Port scans

TCP 3-way handshake

- TCP header has flags
  - SYN is “Synchronize”, it means the sequence number has a special meaning
  - ACK is “Acknowledge”, it means the acknowledgment number has meaning
  - RST: “I have no record of such a connection”
  - Also, FIN, CWR, ECN, URG, PUSH

TCP 3-way handshake

- SYN: I'd like to ope a connection with you, here's my initi sequence number (ISN)
- SYN/ACK: Okay, I acknowledge your ISN and here's mi
- I ACK your ISN

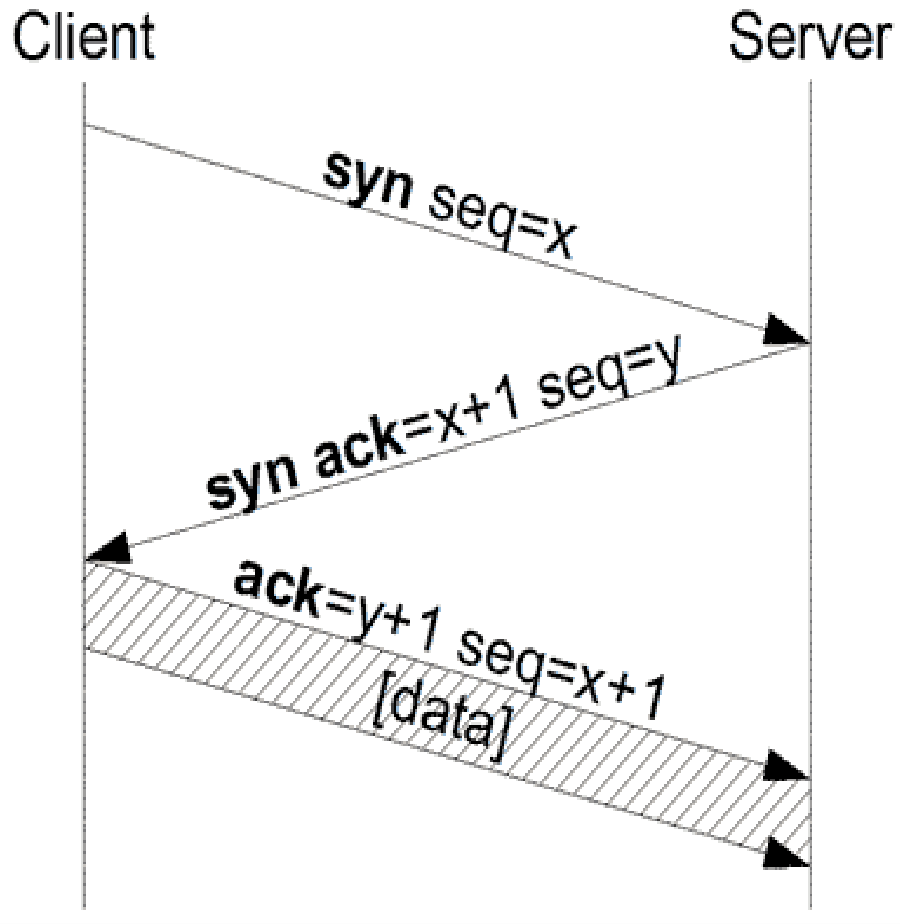


Image from Wikipedia

UDP

- Getting a response is unusual
- No response is common
  - “open | filtered”
- ICMP port unreachable error == closed
  - Type 3, code 3
- Other ICMP errors … filtered

