Missouri University of Science and Technology
Scholars' Mine

Opportunities for Undergraduate Research Experience Program (OURE)

Student Research & Creative Works

01 Jan 2004

NetExaminer: A Network Visualization Tool

Justin Miller

Follow this and additional works at: https://scholarsmine.mst.edu/oure

Recommended Citation

Miller, Justin, "NetExaminer: A Network Visualization Tool" (2004). *Opportunities for Undergraduate Research Experience Program (OURE)*. 247.
https://scholarsmine.mst.edu/oure/247

This Presentation is brought to you for free and open access by Scholars' Mine. It has been accepted for inclusion in Opportunities for Undergraduate Research Experience Program (OURE) by an authorized administrator of Scholars' Mine. This work is protected by U. S. Copyright Law. Unauthorized use including reproduction for redistribution requires the permission of the copyright holder. For more information, please contact scholarsmine@mst.edu.

NetExaminer: A Network Visualization Tool

Justin Miller

Abstract

The purpose of NetExaminer is to provide a tool that can visualize the condition of a network without communicating with the network being monitored. The application is written for operating systems that support wxWidgets, a cross-platform GUI toolkit. MySQL was used to provide the data for NetExaminer. Whereas most tools for gathering and displaying security related information available today display data in a readout form, NetExaminer attempts to take the data and display it graphically. The NetExaminer software takes data in from MySQL and generates a list of hosts that matches a pre-defined dynamic criteria. The project has been a great success, and the application will soon be able to isolate defective and volatile hosts from any network that is being monitored by NetExaminer's data aggregation software.

Keywords

network visualization, network monitoring, graphical user interface, MySQL applications, wxWidgets

Introduction

Certain tools already exist to provide low-level monitoring of network conditions. Tools such as Ethereal provide packet-level monitoring, but with the sheer quantity of information available on a network, it is difficult to discern the state of security on a network with simple data observation. By combining tools that are capable of aggregating network traffic data and the NetExaminer application, the process of isolating dangerous hosts is simplified.

Requirements for Operation

The current version of NetExaminer requires a machine with a working compiler (GCC), wxWidgets (libraries and headers), MySQL (if database is not hosted elsewhere), and the X graphics system. A database must be established to contain the data acquired by intrusion detection systems (IDS) or port-scanning software.

Data Acquisition

The data necessary for NetExaminer can be retrieved in many ways. NetExaminer operates from data presented in its MySQL database, so examination of real-time or logged data can be achieved by simply modifying the MySQL database.

NetExaminer User Interface

The overall interface to NetExaminer is centered around the primary window. Upon program startup, each window is kept in memory and hidden from the user, allowing for fast access to all windows. Windows are also kept open to allow for communication between

windows, allowing for new information to ripple through each of the windows as it is added. All data once retrieved from the MySQL database is stored in internal data structures within memory to allow for fast access to data. Since all data is retrieved at once, concurrency issues are all but eliminated, due to the locking of data in the database while the query to the database server executes.

Expandability by Design

A database schema can vary from design to design. NetExaminer was designed therefore to operate off of a small set of data, with the ability to integrate more data as it is needed. While NetExaminer requires a database with specific table structure, not every field is required, allowing for expandability (source code is freely available to expand on the original design), in addition to the ability to not use certain fields. Due to indexing, there is a certain amount of information that NetExaminer needs to operate, fields such as IP address would be necessary for correct operation.

Speed Through Open Communication

Windows inside NetExaminer can communicate via adapters (pointers) between the windows, with the main window containing the primary data structures that all windows need to output data. Through the use of adapters, each window can access any piece of data that is used throughout the application, and changes made through the adapters apply to the entire application. This means that if a user of NetExaminer needs to modify a username, for example, the rest of the application is effected, and the username will appear different in all windows.

