SHRUTHI KATAPALLY

Project -4

Port Scanner - Roadmap

I’m going to implement Port Scanner the following phases:

Phase 1: Parsing the IP file –Milestone 1

In this phase all the command line arguments are parsed and IP file (which has IP addresses) is read and printed on the command prompt. Reading the IP prefixes to a list of individual IP addresses and printing on the command prompt is also done.

Phase 2: TCP Scan

a) SYN scan :
b) NULL,FIN and Xmas scans
c) ACK scan

Phase 3: Multithreading

Sequence of Steps:

- The ports which are given in the command line are read and stored in a structure.
- Now the tasks are divided such that each task has a ip address, port and a scan type from the arguments we passed while execution.
- If we want to Speed up the process we can create multi threads using the option –speedup.
- We use the wire tap project-3 to capture the destination and source ports and data required such as icmp etc.
- Next, For the TCP Scans: a raw socket is created and flags like SYN,NULL,FIN,XMAS are set according to the requirement and send to the server.
- We use signals to mention the time out for the replies.
- We check the ports to be classified as open | filtered | Unfiltered | Closed | open/filtered-infering the target status .