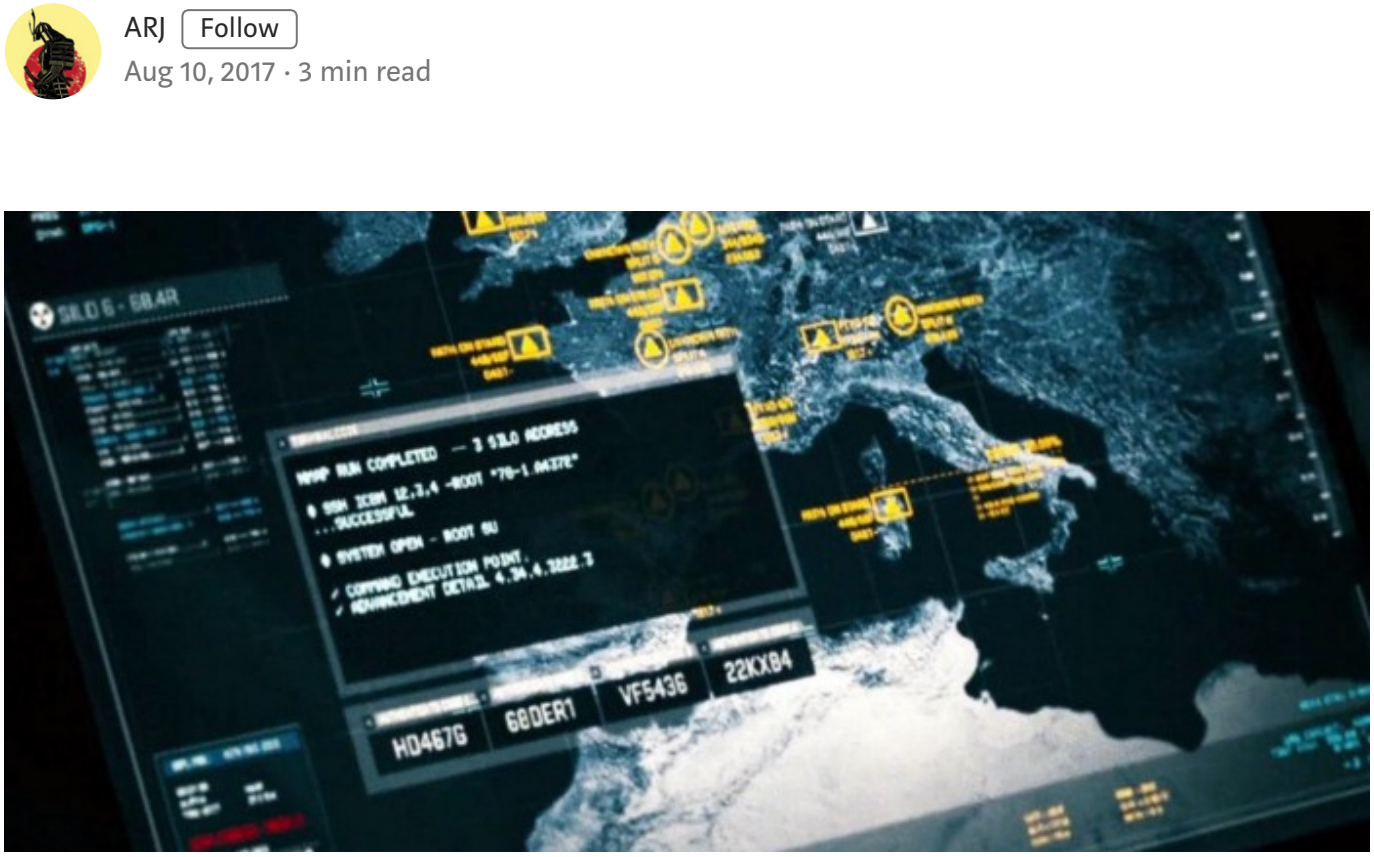
Difference between Nmap TCP SYN Scan and TCP Connect Scan



