Still more networking

UNIX process hierarchy

pstree

pstree -u crandall

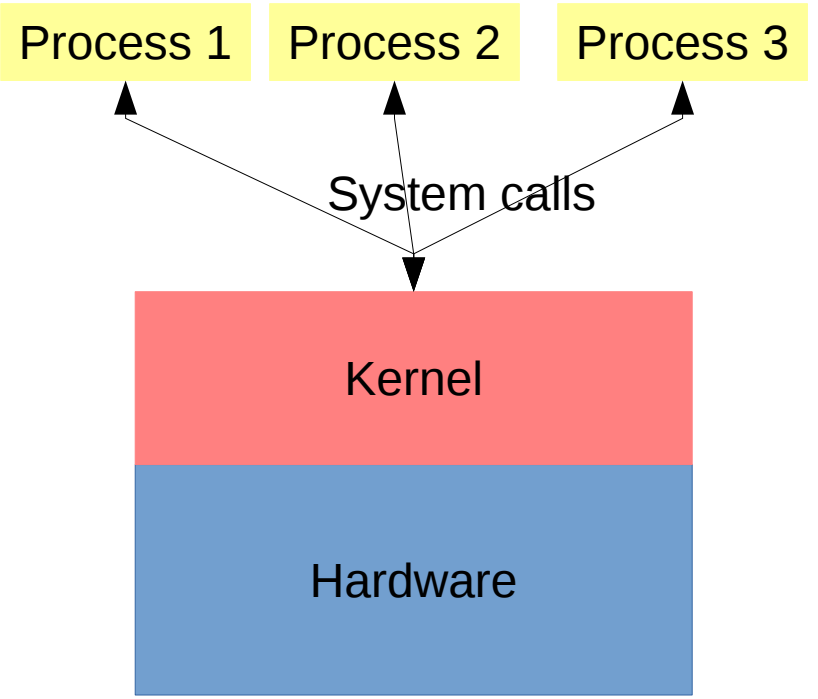
cs /tmp

wget phrack.org

less index.html

strace -f -o bla.txt wget phrack.org

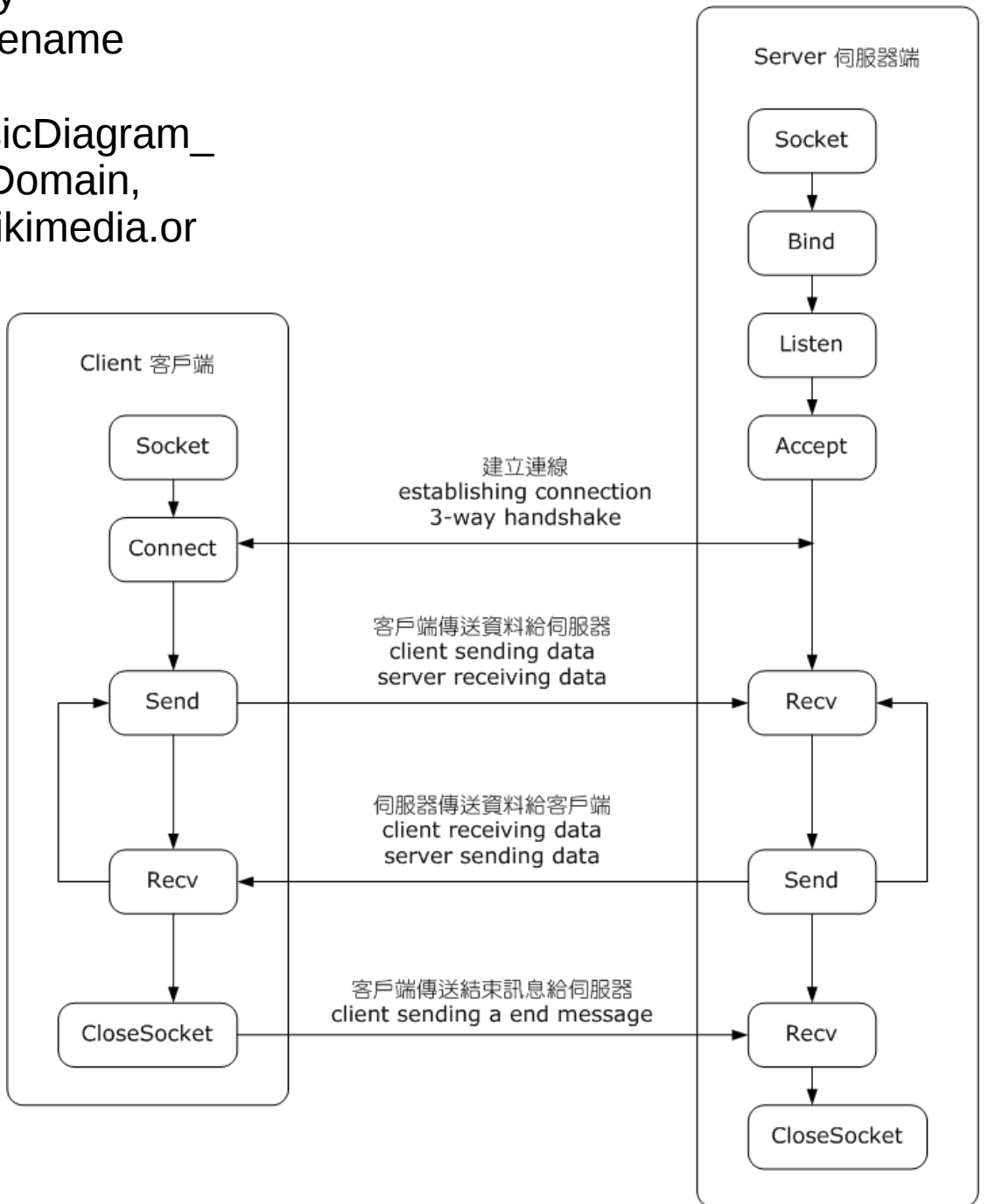
less bla.txt



wget is a web client

- Like your web browser
- httpd (like Apache) is an example of web server
  - Can typically accept connections from multiple clients at the same time
- A network socket = one process on one machine talking to another process on another machine
- The “socket”, “connect”, “listen”, etc. on the next slide are *system calls*

TCP Socket 基本流程圖
TCP Socket flow diagram



By OnionBulb - This PNG image was made by OnionBulb. PNG filename originally is "InternetSocketBasicDiagram_zhtw.png"., Public Domain, https://commons.wikimedia.org/w/index.php?curid=11766896

TCP 3-way handshake (review)

- 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 (review)

