Scanning:

A process looking for a “live” system, identifying those systems and discovering what ports are open or closed. Check if those systems are running any services.

Types of scans:

1. Network scan
2. Port Scan
3. Vulnerability scan

Port Scan:

Port = IP Address + Protocol

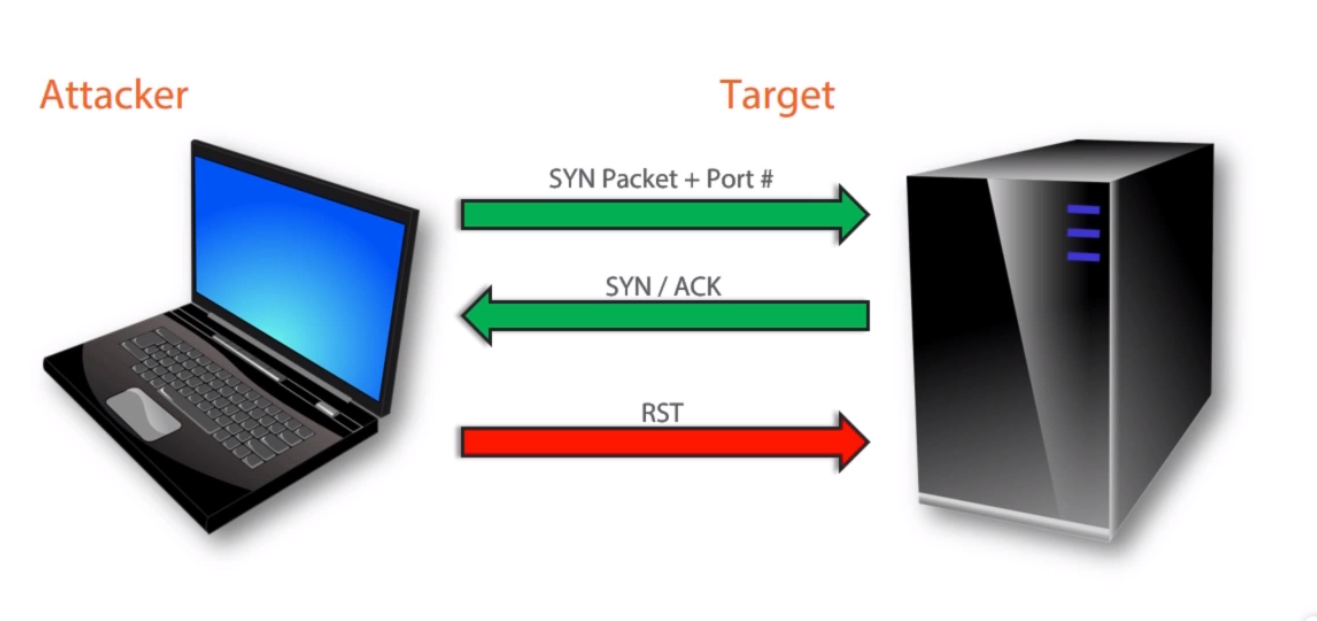
E.g.: 192.168.0.15:80 for HTTP.

