

# Preventing scanning attacks (and beyond)

# Preventing host discovery and port-scanning

**Host discovery** uses ICMP ping echo message

- ➔ ICMP can be disabled or reserved to hosts on the same network

**Port Scanning** uses TCP-syn messages

- ➔ TCP connections can be rejected if a source attempts to initiate multiple connections on multiple ports simultaneously
- ➔ **Packet filtering** can prevent these two scanning techniques