学到许多~

```c
#include <stdio.h>
#include <unistd.h>
#include <sys/types.h>
#include <stdlib.h>
#include <sys/wait.h>
#include <arpa/inet.h>
#include <sys/socket.h>
#include <netinet/in.h>

int main(){
    char *argv[101]={"input"};
    char * envp[]={0,NULL};
    for(int i=1;i<100;i++){
        argv[i]="a";
    }
    //stage1
    argv['A']="\x00";
    argv['B']="\x20\x0a\x0d";
    argv['C']="55555";

    //stage2
    int pid = fork();
    if(pid==0){
        int fd_0[2];
        int fd_2[2];
        pipe(fd_0);
        pipe(fd_2);
        dup2(fd_0[0],0);
        dup2(fd_2[0],2);
        write(fd_0[1],"\x00\x0a\x00\xff",4);
        write(fd_2[1],"\x00\x0a\x02\xff",4);

        //stage3
        envp[0]="\xde\xad\xbe\xef=\xca\xfe\xba\xbe";

        //stage4
        FILE * fp = fopen("\x0a","w");
        fwrite("\x00\x00\x00\x00",4,1,fp);
        fclose(fp);

        execve("input",argv,envp);
    }else{
        // network
        int sd = socket(AF_INET, SOCK_STREAM, 0);
        if(sd == -1) {
            perror("socket Error");
            exit(-1);
        }
        struct sockaddr_in saddr;
        saddr.sin_family = AF_INET;
        saddr.sin_addr.s_addr = INADDR_ANY;
```

```
        saddr.sin_port = htons(atoi(argv['C']));

        sleep(1);
        int ret = connect(sd,
                (struct sockaddr *) &saddr,
                (socklen_t)sizeof(struct sockaddr_in));

        if (ret == -1) {
            perror("Connect error");
            exit(-1);
        }

        send(sd, "\xde\xad\xbe\xef", 4, 0);
        close(sd);

        wait(&ret);
    }

    //printf("hello\n");
    return 0;
}
```