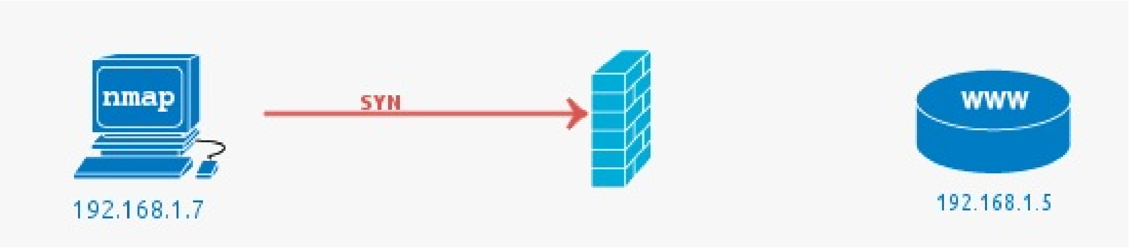


In this example, the firewall passes the traffic to the web server (HTTP -> 80) and the web server responds with the acknowledgement.

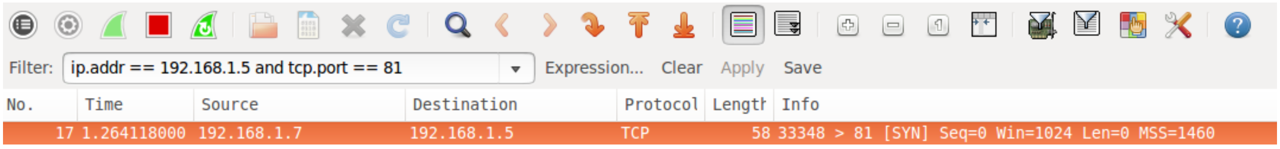
In all these examples a firewall could be a separate hardware device, or it could be a local software firewall on the host computer.

Filtered ports or when the Firewall drops a packet

The job of a firewall is to protect a system from unwanted packets that could harm the system. In this simple example, the port scan is conducted against port 81, as there is no service running on this port, using a firewall to block access to it is best practice.



A filtered port result from Nmap indicates that the port has not responded at all. The SYN packet has simply been dropped by the firewall. See the following Wireshark packet capture that shows the initial packet with no response.



Filter: ip.addr == 192.168.1.5 and tcp.port == 81

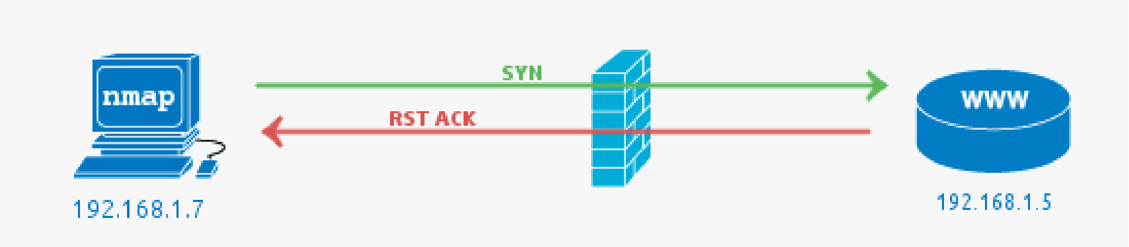
No.	Time	Source	Destination	Protocol	Lengtł	Info
17	1.264118000	192.168.1.7	192.168.1.5	TCP	58	33348 > 81 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

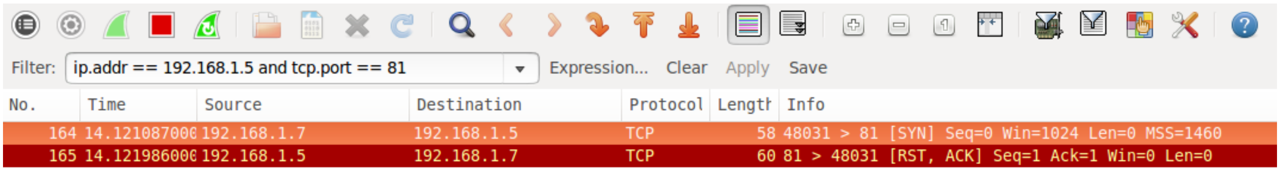
Closed ports or when the Firewall fails

In this case, closed ports most commonly indicate there is no service running on the port, but the firewall has allowed the connection to go through to the server. It can also mean no firewall is present at all.

Note that while we are discussing the most common scenarios, it is possible to configure a firewall to reject packets rather than drop. This would mean packets hitting the firewall would be seen as closed (the firewall is responding with RST ACK).

Pictured below is a case where a firewall rule allows the packet on port 81 through even though there is no service listening on the port. This is most likely because the firewall is poorly configured.
anook2



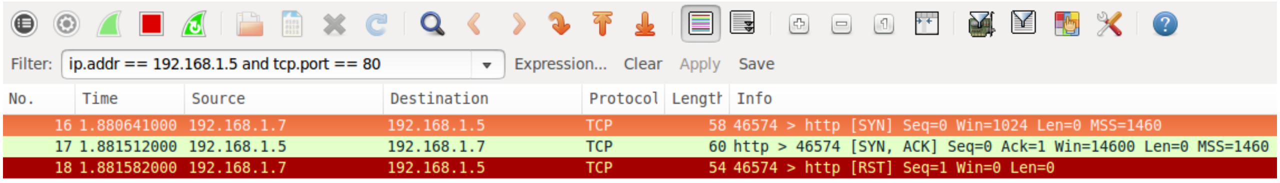


Filter: ip.addr == 192.168.1.5 and tcp.port == 81

No.	Time	Source	Destination	Protocol	Lengtł	Info
164	14.12108700(	192.168.1.7	192.168.1.5	TCP	58	48031 > 81 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
165	14.12198600(	192.168.1.5	192.168.1.7	TCP	60	81 > 48031 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

An Open Port (service) is found

Open Ports are usually what you are looking for when kicking off Nmap scans. The open service could be a publicly accessible service that is, by its nature, supposed to be accessible. It may be a back-end service that does not need to be publicly accessible, and therefore should be blocked by a firewall.



Filter: ip.addr == 192.168.1.5 and tcp.port == 80

No.	Time	Source	Destination	Protocol	Lengtł	Info
16	1.880641000	192.168.1.7	192.168.1.5	TCP	58	46574 > http [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	1.881512000	192.168.1.5	192.168.1.7	TCP	60	http > 46574 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
18	1.881582000	192.168.1.7	192.168.1.5	TCP	54	46574 > http [RST] Seq=1 Win=0 Len=0

An interesting thing to notice in the wireshark capture is the `RST` packet sent after accepting the `SYN ACK` from the web server. The `RST` is sent by Nmap as the state of the port (open) has been determined by the `SYN ACK` if we were looking for further information such as the HTTP service version or to get the page, the RST would not be sent. A full connection would be established.