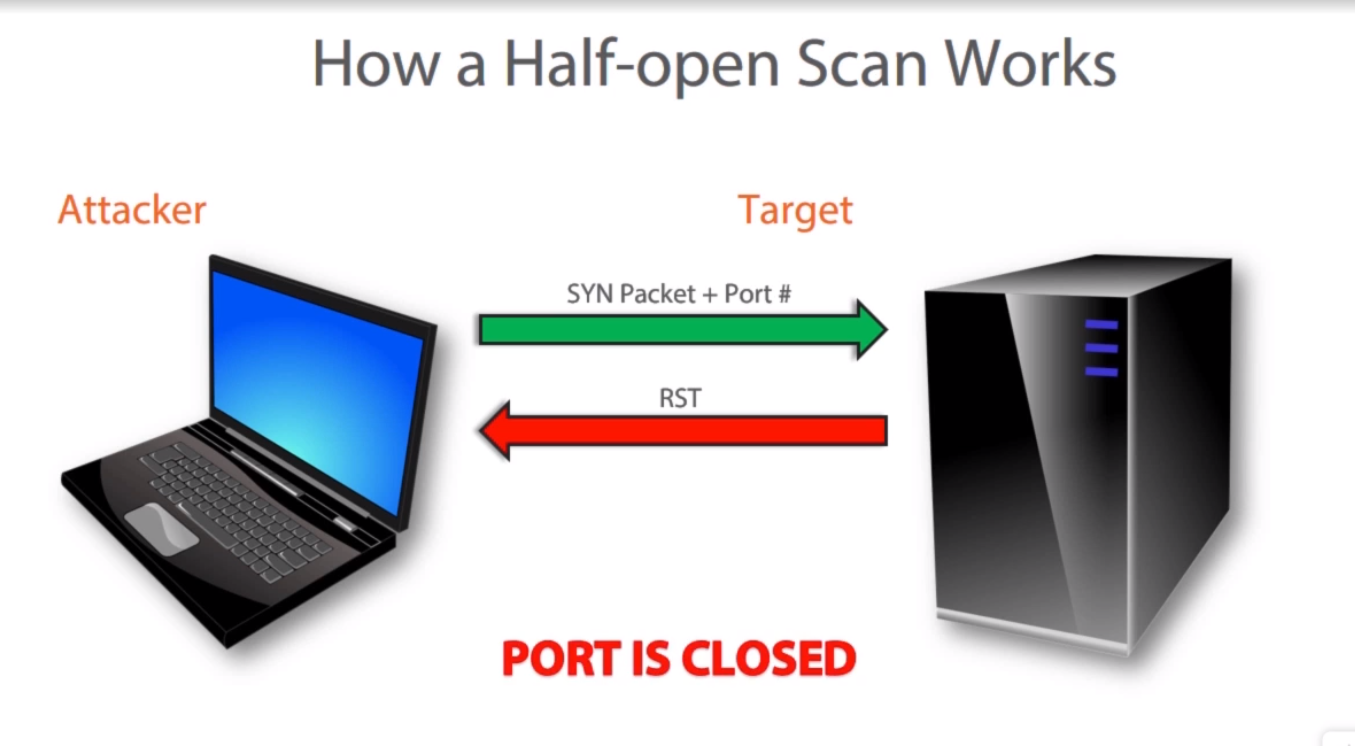
There are around 65,535 ports running on a system.

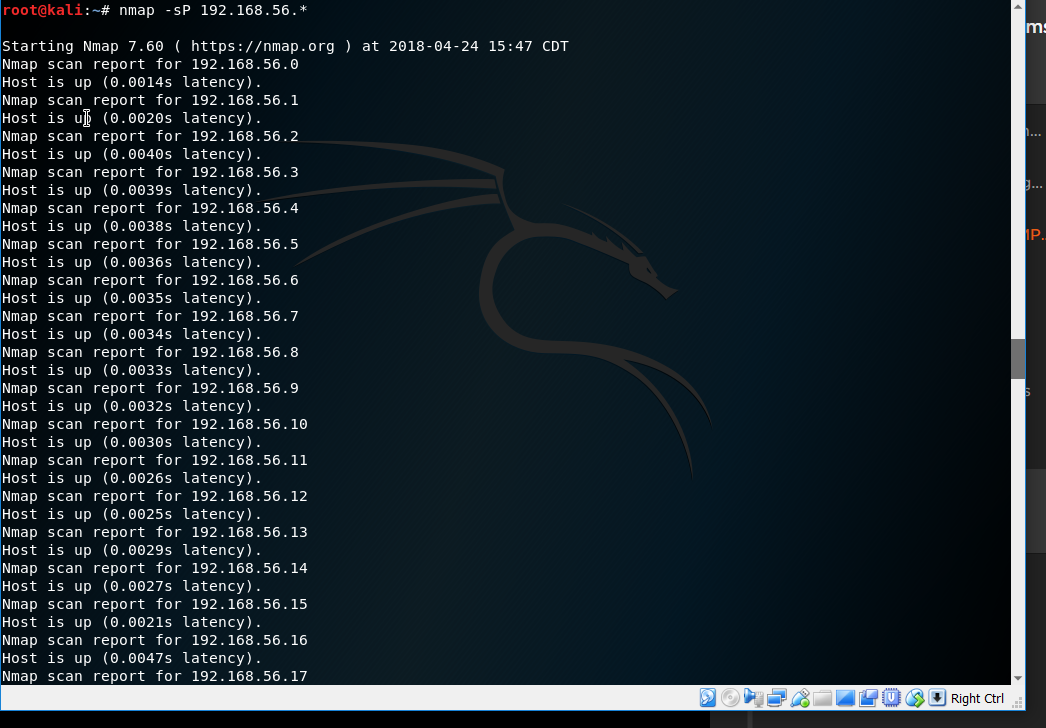
Objectives of scanning:

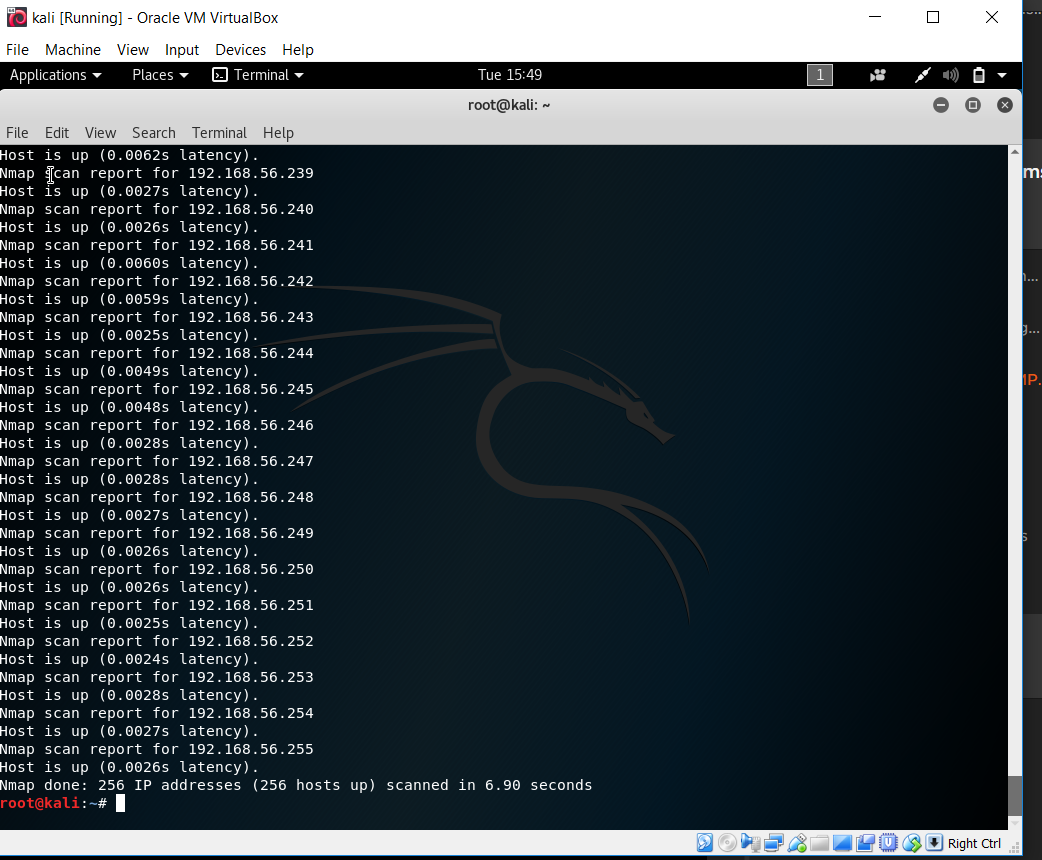
* Identify “Live” hosts
* Gather all IP Addresses
* To check which ports are open/closed.
* Expose OS and architecture
* Check for threats and vulnerabilities.
* Look at the security risks and services

