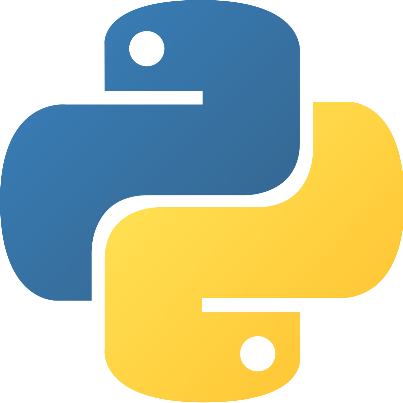
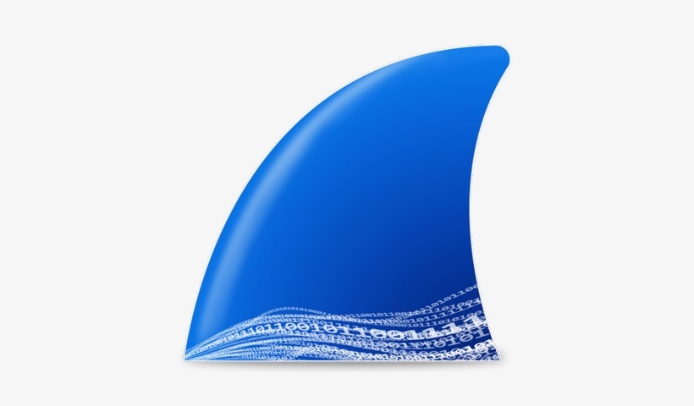
COMPUTER NETWORKS INDUSTRY PROBLEM 1

REPORT

WEB SERVER MONITORING TECHNIQUES :

FORMULATED BY:

DIVIJA PES1UG20CS134

DHATHRI PES1UG20CS141

GAURAV PES1UG20CS150

1. Technique to monitor TCP SYN requests to the web server with wireshark output.

>>WE CREATED A SIMPLE SERVER PROGRAM USING SOCKET PROGRAMMING.

>>ASSOCIATED A SIMPLE HTML FILE,TO CONNECT TO LOCALHOST USING PORT 80

>>IN THE WIRESHARK,WE CHECK THE PACKET LIST WINDOW AND APPLY FILTERS.

1. Technique to monitor TCP reset connections sent to and from the Web Server with wireshark output.

>>WE AGAIN APPLY NECESSARY FILTERS TO CHECK FOR TCP PACKETS WITH RESET CONNECTIONS.

1. Technique to monitor established open connections on a Web Server with netstat output

>>WE USE NETSTAT CALLS SUCH AS

netstat -a

🡪lists all open TCP ports

netstat -s

🡪displays the port statistics

1. Technique to monitor TCP half open connections on the Web Server with netstat output

>>WE USE A NMAP CALL

sudo nmap -sS <ip address>

🡪it displays only half open connections without the three way handshake

1. Technique to monitor requests to a specific application on the Web server with wireshark output

>>WE PING THE IP ADDRESS AND CHOOSE THE LOOPBACK INTERFACE WHILE STARTING THE WIRESHARK PACKET CAPTURE.

In case of windows, it is Adapter for loopback capture.

In case of ubuntu,it is lo interface.

1. Technique to monitor HTTP GET requests to the web server with wireshark output

>> wireshark ->http.request.method==GET

1. Technique to monitor server bandwidth with netstat output

>>nload

🡪a commandline tool that allows users to monitor the incoming and outgoing traffic separately..

nload

>>Iptraf

🡪 is an interactive and colorful IP Lan monitor. It shows individual connections and the amount of data flowing between the hosts.

sudo iptraf-ng

>>nethogs

🡪 reports the PID, user and the path of the program.

sudo nethogs

>>Slurm

🡪  network load monitor that shows device statistics along with an ascii graph. It supports 3 different styles of graphs each of which can be activated using the c, s and l keys.

slurm -s -I <interface>

>>Speedometer

🡪 draws out good looking graphs of incoming and outgoing traffic through a given interface.

speedometer -r <interface > -t <interface>

>>netload

🡪 The netload command just displays a small report on the current traffic load, and the total number of bytes transferred since the program start.

netload <interface>

8.Technique to monitor the port status of a Web Server with nmap output

>>We have written a python code and incorporated nmap with it to give the port status.