Graphical Traffic Analyzer for TcpDump: Documentation
prepared by Rob Haining

1) Installation
   a) Requirements: PHP, MySQL, Web Server, tcpdump, JpGraph
      i) Tested on: PHP 4.3.5, MySQL 3.23.49, Apache 1.3.23, tcpdump 3.6, JpGraph 1.4, Redhat 7
         (1) PHP: http://www.php.com/
         (2) MySQL: http://www.mysql.com/
         (3) Apache: http://www.apache.org/
         (4) Tcpdump: http://www.tcpdump.com/
         (5) JpGraph: http://www.aditus.nu/jpgraph/
         (6) Redhat: http://www.redhat.com/
      ii) Will need Root access for running TcpDump
      iii) Will need to have ability to create a table and grant permissions in MySQL
   b) To Install
      i) Create MySQL table: mysql < mysql_create_table –user=USER –password=PW
         (1) Where USER/PW needs to be replaced with someone who has permissions to create a table and grant permissions on it
      ii) Copy files from ./web/ to your webpage directory [Note: You might want to restrict access to this directory, since sensitive data about traffic through your server will be otherwise publicly displayed.]
      iii) Add the following to your crontab:
         (1) MAILTO=“”
         (2) * * * * * /usr/local/bin/php /var/www/html/incoming_bar.php
         (3) * * * * * /usr/local/bin/php /var/www/html/outgoing_bar.php
         (4) * * * * * /usr/local/bin/php /var/www/html/background_src_bar.php
         (5) * * * * * /usr/local/bin/php /var/www/html/background_dst_bar.php
         (6) * * * * * /usr/local/bin/php /var/www/html/total_pkts.php
   c) To run initially,
      i) ./myTcpdump.php&

2) Basic Concepts of Functionality
   a) There are essentially two components to this system. The first runs tcpdump and inserts its parsed output into a database. As it does this, data that is older than 24 hours is automatically deleted, so as to always have a 24-hour window of traffic that we can analyze.
   b) The second component takes data from this database and displays it in various graphical forms. The index page displays 5 graphs: a linear graph of total traffic over time, a bar graph that displays incoming traffic per port, a bar graph that displays outgoing traffic per port, a bar graph that displays background traffic per source port, and a bar graph that displays background traffic per destination port.[1] From each bar graph, there is the functionality to view a linear graph of traffic over time for each specific port. In this graph, each line will represent a different IP address; additionally, there is a line that represents total traffic on this port. From each of these graphs, the user has the ability to

[1] By “background traffic,” I mean traffic that neither originated from nor was being sent to the current machine.

view a linear graph of traffic over time for a specified port & IP address.

3) Details of Files and what they do
   a) create_mysql_table
      i) Creates a table called “archive” in database “tcpdump” with fields:
         (1) Date
         (2) Time
         (3) Minutes since Unix Epoch
         (4) Protocol
         (5) Source IP
         (6) Source Port
         (7) Destination IP
         (8) Destination Port
   b) myTcpdump.php
      i) Runs tcpdump
      ii) After 60 seconds, kills tcpdump
      iii) Executes dumpToDB.php
      iv) Loops the above 3 steps infinitely
   c) dumpToDB.php
      i) Deletes data from MySQL DB that is older than 24 hours
      ii) Parses through tcpdump output
      iii) Inserts into DB for each packet that is TCP, UDP, or ICMP
         (1) Date, Time, Minutes since Unix Epoch, Protocol, Source IP, Destination IP
         (2) If TCP/UDP, also enters Source Port & Destination Port
   d) Web: index.php
      i) Displays Linear Graph of Total Packets over Time
      ii) Displays Bar Graph of Incoming Packets over Last 24 Hours
      iii) Displays Bar Graph of Outgoing Packets over Last 24 Hours
      iv) Ability to expand on any Port: executes mult_ip_page.php
   e) Web: outgoing_bar.php
      i) Creates Bar Graph of Outgoing Packets over Last 24 Hours, bars are ports
      ii) Ports greater than 1024 are grouped together
   f) Web: incoming_bar.php
      i) Creates Bar Graph of Incoming Packets over Last 24 Hours, bars are ports
      ii) Ports greater than 1024 are grouped together
   g) Web: background_dst_bar.php
      i) Creates Bar Graph of Background Traffic over the Last 24 Hours per destination port
      ii) Ports greater than 1024 are grouped together
   h) Web: background_src_bar.php
      i) Creates Bar Graph of Background Traffic over the Last 24 Hours per source port
      ii) Ports greater than 1024 are grouped together
   i) Web: total_pkts.php
      i) Creates Linear Graph of Total Traffic over Last 24 Hours
   j) Web: mult_ip_page.php
      i) Displays image rendered from mult_ip.php
      ii) Allows ability to expand on specific IP/port over time: single_ip_page.php

k) Web: mult_ip.php
    i) Outputs a Linear Graph of packets per IP over time for a specific port
l) Web: single_ip_page.php
    i) Displays image rendered from from single_ip.php
m) Web: single_ip.php
    i) Outputs a Linear Graph of packets over time for a specific port & ip

4) How to Introduce New Graphs
    a) Given a proficiency in PHP & MySQL, it should be fairly intuitive to create new graphs from this database after studying the graphs already presented here.