

Forum:[Hack Forums](#)

Thread: [Port Enumeration](#)

Clumsy - October 7, 2023, 11:01 pm

How This Script Works

This script is a simple port scanner written in C. It enumerates active ports on the machine by attempting to bind to each port from 1 to 65535. Here's how it works:

The necessary header files are included for standard input/output, socket programming, and error handling.

The main function is defined, which is the entry point of the program.

Variables are declared, including sockfd for the socket file descriptor, portno for the port number, and serv_addr for the server address structure.

An error message is defined for the case when binding to a port fails due to the address already being in use.

The program prints a message indicating that it is enumerating active ports on the machine.

A loop is started to iterate through port numbers from 1 to 65535.

Inside the loop, a socket is created using the socket function. If the socket creation fails, an error message is printed, and the program exits.

The server address structure serv_addr is set up with the appropriate values: the address family is set to AF_INET, the IP address is set to INADDR_ANY (which means any available local IP address), and the port number is set to the current iteration value.

The bind function is called to bind the socket to the server address. If the binding fails, it checks if the error message matches "Address already in use". If it does, it means the port is active, and a message is printed indicating that the port is active.

The socket is closed to release the resources.

The loop continues until all port numbers have been checked.

Finally, a message is printed to indicate that the port enumeration is completed.

The program returns 0 to indicate successful execution.

This script can be used to identify active ports on a machine, which can be helpful for network scanning and security testing purposes.

```
Code #include <stdio.h>
#include <stdlib.h>
```

```

#include <unistd.h>
#include <string.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <errno.h>

int main() {
    int sockfd, portno;
    struct sockaddr_in serv_addr;
    char error_message[] = "Error on binding: Address already in use\n";

    printf("lulz: Enumerating active ports on the machine:\n");

    for (portno = 1; portno <= 65535; portno++) {
        sockfd = socket(AF_INET, SOCK_STREAM, 0);
        if (sockfd < 0) {
            perror("Error opening socket");
            exit(1);
        }

        serv_addr.sin_family = AF_INET;
        serv_addr.sin_addr.s_addr = INADDR_ANY;
        serv_addr.sin_port = htons(portno);

        if (bind(sockfd, (struct sockaddr *) &serv_addr, sizeof(serv_addr)) < 0) {
            if (strcmp(strerror(errno), "Address already in use") == 0) {
                printf("Port %d is active.\n", portno);
            }
        }

        close(sockfd);
    }

    printf("lulz: Port enumeration completed.\n");
    return 0;
}

```