Figure 1: Data Flow in NetExaminer

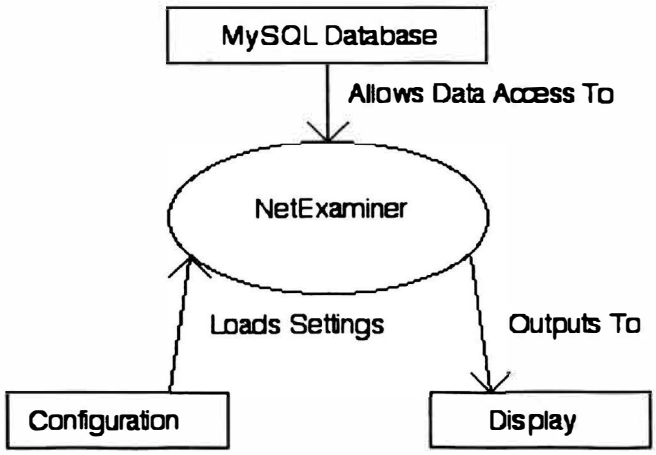


Figure I shows data flow through NetExaminer. Configuration data is loaded from the configuration system (a series of configuration files are read and processed) and MySQL calls are made to access a MySQL database that contains data necessary for NetExaminer's operation. The results obtained from the MySQL database are stored internally and processed by NetExaminer. The processed data is then displayed on the screen.

NetExaminer Configuration

NetExaminer is designed for maximum configurability, and because of this the input must also be configurable.

Cross-Platform Compatibility

By virtue of being written using the wxWidgets toolkit, the NetExaminer application is inherently cross-platform with only a few modifications and a recompile. However, the primary target platform of Linux has presented an excellent alternative for those that do not wish to port it to their target platform. The NetExaminer application can be forwarded over a network using SSH and X, which means that any platform that supports X clients(Windows, OS X, BSD, Linux) can view the application remotely. Examples of this are available in the Screenshots section.

Conclusion

Generic security visualization tools are surprisingly absent from the commercial and free software markets. The open-source community has many free tools for data aggregation, tools such as NMAP (port-scanner), SNORT (lightweight IDS), and Ethereal (packet sniffing). These tools are all excellent resources and work fine for smaller networks, but interpreting the flat log files that these tools generate can be cumbersome for thousands of hosts. With NetExaminer, it is possible to view thousands of hosts, and look only at hosts or groups of hosts that are threatening the network. The modularity of both the configuration and display sections allows for quick changes to both input and output in NetExaminer.

Nomenclature

GUI

GUI is an acronym for Graphical User Interface, and involves the use of a mouse or other input device to navigate a screen interactively, as opposed to a CLI (command line interface), in which data is entered through a keyboard. A GUI toolkit can be used to quickly create applications, and a cross platform GUI toolkit is used to generate applications that can be easily rebuilt on another platform.

Packet-Level Monitoring

Packet-Level Monitoring refers to monitoring traffic across a network at the packet level. Packets are crafted pieces of data that are sent across a network from a source host and decoded at the target host.

Open-Source

Open-Source in the realm of software generally applies to software that has its source code openly available to the public, and does not necessarily imply free use, though in many cases Open-Source is also free.

Intrusion Detection System (IDS)

An intrusion detection system is used to track intrusions made on a network. When coupled with monitoring or an intrusion response system, an IDS can isolate attackers and remove or continue monitoring the intrusion.

Linux

Linux kernel development started in 1992 when Linus Torvalds, a Finnish computer science student, released it to the world on a Usenet group. The Linux kernel is now central to numerous Linux distributions, such as Red Hat, Slackware, SuSE, and Debian. Distributions package tools such as compilers and desktop environments make it easy for developers, users, and server administrators to use. (I)

SSH

SSH stands for secure shell. SSH is essentially a protocol for secure data transmission over a network.

X

X windows is a collection of applications and protocol used as a base for graphical user interfaces on a variety of platforms, including Linux distributions and *BSD releases.

MySQL

MySQL database software is freely available (including source) at http://www.mysql.com. The software is open-source, and is scalable from a small office environment to the corporate level. The wide-spread adoption of MySQL and its inclusion in almost every major Linux distribution. (II)

wxWidgets

Julian Smart created what would become wxWidgets in 1992 to facilitate cross-platform development to avoid the high costs associated with commercially available cross-platform development tools. (III)

Ethereal

Ethereal was originally authored by Gerald Combs, and has since been contributed to by numerous individuals and corporations. Ethereal can analyze data from a network or from a captured file on disk. (IV)

