Activity Viewer: A Tool for Monitoring Network Host Activities

Diana Paterson, Teryl Taylor, Joel Glanfield, Christopher Smith, Carrie Gates[†],
Stephen Brooks, and John McHugh[‡]
Dalhousie University, Halifax, NS, Canada, CA Labs[†] New York, and
University of North Carolina[‡] Chapel Hill, NC

The activity viewer is an interactive visualization tool designed to focus an analyst's attention on changes in and/or differences in temporal activities within an individual host or among a small group of hosts. The hosts could represent a subnet within a larger network or a group of unrelated hosts which the analyst is monitoring.

The visualization displays host activity as a function of time using a small selection of colours to capture a limited number of possible categories used to partition the activity. The nature of the represented activity is arbitrary. It may be quantitatively or qualitatively based and capture complex or simple concepts. The activities of individual hosts are plotted against time in a simple two dimensional grid. Hosts are listed down the vertical axis and time across the horizontal axis. For the time periods in which activity occurs, for a given host, the corresponding square is filled with a colour that indicates the nature of the activity. This layout captures aspects of host activity as a time series of colour coded blocks, with one series per host. This visual organization of the data, allows for temporal variability of host related activity to be placed in historical perspective and the activity of each host for a given time interval can be compared to the activities of its peers.

At present, the activity viewer renders two distinct behaviours: 1) whether a host exhibits client or server behaviour or both and 2) scan response behaviour of a host. Figure 1 shows the activity viewer rendering the client-server behaviour for the active hosts in a small network.

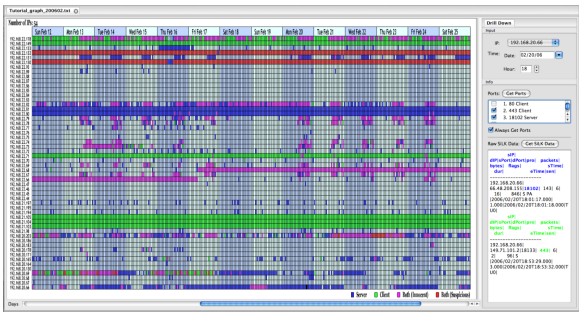

Figure 1: Activity Viewer displaying Client-Server behaviour.

The current implementation displays fourteen days of activity in the main window at one time. This allows the user to view an entire weeks worth of data with a few days from the previous and subsequent weeks for visible context. Activity has been resolved to the hour with each square on the grid representing one hour of activity per host. Each square in the data display is selectable. For each selected data point, the underlying data used to generate the point can be retrieved in the drill down interface on the right side of the main display.