International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 4; Issue: 5; May -2015

CUSTOMIZABLE NETWORK EVENT MANAGER WITH UNIQUE PROTOCOL TRAFFIC

[1]Thirumal K, [2]Mr Ashok B.P
[1]Final Year Student, [2]Assistant Professor
[1,2] Dept. of MCA,The Oxford College of Engineering
Bomannahalli, Bangalore-560068

Abstract : Our application is a powerful tool for analyzing captured data from targeted devices like servers, networks and applications. In addition to these wide varieties of gathering methods supports Business and IT Service, Reporting, dashboard, Discovery and Mapping to facilitate the monitoring and management of your environment. Application is used to monitoring program that capture, stores and also analyzes the reconstructs network events like e-mail, messages, instant messages and voice conversations. Application uses to be here monitoring of all the technology and to gather the required data from the network, then gathered data are saves into the database and reconstructs to it, then it displays this content in an easy-to-understands the format.

Our application helps in-

- Topology Discovery
- Device Monitoring
- Reporting
- Event Collection
- Environmental Monitoring
- Alarm Management
- Configuration Management
- Flow Analysis and Collection

While Application is same to the analyzers in many respects to, it focuses on the protocols are used to communicate with each other .With Application of networking technologies are have to use complex packet and capturing all analysis of software or diagram through network packets in the order to reconstruct the actual data for you presents only the Web pages like e-mails and instant messages or downloaded the files as requested. Application is used by network administrators to enforce to IT policy, parents to be monitor to their children's and those communications.

KEYWORDS: Organizer, Setting and Events.

1. INTRODUCTION

A **computer network** or **data network** is a telecommunications network that allows computers to exchange data. All the computer networks are networked via computing devices to pass their data from one network to another network with the help data connections. The connections are established either using cable or wireless. The best-known computer network is the Internet.

Network computer devices those are completely dependent on network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. When two devices are networked together to exchange information with the other device, it may or

may not have a direct connection to each other.

A networked computers support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications. Physical media in the Computer Network are used to transmit their media signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent.

A computer network follows some properties are:

Facilitate interpersonal communications

People can communicate efficiently and easily through telephone, email, video telephone calls, instant messaging, chat rooms and video conferencing.

Allows data, sharing of files and further types of information

Authorized users may access information store on other computers on the network. Providing an admission to information on storage devices is an important characteristic of many networks.

Allows computing resources and sharing of network

Users may use and access resources provided by devices on the network like print a document on a shared network printer. Distributed computing uses computing resources across a network to complete tasks.

May be insecure

A computer network may possibly used by computer Hackers to deploy computer viruses and to prevent those devices from accessing network or computer worms on devices are attached to the network.

May impede with other technologies

Power line communication strongly disturbs certain form of broadcasting communication such as amateur radio. It may also obstruct with last mile access technologies such as ADSL and VDSL.

May difficult to set up

A computer in complex networks may be tough to set up. It may be expensive to set up an efficient computer network in a large organization.

2. LITERATURE SURVEY

A protocol is a set of laws that govern the interactions between computers on a network. In sort for two computers to speak toward each other with the similar language. Many different types of standards and network protocols are mandatory to make sure that your computer can communicate with more computers placed on the next desk on the world. The OSI (Open Systems Interconnection) Reference replica defines seven layers of networking protocols. The difficulty of these layers is beyond the possibility of this tutorial. However, they can be simplifying into four layers helps to recognize several protocols with which you should be common.