Acknowledgments

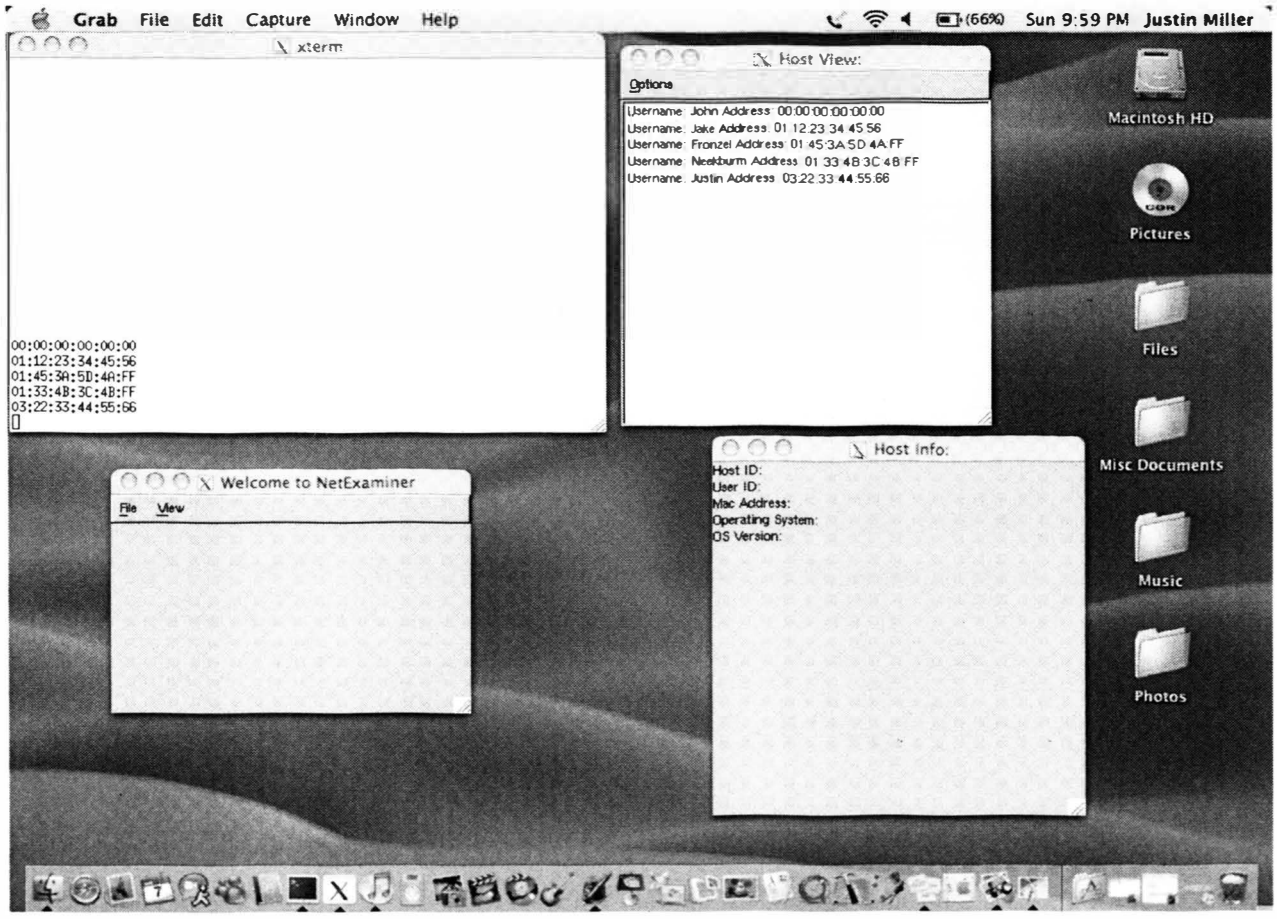
I would like to thank my faculty advisor Dr. Daniel Tauritz (CS) and our partner in the IT department Mr. Brian Buege (Director of Networks and Computing for UMR) for both financial support and research assistance.