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

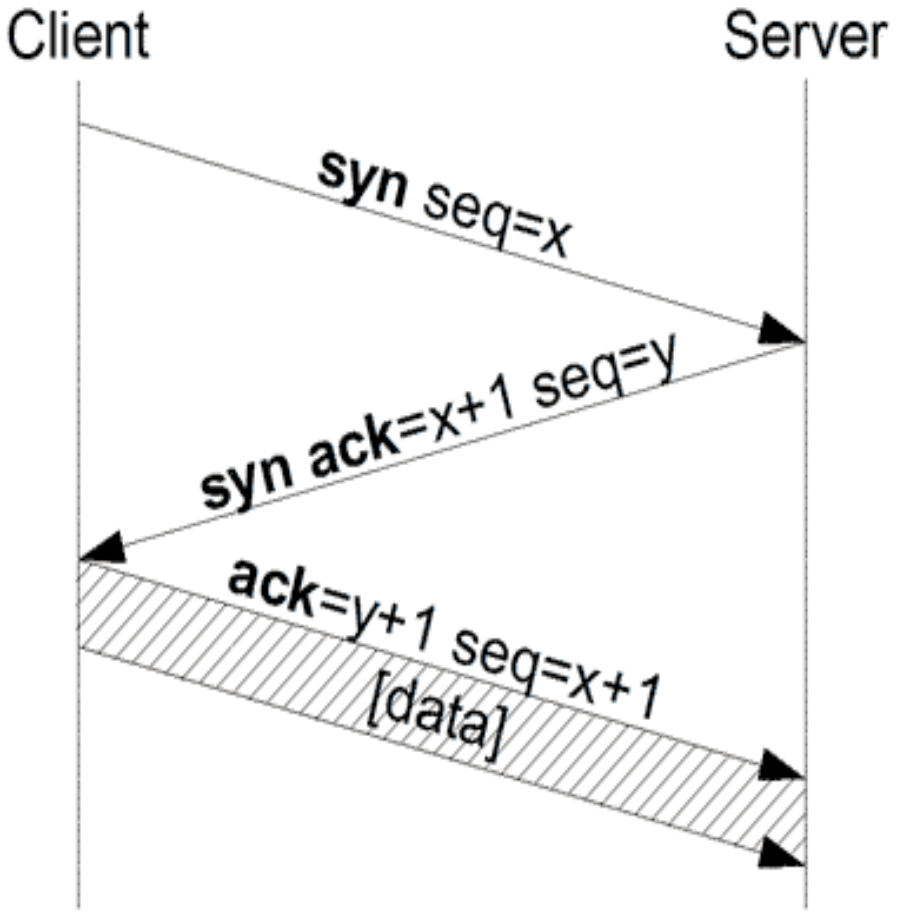


Image from Wikipedia

Open port == listening

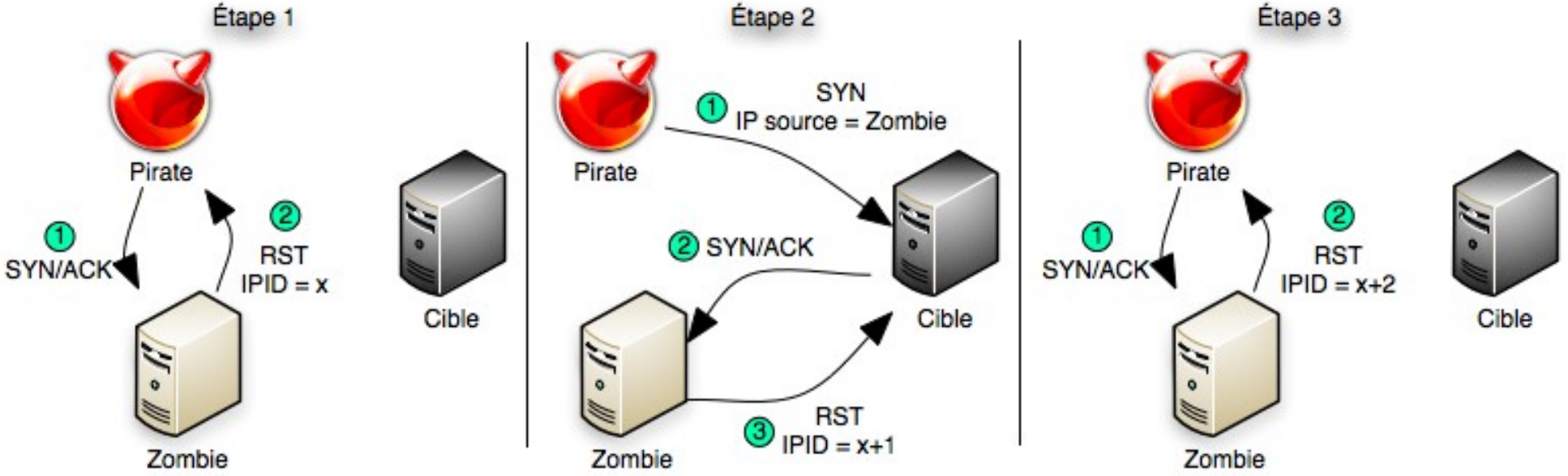
- If you send a SYN packet to port 80 (the HTTP port) on a remote host and that host replies with a SYN/ACK, then we say that port 80 on that machine is “open”
  - In this example, that probably means it's a web server
- If it responds with a RST, we say it's “closed”
- If there is evidence of filtering (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 detection (research on your own)
- 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



Off-path attacks in layer 4

- If you can guess the initial sequence numbers of a TCP connection, you can snipe 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

References

- *NMAP NETWORK SCANNING*, by Gordon “Fyodor” Lyon
- Google “nmap”, “idle scan”, etc.
- *Computer Systems: A Programmer’s Perspective, 3rd Edition*, by Bryant and O’Halloran