ARJ Follow
Aug 10, 2017 · 3 min read

TCP SYN Scan

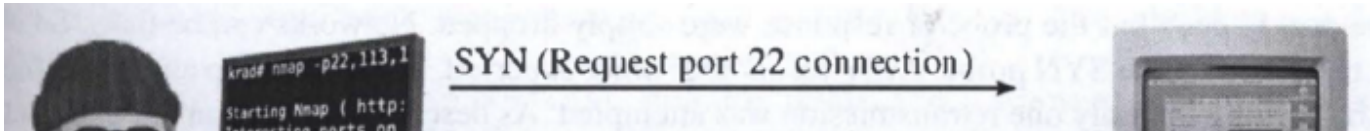
TCP SYN scan is a most popular and default scan in Nmap because it perform quickly compare to other scan types and it is also less likely to block from firewalls.Another reason is that when it comes to states open,closed and filtered ,TCP SYN scan gives a clear definition.Main concept behind this scan is TCP three way handshake. TCP SYN scan required raw-packet privileges that needs root access.

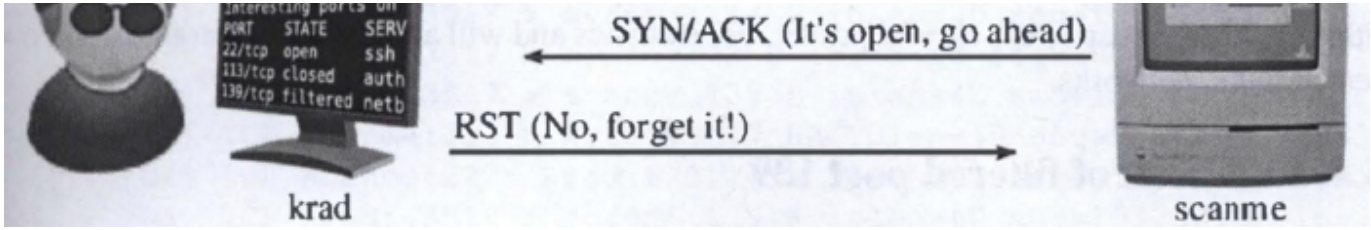
```
root@kali:~# nmap -sS -p22,25,110 scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-10 04:07 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.042s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
PORT    STATE    SERVICE
22/tcp  open     ssh
25/tcp  filtered smtp
110/tcp filtered pop3

Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
```

Open state :





What happened there is that Nmap tries to establish a connection between scanme.nmap.org by sending TCP SYN packet.In this situation server sends a SYN/ACK packets to establish the connection.This is the result that Nmap uses to determine whether the port is open. Nmap reset the connection at the end.

Close state:

TCP SYN packet is sends to the server as the last time and what happned here is server directly reject the connection with RST packet due to the closed port.

filtered port:

In the filtered state, Server doesn't sends a reply back,not even a RST packet to terminate the connection. Most accurate reason can be a firewall on the server side blocks reply packets.So Nmap decides this type of ports as filtered.

Another things is that default SYN scan is not enough for slip through a network with firewalls and intrusion prevention systems.It needs more

improved techniques.

TCP Connect Scan

In the Nmap TCP connection scan, Nmap asks its underlying Operating network to establish a connection with the target server by issuing the “connect” system call.But the problem with this scan is that it takes time to complete and it require to generate more packets to obtain information.In the other hand, targets are more likely to allow the connection because it tries to establish a connection with target same as network enabled applications like web browsers.

Open state :

First two steps are exactly the same as TCP SYN scan and instead of sending a reset(RST) packet ,TCP Connect Scan sends a ACK packet and establish the connection.After the establish the connection, it resets the connection.

Other steps of SYN Connect scan is same as SYN scan which is mentioned in the above section.

So the difference between these two scan types is TCP Connect scan establish a full connection with the target but SYN scan completes only a half of the connection with target.

Networking Nmap Ports Tcp Network Security

150 claps

WRITTEN BY

ARJ

Follow

See responses (3)

More From Medium

Related reads

Reconnaissance: a eulogy in three acts

europa

Feb 11, 2018 · 8 min read

1.5K

Also tagged Tcp

How TCP segment size can affect application traffic flow

Shashank Suresh Kumar in...
Jul 24 · 8 min read ★

33

Related reads

CRLF Injection Into PHP's cURL Options

TomNomNom
Aug 1, 2018 · 7 min read

866