① Recall last class: scanning techniques?
Why? which ports are listening & accepting connections

② What can possibly go wrong?

③ Another method: send junk
The idea: if ports are listening, nonsensical packets are ignored, else a RST packet will be sent. See RFC 793 ⇒ no connections are open.

FIN scan (FIN packet)
sudo nmap -sF

prevention via kernel modification

Xmas scan (packet w/ FIN, URG, PUSH)
sudo nmap -sX

Null (packet w/ no flags)
sudo nmap -sN

④ Decoy scan: ① spoofed connections
② sorta hide yo ass
③ must use real IP else SYN flood (whoops)

sudo nmap -D x.y.10.10, x.y.10.11, 10.42

⑤ SYN flood

⑥ How to create spoofed packets
- nmap
- scapy
- hping3

Why?
- Scanning
- Forge IP
- Impersonation
- Not to Hide yo ass to surf the web

Defenses
- Packet filtering @ router level
- ACLs
- Encryption
- Authentication

⑦ TCP Hijacking
- Take control of a connection btwn victim & host
- MUST be on same network as victim
- Guess correct seq/ack #s
- Still REAL
- Defenses: switched network, encryption