Future Work

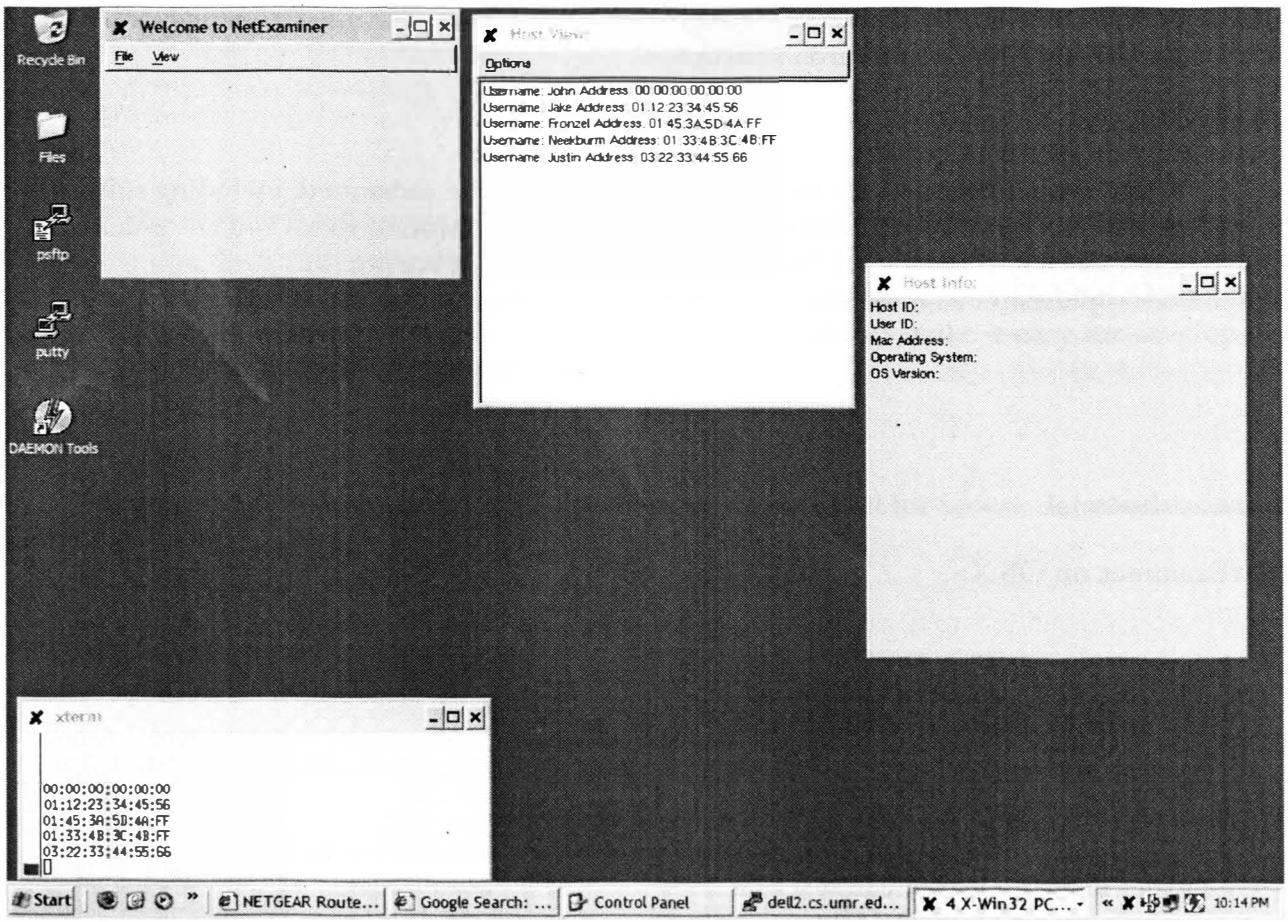
There are numerous ways that NetExaminer could be enhanced, including support for XML(for configuration and data formats), 3d representation of data, and the construction of a database specifically for NetExaminer that would allow for fine tuning of the NetExaminer application to meet the specific needs of a corporation or organization.

Screenshots

NetExaminer on OS X:



NetExaminer on Windows XP:



NetExaminer on SUSE Linux 9.2:

References

1. Linux International - http://www.li.org
2. MySQL - http://www.mysql.com
3. wxWidgets - http://www.wxwidgets.org
4. Ethereal - http://www.ethereal.com