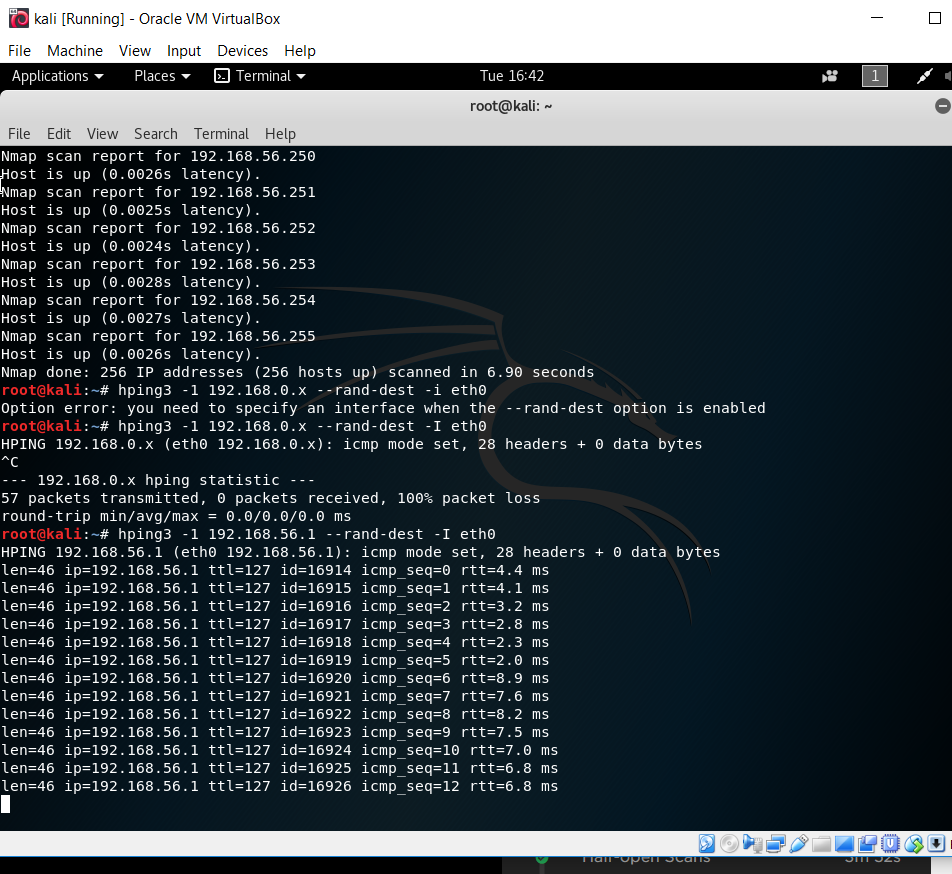
**Half open scan/Stealth scan**

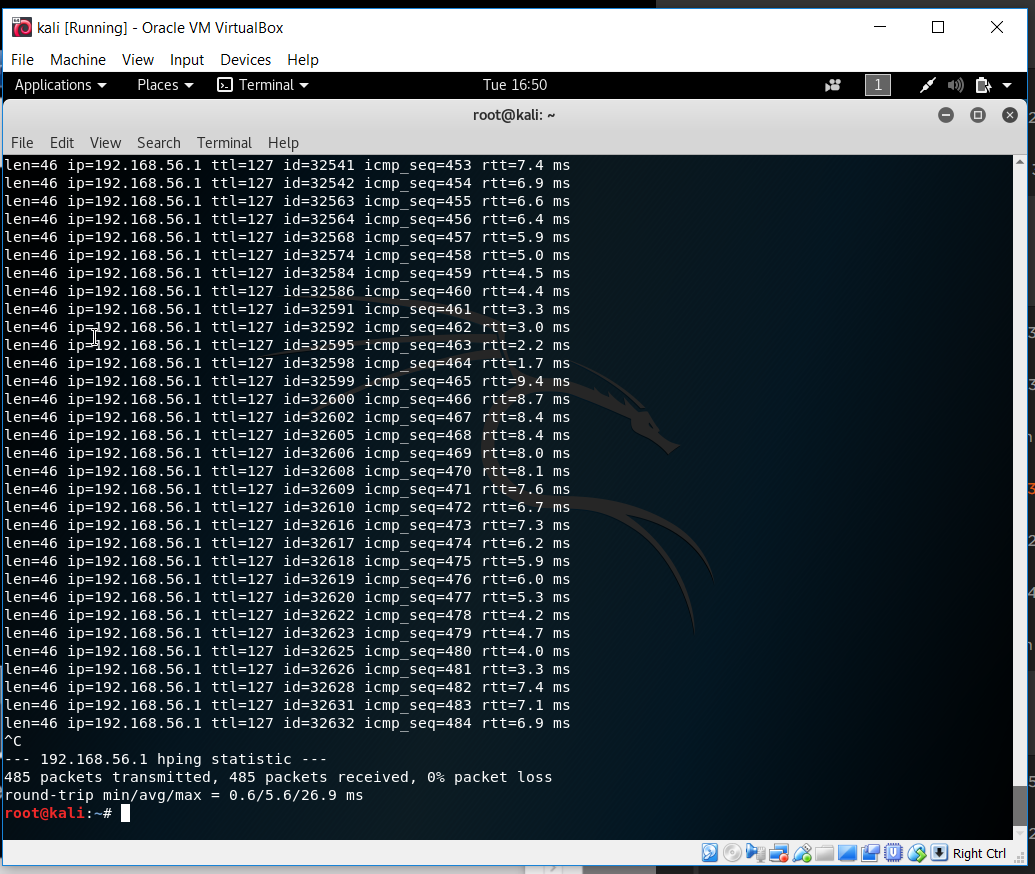


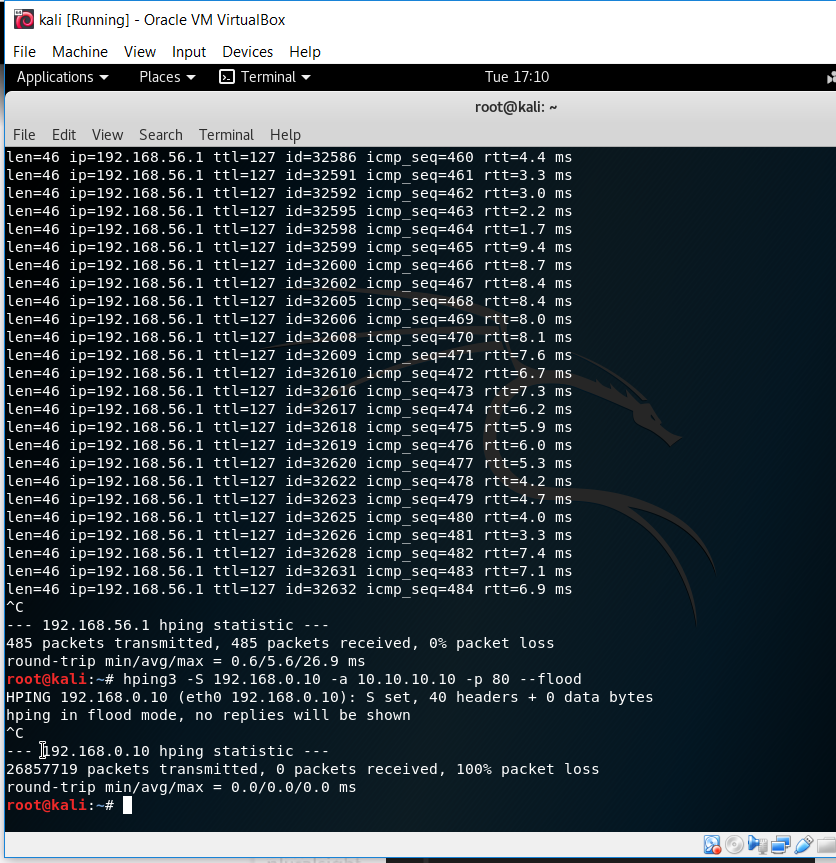












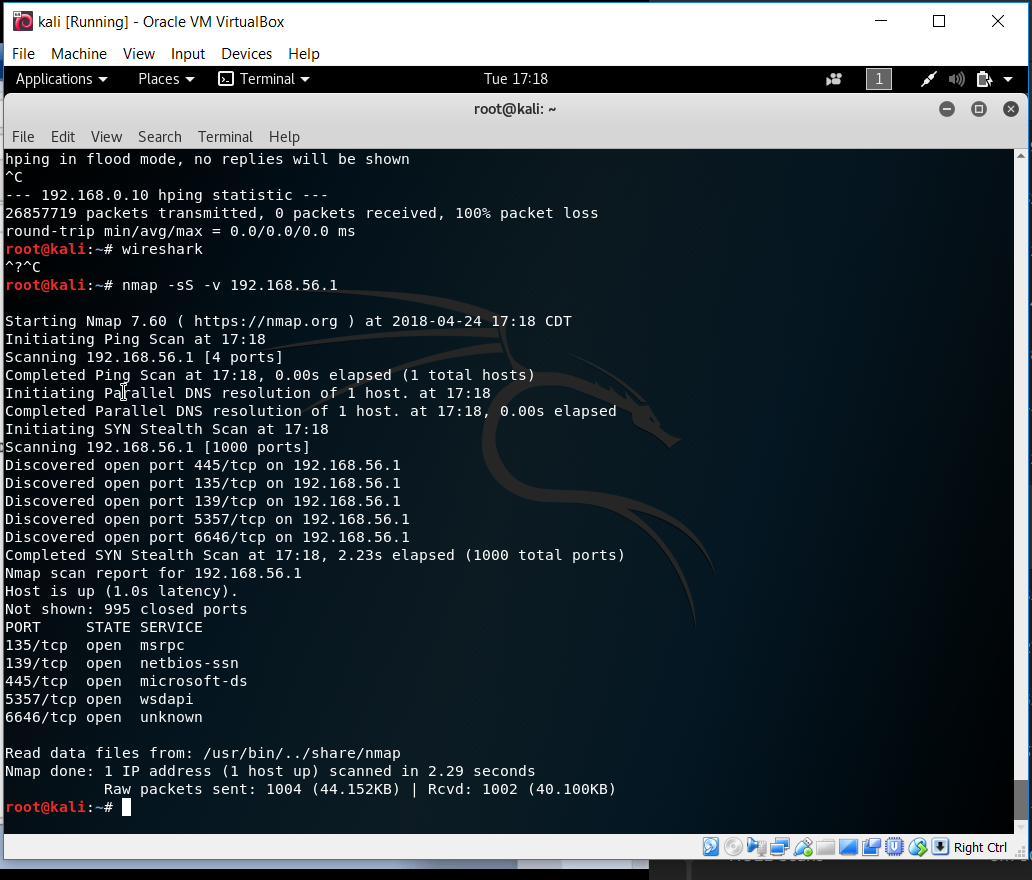
**TCP SYN SCAN ( -sS ) and its implementation**

SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections. SYN scan works against any compliant TCP stack rather than depending on idiosyncrasies of specific platforms as Nmap's FIN/NULL/Xmas, Maimon and idle scans do. It also allows clear, reliable differentiation between the open, closed, and filtered states.

This technique is often referred to as half-open scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and then wait for a response. A SYN/ACK indicates the port is listening (open), while a RST (reset) is indicative of a non-listener. If no response is received after several retransmissions, the port is marked as filtered. The port is also marked filtered if an ICMP unreachable error (type 3, code 0, 1, 2, 3, 9, 10, or 13) is received. The port is also considered open if a SYN packet (without the ACK flag) is received in response. This can be due to an extremely rare TCP feature known as a simultaneous open or split handshake connection

