Ports -

How do you know which ports are open?

Host / server — which ports are open?

What happens when a which ports are closed?

Port 22 - SSH -

what will you do?

To test for open ports?

System - port 80

Accept the connection. ← ↑ Accepting connections

(TCP) SYN - Connection Request

SYN ACK - Connection Accepted

ACK - Connection Established

SYN segment

- SYN ACK

RST -

Port is closed

SYN segment to all the ports

- SYN ACK

Port is open

RST

Port is closed

not used /

Refusing connections.

Tool - nmap - Methodology used by nmap - scans your network / hosts and finds open ports

SYN - nmap - Same method

- Normal / port scan
  - SYN segment
  - SYN -ACK
  - ACK -

Establish a connection on the port

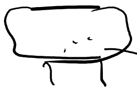
- Stealth scan - open / not

the port

- Stealthscan – open/ not

Secure a port
- close the port
- Prevent any unauthorszed connections.

– SYN Sg
– SYN -ACK } Port is open
– RST Segment – Not connected



– closed/ Not allowing people

- OS fingerprinting

- If not in use, close the port

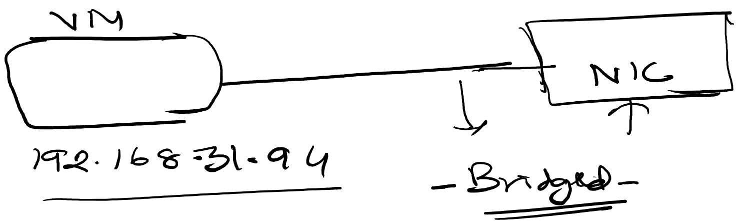
nmap scan – You can determine the OS/

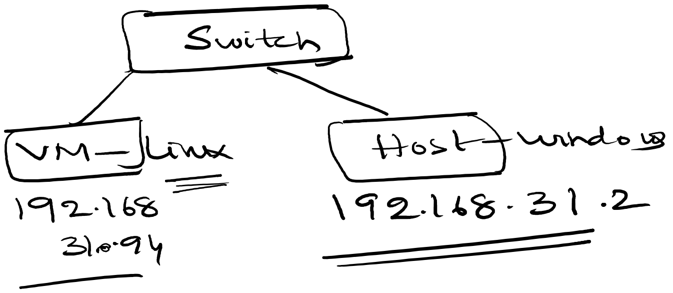
nmap – {To find the OS}

{ 192.168.31.94/24
192.168.31.2/24

Are on the Same Subnet

communicate with each other


VM
NIC
192.168.31.94
– Bridged –


Switch
VM – Linux
192.168
31.94
Host – windows
192.168.31.2