Open port == listening

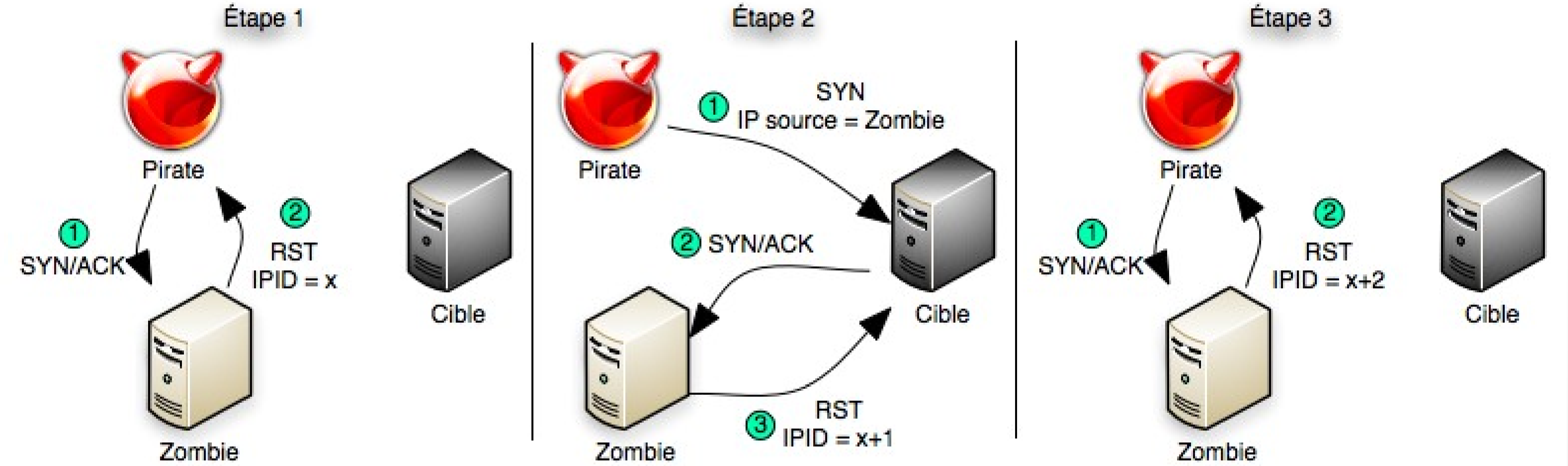
- If you send a SYN packet to port 80 (the HTTP port) on a remote host and that host replies with a SYN/ACK, then we say that port 80 on that machine is “open”
  - In this example, that probably means it's a web server
- If it responds with a RST, we say it's “closed”
- If there is evidence of filtering (no response, ICMP==Internet Control Message Protocol error), we say it's “filtered”

Things nmap can do

- Is a port open? Closed? Filtered?
  - Many ports on one machine is a “vertical scan”
- For a /24 network, which machines are up? Which machines have port 80 open?
  - One port for a range of machines is a “horizontal scan”
- OS and version detection
- Stealth, info about middleboxes, etc.

Idle scan

- Every IP packet sent has an IP identifier
  - In case it gets fragmented along the way
- Old and/or stupid machines use a globally incrementing IPID that is shared state for all destinations



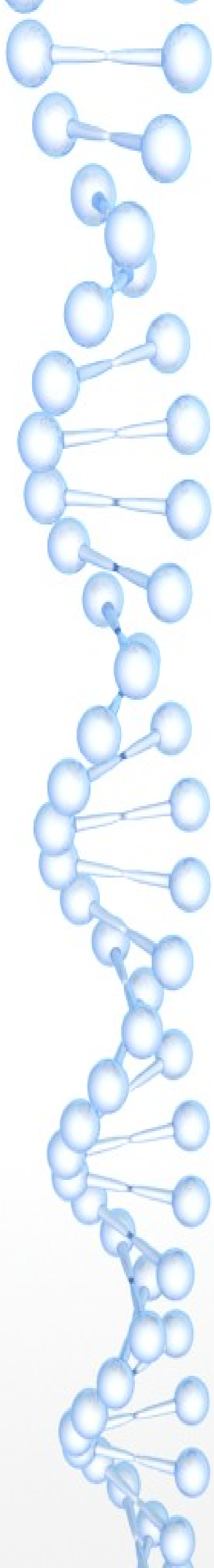
Par Shiningfm — Travail personnel, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=8273541

SYN backlog

- Fixed number of half-open (*i.e.*, SYN-SENT) entries
  - Half is reserved for newer entries
    - And half of remaining half, and so on
- Protects against SYN flood
- (for homework, assume SYN cookies are disabled)

Off-path attacks in layer 4

- If you can guess the initial sequence numbers of a TCP connection, you can hijack it off-path
  - See “Off-Path TCP Exploits...” by Cao *et al.* at USENIX Security 2016 as an example
- There are also off-path threats to privacy
  - See “Counting Packets Sent Between Arbitrary Internet Hosts” by Knockel and Crandall at USENIX FOCI 2014, or Alexander and Crandall PETS 2019



Some hints

- Look at the big picture
- Understand what the TTL is/means
- Physical frame *vs.* packet

Resources

- “man nmap”
- https://nmap.org/book/