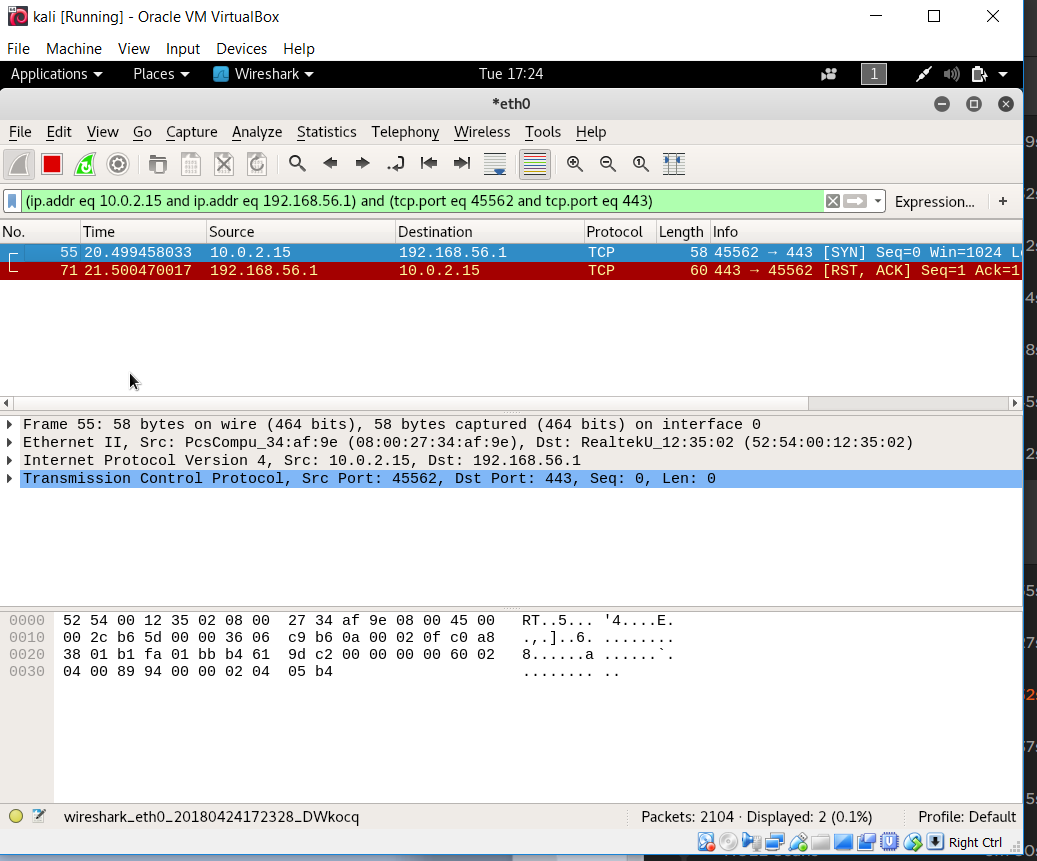
Command used : nmap -sS -v 192.168.56.1

-sS refers to TCP SYN scan type

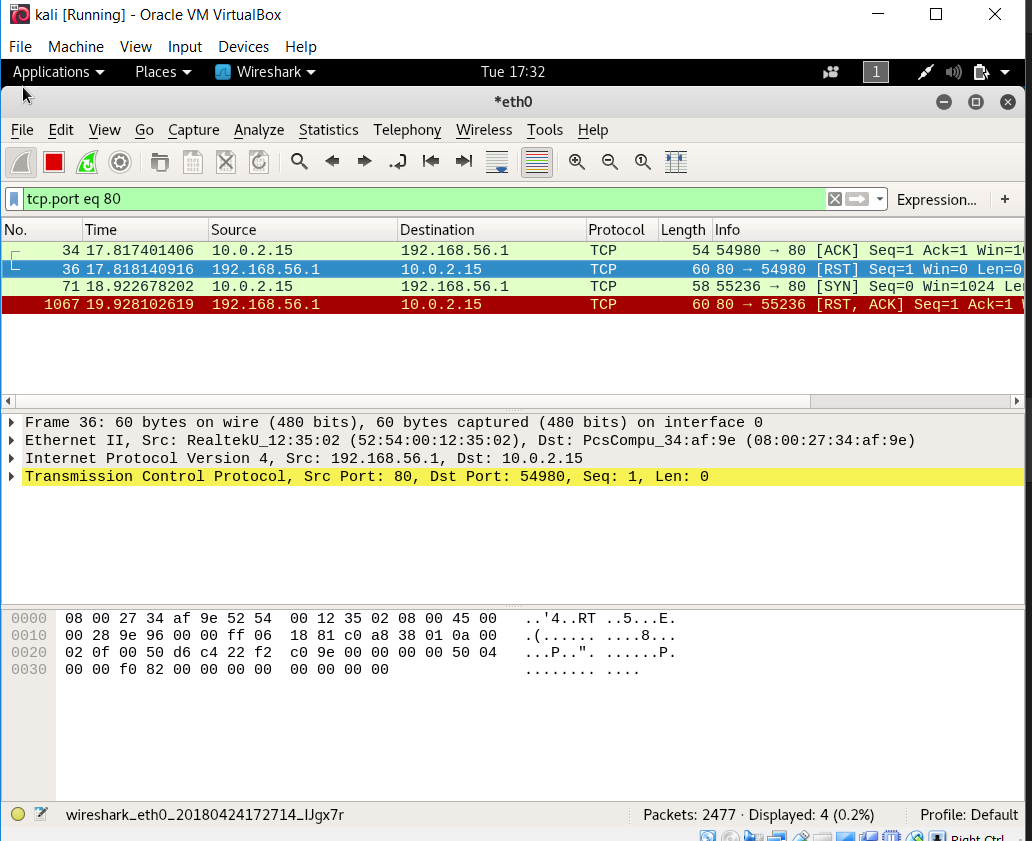


From the above output, we infer that the ports 135, 139, 445, 5357, 6646 are open

Now, open Wireshark to see the traffic. The below image shows that the port 443,45562 or 80 are closed as they have sent an [RST, ACK] which is true according to the output from the nmap TCP SYN scan command.

