SHRUTHI KATAPALLY
Username: shrukata

PROJECT-4 PORT SCANNER

INTRODUCTION:

This project performs scans on ports on a destination system. It performs scans as SYN, NULL, FIN, XMAS and ACK. It after scanning the ports, depending the response will classify them as Open, Filtered, UnFiltered, Open | Filtered.

This project submission has the following things:

- portscanner.c
- Makefile
- Readme

1) portscanner.c :

Options :

1) --help <display options>
2) --ports <ports to scan>
3) --ip <IP address to scan>
4) --prefix <IP prefix to scan>
5) --file <file name containing IP addresses to scan>
6) --scan <one or more scans>

It has parse_args() , which will give the command line options and will populate the ports, scans,ip address and all the required data. We then create the tasks which are needed to be done. Basing on the ip address and port and scan type.

It after performing various scans will check the responses and will find the port classification and will return to the command line.

2) Makefile:

A Makefile is written for the ease of compilation.The file portscanner.c is complied and an object file portscanner.o is generated using this makefile. It is also used for removing the previously generated object file.

3) Readme:

Readme gives the description of the code for the program portscanner.c and the compilation procedure to execute the program. It also contains the output is analyzation.

References and Credits:

Books:

1) http://www.tcpdump.org/pcap.htm
2) http://www.beej.us/guide/bgnet/
3) https://www.wireshark.org/
4) Reference for IPv4 is RFC 791. Reference for Ethernet frame format is: IEEE standard 802.3. http://standards.ieee.org/findstds/standard/802.3-2012.html. ICMP protocol is defined in: RFC 792

5) http://sock-raw.org/papers/syn_scanner

6) http://en.wikipedia.org/wiki/Transmission_Control_Protocol#TCP_checksum_for_IPv4