SHRUTHI KATAPALLY
User Name: shrukata

Project 4: Port Scanner

Introduction

Port Scanners can be used to probe remote hosts to open ports. This project is implemented with IPV4 support. This project is implemented in C language. This portscanner performs TCP SYN (Half-open), TCP NULL, FIN and Xmas scans. These types of scans are available to only privileged users.

Implementation details

The code has been implemented in PortScanner.c

PortScanner.c

The code has been implemented in PortScanner.c

get_task: This is where we calculate what tasks to do and we here divide it basing on the ipaddress, ports and scans which are to be done.
parseargs: Parsing the command line options
start_work:
classify_porttype: We here classify the port type as filtered,unfiltered,open,closed,open|filtered.

EXECUTION :
gcc portScanner.c -lpcap –lm
COMPLIATION :
Example :$ sudo nice ./a.out --ports 6-9 --ip 129.79.246.89 --scan SYN NULL

Resources

- http://sock-raw.org/papers/syn_scanner
- http://www.tcpdump.org/pcap.htm
- https://github.com/
- http://www.binarytides.com
- http://beej.us/guide/bgnet/
- http://en.wikipedia.org/wiki/Transmission_Control_Protocol#TCP_checksum_for_IPv4