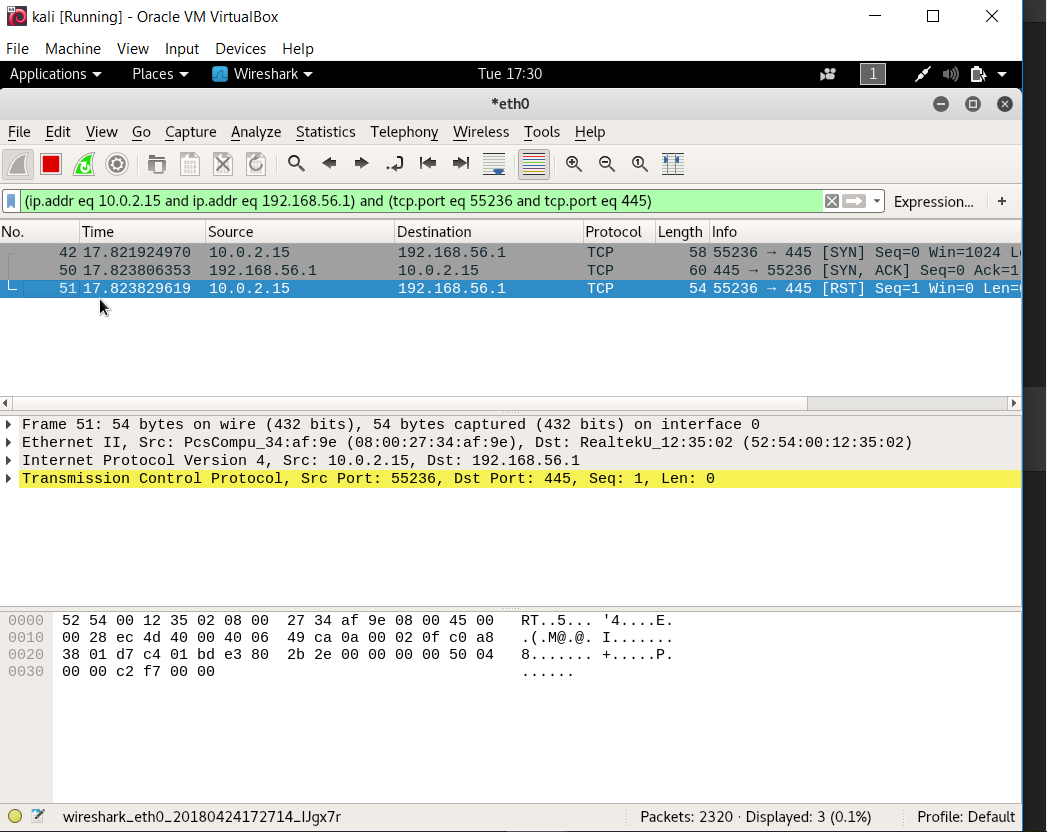


Port 443, 45562 closed



Port 80 closed

Also if we check for anyone of the open ports eg: 445, it is evident that the port is half open since it responded to our SYN with [SYN, ACK] and sends a [RST]



Port 445 is Half Open

**Counter Measures:**

* 1. Configure Firewalls to look for SYN scans
  2. IDS should detect Snort / Nmap
  3. Open only require ports
  4. Filter ICMP messages
  5. Test your own network
  6. To keep firewalls / IDS updated / patched

**Efficient Port Scan Detection Rules (EPSDR)**

Rule 1 alert tcp any any ◊ any any (msg:"FIN Scan"; flags: F; sid: 1000001;)

Rule 2 alert tcp any any ◊ any any (msg:"NULL Scan"; flags: 0;sid : 1000002;)

Rule 3 alert tcp any any ◊ any any (msg:"SYN attack"; flags:S,12;sid : 1000003;)

Rule 4 alert tcp any any ◊ any any (msg:"XMUS attack"; flags:FPU; sid 1000004;)