Portscanner

Aim of project

- Implement a portscanner in C
- Various scan methods e.g. TCP connect scan, TCP SYN scan …
- Console program like nmap

Implemented Scan Methods

- TCP connect scan
- TCP syn scan
- NULL scan
- XMAS scan
- FIN scan
- Maimon scan

Implementation

- SOCK_STREAM socket (TCP socket)
- Use connect() function to try to establish a connection with the target machine
- Check return value of connect() function
- Return value 0 = port is open, else port closed

TCP connect scan

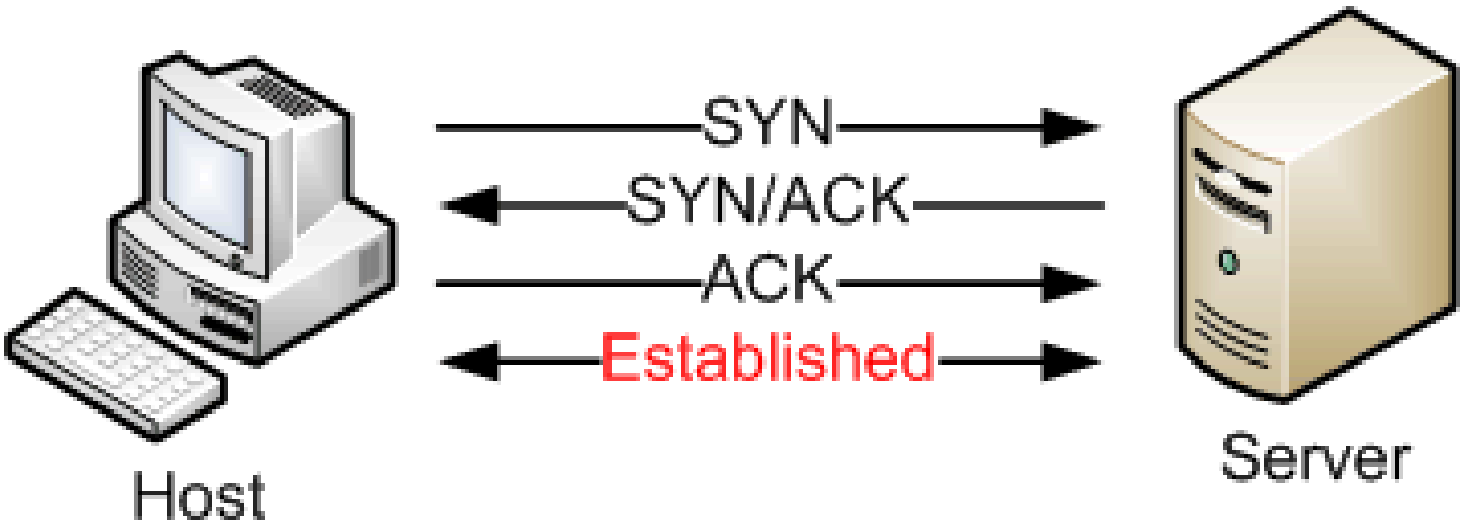
- Simple approach
- Use system call connect() to try to establish a connection
- If connection successful port is open
- Else port is closed

Implementation

- SOCK_STREAM socket (TCP socket)
- Use connect() function to try to establish a connection with the target machine
- Check return value of connect() function
- Return value 0 = port is open, else port closed

TCP Handshake

TCP Three-Step Handshake



Syn scan

Raw socket

Implementation