Several protocols overlap the presentation, application and session layers of networks. There are some protocols listed below:

- DNS (Domain Name System) translates network IP address into conditions understand by humans (such as Domain Names).
- DHCP (Dynamic Host Configuration Protocol) can automatically allocate Internet addresses to users and computers
- FTP (File Transfer Protocol) - a protocol that is use to transfer and operate files on the Internet
- HTTP (Hyper Text Transfer Protocol) - An Internet-based protocol use to sending and receiving web page.
- IRC (Internet Relay Chat) - a protocol uses Internet to chat and further interactions.
- POP3 (Post Office protocol Version 3) - e-mail clients uses this protocol to rescue messages from remote servers on the internet.
- SMTP(Simple Mail Transfer Protocol) - An e-mail messages uses this protocol on the Internet

3. BACKGROUND

3.1 ORGANIZER

- **Retention**

  Retention long-term storage of historical data to make possible correlation of data over timing, and to provide the retentions of necessary for compliance requirements which is Long term and log data retentions is significant in forensic investigations as it is not likely that detection of a network violation will be at the time of the break occurring.

- **Forensic analysis**

  The ability to search across logs on dissimilar nodes and time periods based on the specific criteria. And this mitigates having to aggregates the record information in your head having to search thousands of logs.

- **Search**

  Advanced search allows you to search any data virtually in the Application database .The search engine is able of searching for specific data types such as Web page contents, e-mail message headers, URL text, etc.The search fields are precise for every Application plug-in. You can create an alarm and search for the data that has been already captured .There are two type of search: Search Target and Search Set.

- **Names**

  Aliases are easy-to-remember human understandable names that can substitute IP address or MAC displayed in the Event View and View Group sections of the program's main window will be make it easier to recognize network events and also examine it. Once an alias is assigned to MAC or the IP address, it will be replaced the corresponding of address in the

Event View and Group View sections of the major window. Which you can choose how the hosts are participating in the communications are displayed by MAC Address, by IP Address, or by Host Alias

- **Database**

Application database should have all captured and analyzed network information. At some point the database may extend too large and this will be affect to the programs performance and on the other hand, it will be some records become outdated over time and are no longer needed. We can use different options for managing data base like delete, export, import, delete select and restore.

3.2 SETTINGS

- **Compliance**

Applications can be employed to automate the assembly of compliance the data and producing the reports to that adapt to present the security and governance and auditing processes

- **Setup**

The adapter selection screen has a descend list that allows you to identify the correct network adapter for monitoring. If the computer is connected either by dial-up or LAN by an Ethernet adapter, you would have a just one adapter in the menu and you need to select it that. If your computer is serves as the gateway and Internet for the LAN and has more than one network adapter, you want to select for the adapter that you would like Application to monitor.

- **View**

The Group View shows network actions grouped by the date they occurred, network protocols and hosts unavailable in communications. Checking or upchucking the boxes next to a group will incorporate/exclude the events that belong to the collection to/from the Event List. The hosts are grouped into Parties that illustrate the parties involved in the communication process on network. Party A includes a hostname on the restricted side of the communication. Though, while using your LAN adapter as the main Internet connections method, but also use you're Dial-Up of adapter rarely or assign the IP address dynamically to your computer each time you connect. Party B includes remote hosts which are communicated with the local host(s).

3.3 EVENTS

- **Data aggregation**

Log management aggregates the data from many sources which including applications, databases, servers, security and network providing the ability to secure monitored data to help avoid missing crucial events.

- **Network**

An application shows the data exchange on the network in the network events form. An example for event is a file

downloaded via FTP, a downloaded Web page, or an ICQ instant message and an e-mail message. When we configured the data filtering options, the Event List section will displays the raw list of events that Application filtered from the database for you**.**

Application is a potent network monitoring application that presents a comprehensive picture of users in the network activities. On a busy network you can see more than thousands of network events such as instant messages, web pages and e-mail messages etc.

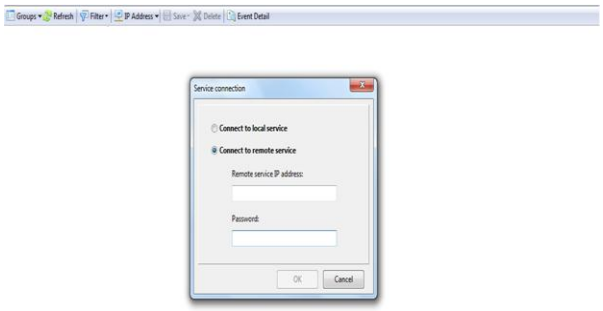
4. IMPLEMENTATON

Over the past a number of years there have been explosive growth in IT, leading to the ever-increasing complexity of corporate networks. Much of this difficulty is an indirect result of the improved use of the Internet and cloud-based systems by businesses, thereby forcing them to extend and expand their IT infrastructures. The result of this expansion and increased complexity is an increase in the number of threats and vulnerabilities causing information security incidents to grow so fast that it has now become a major concern for small and large business enterprises globally.

