CE443 - Computer Networks
TA Session
Today's Topics

1. Introduction to `socat`
2. Introduction to `ssh`
3. Sharing sockets among processes
What Is?
+ A utility that establishes two bidirectional byte streams and transfers data between them.
+ netcat++
  - Streams can be constructed from a large set of different types.
  - Lots of address options may be applied to the streams.

Arguments
- 4
  Use IP version 4 in case that the addresses do not implicitly or explicitly specify a version.

- 6
  Use IP version 6 in case that the addresses do not implicitly or explicitly specify a version.

TCP4-LISTEN: <port>
Listens on [TCP service] and accepts a TCP/IP connection. Only supports IPv4 protocol.

TCP: <host> : <port>
Connects to <port> on <host> using TCP/IP version 4 or 6.

SOCKS4: <socks-server> : <host> : <port>
Connects via <socks-server> to <host> on <port>.

PROXY: <proxy> : <hostname> : <port>
Connects to an HTTP proxy server on port 8080 using TCP/IP version 4 or 6 and sends a CONNECT request for hostname:port.

UNIX-CONNECT: <filename>
Connects to <filename> assuming it is a UNIX domain socket.

UNIX-LISTEN: <filename>
Listens on <filename> using a UNIX domain stream socket and accepts a connection.
What Is?

ssh (SSH client) is a program for logging into a remote machine and for executing commands on a remote machine.

Options

-D <port>
+ Specifies a local “dynamic” application-level port forwarding.
+ ssh will act as a SOCKS server.

-L <port>::<host>::<hostport>
Specifications that the given port on the local (client) host is to be forwarded to the given host and port on the remote side.

-R <port>::<host>::<hostport>
Specifications that the given port on the remote (server) host is to be forwarded to the given host and port on the local side.

Public Key Authentication
+ The client uses his private key, ~/.ssh/id_dsa or ~/.ssh/id_rsa to sign the session identifier and sends the result to the server.
+ The server checks whether the matching public key is listed in ~/.ssh/authorized_keys and grants access if both the key is found and the signature is correct.

ssh Config File
+ User’s configuration file: ~/.ssh/config
+ System-wide configuration file: /etc/ssh/ssh_config

sshfs
+ Secure SHell FileSystem
+ File system capable of operating on files on a remote computer using just a secure shell login on the remote computer.

X Forwarding
+ Running graphical application over SSH

Screen
+ Keep Your SSH Session Running when You Disconnect.
Sharing Sockets

Method 1

+ If a process forks, its child will inherit all file descriptors. So both processes can accept on one socket.
  - If the fork is performed after accepting, the child can use the established socket.
  - If the fork is performed before accept(), then a pool of processes can be created.
+ Using REUSE_PORT option can replace these efforts too.

Method 2

+ Using the dup2 function, it is possible to copy a file descriptor.
  - The dup2() system call creates a copy of the file descriptor.
+ For example:
  - Close file descriptor 0 and 1 (for stdin and stdout) and then dup2 read/write streams of a socket on 0 and 1 fds.
  Then using cin/cout you can communicate with the socket.