Module 18
(More Network Discovery)

• At the end of this module, you should know a little bit more about nmap scanning. You should know one way to identify machines that don't respond to ping request, and you should know how nmap classifies ports that it interrogates.
Do Ping Scans Always Work?

• If hosts don't respond to ping, we must find an alternate way of finding them.

• By default, nmap will perform *host discovery*. In addition to ICMP ECHO REQUEST, nmap sends ICMP TIMESTAMP, TCP SYN to port 443 and TCP ACK to port 80.

• To disable host discovery and still do a default network scan, we provide the -Pn parameter to nmap:
  
nmap -Pn 172.16.28.0/24
Demonstrate This Scan

- In my virtual network, I am running Kali and another host as well. The other host will show up because of services it is running.
Some Scan Types

- Different types of scans might be used to identify ports on devices that are offering services:
  - TCP connect scan (SYN, SYN/ACK, ACK) available in nmap if you are not root
  - TCP SYN scan (half-open scanning, stealthy) SYN/ACK response from listening host RST/ACK from non-listening port
  - TCP FIN scan (Unix hosts send RST for closed ports)
  - TCP Xmas Tree (FIN, URG, PUSH – should get back RST for closed ports)
  - TCP Null scan (should send RST for all closed ports)
  - TCP ACK scan (some firewall rules only allow established connections, i.e, those with ACK set)
  - UDP scan (port unreachable response = closed)
Identifying Services With nmap

• By default, nmap scans the 1,000 most popular service ports.
• It identifies ports as being in one of six different states:
  – Open
  – Closed
  – Filtered
  – Unfiltered
  – Open|Filtered
  – Closed|Filtered
Port Classifications

- **Open**
  - Actively accepting TCP connections, UDP datagrams, or SCTP associations
- **Closed**
  - Accessible, but no application is listening on it.
  - May come alive later.
- **Filtered**
  - nmap cannot determine whether open or closed.
- **Unfiltered**
  - ACK scan shows that packets can get through firewall, but no other response is identified.