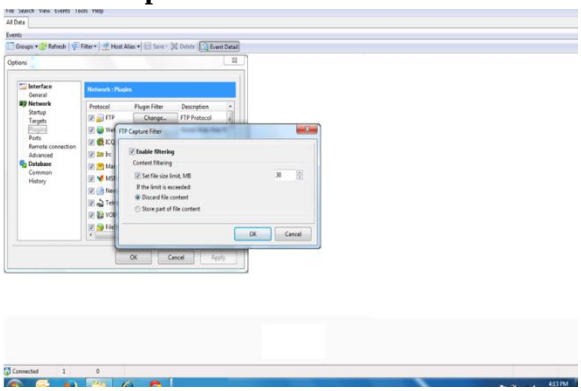
Most of the security devices implemented today provides alerting and logging of known and possibly unknown security actions that occur on IT systems and infrastructures. However, although continuing advance in technology and implementation of security devices such as VPNs and firewalls. Many companies do not monitor the information coming from these devices. Monitoring for security events takes experienced security analysts who have the ability to analyze individual events and filter out the false positives. For most organizations, a large number of fake positives are difficult to manage because they do not have a enthusiastic security staff and people are taken away from their normal responsibilities to spend time responding to false attacks.

5. RESULT

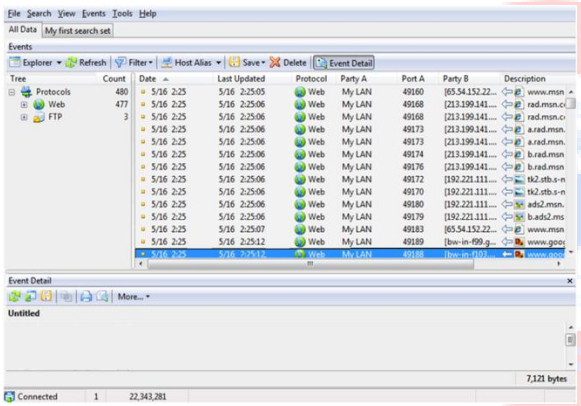
Connection login



FTP filter option



Showing event details for selected activity



7. FUTURE ENHANCEMENTS

With rapid and advances in this competitive environment it is difficult to predict how business will improve and expand in the coming years. Though we have some advance plans for the future enhancements in the current project.

- We can implement practice mode so that new or basic users can have a full idea of the application, it will help user to be comfortable with the tool.
- We can implement more graphical reporting option for more flexible reporting.

6. CONCLUSION

This software helps Improve customer service perception and satisfaction, Increase accessibility through a single point of contact, communication, and information, Increase productivity of support staff by automating processes, policies, and tasks, Reduce IT support costs. The different modules of the project are complete enough to manage and handle the overall process of Network content monitoring.

- Enables you to perform complex queries and notate credentials of interest for investigation
- Helps to facilitate conformity with industry regulations and government
- Provides nationwide Language Support for native language search
- Allows you to delegate authorized end-users to exclude from alerts

8. References

[1] Harry Arden (2011, Feb. 3), Tropical Disease, Online! Tropical Disease", [online], https://play.google.com/store/search?q=tropical+disease&c=apps (Accessed: 28 Feb 2013).
[2] SUSASOFTX (2013), Human Anatomy, Online! Human Anatomy", [online], https://play.google.com/store/search?q=human+anatomy&c=apps (Accessed: 13 Feb 2013).