

# Host Discovery

~ confidentiality



By default, hosts answer to ICMP echo request messages

➡ An attacker scan an entire network to find IP addresses of active hosts

e.g. **nmap** (does that among other things)

# IP Spoofing

integrity  
availability



- Routers do not validate the source
  - Receiver cannot tell that the source has been spoofed
- ➡ An attacker can generate raw IP packets with custom IP source fields
- e.g. DOS (blackhole) and MITM attacks