

PQS for Network Security

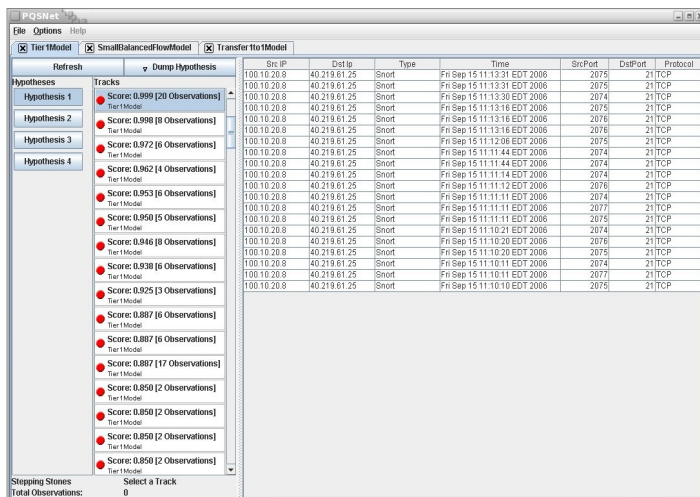
Project description

INTRODUCTION

Modern network environments are protected by dozens of independent, uncoordinated security solutions, that all require individual inspection and viewing. In networks with hundreds of computers the sheer number of virus scanners, log files, personal firewalls, etc can be prohibitive, making it impossible for administrators to review all security information available, and link it with firewall logs, server logs, and intrusion detection systems. Using PQS we have developed a security system that brings together all sources of security information from anywhere in the network, and present it to the administrator in an organized and correlated fashion.

THE APPLICATION

PQS for Network Security offers an enterprise class network security monitoring application that gives a non-stop comprehensive view of the security status of your network, in addition to offering traditional security information management system functionality. Evidence of one attack may be scattered in many different places (think IDS, firewall logs, host and/or server logs). PQS for Network Security collects this information, correlates it, and presents it together to the user. Not only does this save significant amounts of time, it also allows a more in-depth and accurate view of the security status of your network, leading to better protection of your data.

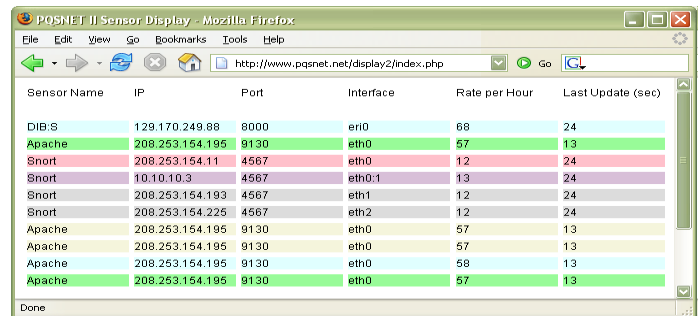


The screenshot shows the PQS application interface. On the left, there is a sidebar with 'Hypotheses 1' through 'Hypothesis 4', each with a score and number of observations. The main window displays a table with columns: Src IP, Dest IP, Type, Time, SrcPort, DestPort, and Protocol. The table contains multiple rows of network traffic data, including Snort and Apache logs.

A FREE VERSION

There is a free version of a PQS based network security application available, complete with model building interface, sensor registry server, and GUI for analysis of the results. This free version comes as a functional demo and is available for download:

<http://www.pqsnet.net/~idesouza/dist/>



The screenshot shows the PQS II Sensor Display web interface in a Mozilla Firefox browser. The browser address bar shows <http://www.pqsnet.net/display2/index.php>. The main content area displays a table with columns: Sensor Name, IP, Port, Interface, Rate per Hour, and Last Update (sec). The table lists various sensors including DIB-S, Apache, and Snort.

PROCESS QUERY SYSTEMS

A PQS is a generic correlation engine that puts the focus on the dynamics of an environment, instead of using traditional static methods. By describing how things change over time, a PQS is able to achieve previously unseen levels of detection and correlation in environments too complex for conventional techniques.

FUNCTIONAL SPECS

This PQS application has the following system requirements (for monitoring up to 1500 hosts):

- PQS platform (either TRAFEN or C-TRACK)
- Pentium 4 or better
- SPARC III or better
- 512 MB RAM
- Java 1.4 or better
- MS Windows XP/2000, Linux 2.6, Solaris > 8

WOULD YOU LIKE TO KNOW MORE?

If you would like to learn more about this PQS application, or if you would like to use this functionality in your environment, please contact:

Vincent Berk
vberk@Dartmouth.EDU
8000 Cummings Hall
Hanover, NH 03755

